universität wien

DISSERTATION

Titel der Dissertation

„Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung in Österreich“

Verfasser

Mag. Christof Tschohl

angestrebter akademischer Grad

Doktor der Rechtswissenschaften (Dr. Jur.)

Wien, 14.10.2011

Studienkennzahl lt. Studienblatt:		A 083 101
Dissertationsgebiet lt. Studienblatt:	lt.	Rechtswissenschaften
Betreuerin / Betreuer:		Prof. Dr. Hannes Tretter

Vorwort und Danksagung

Die Fertigstellung meiner Dissertation markiert einen Meilenstein meiner rechtswissenschaftlichen Ausbildung. Dass damit zugleich die fachliche Brücke zu meiner beruflichen Vergangenheit als Ingenieur der Nachrichtentechnik gebaut wurde, erfüllt mich mit großer Zufriedenheit. Wenn ich nun allen Menschen namentlich danken würde, von denen ich auf meinem Weg dahin Unterstützung erfahren habe, würde das wohl den Rahmen überspannen. All jenen, die hier nicht namentlich erwähnt werden, obwohl sie es verdient hätten, sei daher - passend zum Thema dieser Arbeit - anonym aber nicht weniger herzlich gedankt.

Mein innigster Dank gilt meiner Frau Karen und meinem Sohn Radek, die mit Ihrer positiven Energie Tag für Tag meinen Energiehaushalt auf einem konstant hohen Niveau gehalten haben, umso mehr, als sie mich in der finalen Phase der Fertigstellung dieser Arbeit wohl mehr als Phantom denn als Familienvater wahrgenommen haben. Meinen Eltern und meiner Schwester samt ihrer Familie danke ich für all die Jahre der emotionalen Geborgenheit während meiner Ausbildung. Große Dankbarkeit aussprechen möchte ich auch all meinen Kolleginnen und Kollegen am Ludwig Boltzmann Institut für Menschenrechte (BIM), die mir in den vergangenen vier Jahren eine nicht nur wissenschaftliche Heimat geworden sind. Diese Dissertation basiert auf einem Forschungsprojekt, für dessen Etablierung ich am BIM die Freiheit und die Basis gleichermaßen vorgefunden habe.

Weiters danke ich den vielen Menschen, von denen ich in den zahlreichen Fachdiskussionen im Rahmen der gesamten Arbeit zur Vorratsdatenspeicherung enorm viel gelernt habe, sodass ich an meiner Aufgabe wachsen konnte. Den Respekt, mit dem man sich auch bei inhaltlich nicht selten kontroversen Diskussionen stets begegnet ist, weiß ich sehr zu schätzen. Schließlich gilt mein besonderer Dank meinen lieben Kollegen Markus Kemptner und Ermano Geuer, die mit Ihrer sorgfältigen Durchsicht sowie durch zahlreiche Gespräche zum Thema einen großen Beitrag zur Qualitätssicherung dieser Arbeit geleistet haben.

Beschließen möchte ich dieses Vorwort mit einem Zitat, dass mir durch viele Jahre meiner wissenschaftlichen Ausbildung ebenso Geleit wie Mahnung war und hoffentlich bleiben wird:

„Bescheidenheit ist Einsicht in die Grenzen der Erkenntniskraft“ (Hans Kelsen)

Wien, 15. Oktober 2011 Christof Tschohl

Inhalt – Überblick

Inhaltsverzeichnis

EINLEITUNG

Die vorliegende Arbeit ist eine rechtswissenschaftliche Untersuchung der Datensicherheit im Rahmen der österreichischen Umsetzung der Vorratsdatenspeicherung gemäß der Richtlinie 2006/24/EG, welche die flächendeckende vorrätige Speicherung von Telekommunikationsverbindungs- und Zugangsdaten durch alle Anbieter öffentlicher elektronischer Kommunikationsnetze und -Dienste innerhalb der EU vorschreibt. Die Bereitstellung solcher Dienste beinhaltet regelmäßig die Verarbeitung von personenbezogenen Daten der Nutzer. Die österreichische Umsetzung der Richtlinie erfolgte durch eine Novelle zum Telekommunikationsgesetz (TKG 2003) und wurde am 18. Mai 2011 im Bundesgesetzblatt kundgemacht (BGBl. I Nr. 27/2011), wobei die Speicherverpflichtung für die Anbieter erst mit 1.4.2012 in Kraft treten wird. Das Gesetz enthält jedoch zur Datensicherheit nur relativ grobe Vorgaben, die detaillierte Ausgestaltung bleibt einer Verordnung in Ausführung der §§ 94 Abs. 4 und 102c TKG vorbehalten. Um dem Datenschutzgesetz und dem Telekommunikationsgeheimnis sowie den Vorgaben der Europäischen Menschenrechtskonvention, insbesondere dessen Artikel 8 zum Schutz des Privatlebens und der Korrespondenz zu entsprechen, müssen diese Daten geheim gehalten werden, wozu insbesondere auch Maßnahmen auf der technischen Ebene notwendig sind, die auf der rechtlichen Ebene erfasst und beschrieben werden müssen. Die Verpflichtung zur effektiven Wahrung der Grundrechte aller Nutzer erfordert dabei auch, ein System einer revisionssicheren Protokollierung zu etablieren und so eine ausreichende Nachvollziehbarkeit für den Rechtsschutz zu gewährleisten.

Die Zielsetzung dieser Dissertation ist, im ersten Teil (Kapitel II) ausgehend von den Grundrechten und dem Europarecht bis hin zur innerstaatlichen Umsetzung den normativen Unterbau zu evaluieren, der für die Beschreibung eines Sorgfaltsmaßstabs auf rechtlicher und technischer Ebene bei der Verarbeitung und Übermittlung von Verkehrsdaten relevant ist, unter besonderer Beachtung eines hohen Niveaus an Datensicherheit und Grundrechtsschutz. Die Arbeit behandelt sowohl das Thema der Datensicherheit bei den Anbietern unternehmensintern, als auch im Zusammenhang mit der Übermittlung von personenbezogenen Daten im Falle einer Auskunft an Sicherheits- und Strafverfolgungsbehörden. Da in der Praxis der Schwerpunkt der Datensicherheitsprobleme eindeutig bei der sicheren Übermittlung der Daten liegt, steht im Zentrum des zweiten Teils ein Konzept einer zentralen Datendrehscheibe (Kapitel III). Die sogenannte „Durchlaufstelle“ (DLS) wird in der Arbeit als Referenzmodell entwickelt und dargestellt. Personenbezogene Inhalte werden nach diesem Konzept verschlüsselt zwischen Absender und Empfänger ausgetauscht und sind der DLS nicht zugänglich. Die Beteiligten sind über gesicherte Transportverbindungen mit fortgeschrittenen Signaturen angebunden, identifiziert und authentifiziert. Das System wirkt durch die zentrale Protokollierung aller Auskunftsvorgänge auch auf die Datensicherheit beim Anbieter und die Rechtsschutzmöglichkeiten zurück.

Im Dritten Teil werden im Speziellen insgesamt 13 wesentliche Problemkreise und deren Fragestellungen diskutiert, die für die Praxis mit den Anforderungen an eine sichere Datenübermittlung einhergehen. Die Behandlung jedes Problemkreises schließt mit einem konkreten Vorschlag, wie den jeweiligen Fragen im Rahmen einer Umsetzungsverordnung zur Datensicherheit begegnet werden könnte, um den Vorgaben aus der normativen Analyse des ersten Teils zu entsprechen. Technische Anforderungen werden dabei normativ entsprechend formuliert, um die wesentlichen Funktionen technischer Hilfsmittel rechtlich hinreichend zu determinieren.

I.1 Motivation und Hintergrund

Von November 2009 bis Jänner 2010 befand sich ein Entwurf des Bundesministeriums für Verkehr, Innovation und Technologie (BMVIT) für eine Novelle des Telekommunikationsgesetztes (TKG) zur Umsetzung der „Vorratsdatenspeicherungsrichtlinie“ 2006/24/EG in öffentlicher Begutachtung. Der Begutachtungsentwurf wurde im Auftrag des BMVIT vom Ludwig Boltzmann Institut für Menschenrechte (BIM) erarbeitet, wobei der Autor dieser Dissertation als wissenschaftlicher Mitarbeiter des BIM für die Projektkoordination und die Entwicklung der Inhalte verantwortlich war. Der im Folgenden als „BIM-Entwurf TKG-Novelle 2010“[1] bezeichnete Vorschlag für eine TKG-Novelle ist von hohen grundrechtlichen Anforderungen als Zielsetzung geprägt, um den massiven und flächendeckenden Eingriff in die Grundrechte aller Nutzer durch die Vorratsdatenspeicherung in möglichst engen Grenzen zu halten. Der BIM-Entwurf wurde in der Folge in der politischen Diskussion noch an manchen Stellen abgeändert, blieb aber weitgehend und speziell in seiner wesentlichen Struktur erhalten. Die geänderte Fassung wurde schließlich im Parlament beschlossen und am 18. Mai 2011 im Bundesgesetzblatt kundgemacht (BGBl. I Nr. 27/2011), wobei die Speicherverpflichtung für die Anbieter erst mit 1.4.2012 in Kraft treten wird.

Da die Gesetzesnovelle notwendigerweise die Vorgaben zur Datensicherheit nur auf relativ abstraktem Niveau formuliert und die nähere Ausgestaltung in den §§ 94 Abs. 4 und 102c TKG einer Verordnung überlässt, wurde vom Autor dieser Dissertation in Eigeninitiative in seiner Eigenschaft als wissenschaftlicher Mitarbeiter des BIM ein Konzept für eine Studie zur Datensicherheit erarbeitet und dem BMVIT im Frühjahr 2010 vorgelegt. Die Forschungsmittel für eine unabhängige wissenschaftliche Studie nach dem vorgelegten Konzept zur Erhebung der praktisch bedeutsamsten Fragestellungen zur Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung wurden schließlich im Juni 2010 bewilligt. Finanziert wurde die Studie mit Forschungsmitteln des BMVIT als dem primären Nutznießer der Erkenntnisse, jedoch ohne Vorgaben zur inhaltlichen Gestaltung zu den Ergebnissen. Der Autor dieser Dissertation war als Projektkoordinator - unter der fachlichen Aufsicht des Projektleiters Professor Hannes Tretter, zugleich Betreuer dieser Dissertation - allein verantwortlich für das Konzept und die Ausarbeitung der genannten Studie sowie für die Moderation und sachliche Gestaltung der Round Table Veranstaltungen. Die Ergebnisse wurden festgehalten und als fachliche Grundlage für den Fortschritt der in Verbindung stehenden rechtspolitischen Diskussion aufbereitet. Die Konklusion der Studie besteht in einem konkreten Vorschlag für eine Datensicherheitsverordnung basierend auf §§ 94 Abs. 4 und 102c TKG.

Die Endfassung der Studie wurde im Juli 2011 an die Forschungsförderungsabteilung im Rahmen der FFG Administration des BMVIT übermittelt. Seit der Vorlage des Konzepts für die Studie war gegenüber allen Beteiligten offengelegt, dass es sich dabei zugleich um das Dissertationsprojekt des Studienautors handelt, weshalb der Autor zugleich die uneingeschränkten wissenschaftlichen Verwertungsrechte daran hält. Die Studie ist auf der Website des BIM online publiziert.[2] Obwohl die BIM-Datensicherheitsstudie die Basis für diese Dissertation darstellt, lässt sie sich in ihrer Zielsetzung

---

[1] Begutachtungsentwurf des Bundesministeriums für Verkehr, Innovation und Technologie (BMVIT), ausgearbeitet vom Ludwig Boltzmann Institut für Menschenrechte (BIM) im Auftrag des BMVIT, von 15.11.2009 bis 15.1.2010 in öffentlicher Begutachtung: <http://www.parlinkom.gv.at/PG/DE/XXIV/ME/ME_00117/pmh.shtml> (11.10.2011) [= BIM-Entwurf TKG Novelle 2010];

[2] http://bim.lbg.ac.at/de/digital-rights/studie-zur-datensicherheit-umsetzung-vorratsdatenspeicherung.

doch klar von der Dissertation abgrenzen. Im Fokus der Studie steht die empirische Aufarbeitung der Problemlage und deren Dokumentation, sowie daran anknüpfend der konkrete Vorschlag für eine Umsetzungsverordnung. Die Dissertation hingegen fokussiert darauf, die Zusammenhänge zwischen den normativen Vorgaben des ersten Teils theoretisch mit den jeweiligen Lösungsvorschlägen im dritten Teil zu verbinden und zu erläutern, wobei das im zweiten Teil entwickelte Konzept der „Durchlaufstelle" das Referenzmodell darstellt. Überschneidungen zwischen der BIM-Datensicherheitsstudie und dieser Dissertation bestehen daher vor allem in den Kapiteln II und III, wenngleich die Dissertation hier weiter in die Tiefe geht. Daher wird in diesen Kapiteln davon abgesehen, laufend auf die Studie zu referenzieren. Dort wo die Dissertation in diesen Kapiteln gegenüber der Studie wesentliche Ergänzungen enthält, wird dies explizit angemerkt. In Kapitel IV wird demgegenüber direkt aus der Studie zitiert, soweit dies einen sachlichen Mehrwert birgt, insbesondere bei Verweisen auf den empirischen Teil der Studie.

Der die Studie abschließende Vorschlag für eine Verordnung wurde vom BMVIT aufgegriffen[3] und Anfang August 2011 bis zum 20. September in öffentliche Begutachtung geschickt. Da der Begutachtungsentwurf nach Ende der Begutachtungsfrist auf der Webseite des BMVIT online nicht mehr abrufbar war, wird der gesamte Verordnungsentwurf samt Vorblatt und Erläuterungen vollständig als Anhang dieser Dissertation abgedruckt. In Kapitel IV wird der Verordnungsentwurf nach der BIM-Datensicherheitsstudie überdies im jeweiligen sachlichen Zusammenhang dem Begutachtungsentwurf gegenüber gestellt und allfällige Änderungen werden diskutiert. Der Entwurf zur Verordnung steht nach dem Verlauf der Round Table Diskussionen im Rahmen der BIM-Datensicherheitsstudie auf der Basis eines breiten fachlichen Konsenses und ist durch einen für österreichische Verordnungen unüblich hohen technischen Determinierungsgrad bei gleichzeitiger technologieneutraler Formulierung gekennzeichnet.

Die Verordnung soll nach allfälliger Überarbeitung vom BMVIT im Einvernehmen mit BM.I und BMJ im Spätherbst 2011 erlassen werden. Da der genaue Termin für die Erlassung der Verordnung jedoch ungewiss ist - zumal über die Kostenteilung unter den beteiligten Bundesministerien noch kein Konsens besteht - und um die Arbeit an einem klar abgrenzbaren Punkt abzuschließen, wird für die Dissertation die Zäsur mit dem Begutachtungsentwurf gezogen, zumal die Darstellung ihrer Ergebnisse unabhängig von der politischen Umsetzung stehen kann und auch im Falle einer späteren Umsetzung nicht unvollständig wird. Eingearbeitet wurden bis zur Abgabe noch die beim BMVIT eingelangten Stellungnahmen aus dem Begutachtungsverfahren zum Verordnungsentwurf. Diese Stellungnahmen wurden zwar grundsätzlich nicht veröffentlicht[4], sie wurden dem Autor aber zum Zweck der Berücksichtigung in dieser Dissertation durch das BMVIT zur Verfügung gestellt.

[3] Unter ausdrücklicher Berufung auf die Studie im „Vorblatt zum Entwurf der Datensicherheitsverordnung", vgl. http://www.bmvit.gv.at/ministerium/begutachtungsverfahren/downloads/tkg_dsvo_vorblatt.pdf.

[4] Eine Ausnahme stellt die Stellungnahme des Dachverbands der Internet Service Provider Austria (ISPA) dar, die auf der Website der ISPA veröffentlicht wurde, zur Fundstelle siehe das Literaturverzeichnis.

II THEORETISCHE RECHTLICHE GRUNDLAGEN MIT RELEVANZ FÜR DEN TECHNISCHEN SORGFALTSMAßSTAB ZUR DATENSICHERHEIT

II.1 RECHTLICHE RAHMENBEDINGUNGEN

In diesem Kapitel werden die rechtlichen Rahmenbedingungen dargestellt, deren Vorgaben Auswirkungen auf die Gestaltung der Datensicherheitsmaßnahmen für die Verwendung von Vorratsdaten haben. Den Ausgangspunkt bilden dabei jene Grundrechtsgarantien, die von der Vorratsspeicherung von Telekommunikationsdaten primär berührt sind. Die Einleitende Darstellung der Entwicklung vom Briefgeheimnis aus 1867 bis zum Fernmeldegeheimnis aus 1975 soll dabei ein besseres Verständnis der Zusammenhänge zwischen rechtlichem und technischem Fortschritt fördern. Die Schutzbereiche der jeweiligen Grundrechte werden dabei nicht umfassend dargestellt sondern vielmehr auf die gegenständlichen sachlichen Problemstellungen fokussiert. Die Abhandlung der grundrechtlichen Ebene wird gefolgt von Ausführungen zu den unionsrechtlichen Grundlagen aus der Vorratsdatenspeicherungs-Richtlinie 2006/24/EG. Diese wird eher knapp gehalten, zumal die Regelungen dieser Richtlinie für die in dieser Arbeit fokussierten Fragestellungen nicht allzu ergiebig sind. Eine ausführlichere Darstellung der einfachgesetzlichen Rechtslage in Österreich nach der Umsetzung der Vorratsdatenspeicherungsrichtlinie bildet den Abschluss zur Evaluierung des normativen Unterbaus im Rahmen dieses Kapitels.

II.1.1 RELEVANTE GRUNDRECHTSGARANTIEN

II.1.1.1 BRIEFGEHEIMNIS 1867 (ART 10 STGG)

Allein das Wissen über Kommunikationsvorgänge – selbst ohne Kenntnis des Inhalts – lässt in Zusammenschau mit den Begleitumständen häufig Rückschlüsse auf deren Inhalt zu. Gleichwohl schützt das Briefgeheimnis - zumindest in Österreich[5] – explizit nur den Inhalt, nicht jedoch die „äußeren“ Daten, also Absender, Empfänger, Zeit und Ort der Nachrichtenübermittlung. Diese Einschränkung des Briefgeheimnisses auf den Inhalt von schriftlichen Botschaften ist eingedenk der technischen Möglichkeiten zur Zeit der Entstehung dieses Persönlichkeitsrechtes im 19. Jahrhundert nicht weiter verwunderlich. Das Briefgeheimnis wurde erstmals 1848 im sog. „Pillersdorf’schen Verfassungsentwurf“ in § 20 ausdrücklich vorgesehen[6] und fand auch Eingang in den weitaus grundrechtsfreundlicheren „Kremsierer Entwurf“ aus demselben Jahr.[7] Nachdem die Kaiserliche Reaktion aber allmählich wieder die Oberhand gewann, wurde der für seine Zeit gerade im Hinblick auf seine Grundrechtsgarantien äußerst fortschrittliche jedoch niemals in Kraft getretene Kremsierer

5 Vgl im Gegensatz dazu den weiteren Schutzbereich des Art 10 des deutschen Grundgesetzes (GG), der Organen der öffentlichen Gewalt nicht nur die Kenntnisnahme des Inhalts verwehrt, sondern auch Absender und Empfänger schützt. Im Unterschied zum österreichischen Briefgeheimnis fallen nach dem deutschen Grundgesetz nicht nur Briefe im engeren Sinn sondern auch Telegramme und Postkarten in den Schutzbereich des Briefgeheimnisses; vgl. Weber-Fas, Der Verfassungsstaat des Grundgesetzes, Tübingen 2002, 109.

6 Laurer, Der Geheimnisschutz im österreichischen Grundrechtssystem, EuGRZ 1983, 29.

7 Zum Kremsierer Entwurf vgl. Resch, Entwicklung der Grundrechte in Österreich, Wien 1990, 43f; Text dokumentiert unter http://www.verfassungen.de/at/verfassungsentwurf49-i.htm, (11.10.2011).

Entwurf am 4.3.1849 durch die sog. „oktroyierte Märzverfassung“[8] ersetzt. Obwohl diese am Kremsierer Entwurf orientierte Verfassung in ihrem III. Abschnitt („von dem Reichsbürgerrechte“) auch einen, wenngleich knapp geratenen, Grundrechtskatalog enthält, findet sich dort bemerkenswerter Weise der Schutz des Briefgeheimnisses nicht mehr. Dies erscheint angesichts des kaiserlichen Verlangens nach mehr Kontrolle über seine widerstrebenden Bürger nur konsequent. Erst nach der Zeit des so genannten „Neoabsolutismus“, der durch die Silvesterpatente des Kaisers vom 31.12.1851 eingeleitet wurde und die Märzverfassung noch vor deren tatsächlicher Wirksamkeit außer Kraft setzte, findet das Briefgeheimnis schließlich Eingang in die österreichische Verfassungsordnung, konkret durch die Dezemberverfassung vom 21.12.1867[9]. Wesentlicher Bestandteil dieser Verfassung war das „Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger für die im Reichsrate vertretenen Königreiche und Länder“, welches als StGG 1867[10] nach wie vor und großteils unverändert[11] einen wesentlichen Bestandteil der österreichischen Grundrechtsordnung bildet. Das StGG 1867 garantiert in Art 10: „Das Briefgeheimnis darf nicht verletzt und die Beschlagnahme von Briefen, außer dem Fall einer gesetzlichen Verhaftung oder Hausdurchsuchung, nur in Kriegsfällen oder auf Grund eines richterlichen Befehls in Gemäßheit bestehender Gesetze vorgenommen werden“.

II.1.1.2 Fernmeldegeheimnis 1975 (Art 10a StGG)

Aus dem Briefgeheimnis als systematisches und dogmatisches Vorbild entstand im Jahr 1974 das Fernmeldegeheimnis[12] in Art 10a StGG[13] und trat am 1.1.1975 in Kraft. Zweck des Fernmeldegeheimnisses ist die informationelle Selbstbestimmung und die freie Entfaltung der Persönlichkeit. Technisch muss man sich im Jahr 1975 ein sogenanntes Wählamt, also die Vermittlungsstelle der Telefongesellschaft, als einfache Relais-Station vorstellen. Wer mit wem wann wie lange telefoniert, kann diese rein technisch gar nicht erfassen und protokollieren. Wenn Sie damals über einen „Viertel-Anschluss“ verfügten, wusste höchstens der Nachbar, dass Sie schon wieder stundenlang die Leitung blockieren. Ob der Schutz des neuen Grundrechts - über den nur ein

---

8 Zur oktroyierten Märzverfassung vgl. Resch, Entwicklung der Grundrechte in Österreich, Wien 1990, 46f; Text dokumentiert unter http://www.verfassungen.de/at/verfassung49-i.htm (11.10.2011).

9 Staatsgrundgesetz vom 21. Dezember 1867 betreffend die allen Ländern der österreichischen Monarchie gemeinsamen Angelegenheiten und die Art ihrer Behandlung, RGBl. 146/1867;

10 Staatsgrundgesetz vom 21. Dezember 1867 über die allgemeinen Rechte der Staatsbürger für die im Reichsrate vertretenen Königreiche und Länder, RGBl. 142/1867, in Kraft seit dem 23. Dezember 1867, außer Kraft vom 1. Juli 1934 bis 1. Mai 1945; das StGG gilt gemäß Artikel 149 Abs 1 B-VG auch heute noch als Verfassungsgesetz der Republik Österreich fort.

11 Änderungen erfolgten durch: den Staatsvertrag von St.-Germain-en-Laye vom 10. September 1919, StGBl. 303/1920; Gesetz vom 1. Oktober 1920, womit die Republik Österreich als Bundesstaat eingerichtet wird (Bundes-Verfassungsgesetz), BGBl. Nr. 1/1920; BVG vom 29. November 1973, mit dem das Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger durch die Einfügung einer Bestimmung zum Schutze des Fernmeldegeheimnisses geändert wird, BGBl. 8/1974; BVG vom 12. Mai 1982, zur Änderung des Staatsgrundgesetzes über die allgemeinen Rechte der Staatsbürger durch die Einfügung einer Bestimmung zum Schutz der Freiheit der Kunst, BGBl. Nr. 262/1982; BVG vom 29. November 1988, über dem Schutz der persönlichen Freiheit, BGBl. Nr. 684/1988.

12 Die Patenschaft des Briefgeheimnisses ist unumstritten; siehe die EB zu 10a StGG, AB 960 BlgNR 13. GP, 2; *Funk/Krejci/Schwarz*, Zur Registrierung von Ferngesprächsdaten durch den Gesetzgeber, DRdA 1984, 285; *Wiederin,* Art 10a StGG, in: *Korinek/Holoubek* (Hrsg), Österreichisches Bundesverfassungsrecht Bd. III, Rz 3.

13 BVG vom 29. November 1973, mit dem das Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger durch die Einfügung einer Bestimmung zum Schutze des Fernmeldegeheimnisses geändert wird, BGBl. 8/1974.

Richter verfügen darf - auch Verbindungsdaten umfasst, war bei dessen Entstehung allein deshalb gar kein Thema. Inhaltsüberwachung („Abhören“) hingegen war damals technisch relativ einfach, man musste nur ein Telefon über zwei Drähte parallel schalten. Das Fernmeldegeheimnis sollte daher jener Gefahr für die Vertraulichkeit der Mitteilung entgegentreten, die sich gerade aus der Einschaltung eines Übermittlers ergibt. [14] Insofern besteht der grundrechtliche Schutz des Art 10a StGG jedenfalls, solange die technischen Einrichtungen des Telekommunikationsunternehmens für den Kommunikationsvorgang in Anspruch genommen werden. Schutz bestünde demnach quasi nur, solange die Kommunikation „in der Röhre“ ist. 1975 bestand aufgrund der technischen Möglichkeiten wenig Gefahr einer anderweitigen Aufzeichnung von Kommunikationsvorgängen, im Unterschied zu den digitalen Medien der heutigen Zeit, vor allem dem „Medium E-Mail“, und insbesondere in Verbindung mit der Möglichkeit, komplexe Datenbanken über die äußeren Kommunikationsdaten (Verkehrsdaten) anzulegen.

Zum Zeitpunkt des Inkrafttretens orientierte sich der Begriff des Fernmeldeverkehrs am FernmeldeG, BGBl 1949/170, wobei sich aus den Materialien zu Art. 10a StGG ergibt, dass der historische Verfassungsgesetzgeber einen weiten Begriff vor Augen hatte.[15] Grundrechtlichen Schutz genießt jede Kommunikation, die nicht für die Öffentlichkeit bestimmt ist.[16] Ob die Kommunikation privaten oder öffentlich bekannten Inhalt hat, ist nicht ausschlaggebend für den Schutz.[17] Träger des Grundrechts sind sowohl der Anschlussberechtigte als auch die jeweiligen Benutzer der Anlage.[18] Aus technischer Sicht erfasst das Fernmeldegeheimnis bestimmte Vorgänge der Kommunikation über ein Kommunikationsnetz. Zur Erschließung dieser auslegungsbedürftigen Begriffe erscheint ein Rückgriff auf die Legaldefinition des Begriffs „Kommunikationsnetz“ in § 3 Z 11 TKG zweckmäßig und zulässig. Erfasst ist demnach die elektronische Übertragung von Signalen über Kabel, Funk, optische oder andere elektromagnetische Einrichtungen, einschließlich Satellitennetze, feste (leitungs- und paketvermittelte, einschließlich Internet) und mobile terrestrische Netze, Stromleitungssysteme, soweit sie zur Signalübertragung genutzt werden, Netze für Hörfunk und Fernsehen sowie Kabelrundfunknetze (Rundfunknetze), unabhängig von der Art der übertragenen Informationen. Damit unterliegt – im Hinblick auf den Regelungsbereich der RL 2006/24/EG – neben der Festnetz- und Mobiltelefonie auch die Kommunikation via E-Mail bzw. „Voice over IP“ dem Fernmeldegeheimnis.

II.1.1.2.1 Verkehrsdaten im Schutzbereich des Fernmeldegeheimnisses?

Seit vielen Jahren wird in Österreich innerhalb juristischer Fachkreise kontrovers diskutiert, ob das Fernmeldegeheimnis nur die Inhalte der Kommunikation oder auch die äußeren Informationen zum Kommunikationsvorgang, also die sogenannten Verkehrsdaten[19] umfasst. Die Diskussion dreht sich um die Frage nach dem zeitlichen wie auch dem sachlichen Schutzbereich. Die strafrechtliche

[14] *Badura,* Art 10 GG, Bonner Kommentar, 136. Aktualisierung, Oktober 2008, Rz 52.
[15] Ab 960 BlgNr 13. GP, 2. zitiert nach *Wiederin,* Art 10a StGG, in: *Korinek/Holoubek* (Hrsg), Österreichisches Bundesverfassungsrecht Bd. III, Rz 6.
[16] *Wiederin,* Art 10a StGG, in: *Korinek/Holoubek* (Hrsg), Österreichisches Bundesverfassungsrecht Bd. III, Rz 7.
[17] *Wiederin,* Art 10a StGG, in: *Korinek/Holoubek* (Hrsg), Österreichisches Bundesverfassungsrecht Bd. III, Rz 3.
[18] *Wiederin,* Art 10a StGG, in: *Korinek/Holoubek* (Hrsg), Österreichisches Bundesverfassungsrecht Bd. III, Rz 10.
[19] Zur genauen Definition, was unter Verkehrsdaten zu verstehen ist.

Rechtsprechung und Lehre[20] geht davon aus, dass auch Verkehrsdaten geschützt sind, die nach dem Abschluss des Kommunikationsvorgangs als (technische) Protokolldaten gespeichert bleiben.[21] Dieser Ansicht widerspricht ein Teil der staatsrechtlichen Lehre[22], demzufolge wäre die weitere Verwendung von Verkehrsdaten nach Abschluss der Kommunikation nicht erfasst. Bei dieser Kontroverse ist zu bedenken, dass mit der technischen Entwicklung der letzten drei Jahrzehnte Fragen und Probleme aufgetreten sind, die 1974 bei der Entstehung des Fernmeldegeheimnisses gar nicht vorstellbar waren, weshalb eine rein historische Interpretation des Schutzbereichs dem Schutzzweck nicht gerecht werden kann.

Sieht man den Schutzbereich des Art 10a StGG nur auf einen bestimmten Kommunikationsweg, wäre also weitere Verwendung bereits übermittelter Daten nicht mehr davon erfasst. Dieser Sichtweise wird hier nicht gefolgt, es gilt vielmehr zu differenzieren: Sind zB Aufzeichnungen unter Verletzung des Fernmeldegeheimnisses durch Private entgegen § 119 StGB erfolgt, darf ein Eingriff staatlicher Behörden auf diese Datenträger nur unter den Voraussetzungen der §§ 134ff StPO erfolgen, wobei diese den Eingriffserfordernissen des Art 10a Abs 2 StGG aufgrund der richterlichen Genehmigungspflicht entsprechen. [23] Demzufolge ist also auch die weitere Verwendung der widerrechtlich erlangten Daten vom Schutzbereich des Fernmeldegeheimnisses erfasst.

Zu differenzieren ist zudem, wo die Inhalts- und Verkehrsdaten erhoben werden. Erfolgt die Informationsabfrage bei den Telekommunikationsanbietern, sollte der Schutz des Fernmeldegeheimnisses nach Art 10a StGG jedenfalls greifen.[24] Trotz des abgeschlossenen Kommunikationsvorgangs liegen diese beim Provider gespeicherten Daten außerhalb des Einflussbereiches der Teilnehmer. Ob, wann und wie diese Daten den staatlichen Ermittlungsbehörden zur Verfügung gestellt werden (müssen), entzieht sich der beherrschbaren Sphäre der Datensubjekte, was eben die besondere Schutzbedürftigkeit begründet.

Aufschlussreich für diese Argumentation erscheint auch ein Blick auf die Judikatur des deutschen Bundesverfassungsgerichts. Trotz systematischer Unterschiede zur österreichischen Grundrechtslage ist die Situation vergleichbarDie Rechtsprechung des BVerfG zum Fernmeldegeheimnis kann daher auch für die österreichische Situation wertvolle Argumente beitragen. In der deutschen Judikatur ist Anerkannt, dass das Fernmeldegeheimnis des Art 10 Grundgesetz (GG) neben den Inhaltsdaten auch die näheren Umstände der Kommunikation schützt[25]. Das Bundesverfassungsgericht geht in seiner

---

[20] OGH 26.7.2005, 11 Os 57/05Z = JBl 2006, 130; OGH 6.12.1995, 13 Os 161/95 = JBl 1997, 260; 17.6.1998, 13 Os 68/98 = EvBl 1998/191; Helmreich, Auskunftspflicht des Access-Providers bei Urheberrechtsverletzungen?, ecolex 2005, 379; Reindl, Telefonüberwachung zweimal neu? , ÖJZ 2002, 69; dies., Die nachträgliche Offenlegung der Vermittlungsdaten im Fernmeldeverkehr („Rufdatenrückerfassung"), JBl 1999, 791; Schmölzer, Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr, JBl 1997, 211;

[21] Zu den betrieblichen Zwecken, wofür diese Daten bei einem Anbieter gespeichert werden, sowie zum Nutzen dieser Daten für die Strafverfolgung.

[22] Wiederin, Art 10a StGG, in: Korinek/Holoubek (Hrsg), Österreichisches Bundesverfassungsrecht Bd. III, Rz 12; Wessely, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht?, ÖJZ 1999, 491.

[23] „Wie alle Eingriffe in das Fernmeldegeheimnis ist die nachträgliche Offenlegung von Vermittlungsdaten nur dann zulässig, wenn zusätzlich die Voraussetzungen des Art 8 MRK, des Art10a StGG und des § 1 DSG erfüllt sind." in: Reindl, Die nachträgliche Offenlegung von Vermittlungsdaten des Telefonverkehrs im Strafverfahren („Rufdatenrückerfassung"), JBl 1999, 794 f, 797.

[24] Vgl. Reindl, § 149a, Wiener Kommentar StPO, 40.Lfg, Rz 16.

[25] BVerfGE 85, 386; Vgl Hofmann, Art 10 GG in: Schmidt-Bleibtreu, Grundgesetz Kommentar, 2008[11], 340.

Entscheidung vom 16.Juni 2009[26] sogar weiter. Dort wird nämlich der Schutzbereich des Fernmeldegeheimnisses aus Art 10 Abs 1 GG auf bereits gelesene, aber auf dem Mailserver des Providers gespeicherte Emails anwendet. Hier liegt es zwar in der Entscheidungsmöglichkeit der Nutzer, die Emails nach dem Lesen zu löschen oder auf dem privaten Computer zu speichern. Im Falle der Speicherung der Mails auf dem Server des Anbieters, besteht weiterhin die spezifische Gefährdungslage, zu der Art 10 GG gerade seinen Schutz entfaltet. Eben diese Schutzbedürftigkeit aufgrund der Einschaltung Dritter rechtfertige eine Ausdehnung des Schutzbereichs des Art 10 GG. Dem rein technischen Telekommunikationsbegriff des TKG, welcher den Vorgang ausschließlich bis zum Empfangen des Emails erfasst, folge Art 10 GG daher nicht. Die Auslagerung der E-Mails auf den nicht im Herrschaftsbereich des Nutzers liegenden Mailserver des Providers bedeute nicht, dass die Nutzer mit dem Zugriff auf diese Daten durch Dritte einverstanden seien.[27] „Wer ein Teilnehmer- oder Benutzerverhältnis eingeht, weiß zwar in der Regel, dass es technische Möglichkeiten gibt, auf die Kommunikationsinhalte zuzugreifen. Er willigt damit aber nicht darin ein, dass auf die Kommunikationsinhalte zugegriffen wird.“ [28]

Darüber hinaus ermöglicht die Kenntnis von Verkehrsdaten nicht selten, Rückschlüsse auf den Inhalt der Kommunikation zu ziehen. Moderne Methoden wie Traffic Analysis, Social Network Analysis etc . ermöglichen durch Verknüpfung der Verkehrsdaten mit anderen Daten und Datenbanken einen intensiven Einblick in die Persönlichkeits- und Intimssphäre.[29]

Zusammengefasst bedeutet das: Die Schutzbedürftigkeit von Verkehrsdaten entsteht aus der Einschaltung Dritter in den Kommunikationsprozess, welche die Verfügungsmacht über diese Daten besitzen. Die Intention des Art 10a StGG ist, in Anlehnung an die Diktion des deutschen Bundesverfassungsgerichts, die freie Entfaltung der Persönlichkeit und die informationelle Selbstbestimmung durch Reaktion auf spezifische Gefahrensituationen, die sich während und im Zusammenhang mit fernmelderechtlichen Kommunikationsvorgängen ergeben. Um dem Schutzzweck des Art 10a StGG angemessen Ausdruck zu verleihen, ist also nach richtiger Auffassung eine Einbeziehung der Vermittlungsdaten unabdingbar.[30]

Diese Auffassung wird auch in ständiger Rechtsprechung des OGH zur „Rufdatenrückerfassung“ reflektiert. Der OGH geht offenbar davon aus, dass Vermittlungsdaten „jedenfalls (unter anderem) dem verfassungsrechtlichen Schutz des Fernmeldegeheimnisses“ unterliegen.[31] Die §§ 149a ff StPO (aF)[32] wurden in mehreren Entscheidungen als die „gesetzliche Ausnahmeregelung“ zu Art 10a StGG gesehen, welcher bei Offenlegung der Rufdaten zur Täterausforschung einen gerichtlichen Befehl verlangt.[33] Zusätzlich sei bei jeder Rufdatenrückerfassung eine Prüfung der Verhältnismäßigkeit vorzunehmen, „fallbezogen jene des Eingriffes in das Fernmeldegeheimnis nach Art 10a StGG und in

---

[26] BVerfG, 2 BvR 902/06 vom 16.6.2009, http://www.bverfg.de/entscheidungen/rs20090616_2bvr090206.html (13.12.2011).
[27] BVerfG, 2 BvR 902/06 vom 16.6.2009, Abs 53.
[28] Ibid; vgl. auch BVerfGE 85, 386-398.
[29] Boka/Feiler, die Vorratsdatenspeicherung von Verkehrs- und Standortdaten, in: Zankl (Hg.) Auf dem Weg zum Überwachungsstaat? Neue Überwachungsmaßnahmen im Bereich der Informations- und Kommunikationstechnologie (2009), 157ff.
[30] Vgl. Chadoian, Satenig, Das Fernmeldegeheimnis im Zeitalter der Internet- und Mobilfunküberwachung. Dissertation Wien, Einreichung voraussichtlich Ende 2011.
[31] OGH 17.6.1998, 13 Os 68/98 = EvBl 1998/191.
[32] Seit 1.1.2008 in §§ 134f StPO.
[33] OGH 13 Os 161/95 = JBl 1997, 260.

die Privatsphäre nach Art 8 EMRK, unter Berücksichtigung aller Umstände des Einzelfalls (…), somit bei Eingriffen von Strafverfolgungsbehörden durch Abwägung der mit der Überwachung verbundenen Beeinträchtigung der verfassungsrechtlich geschützten Privatsphäre gegenüber den Interessen der Strafverfolgung."[34]

In der Entscheidung vom 26.07.2005 bestätigte der OGH seine bisherige Ansicht zum Schutzbereich des Art 10a StGG. Er qualifizierte darin sowohl statische, als auch dynamische IP-Adressen als Verkehrsdaten, die prinzipiell dem im Art 10a StGG verankerten Grundrecht des Kommunikationsgeheimnisses unterliegen. Jedoch sei bei Kenntnis der IP-Adresse das Auskunftsbegehren auf Name und Anschrift des Kunden dem diese Adresse in einem bestimmten Zeitraum zugeordnet war, eine Auskunft auf Stammdaten. Diese Entscheidung wurde zurecht kritisiert, denn sie ignoriert, dass für die Auskunftserteilung zwar Provider-intern, aber doch für staatliche Zwecke eine Auswertung von dynamischen IP-Adressen erfolgen muss, die – wie bereits vom Höchstgereicht selbst festgestellt – jedenfalls als Verkehrsdaten dem Grundrecht auf Wahrung des Fernmeldegeheimnisses unterliegen. Spätestens seit dem EuGH-Urteil vom 29.1.2008[35] ist auch diese Rechtsansicht überholt und daher die Auskunft über Name und Adresse zu dynamischen IP-Adressen als Auskunft über Verkehrsdaten zu werten, die nur unter den strengen „Ausnahmebestimmungen" der §§ 134ff StPO erfolgen dürfen.[36]

II.1.1.2.2 Konsequenzen der Zuordnung von Verkehrsdaten in den Schutzbereich

Die praktische Bedeutung dieser Diskussion besteht darin, dass Art 10a StGG Eingriffe in das Fernmeldegeheimnis ausschließlich aufgrund eines richterlichen Befehls zulässt. Für die alltägliche Polizeiarbeit wird dies als unpraktikabel gesehen, weil der Verfahrensaufwand dadurch stark zunimmt. Außerdem entsteht eine noch ungeklärte Rechtsfrage, wenn es um Präventivaufgaben bzw. EAH geht, weil hier gar kein Strafverfahren läuft und ein Gericht daher Verwaltungsaufgaben kontrollieren würde, was Schwierigkeiten im Zusammenhang mit der Gewaltenteilung bedeutet, die allenfalls verfassungsgesetzlich bewältigt werden müssten.[37]

II.1.1.2.3 Kommunikationsgeheimnis des TKG 2003- Verhältnis zu Art 10a StGG

Das Kommunikationsgeheimnis ist in § 93 TKG normiert und steht nicht im Verfassungsrang, ist aber der einfachgesetzliche Ausfluss und lässt sich als die einfachgesetzliche nähere Ausführung des Fernmeldegeheimnisses in Art 10a StGG beschreiben[38]. Vom Kommunikationsgeheimnis sind auch

---

[34] OGH 1.10.2002, 11 Os 64/02.
[35] EuGH 29.1.2007, C-275/06.
[36] Zur Judikaturdivergenz, die zwischen dem OGH in Strafsachen einerseits und in Zivilsachen andererseits (4Ob 141/07z) besteht, siehe unten Kapitel II.1.4.4.4; vgl. zum ganzen auch Chadoian, Satenig, Das Fernmeldegeheimnis im Zeitalter der Internet- und Mobilfunküberwachung.
[37] Vgl. dazu jüngst die teilweise Aufhebung des § 106 StPO durch den Verfassungsgerichtshof, weil dort gerichtliche Rechtsschutzzuständigkeiten gegenüber Handlungen der Kriminalpolizei normiert wurden, die als Verletzung des Gewaltenteilungsgrundsatzes für verfassungswidrig erklärt wurde; VfGH 16.12.2010, G259/09 ua.
[38] Damjanovic (u.a.), Handbuch des Telekommunikationsrechts (2006), 262. Vgl auch Zanger/Schöll, Telekommunikationsgesetz, § 88, Rz 5, die in der Vorgängerbestimmung zu § 93 TKG, welche noch keine

Verkehrsdaten und Standortdaten geschützt. Da es sich um keine Grundrechtsbestimmung handelt, lässt sich daraus aber im Hinblick auf die oben erwähnte verfassungsrechtliche Debatte kein Zwang zu einem Richtervorbehalt oder „Genehmigungsvorbehalt“ (etwa durch RSB, DSK oder sonstige Kontrollstelle) ableiten. Das ändert nichts daran, dass die effektive Wahrung des Kommunikationsgeheimnisses zugleich auch der Wahrung des Fernmeldegeheimnisses dient und dem § 93 TKG daher zentrale Bedeutung zukommt.Mit der einfachgesetzlichen Normierung des Kommunikationsgeheimnisses realisiert der Staat seine Schutzpflicht zur Gewährleistung des Grundrechts auch zwischen Privaten.

Das Kommunikationsgeheimnis nach § 93 TKG wendet sich zunächst an die Dienstanbieter und alle an dessen Tätigkeit mitwirkenden Personen. § 93 Abs 3 und Abs 4TKG sind an alle gerichtet und bilden den vertragsunabhängigen Schutz der Kommunikation. Zwar ist die Verletzung des Kommunikationsgeheimnisses nach den Bestimmungen des TKG selbst sanktionslos, jedoch besteht eine flankierende strafrechtliche Norm in § 119 StGB. Der Schutzbereich und die zu schützenden Datenkategorien des einfachgesetzlichen Kommunikationsgeheimnisses sind weiter gefasst als jene des Art 10a StGG, geschützt sind neben Inhaltsdaten ausdrücklich auch Verkehrs- und Standortdaten schützt, Von § 93 Abs 1 und Abs 2 TKG wird der Schutz auch auf die Daten erfolgloser Verbindungsversuche ausgedehnt, die wohl nicht einmal als Verkehrsdaten zu qualifizieren sind, da sie weder für die Weiterleitung einer Nachricht, noch für die Abrechnung verarbeitet werden.[39]

§ 93 TKG strebt dabei einen umfassenden Schutz der Privatsphäre und der Vertraulichkeit der Kommunikation an. Die auf privatrechtlichem Vertrag begründete, engere Vertrauenssituation zwischen Kommunikationsteilnehmern und Anbietern rechtfertigt eine extensivere Geheimhaltungspflicht der Kommunikationsdaten. Außerdem sind gerade die Anbieter jene Instanz, die bei Eingriffen durch staatliche Behörden primär herangezogen werden. Sie sind es, die im Besitz der Daten sind, über die sie frei verfügen könnten.

Die Geheimhaltungspflicht besteht daher nicht nur während der Abwicklung der Kommunikation selbst, sondern auch über die Vertragsbeziehung hinaus.[40] Auch personell ist die Schutzpflicht in zweifacher Hinsicht ausgedehnt und erfasst einerseits die „ Erfüllungsgehilfen“ des Anbieters, andererseits kommt nicht nur die/der TeilnehmerIn, sondern jede/r BenutzerIn in den Genuss des Kommunikationsgeheimnisses. Dieser persönliche Schutzbereich entspricht übrigens analog jenem des Art 10a StGG. Zulässige Ausnahmen der Verarbeitung durch die Anbieter werden in § 93 Abs 3 Satz 2 TKG genannt. Zulässig sind die übertragungstechnisch erforderliche (Zwischen)speicherung[41], die Aufzeichnung und Rückverfolgung von Telefongesprächen bei eingehenden Notrufen durch Notruforganisationen und die Fälle der Fangschaltung.

Standortdaten unter einfachgesetzlichen Schutz stellte, eine erstmalige Definition im Umfang des Schutzbereiches sahen.

[39] Himberger, Fernmeldegeheimnis und Überwachung (Diss. Wien 2003), 130.

[40] Siehe § 93 Abs 2 Satz 2.

[41] Etwa bei Sprachboxen im Mobilbereich, bei SMS und bei E-Mail Postfächern. Vgl Singer, § 93 TKG in: Stratil(u.a.), Telekommunikationsgesetz 2003, 297.

II.1.1.3 DATENSCHUTZGRUNDRECHT NACH DSG 2000 UND ART 8 EMRK

II.1.1.3.1 SCHUTZBEREICH DES DATENSCHUTZGRUNDRECHTS IM HINBLICK AUF VERKEHRSDATEN

Neben dem Fernmeldegeheimnis nach Art 10a StGG entfaltet auch das Grundrecht auf Datenschutz nach Art 1 § 1 DSG Einwirkungen auf das einfachgesetzliche Kommunikationsgeheimnis.[42] Der im Verfassungsrang stehende § 1 Abs. 1 DSG normiert: „Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht." Mit „Jedermann" ist jede natürliche und juristische Person gemein. Der Anspruch auf Geheimhaltung bedeutet das Recht, dass keine Daten an Dritte übermittelt werden und Daten nicht von Dritten ermittelt werden.[43] Bei Inhalts-, Verkehrs-, und Standortdaten handelt es sich um „personenbezogenen Daten", an denen ein schutzwürdiges Interesse an deren Geheimhaltung bestehen kann. Insofern könnte § 93 TKG auch als konkrete, einfachgesetzliche Ausgestaltung des Grundrechts auf Datenschutz gesehen werden, dem nach § 1 Abs 5 DSG 2000 auch unmittelbare Drittwirkung gegenüber Privaten zukommt.[44]

Im Gegensatz zu Art 10a StGG und auch zu § 93 TKG 2003 ist der Geheimnisbegriff des § 1 DSG materiell zu verstehen[45]. Insofern stehen personenbezogene Daten, die bereits allgemein bekannt sind – unabhängig davon, ob sie als Inhalts-, Verkehrs-, oder Standortdaten anfallen – nicht unter dem grundrechtlichen Schutz des Art 1 Abs 1 DSG, sind aber sehr wohl vom Kommunikationsgeheimnis nach § 93 TKG 2003 erfasst und im Fall von Verkehrs- und Inhaltsdaten auch von Art 10a StGG. Die aus Art 1 § 1 DSG ableitbaren Schutzpflichten der Anbieter werden in den datenschutzrechtlichen Bestimmungen der §§ 96 ff TKG (strenge Zweckbindung, Datensparsamkeit, Auskunft, Löschungspflicht) weiter konkretisiert.

Der in Art 1 § 1 DSG ausdrücklich genannte Anspruch auf Achtung des „Privat- und Familienlebens" ist primär durch Art Art 8 EMRK geschützt, weshalb in materieller Hinsicht das Datenschutzgrundrecht auch durch Art 8 EMRK und die Rechtssprechung des EGMR zu diesem Grundrecht ausgeprägt ist. Wenngleich die beiden Grundrechtsgarantien auch einen völlig eigenständigen Charakter haben, wird aus diesem Grund der Schwerpunkt der Ausführungen in diesem Kapitel auch auf diese Norm und die Rechtssprechung des EGMR dazu gelegt.

II.1.1.3.2 SCHUTZBEREICH DES RECHTS AUF ACHTUNG DES PRIVATLEBENS NACH ART 8 EMRK

Gemäß Art 8 EMRK hat jedermann Anspruch auf Achtung seines Privatlebens. Dadurch werden die wesentlichen Ausdrucksmöglichkeiten der Persönlichkeit geschützt sowie ein Grundsatz der Selbstbestimmung normiert.[46] Der Schutzbereich des Rechts auf Privatleben iSd Art 8 EMRK umfasst

---

[42] Vgl Wiebe, Auskunftsverpflichtung der Access Provider, MR 2005, Beilage 1.

[43] Lehner, Recht auf Datenschutz, in: Heißl (Hrsg.), Handbuch Menschenrechte, 213; dort findet sich insgesamt eine sehr übersichtliche Darstellung des Datenschutzgrundrechts mit ausführlichen Judikaturnachweisen.

[44] Dohr (u.a.), Art 1 § 1, DSG Kommentar, 2008[2],8.Er.-Lfg., 19.

[45] OGH, JBl 1995, 332; Damjanovic (u.a.), Handbuch des Telekommunikationsrechts (2006), 242.

[46] Heißl, Recht auf Privatleben, in: Heißl (Hrsg.), Handbuch Menschenrechte, 161, mit einer umfassenden und übersichtlichen Darstellung zu Art 8 EMRK.

jedenfalls ein Abwehrrecht gegen die staatliche Erforschung der Privatsphäre. Die Möglichkeiten der modernen computergestützten Sammlung und Verwertung von Informationen machen den Schutz persönlicher Daten zu einem wichtigen Teilbereich der Gewährleistungen des Art 8 EMRK.[47] Weiters garantiert Art 8 EMRK auch ein Recht auf Achtung des Briefverkehrs. Davon umfasst sind private und nicht-private schriftliche Mitteilungen, wobei sich der Schutz auf den Kommunikationsvorgang – sowie den Kommunikationsweg einerseits und auf die infolge der Kommunikation gespeicherten Mitteilungen andererseits erstreckt.[48] Vorbild ist der Schutz des Briefverkehrs: Die nicht-öffentlichen Mitteilungen einer Person an eine andere sollen vor Eingriffen des Staates geschützt werden. Daher fallen unter den Begriff des Briefverkehrs im Sinne des Art 8 EMRK auch die Kommunikation per E-Mail und das Telefonieren über das Internet.[49]

Der EGMR entschied ebenso bereits wiederholt, dass auch Telefongespräche als „Briefverkehr/Korrespondenz" iSd Art 8 EMRK anzusehen sind.[50] Art 8 EMRK schützt dabei sowohl geschäftliche als auch private Kommunikation.[51] Aus der Rechtsprechung des EGMR ergibt sich eindeutig, dass auch „äußere Gesprächsdaten", also gewählte Nummer, Zeitpunkt und Dauer, vom Schutzbereich des Art 8 EMRK umfasst sind und ein Eingriff in dieses Grundrecht insbesondere auch dann vorliegt, wenn solche Daten ohne Zustimmung des Betroffenen an staatliche Behörden übermittelt werden.[52] Dies gilt neben Telefonaten auch für die Erhebung von näheren Umständen der E-Mail-Nutzung und der Internetnutzung.[53] Sowohl in der Erhebung wie auch in der Speicherung dieser Daten liegt ein Grundrechtseingriff, selbst wenn die Daten auf legalem Wege erlangt werden.[54]

II.1.1.3.2.1 Abstrakte oder konkrete Betroffenheit

Im Urteil des EGMR Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien vom 28.6.2007 hatte sich der Gerichtshof mit der Frage auseinanderzusetzen, ob das bloße Vorhandensein von Rechtsvorschriften, die eine geheime Überwachung erlauben, ohne dass in einem konkreten Fall Überwachungsmaßnahmen auf eine beschwerdeführende Person tatsächlich angewandt wurden, eine Opfereigenschaft im Sinne des Artikel 34 EMRK begründen kann.[55] Die Beschwerde war gegen ein Gesetz über besondere Überwachungsinstrumente gerichtet. Die Beschwerdeführer behaupteten nicht, dass Überwachungsmaßnahmen tatsächlich gegen sie angeordnet oder eingesetzt wurden, oder dass sie direkt von einer Überwachungsmaßnahme gegen andere Personen betroffen waren. Sie brachten lediglich vor, dass sie aufgrund des Gesetzes selbst zu jedem Zeitpunkt Ziel solcher Maßnahmen sein können, ohne darüber vor, während oder nach der Anwendung der Maßnahme informiert zu werden.[56] In diesem Urteil entschied der EGMR mit

---

[47] Grabenwarter, Europäische Menschenrechtskonvention, 4. Auflage, 2009, Art 8 Rz 10.
[48] Vgl Grabenwarter, Europäische Menschenrechtskonvention, 4. Auflage, 2009, Art 8 Rz 24.
[49] EGMR 22.10.2002 Taylor–Sabori gg. das Vereinigte Königreich.
[50] EGMR 04.05.2000 Rotaru gg. Rumänien = ÖJZ 2001, S. 74 ff.
[51] EGMR 16.12.1992 Niemietz gg. Deutschland = NJW 1993, S. 718.
[52] EGMR 02.08.1984 Malone gg. das Vereinigte Königreich, RN. 83 f.= EuGRZ 1985, S. 17ff.
[53] EGMR 03.07.2007 Copland gg. das Vereinigte Königreich = EuGRZ 2007, S. 415ff.
[54] EGMR 03.07.2007 Copland gg. das Vereinigte Königreich = EuGRZ 2007, S. 415ff.
[55] RN. 59 des Urteils, wobei der EGMR auch auf EGMR 25.06.1997 Halford gg. das Vereinigte Königreich, RN. 55-57, verweist.
[56] RN. 6 des Urteils.

Verweis auf Entscheidungen in früheren Fällen,[57] dass das Bestehen von Rechtsvorschriften, die eine geheime Überwachung erlauben, selbst einen Eingriff in das Recht nach Art 8 EMRK darstellt, unabhängig von irgendwelchen tatsächlich gegen die Beschwerdeführer ergriffenen Maßnahmen.[58]

Es lässt sich also festhalten, dass jede staatliche Verwendung (Erhebung, Speicherung, Verarbeitung und Weitergabe) von personenbezogenen Informationen über das Kommunikationsverhalten einen Eingriff in Art 8 EMRK darstellt. Daraus folgt, dass geheime Überwachungsbefugnisse den vom EGMR verlangten Bestimmtheitserfordernissen auch dann entsprechen müssen, wenn es sich „nur" um die Ermittlung von Verkehrsdaten handelt, weil aus solchen Daten häufig Rückschlüsse auf die Persönlichkeit und das Privatleben von Betroffenen möglich sind.

II.1.1.3.3 HORIZONTALWIRKUNG DES DATENSCHUTZGRUNDRECHTS

Die Verfassungsbestimmung des Artikel 1 § 1 Abs 5 Datenschutzgesetz 2000[59] (DSG 2000) sieht vor, dass „gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, […] soweit sie nicht in Vollziehung der Gesetze tätig werden, das Grundrecht auf Datenschutz mit Ausnahme des Rechtes auf Auskunft auf dem Zivilrechtsweg geltend zu machen [ist]." Die Bestimmung konstituiert somit für Jedermann den grundrechtlichen „Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht" (§ 1 Abs 1 DSG 2000) auch gegenüber privaten Rechtsträgern und verweist den Rechtsschutz in die Zuständigkeit der ordentlichen Gerichte. Das „Grundrecht auf Datenschutz" wird so „mit Drittwirkung ausgestattet", wie in den erläuternden Bemerkungen zur Regierungsvorlage (EBRV) zum DSG 2000[60] schlicht und in dieser Hinsicht zugleich abschließend formuliert.

Der Verfassungsgesetzgeber des Artikel 1 DSG 2000 normierte damit für das Grundrecht auf Datenschutz, was im grundrechtsdogmatischen Schrifttum nicht nur in Österreich seit längerem Gegenstand kontroverser Auseinandersetzungen ist und in systematischer Hinsicht wohl bis heute in Wissenschaft und Praxis nicht einhellig und schon gar nicht dogmatisch konsistent geklärt scheint: Die (hier sogar unmittelbare) Wirkung einer Grundrechtsgarantie auf der horizontalen Ebene der Beziehungen der Privatrechtssubjekte untereinander. Klargestellt ist die Horizontalwirkung allerdings nur dem Grunde nach. So enthält etwa § 1 Abs 2 DSG 2000 im Hinblick auf Eingriffe in das Grundrecht, die nicht durch "den Staat" (in seiner Hoheitsfunktion) erfolgen, keine näheren Parameter dafür, wann ein berechtigtes Informationsinteresse anderer vorliegt, welches die schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegt. „Diesbezüglich sind die einfachgesetzlichen Ausführungsbestimmungen zum Grundrecht, und zwar die §§ 7 und 9, heranzuziehen".[61] Ebenso interpretationsbedürftig erscheint, was unter einer „Beschränkung des Anspruchs auf Geheimhaltung" (§ 1 Abs 2 DSG 2000) - also einem Eingriff in das Grundrecht -

---

[57] Siehe EGMR 06.09.1978 Klass u.a. gg. Deutschland, RN. 41 = NJW 1979, S. 1775 ff.; EGMR 02.08.1984 Malone gg. das Vereinigte Königreich, RN. 64 = EuGRZ 1985, S. 17ff; EGMR 29.06.2006 Weber und Saravia gg. Deutschland, RN 77-79 = NJW 2007, S. 1433ff.

[58] EGMR 29.06.2006 Weber und Saravia gg. Deutschland, RN. 78 = NJW 2007, S. 1433ff, mit Hinweisen auf frühere Urteile in den Fällen EGMR 06.08.1978 Klass u.a. gg. Deutschland und EGMR 02.08.1984 Malone gg. das Vereinigte Königreich.

[59] BGBl. I Nr. 165/1999 idF BGBl. I Nr. 2/2008 (1. BVRBG).

[60] EB RV 1613 BlgNR XX. GP, 35.

[61] Siehe die Erläuterungen zum DSG 2000, EBRV 1613 BlgNR XX. GP, 35.

überhaupt zu verstehen ist. Insbesondere ist die Kategorie eines Grundrechtseingriffs bei der Verwendung personenbezogener Daten im Rahmen vertragsrechtlicher Beziehungen schwieriger zu erfassen. Damit korrespondiert die gleichwohl vorgelagerte Frage, wie weit der Schutzbereich des „Grundrechts auf Datenschutz" reicht. Jedenfalls ist der Schutzbereich unabhängig vom Eingriff zu definieren. Zumal besonders inter privatos die Weitergabe und Verarbeitung personenbezogener Daten regelmäßig zunächst einmal auf Freiwilligkeit beruht und in gegenseitigem Interesse erfolgt. Gleichzeitig sind diese Interessen nicht immer transparent, was wiederum auf die Beurteilung zurückwirkt, ob tatsächlich freiwilliges Einverständnis vorliegt. Damit ist die Frage nach der Zweckbindung bei der Datenverwendung in zivilrechtlichen Beziehungen angesprochen, die schließlich eine entscheidende Rolle hinsichtlich allfälliger Haftungszurechnungen spielt.

II.1.1.3.4 GRUNDRECHTLICHE SCHUTZ- UND GEWÄHRLEISTUNGSPFLICHTEN

Die Entwicklung des Datenschutzrechtes vor dem Hintergrund rasant wachsender technologischer Möglichkeiten steckt schon von ihrer individualrechtlichen Grundkonzeption her in eingriffsabwehrrechtlichen Denkschemen fest, die den realen Verhältnissen nicht gerecht zu werden vermögen. Die Beschäftigung mit datenschutzrechtlichen Entscheidungen erweckt vielfach den Eindruck, es wären die Daten selbst, die es zu schützen gilt, also Datenschutz als Selbstzweck und Legitimation für Datenschützer. Die Schutzbedürftigkeit ist aber vielmehr von den dahinter stehenden Verwendungszusammenhängen und den damit verbundenen Risiken her zu beurteilen. Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person führen zwar dazu, dass der Einzelne Einschränkungen seiner Grundrechte hinzunehmen hat, wenn überwiegende Allgemeininteressen dies rechtfertigen. Der Gesetzgeber muss aber zwischen Allgemein- und Individualinteressen einen angemessenen Ausgleich herstellen. Es scheint daher sachgerecht, den „Datenschutz" nach einem Muster des „Risikorechts" und als „teilhaberechtliche" Konstruktion zu erfassen.[62] Den Staat Treffen dabei grundrechtliche Schutzpflichten, die so zu verstehen sind, dass er eine normative Gestaltung vorzunehmen hat, die einen wirksamen Schutz von Grundrechtspositionen auf der Ebene der Interaktion Privater bietet. Die Grundrechte enthalten dabei immer nur normative Anordnungen und beziehen sich insofern auf eine bestimmte Gestaltung von Rechtsnormen.[63] Die Grundrechte haben dabei in ihren unterschiedlichen Wirkungsdimensionen Einfluss auf die Entwicklung neuer Technologien und deren Innovationspfade, ungewollte Schäden sollen durch grundrechtliche Schutz- und Gewährleistungspflichten verhindert werden.[64] Die staatliche Schutzpflicht gegenüber der Möglichkeit von Grundrechtsverletzungen erfordert, dass ein Rechtsrahmen geschaffen wird, der gewährleistet, dass die Verwendung von Kommunikationsdaten

---

[62] Ladeur, Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion?, DÖV 2009, Jg 62, 45ff.

[63] Dazu ausführlich Holoubek, Grundrechtliche Gewährleistungspflichten, 259 ff.

[64] So das Resümee einer bemerkenswerten Analyse zum Beitrag der Grundrechte im Hinblick auf eine gesellschaftliche und staatliche Innovationsfolgenverantwortung, Eisenberger, Technik der Grundrechte - Grundrechte der Technik, in: Holoubek/Martin/Schwarzer (Hrsg.), Die Zukunft der Verfassung - Die Verfassung der Zukunft? Festschrift für Karl Korinek zum 70. Geburtstag, 128.

der Kunden von Anbietern öffentlicher Kommunikationsdienste konform mit dem Grundrecht auf Datenschutz erfolgt.[65]

In Anlehnung an die Thesen, „gleiche Freiheit" als grundsätzlich positive Freiheit von Menschen durch Menschen im Sinne wechselseitiger Instrumentalisierung zu sehen[66], müssen die grundrechtlichen Verfahrens- und Organisationsmaximen stärker ins Zentrum rücken. Im Kontext moderner Informationstechnologie sind damit Fragen technologischer Sicherungsmechanismen untrennbar verknüpft. So sind etwa Dokumentations- und Informationspflichten und deren tatsächliche Erfüllbarkeit unabdingbare Voraussetzungen eines effektiven Rechtsschutzes im Hinblick auf die Gewährleistung der „informationellen Selbstbestimmung". Angesichts einer mit menschlichem Auge unmöglich zu überschauenden Zahl von Informationsverarbeitungsprozessen in sehr vielen Lebensbereichen, lassen sich diese Aufgaben nur mit Hilfe entsprechender elektronischer Hilfsmittel bewältigen. Ähnliches gilt für Zugriffskontrollen etc. Das moderne Schlagwort hierfür lautet „Information Security Management". Das bedeutet, dass innerhalb einer Organisation - ob nun privat oder staatlich - durch die Definition organisatorischer Abläufe, die eindeutige Benennung der verantwortlichen Personen sowie die Verwendung technischer Mittel sicherzustellen ist, dass Informationen nur für jene Zwecke verwendet werden, für die sie erhoben wurden.

II.1.1.4 Europäische Grundrechte-charta (GRC) nach dem Vertrag von Lissabon

Seit dem Inkrafttreten des Vertrages von Lissabon[67] ist die europäische Grundrechte-Charta (GRC)[68] im Primärrecht der Europäischen Union verbindlich verankert. Datenschutz ist dort für den Anwendungsbereich des Unionsrechts (siehe Anwendungsbereich Art 51 GRC) als eigenes Grundrecht in Art 8 GRC normiert. Für den Bedeutungsgehalt dieses Grundrechts ist die Auslegung der EMRK durch den EGMR beachtlich, weil Art 52 Abs. 3 GRC zur Tragweite der in der GRC garantierten Rechte ausdrücklich bestimmt: „So weit diese Charta Rechte enthält, die den durch die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen, haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird. Diese Bestimmung steht dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt."

Flankiert wird diese Bestimmung durch eine sog. Günstigkeitsklausel in Art 53 GRC: „Keine Bestimmung dieser Charta ist als eine Einschränkung oder Verletzung der Menschenrechte und Grundfreiheiten auszulegen, die in dem jeweiligen Anwendungsbereich durch das Recht der Union und das Völkerrecht sowie durch die internationalen Übereinkommen, bei denen die Union, die Gemeinschaft oder alle Mitgliedstaaten Vertragsparteien sind, darunter insbesondere die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten, sowie durch die Verfassungen der Mitgliedstaaten anerkannt werden."

---

[65] Siehe dieselbe Argumentation bei Kotschy, Datenschutzrechtliche Fragen im Zusammenhang mit dem neuen Verbraucherkreditrecht, ÖBA 2011, 312.

[66] Suhr, Freiheit durch Geselligkeit, EuGRZ 1984, Jg 11, 529.

[67] BGBl. III Nr. 132/2009. Nachdem Tschechien als letzter Staat den Lissabon-Vertrag am 3. November 2009 ratifizierte trat der Vertrag gem. dessen Art. 6 Abs. 2 am 1. Dezember 2009 in kraft.

[68] Gem. Art. 6 I EUV ist die GRC mit den Verträgen gleichrangig und somit nunmehr Bestandteil des Primärrechts.

Von besonderer Bedeutung für den Grundrechtsschutz in der EU ist der neue Art 6 EUV, der in Abs. 2 kurz und bündig bestimmt: „Die Union tritt der (EMRK) bei." Weiters normiert Abs. 3 die Grundrechte aus der EMRK und aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedsstaaten als allgemeine Grundsätze, die Teil des Unionsrechts sind. Der Grundrechtsschutz wird somit dreifach abgestützt, wobei in dieser Arbeit der Fokus auf die Rechte der EMRK gelegt wird.[69]

In der Rechtssprechung des EGMR wird Datenschutz als spezifischer Teilaspekt vom Schutz der Privatsphäre nach Art 8 EMRK ausgestaltet, zum Teil unter Rückgriff auf die Datenschutzkonvention[70] des Europarats[71]. Das DSG 2000 wiederum setzt innerstaatlich die Datenschutzrichtlinie 95/46/EG um und verweist dabei auch auf die Rechtfertigungsgründe des Art 8 EMRK. Es entsteht damit auf der Ebene der Grundrechte eine Gemengelage, die durch die wechselseitigen Günstigkeitsklauseln auf nationaler wie auf europäischer Ebene jeweils das höchste Schutzniveau zum Verbindlichen Maßstab werden lässt. Durch die Rechtsprechung des EGMR ist anerkannt, dass Art 8 EMRK neben Inhaltsdaten auch Verkehrsdaten erfasst und schützt.[72]

II.1.2 Bestimmtheit und Verhältnismäßigkeit von Eingriffen

II.1.2.1 Bestimmtheit der gesetzlichen Grundlage

Eingriffe in den Schutzbereich des Art 8 EMRK sind nicht automatisch unzulässig, sondern bedürfen einer Rechtfertigung. Gemäß Art 8 Abs 2 EMRK ist zunächst eine gesetzliche Grundlage für Eingriffe erforderlich. Aus dem Erfordernis einer gesetzlichen Grundlage in Verbindung mit dem in der Präambel der EMRK verankerten Rechtsstaatsprinzip leitet der EGMR zudem ab, dass das eingreifende innerstaatliche Recht hinreichend bestimmt und für die Bürger zugänglich sein muss.[73] Das Gesetz muss adäquate Hinweise über die Bedingungen und Umstände enthalten, unter denen die Behörden befugt sind, in das Recht auf Achtung des Privatlebens und des Briefverkehrs einzugreifen.[74]

Räumt das nationale Recht der Exekutive oder dem zuständigen Richter bei der Anordnung von Maßnahmen Ermessen ein, dann verlangt das Bestimmtheitserfordernis – auch und gerade bei geheimen Maßnahmen –, dass der zulässige Zweck der Maßnahme, die Reichweite und Grenzen des Ermessens sowie die Kriterien, nach denen es auszuüben ist, hinreichend erkennbar sind,

---

[69] Siehe zu diesem Verhältnis Heißl, Happy End einer unendlichen Geschichte? Der Beitritt der EU zur EMRK und seine Auswirkungen auf Österreich, in: Holoubek/Martin/Schwarzer (Hrsg.), Die Zukunft der Verfassung - Die Verfassung der Zukunft? Festschrift für Karl Korinek zum 70. Geburtstag, S. 131.

[70] Europarat, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, 28.1.1981., SEV Nr. 108, abrufbar auf der Web-Seite des Europarat-Vertragsdienstes unter http://conventions.coe.int/Treaty/ger/Treaties/Html/108.htm (13.10.2011).

[71] ZB EGMR 20.03.1987 Leander gg. Schweden.

[72] EGMR 02.08.1984, Malone gg.Vereinigtes Königreich = EuGRZ 1985, 23f.

[73] EGMR 24.08.1998 Lambert gg. Frankreich = ÖJZ 1999, S. 570ff.

[74] EGMR 28.06.2007 Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien, RN 74-75 unter Verweis auf die Urteile EGMR 02.08.1984 Malone gg. das Vereinigte Königreich, RN 67; EGMR 30.07.1998 Valenzuela Contreras gg. Spanien, RN 46; und EGMR 12.05.2000 Khan gg. das Vereinigt Königreich, RN 26.

insbesondere, dass vorhersehbar ist, unter welchen Umständen Eingriffe zulässig sind.[75] Die Anforderungen an die Vorhersehbarkeit im Einzelnen hängen von der Eingriffsintensität der jeweiligen Maßnahme ab. Im Hinblick auf das Missbrauchsrisiko, das jedem geheimen Überwachungssystem innewohnt, müssen solche Maßnahmen auf einem besonders präzisen Gesetz beruhen.[76] Klare und detaillierte Bestimmungen müssen insofern einer immer komplexer werdenden Technologie Rechnung tragen.[77]

Auch wenn Strafverfolgungsorgane um die Herausgabe von Daten „bitten", ohne das Telekommunikationsunternehmen dazu zu verpflichten, ist erforderlich, dass die freiwillige Übermittlung der angeforderten Daten nach innerstaatlichem Recht rechtmäßig und die Befugnis der Strafverfolgungsorgane zur Anforderung solcher Daten detailliert geregelt ist.[78] In jedem Fall muss der Staat angemessene Maßnahmen ergreifen, um zu verhindern, dass Dritte unbefugt Kenntnis von überwachten Telekommunikationsinhalten erlangen.[79]

II.1.2.2 Erforderlichkeit und Verhältnismäßigkeit

Die Prüfung der Verhältnismäßigkeit von Grundrechtseingriffen wird in der Grundrechtswissenschaft durch folgendes Frageschema gekennzeichnet, welches aus der ständigen Praxis der europäischen und nationalen Höchstgerichte ableitbar ist:

Ist die Datenverarbeitung ein Eingriff in die informationelle Selbstbestimmung?

Ist der Eingriff gesetzlich vorgesehen und hinreichend bestimmt?

Dient der Eingriff einem legitimen Ziel?

Ist die Datenverarbeitung abstrakt geeignet, den Zweck zu erreichen?

Gibt es gelindere Mittel, den Zweck zu erreichen?

Besteht ein angemessenes Verhältnis zwischen nachteiligen Konsequenzen und Nutzen?

Liegt eine gesetzliche Grundlage der fraglichen Maßnahme nach den vorgenannten Kriterien vor, so muss die Maßnahme nach Art 8 Abs 2 EMRK zusätzlich in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig sein. Die einzelnen Staaten haben nach der Rechtsprechung des Gerichtshofs einen Beurteilungsspielraum bezüglich der Frage, ob eine Maßnahme zu einem der in Art 8 Abs 2 EMRK genannten Zwecke

---

[75] EGMR 02.08.1984 Malone gg. das Vereinigte Königreich = EuGRZ 1985, S. 17 ff.
[76] EGMR 25.03.1998 Kopp gg. die Schweiz = ÖJZ 1999, S. 115 ff.
[77] EGMR 28.06.2007 Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien, RN 74-75 unter Verweis auf die Urteile EGMR 24.04.1990 Kruslin gg. Frankreich, RN 33; EGMR 24.04.1990 Huvig gg. Frankreich, RN 32; EGMR 16.02.2000 Amann gg. die Schweiz, RN 56; und EGMR 29.06.2006 Weber und Saravia gg. Deutschland, RN 93.
[78] EGMR 02.08.1984 Malone gg. das Vereinigte Königreich = EuGRZ 1985, S. 17 ff.
[79] EGMR 17.07.2003 Craxi gg. Italien.

notwendig ist. Hinter der Formulierung „in einer demokratischen Gesellschaft (…) notwendig“ verbirgt sich der Grundsatz der Verhältnismäßigkeit, wie er in vergleichbarer Weise auch bei vielen Grundrechten nationaler Verfassungen als Bedingung für die Zulässigkeit von Grundrechtseingriffen normiert ist.[80]

In einer demokratischen Gesellschaft notwendig ist eine Maßnahme nur, wenn ein in Anbetracht des Stellenwerts des garantierten Freiheitsrechts hinreichend „dringendes soziales Bedürfnis“ nach ihr besteht, sie einen legitimen Zweck verfolgt und ihre Eingriffsintensität nicht außer Verhältnis zu dem Gewicht des Zwecks steht.[81] Der EGMR hat dazu eindeutig erklärt, dass das Interesse des Staates gegenüber den Interessen des Einzelnen an der Achtung seiner Privatsphäre abgewogen werden müsse.[82] Eingriffe sind zwar nicht auf das unerlässliche Maß beschränkt, aber ein bloßes Nützlichsein oder Wünschenswertsein genügt nicht.[83] Sind die genannten Kriterien erfüllt, so liegt keine Verletzung von Art 8 EMRK vor. Eine Beschränkung von Grundrechten ist nur insoweit zulässig, als sie zur Erreichung des angestrebten Zweckes geeignet und erforderlich ist, und der Eingriff seiner Intensität nach nicht außer Verhältnis zur Bedeutung der Sache und den von den Betroffenen hinzunehmenden Einbußen steht.

Zur Beurteilung der Verhältnismäßigkeit von Grundrechtseingriffen ist wesentlich, unter welchen Voraussetzungen welche und wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind. Maßgebend sind also insbesondere die Gestaltung der Einschreitschwellen, die Zahl der Betroffenen und die Intensität der Beeinträchtigungen. Im Bereich der Telekommunikationsüberwachung ist von Bedeutung, ob die Betroffenen als Personen anonym bleiben, welche Informationen erfasst werden können und welche Nachteile den Grundrechtsträgern aufgrund der Überwachungsmaßnahme drohen. Auf Seiten der mit dem Eingriff verfolgten Zwecke ist das Gewicht der Ziele maßgeblich, denen die Telekommunikationsüberwachung dient. Es hängt unter anderem davon ab, wie bedeutsam die Rechtsgüter sind, die mit Hilfe der Maßnahme geschützt werden sollen und wie wahrscheinlich der Eintritt einer Rechtsgutverletzung ist.[84]

II.1.2.3 Anforderungen an einen effektiven Rechtsschutz

Um die effektive Anwendung der oben genannten Prinzipien sicherzustellen, verlangt der Gerichtshof die folgenden Mindestsicherungen, die ausdrücklich im kodifizierten Recht angeordnet werden müssen, um Missbrauch zu vermeiden: Das Wesen der Straftaten, die Anlass zu einem Abhörbeschluss geben können; eine Definition jener Personengruppen, deren Kommunikation überwacht werden kann; eine Begrenzung der Dauer einer solchen Überwachung; das Verfahren, nach dem bei der Untersuchung, Verwendung und Speicherung der erlangten Daten vorgegangen wird; die Schutzmaßnahmen, die zur Anwendung kommen, wenn die Daten an Dritte übertragen werden; und die Umstände, unter denen die erlangten Daten gelöscht oder die Aufnahmen

[80] Grabenwarter, EMRK[4], § 18 Rz 14, S. 116.
[81] EGMR 25.03.1983 Silver gg. das Vereinigte Königreich = EuGRZ 1984, S. 147 ff.
[82] EGMR 26.03.1987 Leander gg. Schweden.
[83] EGMR 25.03.1983 Silver gg. das Vereinigte Königreich = EuGRZ 1984, S. 147 ff.
[84] So auch das deutsche Bundesverfassungsgericht in BVerfGE 100, 313 (375 f).

vernichtet werden können oder müssen.[85] Für den Fall, dass unbeteiligte Dritte von einer Überwachungsmaßnahme betroffen sind (zB als Gesprächspartner eines Verdächtigen), müssen Sicherungsvorkehrungen in Bezug auf deren Daten vorgesehen werden.[86]

II.1.2.3.1 KONTROLLE DER BEHÖRDEN

Nach dem Urteil des EGMR im Fall *Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien* stellt es eine Verletzung des Art 8 EMRK dar, wenn es an einer nachträglichen Überprüfung des Einsatzes geheimer Überwachungsmaßnahmen durch Einrichtungen oder Beamte fehlt, die entweder außerhalb der die Überwachungsmittel einsetzenden Dienstbehörde angesiedelt sind oder zumindest bestimmte Qualifikationen aufweisen müssen, die ihre Unabhängigkeit und die Einhaltung des Rechtsstaatsprinzips sicherstellen.[87] In diesem Fall erkannte der EGMR eine Verletzung insbesondere darin, dass niemand außerhalb der Behörde – die die Überwachungsmaßnahmen ergriff – etwa überprüfte, ob diese Maßnahmen tatsächlich den Auflagen der Ermächtigungen für die Überwachungsmaßnahmen entsprachen oder ob die Originaldaten den Tatsachen entsprechend in die schriftlichen Berichte übernommen wurden. Ebenso gab es auch keine unabhängige nachprüfende Kontrolle, ob die Originaldaten innerhalb der erlaubten zehntägigen Frist tatsächlich gelöscht wurden, wenn die Überwachung sich als ergebnislos herausstellte.[88] Insbesondere kritisierte der EGMR das Fehlen einer richterlichen Überprüfung der Überwachungsergebnisse zur Wahrung des Rechtsstaatsprinzips.[89]

Der Gerichtshof verlangt weiters,[90] dass die generelle Kontrolle über das System geheimer Überwachungen nicht einem politischen Amtsträger und Mitglied der Exekutive anvertraut werden darf, der direkt in die Auftragsvergabe für besondere Überwachungsmaßnahmen involviert ist, sondern *externen* unabhängigen Einrichtungen, wie etwa einem vom Parlament oder einer unabhängigen Kommission gewählten Ausschuss,[91] oder einem von diesen bestellten besonderen Kommissar, der ein hohes Richteramt innehat oder dazu qualifiziert ist.[92] Erforderlich ist nach Ansicht des EGMR ebenso, dass die zur geheimen Überwachung zuständige Behörde regelmäßig an eine unabhängige Einrichtung oder die Öffentlichkeit über die gesamte Verwendung des Systems oder die in Einzelfällen angewandten Maßnahmen berichtet.[93] Die Übermittlung von Informationen an andere Dienststellen hat sehr strengen Anforderungen zu unterliegen. Die diesbezüglich notwendige

---

[85] EGMR 28.06.2007 Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien, RN 76, unter Verweis auf das Urteil EGMR 29.06.2006 Weber und Saravia gg. Deutschland, RN 95, mit weiteren Rechtsprechungshinweisen; in EGMR 04.05.2000 Rotaru gg. Rumänien wurde Für den Fall einer Informationssammlung und -speicherung durch einen Geheimdienst ähnlich entschieden.
[86] EGMR 16.02.2000 Amann gg. die Schweiz = ÖJZ 2001, S. 71 ff.
[87] RN 85 des Urteils, im Unterschied zu den Urteilen EGMR 06.07.1978 Klass u.a. gg. Deutschland, RN 70, sowie Weber und Saravia, RN 57.
[88] RN 85 des Urteils unter Verweis auf die gegenteiligen Beispiele in den Fällen Klass u.a. gg. Deutschland, RN 20; EGMR 29.06.2006 Weber und Saravia gg. Deutschland, RN 100;
[89] RN 85 des Urteils.
[90] RN 87 des Urteils.
[91] Wie es im Fall EGMRR 06.09.1978 Klass u.a. gg. Deutschland, RN 53, der Fall war.
[92] Wie es im Fall EGMR Christie, S. 123-130, 135 und 137, der Fall war.
[93] RN 88 des Urteils.

Kontrolle könne etwa einem Beamten, der für die Ausübung eines Richteramts qualifiziert ist, oder einer unabhängigen Kommission anvertraut werden.[94]

II.1.2.3.2 Information der Betroffenen und Rechtsmittel

Im Regelfall ist man sich eines Grundrechtseingriffes durch staatliche Behörden bewusst und kann daher im Falle einer Grundrechtsverletzung alle vorhandenen Rechtsbehelfe ausschöpfen. Nun liegt es aber gerade in der Natur geheimer Ermittlungs- und Überwachungsmaßnahmen, dass die Betroffenen nichts von allfälligen Eingriffen erfahren und daher auch keine allenfalls zur Verfügung stehenden Rechtsmittel ausschöpfen können. Die (zumindest nachträgliche) Information von Betroffenen durch die Behörden ist aber essentielle Voraussetzung dafür, dass diese den Eingriff auf seine Rechtmäßigkeit hin prüfen und sich erforderlichenfalls rechtlich zur Wehr setzen können.

Aus dem Rechtsstaatsprinzip ergeben sich nach der Rechtssprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) konkrete materiell- und prozessrechtliche Anforderungen an das innerstaatliche Recht. So muss das nationale Recht einen hinreichenden und effektiven Schutz vor willkürlichen Rechtseingriffen und vor Missbrauch gewährleisten, wobei der Gerichtshof betont, dass dieses Risiko gerade bei Maßnahmen ohne Wissen des Betroffenen „evident" ist.[95] Einerseits enthält jedes materielle Grundrecht auch bestimmte prozessuale Garantien, die sicherstellen sollen, dass der gesamte materielle Schutzumfang des Grundrechts in einem rechtsstaatlich geordneten Verfahren effektiv geltend gemacht werden kann. Diese Wirkungsebene der Grundrechte wird in der Literatur mit dem Begriff des „status activus processualis"[96] umschrieben. In vielfältigen Zusammenhängen wurden in der Rechtsprechung nationaler Höchstgerichte und des EGMR aus bestimmten materiellen Grundrechten prozessuale Gewährleistungen abgeleitet (zB Art 2, 3 und 8 EMRK), auf die hier nur teilweise eingegangen werden soll. So hat der EGMR etwa in den bekannten „Britischen Fürsorgefällen"[97] festgestellt, dass Art 8 EMRK – soweit es um die Durchsetzung eines aus dem Recht auf Achtung des Familienlebens erfließenden Interesses geht – die gesetzliche Einräumung einer Parteistellung gebietet, damit dieses grundrechtliche Interesse auch verfahrensförmig geltend gemacht werden kann.

Im Fall Klass und andere gegen Deutschland[98] befand der EGMR, dass eine grundsätzlich nach Art 8 EMRK zulässige geheime Überwachungsmaßnahme unter dem Gesichtspunkt eines effektiven Rechtsschutzes nach Art 13 EMRK wegen mangelnder Informationsverpflichtungen zu beanstanden sein kann. Der EGMR gibt wiederholt zu bedenken, dass nach Wegfall der Maßnahme eine Information der Betroffenen im Allgemeinen notwendig ist, um gegen die jeweilige Maßnahme Beschwerde einzulegen. Darüber hinaus muss nach der Rechtsprechung des EGMR das innerstaatliche Recht im Zusammenhang mit geheimen Überwachungsmaßnahmen durch staatliche Behörden wegen des Fehlens öffentlicher Kontrolle und der Gefahr des Machtmissbrauchs bestimmte Schutzvorkehrungen gegen willkürliche Eingriffe in die Rechte nach Art 8 EMRK

---

[94] RN 89 des Urteils unter Verweis auf das Urteil im Fall EGMR 29.06.2006 Weber und Saravia, RN 125-28.
[95] EGMR 02.08.1984 Malone gg. das Vereinigte Königreich = EuGRZ 1985, S. 17 ff.
[96] Ausdruck nach der Status-Lehre Georg Jellineks von Häberle, in: Martens/Häberle/Bachof/Brohm (Hrsg.) in: Grundrechte im Leistungsstaat, 1972, 86 ff.
[97] EGMR 28.02.1983 W. gg. das Vereinigte Königreich.
[98] Vgl EGMR 06.09.1978 Klass u.a. gg. Deutschland = NJW 1979, S. 1755 ff.

vorsehen.[99] Der Gerichtshof fordert überzeugende Nachweise dafür, dass adäquate und effektive Rechtsschutzgarantien gegen einen Missbrauch vorhanden sind. Er beurteilt dies anhand aller Umstände eines Falles, wie etwa nach Wesen, Umfang und Dauer der möglichen Maßnahmen, den Voraussetzungen für ihre Anordnung, den für die Anordnung, Durchführung und Aufsicht über die Maßnahme befugten Behörden, und den im nationalen Recht vorgesehenen Rechtsmitteln.[100]

Schließlich stellt der EGMR im Urteil Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien fest, dass nach bulgarischem Recht die von geheimer Überwachung betroffenen Personen zu keinem Zeitpunkt und unter keinen Umständen über diese Tatsache informiert waren. Nach Auffassung des Gerichtshofes kann die Tatsache, dass die von solchen Maßnahmen betroffenen Personen während der Überwachung oder nach deren Ende nicht auf diese aufmerksam gemacht werden, nicht per se zu dem Schluss führen, dass der Eingriff nicht gemäß Absatz 2 des Artikel 8 gerechtfertigt war, da es gerade die Unwissenheit über die Überwachung ist, die deren Effizienz bewirkt. Allerdings muss eine Information der betroffenen Personen erfolgen, sobald eine solche ohne Gefährdung des Überwachungszweckes nach ihrer Beendigung stattfinden kann.[101] Das Ergebnis ist, dass außer bei einer weiteren Verfolgung aufgrund der erlangten Ergebnisse verdeckter Überwachung oder im Falle eines Informationslecks, die betroffenen Personen nicht herausfinden können, ob sie überhaupt überwacht wurden und es ihnen daher nicht möglich ist, eine Feststellung der Rechts- bzw Konventionswidrigkeit der Überwachungsmaßnahme oder eine Entschädigung für einen rechtswidrigen Eingriff in ihre Rechte nach Art 8 EMRK zu erlangen. Das bulgarische Recht unterließ damit eine wichtige Sicherungsmaßnahme gegen den unzulässigen Einsatz von Überwachungsmaßnahmen.[102]

II.1.3 Die Richtlinie 2006/24/EG im Licht der bisherigen Speicherpraxis[103]

II.1.3.1 Betroffene Datenarten

Bei jeder Telefon-, Internet- und E-Mail-Kommunikation werden bestimmte Daten notwendigerweise erzeugt und verarbeitet. Dabei wird erfasst, wer mit wem wann und wie lange kommuniziert hat: die Standort-Informationen der Kommunikationsteilnehmer zum Zeitpunkt der Verbindung sowie weitere Daten zur Identifizierung der Anschlüsse bzw. der verwendeten Endgeräte. Das betrifft auch

---

[99] Siehe die EGMR Urteile EGMR 28.06.2007 Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien, RN 77; EGMR 06.09.1978 Klass u.a. gg. Deutschland, RN 54-56; EGMR 26.03.1897 Leander gg. Schweden, RN 60-67; EGMR 25.06.1997 Halford gg. das Vereinigte Königreich, RN 49; EGMR 25.03.1998 Kopp gg. die Schweiz, RN 64; und EGMR 29.06.2006 Weber und Saravia gg. Deutschland, RN 94.

[100] Siehe die Urteile in den Fällen EGMR 28.06.2007 Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien, RN 77; EGMR 06.09.1978 Klass u.a. gg. Deutschland, RN 50.

[101] RN 90 des Urteils unter Verweis auf die Urteile EGMR 06.09.1978 Klass u.a. gg. Deutschland, RN 58; EGMR 26.03.1987 Leander gg. Schweden, RN 66; sowie EGMR 29.06.2006 Weber und Saravia gg. Deutschland, RN 135.

[102] RN 91 des Urteils.

[103] In dieses Kapitel weitgehend eingearbeitet wurde ein kürzlich publizierter Aufsatz des Autors: Tschohl, Christof (2011), Der Europäische Vorrat an Daten über Kommunikationsverhalten, in: Bielefeld ua. (Hrsg.), Jahrbuch Menschenrechte (2011), Nothing to hide - nothing to fear? Datenschutz - Transparenz - Solidarität, Böhlauverlag, Wien/Köln/Weimar, 74ff.

Dienste wie SMS und MMS. Beim Internetzugang wird im System eines Anbieters regelmäßig erfasst, mit welcher Internet-Protokoll-Adresse (IP-Adresse) ein Teilnehmer zu einem bestimmten Zeitpunkt eine Internetverbindung hergestellt hat. Dies bedeutet eine starke Relativierung der „Anonymität" im Internet, weil bei vielen Diensten und Anwendungen die „Spur" der *IP*-Adresse gespeichert wird. Kennt man etwa die IP-Adresse zu einem Forumeintrag, so lässt sich diese auf die Person zurückführen, welcher der Anschluss gehört. Allerdings lässt sich daraus nicht ableiten, welche Person tatsächlich den Dienst benutzt hat. Inhalte dürfen nach wie vor nicht gespeichert werden. Abgesehen von den E-Mail-Verbindungsdaten, die durch die Richtlinie zur Vorratsdatenspeicherung nun erfasst sind, werden die eben beschriebenen Daten von allen Telekom- und Internetanbietern unabhängig von der Richtlinie zu Betriebszwecken gespeichert. Die zulässige Speicherdauer hing bisher davon ab, welchem konkreten Zweck die Daten dienten, wobei keine absoluten Löschungsfristen existierten. Ausschließlich technisch bedingte Speicherung ist zumeist nur für eher kurze Zeiträume (einige Tage oder Wochen) notwendig, während rechnungsrelevante Daten je nach Geschäftsmodell und System der Anbieter üblicherweise für drei bis sechs Monate gespeichert werden. Weil hier einiger Spielraum besteht, werden schon bisher die meisten Daten, soweit sie für die Verrechnung relevant sind, bis zu sechs Monate lang gespeichert (sogenannte *„Billing-Daten"*).

Log-Files zur technischen Betriebssicherung (etwa zur Wartung, Störungsbehebung oder Fehlerdokumentation), insbesondere beim Internet-Zugang (Zuordnung einer *IP*-Adresse zu einem bestimmten Teilnehmer), und die Standortdaten bei Mobilfunkverbindungen wurden seit Beginn der großen Digitalisierungs- und Mobilfunkwelle Ende der 90er Jahre von vielen Anbietern nicht selten unbedarft aufbewahrt, ohne konkrete Löschungsfristen vorzusehen. Aus dem Zweck der Verwendung war schlicht keine Bedrohung der Privatsphäre der Nutzer zu sehen. Doch sehr schnell erkannten die Ermittlungsbehörden (Polizei, Staatsanwaltschaft und Gerichte) den Nutzen dieser Informationen und begehrten immer häufiger Auskünfte, zumeist mit Erfolg. Auf Anbieter, die zum Schutz ihrer Kunden im Einzelfall behaupteten, sie hätten die Daten bereits gelöscht, wurde mittels Androhung von Hausdurchsuchungen, Beschlagnahmen oder der Ladung von MitarbeiterInnen als Zeugen teilweise massiv Druck ausgeübt. Diese Situation der Rechtsunsicherheit führte schließlich dazu, dass sich die Telekom-Branche mit Vertretern der Justiz darauf einigte, auch diese Daten regelmäßig für sechs Monate verfügbar zu halten, unabhängig von eigenem betrieblichem Bedarf. Gesetzliche Grundlage gab es dafür keine, vielmehr wurde in guter österreichischer Manier eine Art *„Gentlemen's-Agreement"* getroffen, freilich ohne nachvollziehbare schriftliche Dokumentation.

Das bedeutet zusammengefasst, dass – zumindest in Österreich – schon vor der (hierzulande noch ausstehenden) Umsetzung der Vorratsdatenspeicherungs-Richtlinie die meisten Daten für üblicherweise sechs Monate gespeichert und entsprechend den bestehenden Befugnissen auch an Sicherheits- und Strafverfolgungsbehörden ausgefolgt wurden und werden. Allerdings sind die Aufzeichnungen lückenhaft, weil etwa bei *Flat-Rate*-Tarifmodellen möglicherweise gar keine Verbindungsdaten für die Verrechnung benötigt werden. Eine historische Dokumentation von Senderstandorten im Mobilfunk wird bislang mangels Verpflichtung kaum geführt. Wenn also eine per *„Cell-ID"* identifizierte Funkzelle vor fünf Monaten an einem anderen Standort im Einsatz war, ist dies zumeist nicht nachvollziehbar. Bei Internet-Diensten über Mobiltelefone werden die zugewiesenen *IP*-Adressen regelmäßig gar nicht erfasst. Schließlich findet zu *E-Mail*-Diensten bisher überhaupt keine Protokollierung der Verbindungsdaten statt. Diese „Lücken" wurden nun durch die Richtlinie geschlossen. Die Daten mussten bisher entsprechend der Telekom-Datenschutz-Richtlinie 2002/58/EG gelöscht werden, sobald sie für Betriebszwecke nicht mehr notwendig sind. Weil die

Speicherpflicht unabhängig von einem bestimmten Anlass oder einem konkreten Verdacht auf rechtswidriges Handeln besteht, werden die bisherigen grundsätzlichen Speicherverbote und Löschungsverpflichtungen ins Gegenteil verkehrt.

II.1.3.2 Inhaltliche Vorgaben der Richtlinie

Aufgrund der im Jahr 2006 verabschiedeten Richtlinie 2006/24/EG (Vorratsdatenspeicherungs-Richtlinie) sind sämtliche Anbieter öffentlich zugänglicher Telekommunikationsdienste und Anbieter öffentlicher Kommunikationsnetze (nachfolgend kurz *„Anbieter"*) verpflichtet, das gesamte Kommunikationsverhalten ihrer Nutzer für mindestens sechs Monate bis maximal zwei Jahre zu protokollieren. Die EU-Mitgliedstaaten müssen ihren heimischen Anbietern diese Datenspeicherung auf Vorrat gesetzlich vorschreiben, damit die Daten zur Verfolgung schwerer Straftaten europaweit zur Verfügung stehen. Die Speicherung betrifft alle Nutzer, unabhängig von einem konkreten Verdacht.

Die von den Anbietern vorrätig gespeicherten Daten sollen entsprechend der Vorratsdatenspeicherungs-Richtlinie dem Zweck der Verfolgung schwerer Straftaten, insbesondere Terrorismus und organisierter Kriminalität, dienen. Allerdings ist den Mitgliedstaaten bewusst die Regelung überlassen, was unter „schweren Straftaten" zu verstehen ist bzw. ob die Daten auch für präventive Gefahrenabwehr, für Zwecke der Nachrichtendienste oder für völlig andere Interessen verfügbar sein sollen, etwa für die Verfolgung von Urheberrechtsverletzungen oder andere zivilrechtliche Streitigkeiten. Die Aufklärung schwerer Straftaten dient damit bloß als Argument, den „Bauchladen" mit Daten zu füllen; wer sich daraus bedienen darf, können sich die Mitgliedsstaaten aussuchen. Die Erfahrung lehrt, dass mit der Sammlung umfassender und aufschlussreicher Datenbestände die Flut an Begehrlichkeiten nicht lange auf sich warten lässt. Durchsetzen wird sich wohl, wer im Heimatstaat die stärkste Lobby hat. Dass Regierungen von EU-Staaten Maßnahmen, die in der eigenen Bevölkerung unpopulär sind, wenn möglich gerne auf EU-Ebene beschließen, um den „Schwarzen Peter" dann nach Brüssel zu schieben, ist ebenfalls ein bekanntes Phänomen.

Erstaunlicherweise wird die Richtlinie auf EU-Ebene als reine Maßnahme der Harmonisierung des europäischen Binnenmarkts und nicht einmal teilweise als Maßnahme der „Polizeilichen und Justiziellen Zusammenarbeit in Strafsachen", der vormals sogenannten dritten Säule der EU, gehandelt. Dadurch konnte die Richtlinie praktischerweise mit Mehrheitsbeschluss durch den Rat und das Parlament verabschiedet werden, denn eine (für die damalige dritte Säule notwendige) Einstimmigkeit im Rat wäre politisch nicht zu erreichen gewesen. Zweifel scheinen angebracht, ob eine Marktharmonisierung überhaupt bewirkt werden kann und nicht diskriminierend wäre, wenn die Speicherzeiträume zwischen sechs und 24 Monaten divergieren und einheitliche Regelungen weder zum Ersatz der beträchtlichen Investitionskosten noch zum Zugang zu den Daten existieren. Der EuGH hat die wettbewerbsrechtliche Natur der Richtlinie anlässlich einer Nichtigkeitsklage der Republik Irland, unterstützt durch die Slowakei, dennoch bestätigt (10.2.2009, C-301/06).[104]

[104] Der Vollständigkeit halber sei angemerkt, dass der irischen Regierung seinerzeit die EU-Regelung zur Vorratsdatenspeicherung zu wenig weit ging und nicht etwa Grundrechtsbedenken diese Klage motiviert haben.

Ohne Zweifel betrifft die Speicherpflicht auch den Wettbewerb und erfordert Regelungen im Rahmen des Binnenmarkts. Weil dadurch die Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) in ihrem zentralen Zweckbindungs- und Löschungsgrundsatz abgeändert wurde, war schon rein formal dieselbe Kompetenzgrundlage heranzuziehen. Notwendig gewesen wären aber flankierende Regelungen im Strafrechtsbereich durch einen entsprechenden Rahmenbeschluss. Das Problem besteht nämlich darin, dass sich gar nicht beurteilen lässt, wie schwer der Eingriff in die Grundrechte der Menschen in Europa wiegt, wenn nicht einheitlich und vorab geregelt ist, für welche Zwecke die Daten verwendet werden dürfen, wie der Zugang organisiert ist und welche Rechtsschutzvorkehrungen zu garantieren sind. Die Richtlinie erschöpft sich diesbezüglich in einem Verweis auf den Grundsatz der Verhältnismäßigkeit und Artikel 8 Absatz 2 EMRK, der die legitimen Zwecke zur Beschränkung der Privatsphäre anführt. Die Rechtswissenschaft nennt eine solche Norm „unterdeterminiert".

Die Richtlinie selbst schreibt den Mitgliedstaaten in Art 10 vor, der EU Kommission jährlich statistische Daten zu liefern, mit der die Wirksamkeit der Maßnahme beurteilt werden kann. Nun liegt der erste Bericht der Kommission vor – mit deutlicher Verspätung von mehr als einem halben Jahr – und die geforderten Nachweise fehlen noch immer. Der Bericht hält dazu fest: „Dieses Ziel konnte bislang nicht erfüllt werden, weil die meisten Mitgliedstaaten die Richtlinie erst in den vergangenen zwei Jahren vollständig umgesetzt und zudem die Quellen der statistischen Daten unterschiedlich ausgelegt haben."[105]

In Österreich wurde die Richtlinie zur Vorratsdatenspeicherung nun umgesetzt, nachdem massive Bedenken im Hinblick auf die Wahrung von Grundrechten diesen Prozess lange verzögert hatten.[106] Die rechtliche Umsetzung wird dabei primär im Telekommunikationsgesetz (TKG 2003) erfolgen, weil dieses Gesetz die Anbieter von Kommunikationsdiensten (nachfolgend kurz: Anbieter) adressiert und hier der Kern der Richtlinie, die Speicherpflicht der Verkehrsdaten zur elektronischen Kommunikation, normiert werden muss. Die Verwendung der Daten und die prozessualen Regeln dazu werden demgegenüber in der Strafprozessordnung (StPO) und im Sicherheitspolizeigesetz (SPG) normiert.

Die Richtlinie zur Vorratsdatenspeicherung gestattet nicht, dass Inhaltsdaten gespeichert werden (ausdrücklich Art 1 (2) RL 2006/24/EG). Unzulässig wäre daher, wenn Anbieter von Internet-Zugangsdiensten die aufgerufenen Internet-Adressen (URL) speichern würden. Gespeichert werden jedoch die Informationen, welcher Teilnehmer zu welchem Zeitpunkt mit welcher Internet-Protokoll

---

[105] „Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24/EG)" der EU Kommission, http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_de.pdf (18.4.2011), S 23; Eine ausführliche Zusammenfassung aller Bedenken auf Ebene der europäischen Zivilgesellschaft und die Widerlegung der beschwichtigenden Ausführungen des Kommissionsberichts enthält der parallel dazu veröffentlichte „Schattenbericht" der European Digital Rigts (EDRi), http://www.edri.org/files/shadow_drd_report_110417.pdf (18.4.2011).

[106] Weil Österreich dieser Richtlinie im Jahr 2006 aber zugestimmt hat und in der Folge auch die Klagemöglichkeit dagegen ungenutzt ließ, kann die Frage der Grundrechtskonformität der Richtlinie selbst jedoch letztlich nur durch den EuGH europarechtlich entschieden werden. Wenn Österreich die Richtlinie bis Anfang Mai 2011 nicht umsetzt, sind empfindliche Strafzahlungen an die EU unvermeidbar. Lesen Sie dazu ausführlich Tschohl, Stellungnahme zur TKG-Novelle 2010 im Rahmen des parlamentarischen Begutachtungsverfahrens, 15.1.2010, http://www.parlinkom.gv.at/PG/DE/XXIV/ME/ME_00117_B9/pmh.shtml (18.4.2011).

Adresse (IP-Adresse) eine Verbindung zum Internet hergestellt hat. Durch IP-Adressen können Rechner im Internet oder einem lokalen IP-Netzwerk (LAN) eindeutig identifiziert und adressiert werden.

II.1.4 Die neue Rechtslage nach Umsetzung der Vorratsdatenspeicherung

Nach einer langen und intensiven Vorbereitungsphase wurde am 28. April 2011 im Nationalrat die Umsetzung der Vorratsdatenspeicherungs-Richtlinie 2006/24/EG beschlossen. Damit wird nun die flächendeckende und verdachtsunabhängige Speicherung von Verkehrs- und Standortdaten auch in den Österreichischen Rechtsbestand Einzug halten. Die Umsetzung erfolgte dabei einerseits durch eine Novelle zum TKG 2003[107], andererseits durch flankierende Novellierung der relevanten Bestimmungen in der StPO sowie im SPG[108]. Nachfolgend sollen jene Regelungsbereiche der neuen Rechtslage dargestellt werden, die zu den Fragen zur Datensicherheit eine Berührung aufweisen.[109]

II.1.4.1 Die Unterscheidung „Vorratsdaten" und „betriebsnotwendige Daten"

Eine einheitliche Speicherfrist von 6 Monaten besteht nun künftig im Rahmen der Vorratsdatenspeicherung gemäß § 102a TKG. Der Begriff „Vorratsdaten" ist dabei gesetzlich in § 92 (3) Z 6b TKG definiert. Es handelt sich dabei nicht um eine neue Kategorie von Daten, vielmehr sind davon Verkehrsdaten und die damit verbundenen Stammdaten erfasst. Die Unterscheidung liegt also nicht in der Art der Daten sondern in der Zweckbestimmung der Speicherung. Wenn nämlich Verkehrsdaten für betriebliche Zwecke nicht mehr benötigt werden, müssen sie grundsätzlich gelöscht werden. Aufgrund der Speicheranordnung in § 102a TKG müssen bestimmte Verkehrsdaten aber nunmehr für 6 Monate jedenfalls aufgezeichnet werden. Wenn die Verkehrsdaten nur noch deshalb gespeichert sind, handelt es sich um Vorratsdaten.

Die Unterscheidung hat mehrerlei Konsequenzen. Die Speicherung erfolgt „ausschließlich zur Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs. 2 a StPO rechtfertigt" (§ 102a (1) TKG). Das heißt also, dass die Anbieter diese Daten für eigene Zwecke gar nicht verarbeiten dürfen. Daher ordnet § 102c (1) TKG auch an, dass die Speicherung der Vorratsdaten so zu erfolgen hat, dass „ eine Unterscheidung von nach Maßgabe der §§ 96, 97, 99, 101 und 102 gespeicherten Daten möglich ist". Diese Vorschrift bedeutet, dass die Anbieter Vorratsdaten zwar nicht physisch getrennt (z.B. in einem anderen Data-Warehouse), aber doch logisch getrennt – d.h. in einer eigenen Datenbank – speichern müssen. Dazu kommt, dass die Anbieter schon in ihrem Datenbanksystem technisch und organisatorisch gewährleisten müssen, dass Zugriffe nur nach dem 4-Augen-Prinzip erfolgen und jeder Zugriff revisionssicher protokolliert wird (§ 102c (2) TKG). In Bezug auf Vorratsdaten besteht zudem eine europarechtliche Verpflichtung nach Art 10 der RL 2006/24/EG jährliche eine Statistik über die Verwendung dieser Daten zu übermitteln.

---

[107] BGBl I 27/2011, basierend auf RV 1074 BlgNR XXIV. GP.
[108] BGBl I 33/2011, basierend auf RV 1075 BlgNR XXIV. GP.
[109] Eine gute Übersicht samt starker aber doch berechtigter Kritik zur österreichischen Umsetzung bieten Feiler/Stahov, Die Einführung der Vorratsdatenspeicherung in Österreich, Medien und Recht 3/11, 111 ff.

Eine weitere Konsequenz ist, dass eine Auskunft über Vorratsdaten gemäß § 102b (1) TKG „ausschließlich aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft zur Aufklärung und Verfolgung von Straftaten [zulässig ist], deren Schwere eine Anordnung nach § 135 (2a) StPO rechtfertigt". Hier wurde mit einem grammatikalischen Kunstgriff bewusst vermieden, den Begriff „schwere Straftaten" zu verwenden, den die Richtlinie zur Vorratsdatenspeicherung vorgibt. Doch von diesem Grundsatz gibt es weitreichende und schwerwiegende Ausnahmen, die in § 99 (5) Z 2 bis 4 TKG vorgezeichnet sind und sich erst durch die korrespondierenden Bestimmungen in § 76a (2) StPO und § 53 (3a) und (3b) SPG voll erschließen. Dazu jedoch näheres in Kapitel 2.1.

Den Anbietern bleibt ein veritabler Freiraum, entsprechend den jeweiligen betrieblichen und technischen Notwendigkeiten selbst zu definieren, wann die gespeicherten Verkehrsdaten zu Vorratsdaten werden und daher in die „Vorratsdatenbank" überführt bzw. in den betriebsinternen Systemen gelöscht werden. Die Gestaltung der Tarifmodelle und die Art der technischen Erfassung der Verrechnungsrelevanten Kriterien spielen dabei eine zentrale Rolle. Für IP-Adressen Logfiles besteht aber kaum eine Rechtfertigung, diese länger als ein paar Stunden im live System zu halten und dann unverzüglich als Vorratsdaten zu kennzeichnen. E-Mail Verkehrsdaten sind in keinem bekannten Anbietermodell verrechnungsrelevant und müssen auch zu technischen Zwecken nicht gespeichert werden. Diese Daten werden daher von der ersten Erfassung an Vorratsdaten sein. Ein gewisser Druck besteht für die Anbieter jedoch, ihre jeweilige Speicherpolitik von vornherein transparent nach außen zu kommunizieren. Denn einerseits wollen die Sicherheitsbehörden schon im Vorhinein abschätzen können, auf welche Rechtsgrundlage sie ein Auskunftsbegehren stützen. Andererseits wird mit In Kraft treten der TKG Novelle zu erwarten sein, dass viele Kunden ein datenschutzrechtliches Auskunftsbegehren nach § 26 DSG erheben werden. Klare und transparente Regelungen könnten hier einen enormen Arbeitsaufwand für die Rechtsabteilungen der Unternehmen verhindern.

II.1.4.2 Datentypen im Einzelnen

II.1.4.2.1 Datenkategorien aus rechtlicher Sicht

Bei jedem Kommunikationsvorgang werden bestimmte Daten verarbeitet bzw. erzeugt. Diese Daten werden von den Netz- bzw. Dienstanbietern zu Betriebszwecken gespeichert, zum Teil aus technischen Gründen, zum Teil für die Rechnungslegung bzw. Vertragsabwicklung. Die Daten müssen gemäß § 99 Telekommunikationsgesetz (TKG) gelöscht werden, sobald sie für Zwecke der Entgeltverrechnung oder des technischen Betriebes nicht mehr notwendig sind. Die Dauer der Aufbewahrung hängt davon ab, welchem Zweck die Daten dienen. Ausschließlich technisch bedingte Speicherung ist zumeist nur für eher kurze Zeiträume (einige Tage oder Wochen) notwendig, während rechnungsrelevante Daten je nach Geschäftsbedingungen des Anbieters üblicherweise mindestens zwischen 3 und 6 Monaten gespeichert werden. Die Zeiträume unterscheiden sich je nach System der Anbieter. Eine einheitliche Aufbewahrungsfrist von mindestens 6 Monaten aber höchstens 2 Jahren wird es erst geben, wenn die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung

in innerstaatliches Recht umgesetzt wird, was in Österreich derzeit noch nicht der Fall ist.[110] Das Telekommunikationsgesetz (TKG) definiert drei Kategorien von Daten:

II.1.4.2.1.1 STAMMDATEN

Ermittlungsrelevante Informationen über die Kommunikation von Teilnehmern müssen auf bestimmte Personen zurückgeführt werden. In der Praxis werden Auskünfte über die Stammdaten eines bestimmten Anschlusses oder über den Absender einer bestimmten Nachricht begehrt. Ein Anbieter kann dabei nur dann eine zuverlässige Auskunft erteilen, wenn die Polizei den Zeitpunkt bzw. einen möglichst genauen Zeitraum der Nachrichtenübermittlung bekannt gibt. Die Rechtsgrundlage dafür ist im Präventiven Bereich § 53 Abs 3a Z 1 SPG, im Anwendungsbereich der StPO ist die gesetzliche Grundlage systematisch unpassend im Telekommunikationsgesetz selbst zu finden (§ 103 Abs 4 TKG). Für Auskünfte über Stammdaten gibt es keine Einschränkungen auf bestimmte Delikte oder Mindeststrafdrohungen. Erforderlich ist weder ein Gerichtsbeschluss noch eine Anordnung der Staatsanwaltschaft. Für Stammdatenauskünfte ist das rechtliche Schutzniveau am geringsten.

II.1.4.2.1.2 VERKEHRSDATEN

Verkehrsdaten werden zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet (§ 92 Abs 3 Z 4 TKG). Es handelt sich um die äußeren (vom Inhalt unabhängigen) Informationen über einen Kommunikationsvorgang, vereinfacht also: Wer, mit wem, wann, wie lange, welcher Anschluss, welcher Dienst. Bei Telefonverbindungen sind dies die Ruf- bzw. Teilnehmernummer der Kommunikationspartner, der Zeitpunkt des Beginns und die Dauer der Verbindung. Bei Mobilfunkverbindungen werden darüber hinaus auch die eindeutige Kennung der SIM-Karte (IMSI) sowie die eindeutige Kennung des Endgerätes (IMEI) erfasst. Beim Aufbau einer Internetverbindung wird bei allen Internet-Zugangsanbietern die Internet-Protokoll-Adresse (IP-Adresse) protokolliert, die dem jeweiligen Teilnehmer dabei zugewiesen wurde. Die Internet-Zugangsanbieter dürfen jedoch nicht aufzeichnen, welche Internetseiten vom Teilnehmer aufgerufen wurden. Bei E-Mail Diensten zählen die E-Mail Adresse und die IP-Adresse, mit welcher der Zugriff auf das E-Mail Konto erfolgte, zu den Verkehrsdaten.

II.1.4.2.1.3 UNTERFALL DER VERKEHRSDATEN: ZUGANGSDATEN

Zugangsdaten stellen eine Unterkategorie der Verkehrsdaten dar. Es handelt sich hierbei um „Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz

---

[110] Ein Begutachtungsentwurf des Bundesministeriums für Verkehr, Innovation und Technologie (BMVIT), ausgearbeitet vom Ludwig Boltzmann Institut für Menschenrechte (BIM) im Auftrag des BMVIT, befand sich bis 15.1.2010 in öffentlicher Begutachtung: http://www.parlinkom.gv.at/PG/DE/XXIV/ME/ME_00117/pmh.shtml (abgerufen am 30.3.2010). Siehe dazu die Stellungnahme des BIM, in der die verdachtsunabhängige und flächendeckende Speicherung aller Verbindungsdaten als grundrechtswidrig abgelehnt wird: http://www.parlinkom.gv.at/PG/DE/XXIV/ME/ME_00117_B9/pmh.shtml (abgerufen am 30.3.2010).

beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für die Kommunikation verwendeten Netzwerkadressierung zum Teilnehmer notwendig sind“ (§ 92 Abs 3 Z 4a TKG). Somit gilt im Prinzip, das zu den Verkehrsdaten gesagte. Die IP-Adresse des Teilnehmers, die mit Herstellung der Internetverbindung durch den Anbieter dem Teilnehmer zugewiesen wird, ist somit nicht nur im allgemeinen Verkehrs- sondern im speziellen auch Zugangsdatum.[111]

II.1.4.2.1.4 STANDORT-DATEN

Bei Mobilfunkverbindungen enthält jeder Verbindungs-Datensatz die Kennung der Funkzelle (Cell-ID) zu Beginn der Verbindung - also die Information über den geographischen Standort des Mobilen Endgeräts (Mobiltelefon, mobiles Internet-Modem). Bei diesen Daten handelt es sich um Standortdaten im Sinne des § 92 Abs 3 Z 6 TKG. Die Speicherung dieser Information ermöglicht die Auswertung von Senderstörungen, sowie eine Abschätzung der Senderkapazitäten.

II.1.4.2.2 DATENKATEGORIEN AUS TECHNISCHER SICHT

Die folgende Darstellung zielt darauf ab, ein Verständnis dafür zu schaffen, welchen Aussagegehalt und damit Nutzen diese Daten überhaupt für polizeiliche Ermittlungen haben. Dies soll für jede in der Praxis relevante Art von Daten einzeln ausgeführt werden.

II.1.4.2.2.1 IMSI (INTERNATIONAL MOBILE SUBSCRIBER IDENTITY)

Diese Nummer ist die eindeutige, weltweit einzigartige Teilnehmerkennung in Mobilfunknetzen. Technisch vereinfacht gesprochen stellt die IMSI den Link zwischen SIM-Karte eines mobilen Endgeräts und der Rufnummer beim Anbieter her. Wenn der Teilnehmer z.B. seine Rufnummer beim selben Anbieter ändern lässt, kann er weiterhin dieselbe SIM-Karte verwenden, die IMSI bleibt dieselbe und ist weltweit einmalig (im Gegensatz zur Rufnummer, die einem anderen Teilnehmer später zugeordnet werden kann). Die IMSI ist in jedem Gesprächsdatensatz enthalten.

II.1.4.2.2.2 IMEI (INTERNATIONAL MOBILE STATION EQUIPMENT IDENTITY):

Die IMEI identifiziert eindeutig jedes GSM- oder UMTS-Endgerät, die Nummer ist in jedem Rufdatensatz enthalten. Über die IMEI ist auch der Gerätetyp bzw. der Hersteller identifizierbar. Diese Information kann z.B. zur Fehlersuche nützlich sein, wenn Kundenbeschwerden sich häufen und bestimmte Fehlerbilder typisch für bestimmte Produkte sind. Zu Marketingzwecken (z.B. um gezielte Angebote auf den Markt zu bringen) kann für den Anbieter interessant sein, welche Geräteserien besonders häufig im Einsatz sind, wobei diese Auswertungen anonym erfolgen müssen (vgl. § 99 TKG). Bei Sperrung der IMEI kann das Gerät nicht mehr benützt werden, zumindest mit keiner SIM-Karte dieses Anbieters. Allerdings führt mittlerweile kein Anbieter in Österreich solche Sperrungen durch, weil die meisten Endgeräte eine willkürliche Änderung der IMSI zulassen. In

[111] Vgl. dazu auch OGH GZ 15Os172/10y und OLG Linz GZ 9Bs35/05v m.w.N.

manchen EU-Staaten gibt es diese Praxis aber noch. Üblicherweise wird lediglich auf Kundenanfrage die SIM-Karte des gestohlenen Geräts gesperrt, das Gerät kann aber mit anderen SIM-karten weiter verwendet werden. Die IMEI ist grundsätzlich in jedem Datensatz für abgehende Gespräche enthalten, wird aber nicht in jedem Fall in die Datensätze der passiven Seite übernommen.

II.1.4.2.2.3 PUK (PIN UNLOCK KEY):

Wenn ein Mobiltelefon durch einen PIN-Code (Personal Identification Number) gesperrt ist, wird für die Entsperrung der PUK benötigt. Mittels Eingabe des PUK Codes kann das Gerät entsperrt werden, dadurch können am Gerät gespeicherte Informationen wie gewählte Rufnummern, angenommene Anrufe, Anrufe in Abwesenheit, SMS Inhalte etc. herausgelesen werden. Dafür muss man über das Gerät verfügen.

II.1.4.2.2.4 INTERNET PROTOKOLL (IP)-ADRESSEN:

Durch IP-Adressen können Rechner im Internet oder einem lokalen IP-Netzwerk (LAN) eindeutig identifiziert und adressiert werden. Jedem Rechner wird, um an der Datenübertragung und Kommunikation im Internet teilnehmen zu können, eine IP-Adresse für die Dauer der Verbindung zugewiesen. Die Rechner kommunizieren dabei über das TCP/IP-Protocol[112] miteinander.

Die TKG-Novelle unternimmt in § 92 (3) Z 16 TKG erstmals eine Legaldefinition, was in dieser Hinsicht unter einer IP-Adresse zu verstehen ist: „'Öffentliche IP-Adresse' eine einmalige numerische Adresse aus einem Adressblock, der durch die Internet Assigned Numbers Authority (IANA) oder durch eine regionale Vergabestelle (Regional Internet Registries) einem Anbieter eines Internet-Zugangsdienstes zur Zuteilung von Adressen an seine Kunden zugewiesen wurde, die einen Rechner im Internet eindeutig identifiziert und im Internet geroutet werden kann. (...)“ Durch die Einschränkung, dass nur „öffentliche IP-Adressen“ der Speicherpflicht unterliegen – technisch determiniert durch das Kriterium der „Routbarkeit im Internet“ - sind dabei keine IP-Adressen erfasst, die innerhalb eines privaten TCP/IP Netzwerkes vergeben werden. Private Netzwerke – mögen sie auch von großem Umfang sein, wie etwa das Netzwerk des Zentralen Informatik Dienst (ZID) der Universität Wien – unterliegen daher nicht der Speicherpflicht im Rahmen der Vorratsdatenspeicherung.[113]

II.1.4.2.2.5 E-MAIL

Ebenfalls neu ist die Legaldefinition der E-Mail in § 92 (3) Z 12 TKG: „'E-Mail' elektronische Post, die über das Internet auf Basis des „Simple Mail Transfer Protocol“ (SMTP) versendet wird;“ Ergänzt wird dies um die Definition in § 92 (3) Z 15 TKG: „'E-Mail-Dienst' einen Kommunikationsdienst im Sinne

---

[112] Transmission Control Protocol and Internet Protocol. TCP steht für den virtuellen beiderseitigen Kommunikationskanal unter Verwendung des Internet Protocol (IP), welches die Adressierung im Netz festlegt.

[113] Vgl. dazu die EB zur RV § 92 (3) Z 16, Nr. 1074, XXIV. GP, http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01074/fname_206854.pdf (18.4.2011). Sämtliche dem Parlament als Regierungsvorlage vorgelegten Dokumente zur TKG Novelle sowie die Berichterstattung aus dem zuständigen Ausschuss für Forschung, Innovation und Technologie (FIT) sind abrufbar unter http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01074/index.shtml.

von § 3 Z 9, welcher den Versand und die Zustellung von E-Mails auf Basis des „Simple Mail Transfer Protocol“ (SMTP) umfasst;“ Durch die Einschränkung auf Dienste, die mittels SMTP Protokoll operieren, sind jedenfalls nur klassische E-Mail-Dienste von der Speicherpflicht betroffen, Chat-Dienste oder sonstige Einrichtungen zur elektronischen Kommunikation auf Basis anderer technischer Protokolle sind nicht erfasst. Web-Mail-Dienste sind daher grundsätzlich genauso speicherpflichtig, allerdings hängt dies auch davon ab, ob es sich überhaupt um einen „Kommunikationsdienst“ iSd § 3 Z 9 TKG handelt – also insbesondere, ob eine „gewerbliche Dienstleistung“ im Sinne dieser Bestimmung vorliegt – und ob dieser Dienst auch öffentlich zur Verfügung steht. Denn nach § 102a (1) TKG, der zentralen Bestimmung zur Vorratsspeicherung, sind überhaupt nur „Anbieter von *öffentlichen* Kommunikationsdiensten“ speicherpflichtig. Schließlich stellt sich speziell bei E-Mail-Diensten die Frage, ob der jeweilige Anbieter der inländischen Rechtslage unterliegt, was ohne Sitz oder Niederlassung im Inland nicht der Fall ist. Wer also mit seinem E-Mail Verkehr der Vorratsdatenspeicherung entgehen will, kann sich für einen Anbieter entscheiden, der in einem Land ohne Pflicht zur vorrätigen Speicherung seinen Sitz hat und die Verkehrsdaten auch tatsächlich nicht speichert.

II.1.4.3 Die indirekte Überwachung von Inhalten

Das Interesse der Sicherheitsbehörden an einer Auskunft über einen – hinter einer IP-Adresse stehenden – Teilnehmer besteht überhaupt nur darin, einen bereits bekannten Inhalt (z.B. die Nutzung eines Online-Dienstes, den Zugriff auf eine Website oder den Eintrag in einem Online-Forum) einer bestimmten Person zuordnen zu können. Der Inhalt ist also schon vorher bekannt, bleibt aber ohne die Verkehrsdatenauskunft, die erst den Personenbezug herstellt, anonym. Die Information darüber, welchem Teilnehmer eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, stellt sozusagen den „missing link“ her, um öffentlich bekannte oder bei einem Dienstanbieter ausgeforschte Kommunikationsinhalte mit einer bestimmten Person zu verbinden. Zwar dürfen Internet-Zugangsanbieter wie gesagt nicht aufzeichnen, welche Internetseiten vom Teilnehmer aufgerufen wurden. Allerdings sind viele Internetseiten bzw. -dienste technisch derart konzipiert, dass bei Zugriffen auf diese Seiten oder Dienste die IP-Adresse des Teilnehmers sowie der Zeitpunkt des Zugriffs durch den Host-Anbieter[114] protokolliert und bei manchen Anwendungen auch mit bestimmten Inhalten verknüpft wird (zB bei Einträgen in einem Online-Forum). Bei vielen Online-Diensten existieren auch Aufzeichnungen über das konkrete Nutzungsverhalten (z.B. Einkäufe bei Amazon.com, EBay, Suchanfragen bei Google,…).

Gleichzeitig lässt sich daraus noch nicht ableiten, ob der Anschlussinhaber auch mit dem Urheber der Kommunikation identisch ist. Die Information ist vielmehr bloß ein erster Ermittlungsansatz. Die Zuordnung von Verbindungsdaten (insbesondere IP-Adressen) zu einer bestimmten Person lässt selbst keine Rückschlüsse darüber zu, ob diese Person auch tatsächlich am fraglichen Kommunikationsvorgang beteiligt war. Hierzu bedarf es weiterer konkretisierender Indizien, welche gerade bei der Erforschung von Kommunikationsvorgängen im Internet häufig schwer fassbar sind. Anschaulich lässt sich eine IP-Adresse als eine Art KFZ-Kennzeichen auf dem „Datenhighway“

[114] Host-Provider ist jener Dienstanbieter, der den Speicherplatz für Web-Seiten zur Verfügung stellt. Zu den verschiedenen Arten von Providern siehe die Web-Seite des Datenschutzexperten und Richter des OLG Salzburg, Franz Schmidbauer: http://www.internet4jurists.at/provider/provider1a.htm (18.4.2011).

beschreiben. Vielfach wird daher eine Art „IT-Lenkererhebung“ erforderlich sein, um Aussagekraft und Zuverlässigkeit der ermittelten Daten beurteilen zu können; denn eine reine Gefährdungshaftung für Inhaber von Internet- oder Telefonanschlüssen ist der österreichischen Rechtsordnung bislang nicht bekannt. Der Aussagekraft und mit ihr verbunden dem tatsächlichen Nutzen der Daten für den angestrebten Zweck kommen für die Verhältnismäßigkeit der behördlichen Befugnisse entscheidende Bedeutung zu, die bereits abstrakt in jeden Abwägungsvorgang mit einzubeziehen sind.

Die Judikatur des OGH in Strafsachen behandelte Auskünfte über Name und Anschrift zu einer bestimmten (bereits bekannten) IP-Adresse bisher als Stammdatenabfrage nach § 103 (4) TKG. Dass der Anbieter im Falle von dynamischen IP-Adressen für die Auskunft intern die Aufzeichnung der Zugangsdaten (also Verkehrsdaten) auswerten muss, wurde nach dieser sogenannten „Ergebnisorientierten“ Sichtweise für unbeachtlich erklärt[115]. Damit bestanden schon bisher in Bezug auf IP-Adressen keine materiellen Einschränkungen auf bestimmte schwerere Delikte. Richtervorbehalt oder sonstige Formerfordernisse mit Rechtsschutzcharakter gibt es bei Stammdatenauskünften ebenso keine, vielmehr ist sogar die Kriminalpolizei ohne Anordnung der Staatsanwaltschaft auskunftsberechtigt.

Diese Auslegung verkennt völlig, dass diese Ermittlungsbefugnisse eigentlich eher in der Nähe einer Inhaltsüberwachung anzusiedeln ist. Allerdings sind eben zumindest zwei Ermittlungsschritte notwendig. Zunächst muss nämlich beim Dienstanbieter die IP-Adresse zum ermittlungsrelevanten Inhalt erheben, die Rechtsgrundlage dafür bietet § 18 (4) E-Commerce Gesetz (ECG). Oder diese Information ist auf anderem Weg bekannt geworden, etwa durch Beschlagnahme oder Auswertung eines Servers. Aus dieser Perspektive liegen zunächst noch gar keine personenbezogenen Daten vor, weil der Dienstanbieter nach ECG den Bezug zu einem bestimmten Teilnehmer selbst gar nicht herstellen kann. Dieser Bezug ergibt sich erst aus dem zweiten Ermittlungsschritt durch die Auswertung beim Internet-Zugangsanbieter. Weil sich das Ausmaß dieses Eingriffs in das Datenschutzgrundrecht aber erst „über 2 Ecken“ erschließt, scheint der eher sorglose Umgang mit dieser Eingriffsermächtigung weiter zu bestehen.

Im Zivilrecht hat der OGH in einer der zu diesem Thema bedeutendsten Entscheidungen in jüngerer Zeit zu GZ 4 Ob 41/09x (Rechtssache LSG gg Tele 2) diese Problematik unter ausdrücklichem Bezug auf die strafrechtliche Judikatur erkannt, wonach dynamische IP-Adressen jedenfalls als Verkehrsdaten zu behandeln sind[116]. Mit der Legaldefinition der öffentlichen IP-Adresse in § 92 (3) Z 16 TKG in Verbindung mit der ausdrücklichen neuen Rechtsgrundlage für Stammdatenauskünfte an Justizbehörden in § 90 (7) TKG löst der Gesetzgeber diese Judikaturdivergenz nun auf.[117] Sachlich besteht das Problem auf Grund der weiten Ausnahmen über § 99 (5) TKG in Verbindung mit § 76a (2) StPO aber fast unverändert weiter (Details dazu sogleich).

---

[115] Siehe OGH 26.7.2005, 11 Os 57/05z.

[116] So im Ergebnis auch VfGH G 31/08 vom 1. Juli 2009, wenngleich diese Frage dort nicht mit derselben Tiefe behandelt wird, sondern lediglich die Speicherverpflichtung thematisiert wird.

[117] Vgl. dazu die EB zur RV § 90 (7) sowie zu 92 (3) Z 16, Nr. 1074, XXIV. GP, http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01074/fname_206854.pdf (11.10.2011).

II.1.4.4 Ermittlungsbefugnisse der Justiz- und Sicherheitsbehörden

II.1.4.4.1 Abgrenzung StPO - SPG

Die Anbieter sind verpflichtet, der Polizei die oben beschriebenen Daten auf Anordnung mit unterschiedlichen formellen Voraussetzungen jederzeit herauszugeben. Die Polizei handelt dabei entweder im Auftrag eines Gerichts bzw. der Staatsanwaltschaft im Rahmen der Strafprozessordnung (StPO) als Kriminalpolizei, oder im Rahmen der Erfüllung ihrer Aufgaben nach dem Sicherheitspolizeigesetz (SPG). Dabei überlagern sich die Aufgabenbereiche teilweise, besonders im Bereich der organisierten Kriminalität, wo die Polizei innerhalb und außerhalb konkreter Strafverfahren nicht selten im selben Umkreis ermittelt. Manche Befugnisse kommen der Polizei sowohl nach der StPO als auch nach dem SPG zu, jedoch zum Teil mit unterschiedlichen Bedingungen bezüglich Voraussetzungen, Genehmigungserfordernissen, Informationspflichten und Rechtsschutzvorkehrungen. Die jeweiligen Anwendungsbereiche lassen sich dabei grob wie folgt voneinander abgrenzen: Die Aufklärung und Verfolgung bereits begangener Straftaten erfolgt nach den Regeln der StPO, das gilt insbesondere auch, wenn durch die fraglichen Tathandlungen bereits ein strafbarer Versuch vorliegt. Demgegenüber erfolgen die Abwehr einer drohenden Gefahr sowie die allgemeine Gefahrenerforschung nach den Regeln des SPG, also regelmäßig in einem Stadium vor der tatsächlichen Ausführung der Straftat. Schwierig wird die Abgrenzung immer dann, wenn bereits ein gerichtlich strafbarer Tatbestand verwirklicht wurde, die Gefahr aber noch immer andauert, z.B. nicht selten im Falle einer gefährlichen Drohung (§ 107 StGB) oder der Entführung einer Person (§§ 100 ff StGB).

II.1.4.4.2 Ermittlungsbefugnisse nach der StPO

Im StPO Bereich liegt die Verantwortung für die Ermittlungen bei der Staatsanwaltschaft. Grundsätzlich darf ein Anbieter Verkehrsdaten, die noch zu Betriebszwecken gespeichert sind, nur aufgrund einer schriftlichen und gerichtlich bewilligten Anordnung an die Polizei ausfolgen. Die faktische Abwicklung aller Verkehrsdatenauskünfte erfolgt jedoch in der Praxis fast ausschließlich durch die Kriminalpolizei. Zulässig ist eine Auskunft jedenfalls, „wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können“ (§ 135 (2) Z 3 StPO). Betrifft eine Auskunft Vorratsdaten, ist das Auskunftsbegehren auf die neue Bestimmung des § 135 (2a) StPO zu stützen, wobei jedoch die Voraussetzungen die selben sind, also eine Strafdrohung von mehr als einem Jahr und eine gerichtliche Bewilligung. Dabei sind § 102b TKG und § 135 (2a) StPO korrespondierende Normen.

In Bezug auf IP-Adressen und E-Mail Verkehrsdaten besteht jedoch eine wesentliche Ausnahme, mit der diese Ermittlungsbefugnisse aus der Grundsatzkonstruktion der Auskunft über Daten einer Nachrichtenübermittlung (Strafdrohungsgrenze und Richtervorbehalt) herausgelöst wurden. Hier korrespondieren § 99 (5) Z 2 TKG und § 76a (2) StPO. Demnach sind Auskünfte über diese Daten, auch wenn sie Vorratsdaten sind, ohne jede Einschränkung auf Strafdrohungen oder bestimmte

Straftatbestände für den gesamten Bereich des gerichtlichen Strafrechts zulässig.[118] Auch der Richtervorbehalt gilt diesbezüglich nicht, die Maßnahme muss lediglich vom Staatsanwalt angeordnet werden. Weil es bei Auskünften nach § 76a (2) StPO keine „Betreiberanordnung" gemäß § 138 (3) StPO gibt, würde es nach derzeitiger Rechtslage auch keinen Kostenersatz nach der Überwachungskostenverordnung (ÜKVO) geben. Es ist jedoch zu erwarten, dass hier im Zuge der notwendigen Anpassung der ÜKVO noch ein Kompromiss zwischen der Justiz und der Telekom-Branche geben wird.

Die primäre Intention dieser Bestimmung bei der Entstehung war, die Zulässigkeit von Auskünften über Teilnehmer hinter einer dynamischen IP-Adresse auch für den niederschwelligen Strafrechtsbereich (also bei Strafdrohungen bis zu einem Jahr) zu normieren. Rechtspolitisch lässt sich das völlige Fehlen materieller Einschränkungen und einer richterlichen Genehmigung mit der bisherigen Praxis erklären, IP-Adressen Auskünfte als reine Stammdatenabfragen zu qualifizieren. Grundrechtlich rechtfertigen lässt sich das Ergebnis damit jedoch nicht, insbesondere nicht für die Ausnahme bezüglich E-Mail Daten. Damit wird nämlich zulässig, selbst für jedes Bagatelldelikt eine Auskunft über den gesamten aktiven E-Mail Verkehr (d.h. alle Emails, die von dieser Adresse aus versendet wurden) in den letzten 6 Monaten ohne richterliche Genehmigung zu verlangen.

II.1.4.4.3 ERMITTLUNGSBEFUGNISSE NACH DEM SPG

Das SPG ist maßgeblich, wenn es nicht um die Aufklärung bereits begangener Straftaten, sondern um die Abwehr bzw. Vorbeugung bevorstehender gefährlicher Angriffe geht, aber auch im Rahmen der ersten allgemeinen Hilfeleistungspflicht (§ 19 SPG).

Mit der am 1.1.2008 in Kraft getretenen Novelle des SPG[119] wurde – insbesondere über § 53 Abs 3a und Abs 3b SPG – die Erteilung von Auskünften über personenbezogene Verkehrs- und Standortdaten durch Anbieter öffentlicher Telekommunikationsdienste an Sicherheitsbehörden neu geregelt. Neben der bereits bisher bestehenden Befugnis zur Ermittlung von Stammdaten (vgl. § 53 Abs 3a Z 1 SPG) sind nunmehr die Sicherheitsbehörden ausdrücklich ermächtigt, von Anbietern von Telekommunikationsdiensten und sonstigen Dienstanbietern kostenlos Auskunft zu IP-Adressen zu verlangen. Begehrt wird entweder die IP-Adresse zu einer - anhand relevanter Kriterien, etwa Pseudonym, Internetforum und Zeitraum[120] - bestimmten Nachricht samt dem Zeitpunkt ihrer

---

[118] Unter diese Ausnahmebestimmung fallen auch Auskünfte zur IMEI (Gerätekennung) und IMSI (Kennung der SIM-Karte) im Bereich des Mobilfunks.

[119] SPG Novelle 2007, BGBl Nr. 114/2007. Zur Novelle ausführlich und kritisch *Tretter,* Österreich: Aktuelle datenschutzrechtliche Herausforderungen, in: Zukunft. Die Diskussionszeitschrift für Politik, Gesellschaft und Kultur, 01/2010, 18 ff; detailliert mit Bezug auf eine Sammelanfechtung der novellierten Bestimmungen vor dem VfGH: *ders.,* Grundrechtliche Probleme der Verwendung personenbezogener Daten durch die Sicherheitsbehörden, in: Österreichische Juristenkommission (Hg.), Alles unter Kontrolle? Überwachung - Privatsphäre - Datenschutz [= Kritik und Fortschritt im Rechtsstaat, Band 34], Wien - Graz 2009, 55ff; sämtliche Individualanträge im Namen von 27 AntragstellerInnen aus unterschiedlichen Berufsgruppen, auf die sich *Tretter* in beiden Aufsätzen bezieht, wurden vom Verfassungsgerichtshof zu G 147, 148/08 als unzulässig zurückgewiesen. Im Wesentlichen begründete der VfGH seine Entscheidung damit, dass die unmittelbare und gegenwärtige rechtliche Betroffenheit der AntragstellerInnen nicht ausreichend dargelegt wurde. Am 15.1.2010 haben die BeschwerdeführerInnen dieses Verfahrens Individualbeschwerde gemäß Art. 34 EMRK beim Europäischen Gerichtshof für Menschenrechte (EGMR) erhoben.

[120] Erlass des BM.I zu § 53 Abs 3b und 3b SPG, GZ 94762_101-GD_08.

Übermittlung (§ 53 Abs 3a Z 2 SPG), oder Name und Anschrift des Teilnehmers zu einer bereits bekannten IP-Adresse (§ 53 Abs 3a Z 3 SPG).

In diesen Fällen ist keine gerichtliche oder sonstige Genehmigung[121] notwendig. Der Anbieter erhält von einer der insgesamt 12 berechtigten Dienststellen[122] eine schriftliche Anfrage und muss die angeforderten Daten ohne weiteres ausfolgen. Für den präventiven Bereich gibt es auch nach der Novellierung der §§ 53 (3a) und (3b) SPG anlässlich der Vorratsdatenspeicherung keine Einschränkungen auf bestimmte Delikte oder den Schutz bestimmter besonders hochwertiger Rechtsgüter. Zwar findet sich prima facie eine solche Einschränkung in § 53 (3a) Z 2 und 3 SPG, wonach die Datenauskunft „eine wesentliche Voraussetzung zur Abwehr einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht“ (EAH, vgl. § 19 SPG) sein muss. Allerdings gilt diese Rechtsgütereinschränkung nur für die Aufgabe der EAH, denn zur „Abwehr allgemeiner Gefahren (§ 16 SPG)“ steht die Befugnis ohne Einschränkung zu.

Korrespondierend zu diesen Befugnissen wurden in § 99 (5) Z 3 und 4 TKG die Ausnahmen normiert, nach denen abweichend von § 102b TKG Verkehrsdatenauskünfte nach dem SPG auch im Hinblick auf Vorratsdaten zulässig sind, die nicht älter als 3 Monate sind. Betroffen sind dieselben Datenarten wie bei der eben beschriebenen Ausnahmekonstruktion des § 76a (2) StPO iVm § 99(5) Z 2 TKG, also insbesondere IP-Adressen und E-Mail Verkehrsdaten. Für den Bereich des SPG wurden diese Ausnahmen im rechtspolitischen Entstehungsprozess ausdrücklich diskutiert und in dieser Form übernommen, weil das SPG selbst in § 53 Abs. 3a schon die Auskunftsbefugnis darauf einschränkt, dass immer ein Bezug zu einer bestimmten Nachricht zu einem möglichst genauen Zeitraum notwendig ist. Damit erfährt die Tragweite der Ausnahme auf SPG Seite eine entscheidende und notwendige Einschränkung, die im Vergleich dazu der StPO fehlt. Begehrt wird entweder die IP-Adresse zu einer - anhand relevanter Kriterien, etwa Pseudonym, Internetforum und Zeitraum[123] - bestimmten Nachricht samt dem Zeitpunkt ihrer Übermittlung (§ 53 Abs 3a Z 2 SPG), oder Name und Anschrift des Teilnehmers zu einer bereits bekannten IP-Adresse (§ 53 Abs 3a Z 3 SPG).

II.1.4.4.4 IP-Adressen und Urheberrecht

In der rechtspolitischen Debatte zur Umsetzung der Vorratsdatenspeicherung wurde wiederholt gefordert, dass Auskünfte über Name und Anschrift zu einer IP-Adresse auch in Bezug auf den Schutz von geistigem Eigentum (Urheberrecht) im Rahmen eines Zivilverfahrens zulässig sein sollten. Diese

---

[121] Weder durch den Rechtsschutzbeauftragten des Bundesministeriums für Inneres (BM.I) noch durch die Datenschutzkommission, die für solche Genehmigungen abstrakt in Frage kämen.

[122] Die Bestimmung kennt selbst keine Einschränkungen, sondern sieht ein Auskunftsrecht sämtlicher Sicherheitsbehörden vor. Die Wirtschaftskammer Österreich (WKO) konnte in Verhandlungen mit dem BM.I jedoch erreichen, dass per Erlass des BM.I zu § 53 Abs 3a und 3b SPG, GZ 94762_101-GD_08 (abrufbar auf der Web-Seite der WKO unter http://portal.wko.at/wk/format_detail.wk?AngID=1&StID=386310&DstID=5000 (10.10.2011) ein einheitlicher Vollzug geregelt wird. Demnach sind folgende Dienststellen auskunftsberechtigt: Die 9 Landeskriminalämter (LKA), das Bundeskriminalamt, das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) und das Büro für interne Angelegenheiten (BIA → mit BGBl. I Nr. 72/2009 nunmehr umgewandelt in das „Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung“ - BAK).

[123] Der Zeitraum muss dabei gemäß einem Erlass des BM.I zu § 53 Abs 3b und 3b SPG, GZ 94762_101-GD_08, auf eine Stunde eingeschränkt werden.

Forderung wurde in der Folge jedoch nicht erfüllt. Weil das TKG nunmehr wie beschrieben eine abschließende Aufzählung der zulässigen Auskunftsfälle enthält, in der jedoch der Auskunftsanspruch des § 87b UrHRG nicht enthalten ist, geht dieser auf zivilrechtlicher Ebene weiterhin ins Leere.[124]

Von Seiten des BMVIT wurde dabei argumentiert, dass es bei der Vorratsdatenspeicherung um die Bekämpfung „schwerer Straftaten" gehe, und nicht um die Sicherung zivilrechtlicher Ansprüche. Die IP-Adressen Auskünfte sollen zur Verfolgung von Urheberrechtsverletzungen dann zulässig sein, wenn das zivilrechtliche Interesse auch strafrechtlich geschützt ist. Die Interessen der Urheber können daher auch über das Strafverfahren geschützt werden, die Strafnorm in §91 UrHRG gehört schon lange zum Rechtsbestand. Hier besteht allerdings eine ganz andere Hürde, die mit dem TKG nichts zu tun hat. Seit die StPO Reform am 1.1.2008 in Kraft getreten ist, findet nämlich bei sogenannten Privatanklagedelikten – zu denen auch § 91 UrHRG gehört – kein Ermittlungsverfahren mehr statt (§ 71 (1) StPO). Aus diesem Grund greift hierzu auch die neue Bestimmung des § 76a (2) StPO nicht, obwohl davon ansonsten alle gerichtlich strafbaren Handlungen erfasst sind. Bereits im Sommer 2009 wurde eine Ministerialvorlage des BMJ zur Einführung eines eingeschränkten Ermittlungsverfahrens bei Privatanklagedelikten in öffentliche Begutachtung versendet, um mögliche Rechtsschutzlücken, nicht nur in Bezug auf das Urheberrecht, zu schließen. So man dies tatsächlich als „Lücke" sehen will, könnte diese jedenfalls durch entsprechende Änderungen in der StPO geschlossen werden, das TKG steht dem nicht entgegen.

II.1.5 Beurteilung der österreichischen Rechtslage nach der Umsetzung der Vorratsdatenspeicherung

Dass die von der Vorratsdatenspeicherung betroffenen Daten im Schutzbereich des Art 8 EMRK liegen wurde bereits oben in Kapitel II.1.1.3.2 dargestellt, ebenso die materiellen Rahmenbedingungen. Nachfolgend soll die neue Rechtslage nach Umsetzung der Vorratsdatenspeicherung in Österreich einer Bewertung am Maßstab der Rechtssprechung des EGMR zu Art 8 EMRK unterzogen werden.

Die Überwachung der Tele- und Internetkommunikation und die Weiterverarbeitung der hierdurch ermittelten Daten auf Grundlage der §§ 53 Abs 3a und 3b SPG ermöglichen schwerwiegende Eingriffe in das Recht auf Geheimhaltung personenbezogener Daten, in das Recht auf Achtung der Privatsphäre und die Kommunikationsfreiheit. Nach § 53 Abs 3a und 3b SPG können Stammdaten, Verkehrsdaten und Standortdaten Gegenstand der Datenerhebung sein. Die Erhebung der Verbindungsdaten der Telekommunikation (§ 53 Abs 3a SPG) und der Standortkennung (§ 53 Abs 3b SPG) betreffen zunächst zwar nur die technische Abwicklung des Telekommunikationsvorgangs. Das Ermittlungsergebnis betrifft aber stets personenbezogene Daten. Verbindungsdaten lassen außerdem Rückschlüsse auf das Kommunikationsverhalten, das soziale Umfeld und unter Umständen auch auf persönliche Angelegenheiten und Gewohnheiten zu.[125] Die Standortkennung eingeschalteter Mobilfunkendeinrichtungen kann zur Erstellung eines Bewegungsbildes verwendet werden, über das gegebenenfalls auf Gewohnheiten der betroffenen Personen oder auf Abweichungen hiervon geschlossen werden kann.

---

[124] Diese Situation besteht seit der Entscheidung des OGH zu GZ 4 Ob 41/09x (Rechtssache LSG gg Tele 2).
[125] So auch das deutsche Bundesverfassungsgericht in BVerfG 107, 299 (318 ff).

II.1.5.1 Bestimmtheit der gesetzlich vorgesehenen Grundrechtseingriffe

Wesentliche Bestimmungen des SPG zur Ermittlung von Kommunikationsdaten erfüllen die unter Kapitel II.1.2 dargestellten Bestimmtheitsanforderungen nach der Rechtssprechung des EGMR nicht. Die Befugnis zur Einholung von Auskünften über IP-Adressen und Teilnehmernummern nach § 53 Abs 3a SPG etwa kennt keine Einschränkung auf bestimmte Straftaten. „Wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen", muss der Polizei die Identität des Teilnehmers bekannt gegeben werden, und zwar ohne materielle Einschränkung für alle Aufgaben der Sicherheitspolizei. Das SPG und auch die Gesetzesmaterialien enthalten keine Hinweise, was unter einer „konkreten Gefahrensituation" zu verstehen ist und auch nicht, für welche Rechtsgüter eine solche konkrete Gefahr vorliegen muss. Die Norm kennt auch keine Einschränkung, dass solche Daten nur über verdächtige Personen erhoben werden dürfen. Außerdem trifft § 53 Abs 3a SPG keine Aussagen zur Form der Anfragen, ein allenfalls einzuhaltendes Verfahren oder zu Löschungsverpflichtungen. Normiert ist bloß, dass die ersuchte Stelle verpflichtet ist, die Auskunft „unverzüglich und kostenlos" zu erteilten.

Ähnliches gilt für die neue Bestimmung des § 76a Abs. 2 StPO, nach welcher zur Aufklärung jeder mit gerichtlicher Strafe bedrohten Handlung Name und Anschrift zu einer bestimmten IP-Adresse ausgeforscht werden dürfen, also ohne Einschränkung auf bestimmte Delikte oder einen gewissen Mindeststrafrahmen. Für Auskünfte über IP-Adressen ist auch nicht vorgesehen, dass eine Anordnung der Staatsanwaltschaft einer gerichtlichen Bewilligung bedarf, wie dies für sonstige „Auskünfte über Daten einer Nachrichtenübermittlung" gemäß § 134 ff. StPO vorgesehen ist.

Etwas differenzierter ist die Befugnis zur Ermittlung von Standortdaten gemäß § 53 Abs 3b SPG zu sehen. Diese besteht nur zur Lokalisierung der von dem gefährdeten Menschen mitgeführten Endeinrichtung. Das bedeutet, dass aufgrund dieser Befugnis keine Tatverdächtigen lokalisiert werden dürfen, sondern nur z.B. vermisste Personen (Lawinenopfer, Tourengeher, aber auch Entführungsopfer). Eine Lokalisierung eines Tatverdächtigen muss nach den Regeln der Strafprozessordnung (StPO) aufgrund einer gerichtlichen Bewilligung erfolgen. Allerdings besteht - abgesehen von der stichprobenartigen Kontrolle durch den Rechtsschutzbeauftragten des BM.I - kaum verfahrensmäßige Sicherungen vorhanden sind, um zu gewährleisten, dass diese Beschränkung auch tatsächlich beachtet wird.

II.1.5.2 Informationspflichten der Strafverfolgungs- und Sicherheitsbehörden

Für die Regeln zur Information Betroffener bestehen unterschiedliche Regime im Strafprozess und im Sicherheitspolizeirecht. Erfolgt eine Datenermittlung im Auftrag des Gerichts bzw. der Staatsanwaltschaft nach der StPO, müssen Betroffene von der Durchführung der Ermittlungsmaßnahme durch die Staatsanwaltschaft verständigt und über ihre Rechte informiert werden (§ 138 f StPO), hierauf können sie bei Gericht die Vernichtung der Ergebnisse beantragen, wenn diese für ein Strafverfahren nicht von Bedeutung sein können oder als Beweismittel nicht verwendet werden dürfen. Diese Rechte beziehen sich nicht nur auf den Beschuldigten des Strafverfahrens sondern auf alle von den Ermittlungsmaßnahmen Betroffenen. Wenn also tatsächlich ein gerichtliches Strafverfahren - wenn auch nur ein Ermittlungsverfahren ohne Hauptverhandlung - geführt würde, würden die Betroffenen davon erfahren und könnten sich auch rechtlich zur Wehr

setzen. Falls die Daten durch die Polizei ermittelt würden, die Ermittlungen aber nicht zu einem gerichtlichen Strafverfahren (Ermittlungsverfahren nach der StPO) führen, ist gesetzlich nicht vorgesehen, dass die Betroffenen davon erfahren. Und selbst wenn Daten aus einem Gerichtsakt schließlich gelöscht werden, ist das Schicksal derselben Daten, die sich auch noch im Polizeiakt befinden, rechtlich unklar.

Im präventiven Bereich nach SPG besteht nach der neuen Rechtslage eine Differenzierung: Eine Informationspflicht der Behörden besteht nur dann, wenn für die Auskunft Vorratsdaten verwendet wurden. Diese Differenzierung ist sachlich nicht nachvollziehbar und führt im Ergebnis dazu, dass im präventiven Bereich - wo regelmäßig eher aktuelle Daten ermittelt werden - kaum eine Information durch die Sicherheitsbehörden stattfinden müssen wird. Den auskunftspflichtigen Anbietern kommt ebenfalls keine Berechtigung zu, betroffene Personen über die Lokalisierung zu informieren, weil dies den Zweck der Datenanwendung gefährden könnte. Für Datenübermittlungen gemäß § 53 Abs 3a und 3b SPG kommen pauschale Ausnahmebestimmungen von der Informationspflicht zum Tragen (§ 24 Abs 3 Z 1, Abs 4 DSG 2000). Diese Rechtsansicht- und Praxis[126] ist in der Beantwortung einer parlamentarischen Anfrage an den Innenminister vom 27. März 2008 dokumentiert.[127]

Eine Information der betroffenen Personen sollte erfolgen, sobald eine solche ohne Gefährdung des Überwachungszweckes nach ihrer Beendigung stattfinden kann.[128] Ansonsten sind Betroffene niemals in der Lage herausfinden, ob sie überhaupt überwacht wurden. Damit ist auch eine Feststellung der Rechts- bzw Konventionswidrigkeit einer allfälligen Überwachungsmaßnahme oder eine Entschädigung für einen rechtswidrigen Eingriff in ihre Rechte nach Art 8 EMRK unmöglich. Auch insoweit sind die vom EGMR gestellten Anforderungen an den Rechtsschutz im Fall geheimer Überwachungsmaßnahmen und Datenverwendungen in der österreichischen Rechtsordnung nicht erfüllt bzw. unzulänglich umgesetzt.

II.1.5.3 RECHTSSCHUTZINSTRUMENTE

In Österreich bestehen bezüglich der sicherheitsbehördlichen Befugnisse zur Datenerhebung keine wirksamen Kontroll- und Rechtsschutzinstrumente im Sinne des Rechts auf eine wirksame Beschwerdemöglichkeit gemäß Art 13 EMRK, die der Gefahr des Missbrauchs dieser Befugnisse wirksam entgegenstehen. Das Datenschutzgesetz 2000 (DSG) sieht dermaßen umfassende Ausnahmen von der (grundsätzlich bestehenden) Informationspflicht vor, dass im Anwendungsbereich der beschriebenen Bestimmungen kaum Spielraum bleibt, Betroffene in Kenntnis zu setzen. Auch der Rechtsschutzbeauftragte (RSB) beim Bundesministerium für Inneres (BM.I), der kommissarisch die Rechte der Betroffenen wahrnehmen soll, bietet keinen ausreichend effektiven Rechtsschutz. Dieser gehört organisatorisch jener ministeriellen Behörde an, die für die Überwachungsmaßnahmen in letzter Instanz verantwortlich ist – dem BM.I. Er ist zwar sachlich weisungsfrei gestellt, aber schon allein wegen seiner organisatorischen Eingliederung in das Innenministerium nicht unabhängig. Weiters wird er von der Exekutive bestellt, nämlich vom

[126] Die vom Wortlaut der Normen durchaus gedeckt ist.
[127] Beantwortung der parlamentarischen Anfrage 3430/AB vom 27. März 2008 zu 3407/J, XXIII. GP.-NR.
[128] EGMR 28.06.2007 Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien RN 90 unter Verweis auf die Urteile EGMR 06.09.1978 Klass u.a. gg. Deutschland, RN 58; EGMR 26.03.1987 Leander gg. Schweden, RN 66; sowie EGMR 29.06.2006 Weber und Saravia gg. Deutschland, RN 135.

Bundespräsidenten auf Vorschlag der Bundesregierung (§ 91a Abs 2 SPG), die Präsidenten des Nationalrats sowie der Höchstgerichte haben im Zuge der Bestellung lediglich Anhörungsrechte. Die persönlichen Qualifikationsvoraussetzungen entsprechen auch nicht jenen eines unabhängigen Richters (vgl. § 91b Abs 1 SPG). Der RSB entspricht daher nicht den vom EGMR geforderten Kriterien einer unabhängigen Kontrollinstanz. Abgesehen davon verfügt der Rechtsschutzbeauftragte auch nicht über eine personelle Ausstattung, die ihm eine effektive bundesweite Kontrolltätigkeit ermöglichen würde.

Die Regeln der StPO sind in Bezug auf die Rechtsschutzinstrumente weniger unzulänglich als jene des SPG. Allerdings bestehen auch hier Defizite. Zu nennen ist die neue Regelung des § 76a Abs. 2 StPO, der wie dargestellt Auskünfte über IP-Adressen ohne richterliche Kontrolle zulässt. Nachträgliche Beschwerdemöglichkeiten bestehen wohl nach den §§ 139 f StPO, diese sind allerdings davon abhängig, dass die Staatsanwaltschaft ihrer Informationspflicht gemäß § 139 StPO auch tatsächlich nachkommt. Kontrollinstrumente, um die Einhaltung dieser Verpflichtung sicherzustellen - nämlich wenn ansonsten am Verfahren nicht beteiligte Dritte von den Überwachungsmaßnahmen betroffen waren - bestehen aber auch hier nicht.

II.1.5.4 Verhältnismäßigkeit der gesetzlich vorgesehenen Grundrechtseingriffe

Die pauschale Ermächtigung zur vorsorglichen Überwachung der Telekommunikation für Zwecke der Verhütung von nicht näher genannten Straftaten genügt den Anforderungen der Verhältnismäßigkeit im engeren Sinne nicht. Angesichts der Rechtsprechung des EGMR erweist sich die österreichische Rechtslage auch aus diesem Blickwinkel als konventionsrechtlich bedenklich. Grundrechtlich bedeutsam ist ferner die große Streubreite der möglichen Eingriffe. Erfasst werden nicht nur potenzielle Straftäter, sondern auch sämtliche Personen, mit denen diese im betreffenden Zeitraum Telekommunikationsverbindungen nutzen. Dazu können etwa auch Personen gehören, die in keiner Beziehung zu einer möglicherweise zu verhütenden oder später zu verfolgenden Straftat stehen, wie etwa Kontakt- und Begleitpersonen oder gänzlich unbeteiligte Dritte. Dass die Betroffenen den Überwachungsmaßnahmen in einer Situation vermeintlicher Vertraulichkeit ausgesetzt werden verleiht dem Eingriff zusätzliches Gewicht.[129] Die Freiheit der Menschen wird damit auch mittelbar beeinträchtigt, weil umfangreicher und unvorhersehbarer Einsatz von Überwachungsmethoden dazu führt, dass Telekommunikation subjektiv nicht mehr unbefangen stattfindet. Auch die Pressefreiheit ist von derartigen Maßnahmen betroffen, da das Vertrauen von Informanten in die Integrität von Kommunikationswegen massiv beeinträchtigt sein kann und damit die Arbeit der Presse als „public watchdog“, die auf solche Informanten angewiesen ist, behindert wird.

Gegen die angesprochenen Maßnahmen können Betroffene frühestens dann mit rechtlichen Mitteln vorgehen, wenn die Maßnahmen bereits vollzogen sind und sie über die Tatsache, dass solche Maßnahmen getroffen wurden, informiert wurden oder davon auf andere Weise Kenntnis erlangen konnten.[130] Bei Maßnahmen der Vorfeldermittlung ist aufgrund der Ungewissheit, ob und wann Straftaten begangen werden, regelmäßig mit einer längeren Zeitdauer bis zu einer (allfälligen)

[129] So auch das deutsche Bundesverfassungsgericht in BVerfG 34, 238 (247); 107, 299 (321).
[130] Vgl VfSlg 17.102/2004; und BVerfG 107, 299 (321).

Unterrichtung zu rechnen als bei sonstigen Überwachungsmaßnahmen.[131] Selbst durch eine erst spät erfolgende Mitteilung wird auch die in Art 13 EMRK enthaltene Garantie effektiven Rechtsschutzes berührt. Die Schwere der Grundrechtsbeeinträchtigung ist zusätzlich erhöht, wenn gegen einen Eingriff nicht in angemessener Zeit Rechtsschutz begehrt und dessen Folgen dadurch gegebenenfalls beseitigt werden können. Die Eingriffsschwere wird durch die Möglichkeit der Behörden, die erhobenen Daten – wie in § 53 Abs. 2 SPG vorgesehen – allgemein zu Zwecken der Gefahrenabwehr und zu weiteren Zwecken nach Abs 1 leg cit zu speichern, zu verändern oder zu nutzen, noch weiter verstärkt. Die Verwertung in anderen Zusammenhängen ist ein eigenständiger Eingriff.[132] Die Datenerhebung im Vorfeld der Begehung von Straftaten kann aufgrund der fehlenden Begrenzung auf eine konkret in Verwirklichung begriffene oder schon begangene Straftat vielfältig nutzbare Informationen ergeben. Die Bindung an den Zweck, den das zur Kenntnisnahme der Daten ermächtigende Gesetz festgelegt hat, wird bei der weiteren Verwertung der erlangten Informationen praktisch kaum haltbar sein. Die Möglichkeit der Verwendung der erhobenen Daten zu unbestimmten oder noch nicht bestimmbaren Zwecken erhöht damit die Schwere des Eingriffs schon in der Phase der Erhebung. Die vorgesehenen Eingriffe in das Grundrecht des § 1 DSG 2000 und des Art 8 EMRK sind daher im engeren Sinne nicht verhältnismäßig.

Aus all dem folgt, dass die genannten Bestimmungen des SPG und der StPO den vom EGMR aufgestellten Determinierungsanforderungen nicht gerecht werden. Vor solch einem Hintergrund befand der Gerichtshof im Urteil Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien, dass Eingriffe in die Rechte von Beschwerdeführern ohne ausreichende Sicherheitsvorkehrungen gegen das jedem Überwachungssystem immanente Missbrauchsrisiko im Sinne des Art 8 EMRK nicht „gesetzlich vorgesehen" im Sinne des Absatz 2 dieses Konventionsrechtes sind und schon aus diesem Grund eine Verletzung des Art 8 EMRK bewirken. Diese Feststellung schließe – so der EGMR – sogar die Notwendigkeit einer Prüfung aus, ob die Maßnahme „in einer demokratischen Gesellschaft notwendig" zur Erreichung eines der darin aufgezählten Ziele war.[133]

II.1.5.5 Umsetzung der Vorratsdatenspeicherung und Auswirkungen auf das Kommunikations- und Fernmeldegeheimnis

Die RL 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsdatenspeicherung verpflichtet die Mitgliedstaaten zu einer umfassenden Speicherung von Verkehrs- und Standortdaten, die im Bereich der Telekommunikation und im Internet anfallen.[134] Die Speicherungspflicht wird durch Umsetzung den privaten Telekommunikationsunternehmen und Internet-Providern übertragen, die diese Daten für staatliche Zwecke „der Ermittlung, Feststellung und Verfolgung von schweren Straftaten"[135] aufzubewahren haben und die „nur in bestimmten

[131] BVerfG 107, 299 (322).
[132] So auch das deutsche Bundesverfassungsgericht in BVerfG 110, 33 (68 f).
[133] EGMR 28.06.2007 Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien, RN 93, unter Verweis auf die Urteile EGMR 02.08.1984 Malone gg. Vereingtes Königreich, RN 82;EGMR 24.04.1990 Kruslin gg. Frankreich, RN 37; EGMR 24.04.1990 Huvig gg. Frankreich, RN 36; und EGMR 12.05.2000 Khan gg. Vereingtes Königreich, RN 28.
[134] Vgl. Art 5 der RL 2006/24/EG.
[135] Art 1 RL 2006/24/EG.

Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden“[136] sollen.

Dabei bewirkt bereits die Speicherung der Verkehrsdaten ein Eingriff in das Grundrecht auf Wahrung des Fernmeldegeheimnisses sowie auf Achtung des Privatlebens und der Korrespondenz. Die privaten Unternehmen handeln dabei ausschließlich für staatliche Zwecke, wenn sie zur Speicherung von Verkehrsdaten verpflichtet werden, um diese dann bei Bedarf an die zuständigen Behörden weiterzuleiten. Bisherige Speicherungen von Verkehrsdaten dürfen nur zu Verrechnungszwecken erfolgen und sind auf das „unbedingt notwendige Minimum zu beschränken“[137]. Die zu speichernden Datenkategorien in Art 5 und der geforderte Zeitrahmen gemäß Art 6 der RL gehen weit über die bisherigen vertraglich notwendigen Erfüllungsverpflichtungen der Provider und Telekommunikationsanbieter hinaus. Durch diese Auslagerung der staatlichen Speicherungspflicht auf Private darf keine Umgehung von grundrechtlichen Schutzstandards erfolgen. Die Speicherung der Verkehrs- und Standortdaten ist aus diesem Grund den staatlichen Behörden zuzurechnen, welche die Grundrechte zu wahren haben.

Durch die Umsetzung der Richtlinie zur Vorratsdatenspeicherung bestehen erweiterte Speicherpflichten für Anbieter, die als Eingriff in das Kommunikationsgeheimnis nach § 93 TKG 2000 zu qualifizieren sind. Diese sind aber im Gegensatz zu den bisherigen Speicher- und Verwendungsbefugnissen jedenfalls nicht für die Besorgung eines Kommunikationsdienstes oder Notrufdienstes erforderlich. Die Speicherung der Verkehrsdaten und Standortdaten auf Vorrat durchbricht also das bisherige System der strengen Zweckbindung und der Datensparsamkeit bezüglich der Erfüllung des Kommunikationsdienstes. Sie setzt einen neuen Zweck[138], geht weit über ihre Notwendigkeit hinaus und ist umfassend. Eine Rechtfertigung des Eingriffes mit den bisherigen Ausnahme- und Rechtfertigungsbestimmungen nach § 93 Abs 3 Satz 2 TKG und den datenschutzrechtlichen Verwendungsbefugnissen nach §§ 96 ff TKG ist nicht möglich. Vorratsdatenspeicherung setzt im TKG neue Maßstäbe, denen mit schärferen Schutzpflichten der Anbieter begegnet werden muss. Diesen kommt aufgrund des enorm zu steigernden Datenumfanges eine größere Verantwortung zu als bisher, die sie mit „angemessenen Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen“[139] wahrzunehmen haben.

In diesem Licht ist etwa die neue Bestimmung des § 102c Abs 2 TKG zu sehen, der die Anbieter verpflichtet, die Daten durch geeignete technische und organisatorische Maßnahmen vor „unrechtmäßiger Zerstörung, zufälligem Verlust oder unrechtmäßiger Speicherung, Verarbeitung und Zugänglichmachung“ zu schützen. Weiters ist es wichtig, dass die Daten nur einem geschlossenen, möglichst kleinen Personenkreis zugänglich sind, die dazu speziell ermächtigt wurden.[140] Mögen diese Regelungen auch begrüßenswert sein, so greifen sie für eine umfassende Gewährleistung eines hinreichenden Sorgfaltsmaßstabes doch zu kurz. Daher ist umso wichtiger, dass eine Verordnung zur näheren Bestimmung der Datensicherheitsmaßnahmen gemäß §§ 94 Abs. 4 und 102c TKG diesen Anforderungen gerecht wird und einen größtmöglichen Schutzstandard festlegt.

---

[136] Art 4 RL 2006/24/EG.
[137] § 99 Abs 2 TKG.
[138] Nämlich „die Ermittlung, Feststellung und Verfolgung von schweren Straftaten“.
[139] Art 1 § 1 Abs 2 DSG
[140] § 102c Abs 2, 3.Satz TKG.

II.2 Datensicherheit beim Anbieter (Speicherung und Zugang intern)

II.2.1 Das „Vorratsdaten-Urteil“ des deutschen Bundesverfassungsgerichts

II.2.1.1 Grundrechtliche Situation in Deutschland

In Deutschland stellt sich die Grundrechtliche Situation wie folgt dar: Vorratsdaten unterfallen aus verfassungsrechtlicher Perspektive dem Fernmeldegeheimnis (Art. 10 GG). Während Art. 10 Abs. 1 GG nur von der Unverletzlichkeit des Fernmeldegeheimnisses ausgeht, jedoch dessen Inhalt und Weite nicht näher umschreibt, findet ist einfachgesetzlich normiert in § 88 Abs. 1 dTKG eine Definition, die verschiedene, von der Rechtsprechung entwickelte, Aspekte des Fernmeldegeheimnisses umschreibt.[141] Demnach unterfallen dem Fernmeldegeheimnis zum einen der Inhalt der Telekommunikation und dessen nähere Umstände. Damit ist also nicht nur der schlichte Inhalt umfasst, sondern auch, wer an der Kommunikation zu welchem Zeitpunkt beteiligt war. Ebenfalls dem Fernmeldegeheimnis unterfallen erfolglose Verbindungsversuche. Damit sind Vorratsdaten, da sich aus Ihnen erschließen lässt, dass von einer bestimmten IP oder einer bestimmten Mobilfunknummer eine Verbindung zu einem bestimmten Zeitpunkt zum Internet oder Mobilfunknetz aufgebaut wurde, auch wenn die Inhalte der Kommunikation nicht gespeichert werden unproblematisch vom Fernmeldegeheimnis umfasst. Das Fernmeldegeheimnis erweist sich damit als absolut technologieneutral[142] und sein Schutz endet erst, wenn der Übertragungsvorgang abgeschlossen ist.[143] Damit soll letztendlich verhindert werden, dass die Kommunikation über Fernkommunikationsmittel unterlassen wird, weil die Beteiligten befürchten, dass der Staat aus diesem Kommunikationsvorgang Erkenntnisse gewinnt und sei es nur die Tatsache, dass überhaupt eine Kommunikation stattgefunden hat.[144]

Das Fernmeldegeheimnis steht in Deutschland auf bundesrechtlicher Ebene nicht unter einem Richtervorbehalt.[145] Dies bedeutet aber im Umkehrschluss nicht, dass ein Eingriff in Art 10 GG sich zur Gänze einer vorherigen richterlichen Anordnung entzieht. Rechtsdogmatisch wird hier im Rahmen der Verhältnismäßigkeit angesetzt. Je nach Schwere des Eingriffs kann, unter Abwägung aller anderen Rechtsgüter, eine präventive richterliche Kontrolle erforderlich sein.[146] Nach der Rechtsprechung des deutschen Bundesverfassungsgerichts (BVerfG) ist der Richter – bedingt durch

---

[141] Diese Norm wurde im Zuge der Privatisierung der Telekommunikationsdienste, da man sich gegenüber der staatlichen Bundespost direkt auf Art. 10 GG berufen konnte, dies aber gegenüber einem Privatunternehmen nicht direkt möglich ist. Nähere Einzelheiten hierzu vgl. Spindler/Schuster, Recht der elektronischen Medien, 2. Auflage 2011, § 88 TKG, Rn. 3. Weitere einfachgesetzliche Erwähnung findet sich in § 206 Abs 5 dStGB, der Eingriffe in das Fernmeldegeheimnis strafrechtliche sanktioniert.

[142] Eckhardt, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Auflage 2011, § 88 TKG, Rn. 4.

[143] Baldus, in: Epping/Hillgruber, Beck’scher Onlinekommentar GG, Stand: 1.07.2011 Edition: 11, Art 10, Rn. 10.

[144] Baldus, in: Epping/Hillgruber, Beck’scher Onlinekommentar GG, Stand: 1.07.2011 Edition: 11, Art 10, Rn. 8 f.

[145] Einen Richtervorbehalt zum Schutz des Fernmeldegeheimnisses sieht in Deutschland nur die Brandenburgische Verfassung vor, wo bei diese eine mindestens nachträgliche richterliche Kontrolle vorschreibt (vgl. Durner, in: Maunz/Düring, Grundgesetz, 62. Ergänzungslieferung 2011, Rn. 152 m.w.N.).

[146] Durner, in: Maunz/Düring, Grundgesetz, 62. Ergänzungslieferung 2011, Rn. 154.

seine persönliche und sachliche Unabhängigkeit – am besten geeignet, abzuwägen, ob eine konkrete Maßnahme im ihm vorliegenden Fall verhältnismäßig ist.[147]

II.2.1.2 Vergleichbarkeit mit der Grundrechtslage in Österreich

Trotz der systematischen Unterschiede zur österreichischen Rechtslage, ist die Problemlage in Deutschland doch dieselbe. Inwiefern Vorratsdaten dem Fernmeldegeheimnis nach Art. 10a StGG unterfallen ist in Österreich wie bereits dargestellt nicht abschließend geklärt. Während der OGH verneint, dass es sich bei IP-Adressen um Verkehrsdaten handelt, bejaht dies der Verwaltungsgerichtshof. Praktische Auswirkungen hätte dies, da nur Art 10a StGG einen Richtervorbehalt vorsieht. Jedoch sind die Vorgaben des BVerfG für Österreich in jedem Fall von Relevanz. Der Grundrechtsschutz im Kommunikationsverkehr ist nicht durch Art 10a StGG erschöpfend geregelt. Selbst wenn dieser im Hinblick auf Verkehrsdaten nicht für einschlägig gehalten wird, muss die Vorratsdatenspeicherung in ihrer Ausgestaltung trotz allem mit der EMRK in Einklang stehen. Dabei wird es eines ebenso hohen Schutzniveaus bedürfen, wie es das BVerfG bezüglich der Vorratsdatenspeicherung vorgegeben hat. Damit sind, unabhängig von der exakten Einordnung der Vorratsdaten in den Schutzbereich bestimmter Grundrechte, die Vorgaben des BVerfG auch in der nationalen Umsetzung zu berücksichtigen, um eine verhältnismäßige Ausgestaltung zu erreichen.

II.2.1.3 Allgemeine einleitende Aussagen aus dem Urteil

Das BVerfG erklärte in seinem Urteil zur Vorratsdatenspeicherung [148]zunächst die bis zum Erlass des geltenden Vorschriften §§ 113a, b dTKG vollständig und § 100g Abs.1 Satz 1 dStPO, insofern er sich auf § 113 a dTKG bezieht, für nichtig mit dem Ergebnis, dass die gespeicherten Daten sofort mit der Urteilsverkündung zu löschen waren. Die Ergebnisse der Anfragen, die Sicherheitsbehörden während der Geltung der einstweiligen Anordnungen gestellt hatten, dürfen von den Speicherverpflichteten nicht herausgegeben werden. Auch diese Daten waren umgehend zu löschen.

Indes ist hervorzuheben, dass das BVerfG eine Vorratsdatenspeicherung in Bezug auf ihren Umfang und ihren Zweck grundsätzlich für mit Art. 10 GG (Brief, Post- und Fernmeldegeheimnis) vereinbar hält, sofern gewisse verfassungsrechtliche Rahmenbedingungen eingehalten werden.[149] Dabei ist insbesondere sicherzustellen, dass keine Speicherung zu unbestimmten oder nicht bestimmbaren Zwecken erfolgt. Hierbei ist dem Gewicht der weitreichenden Datenerfassung Rechnung zu tragen. Der Gesetzgeber ist also herausgefordert, eine normenklare Begrenzung der Datenerhebung und -verwendung auf den unbedingt erforderlichen Teil zu kodifizieren.[150] Bemängelt wurde bei § 113 a

---

[147] BVerfGE 107,299 (325).
[148] BVerfG 1 BvR 256/08, Urteil vom 2.3.2010.
[149]Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 398; Das BVerfG grenzt insbesondere die Konstellation vom Volkszählungsurteil ab (BVerfGE 65, 1, 46). Verboten ist also nur eine Speicherung personenbezogener Daten aus Vorrat zu unbestimmten oder nicht bestimmbaren Zwecken (vgl. Rn. 206).
[150] BVerfG 1 BvR 256/08, Rn. 206, 214; dazu kritisch Möstl, Das Bundesverfassungsgericht und das Polizeirecht – Zwischenbilanz aus Anlass des Urteils der Vorratsdatenspeicherung, DVBl. 2010, S. 808, 813, der die

dTKG vor allem, dass diesem kein Ausnahmecharakter mehr zukommt und der Gesetzgeber damit nicht zuletzt auch über die europarechtlichen Vorgaben hinausgeschossen ist.[151]

Das BVerfG hebt dabei eingehend die Gefahren hervor, die in der Vorratsdatenspeicherung zu sehen sind; aus seiner Sicht handelt es sich bei der Vorratsdatenspeicherung um einen besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher unbekannt ist. Dies, so das Gericht, sei darauf zurückzuführen, dass sich aus den gespeicherten Daten lassen, auch ohne die Speicherung von Inhaltsdaten, bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen lassen.[152] Ebenfalls ist es durch eine solche anlasslose Speicherung möglich, nach Nutzung der Telekommunikation, aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers zu erstellen.[153] Im Übrigen wird der Begriff des Eingriffs im Rahmen der Entscheidung völlig anders als bisher interpretiert. War bislang ein Eingriff durch den Staat unmittelbar erforderlich, so genügt nunmehr die Speicherung der Vorratsdaten durch das Telekommunikationsunternehmen und zwar unabhängig davon, ob staatliche Stellen auf die Daten Zugriff erhalten oder nicht.[154] Anders gesprochen wird Art. 10 GG vom BVerfG somit dahingehend interpretiert, dass ein verfassungsmäßiges Recht auf Anonymität im Internet besteht, so dass ein Eingriff in diese Anonymität einer Rechtfertigung bedarf.[155]

Dabei sind nach dem BVerfG zwei Gebiete zu unterscheiden: Speicherung und Zugriff. Diese und deren Sicherungsmechanismen stellen zwei Bereiche dar, die nur in ihrer Gesamtheit die Verhältnismäßigkeit der Vorratsdatenspeicherung sicherstellen können. Bezüglich der Anordnung der Speicherung, darf diese nur bei genügender Sicherheit erfolgen, der Abruf darf wiederum nur erfolgen, wenn er ebenfalls abgesichert ist. Zugriffe müssen hierbei gesichert werden und transparent erfolgen; erst dann ist die Speicherung als verhältnismäßig anzusehen, da nur auf diese Weise vermieden werden kann, dass beim Bürger ein Gefühl der permanenten Überwachung sämtlicher Lebensbereiche entsteht.[156] Zugleich unterstreicht das BVerfG im Gegenzug aber auch das Interesse staatlicher Stellen an Kommunikationsverbindungen im Internet zur Wahrung der Rechtsordnung, um das entstehen rechtsfreier Räume zu unterbinden.[157]

Zusammenfassend lässt sich festhalten: Das BVerfG hält die Speicherung der TK-Daten aller Benutzer deutscher TK-Infrastrukturen für mit dem Grundgesetz vereinbar.[158] An die Art und Weise der Speicherung werden aber strenge Anforderungen gestellt.[159]

Anforderungen an die Normenklarheit, vor allem aus Perspektive der Polizei, als am Rande des handhabbaren ansieht.

[151] Ibid, Rn. 279.

[152] Albers/Reinhardt, Entscheidungsbesprechung – Vorratsdatenspeicherung im Mehrebenensystem: Die Entscheidung des BVerfG vom 2.3.2010, ZJS 2010, S. 767, 770.

[153] Schmidt, Auswirkungen des Urteils zur Vorratsdatenspeicherung auf die Praxis, in: AnwZert ITR 5/2010, Anm. 2 (Publikation enthält keine Seitenzahlen).

[154] Wolff, Vorratsdatenspeicherung – Der Gesetzgeber gefangen zwischen Europarecht und Verfassung?, NVwZ 2010, S. 751, 752; BVerfG 1 BvR 256/08, Rn. 193.

[155] Ibid, S. 753.

[156] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 398.

[157] BVerfG 1 BvR 256/08, Rn. 260.

[158] Ibid, Rn. 205.

[159] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 398.

Hervorgehoben werden hierbei vom Gericht insbesondere die Punkte Zugriff des Staates auf Daten, Anforderung an die Datensicherheit und Verfahrensregelungen. Zulässig soll ein Zugriff auf die Daten nach dem Willen des Gerichts weiterhin zur Aufklärung schwerer Straftaten und auch Ordnungswidrigkeiten sein. Dazu ist der Gesetzgeber verpflichtet einen abschließenden Katalog aufstellen.[160] Dabei wiederum ist er nicht an eine Begrenzung auf Straftaten gegen Leben, Körper und Freiheit gebunden.[161]

Ebenfalls steht es dem Gesetzgeber frei, auf bereits bestehende Kataloge zurückzugreifen oder einen neuen Katalog, der zum Beispiel Straftatbestände enthalten kann, die typischerweise im Zusammenhang mit Telekommunikation stehen, zu schaffen; entscheidend ist aber, dass im Rahmen der Strafnorm eine gewisse schwere der Tat zum Ausdruck kommt, welche sich an objektiven Kriterien, wie etwa am Strafrahmen, festmachen lässt.[162] Im Rahmen von Ordnungswidrigkeiten müssen diese jedoch besonders schwer wiegen, da die Aufhebung der Anonymität im Internet einen besonders schweren Eingriff darstellt.[163]

Dies bedeutet aber im Rahmen der Strafverfolgung im Gegenzug auch, dass es eines, zumindest durch bestimmte Tatsachen begründeten Verdachts bedarf, bevor ein Zugriff auf die Daten erfolgt, ebenso wie es im Rahmen der Gefahrenabwehr notwendig ist, dass eine Gefahr für Leib und Leben, für den Bestand des Bundes oder eines Landes oder die Abwehr einer gemeinen Gefahr vorliegt.[164] Hierbei zieht das BVerfG die im Rahmen der Entscheidung zur sog. Onlinedurchsuchung entwickelten Grundsätze heran[165] und macht den Zugriff im präventiven Bereich von einer konkreten Gefahr abhängig, die sich durch den jeweiligen Einzelfall, die zeitliche Nähe des Umschlagens einer Gefahr in einen Schaden und den Bezug auf individuelle Personen als Verursacher auszeichnet[166] und verlangt damit einen „konkreten personenbezogenen Gefahrenverdacht".[167] Dies gilt, im Unterschied zum nichtvirtuellen Raum[168], auch gleichermaßen für nachrichtendienstliche Tätigkeit, da die Beeinträchtigung durch den Eingriff im Vergleich zur polizeilichen Tätigkeit identisch ist.[169] Zusammenfassend gesagt will das BVerfG mit diesen Anforderungen verhindern, dass staatliche Stellen Auskünfte „ins Blaue hinein" anfordern, ohne dass ein Anfangsverdacht oder eine konkrete Gefahr überhaupt bestehen.[170]

---

[160] Beulke, Strafprozessordnung, 11. Auflage 2010, Rn. 254a.
[161] Schmidt, Auswirkungen des Urteils zur Vorratsdatenspeicherung auf die Praxis, in: AnwZert ITR 5/2010, Anm. 2 (Publikation enthält keine Seitenzahlen).
[162] BVerfG 1 BvR 256/08, Rn. 228 m.w.N.
[163] Ibid, Rn. 262, 291.
[164] Albers/Reinhardt, Entscheidungsbesprechung – Vorratsdatenspeicherung im Mehrebenensystem: Die Entscheidung des BVerfG vom 2.3.2010, ZJS 2010, S. 767, 772. Damit definiert das BVerfG für den präventiven Bereich den Eingriff rechtsgutsbezogen und nicht straftatenbezogen, dazu kritisch Möstl, Das Bundesverfassungsgericht und das Polizeirecht – Zwischenbilanz aus Anlass des Urteils der Vorratsdatenspeicherung, DVBl. 2010, S. 808, 811.
[165] BVerfGE 120, 274, 328.
[166] BVerfG 1 BvR 256/08, Rn. 231;
[167] Möstl, Das Bundesverfassungsgericht und das Polizeirecht – Zwischenbilanz aus Anlass des Urteils der Vorratsdatenspeicherung, DVBl. 2010, S. 808, 811.
[168] Dazu kritisch Wolff, Vorratsdatenspeicherung – Der Gesetzgeber gefangen zwischen Europarecht und Verfassung?, NVwZ 2010, S. 751, 753, der auf Unterschiede zwischen Polizei und Nachrichtendienste außerhalb des virtuellen Raums anhand von § 8 Abs. 2 BVerfSchG (Bundesverfassungsschutzgesetz) verweist.
[169] BVerfG 1 BvR 256/08, Rn. 232f.
[170] Ibid, Rn. 261.

Das BVerfG hebt explizit die Möglichkeit hervor, bei Verletzungen angemessenen Schadensersatz auch für immaterielle Schäden zu erhalten. Ebenfalls angesprochen wird die Frage nach Beweisverwertungsverboten im Straf- und wohl auch im Zivilverfahren.[171] Auch ist der unabhängige[172] Datenschutzbeauftragte in die Kontrolle der Einhaltung der Vorschriften mit einzubeziehen.[173] Insbesondere obliegt ihm die Kontrolle der Unternehmen, die der Speicherpflicht unterliegen, wobei er dann durch seine jährlichen Berichte auf etwaige Missstände hinzuweisen hat.[174] Damit korrespondiert, dass das BVerfG weiters ein ausgeglichenes System zur Sanktionierung von Verstößen gegen gesetzliche Vorgaben oder Weisungen der Aufsichtsbehörden verlangt, das auch Verstöße gegen die Datensicherheit entsprechend würdigt.[175] Nur durch eine solche Vorgehensweise kann letztlich die Verhältnismäßigkeit der Vorratsdatenspeicherung gewährleistet werden.[176]

„Die Anforderungen erstrecken sich auch auf eine fristgerechte Löschung der Daten, so dass diese auch zu protokollieren ist, dem Vier-Augen-Prinzip unterliegt und der Datenschutzbeauftragte in die Kontrolle einzubeziehen ist. Auch muss ein Sanktionssystem etabliert werden, wenn Daten, die hätten gelöscht werden müssen, zur Verfügung standen oder Daten dem unbefugten Zugriff Dritter ausgesetzt waren und dadurch Grundrechte der Betroffenen verletzt wurden.“[177] Weiters darf die Speicherung der Telekommunikationsverkehrsdaten nicht das Ziel haben, allgemein und umfassend sämtliche Daten vorsorglich zu speichern, welche präventiv zur Gefahrenabwehr oder repressiv zur Strafverfolgung für staatliche Stellen von Nutzen sein könnten. Sobald der Gesetzgeber dieses Ziel verfolgt, führt dies automatisch zur Verfassungswidrigkeit des Gesetzes. Es muss sich also zwingend – um die Anforderungen de BVerfG auf einen Punkt zu bringen – um eine Regelung handeln, die auch des Ausnahmecharakters der Vorratsdatenspeicherung gewahr wird.[178]

II.2.1.4 Anforderungen an die gesetzliche Konkretisierung

Das Gericht gibt dem Gesetzgeber durch sein Urteil genaue legistische Vorgaben mit einem relativ engen Spielraum. Lediglich die konkrete technische Ausgestaltung darf er hierbei der Aufsichtsbehörde oder dem Verordnungsgeber überlassen. Alle anderen Regelungen bedürfen einer exakten gesetzlichen Normierung. Der Gesetzgeber muss diesen „besonders hohen Sicherheitsstandard in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgeben“.[179]

---

[171] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 400; BVerfG 1 BvR 256/08, Rn. 252.
[172] Vgl. zum Begriff des unabhängigen Datenschutzbeauftragten EuGH, Az. C518/07.
[173] BVerfG 1 BvR 256/08, Rn. 225.
[174] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 400.
[175] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 400; BVerfG 1 BvR 256/08, Rn. 224 f., 252
[176] BVerfG 1 BvR 256/08, Rn. 239, 246
[177] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 400.
[178] BVerfG 1 BvR 256/08, Rn. 218.
[179] Das Normenklarheitsgebot erlangt, ebenso wie der Bestimmtheitsgrundsatz, eine zunehmend stärkere Bedeutung. Vgl. dazu Albers/Reinhardt, Entscheidungsbesprechung – Vorratsdatenspeicherung im

Damit verbietet sich für den Gesetzgeber ein wie bisher in § 113a Abs. 10 dTKG generalklauselartiger, auf die „im Bereich der Telekommunikation übliche Sorgfalt“ bezugnehmender, Verweis, der den Speicherverpflichteten Art und Maß der Sicherung frei überlässt.[180] Ebenfalls unzulässig ist es den Aspekt der Wirtschaftlichkeit, wie in § 109 dTKG, mit einzubeziehen und deswegen Abstriche zu machen. Die Vorschriften dürfen also keiner Aufweichung durch nicht sicherheitsrelevante Erwägungen unterliegen.[181] Orientierungsmaßstab muss vielmehr der „jeweiligen Stand der Technik“ sein, weswegen eine statische Festlegung ebenfalls ausscheidet. Dazu darf sich der Gesetzgeber einer Generalklausel bedienen.[182] Die Datensicherheit muss hierbei oberste Priorität haben.[183]

Hinsichtlich der Datensicherheit fordert das Gericht „gesetzliche Regelungen, die einen solchen besonders hohen Sicherheitsstandard in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgeben.“ Dabei hat sich dieser Standard an dem Entwicklungsstand der Fachdiskussion zu orientieren. Dies bedeutet, dass er neue Erkenntnisse und Einsichten fortlaufend aufzunehmen hat und nicht unter dem Vorbehalt einer freien Abwägung mit allgemeinen wirtschaftlichen Gesichtspunkten stehen darf.[184] „Nur wenn diesbezüglich hinreichende anspruchsvolle und normenklare Regelungen getroffen sind, ist der in einer solchen Speicherung liegende Eingriff verhältnismäßig im engeren Sinne“, so das Gericht. Gerade dies wird durch die angegriffenen Vorschriften weder in Bezug auf eine hinreichende Datensicherheit noch bezüglich einer hinreichenden Begrenzung der Verwendungszwecke der Daten garantiert.[185] Folglich kann ein in qualifizierter Weise dem Grunde nach den konkretisierter Schutzstandard nur dann vorliegen, wenn der Gesetzgeber die Schutzmechanismen selbst benennt. Nur deren Ausgestaltung kann er auf Verordnungen oder Aufsichtsbehörden delegieren. Keinesfalls darf die Entscheidung über Art und Maß der Sicherung in irgendeiner Weise beim Telekommunikationsanbieter selbst liegen.[186] Dabei ist auch ein Zustand nicht tragbar, in dem die Speicherpflicht zwar verbindlich ist, jedoch eine technische Konkretisierung nicht vorliegt, wie es bisher in § 113 a a.F. dTKG der Fall gewesen war.[187]

Weiters werden vom Gericht auch die nähere Voraussetzungen an eine anspruchsvolle Verschlüsselung umrissen: Die Verschlüsselung ist dann als anspruchsvolle Verschlüsselung anzusehen, wenn sie nach dem derzeitigen Stand der Technik ohne erheblichen Aufwand nicht zu überwinden ist. Ferner ist es hierbei erforderlich durch organisatorische Maßnahmen sicherzustellen,

---

Mehrebenensystem: Die Entscheidung des BVerfG vom 2.3.2010, ZJS 2010, S. 767, 772, Fn. 35 m.w.N; vor allem die Entscheidung BVerfGE 113, 33, 53 ist hier von Bedeutung. Dort geht es um vorbeugende Telekommunikationsüberwachung. Ein Grund für eine detaillierte Ausgestaltung der Normen ist nach Ansicht des BVerfG nicht zuletzt die Tatsache, dass sich so der Betroffene – zumindest theoretisch – auf den Grundrechtseingriff einstellen kann.

[180] BVerfG 1 BvR 256/08, Rn. 224ff., 269ff.

[181] Ibid, Rn. 271.

[182] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 399; BVerfG 1 BvR 256/08, Rn. 224, 273

[183] BVerfG 1 BvR 256/08, Rn. 222.

[184] Schmidt, Auswirkungen des Urteils zur Vorratsdatenspeicherung auf die Praxis, in: AnwZert ITR 5/2010, Anm. 2 (Publikation enthält keine Seitenzahlen).

[185] Ibid.

[186] BVerfG 1 BvR 256/08, Rn. 225

[187] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 399; BVerfG 1 BvR 256/08, Rn. 271ff.

dass die Schlüssel und ggf. das Passwort ebenfalls sicher aufbewahrt werden.[188] Außerdem sind die Daten von den weiteren IT-Systemen des Speicherverpflichteten separiert zu speichern. Sie sind von anderen Systemen hardwaremäßig zu trennen und vom Internet zu entkoppeln.[189] Nicht genügend ist es nach Auffassung des BVerfG, die Daten, die zur Vorratsdatenspeicherung gedacht sind, durch eine Kennzeichnung in der Datenbank von Daten für Abrechnungszwecke zu separieren.[190] Weiters darf sich kein Rückschluss auf den Inhalt der Kommunikation ergeben, so dass auch die Speicherung der von den Kunden aufgerufenen Internetseiten durch die Unternehmen grundsätzlich untersagt ist.[191] Außerdem hat der Zugriff auf die Daten einem gesicherten Zugriffsregime zu unterliegen, wofür die Unternehmen, die der Speicherpflicht unterliegen, gesetzlich zu verpflichten sind. Beispielhaft wird vom BVerfG das Vier-Augen-Prinzip angeführt,[192] so dass der Zugriff auf Daten nicht durch Einzelpersonen, sondern nur durch zwei oder mehr Personen möglich ist.[193] Ferner erforderlich ist eine revisionssichere Protokollierung des Zugriffs. Damit verlangt das BVerfG, dass einerseits ein Zugriff auf die Daten überhaupt nur möglich ist, wenn der Zugriff auch protokolliert wird. Andererseits muss dieses Protokoll nicht unabänderbar sein, um revisionssicher zu sein.[194]

II.2.2 Konsequenzen des BVerfG-Urteils für die TKG-Novelle in Österreich

Im Entstehungsprozess der Umsetzung zur Vorratsdatenspeicherung in Österreich brachte die Entscheidung des dt. BVerfG entscheidende Impulse im Hinblick auf die Frage der Datensicherheit und damit verbunden der Art der Datenbankhaltung, der Übermittlung und der Protokollierung. Hier hat auch der ursprüngliche BIM-Entwurf zur TKG-Novelle 2010 die wesentlichsten Nachbesserungen erfahren. In der Begründung des BVerfG zur Aufhebung der dt. TKG-Novelle wird zentral die mangelnde Gewährleistung eines besonders hohen Standards hinsichtlich der Datensicherheit hervorgehoben. Dort wird insbesondere kritisiert, dass ein bloßer Verweis auf die im Bereich der Telekommunikation allgemein erforderliche Sorgfalt, welcher die nähere Konkretisierung der Maßnahmen den einzelnen Dienstleistern überlässt, zu unbestimmt sei. Das deutsche Höchstgericht fordert Instrumente zur Gewährleistung der Datensicherheit, zB getrennte Speicherung, asymetrische Verschlüsselung, Vier-Augen-Prinzip verbunden mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln, revisionssichere Protokolierung von Zugriff und Löschung.

Die für diese Fragen maßgeblich bestimmenden gesetzlichen Grundlagen im TKG sind:

§ 94 Abs. 4 TKG, welcher die näheren Regelungen betreffend die Übertragung der Daten enthält: „Die Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von

---

[188] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 399.
[189] Ibid.
[190] Ibid.
[191] BVerfG 1 BvR 256/08, Rn. 218
[192] Ibid, Rn. 224; näher dazu unten zur Protokollierung in Kapitel IV.2.8.1.
[193] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 399; Albers/Reinhardt, Entscheidungsbesprechung – Vorratsdatenspeicherung im Mehrebenensystem: Die Entscheidung des BVerfG vom 2.3.2010, ZJS 2010, S. 767, 772.
[194] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 399.

Verkehrsdaten erfordern, einschließlich der Übermittlung von Vorratsdaten, nach den Bestimmungen der StPO sowie des SPG, hat unter Verwendung einer Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt, zu erfolgen. Die Daten sind unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie als "Comma-Separated Value (CSV)" - Dateiformat zu übermitteln. (…)". Diese Bestimmung ist durch eine Verordnung näher zu präzisieren, welche die an der Praxis orientierten Details festlegt. Die Conclusion der vorliegenden Studie besteht eben aus einem konkreten Regelungsvorschlag samt Erläuterungen für eine solche Verordnung.

§ 102c, der generell die Datensicherheit, Protokollierung und die Statistik regelt, wobei Absatz 1 leg cit den Rahmen wie folgt vorgibt: „Die Speicherung der Vorratsdaten hat so zu erfolgen, dass eine Unterscheidung von nach Maßgabe der §§ 96, 97, 99, 101 und 102 gespeicherten Daten möglich ist. Die Daten sind durch geeignete technische und organisatorische Maßnahmen vor unrechtmäßiger Zerstörung, zufälligem Verlust oder unrechtmäßiger Speicherung, Verarbeitung, Zugänglichmachung und Verbreitung zu schützen. Ebenso ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den Vorratsdaten ausschließlich dazu ermächtigten Personen unter Einhaltung des Vier-Augen-Prinzips vorbehalten ist. Die Protokolldaten sind drei Jahre ab Ende der Speicherfrist für das betreffende Vorratsdatum zu speichern. Die Kontrolle über die Einhaltung dieser Vorschriften obliegt der für die Datenschutzkontrolle gemäß § 30 DSG 2000 zuständigen Datenschutzkommission. (…)". Diese Bestimmung ist ebenfalls durch Verordnung zu konkretisieren und wird gemeinsam mit der Verordnung nach § 94 Abs 4 erlassen werden.

Eine (in Österreich zumindest logisch) getrennte Datenbankhaltung war schon im ursprünglichen BIM-Entwurf[195] vorgesehen. Die verschärften Zugriffsvoraussetzungen beim Anbieter intern wurden erst nach dem Urteil des BVerfG aufgenommen. Im Zentrum stehen dabei die Vorgaben des BVerfG, wonach die Zugriffe auf Vorratsdaten beim Anbieter intern nur unter Einhaltung eines 4-Augen-Prinzips unter revisionssicherer Protokollierung erfolgen dürfen. Dies setzt eine entsprechende Entkoppelung der Datenbankinfrastruktur für Vorratsdaten voraus, die beim Anbieter einen nicht unwesentlichen Aufwand zum (insbesondere softwaremäßigen) Aufbau dieser Infrastruktur verursachen.

Die sehr detaillierten Vorgaben des BVerfG für einen sicheren Datentransfer haben dazu geführt, dass vom ursprünglichen Konzept einer verschlüsselten Übermittlung per E-Mail abgegangen wurde. Da E-Mail per se ein unsicheres Medium ist, sind entsprechend hohe Datensicherheitsstandards im Sinne dieser Vorgaben kaum zu erreichen. Außerdem zeigt die internationale Kooperation im Rahmen von Europol, wie schwierig es ist, bei einer großen Zahl von dezentralen Kommunikationspartnern die notwendigen Sicherheitszertifikate auf Stand zu halten (diese müsse aus Sicherheitsgründen regelmäßig erneuert werden). Daher wurde schließlich in § 94 Abs. 4 TKG die „Verwendung einer Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt" vorgeschrieben. Diese Formulierung ist flexibler und schreibt zugleich einen Sicherheitsstandard vor, der bei Verwendung einer auf dem SMTP-Protokoll basierenden Technologie nur schwer zu erreichen ist.[196] Auch die Formulierung „unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie"[197] (im Gegensatz

[195] Vgl. § 102c BIM-Entwurf TKG Novelle 2010.
[196] Details dazu unten beim Vergleich der Konzepte DLS und S/MIME in Kapitel III.2.
[197] § 94 Abs. 4 TKG.

zur „Übertragung per E-Mail“ nach dem ursprünglichen BIM-Entwurf zur TKG-Novelle) „ist eine Ergänzung zur Erfüllung anspruchsvoller Datensicherheitsstandards, wie sie insbesondere im Urteil des deutschen Bundesverfassungsgerichts zu BVerfG, 1 BvR 256/08 vom 2.3.2010 beschrieben werden. Die Formulierung lässt genügend Spielraum, die nähere technische Ausgestaltung durch Verordnung zu regeln und stellt gleichzeitig einen Auftrag an den Verordnungsgeber dar.“[198]

II.3 DATENSICHERHEIT BEI DER ÜBERMITTLUNG

II.3.1 DAS „VORRATSDATEN-URTEIL“ DES DEUTSCHEN BUNDESVERFASSUNGSGERICHTS

II.3.1.1 ZUGRIFF DURCH STAATLICHE BEHÖRDEN

Abfrage und Übermittlung von Telekommunikationsverkehrsdaten sind nach Ansicht des BVerfG aus verfassungsrechtlichen Gründen unter einen Richtervorbehalt zu stellen und bedürfen einer Eingrenzung zum einen für einen bestimmten Zeitraum und zum anderen für einen bestimmten Anschluss.[199] Auch wenn der Richtervorbehalt in Art. 10 Abs. 2 GG keine ausdrückliche Erwähnung findet, so ist er doch notwendig, was aus dem Grundsatz der Verhältnismäßigkeit folge. das BVerfG löst damit auch in gewisser Weise das Spannungsverhältnis zum subsidiären vom BVerfG entwickelten „IT-Grundrecht“[200], das Eingriffe in den Schutzbereich ebenfalls unter einen Richtervorbehalt stellt.[201] Dabei sind die zu übermittelnden Daten im Anordnungsbeschluss hinreichend selektiv und eindeutig zu bezeichnen. Sind diese Voraussetzungen nicht gegeben, darf der Anbieter weder berechtigt noch verpflichtet sein die Daten herauszugeben.[202]

Folglich wird man sicherstellen müssen, dass dem betroffenen Dienstanbieter die Möglichkeit der Beschwerde offen steht, um die Anbieter nicht mit den richterlichen Anordnungen, die sie ggf. für zu unbestimmt halten, alleine zu lassen und ihnen nur die Wahl zwischen einer etwaigen Verletzung der Grundrechte ihrer Kunden oder dem Vorwurf der Verhinderung der Aufklärung von Verbrechen zu lassen, ohne dass sie die Möglichkeit haben, die Rechtmäßigkeit der vorliegenden Anordnung erneut einer gerichtlichen Kontrolle zu unterwerfen. In der Tatsache, dass die Speicherung und Zugriffssicherung auf privater Seite und das Herausgabeverlangen auf staatlicher Seite angesiedelt ist, liegt ein vom BVerfG hervorgehobener zusätzlicher Sicherungsmechanismus.[203]

Damit ist eine Herausgabe sämtlicher Daten eines Anbieters ausgeschlossen. In der Folge scheidet ebenfalls die Möglichkeit aus, die Daten für eine Rasterfahndung oder zur geheimdienstlichen

---

[198] EB zur RV zu § 94 Abs. 4 TKG, BlgNR 1074, XXIV. GP.
[199] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 400; BVerfG 1 BvR 256/08,. Rn. 247 ff
[200] BVerfGE 120, 274.
[201] Wolff, Vorratsdatenspeicherung – Der Gesetzgeber gefangen zwischen Europarecht und Verfassung?, NVwZ 2010, S. 751, 752.
[202] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 400; BVerfG 1 BvR 256/08, Rn. 249.
[203] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 400.

Analyse einer abstrakten Gefahrenlage zu benutzen.[204] Damit berechtigt lediglich der konkrete Verdacht einer schweren Straftat, die der Gesetzgeber noch genauer konkretisieren muss, zur Datenauskunft. Das BVerfG ist sich dabei auch der Tatsache bewusst, dass die Daten damit für Nachrichtendienste und die Gefahrenabwehr kaum Verwendung finden können und nimmt dies aber, wie bereits im Rahmen der sog. „Online-Durchsuchung" bei der wegweisenden Entscheidung zum „IT-Grundrecht"[205], in Kauf.[206]

II.3.1.1.1 Verkehrsdaten mittelbar (IP-Adressen)

Das BVerfG hält die die Nutzung der auf Vorrat gespeicherten Daten im Rahmen des Auskunftsverfahrens nach § 113 dTKG zur Ermittlung des Anschlussinhabers einer dynamischen IP-Adresse am weitesten für zulässig. Hierfür bedarf es bei hinreichendem Anfangsverdacht bzw. konkreter Gefahr bzgl. einer Straftat oder sogar schwerwiegender einzelner durch den Gesetzgeber zu benennender Ordnungswidrigkeiten keines Richtervorbehalts.[207] Die zentrale Argumentation des BVerfG führt dazu aus, dass der Zugriff auf diese Daten einen wesentlich geringeren Eingriff in das Fernmeldegeheimnis für die Betroffenen darstellt als der Zugriff auf sämtliche Verkehrsdaten eines Teilnehmers.[208] Zwingend ist für das BVerfG jedoch im Regelfall die Benachrichtigung der Nutzer von einer solchen Auskunft.[209]

Keinesfalls zulässig wäre es den staatlichen Behörden direkten Zugriff auf die Daten zu belassen.[210] Es liegt also stets ein Verstoß gegen Art. 10 GG vor, wenn die speicherverpflichteten Privaten – auch freiwillig – ihren kompletten Datenbestand den Behörden zur Verfügung stellen. Es ist aus verfassungsrechtlicher Perspektive nur erlaubt, Daten nach richterlicher Anordnung zu übermitteln, wobei auch dann nur solche Daten übermittelt werden dürfen, die zu der jeweiligen Anordnung passen.[211]

Folglich darf der Abruf der Daten durch den Staat stets nur der zweite Schritt sein, dem das Speichern der Daten beim Anbieter vorausgegangen ist, so dass die Daten zunächst nur in der Hand diverser privater Einzelunternehmen sind. Es ist hierbei durch besondere technische Vorkehrungen sicherzustellen, dass kein direkter Zugriff auf die Daten erfolgen kann, sondern eine Herausgabe nur anlassbezogen nach rechtlich fixierten Kriterien möglich ist. Diese Trennung dient dabei nicht zuletzt auch der Transparenz und Kontrolle der Datenverwendung, welche einer genaueren rechtlichen Ausgestaltung bedarf.[212]

---

[204] BVerfG 1 BvR 256/08, Rn. 232
[205] BVerfGE 120, 274, 331.
[206] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 401; BVerfG 1 BvR 256/08, Rn. 234.
[207] BVerfG 1 BvR 256/08, Rn. 254 ff.).
[208] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 401
[209] BVerfG 1 BvR 256/08, Rn. 263.
[210] Ibid, Rn. 250.
[211] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 401.
[212] BVerfG 1 BvR 256/08, Rn. 214, 249.

Die Daten unterfallen auch dann noch dem Schutzbereich von Art. 10 GG, nachdem sie einmal in die Hände des Staates gelangt sind. Vielmehr setzt sich der Schutz an den dort vorhandenen Daten fort.[213] Eine Weitergabe der Daten darf somit nur auf gesetzlicher Grundlage erfolgen. Diese muss ebenfalls den verfassungsrechtlichen Anforderungen genügen. Damit kann eine Weitergabe nur unter den Voraussetzungen zulässig sein, unter denen auch der Zugriff überhaupt möglich war, da ein gleiches Schutzniveau gewährleistet werden muss.[214]

Neu ist im Bereich des § 113 dTKG und erheblich erweitert im Rahmen des § 100g dStPO ist die Forderung des BVerfG nach Transparenz bzgl. der Datenverwendung und zur Gewährleistung eines effektiven Rechtsschutzes.[215] Nach bisher geltender Rechtslage erfuhren die Betroffenen von der Auskunft im Regelfall nichts. Erst im Rahmen einer anwaltlichen Abmahnung wegen angeblicher Handlungen im Internet erfuhren viele Betroffene von einer Auskunft nach § 113 dTKG.

Nun sind sie direkt nach Abruf der Daten nach § 113 dTKG zu benachrichtigen.[216] Dies zeige nach Auffassung des Gerichts nicht zuletzt die Parallelwertung zur Wohnungsdurchsuchung (§§ 102, 103, 106 dStPO), bei der der Wohnungsinhaber auch ein Anwesenheitsrecht hat; ein ähnliches Recht sei auch demjenigen einzuräumen, auf dessen Daten zugegriffen wurde.[217] Abgesehen werden darf von einer Benachrichtigung nur, wenn in diesem Fall damit auch der Zweck der Auskunft gefährdet wird, also lediglich im Rahmen der Gefahrenabwehr und im Rahmen nachrichtendienstlicher Tätigkeit. Nach Abschluss der heimlich durchgeführten Maßnahme ist der Betroffene im Regelfall jedoch hiervon in Kenntnis zu setzen.[218] Die sei, so das BVerfG, nicht zuletzt aus dem Gebot des effektiven Rechtsschutzes (Art. 19 Abs 4 GG) zu folgern.[219]

Von einer nachträglichen Benachrichtigung darf folglich nur dann abgesehen werden, wenn verfassungsrechtlich geschützte Rechte Dritter im Raum stehen, was aber sehr einschränkend interpretiert werden muss.[220] Im Übrigen muss, wenn keine direkte Benachrichtigung erfolgt, der Grund für das Unterbleiben einer solchen aktenkundig gemacht werden, damit das behördliche Vorgehen stets nachvollzogen werden kann.[221] Ebenfalls richterlich angeordnet werden muss für Auskünfte nach §100g dStPO das Ausbleiben der Benachrichtigung, was bisher ebenfalls nicht vorgesehen war.[222]

---

[213] Ibid, Rn. 236.
[214] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 401.
[215] BVerfG 1 BvR 256/08, Rn. 243.
[216] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 401.
[217] BVerfG 1 BvR 256/08, Rn. 243
[218] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 401; Albers/Reinhardt, Entscheidungsbesprechung – Vorratsdatenspeicherung im Mehrebenensystem: Die Entscheidung des BVerfG vom 2.3.2010, ZJS 2010, S. 767, 772 f.
[219] Möstl, Das Bundesverfassungsgericht und das Polizeirecht – Zwischenbilanz aus Anlass des Urteils der Vorratsdatenspeicherung, DVBl. 2010, S. 808, 814.
[220] Vgl. hierzu BVerfGE 109, 279, 364.
[221] BVerfG 1 BvR 256/08, Rn. 263.
[222] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 401.

II.3.1.2 Auswirkungen des Urteils über die Vorratsdatenspeicherung hinaus

Auskünfte im Rahmen des urheberrechtlichen Auskunftsanspruchs sind durch die Entscheidung des Gerichts bezüglich einer Verwendung der Vorratsdaten ausgeschlossen. „Das Gericht erlaubt für die Suche nach dem Anschlussinhaber nach § 113 dTKG, der letztlich dieselbe Zuordnung vornimmt wie § 101a UrhG auf öffentlich-rechtlicher Ebene, die Verwendung nur bei Straftaten oder schweren Ordnungswidrigkeiten.“[223]

Bei Zugriffen auf die Vorratsdaten verlangt das BVerfG aber einen absoluten Richtervorbehalt, dessen Umgehung unzulässig ist und darüber hinaus auch einen Richtervorbehalt für die nicht erfolgte Mitteilung der Maßnahme an den Betroffenen.[224] Es ist Aufgabe des Gerichts zu beurteilen, inwiefern die beantragte Datenabfrage den gesetzlichen Voraussetzungen entspricht, wobei die sorgfältige Prüfung der Eingriffsvoraussetzungen, insbesondere der Eingriffsschwelle, besonders sorgfältig zu prüfen ist. Im Anschluss bedarf es einer „gehaltvollen“ Begründung, die die abzufragenden Daten individuell bezeichnet, so dass kein Interpretationsraum auf Seiten des Dienstanbieters mehr besteht und dieser auch keine eigene Prüfung anstellen muss.[225]

Das BVerfG verpflichtet weiters in seiner Entscheidung auch die Fachgerichte, Rechtsverstöße im Zusammenhang mit der Vorratsdatenspeicherung mit der Annahme von Beweisverwertungsverboten und Schadensersatzansprüchen zu sanktionieren.[226] Bei einer heimlichen Durchführung der Maßnahme ist dem Betroffenen Rechtsschutz auch im Nachhinein zu gewähren.[227]

II.3.2 Die Mediatisierung der Abfragen über eine CSV-Datei gemäß § 94 Abs. 4 TKG

Wie eben dargestellt verlangt der effektive Grundrechtsschutz im Zusammenhang mit Verkehrsdatenabfragen auch nach Auffassung des deutschen Bundesverfassungsgerichts eine klare Mediatisierung auf technischer Ebene zwischen der Abfrage von Daten durch staatliche Behörden und den Datenbanken der Anbieter. Diese Auffassung wurde bereits vor der Entscheidung des BVerfG im März 2010 im BIM-Entwurf zur TKG-Novelle im September 2009 vertreten und in der Ausgestaltung des Vorschlags zu § 94 Abs. 4 TKG berüchsichtigt[228]. Aus Sicht der technischen Vorgaben beinhaltet der zentrale Vorschlag dort, die Daten mittels einer sog. CSV Datei (Comma Separate Value) durch verschlüsselte E-Mail zu übermitteln.[229]

Die Form der Übermittlung durch verschlüsselte E-Mail unter Verwendung des S/MIME Standards wurde in weiterer Folge überdacht, nicht zuletzt weil das bei der Umsetzung der Vorratsdatenspeicherungsrichtlinie federführende BMVIT nach der Veröffentlichung des Urteils des BVerfG erkannte, dass für eine ausreichende Datensicherheit nicht allein die Verschlüsselung der Inhalte sondern auch eine Transportverschlüsselung, eine sichere Authentifizierung sowie

---

[223] Ibid. S. 402.
[224] Ibid.
[225] BVerfG 1 BvR 256/08, Rn. 249.
[226] Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 403.
[227] BVerfG 1 BvR 256/08, Rn. 251.
[228] Siehe die Erläuterungen zu § 94 Abs. 4 BIM-Entwurf TKG Novelle 2010.
[229] Etwas ausführlicher dazu unten in Kapitel IV.2.5.

Identifizierung der Teilnehmer am Datenaustausch von großer Bedeutung ist. Diese Komponenten sind jedoch bei einer E-Mail Kommunikation mit SMTP Technologie wenn überhaupt nur sehr aufwendig hinreichend zu erfassen. Daher folgte das BMVIT schließlich dem Vorschlag des BIM, diese und weitere Fragen der Datensicherheit in einer Studie einer näheren Betrachtung zu unterziehen und bereits die Zwischenergebnisse der Untersuchung in die endgültige Ausgestaltung des § 94 Abs. 4 TKG zu einfließen zu lassen. Dies führte schließlich zur finalen Ausgestaltung des § 94 Abs. 4 TKG:

„(4) Die Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, einschließlich der Übermittlung von Vorratsdaten, nach den Bestimmungen der StPO sowie des SPG, hat unter Verwendung einer Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt, zu erfolgen. Die Daten sind unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie als "Comma-Separated Value (CSV)" - Dateiformat zu übermitteln. Ausgenommen davon ist die Übermittlung von Daten in den Fällen des § 98, von Daten in den Fällen von § 99 Abs. 5 Z 3 und 4 bei Gefahr in Verzug, von Standortdaten in den Fällen der Feststellung des aktuellen Standortes gemäß §§ 134 ff StPO sowie die Übermittlung von begleitenden Rufdaten im Rahmen einer Überwachung von Nachrichten. Durch Verordnung kann der Bundesminister für Verkehr, Innovation und Technologie im Einvernehmen mit den Bundesministern für Inneres und für Justiz die näheren Bestimmungen zur einheitlichen Definition der Syntax, der Datenfelder und der Verschlüsselung, zur Speicherung und Übermittlung der Daten sowie die näheren Bestimmungen betreffend die Speicherung der gemäß § 102c angefertigten Protokolle festsetzen. Nach Erlass der Verordnung ist unmittelbar dem Hauptausschuss des Nationalrates zu berichten."

II.3.2.1 Die Branchenempfehlung "EP020" für eine Technische Richtlinie zur Datenübermittlung

Mit der Vorgabe des § 94 Abs. 4 TKG, die Übermittlung von Verkehrsdaten an Sicherheits- und Strafverfolgungsbehörden in Form einer CSV-Datei durchzuführen, geht die Notwendigkeit einher, die Datenfelder und die Syntax einer solchen Datei vorab in einer „Technischen Richtlinie" per Verordnung festzulegen. Eine solche Verordnungsermächtigung ist daher in dieser Norm auch ausdrücklich enthalten. Im Verlauf der Entstehung des BIM-Entwurfs zur TKG Novelle war aus den Diskussionen mit Vertretern des BMI und des BMJ das Argument im Raum, dass eine völlig eigenständige „österreichische Lösung" für eine Schnittstelle zur Datenübermittlung deshalb fragwürdige sei, weil in Anlehnung an die Richtlinie 2006/24/EG zur Vorratsdatenspeicherung bereits ein ETSI-Standard existiere, der alle Definitionen bereits einheitlich für alle Anbieter enthalte und nur noch technisch umgesetzt werden müsse. Demgegenüber müsse eine völlig andere Lösung erst sehr aufwändig unter Einbeziehung der Telekommunikationsbranche erarbeitet werden und sei daher nicht ökonomisch.[230] Um diesem Argument praktisch zu begegnen, war der Beweis notwendig, dass eine solche Harmonisierung für die Schnittstelle zum Datenaustausch durch die Verwendung einer CSV-Datei sogar erleichtert würde, weil es sich bei CSV um einen völlig technologieneutralen

[230] Zur Begründung, warum aus Sicht des Grundrechtsschutzes eine direkte, nicht technisch mediatisierte Schnittstelle zwischen Behörden und Anbietern – wie im ETSI-Standard vorgesehen – abzulehnen ist, sei hier auf die Auszüge aus dem Urteil des deutschen Bundesverfassungsgerichts sowie auf das vorhergehende Kapitel zur CSV-Datei (II.3.2) verwiesen; zum ETSI Standard sowie zum Kostenargument siehe unten Kapitel IV.2.5.

Standard handelt und lediglich zu klären ist, an welcher Stelle der CSV-Datei welche Information zu finden ist und welche Syntax bei der Darstellung verwendet wird. Daher wurde vom Projektkoordinator und Autor der vorliegenden Arbeit bereits im Sommer 2009 angeregt, die österreichische Telekom-Branche solle sich – aus eigener Initiative und im Interesse einer auch ökonomischen Lösung – damit beschäftigen, einen Vorschlag für eine solche harmonisierte „technische Richtlinie“ auf Basis der Vorschläge des BIM zu § 94 Abs. 4 TKG zu erarbeiten.

Konkret geschah dies sodann ab November 2009 durch den AK-TK, in dem die österreichische Landschaft der Internet- und Telekommunikationsdienste Anbieter repräsentiert ist. Der "Arbeitskreis für technische Koordination für öffentliche Kommunikationsnetze und -dienste" (AK-TK) dient primär der Förderung der Zusammenarbeit und des Erfahrungsaustausches zwischen den Anbietern öffentlicher Kommunikationsnetze und -dienste. Die Plattform wurde geschaffen, um im Hinblick auf administrative und technisch-betriebliche Aufgaben, die sich insbesondere im Zusammenhang mit der Netzzusammenschaltung stellen, konkrete Fragen zu definieren und gemeinsame Festlegungen mit dem Ziel bestmöglicher Lösungen auszuarbeiten.[231] Im AK-TK wurde eine Arbeitsgruppe zur Schnittstellendefinition eingerichtet. Die Arbeitsgruppe erhielt vom Plenum des AK-TK Ende 2009 folgendes Mandat:

"Im Rahmen des AK-TK wird eine Arbeitsgruppe mit dem Titel „Schnittstellendefinition zur Vorratsdatenspeicherung“ (kurz „Schnittstellendefinition“) eingesetzt. In dieser Arbeitsgruppe soll eine technische Richtlinie erarbeitet werden, welche die Erfordernisse nach TKG Entwurf § 94 (4) erfüllt und in der Arbeitsgruppe abgestimmt wird. Die für diese Arbeiten erforderlichen Experten können im Rahmen der Arbeitsgruppe beigezogen werden. Die Arbeiten sind ehestens zu beginnen. Ziel ist es, eine in der Arbeitsgruppe abgestimmte Empfehlung zum Plenum des AK TK Ende Januar 2010 vorzulegen."

Planmäßig wurde bis Ende Jänner 2010 im AK-TK eine Empfehlung für eine technische Richtlinie (EP020) erarbeitet. Die EP020 definiert dabei die Struktur der Datei, die einer Behörde als Antwort auf ein Auskunftsbegehren übermittelt wird. Die Definition einer Schnittstelle gestaltet die Anfrage - Antwort - Kommunikation zwischen Behörden und Anbietern, also wie die Datei zu übermitteln ist. Dieser Teil zur Frage der Übermittlung der Daten ist in der finalen Version der Branchenempfehlung EP020 nur mit wenigen Ansätzen enthalten, die sich auf das Konzept der „Durchlaufstelle“ beziehen (siehe dazu Kapitel III).

Das Mandat wurde mit der Erstellung und Abstimmung der Ausgabe 2 der EP 020 im Jänner 2010 erfüllt. Das Mandat wurde schließlich im 32. Plenum des AK-TK im November 2011 wie folgt erweitert:

„Die Arbeitsgruppe Vorratsdatenspeicherung des AK TK soll die Schnittstellendefinition EP 020 überarbeiten. Insbesondere ist diese Schnittstellendefinition den geänderten Rahmenbedingungen anzupassen und weiters sind Klarstellungen im Zusammenhang mit offenen Fragen zu ergänzen. Im Zusammenhang mit der Überarbeitung der Schnittstellendefinition soll die Arbeitsgruppe auch eine Plattform für die Diskussion mit dem Boltzmann Institut für Menschenrechte und anderen Experten darstellen. Diese Diskussion soll aktuelle Themen im Zusammenhang mit der Umsetzung der Vorratsdatenspeicherung unter Berücksichtigung der bis Mai 2011 notwendigen Umsetzung der

[231] Siehe die Beschreibung auf der Internetseite des AK-TK unter http://www.oefeg.at/ak-tk/.

Rahmenrichtlinie ermöglichen. Hier geht es um die Möglichkeit, den Branchenstandpunkt gegenüber dem Boltzmann Institut für Menschenrechte zu artikulieren."

Die insgesamt 15 Treffen der „AG Schnittstellendefinition" des AK-TK standen seit dem Kick-off-meeting des BIM am 16.November 2011 bei insgesamt 9 Treffen explizit im Zusammenhang mit der Studie des BIM zur Datensicherheit. Inhaltlich wurde an die Arbeit zur EP020 und an diese Empfehlung selbst angeknüpft. Nach Beschluss der Novellen zum TKG 2003, StPO und SPG am 28. April 2011 in zweiter Lesung im Nationalrat wurde mit der Überarbeitung der EP 020 selbst begonnen. Die finale Version der EP020 wurde für den Begutachtungsentwurf zur Datensicherheitsverordnung dort integriert. Im Rahmen des Vorschlages für die Umsetzungsverordnung bildet die EP020 normativ selbst einen integralen Bestandteil der Verordnung. Dieser Arbeit wird die finale Version der EP020 als Anhang B) beigelegt.

II.4 Gesetzliche Determinierung des Sorgfaltsmaßstabes

Für den Untersuchungsgegenstand dieser Arbeit ist zunächst der erste Grundsatz wesentlich, den die Richtlinie 2006/24/EG in Art 7 lit a) aufstellt: „Die auf Vorrat gespeicherten Daten sind von der gleichen Qualität und unterliegen der gleichen Sicherheit und dem gleichen Schutz wie die im Netz vorhandenen Daten". Diese Festlegung bewirkt auf jeden Fall, dass bestehende Schutzgesetze und Systeme auf technischer und organisatorischer Ebene bei den Anbietern als Mindeststandard nicht unterschritten werden dürfen.

Darüber hinaus bestehen grundrechtliche Schutz- und Gewährleistungspflichten, die den Staat dazu anhalten, einen entsprechenden Rechtsrahmen zu gestalten, damit ein effektiver Schutz gegen mögliche Bedrohungen für grundrechtlich geschützte Interessen besteht.[232] Insoweit der im Folgenden dargestellte bestehende Rahmen bestimmte vorhersehbare Risiken nicht abdeckt, trifft den Gesetzgeber bzw. auch die Verwaltung die Pflicht, positive Maßnahmen zu ergreifen. Konkret heißt das im gegenständlichen Zusammenhang vor allem, dass eine entsprechende Datensicherheitsverordnung zu erlassen ist, mit der die Risiken so gering wie möglich gehalten und der Rechtsschutz gefördert werden soll.

II.4.1 Die bevorstehende Umsetzung des 3. EU Telekom-Rahmenpakets

Der Sorgfaltsmaßstab für die interne Datenverarbeitung durch den Anbieter war bereits bisher im 12. Abschnitt des TKG (Kommunikationsgeheimnis und Datenschutz) insbesondere in Ausführung der Richtlinie 2002/58/EG gesetzlich determiniert. Die Branche der Telekommunikation ist mit rechtlichen Vorgaben zu Datensicherheit und Datenschutz in einem Ausmaß und mit einem Determinierungsgrad konfrontiert, der sich - abgesehen vom Bankensektor - in kaum einem anderen Wirtschaftszweig findet. Im Allgemeinen werden die bestehenden Sicherheitsvorkehrungen bei den Anbietern daher als ausreichend gesehen. Zu berücksichtigen ist darüber hinaus, dass sich aktuell eine Novellierung des Telekommunikationsrechts in Österreich in der finalen Phase der gesetzlichen

[232] Siehe dazu die rechtsdogmatischen Grundlagen oben in Kapitel II.1.1.3.3.

Umsetzung befindet[233], um das 3. Telekom-Paket der EU[234] umzusetzen, wobei viele der Vorgaben aus den EU Richtlinien die allgemeine Datensicherheit betreffen. Auf diese Novellierung wird in dieser Studie nur am Rande eingegangen, soweit es wesentliche Überschneidungen zu den hier erörterten Fragestellungen gibt.

Die Regelung darüber hinausgehender Sicherheitsvorschriften, liegen im Spielraum der Mitgliedsstaaten, höhere Sicherheitsanforderungen zu erlassen (Art 7 Abs 1 RL 2006/24/EG, arg. „zumindest folgende Grundsätze"). Die oben dargestellte Entscheidung des deutschen Bundesverfassungsgerichts (BVerfG, 1 BvR 256/08 Urteil vom 2.März 2010) zur dortigen Aufhebung der deutschen Umsetzung der Vorratsdatenspeicherungs-Richtlinie zeichnet dazu den Raster, der insbesondere die Basis für das Programm der Diskussionen im empirischen Teil darstellt. Konkretisierungen sind vor allem notwendig, wo die Besonderheiten der „Vorratsdaten" dies erfordern. Damit sind das 4-Augen-Prinzip und die revisionssichere Protokollierung bei internen Datenzugriffen angesprochen, weil die Unternehmen Vorratsdaten für eigene operative Zwecke gar nicht verwenden dürfen.

II.4.2 Relevanz des ISO 27000 Standard für den Sorgfaltsmaßstab

Als bekannteste und am weitesten verbreitete (wenngleich unverbindliche) Norm für einen Datensicherheitsstandard wurde zu Beginn die ISO 27000 Zertifizierung behandelt. Auf Grund des enormen Zeit- und Kostenaufwandes bei einer Realisierung dieses Standards ist dieser Weg nicht empfehlenswert, zumal insbesondere kleinere Anbieter den hohen organisatorischen und technischen Anforderungen kaum mit wirtschaftlich verhältnismäßigen Mitteln gerecht werden könnten. Die ISO selbst arbeitet seit mehr als einem Jahr daran, die ISO 27000 Standards für Klein- und Mittelunternehmen (KMU´s) angemessen umzugestalten. Verwertbare Ergebnisse dazu liegen bislang keine vor. Eine ISO 27000 Zertifizierung als Sorgfaltsmaßstab heranzuziehen, wäre jedenfalls überschießend und würden für viele Anbieter einen untragbaren wirtschaftlichen Aufwand bedeuten.

---

[233] Zum Zeitpunkt des Abschlusses dieser Studie sind gerade die finalen rechtspolitischen Diskussionen nach der parlamentarischen Begutachtung eines Entsprechenden Ministerialentwurfes des BMVIT im Gange. Die Stellungsnahmen zum Ministerialentwurf (269/ME) sind unter http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00269/index.shtml abrufbar.

[234] Das sog. „Telekomreformpaket" besteht aus folgenden Richtlinien: RL 2009/140/EG zur Änderung der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und –dienste, der RL 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung und der RL 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und -dienste (Rahmenrichtlinie), ABl. Nr. L 337 vom 18.12.2009, S. 37, sowie der RL 2009/136/EG zur Änderung der RL 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und –diensten, der RL 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der VO (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, ABl. Nr. L 337 vom 18.12.2009, S. 11 und weiters der VO (EG) Nr. 1211/2009 zur Einrichtung des Gremiums Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) und des Büros zur Einsetzung des neuen Gremiums der europäischen Telekom-Regulierungsbehörden (GEREK).

II.4.3 Bestehende Haftungsbestimmungen zur Datensicherheit

Die strafrechtliche sowie die zivilrechtliche Haftung bei Verletzung der besonderen Sicherheitsvorschriften nach dieser Verordnung richtet sich nach den allgemeinen gesetzlichen Haftungsbestimmungen, insbesondere des § 302 StGB, der §§ 31, 32, 33, 51 und 52 DSG. Für die Anknüpfung einer möglichen Haftung nach dem Verbandsverantwortlichkeitsgesetz (VbVG) in Verbindung mit den jeweiligen strafrechtlichen Haftungsbestimmungen hat der Anbieter intern zu dokumentieren, welche Entscheidungsträger und Mitarbeiter (§ 2 VbVG) für die Verarbeitung von Vorratsdaten verantwortlich sind. Die interne Dokumentation und bestehende interne Betriebsdaten-Richtlinien sowie relevante Protokollierungsdaten sind dem zuständigen Gericht oder der Datenschutzkommission im Falle eines Verfahrens, in dem ein datenschutzrechtlicher Anspruch geltend gemacht wird, zur Verfügung zu stellen.

Festzuhalten ist, dass sich die Zielsetzung dieser Arbeit auf jene Regelungsgegenstände konzentriert, die im Rahmen der Umsetzungsverordnung zu §§ 94 Abs. 4 und 102c TKG zur Datensicherheit liegen. Die Normierung von Haftungsbestimmungen, die über das bestehende gesetzliche Maß hinaus gehen, würde die Verordnungsermächtigung überschreiten und wäre daher verfassungsrechtlich unzulässig. Nachfolgend soll daher nur die bestehende Rechtslage im Überblick dargestellt werden, ohne dazu rechtspolitische Änderungsvorschläge zu benennen.

II.4.3.1 Haftung des Staates und seiner Beamte

Für die Haftung des Staates kommen mehrere Szenarien in Betracht. Zum einen ist ein Amtshaftungsanspruch denkbar, weiters nicht ausgeschlossen, ist die Haftung einzelner Beamter auf Grund von Amtsmissbrauch. Aber auch aus den Normen des DSG kann sich eine direkte Haftung auch staatlicher Stellen ergeben. Somit sind grundsätzlich sowohl Zivil- als auch Strafverfahren denkbar. Im Folgenden soll auf Gemeinsamkeiten und Unterschiede der einzelnen Haftungsformen eingegangen werden.

II.4.3.1.1 Haftung nach dem AHG

Nach dem Amtshaftungsgesetz (AHG) haftet der Bund für Schäden gem. § 1 Abs 1 AHG. Hierbei sind zunächst zwei Fälle denkbar, nach denen es zur Haftung kommen kann. Auf der einen Seite kann der Fall eintreten, dass, durch das Fehlverhalten einzelner Beamter[235] oder die Tatsache, dass durch technische Entwicklungen, der Kommunikationsvorgang nicht mehr für sicher gehalten werden kann (z.B. durch Algorithmenverfall[236] und Dritte dadurch Einblick in gespeicherte oder übermittelte Daten erhalten.[237]

---

[235] Zu deren persönlicher strafrechtlicher Haftung siehe unter II.4.3.1.2.

[236] Von Algorithmenverfall ist dann auszugehen, wenn die verwendeten Algorithmen nicht mehr dem Stand der Technik entsprechen und damit nicht mehr sicher sind (vgl. Schemmann, Die Beweiswirkung elektronischer Signaturen und die Kodifizierung des Anscheinsbeweises in § 371a Abs. 1 Satz 2 ZPO, ZZP 118 (2005), 161.)

[237] Reischauer in Rummel[3], § 1328a, Rz 17.

Auf beide Arten ist es möglich, dass Inhalte des Kommunikationsvorgangs in die Hände unbefugter Dritter gelangen. Dem ersten Fall kann schon allein dadurch entgegengewirkt werden, dass an der Abfrage der Daten mehr als nur eine Person beteiligt ist[238]. Etwas komplizierter gestaltet sich der zweite Fall. Der Staat muss damit automatisch gehalten sein, die technische Entwicklung stetig im Auge zu behalten, und entsprechend rasch zu reagieren. Ein Zurückziehen auf die Position, das System habe zum Zeitpunkt der Einrichtung alle technischen Anforderungen zur Datensicherheit erfüllt, wäre nicht genügend. Ebenso wie es außerhalb des virtuellen Raums zur Amtshaftung führt, wenn staatlicherseits eine gewerbliche Genehmigung unter einer Auflage ausgesprochen wird, die Einhaltung dieser Auflage aber nicht überprüft wird und dadurch letztendlich ein Schaden entsteht.[239] So muss es bei der Datenübermittlung folgerichtig zur Haftung führen, wenn der Staat nicht oder nicht genügend dafür Sorge trägt, die Sicherheit seiner Systeme „up-to-date" zu halten.

Da sich die Vorschriften des Schadensersatzes nach den Regelungen des Zivilrechts richten (vgl. § 1 Abs 1 S 1 AHG), war für den Ersatz immaterieller Schäden in Geld im Rahmen der Amtshaftung zunächst kein Raum. Immaterielle Schäden sind nach den Regelungen des bürgerlichen Rechts nämlich nur dann ersatzfähig, wenn es dafür eine ausdrückliche Regelung gibt (beispielsweise § §1325, 1328 ABGB oder § 31 e KSchG).

Durch eine Gesetzesänderung im Jahre 2004[240] wurde jedoch § 1328a ABGB neu geschaffen, der in bestimmten Fällen den Raum für nicht materiell bemessbaren Schadensersatz für Verletzung der Privatsphäre[241] eröffnet. Dieser umfasst auch den ideellen Schaden. Diese Entschädigung soll die mit dem Verlust der Privatsphäre einhergehenden Unlustgefühle des Geschädigten kompensieren.[242] Allerdings legt § 1328a ABGB hohe Hürden für die Geltendmachung von immateriellen Schäden. Diese sind auf erhebliche Eingriffe beschränkt. Dabei entscheidend ist die Intensität des Eingriffs für den § 1328a ABGB beispielhaft die Bloßstellung in der Öffentlichkeit anführt.

Dadurch dass ein Fall der Amtshaftung vorliegt, ergibt sich keine Beweislastumkehr, daran ändert letztlich auch die Tatsache nichts, dass der Staat sich stets rechtskonform zu verhalten hat.[243] Dabei ist jedoch nicht das Fehlverhalten einer einzelnen staatlichen Stelle zu beweisen, sondern nur das Fehlverhalten als solches, also im vorliegenden Fall beispielsweise, dass Vorratsdaten an nichtberechtigte Personen gelangt sind.

II.4.3.1.2 HAFTUNG NACH STGB

Eine Heranziehung des Straftatbestandes des § 302 StGB käme nur bei einer behördlichen Amtspflichtverletzung in Betracht, weil nur hier Beamte handeln können. Vorraussetzung für dessen Anwendbarkeit ist nämlich, dass der Täter § 74 Abs 1 Z 4 StGB unterfällt und damit im

[238] Näheres dazu unter Kapitel II.4.3.1.2.
[239] OGH, Entscheidung vom 09. 06. 1992, Gz 1Ob16/92; 1Ob93/00h.
[240] ZivRÄG 2004, BGBl I 2003/91.
[241] Was dabei unter Privatsphäre zu verstehen ist, ist aus der EMRK und Vorschriften des StGB zu entnehmen (vgl. Hinteregger in Kletečka/Schauer, ABGB-ON 1.00 § 1328 a, Rz. 2 (www.rdb.at).
[242] Hinteregger in Kletečka/Schauer, ABGB-ON 1.00 § 1328 a, Rz 8 (www.rdb.at).
[243] Reischauer in Rummel[3], § 1298, Rz. 30a m.w.N.

strafrechtlichen Sinne Beamter ist[244]. Dies schränkt allein den Kreis der möglichen Täter weit ein. Für eine Erfüllung des Straftatbestandes des § 302 StGB ist es erforderlich, dass der Beamte seine Befugnisse, die ihm kraft seines Amtes gegeben sind, missbraucht. Entscheidend ist also, ob der Beamte einen Hoheitsakt vornimmt missbräuchlich, also entgegen der gesetzlichen Vorschriften vornimmt.[245]

In der Praxis kommt es gelegentlich zu Verurteilungen nach § 302 StGB mit datenschutzrechtlicher Relevanz. Ein mehrfach aufgetretener Fall ist der, dass Polizeibeamte, ohne dass es dafür eine dienstliche Veranlassung gegeben hätte, eine EKIS/SIS-Abfrage[246] durchführen und diese Daten dann an Dritte übermitteln. Zumeist wurden KFZ-Kennzeichen in die Datenbank eingegeben[247], um Informationen über die Fahrzeughalter zu erlangen, aber es wurde auch schon konkret danach gesucht, inwiefern gegen eine bestimmte Person ein Haftbefehl vorliegt[248].

Übertragen auf die Vorratsdatenspeicherung besteht eine ungleich niedrigere Gefahr des Amtsmissbrauchs als bei einer EKIS/SIS-Abfrage. Kann die EKIS/SIS-Abfrage von einem Polizeibeamten alleine am Dienst-PC aus durchgeführt werden, so bedürfte es für einen „erfolgreichen" Amtsmissbrauch in Bezug auf Vorratsdaten schon dem kollusiven Zusammenwirken von zwei Personen. Die von Dritten unbemerkte Abfrage durch eine Person bei der Polizei oder der Staatsanwaltschaft ist jedoch nur eingeschränkt möglich. Dafür sorgen einerseits der Richtervorbehalt und auf der anderen Seite behördeninterne Kontrollmechanismen. Missbrauchsanfällig sind daher vor allem jene Ermittlungsbefugnisse, die keine solchen Kontrollmechanismen vorsehen, insbesondere § 53 Abs. 3a SPG und § 76a Abs. 2 StPO.[249]

Eine Haftung aus § 302 Abs 1 StGB wird somit in der Praxis eher eine untergeordnete Rolle spielen. Käme es zu einer Haftung, wäre diese - darin liegt ein großer Unterschied zur Haftung nach dem AHG - in jedem Fall unabhängig davon, ob für den Betroffenen tatsächlich ein Schaden eingetreten ist. Die Schädigung liegt also etwa nicht in einem konkreten Schaden, der dem Geschädigten auf Grund der

---

[244] Der Täter muss also zwingend ein österreichischer Beamter oder eine einem österreichischen Beamten gleichgestellte Person sein (vgl. Bertel in WK^2 § 302, Rz. 1 1 ff.).

[245] Bertel in WK^2 § 302, Rz. 22.

[246] Bei EKIS handelt es sich um das Elektronischen Kriminalpolizeilichen Informationssystem, eine Datenbank der Kriminalpolizei, die folgende Daten umfasst: das Strafregister (Rechtsgrundlagen: Strafregistergesetz / Tilgungsgesetz), die KFZ - Fahndungs- / Informationsdatei (Rechtsgrundlagen: § 57 SPG iVm § 169 Abs. 2 StPO), die Personenfahndungsdatei (Rechtsgrundlagen: § 57 SPG iVm § 169 Abs. 1 StPO), die Personeninformationsdatei (enthält sicherheitspolizeiliche, passrechtliche und waffenrechtlich relevante Informationen, Rechtsgrundlagen: § 57 SPG, § 22b Passgesetz sowie § 55 WaffG), die Sachenfahndungsdatei (Rechtsgrundlagen: § 57 SPG iVm § 169 Abs. 2 StPO, § 22b Passgesetz), die Kulturgutfahndungsdatei (Rechtsgrundlagen: §§ 53 Abs. 1 Z 5, 53a Abs. 1 und 57 SPG iVm § 169 Abs. 2 StPO), der Kriminalpolizeiliche Aktenindex (enthält Informationen über die wegen des Verdachts einer vorsätzlich begangenen, von Amts wegen zu verfolgenden gerichtlich strafbaren Handlung an die Staatsanwaltschaften erstatteten Abschlussberichte der Kriminalpolizei, Rechtsgrundlagen: § 57 SPG iVm § 100 Abs. 2 Z 4 StPO), die Erkennungsdienstliche Evidenz samt AFIS (= automationsunterstütztes Fingerabdrucksystem) und die DNA-Datenbank (Rechtsgrundlagen: § 75 SPG). (vgl. http://www.bmi.gv.at/cms/BMI_Datenschutz/ekis/start.aspx). Bei SIS, handelt es sich um das Schengen Informationssystem, eine Datenbank die Daten enthält, die für die Einreise und den Aufenthalt im Schengenraum, von Bedeutung sind (vgl. https://www.dsk.gv.at/site/6226/default.aspx).

[247] Wie im Fall OGH, Beschluss vom 26.03.2009, Gz 12Os2/09z oder OGH, Beschluss vom 19. 10. 2010, Gz 14 Os 105/10p.

[248] Vgl. OGH, Beschluss vom 15. 06. 2010, Gz 14 Os 64/10h.

[249] Zur Kritik dieser Befugnisse vgl. oben in Kapitel II.1.5.

unberechtigten Datenverwendung entsteht; vielmehr liegt der Schaden bereits in der unberechtigten Datenverwendung selbst. Auch dies folgt nicht zuletzt aus dem Grundrecht auf Datenschutz in § 1 DSG.[250] Insbesondere gibt es keine Erheblichkeitsschwelle. Im Übrigen verdängt § 302 StGB § 301 StGB, der, wenn der Täter Beamter ist, somit nicht mehr anzuwenden ist.[251]

II.4.3.1.3 HAFTUNG NACH DEM DSG

Auch nach dem DSG ist eine staatliche Haftung denkbar. Schadensersatz ist im DSG in § 33 DSG geregelt. Dieser verweist Streitigkeiten hierüber, ebenso wie das AHG, an die Zivilgerichtsbarkeit (§ 33 Abs 4 iVm § 32 Abs 4 DSG).

Ein Schadenersatzanspruch steht den Betroffenen gem § 33 Abs 1 S 1 DSG zunächst dann zu, wenn die Daten entgegen der Bestimmungen des DSG verwendet wurden. Dies wäre bei einem Gelangen von Vorratsdaten in die Hände unbefugter Dritter stets zu bejahen, ein Verstoß gegen § 1 Abs 1 DSG wäre in jeden Fall gegeben. Würde durch einen solchen Fall ein tatsächlicher Vermögensschaden entstehen, wäre der Voraussetzungen des § 33 Abs 1 S 1 DSG bereits genügt und dem Betroffenen stünde, nach den Vorschriften der §§ 1293 ff ABGB, eine Entschädigung zu.[252]

Ideeller Schaden ist nur dann ersatzfähig, wenn die Datenverwendung einer öffentlichen Bloßstellung gleichkommt (§ 33 Abs 1 S 2 DSG). Hier gibt es insofern eine gewisse Parallele zur Regelung des § 1328a ABGB. Die Vorschrift zieht hier Parallelen zum Mediengesetz. Eine Bloßstellung in diesem Sinne ist nicht die Offenbarung jeder vielleicht peinlichen Situation, vielmehr liegt die Eingriffsschwelle sehr hoch: die Bloßstellung muss als solche enthüllend sein und intimste Details[253] aus dem Leben der betroffenen Person offenbaren.[254]

Im Unterschied zur Amtshaftung ergibt sich im Rahmen des § 33 Abs 3 DSG in gewissem Umfang eine Beweislastumkehr. Ein Entkommen aus der Haftung ist demnach nur dann möglich, wenn nachgewiesen werden könnte, dass der Umstand, durch den die Daten offenbart wurden, von Seiten des Staates nicht zu vertreten wäre.[255] Dies dürfte bei beiden hier geschilderten Szenarien nur schwerlich möglich sein.

Im Übrigen kann sich auch aus der Verletzung von § 1 DSG iVm den Vorschriften des bürgerlichen Rechts als Schutzgesetz ein Schadenersatz ergeben. Zumindest ein ideeller Schaden, der nach §§ 1 iVm 33 DSG ersatzfähig ist, verdrängt dabei aber die Geltendmachung nach § 1328a ABGB iVm § 1 DSG.[256] Es wäre nur für materielle Schäden eine zusätzliche Geltendmachung über § 1311 S 2 ABGB iVm. § 1 DSG möglich.

---

[250] OGH, Beschluss vom 12. 08. 2010, Gz 12 Os 28/10z. m.w.N.
[251] Pilnacek in WK² § 301, Rz, 16.
[252] Dohr/Pollirer/Weiss, DSG², 11. Er.-Lfg., § 33, Anm. 2.
[253] Darunter fielen zB Details über etwaige gewalttätige Auseinandersetzungen in der Ehe, vgl. OGH, Entscheidung vom 14. 12. 1998, Gz 18Bs272/98.
[254] Dohr/Pollirer/Weiss, DSG², 11. Er.-Lfg., § 33, Anm. 4.
[255] Dohr/Pollirer/Weiss, DSG², 11. Er.-Lfg., § 33, Anm. 5.
[256] Reischauer in Rummel³, § 1328a, Rz. 19.

II.4.3.2 HAFTUNG DER DIENSTANBIETER

Auch die Dienstanbieter können sich, wie auch der Staat, der Haftung ausgesetzt sehen. Nachfolgend soll auf Gemeinsamkeiten und Unterschiede der Haftung eingegangen werden.

II.4.3.2.1 KEINE HAFTUNG NACH § 302 STGB

Wie bereits geschildert ist § 302 StGB nur auf das Fehlverhalten von Beamten anwendbar. Nicht in Betracht käme damit Beispielsweise eine Anwendung von § 302 StGB auf Bedienstete der Telekom Austria GmbH, die vor der Privatisierung dem staatlichen bereich zuzurechnen gewesen wäre.[257]

II.4.3.2.2 HAFTUNG NACH DEM DSG

Für die Haftung nach dem DSG gilt im Prinzip, das unter II.4.3.1.3 gesagte. Auch die Anbieter trifft die Pflicht zum Schadenersatz nach § 33 DSG iVm § 1 DSG. Jedoch trifft sie nur Verantwortung für die Sicherheit der Systeme, die sie selbst unter Kontrolle haben. Eine Haftung für die Sicherheit des Übertragungsweges wird daher ausscheiden. Die Kommunikation zwischen Staat und Anbieter ist der staatlichen Seite zuzuordnen. Diese Kommunikation erfolgt entweder durch den Staat oder auf dessen Anforderung und ist diesem damit auch entsprechend zuzurechnen. Wenn die staatlichen Vorgaben zur Übermittlung bezüglich der Datensicherheit unzureichend sind, fällt dieses Verschulden ebenfalls dem Staat zur Last. Alles was außerhalb dieser Übermittlung an den Staat abläuft, ist schließlich den Anbietern selbst zuzurechnen.

II.4.3.3 RÜCKGRIFF DES STAATES

In bestimmten Fällen kann es für den Staat wiederum möglich sein, sich durch Rückgriff schadlos zu halten. Kommt digitale Signaturtechnik zum Einsatz, so ist die A-Trust GmbH, als einziger staatlich akkreditierter Signaturanbieter gem. § 23 SigG, haftbar. Während sich eine geschädigte Person nicht an den ZDA halten kann, da diese wohl kaum auf die Sicherheit des Zertifikates vertraut hat (§ 23 Abs 1 SigG), ist dies für staatliche Stellen durchaus möglich. Sieht sich der Staat Schadenersatzforderungen ausgesetzt, für die er auch nach den Vorschriften des AHG oder des DSG zuvörderst einzustehen hat, kann dieser sich im Rahmen des § 23 SigG bei der A-Trust dann schadlos halten, wenn mangelnde Signatursicherheit qualifizierter Signaturen[258] für den Schaden verantwortlich ist.

Die Haftungsbestimmungen des § 23 SigG weichen dabei im Großen und Ganzen recht stark vom normalen Deliktsrecht des ABGB ab. So enthält § 23 Abs 3 S 2 SigG eine spezielle Beweislastregelung bereit, die, für den Fall, dass *wahrscheinlich* Pflichten nach § 23 Abs 1 oder 2 SigG verletzt wurden; in

---

[257] Insbesondere ist § 112 TKG hier nicht anwendbar (vg. auch *Bertel* in WK^2 § 302, Rz 18).

[258] Die Haftung für nicht qualifizeirte Signaturen ist quasi nicht existent (vgl. hierzu Vonkilch, Die Haftung der Zertifizierungsanbieter nach dem SigG und ihre Pflichtversicherung, VR 2001, S. 122). Der Einsatz sog. Verwaltungssignaturen kommt aus eben diesem Grund auch nicht in Betracht (vgl.Forgo, Königsweg Verwaltungssignatur, RFG 2004/29).

diesem Fall bereits die Vermutung aufgestellt, dass diese Pflichtverletzung für den Schaden kausal ist. Dies wiederum kann der ZDA widerlegen, wenn er es als *wahrscheinlich* dartut, dass der Schaden nicht auf Grund einer Pflichtverletzung auf seiner Seite entstanden ist. Daraus ergibt sich in S 2 der Vorschrift eine Beweiserleichterung für denjenigen, der auf die Sicherheit der Signatur vertraut, jedoch keine wirkliche Beweislastumkehr, da da es zwur Widerlegung der Vermutung in S 2 gemäß S 3 keines Gegenbeweises bedarf.[259]

Bei der Gesetzgebung stand die Einführung einer Gefährdungshaftung durchaus zur Debatte, der Gesetzgeber entschied sich jedoch für eine Verschuldenhaftung mit eingeschränkter Beweislastumkehr.[260] Zusammenfassend kann also gesagt werden, dass dem Staat in gewissen Umfang auch eine Rückgriffsmöglichkeit bei der A-Trust GmbH zur Verfügung steht.

II.4.3.4 Möglichkeiten zum IT-Outsourcing

Die Möglichkeiten zum IT-Outsourcing bei der Vorratsdatenspeicherung sind beschränkt. Heute wird zunehmend Cloud-Computing verwendet um technische Ressourcen nicht direkt im Unternehmen verfügbar halten zu müssen.

II.4.3.4.1 Standard Cloudtechnologie

Technisch gesehen macht es für einen Telekommunikationsunternehmen keinen Unterscheid, wo sie ihre Daten speichern. Rechtlich gesehen unterliegen die Daten jedoch dem Recht des jeweiligen Staates in dem sie gespeichert sind. Eine Auslagerung ins Ausland dürfte damit nicht zulässig sein. Unterlägen die Daten ausländischem Datenschutzrecht, könnten Verstöße allenfalls nicht mit den in Österreich vorgesehenen Sanktionen geahndet werden. Auch passt das Wesen der Cloud nicht zu den strengen Vorgaben des Datenschutzrechts. Was wäre, wenn der heimische Cloud-Anbieter beschließt, seine Serverinfrastruktur aus Kostengründen nach China zu verlagern?[261] Dies würde der Anbieter wohl nicht einmal bemerken. Plötzlich könnten sich eventuell chinesische Behörden Zugang zu österreichischen Vorratsdaten verschaffen. Auch eine Verlagerung in Staaten wie die USA wäre extrem bedenklich.[262]

Es spricht allein aus diesen Gründen viel dafür, dass schon allein um sich nicht etwaigen Haftungsfolgen auszusetzen, der Diensteanbieter gehalten ist, die Daten unter seiner alleinigen Kontrolle zu halten.

---

[259] Vonkilch, Die Haftung der Zertifizierungsanbieter nach dem SigG und ihre Pflichtversicherung, VR 2001, S. 122.

[260] Einzelheiten hierzu bei Vonkilch, Die Haftung der Zertifizierungsanbieter nach dem SigG und ihre Pflichtversicherung, VR 2001, S. 122 m.w.N.

[261] Auf diesen Umstand machen Heidrich und Wegener aufmerksam (Heidrich/Wegener, Cloud Computing und Datenschutz, MMR 2010, 803, 806.

[262] Spies/Schröder, Auswirkungen der elektronischen Beweiserhebung (eDiscovery) in den USA auf deutsche Unternehmen, MMR 2008, 275 ff.

II.4.3.4.2 DIE CLOUD ALS BLACK BOX

Eine Möglichkeit die eventuell bestehen könnte, wäre die Auslagerung von Daten in eine Cloud, die als „Black Box" ausgestaltet ist. Diese Daten müssten dann so verschlüsselt sein, dass sie gegen sämtliche Zugriffe abgesichert sind, auch gegen etwaigen Zugriff von Behörden aus dem Speicherland. Voraussetzung hierfür wäre ein komplexes, noch nicht völlig erforschtes Verschlüsselungsverfahren, die sogenannte Fully Homorphic Encryption (FHE). Allerdings ist die Entwicklung noch nicht soweit vorangeschritten, dass man diese Technologie als ausgereift bezeichnen könnte. Davon abgesehen ergeben sich trotzdem immer noch Probleme bezüglich der Datenintegrität[263]

Somit muss auch eine als Black-Box ausgestaltetet Cloud am Ende als zulässige Möglichkeit ausscheiden. Hier bleibt abzuwarten, wie sich der Stand der Technik entwickelt.

II.4.3.4.3 PRIVATE-CLOUD

Weiters könnte natürlich der Anbieter eine Private Cloud aufbauen und entweder selbst oder durch Dritte eine Cloud nach genauen Vorgaben (österreichische Server, bis ins Detail festgelegtes Zugriffsregime, usw.) aufbauen. Durch so ein Vorgehen könnte datenschutzrechtlichen Vorgaben genügt werden, die Vorteile der Cloud, nämlich den Abbau eigener, kostspieliger Rechnerstrukturen, wären aber auch nicht mehr gegeben, da der Aufbau einer Private-Cloud natürlich ungleich höhere Kosten hervorruft.[264]

Damit dürfte der Einsatz einer Private-Cloud keinerlei datenschutzrechtliche Bedenken hervorrufen, jedoch dürfte ein ökonomischer Nutzen für die Anbieter nicht gegeben sein und somit in der Praxis auch dieser Cloud-Typ nicht zur Anwendung kommen, weil es sich quasi um eine Cloud handelt, die aller finanziellen Vorteile beraubt ist.

II.4.3.4.4 ZUSAMMENFASSUNG

Nach alldem erscheint die Cloud-Technologie nach derzeitigem Stand der Technik als für die Vorratsdatenspeicherung ungeeignet. Datenschutzrechtliche Vorgaben könnten nicht eingehalten werden bzw. könnte deren Einhaltung nach jetzigem Technikstand nicht vergleichbar mit einer Speicherung beim Anbieter selbst garantiert werden. Oder der finanzielle Nutzen wäre so gering, dass der Anbieter ohnehin auf eigene Speicherung zurückgreifen wird.

---

[263] Heidrich/Wegener, Cloud Computing und Datenschutz, MMR 2010, 803, 806 f.
[264] Heidrich/Wegener, Cloud Computing und Datenschutz, MMR 2010, 803 und 807.

III KONZEPT DER DURCHLAUFSTELLE (DLS) ZUR SICHEREN DATENÜBERMITTLUNG

III.1 ALLGEMEIN

Die Notwendigkeit einer Umsetzung der Vorratsdatenspeicherung erfordert auch, die Schnittstelle zur Übergabe der Daten zwischen Behörden und Telekommunikationsanbietern rechtlich zu regeln. Dabei wird für eine realistische Einschätzung davon ausgegangen, dass auf Seiten der Behörden insgesamt 15 Stellen (n) abfrageberechtigt sein werden (nach internem Erlass des BMI derzeit für den Regelfall 12, für die Zukunft wird seitens des BMI jedoch von 15 ausgegangen, einschließlich einer Stelle, die für Abfragen der Justiz unabhängig von der Kriminalpolizei allenfalls eingerichtet werden könnte). Auf Seiten der Anbieter sind nach Angaben der RTR aktuell ca. 200 Unternehmen (m) zur Entrichtung des Finanzierungsbeitrages nach § 34 KommAustriaG verpflichtet und damit nach dem TKG-Entwurf zur Umsetzung der Vorratsdatenspeicherung speicher- und auskunftspflichtig gem. §§ 102a und 102b TKG. Das Konzept der Durchlaufstelle (DLS) wurde dazu als Referenzmodell im Rahmen der BIM- Datensicherheitsstudie entwickelt, welches im Folgenden anhand der primär erforderlichen Funktionen erläutert wird. Die DLS stellt eine Art elektronisches Postfach dar, über das anfragende und abfragende Stellen miteinander kommunizieren und Informationen sicher austauschen.

III.1.1 SCHEMATISCHE DARSTELLUNG

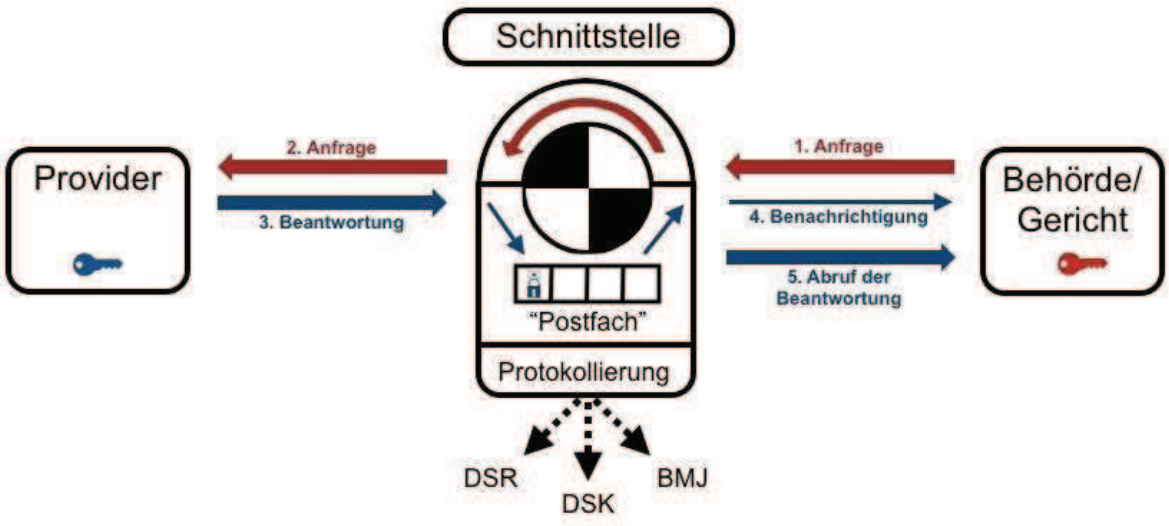

Abbildung 1: System der Durchlaufstelle (DLS)

Die DLS ist ein Modell für technische und prozedurale Abläufe, nicht jedoch eine Art neue Behörde oder Dienststelle. Die DLS hat vier Grundfunktionen: 1. Identifizierung, Authentifizierung, 2. Verschlüsselung (Datensicherheit im engeren Sinn), 3. Weiterleitung von Anfragen und deren Beantwortung (Postfachfunktion) und 4. Protokollierung der Auskunftsfälle einschließlich Erstellung einer Statistik.

Hierfür muss sich in einer sicheren öffentlichen Infrastruktur ein Server befinden, über den - technisch gesehen - die Anfragen abgewickelt werden. Eine Kommunikation über diesen Server ist dabei nur möglich, wenn die entsprechenden Stellen über eine Berechtigung (Authentifizierung) verfügen. Die verschiedenen Aufgaben im Zusammenhang mit der DLS (zB Schlüsselverwaltung, Benutzerverwaltung, etc.) können von verschiedenen Stellen übernommen werden, unabhängig davon, wo die DLS als Server rein physisch betrieben wird.[265] Die DLS ist zwingend die Drehscheibe zur Kommunikation für alle Auskunftsfälle. Kern ist dabei, dass die jeweilige Seite ihre Anforderung/Antwort sicher über die DLS samt dem notwendigen Anhang (Anbieter-Anordnung nach § 139 Abs. 3 StPO, CSV-Datei mit den begehrten Daten) übermittelt.[266]

III.1.2 Identifizierung und Authentifizierung

Um sicherzustellen, dass ein Kommunikationspartner auch die Berechtigung zu einer Anfrage/Auskunft hat, muss sich dieser über den elektronischen Weg auch eindeutig identifizieren und authentifiziert können. Das heißt, dass im Vorfeld schon zwischen den Kommunikationspartnern ein Weg zu finden ist, um den anderen auch sicher zu erkennen.

Bei der DLS wird die gesamte Identifikation und Authentifizierung zentral verwaltet. Dies geschieht hier über das Anmelden an den Server mittels Benutzername und Passwort (und allenfalls einer persönlichen ID). Sobald sich also ein Teilnehmer bei dem Server anmeldet, kann (eine sichere IT-Umgebung vorausgesetzt) der Kommunikationspartner davon ausgehen, dass schon im Vorfeld die Authentifizierung sichergestellt ist.

III.1.2.1 Anfrageberechtigte Stellen

Der Regelfall für einen Zugriff auf Vorratsdaten ist nach der gesetzlichen Umsetzung der Vorratsdatenspeicherung eine gerichtlich bewilligte Anordnung des Staatsanwalts, das selbe gilt auch für betriebsnotwendige Daten, also Verkehrsdaten die beim Anbieter noch für rechtmäßige betriebliche Zwecke gespeichert werden. Verkehrsdatenauskünfte sind auch im SPG vorgesehen, im Vergleich zur StPO aber eingeschränkter. Für die Praxis ist aber zu bedenken, dass auch die Anfragen nach der StPO durch die Kriminalpolizei im Auftrag der Strafjustiz durchgeführt werden.[267] Organisatorisch ist es also klar überwiegend die Polizei, die ein Auskunftsbegehren an den Anbieter stellt oder zumindest weiterleitet. Die StPO kennt dabei keine Einschränkung, von welcher Organisationseinheit innerhalb der Polizei eine Anordnung der Staatsanwaltschaft weitergeleitet wird.

Auch im Sicherheitspolizeigesetz sind die abfrageberechtigten Stellen derzeit nicht eingegrenzt. Eine Beschränkung auf 12 anfrageberechtigte Stellen besteht aber aufgrund eines internen Erlasses des BMI, der für Mitglieder der Wirtschaftskammer Österreich (WKO) über die Website der WKO

[265] Vgl. BIM-Datensicherheitsstudie, S. 90.
[266] Ibid, S. 109 und 167.
[267] Siehe dazu oben die Erläuterung der Rechtslage in Kapitel II.1.4.4.

publiziert wurde[268]. Es ist rechtspolitisch unwahrscheinlich, dass diese anfrageberechtigten Stellen in das SPG ausdrücklich aufgenommen werden, eine Verankerung in der Verordnung zu §94 TKG scheitert daran, dass eine solche Regelung als Durchführungsverordnung nicht zum TKG sondern zu § 53 Abs. 3a und 3b SPG ergehen müsste.

Obwohl weder aus der StPO noch aus dem SPG eine Einschränkung ableitbar ist, welche behördlichen Stellen innerhalb der Polizei, der Staatsanwaltschaft oder der Gerichte an die DLS über den Portalverbund angeschlossen werden sollen, muss dies aus rein praktischen Gründen in der technischen Umsetzung erfolgen. Da nämlich jede abfrageberechtigte Stelle eindeutig identifiziert und authentifiziert werden muss, ist eine endliche Zahl von abfrageberechtigten Stellen bei der DLS zu definieren und zu implementieren. In den Diskussionen im Rahmen des 2. Round Tables zur BIM-Datensicherheitsstudie wurde von Seiten des BMI und des BMJ angenommen, dass künftig insgesamt 15 abfrageberechtigte Stellen – einschließlich einer Stelle der Justiz unabhängig von der Polizei – an die DLS angebunden werden sollen.[269]

III.1.2.2 DLS VIA PORTALVERBUND

Da schon eine vorhandene Infrastruktur seitens der Behörden bezüglich Benutzerverwaltung existiert, ist es naheliegend, diese in das Konzept der Durchlaufstelle einzubeziehen. Die genannte Infrastruktur bezieht sich auf den so genannten Portalverbund.[270] Dies ist eine Infrastruktur, die eine Benutzerauthentifizierung vornimmt und diese zwischen darin eingebundenen Serveranwendungen verteilt. Das heißt, sämtliche Behörden (BMI, BKA, DSK, BMJ, Exekutive, …), die standardgemäß schon in den Portalverbund eingebunden sind, können mit ihren bestehenden Benutzerkonten innerhalb der Portalverbundstrukturen auf die Durchlaufstelle zugreifen und dort ihre Anfragen an die Anbieter stellen. Durch diesen Portalverbund ist auch mit einem hohem Maß an Sicherheit gewährleistet, dass eine Berechtigung zur jeweiligen Anwendung (Im Falle der Justiz oder der Exekutive eine Anfrage, DSK und BMI Protokolle) gegeben ist. Die Anbindung der auskunftspflichtigen Telekom- und Internetanbieter würde über die Anwendung (DLS) erfolgen, da der Portalverbund selbst nur für Behörden konzipiert ist. Dazu gibt es im Bundesrechenzentrum (BRZ), das den Portalverbund betreibt, bereits einen gewissen Erfahrungsschatz, weil auf diese Weise etwa der Elektronische Rückverkehr (ERV) zur sicheren Kommunikation zwischen Gerichten und Rechtsanwälten abgewickelt wird und hierzu die Rechtsanwälte authentisch angebunden sind.

Die Anwendung selbst könnte etwa im Auftrag des BMVIT im Bundesrechenzentrum (BRZ) angesiedelt werden. Das BRZ steht dabei vorzugsweise zur Auswahl, da hier schon eine bestehende Anbindung der betroffenen Behörden zum Portalverbund vorhanden ist, ebenso eine ausreichende und sichere IT-Infrastruktur zum Betrieb der Anwendung (DLS) selbst. Das bedeutet, die Anwendung

---

[268] Erlass des BM.I zu § 53 Abs 3a und 3b SPG, GZ 94762_101-GD_08 (abrufbar auf der Web-Seite der WKO unter http://portal.wko.at/wk/format_detail.wk?AngID=1&StID=386310&DstID=5000 (10.10.2011); demnach sind folgende Dienststellen auskunftsberechtigt: Die 9 Landeskriminalämter (LKA), das Bundeskriminalamt, das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) und das Büro für interne Angelegenheiten (BIA → mit BGBl. I Nr. 72/2009 nunmehr umgewandelt in das „Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung“ - BAK); vgl. dazu bereits oben Kapitel II.1.4.4.3.

[269] Vgl. BIM-Datensicherheitsstudie S 101 und auf S 161 im Rahmen der Erläuterungen zu § 9 Begutachtungsentwurf Datensicherheitsverordnung (DSVO).

[270] Nähere Erläuterung siehe http://portal.bmi.gv.at/ref/downloads/PVWhitepaper.pdf.

(DLS) könnte im BRZ (housing) auf Equipment des BRZ (hosting) betrieben werden. Eine andere, davon unabhängige Frage ist, wer die Anwendung organisatorisch betreiben würde.

III.1.3 VERSCHLÜSSELUNG

Um die Daten während der Kommunikation (Übertragungsweg + „Zwischenlagerung" bis zur Verwendung) ausreichend vor Dritten zu schützen, müssen die angefragten Daten sowie die Anfrage selbst verschlüsselt werden. Die Schlüssel müssen schon im Vorfeld zwischen den Kommunikationspartnern vereinbart werden. Die Verschlüsselung der zu übertragenden Inhalte ist von der Transportverschlüsselung, also vom nach außen sicheren Übertragungskanal (etwa über eine https-Verbindung und entsprechende Sicherheitszertifikate) zu unterscheiden.

III.1.3.1 VERSCHLÜSSELUNG DER DATEN[271]

Zur Verschlüsselung der Daten selbst gibt es unterschiedliche Verfahren:

Symmetrische Verschlüsselungsverfahren: Die kommunizierenden Parteien verwenden zur Ver- und Entschlüsselung denselben Schlüssel, das heißt neben der verschlüsselten Information muss auch der Schlüssel übermittelt werden. Das Problem beim Einsatz symmetrischer Verfahren ist, dass der Schlüssel über einen sicheren Kanal übertragen werden muss, denn die Sicherheit des Verfahrens hängt von der Geheimhaltung des Schlüssels ab. Der Vorteil liegt in der größeren Geschwindigkeit, mit der die verschlüsselte Übertragung stattfinden kann.

Asymmetrische Verschlüsselungsverfahren: Jede der kommunizierenden Parteien besitzt ein Schlüsselpaar, das aus einem geheimen Teil (private key) und einem nicht geheimen Teil (public key) besteht. Der öffentliche Schlüssel ermöglicht es jedem, Daten für den Inhaber des privaten Schlüssels zu verschlüsseln. Die kommunizierenden Parteien müssen keinen gemeinsamen geheimen Schlüssel kennen, das Verfahren wird daher auch als Public-Key-Verfahren bezeichnet. Dafür ist eine Public-Key-Infrastruktur erforderlich, über die (vereinfacht dargestellt) die Ausstellung vertrauenswürdiger digitaler Zertifikate zur sicheren Übertragung organisiert wird. Die zentrale Herausforderung liegt darin, sicherzustellen, dass der öffentliche Schlüssel wirklich echt ist. Der Vorteil ist eine deutliche Minimierung des Sicherheitsrisikos, da jeder Benutzer nur seinen eigenen privaten Schlüssel geheim halten muss. Im Gegensatz dazu muss bei einem symmetrischen Verschlüsselungssystem jeder Teilnehmer alle Schlüssel geheim halten, was mit steigendem Aufwand verbunden ist, je mehr Teilnehmer daran beteiligt sind (große Zahl an Schlüsseln). Nachteilig ist, dass asymmetrische Kryptosysteme aufgrund der Verschlüsselungsalgorythmen im Vergleich zu den symmetrischen Verfahren sehr langsam sind.

Hybride Verschlüsselungssysteme: Der Geschwindigkeitsnachteil asymmetrischer Verfahren wird in der Praxis durch die Verwendung hybrider Systeme umgangen. Dabei werden die zu übertragenden Daten mit einem zufällig generierten Schlüssel (sog. „session key") symmetrisch verschlüsselt (deutlich schneller) und der jeweils verwendete Schlüssel unter Verwendung einer asymmetrischen

[271] Ein guter Überblick zu den verschiedenen Verschlüsselungsverfahren ist zu finden bei http://www.e-teaching.org/technik/datenhaltung/datenschutz/verschluesselung/.

Verschlüsselung an die Teilnehmer verteilt. Diese Variante löst das Schlüsselverteilungsproblem und erhält dabei den Geschwindigkeitsvorteil der symmetrischen Verschlüsselung. Das Verfahren entspricht dem Stand der Technik und wird der Anforderung einer technisch anspruchsvollen Verschlüsselung jedenfalls gerecht.

Die Verwaltung der öffentlichen Schlüssel erfolgt in der DLS vereinfacht dargestellt zentral. Dadurch ergibt sich Vorteil, dass diese im Wartungsfall unverzüglich (keine toten Schlüssel) und mit geringem Aufwand geändert werden können. Gleichzeitig kann über die DLS eine sichere Public Key Infrastruktur realisiert werden, was die Datensicherheit enorm erhöht. Eine zentrale Anforderung an das System ist dabei aber, dass die DLS selbst nicht über die privaten Schlüssel verfügt, durch welche die übertragenen Inhalte ersichtlich werden. Diese Schlüssel müssen auf einem anderen Weg – technisch abseits der DLS – zwischen den am Datenaustausch beteiligten Anbietern und Behörden ausgetauscht werden. Die DLS ist damit „blind" gegenüber den übertragenen Inhalten. Nur so ist aus der Perspektive einer grundrechtlichen Gewährleistungspflicht zu rechtfertigen, dass der Transfer über eine zentrale Instanz erfolgt. Andernfalls wäre das Potential der technischen Auswertungsmöglichkeiten aller zentral übertragenen Inhalte viel zu hoch und im Sinne der Pflicht zur Wahrung der Verhältnismäßigkeit des Grundrechtseingriffes überschießend.

III.1.3.2 VERSCHLÜSSELUNG DES KOMMUNIKATIONSWEGES

Abseits der Verschlüsselung der Daten selbst muss auch die Übertragung der Daten und Informationen in beide Richtungen verschlüsselt werden. Die Kommunikation zwischen DLS und Kommunikationspartnern funktioniert via https[272] oder ähnlichen verschlüsselten Verbindungen. Solche Verbindungen können mit allen gängigen Browser-Anwendungen (Internet Explorer®, Firefox®, …) ohne Vorkonfiguration oder Wartung verwendet werden und sind ausreichend sicher.

III.1.4 ABLAUF EINES AUSKUNFTSBEGEHRENS

Eine Anfrage muss eindeutig formuliert sein, um die Rechtsgrundlage(n) zum Auskunftsbegehren zweifellos ersichtlich zu machen. Durch eine vorgefertigte Eingabemaske ist ein missverständliches oder überschießendes Auskunftsbegehren ausgeschlossen. Eine Verteilung von Formularen ist nicht notwendig, die elektronischen Eingabemasken können von vornherein benutzerfreundlich gestaltet werden. Die Fehleranfälligkeit lässt sich dadurch auf ein Minimum reduzieren. Der Vorgang der Anfrage wird dadurch stark vereinfacht und spart sowohl bei den Behörden als auch bei den Anbietern Zeit und Ressourcen.

Eine Anfrage nach Daten an einen oder mehrere Anbieter kann regelmäßig bereits personenbezogene Daten mit schutzwürdigem Geheimhaltungsinteresse enthalten. Daher muss bereits die Anfrage selbst verschlüsselt an die DLS übermittelt werden. In der DLS wird die Anfrage entgegengenommen und in das Postfach bzw. die Postfächer eines oder mehrerer ausgewählter Anbieter zugestellt (siehe Schritt 1. in Abb. 1). Zugleich können hier von der DLS automatisiert die

[272] Https steht für „hyper text transfer protocoll secure" und ist der am stärksten verbreitete Standard zur Realisierung von sicheren Verbindungswegen im Internet, der zB häufig bei Online-banking Systemen zum Einsatz kommt; siehe dazu zB http://searchsoftwarequality.techtarget.com/definition/HTTPS.

ersten wesentlichen Protokollinformationen erfasst werden, etwa der Zeitpunkt der Anfrage, die anfragende Behörde oder der adressierte Anbieter sowie die gewünschten Datenarten. Als zentrale technische Klammer zur Nachvollziehbarkeit und Abwicklung aller Auskunftsvorgänge wird jeder Anfrage durch die DLS automatisch eine einmalige fortlaufende Nummer („Uniqu ID“) vergeben.

Nach Hinterlegung der Anfrage im DLS-Postfach des Anbieters wird dieser automatisch über das Einlagen der Anfrage informiert. Dies kann auch über ungesicherte Medien, zB ein herkömmliches E-Mail erfolgen, weil diese Information der DLS keine schutzwürdigen Daten enthält und lediglich der Beschleunigung des Auskunftsverfahrens dienen soll. Der Anbieter kann sodann jederzeit die gesicherte Verbindung zur DLS herstellen und das Auskunftsbegehren abholen (siehe Schritt 2. in Abb. 1). Die Entschlüsselung der Anfrage unternimmt der Anbieter innerhalb seines eigenen Systems mit Hilfe des privaten Schlüssels, den er zuvor von der Anfragenden Behörde über einen anderen sicheren Kanal abseits der DLS erhalten hat. So bleibt schon der Inhalt der Anfrage – wie später auch der Beantwortung – der DLS selbst verborgen.

Der Anbieter bearbeitet die Anfrage intern bei grundsätzlich freier Gestaltung, wie er die Übertragung der begehrten Daten aus seinem System in die CSV-Datei bewerkstelligt. Dem Anbieter bleibt überlassen, ob er diesen Vorgang teilweise automatisiert oder manuell aus seinem System überträgt. Vorgeschrieben ist jedoch, dass er die internen Zugriffe auf Vorratsdaten einer revisionssicheren Protokollierung unterwirft. Die die Anfragebeantwortung enthaltende CSV-Datei wird mit dem privaten Schlüssel des Anbieters verschlüsselt und nach der Verschlüsselung mit einem „Header“ versehen, der die – nicht personenbezogenen – Informationen für die Protokollierung und die Statistik in der DLS enthält. Hier werden für die DLS einseh- und verarbeitbar etwa die Informationen übertragen, welche Kategorien von Daten enthalten sind (zB IP-Adressen, Telefonverbindungsdaten, etc) und um wie viele Datensätze es sich handelt. Die verschlüsselte CSV-Datei samt unverschlüsseltem Header wird über den gesicherten Verbindungsweg an die DLS übertragen. Die Antwort wird dabei durch die Verknüpfung mit der „Uniqu ID“ automatisch in das richtige Postfach in der DLS jener Behörde zugestellt, von der die Anfrage ausging (siehe Schritt 3. in Abb. 1).

Zur Beschleunigung des gesamten Vorgangs wird die anfragende Behörde von der DLS automatisch darüber verständigt, dass die Beantwortung in das DLS-Postfach zugestellt wurde (siehe Schritt 4. in Abb. 1). Wie zu schritt 2. ausgeführt kann auch diese Verständigung über eine herkömmliche ungesicherte E-Mail erfolgen, weil keine schutzwürdigen Informationen enthalten sind. Wie die Information auf Seiten der Behörden an die richtigen bearbeitenden Beamten gelangt bleibt der behördeninternen Systemen vorbehalten.

Schließlich kann die Behörde wieder über die gesicherte Verbindung zur DLS auf ihr Postfach dort zugreifen und die verschlüsselte Beantwortung herunterladen (siehe Schritt 5. in Abb. 1). Die Entschlüsselung erfolgt sodann im internen System der Behörden mit dem privaten Schlüssel des Anbieters, der zuvor über einen von der DLS unabhängigen Kanal ausgetauscht wurde.

Die Daten dürfen bis zur Einsicht des Behördenmitarbeiters von keinem Dritten eingesehen werden können. Das heißt es müssen Vorkehrungen getroffen werden, um den Zugang für Unbefugte zu verhindern. Die Durchlaufstelle muss technisch so abgesichert sein, dass es Dritten nicht möglich ist, Einsicht in die Daten zu erhalten. Weiters werden sämtliche Daten sofort nach Abholung oder (bei Nichtabholung) innerhalb eines vordefinierten Zeitraumes automatisch gelöscht. Der Zugang zu den

Daten durch Dritte kann so mit relativ geringem Aufwand technisch verhindert werden. Bei Abruf der Daten von der DLS durch die befugten Behördenmitarbeiter kann die behördeninterne Speicherung ohne großen Aufwand auf einem Teil des Datei- oder Datenbanksystems erfolgen, der durch entsprechende Zugangsberechtigungen gesichert ist.

III.1.5 PROTOKOLLIERUNG

Um eine sinnvolle Protokollierung zu erlangen muss diese lückenlos, einheitlich und revisionssicher sein. Dies ist vor allem für 2 Aspekte von hoher Bedeutung. Erstens zur Prävention von Missbrauch und nachträglicher Prüfbarkeit muss jeder Vorgang einer An- und Abfrage von Daten mit Referenzmaterialien (Geschäftszahl des Polizeiakts, Richterliche Bewilligung der StA-Anordnung, …) abgeglichen werden können. Zweitens um Missbrauchsfälle und Sicherheitslücken ausfindig machen zu können. Im Falle eines Missbrauches oder des Verlierens von Daten allgemein oder an bestimmte Dritte muss festgestellt werden können, bei welchem Verfahrensschritt dies passiert ist. Dazu ist ein lückenloses Protokoll unerlässlich.

Grundsätzlich findet die Protokollierung bei der DLS statt. Um aber eine ausreichende Protokollierung zu gewährleisten, ist zusätzlich zur Auskunftsdatei das Mitsenden einer Protokolldatei seitens des Anbieters notwendig. Wenn ein Anbieter Daten als Vorratsdaten bezeichnet, heißt dies, dass er die Daten für sonstige Zwecke nicht mehr benötigt. Ohne die Verpflichtung zur Vorratsdatenspeicherung wären sie daher gelöscht worden. Dies ist der Grund dafür, dass eine Protokollierung des Zugriffs auf Vorratsdaten vorgeschrieben ist. Es darf also gemäß TKG keinen Zugriff auf diese Daten ohne Auftrag geben. Diesem Zweck dient auch die Norm des § 102c Abs. 1 erster Satz TKG, wonach die Speicherung von Vorratsdaten so zu erfolgen hat, dass ihre Unterscheidung von „Billingdaten“ möglich ist. Das bedeutet zwar keine physisch, wohl aber logisch getrennte Speicherung (realisiert spätestens über die internen Zugriffssysteme). Um dies kontrollieren zu können, ist eine Art "doppelte Buchführung" vorgesehen. In der DLS werden die Aufträge protokolliert. Jeder Anbieter ist verpflichtet, eine revisionssichere Protokollierung des Zugriffs auf Vorratsdaten durchzuführen. Vergleicht man diese beiden Protokoll-Aufzeichnungen, so darf es keinen Unterschied geben. Das heißt andererseits, dass ein Anbieter den internen Zugriff auf Vorratsdaten nur dann erlauben darf, wenn ein entsprechender Auftrag einer anfrageberechtigten Stelle vorliegt.

„Revisionssicher“ bedeutet in diesem Zusammenhang, dass diejenigen, die auf die Daten zugreifen, nicht in der Lage sein dürfen, das Protokoll zu manipulieren. Es darf also niemanden in einem Unternehmen geben, der sowohl Zugriff auf Daten als auch Zugriff auf Protokolldaten hat. Üblicherweise sind die Zugriffsberechtigungen auf Daten in einem anderen Teil des Unternehmens angesiedelt als der Zugriff auf Protokolldaten.

Aus Sicht der Anbieter ist zu bedenken, dass die Grundgesamtheit aller Protokolldaten, die zur Erstellung der Statistik notwendig ist, auch wettbewerbsrelevant ist. Die Hitliste der meisten Datenauskünfte an die Polizei wäre vermutlich eine Schlagzeile, welche die Telekom-Branche eher vermeiden möchte. Insofern besteht bei den Anbietern selbst ein schutzwürdiges Geheimhaltungsinteresse, das über die DLS bereits technisch abgesichert werden sollte.

III.1.6 VERLAUF EINER DATENAUSKUNFT VIA DLS TECHNISCH/SCHEMATISCH

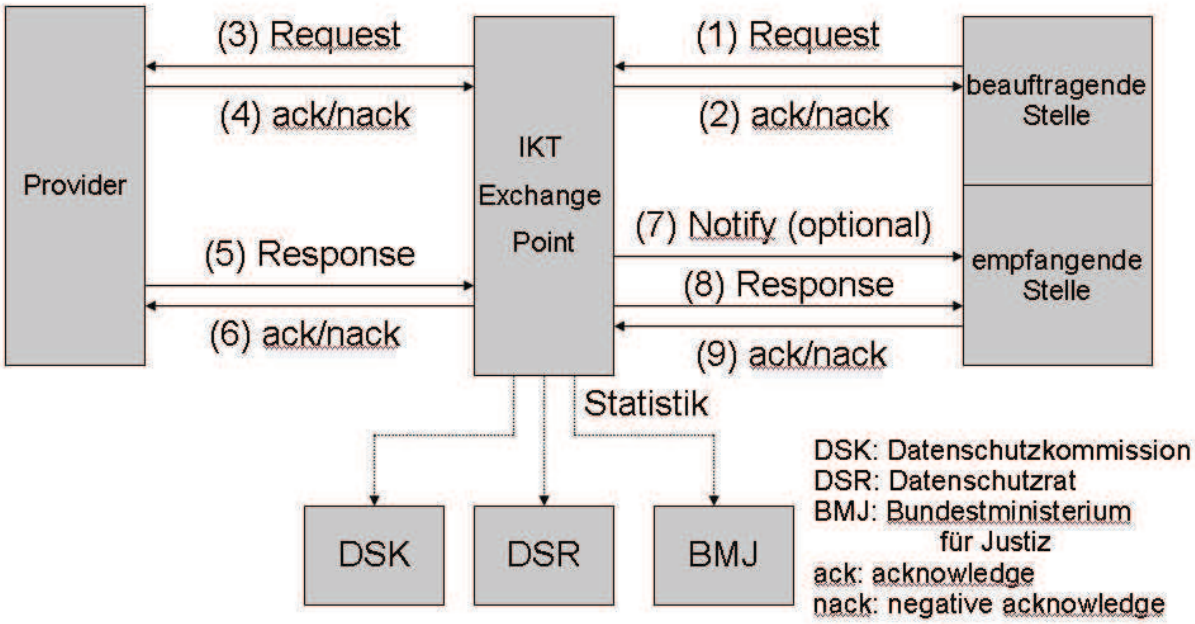

Abbildung 2: Schematische Darstellung des Systems der DLS im Flussdiagramm

Die Pfeile geben die Richtungen der Datenflüsse an. Die beauftragende und die empfangende Stelle müssen im Regelfall identisch sein.

„(1) Request“ enthält alle zur Durchführung des Auftrags notwendigen Daten und wird von der beauftragenden Stelle an die DLS übermittelt. Optional kann angegeben werden, ob und, wenn ja, wie die empfangende Stelle in Schritt „(7) Notify“ über das Eintreffen der Daten benachrichtigt werden möchte. Die DLS führt automatisierte Formalüberprüfungen aus.

„(2) ack/nack“, „(4) ack/nack“, „(5) ack/nack“ sowie „(10) ack/nack“ enthalten Bestätigungen der Übernahme der übermittelten Daten. „nack“ lehnt die Übernahme der Daten im Fehlerfall ab.

„(3) Request“ enthält die in (1) übermittelten Daten, abgesehen von den Daten zur Notifikation. Der angefragte Anbieter führt die formale, rechtliche und inhaltliche Prüfungen des Auftrags durch und erhebt die notwendigen Daten für die Auftragsbeantwortung sowie die Daten für Statistikzwecke.

„(5) Response“ enthält die Daten laut Auftrag und rechtlicher Zulässigkeit in verschlüsselter Form, so dass nur die empfangende Stelle die Daten entschlüsseln kann. Zusätzlich werden Daten für Statistikzwecke übertragen. Die DLS speichert die Daten für die empfangende Stelle zwischen und löscht sie nach Übermittlung oder nach einer zu definierenden maximalen Speicherdauer.

Mit „(7) Notify“ wird die empfangende Stelle über das Vorliegen der beauftragten Daten informiert.

„(8) Response“ enthält die in (5) übertragenen und für die empfangende Stelle bestimmten verschlüsselten Daten.

„Statistik“ überträgt die von den Anbietern in (5) übertragenen sowie von der DLS erhobenen Daten für die definierten statistischen Auswertungen gemäß §102c Abs. 2 bzw. Abs 3 TKG.

Sämtliche Daten werden auf Link-Ebene verschlüsselt, d.h. Daten werden ausschließlich verschlüsselt über Datenleitungen übertragen. Alle beteiligten Kommunikationspartner werden eindeutig identifiziert und authentifizieren sich gegenseitig.

Alle beteiligten Stellen protokollieren ein- und ausgehende Daten, um Nachweisen zu können, dass und wann Daten übermittelt und von der Gegenstelle angenommen wurden, und um ihren Verpflichtungen gemäß § 102c Abs. 2 TKG nachkommen zu können. Mit diesen Protokolldaten werden Nicht-Abstreitbarkeitsanforderungen erfüllt.

Notwendige Mechanismen zur Integritätsprüfung, zum Management kryptografischer Schlüssel sowie zum Übermitteln von Protokolldaten für Zwecke der Kontrolle des Datenschutzes und zur Gewährleistung der Datensicherheit gemäß §102c Abs. 4 TKG sind nicht Teil des Schaubilds zum Datenfluss.

III.1.7 KONFIGURATION DER ANFRAGEMASKE

Die DLS soll die Drehscheibe zur Kommunikation für alle Auskunftsfälle sein. Kern ist dabei, dass die jeweilige Seite ihre Anforderung/Antwort sicher über die DLS samt dem notwendigen Anhang (Betreiber-Anordnung nach § 139 Abs. 3 StPO, CSV-Datei mit den begehrten Daten) übermittelt.

Für Anfragen nach dem SPG ist schon bisher eine Verwendung von normierten Formularen gemäß verwaltungsinternem Erlass des BIM vorgesehen. Bei Anfragen nach der StPO gibt es zwar Formulare, denen jedoch kein justizintern zwingender Erlass zugrunde liegt und die in der Praxis auch nicht durchgehend verwendet werden. Anfragen nach der StPO enthalten als Beilage die Anordnung des Staatsanwalts mit der prosaischen Beschreibung des Auskunftsbegehrens. Die Spezifikation der DLS muss aber nicht enthalten, wie auf Seiten der Behörden die jeweiligen Web-Formulare aussehen. Eine Formalisierung wird jedoch auf Behördenseite aus eigenem Interesse einer einheitlichen und geordneten Abwicklung angestrebt.

Auch auf der Seite der Anbieter muss nicht spezifiziert werden, ob, inwieweit und wie die Beantwortung von Auskunftsbegehren (teil-)automatisiert wird. Durch die EP020[273] wird einheitlich festgelegt, wie die CSV-Datei aussehen muss. Wie die einzelnen Anbieter diese Datei „befüllen“ bleibt deren Entscheidung.

Bei der Übermittlung eines Auskunftsbegehrens via DLS muss jedoch ausgewählt werden, auf welcher Rechtsgrundlage die Anordnung ergeht. Dies dient der statistischen Erfassung über die DLS und beinhaltet keine Determinierung der Formulare oder Webmasken, die bei den Behörden für die Anordnungen verwendet werden. Eine Determinierung ergibt sich allerdings aus der Spezifikation der Felder der CSV-Datei gemäß der EP020, die als integraler Bestandteil in den Begutachtungsentwurf zur Datensicherheitsverordnung übernommen wurde. Die technische Definition der Datenfelder der CSV-Datei orientierte sich streng an den gesetzlich zulässigen Fällen.

[273] Siehe oben Kapitel II.3.2.1 zur EP020.

Daraus ergibt sich, welche Informationen dem Anbieter als Suchkriterien zur Verfügung stehen können und welche Daten darauf basierend ausgewertet werden und als Antwort übermittelt werden können. Damit sind die gesetzlich zulässigen Anwendungsfälle (Use-Cases) auch auf der technischen Ebene fixiert. Diese Einschränkungen müssen natürlich auch bei der Gestaltung allfälliger elektronischer Abfragemasken berücksichtigt werden.

III.2 KONZEPTE IM VERGLEICH (DURCHLAUFSTELLE (DLS) VS. S/MIME)

III.2.1 EINLEITUNG

Der ursprüngliche Begutachtungsentwurf zur TKG Novelle zur Umsetzung der Vorratsdatenspeicherung in der Fassung des BIM-Entwurfes[274] sah in § 94 Abs. 4 TKG explizit vor, dass die Übermittlung der Daten durch verschlüsselte E-Mail unter Verwendung des S/MIME Standards erfolgen soll. Im Zuge der finalen Umsetzungsdiskussionen zur TKG-Novelle im Jänner und Februar 2011 waren auch die Diskussionen zur Datensicherheit im Rahmen der BIM-Datensicherheitsstudie soweit gediehen, dass die Vorgaben zur sicheren Datenübermittlung schon in der endgültigen Regierungsvorlage und schließlich in der gesetzlich verabschiedeten Version durch eine flexiblere und technologieneutrale Formulierung ersetzt wurden. § 94 Abs. 4 TKG lautet daher nunmehr in der geltenden Fassung: „Die Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, einschließlich der Übermittlung von Vorratsdaten, nach den Bestimmungen der StPO sowie des SPG, hat unter Verwendung einer Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt, zu erfolgen. Die Daten sind unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie als “Comma-Separated Value (CSV)“ - Dateiformat zu übermitteln.“

Im Zuge des 1. und des 2. Round Tables im Rahmen der BIM-Datensicherheitsstudie[275] wurden unterschiedlichen Konzepte vorgestellt und eine Abschätzung und Abwägung der Vor- und Nachteile erläutert. Behandelt wurden zwei Grundkonzepte mit unterschiedlichen Ausführungen, welche an Aufwand und Sicherheit in einigen Aspekten stark variieren.

1. Übergabe und Anfrage via verschlüsselter Email (in weiterer Folge kurz: S/MIME[276])

2. Übergabe und Anfrage via zentraler Durchlaufstelle (in weiterer Folge kurz: DLS)

Dieser nachfolgend abgehandelte Vergleich soll auf der theoretischen Ebene zeigen, welche für die Datensicherheit wesentlichen Aspekte zu berücksichtigen sind und wie diese optimiert werden können. In der praktischen Diskussion hat er den wesentlichen Grundstein dafür gelegt, dass die praktischen Umsetzungsmöglichkeiten des Systems der DLS in der Folge bis zum 6.

[274] BIM-Entwurf TKG Novelle 2010, Fundstelle siehe Literaturverzeichnis.
[275] Zur Methode und Zusammensetzung der insgesamt 6 Round Table Diskussionen im Rahmen der BIM-Datensicherheitsstudie siehe unten Kapitel IV.1.
[276] Details zu diesem Standard nachlesbar zB auf der Website des „Zentrum für sichere Informationstechnologie–Austria“: http://www.a-sit.at/de/dokumente_publikationen/flyer/email_sicherheit.php.

Round Table ernsthaft und intensiv diskutiert wurden und schließlich die DLS von allen Beteiligten als das bevorzugte Modell angesehen wurde.

III.2.2 Notwendige Technische Voraussetzungen

III.2.2.1 Identifikation und Authentifizierung

Um sicherzustellen, dass ein Kommunikationspartner auch die Berechtigung zu einer Anfrage/Auskunft hat, muss sich dieser über den elektronischen Weg auch eindeutig identifizieren und authentifiziert können. Das heißt, dass im Vorfeld schon zwischen den Kommunikationspartnern ein Weg zu finden ist, um den anderen auch sicher zu erkennen.

III.2.2.1.1 S/MIME

Im Falle von S/MIME funktioniert dies über eine sogenannte qualifizierte Signatur

a. Über Drittanbieter: Sämtliche beteiligten Kommunikationspartner vereinbaren mit einer zentralen Stelle eine eindeutige Signatur. Wird nun eine Mail mit Signatur versendet, so wird vom Empfänger bei dieser Stelle angefragt, ob der Sender vertrauenswürdig ist und auch der ist, der er zu sein vorgibt. Bei Änderungen bei den Behörden oder den Anbietern muss die Vertrauensstellung nur einmal (mit dem Drittanbieter) neu ausgehandelt werden. Nachteil dabei ist, dass „ein Dritter“ mit einbezogen werden muss, dadurch entstehen zusätzliche Kommunikationswege, welche in Folge auch zusätzliche Angriffspunkte bezüglich IT-Sicherheit bedeuten.

b. Bilateral: Es muss im Vorfeld eine Signatur zwischen den Kommunikationspartnern selbst kommuniziert werden, um die Vertrauensstellung während des Emailverkehres sicherzustellen. Die Signaturen müssen zwischen allen Partnern einzeln ausgehandelt werden, was einen massiven (n x m) Mehraufwand bedeutet. Bei einer Änderung müssen die Signaturen mit allen Kommunikationspartner erneuert werden. Bezüglich Datensicherheit ist dieser Weg im Normalfall relativ sicher. Bei Änderungen auf Seiten der Kommunikationspartner können allerdings massive Sicherheitsprobleme auftraten, da „tote Signaturen“ länger im Umlauf sein können und dadurch auch länger einem potentiellen Missbrauch ausgesetzt sind.

III.2.2.1.2 DLS

Bei der DLS wird die gesamte Identifikation und Authentifizierung zentral verwaltet. Dies geschieht hier über das Anmelden an den Server mittels Benutzername und Passwort (und allenfalls einer persönlichen ID). Sobald sich also ein Teilnehmer bei dem Server anmeldet, kann (eine sichere IT-Umgebung vorausgesetzt) der Kommunikationspartner davon ausgehen, dass schon im Vorfeld die Authentifizierung sichergestellt ist.

a. Mit eigener Benutzerverwaltung: Die Verwaltung muss von einer unabhängigen Stelle organisiert und durchgeführt werden, was einen finanziellen Aufwand bedeutet, der mit dem (n x m) Aufwand zum Signaturaustausch im SMIME Konzept zu vergleichen ist.

b. Mit Anbindung über den Portalverbund: Es wird eine schon vorhandene Benutzerstruktur seitens der Behörden verwendet (siehe unten S 9). Der Mehraufwand zur Wartung der Benutzerstruktur ist stark vermindert, da bzgl. Authentifizierung der Behörden auf vorhandene Strukturen zurückgegriffen wird.

III.2.2.2 VERSCHLÜSSELUNG

Um die Daten während der Kommunikation (Übertragungsweg + „Zwischenlagerung" bis zur Verwendung) ausreichend vor Dritten zu schützen, müssen die angefragten Daten sowie die Anfrage selbst verschlüsselt werden. Die Schlüssel müssen schon im Vorfeld zwischen den Kommunikationspartnern vereinbart werden.

III.2.2.2.1 VERSCHLÜSSELUNG DER DATEN

III.2.2.2.1.1 S/MIME

Sämtliche Schlüssel müssen bei jedem Kommunikationspartner vorliegen. Das heißt:

1. Im Falle einer Änderung müssen die betroffenen Schlüssel überall geändert werden, was einen hohen Wartungsaufwand mit sich bringt und wiederum die Gefahr erhöht, dass in einer Übergangsphase „tote Schlüssel" verwendet werden können.

2. Sämtliche Schlüssel sind vielfach abgespeichert, was auch ein erhöhtes Sicherheitsrisiko (bezüglich Erlangen der Schlüssel von Unbefugten) mit sich bringt.

Außerdem muss die Verschlüsselung der Daten selbst vom Anwender bewusst (quasi „manuell") angewendet werden, was einen erhöhten Anwendungsaufwand bedeutet. **Wichtig ist** hier festzuhalten, dass der S/MIME Standard lediglich eine Verschlüsselung auf dem Übertragungsweg beinhaltet. Das bedeutet dass die Daten im Post-Ausgang der E-Mail Anwendungen („gesendete Objekte") sowie im Backup-System des jeweiligen E-Mail Servers unverschlüsselt vorliegen. Um den unionsrechtlichen Datensicherheitsvorschriften zu entsprechen muss sichergestellt werden, dass die zur Übertragung genutzte E-Mail nach jeder Übertragung aus der E-Mail Anwendung tatsächlich gelöscht wird (also auch aus den „gelöschten Objekten"). Ohne Automatisierung lässt sich das praktisch nicht gewährleisten, wie eine solche bei gängigen E-Mail Klients implementiert werden soll, ist fraglich.

III.2.2.2.1.2 DLS

Die Schlüsselverwaltung erfolgt vereinfacht dargestellt zentral. Dadurch ergibt sich der Vorteil, dass diese im Wartungsfall unverzüglich (keine toten Schlüssel) und mit geringem Aufwand geändert

werden können. Gleichzeitig kann über die DLS eine sichere Public Key Infrastruktur realisiert werden, was die Datensicherheit enorm erhöht.

III.2.2.2.2 Verschlüsselung des Kommunikationsweges

Abseits der Verschlüsselung der Daten selbst muss auch die Übertragung der Daten und Informationen in beide Richtungen verschlüsselt werden.

III.2.2.2.2.1 S/MIME

Die Mailübertragung selbst muss verschlüsselt werden. Dem E-Mail Protokoll SMTP ist inhärent, dass die Priorität die Übermittlung ist, die Sicherheitselemente des S/MIME Standards sind plastisch formuliert nur Zubauten. Das heißt nach den gängigen Methoden, wenn sich die beteiligten Server nicht automatisch binnen kurzer Zeit auf einen Schlüssel einigen können, wird die Nachricht unverschlüsselt übermittelt. Um diesem – in der technischen Natur des Mediums E-Mail gelegenen – Problem zu begegnen, müssen sämtliche Server aller Kommunikationspartner vorkonfiguriert werden. Dadurch entsteht ein außerordentlich hoher Aufwand bei der Implementierung und ein ebenso beträchtlicher Aufwand bei Änderungen (n x m – Problem)

III.2.2.2.2.2 DLS

Die Kommunikation zwischen DLS und Kommunikationspartnern funktioniert via https oder ähnlichen verschlüsselten Verbindungen. Solche Verbindungen können mit allen gängigen Anwendungen (Internet Explorer®, Firefox®, …) ohne Vorkonfiguration oder Wartung verwendet werden und sind ausreichend sicher.

Sämtliche Benachrichtigungen, welche von der DLS automatisch verschickt werden (Neuzugang im Postfach, anliegende Anfrage, …) beinhalten keine sicherheitsrelevanten Informationen mehr und können unverschlüsselt übertragen werden.

III.2.2.3 Protokollierung

III.2.2.3.1 S/MIME

Bei diesem Verfahren ist der Großteil der Protokollierung manuell zu erledigen. Das heißt, eine lückenlose revisionssichere Protokollierung ist gerade im Missbrauchsfall kaum gegeben. Eine einheitliche und revisionssichere Protokollierung bei diesem Verfahren zu gewährleisten ist - wenn überhaupt - nur mit hohem Aufwand erreichbar. Die dem Anbieter für interne Zugriffe vorgeschriebene revisionssichere Protokollierung kann nämlich nicht automatisch erfassen, wann, von wem und wofür die Auskunft begehrt wurde, ebenso wenig, wann und an wen die Übermittlung der Daten tatsächlich erfolgte und schließlich ob die Daten tatsächlich bei der richtigen Stelle angekommen sind. Um die entsprechenden Einträge bei der internen Protokollierung im Fall einer Kontrolle rechtfertigen zu können, muss der Anbieter die E-Mails zu Anfrage, Auskunft und

Empfangsbestätigung aufbewahren und dem jeweiligen Auskunftsfall systematisch zuordnen können.

Wenn ein Problem auftritt, oder eine Abfolge überprüft werden soll, so ist dies also mit sehr hohem Aufwand verbunden, da sämtliche Protokolle aller Kommunikationsteilnehmer zusammengetragen (wider unter erhöhtem und kompliziertem Vorgang, da die Übermittlung der Protokolle ebenfalls gesichert von statten gehen muss), vereinheitlicht und erst manuell auf Konsistenz überprüft werden müssen.

III.2.2.3.2 DLS

Hier ist der gesamte Ablauf vom Auskunftsbegehren bis zur Abholung der Daten lückenlos, automatisiert und revisionssicher protokolliert und zentral ohne sicherheitstechnischen Mehraufwand abrufbar. Darüber hinaus wäre ohne besondere Schwierigkeit möglich, die Art der aus den Protokolldaten gewünschten Informationen je nach dem intendierten Bestimmungszweck und Empfängerkreis vorab zu konfigurieren und die Auswertung zu automatisieren. ZB unterscheidet sich der Informationsgehalt für die Statistik, die der EU-Kommission jährlich vorzulegen ist, deutlich von den Anforderungen, die etwa die DSK für die Beurteilung eines Auskunftsbegehrens nach § 26 DSG benötigt. Während letztere einen Personenbezug notwendigerweise erfordern, haben diese Informationen in der Statistik nichts verloren. Die Rechtsschutzbeauftragten sind wiederum nur an einem bestimmten Ausschnitt aus der Gesamtmenge aller Auskunftsfälle interessiert, je nach den in ihren Zuständigkeitsbereich fallenden Rechtsgrundlagen. Durch die automatische und lückenlose Protokollierung über die DLS könnten diese Anforderungen einmalig maßgeschneidert implementiert werden, die Auswertungen würden dann je nach Anforderung bzw. Berechtigung auf Knopfdruck erfolgen. Der operative Aufwand wäre damit verschwindend gering und muss bei einer Beurteilung der Kosten dem anfänglichen Implementierungsaufwand gegenüber gestellt werden.

III.2.3 Ablauf eines Auskunftsbegehrens

Eine Anfrage muss eindeutig formuliert sein, um die Rechtsgrundlage(n) zum Auskunftsbegehren zweifellos ersichtlich zu machen.

III.2.3.1 S/MIME

Hier muss das gesamte Auskunftsbegehren in einer Email so formuliert werden, damit sämtliche Rechtsgrundlagen ersichtlich und überschießende oder fehlerhafte Auskünfte vermieden werden. Der (im StPO Bereich von der StA) beauftragte Mitarbeiter der Behörde muss dies formulieren, was einen erhöhten Aufwand erfordert, einschlägige Rechtskenntnisse müssen vorausgesetzt werden. In der Praxis wird dies ohne die Verwendung von Formularen schwer zu bewältigen sein. Solche Formulare sollten benutzerfreundlich, zugänglich und obligatorisch sein. Die Verbreitung muss beim S/MIME Konzept im Dienstweg erfolgen und entsprechend kommuniziert werden.

III.2.3.2 DLS

Durch eine vorgefertigte Eingabemaske ist ein missverständliches oder überschießendes Auskunftsbegehren ausgeschlossen. Eine Verteilung von Formularen ist nicht notwendig, die elektronischen Eingabemasken können von vornherein benutzerfreundlich gestaltet werden. Die Fehleranfälligkeit lässt sich dadurch auf ein Minimum reduzieren. Der Vorgang der Anfrage wird dadurch stark vereinfacht und spart sowohl bei den Behörden als auch bei den Anbietern Zeit und Ressourcen.

III.2.4 Empfang der Daten

Die Daten dürfen bis zur Einsicht des Behördenmitarbeiters von keinem Dritten eingesehen werden können. Das heißt es müssen Vorkehrungen getroffen werden, um den Zugang für Unbefugte zu verhindern.

III.2.4.1 S/MIME

Da die Daten hier als Mail im Posteingang eines Behördenmitarbeiters landen, ist dies nach der Eingabe des Schlüssels nur unter einem sehr hohem Aufwand an Sicherheitsvorkehrungen inklusive massiven Sicherheitsvorschriften in den einzelnen Büros möglich. Es müssten einerseits sämtliche Rechner bei den Auskunftsberechtigten Behörden erhöhten Sicherheitsstandards angepasst werden, um sie gegen Angriffe zu schützen und in den Büros muss sichergestellt werden, dass der Zugang zu den Rechnern, auf denen Auskünfte gespeichert werden, nur den befugten Organwaltern möglich ist. Diese Sicherheitsmaßnahmen sind mit beträchtlichem Aufwand verbunden.

III.2.4.2 DLS

Die Durchlaufstelle ist technisch schon so konfiguriert, dass es Dritten unmöglich ist, Einsicht in die Daten zu erhalten. Weiter werden sämtliche Daten sofort nach Abholung oder (bei Nichtabholung) innerhalb eines vordefinierten Zeitraumes automatisch gelöscht. Der Zugang zu den Daten durch Dritte ist also mit geringem Aufwand technisch unterbunden. Bei Abruf der Daten von der DLS durch die befugten Behördenmitarbeiter kann die behördeninterne Speicherung ohne großen Aufwand auf einem Teil des Datei- oder Datenbanksystems erfolgen, der durch entsprechende Zugangsberechtigungen gesichert ist.

III.3 Bewertung des Vergleichs - Operative Vorteile der DLS

III.3.1 Seitens der Sicherheitsbehörden

Vorteil der DLS ist die Reduktion der Kommunikationswege zwischen den abfragenden Stellen und den Netzanbietern (*n x m Problem*). Alle in der DLS zentral und automatisiert laufende Prozesse müssen derzeit zwischen *n* Behörden und *m* Anbietern ebenfalls ablaufen. Weiters stellt die Durchlaufstelle die zentrale Verfügbarkeit von Protokolldaten sicher, welche ansonsten einmal jährlich zur Berichterstattung an die EU-Kommission (wahrscheinlich durch das BMJ) bei allen Anbietern eingesammelt und einheitlich zusammengeführt werden müssten.

Die Anfrageprozedere wird enorm vereinfacht und beschleunigt. Es gibt eine zentrale Anlaufstelle für Anfragen. Dabei ist gewährleistet, dass die Anfrage beim Anbieter richtig und rasch zugestellt wird, wobei bei der anfragenden Stelle nicht jedes Mal der Aufwand entsteht, die richtigen und aktuellen Kontaktdaten des Anbieters auszuforschen. Durch die Formalisierung der Anfrageprozedur über die DLS werden Rückfragen sehr wahrscheinlich seltener. Auch die richtige Zustellung der Antwort an die richtige Einheit wird über die DLS durch Verknüpfung über die Uniqu-ID gewährleistet, dass eine Auskunft „verlorengeht“ ist technische äußerst unwahrscheinlich.

Die Abwicklung der Anfragen und Auskünfte könnte über die DLS erleichtert werden, insbesondere die Einbindung über den Portalverbund würde Synergie-Effekte bringen, weil damit auf Seiten des BMI bereits gute Erfahrungen bestehen. Ein Anreiz wäre jedenfalls, dass damit eine Drehscheibe zum sicheren Austausch von Informationen mit allen Anbietern bestünde, die auch über den Bereich von Verkehrsdatenauskünften genutzt werden könnte. Angesprochen ist vor allem die Möglichkeit einer elektronischen Stammdatenauskunft im Bereich der Telefon-Anbieter. Festgehalten wird, dass es für das BM.I nicht darum geht, eine unmittelbare Schnittstelle zur Kundendatenbank des Anbieters herzustellen. Vielmehr besteht der Wunsch, es soll einen elektronischen Hin- und Rückkanal geben, der zu einer möglichst raschen Abwicklung führt. In wie weit ein Anbieter solche Auskunftsvorgänge automatisiert, soll dem jeweiligen Anbieter überlassen bleiben - insbesondere im Hinblick auf kleine Anbieter, die nur wenig betroffen sind - solange die Auskunft in vertretbarer Zeit abgewickelt werden kann. Große Anbieter könnten durch eine (Teil-)Automatisierung in eigener Verantwortung die Auskünfte optimieren. Weiters wird eingeräumt, dass eine Anbindung an ein elektronisches System für Stammdatenauskünfte über die DLS nicht gesetzlich verpflichtend als ausschließliche Übermittlungsvariante für alle Anbieter eingerichtet werden müsste. Per Gesetz und/oder Verordnung soll die Möglichkeit einer solchen Anbindung normiert werden. Wenn zumindest die großen (insbesondere Mobilfunk-) Anbieter sich anschließen, würde der Zweck erfüllt.[277]

Durch stärkere Automatisierung und die zentrale Kommunikation über die DLS wird bei den Auskunftsbegehren von Seiten des Bundeskriminalamts eine Aufwandsersparnis erwartet. Die größte Aufwandsreduzierung besteht vor allem darin, dass im Vergleich zur S/MIME - Variante die laufende Erneuerung der Sicherheitszertifikate zentral erfolgt und damit massiv erleichtert wird. Die Erfahrung

[277] BIM-Datensicherheitsstudie S. 100.

aus der Europol Kooperation zeigt, dass dies bei einer dezentralen sicheren Kommunikation zwischen vielen Stellen ein enormer Aufwands- und damit Kostensteigerungsfaktor ist.[278]

Größter operativer Vorteil ist, dass das Anfrageprozedere enorm vereinfacht und beschleunigt wird., da es gibt eine zentrale Anlaufstelle für Anfragen.[279]

III.3.2 Seitens der Datenschutzkommission/des Rechtsschutzbeauftragten

Die Protokollierung erfolgt direkt bei der DLS selbst. Sämtliche Protokolle können folglich über eine entsprechende Eingabemaske abgefragt werden. Die Protokollierung bei der DLS ist nur indirekt personenbezogen, die Protokolldaten enthalten keine Informationen, welche Teilnehmer von der Auskunft betroffen sind. Für diese Information muss die DSK bzw. der RSB direkt auf Seiten der Behörden entsprechend den jeweiligen gesetzlichen Befugnissen Auskünfte einholen bzw. Akteneinsicht nehmen. Über die Verknüpfung mit der Uniqu-ID lässt sich aber der Verlauf einer Auskunft von der Anfrage bis zur Zustellung der Antwort lückenlos nachvollziehen. Die DSK kann im Falle eines datenschutzrechtlichen Auskunftsbegehrens gemäß § 26 DSG auch auf Seiten der Anbieter die interne Protokollierung einsehen, wobei auch hier durch Verknüpfung über die Uniqu-ID die Nachverfolgung des Auskunftsvorganges deutlich erleichtert ist.

Für den RSB hat die Protokollierung in der DLS einen weiteren Vorteil, weil er die Zahl der gemäß § 91c Abs. 1 SPG gemeldeten Datenauskünfte mit den tatsächlich über die DLS abgewickelten Auskünfte vergleichen kann. Die statistischen Werte, zB wie viele Datensätze von welcher Datenkategorie in einer Antwort enthalten waren, können dem RSB Anhaltspunkte für eine Stichprobenkontrolle geben. Die lückenlose Nachvollziehbarkeit des gesamten Auskunftsvorganges erleichtert die Kontrolltätigkeit auch im Einzelfall. Mittelfristig sollte damit jedenfalls die Meldedisziplin der Beamten gestärkt werden.

III.3.3 Seitens der Anbieter

Für die Anbieter würde die DLS einen geringeren Implementierungsaufwand als der Aufbau direkter Kommunikationswege zu allen auskunftsberechtigten Stellen bedeuten. Hervorgehoben wird, dass das vorgestellte Konzept aber zentral die Frage der Datensicherheit betrifft: „Wie kommen die Daten sicher an Ihren Bestimmungsort?“ [280]

Ein weiterer Vorteil liegt in der teilweisen Auslagerung der standardisierten Protokollierung. Gleichzeitig entstehen im System der DLS weniger technische Vorgaben zur Realisierung der Abfrage, standardisiert sind lediglich der Anfragecode und das Ausgabeformat, definiert nach der Technischen Richtlinie. Die Entscheidung über die Herausgabe der Daten liegt trotz hohem Automatisierungsgrad immer noch beim Anbieter. Es gibt eine zentrale Stelle zur Übermittlung der Auskünfte. Die Verifizierung des Anfragestellers ist seitens der Anbieter nicht mehr notwendig, weil diese Aufgabe von der DLS übernommen wird.

---

[278] Ibid, S. 108.
[279] Ibid, S. 61.
[280] Ibid, S. 89.

III.3.4 Argument bzgl. Internationale Kooperation

Erweiterungen sind durch die zentrale Administration leicht möglich. D.h. auch ohne Realisierung der ETSI-Schnittstelle zur Data Retention könnte eine europaweite Kooperation gewährleistet werden. Durch die gesetzliche Determinierung, dass das Format der Datenübermittlung immer CSV sein muss, und die Datenausgabe immer als Push gestaltet ist, sollte vorgebeugt sein, dass die Behörden keine unmittelbaren Zugriffe auf die Datenbanksysteme der Anbieter durch normierte Schnittstellen bekommen.

III.3.5 Seitens der Richter/Staatsanwälte

Keine nachteiligen Änderung zum Status quo, sofern der Staatsanwaltschaft eine eigene Mailbox zur Verfügung gestellt wird.

III.3.6 Spätere technische oder gesetzliche Änderungen

Durch die zentrale Realisierung der Abfrage durch eine Eingabemaske ist die Abfrage bei entsprechenden gesetzlichen Änderungen auch technisch relativ einfach einschränkbar oder erweiterbar. Nach der Grundkonzeption sollen so auch die Use-Cases wirksam auf die gesetzlich zulässigen Fälle eingeschränkt werden.

III.3.7 Resümee

Die Implementierung der S/MIME Methode erscheint zunächst weniger aufwändig, da jedenfalls keine zusätzliche IT-Umgebung (Hardware) nötig ist. Nicht ersparen lässt sich jedoch auch nach diesem Konzept die Implementierung gewisser Softwareanforderungen, denn eine Publik-Key-Infrastruktur zur zuverlässigen Authentifizierung ist auch hier notwendig. Dieser Aufwand ist – zwar nicht bzgl. der Programmierung aber operativ - im Vergleich zur DLS sogar höher, weil die Kommunikation ja zwischen (angenommen) 15 behördlichen Stellen und 200 Anbietern erfolgen muss (n x m – Problem).

Schließlich würde die Ausarbeitung und Verbreitung von benutzerfreundlichen Formularen entsprechend der neuen Rechtslage nach der TKG-Novelle einen Aufwand darstellen, der verglichen mit der einmaligen Einrichtung von Abfragemasken nicht geringer aber weniger effektiv sein wird. Dabei ist das S/MIME Konzept, um eine ausreichende Sicherheit zu gewährleisten, sehr wartungsanfällig (was passiert mit den Daten, wenn eine E-Mail nicht zustellbar ist?) und kann trotz höherem laufendem Aufwand nicht den Sicherheitsstandard der DLS erlangen.

Um die DLS zu realisieren, bedarf es zu Beginn eines höheren Aufwands für die erstmalige Einrichtung der Software-Anwendung. Allerdings würden die laufenden Kosten sowohl auf Behörden- als auch auf Anbieterseite sinken. Ein Betrieb im Rahmen des Portalverbunds beim BRZ könnte diese Wirkung optimieren.

Die Wartungskosten könnten auf ein Minimum gesenkt werden, weil die wichtigsten Anwendungselemente nicht bei 200 Anbietern sondern zentral bei einer Stelle „gehostet“ werden. Schließlich wird der Ablauf eines Auskunftsbegehrens für alle Beteiligten sehr stark vereinfacht, was sich im Zeitaufwand und somit auch in den Bearbeitungskosten positiv niederschlägt. Die Protokollierung könnte zuverlässig und mit deutlich geringerem Aufwand erfolgen – allein schon bezogen auf das unionsrechtlich geforderte und daher unabdingbare Ausmaß für die Statistik. Darüber hinaus könnte die Protokollierung ohne Mehraufwand für die verschiedenen Rechtsschutzzwecke (DSK, RSB) optimiert werden und auch diese Organe operativ entlasten.

E-Mail bietet eine weniger standardisierte Lösung. Die Antworten hängen von der Implementierung des E-Mail Servers ab. Es kann zu Fehlermeldungen kommen wie z.B. Mailbox voll, Adressat out-of-office, generelles Zurückweisen der E-Mail (*bounce*). Aus technisch-wissenschaftlicher Sicht wird E-Mail (S-MIME) nicht als optimale Lösung für die Implementierung einer transaktionalen Schnittstelle gesehen. Es ist zwar theoretisch möglich, auch mit S/MIME eine ausreichende Sicherheit zu erzielen. Damit erhöht sich allerdings dann der Aufwand in der Umsetzung deutlich, weil man für die S/MIME Variante „Zubauten“ vor allem im Bereich der Authentifizierung benötigen würde, die der Standard grundsätzlich nicht enthält.[281]

Das Konzept der DLS ist zuverlässiger und sicherer als die Übertragung per S/MIME. Die Implementierung eines einheitlichen Prozesses – wie es bei der DLS der Fall ist – vermindert das Fehler- und das Sicherheitsrisiko.[282] Große Vorteile für die Datensicherheit und Synergieeffekte bewirkt zudem die Einbindung der DLS als Anwendung in den Portalverbund des Bundes im Hinblick auf sichere Identifikation, Authentifizierung sowie der sicheren verschlüsselten Übermittlung von personenbezogenen Daten.

[281] Ibid, S. 98 f.
[282] Ibid, S. 95.

III.4 Zusammenfassende tabellarische Gegenüberstellung DLS - S/MIME

Identifikation und Authentifizierung				
	S/MIME (über Dritte)	S/MIME (Bilateral)	DLS (eigene Benutzerverwaltung)	DLS (mit Portalverbund)
Implementierungsaufwand	Mittel	Hoch	Hoch	Hoch
Wartungsaufwand	Mittel	Hoch	Mittel	Gering
Anwendungsaufwand	Gering	Gering	Gering	Gering
Sicherheit	Ausreichend	Ausreichend	Sehr gut	Sehr gut

Verschlüsselung (Daten)		
	S/MIME	DLS
Implementierungsaufwand	Hoch	Hoch
Wartungsaufwand	Hoch	Gering
Anwendungsaufwand	Mittel	Gering
Sicherheit	Ausreichend	Sehr gut

Verschlüsselung (Verbindung)		
	S/MIME	DLS
Implementierungsaufwand	Hoch	Hoch
Wartungsaufwand	Hoch	Gering
Anwendungsaufwand	Gering	Gering
Sicherheit	Sehr gut	Sehr gut

Protokollierung		
	S/MIME	DLS
Implementierungsaufwand	Hoch	Hoch
Wartungsaufwand	Hoch	Gering
Anwendungsaufwand	Hoch	Gering
Sicherheit	Unzureichend	Sehr gut

Workflow Auskunftsbegehren		
	S/MIME	DLS
Anwendungsaufwand	Mittel	Gering
Sicherheit	Mittel	Sehr gut

Empfang der Daten		
	S/MIME	DLS
Implementierungsaufwand	Hoch	Gering
Anwendungsaufwand	Gering	Gering
Sicherheit	Unzureichend	Sehr gut

IV Wesentliche Problemkreise und Fragestellungen für die Praxis

IV.1 Hintergrund zur Erhebung der in der Praxis wesentlichen Fragen

Der Zusammenhang zwischen dieser Arbeit und der BIM-Studie zur Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung wurde bereits einleitend in Kapitel I.1. dargestellt. Im Rahmen dieser Studie führte der Autor dieser Dissertation als Studienautor und wissenschaftlicher Mitarbeiter des Ludwig Boltzmann Institut für Menschenrechte (BIM) zur Erhebung der praktisch bedeutsamsten Fragestellungen zur Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung von November 2010 bis Juni 2011 insgesamt Fünfzehn Diskussionsveranstaltungen mit den Stakeholdern durch, die am Austausch von Vorratsdaten nach der gesetzlichen Umsetzung der Richtlinie in Österreich beteiligt sind. Da hier eine relativ neue und technisch komplexe Thematik diskutiert wurde, war es notwendig, einerseits sachlich möglichst alle Betroffenen einzubinden, und andererseits fachlich eine ausreichende Durchmischung von rechtlicher und technischer Expertise zu erreichen. Sehr viele Fragen waren auf technischer Ebene mit den unmittelbar Betroffenen, und hier vor allem mit den Internet- und Telekommunikationsanbietern zu erschließen. Der methodische Ansatz im Rahmen der Ausarbeitung der Studie bildete dabei zwei unterschiedliche Kommunikationsstränge und vernetzte diese miteinander. Die Diskussionsrunden teilten sich daher in Neun Arbeitsgruppentreffen mit der Internet- und Telekomwirtschaft im Rahmen des „Arbeitskreis Telekommunikation“ (AK-TK)[283] und Sechs Round Table Diskussionen, an denen sämtliche Stakeholder beteiligt waren.

Eingeladen zu diesen Round Table Diskussionen waren Vertreter der Telekom-Branche sowie der zugehörigen Interessenvertretungen (WKO, ISPA) sowie Vertreter aller staatlichen Stellen, die im Zusammenhang mit der Umsetzung der Vorratsdatenspeicherung und der operativen Abwicklung von Auskunftsbegehren bezüglich dieser Daten Aufgaben zu erfüllen haben. Konkret betrifft dies die Ministerien BMVIT, BMJ, BM.I und BMF, den Verfassungsdienst des Bundeskanzleramts, das Bundeskriminalamt, die Rechtsschutzbeauftragten der Justiz und des Innenministeriums, die Datenschutzkommission, die Vereinigung österreichischer Richterinnen und Staatsanwältinnen und das Bundesrechenzentrum. Schließlich wurden auch regelmäßig Experten zur Datensicherheit der Technischen Universität Wien hinzugezogen.

Die Round Table Diskussionen hatten zum Ziel, die Möglichkeiten für die Umsetzung eines sicheren Konzepts zur bestmöglichen Wahrung grundrechtlich geschützter Interessen bei gleichzeitig ökonomischer Gestaltung der Verfahrensabläufe auszuloten, alle wesentlichen Fragen zu erheben und zu diskutieren sowie praktikable und zugleich hohe Datensicherheitsstandards auf der Basis eines möglichst breiten Konsens zu beschreiben. Als Referenzmodell für die Diskussionen wurde dabei zuvor das Konzept für eine zentrale „Datendrehscheibe“, nämlich der Durchlaufstelle (DLS) vorgeschlagen und in vorbereitenden Sitzungen der „Arbeitsgruppe Schnittstellendefinition“ des AK-TK diskutiert und verfeinert. Die Vorarbeiten im Rahmen des AK-TK wurden über den Round Table E-Mail Verteiler allen zugänglich gemacht und dienten als Diskussionsbasis. Oft stellte sich im Rahmen

[283] Zur Beschreibung des AK-TK siehe die Ausführungen zur Branchenempfehlung EP 020 in Kapitel II.3.2.1.

der Round Table Diskussionen die Notwendigkeit weiterer Klärungen und Diskussionen auf Seiten der Anbieter heraus. In diesen Fällen wurden AK-TK Treffen zwischen den Round Table Diskussionen abgehalten, deren Ergebnisse wiederum zur weiteren Diskussion an den großen Verteilerkreis weitergeleitet wurden. Auf der Seite der staatlichen Behörden wurden notwendige Abklärungen ebenfalls akkordiert und dann durch die Round Table Diskussionen wieder allen zugänglich gemacht. Auf diese Weise wurden die unterschiedlichen Kommunikationsstränge miteinander möglichst effektiv vernetzt.

Das Ziel der gesamten Datensicherheitsstudie war die Ausarbeitung eines Konzepts, welches den praktischen Ansprüchen aller Beteiligten genügen und gleichzeitig ein Höchstmaß an technischer und rechtlicher Sicherheit bieten sollte. Zu diesem Zweck wurde ein breites Netzwerk der Stakeholder etabliert, in dessen Rahmen die lösungsorientierte Diskussion vorangetrieben wurde. Das BIM übernahm im Rahmen der Studie die Verantwortung für den Diskussionsprozess zur Entwicklung eines Datensicherheitskonzepts, das per Verordnung im Herbst 2011 und auf der Ebene der technischen Implementierung bis 1.4.2012 umgesetzt werden soll. Das Konzept wurde durch den Studienautor ausgearbeitet und in den oben beschriebenen Diskussionsrunden zur Diskussion gestellt und mit einem Alternativkonzept basierend auf dem S/MIME-Standard . Die Auf- und Nachbereitung der fachlichen Grundlagen erfolgten ebenfalls durch den Studienautor, der dabei auch auf die Unterstützung von externen Experten und Expertinnen hinsichtlich technischer und rechtlicher Fragestellungen zurückgreifen konnte.[284]

IV.2 Themenkreise im Einzelnen

Im Rahmen dieses Kapitels werden nun jene Themen- und Fragenkomplexe einzeln herausgehoben, die sich im Zuge der Ausarbeitung des Referenzkonzepts der DLS und in den oben beschriebenen Diskussionsrunden als wesentlich gezeigt haben. Wo dies dem Verständnis der Problemlage dient, wird aus der Zusammenfassung zu den Round Table Diskussionen aus der BIM-Datensicherheitsstudie zitiert.

Jeweils am Ende der einzelnen Themenkomplexe wird als eigenes Unterkapitel ein „Lösungsvorschlag für eine Datensicherheitsverordnung (DSVO)“ angeführt, der die jeweils thematisch zusammenhängenden Bestimmungen des Entwurf für eine Datensicherheitsverordnung aus der BIM-Datensicherheitsstudie enthält[285]. §§ Bezeichnungen beziehen sich auf diesen Entwurf. Falls sich zwischen den Vorschlägen aus der BIM-Datensicherheitsstudie und dem am 10. August 2011 durch das BMVIT in Begutachtung geschickten Entwurf zur Datensicherheitsverordnung Änderungen ergeben haben, wird die Begutachtungsversion der ursprünglichen Version gegenüber gestellt. Zur besseren Unterscheidung werden die jeweils für die Begutachtung geänderten Bestimmungen in einer anderen Schriftart wiedergegeben und kommentiert. Da der Begutachtungsentwurf leider nur für die Zeit der Begutachtung (bis 20. September 2011) auf der Internetseite des BMVIT veröffentlicht wurde, wird der gesamte Begutachtungsentwurf zur DSVO samt den erläuternden Bemerkungen als Anhang zu dieser Dissertation abgedruckt.

---

[284] Vgl. die ausführlichere Beschreibung der Prozesse in BIM-Datensicherheitsstudie, Kapitel IV.A, S 63 ff.
[285] Siehe dazu den gesamten Vorschlag für eine DSVO samt Erläuterungen in der BIM-Datensicherheitsstudie in Kapitel V. S 137 ff.

IV.2.1 Anwendungsbereich des Systems der DLS

IV.2.1.1 Welche Datenauskünfte sollen über die DLS abgewickelt werden?

Die Vorgaben zur sicheren Übertragung der Daten im Schutzbereich des Telekommunikationsgeheimnisses regelt § 94 Abs. 4 TKG: „Die Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, einschließlich der Übermittlung von Vorratsdaten, nach den Bestimmungen der StPO sowie des SPG, hat unter Verwendung einer Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt, zu erfolgen. Die Daten sind unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie als "Comma-Separated Value (CSV)" - Dateiformat zu übermitteln (...)".

In den Erläuterungen zu § 94 Abs. 4 TKG[286] wird der Spielraum abstrakt beschrieben, den der Verordnungsgeber bei der Ausgestaltung dieser Bestimmung hat: „Die Bestimmung identifiziert die maßgeblichen Indikatoren zur Datensicherheit bei der Übermittlung von Verkehrsdaten. Die Übertragungstechnologie, welche durch eine Verordnung („Technische Richtlinie") nach dieser Bestimmung zu konkretisieren ist, soll durch sichere „Identifikation und Authentifizierung von Sender Empfänger" sicherstellen, dass die durch das Kommunikationsgeheimnis geschützten Verkehrsdaten tatsächlich nur Behörden und Gerichten zugänglich sind, denen eine gesetzliche Auskunftsbefugnis zusteht. Dabei muss auf technischer Ebene die Datenintegrität gewahrt sein. Das bedeutet, dass jede allfällige Veränderung der übermittelten Daten auf dem Übertragungsweg für den Empfänger sofort identifizierbar wäre und dieser sich damit auf die Richtigkeit der Daten nicht mehr verlassen darf. Die Formulierung „unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie" (im Gegensatz zur Fassung im ursprünglichen Begutachtungsentwurf vom Dezember 2009[287] „Übertragung per E-Mail") ist eine Ergänzung zur Erfüllung anspruchsvoller Datensicherheitsstandards, wie sie insbesondere im Urteil des deutschen Bundesverfassungsgerichts zu BVerfG, 1 BvR 256/08 vom 2.3.2010 beschrieben werden.[288] Die Formulierung lässt genügend Spielraum, die nähere technische Ausgestaltung durch Verordnung zu regeln und stellt gleichzeitig einen Auftrag an den Verordnungsgeber dar. Die gesetzlich vorgezeichneten Indikatoren sind dabei technologieneutral formuliert. Wesentlich ist, dass die eingesetzte Technologie den Zielvorgaben entspricht." [289]

Am 7.4.2011 wurde die TKG Novelle zur Umsetzung der Vorratsdatenspeicherung im Ausschuss für Forschung, Innovation und Technoloige (FIT Ausschuss) des Nationalrats diskutiert[290]. In diesem Rahmen wurde ein Antrag für eine Ausschussfeststellung zum Thema Datensicherheit eingebracht, der eine Grundsatzerklärung für die Implementierung der Durchlaufstelle enthält. Diese Ausschussfeststellung wurde mit den Stimmen der Regierungsfraktionen angenommen und lautet

---

[286] EB zur RV Nr. 1074 der BlgNR XXIV. GP.

[287] Begutachtungsentwurf des Bundesministeriums für Verkehr, Innovation und Technologie (BMVIT), ausgearbeitet vom Ludwig Boltzmann Institut für Menschenrechte (BIM) im Auftrag des BMVIT, von 15.11.2009 bis 15.1.2010 in öffentlicher Begutachtung: http://www.parlinkom.gv.at/PG/DE/XXIV/ME/ME_00117/pmh.shtml (07.10.2011).

[288] Dazu ausführlich die Darstellung des Urteils des BVerfG oben in Kapitel II.3.1.

[289] Vgl. die Erläuterungen zu § 1 DSVO-Entwurf in der BIM-Datensicherheitsstudie S 147 f.

[290] siehe dazu den Ausschussbericht: Nr. 1157 BlgNR XXIV. GP.

wie folgt: „Für die Datensicherheit und die Nachvollziehbarkeit der Zugriffe auf den Datenvorrat ist das Zusammenspiel der Bestimmungen der §§ 94 Abs. 4 und 102c TKG von besonderer Bedeutung. Während § 94 Abs. 4 den Aspekt der technischen Datenintegrität und der Determinierung der Verordnungsermächtigung über die Art der Verschlüsselung betrifft und die maßgeblichen Indikatoren zur Datensicherheit bei der Übermittlung von Verkehrsdaten identifiziert, um durch sichere ‚Identifikation und Authentifizierung von Sender und Empfänger' sicherzustellen, dass die durch das Kommunikationsgeheimnis geschützten Verkehrsdaten tatsächlich nur Behörden und Gerichten zugänglich sind, denen eine gesetzliche Auskunftsbefugnis zusteht, regelt § 102c Zugriffs- und Sicherheitsbestimmungen. Einerseits muss jeder Zugriff auf Vorratsdaten durch zwei Personen mit einer besonderen Ermächtigung hierzu autorisiert sein, um zu gewährleisten, dass nicht eine einzelne Person unbemerkt und unkontrolliert auf diese Daten zugreifen kann. Andererseits müssen Zugriffe auf Vorratsdaten beim Anbieter revisionssicher protokolliert werden. Die wichtigsten Kriterien sind dabei der Schutz vor Veränderung und Verfälschung, die Vollständigkeit, die Ordnungsmäßigkeit, die Sicherung vor Verlust, die Einhaltung der Aufbewahrungsfristen sowie die Dokumentation, Nachvollziehbarkeit und Prüfbarkeit des Verfahrens, wozu etwa bei Anordnungen der Staatsanwaltschaft auch die Angabe der Geschäftszahl der ermittelnden Kriminalpolizei zählt. Der Ausschuss geht davon aus, dass sämtliche Zugriffe und Übermittlungen von wem auch immer auf Vorratsdaten gemäß § 94 Abs. 4 TKG lückenlos protokolliert werden. Der Ausschuss geht weiters davon aus, dass ein automatisches zentrales System der Protokollierung solcher Abfragen und Übermittlungen notwendig ist, wobei unter dieser Protokollierung nicht die in § 102c Abs. 2 genannte zu verstehen ist. Sie wird vielmehr nur jene Daten umfassen, die zur statistischen Auswertung und zur Verknüpfung mit der gemäß § 102c Abs. 2 erfolgenden Protokollierung dient. Wünschenswert ist die Einrichtung einer ‚Datendrehscheibe' (‚Durchlaufstelle', kurz: DLS). Da jeder Auskunftsfall über die DLS mit einer fortlaufenden einmaligen Nummer versehen wird, kann im Falle einer Nachprüfenden Kontrolle über die Protokollierung bei der DLS zur Protokollierung beim Anbieter gemäß § 102c Abs. 2 verknüpft werden. Zugang zu den übermittelten personenbezogenen Daten soll die DLS selbst nicht bieten, die Daten liegen dort nur verschlüsselt bis zur Abholung bereit und werden bei der Abholung automatisch gelöscht." Festzuhalten ist an dieser Stelle, dass diese Ausschussfeststellung sachlich auf der Arbeit zur Entwicklung der Schnittstellenbeschreibung und eines sicheren Systems der Datenübermittlung in den Round Table Diskussionen basiert, die im Rahmen der BIM-Datensicherheitsstudie ausgearbeitet wurde. Die Ausschussfeststellung bezieht sich auf den Diskussions- und Einigungsstand beim 3. der insgesamt 6 Round Table Veranstaltungen am 24.3.2011, bei dem die Grundsatzeinigung auf das Konzept der Durchlaufstelle bereits Konsens unter allen Beteiligten war.[291]

Die Bestimmung des § 94 Abs. 4 TKG erfasst daher eindeutige alle Arten von Datenauskünften und macht dabei insbesondere keine Unterscheidung, ob es sich nun um Auskünfte über Vorratsdaten[292] handelt oder um Auskünfte über Daten, die aus betrieblichen Gründen beim Anbieter noch gespeichert sind (Betriebsdaten[293]). Soweit es nämlich um die Übermittlung von Verkehrsdaten, Zugangsdaten und Standortdaten für Auskünfte gegenüber Sicherheits- und Strafverfolgungsbehörden geht, die beim Anbieter für betriebliche Zwecke gespeichert sind, sind die Datensicherheitsvorschriften auch für diese Daten relevant. Wenn also die DLS das System zur

[291] Siehe die Dokumentation des 3. Round Tables in der BIM-Datensicherheitsstudie S 105 ff.
[292] Zur Definition von „Vorratsdaten" siehe oben Kapitel II.1.4.1.
[293] Zur Abgrenzung und Definition siehe unten Kapitel IV.2.6.

sicheren Datenübermittlung darstellt, dann müssen alle in § 94 Abs. 4 TKG genannten Datenauskünfte auch über die DLS abgewickelt werden. Denselben Standard auf die Abwicklung aller Datenauskünfte anzuwenden ist dabei nicht nur konsequent sondern auch aus rein praktischen Gründen notwendig. Viele Auskünfte werden nämlich künftig wohl „gemischte" Datensätze enthalten, also in derselben Auskunft Vorratsdaten und Betriebsdaten.[294] Hinsichtlich jener Bestimmungen, die Datensicherheitsmaßen innerhalb des Betriebes des Anbieters betreffen, ist die Verordnung allerdings nur für Vorratsdaten maßgeblich, denn nur für diese gelten gemäß § 102c TKG die strengen Zugriffsbestimmungen. Ansonsten gilt der allgemeine Sicherheitsmaßstab, den das TKG 2003 und das DSG 2000 vorgeben[295].

IV.2.1.2 AUSNAHMEN VON DER ÜBERMITTLUNG VIA DLS

§ 94 Abs. 4 TKG sieht ausdrücklich vor, dass es Ausnahmen vom Regime der Datensicherheitsverordnung geben soll: "Ausgenommen davon ist die Übermittlung von Daten in den Fällen des § 98, von Daten in den Fällen von § 99 Abs. 5 Z 3 und 4 bei Gefahr in Verzug, von Standortdaten in den Fällen der Feststellung des aktuellen Standortes gemäß § 134 ff. StPO sowie die Übermittlung von begleitenden Rufdaten im Rahmen einer Überwachung von Nachrichten."

Die erläuternden Bemerkungen zu § 94 Abs. 4 TKG im Rahmen der Regierungsvorlage zur TKG Novelle führen dazu aus: „Ausdrücklich gesetzlich gefordert ist eine Verschlüsselung bei der Übermittlung. Davon ausgenommen sein soll die Übermittlung von Daten in Notfällen. In diesen Fällen soll daher die bisher praktizierte Übermittlungsform beibehalten werden, also Auskünfte per Telefon oder Fax. Die weiteren Ausnahmen vom Grundsatz der Übermittlung in einem CSV File berücksichtigen die in der Praxis wichtigen Fälle, in denen aufgrund der besonderen Dringlichkeit (insbesondere bei Standortdatenauskünften, etwa zur Lebensrettung oder bei zeitkritischen Observationen) dieses Verfahren nicht zweckmäßig wäre. Außerdem sind die sogenannten „S-Records" (das sind die begleitenden Verkehrsdaten bei einer Inhaltsüberwachung von Telefongesprächen) berücksichtigt, welche über eine besondere technische Schnittstelle gemeinsam mit der Inhaltsüberwachung abgewickelt werden." [296]

Aufgezählt werden also jene Fälle, in denen eine Beantwortung von Auskunftsbegehren durch den Anbieter nach einem anderen Regime vorgesehen oder zumindest zulässig ist und eine Verschlüsselung gemäß § 94 Abs. 4 TKG nicht zwingend durchzuführen ist. Die auf § 98 TKG 2003 bezogene Ausnahme adressiert die Identifizierung und Lokalisierung von Anschlüssen bzw. Endgeräten, von denen ein Notruf abgesetzt wurde. Für diese Fälle soll es künftig nach der Umsetzung des neuen Telekom Rechtsrahmens eine eigene Schnittstelle geben, um eine sofortige Reaktion der Notrufträger zu ermöglichen, wobei damit eine automatische nachträgliche Information der Betroffenen verbunden ist. Die Umsetzung dieser gemeinschaftsrechtlichen Verpflichtung steht

---

[294] Vgl. die Dokumentation des 2. Round Tables in der BIM-Datensicherheitsstudie S. 100.
[295] Näher dazu unten in Kapitel IV.2.4.
[296] EB zur RV § 94 Abs. 4, Nr. 1074, XXIV. GP, http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01074/fname_206854.pdf (07.10.2011). Sämtliche dem Parlament als Regierungsvorlage vorgelegten Dokumente zur TKG Novelle sowie die Berichterstattung aus dem zuständigen Ausschuss für Forschung, Innovation und Technologie (FIT) sind abrufbar unter http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01074/index.shtml.

unmittelbar bevor, daher ist dieser Fall aus dem Anwendungsbereich dieser Verordnung ausgeklammert.[297] Die ebenfalls ausdrücklich genannte Übermittlung von begleitenden Rufdaten im Rahmen einer Überwachung von Nachrichten erfolgt über die ETSI Schnittstelle zur Inhaltsüberwachung durch Übergabe der sogenannten „S-Records".[298] Dabei handelt es sich nicht um Auskünfte über historische Verkehrsdaten sondern um die „live-Daten" von Gesprächen, die einer Inhaltsüberwachung unterzogen werden. Da hierzu notwendigerweise eine völlig andere technische Schnittstelle existiert, sind diese Fälle schon aus technischen Gründen vom System der DLS auszunehmen. Grundsätzlich gilt aber, dass Ausnahmen eng und klar zu definieren und möglichst einer besonderen Missbrauchskontrolle zu unterwerfen sind, weil parallele Kommunikationswege immer die Gefahr einer Umgehung der vorgeschriebenen Sicherheitsstandards in sich bergen.

IV.2.1.2.1 Dringliche Datenauskünfte über die DLS?

Die in § 94 Abs. 4 TKG vom allgemeinen Sicherheitsregime ausgenommenen Fälle des § 99 Abs. 5 Z 3 und 4 TKG bei Gefahr im Verzug gemäß Z 2 beziehen sich auf Anfragen nach § 53 Abs. 3a und 3b SPG, wenn aufgrund der besonderen Umstände des Falles der Zweck der Auskunft (zB die Abwehr einer gegenwärtigen oder unmittelbar drohenden Gefahr) dadurch gefährdet wäre, dass die Abwicklung der Auskunft über das System der DLS zu lange dauern würde und daher eine schnellere Form der Beauskunftung unerlässlich ist, zB eine telefonische Auskunft über die Standortdaten des Endgerätes einer akut gefährdeten Person.[299]

Standortdatenanfragen nach § 53 Abs. 3b SPG werden dabei schon aufgrund des dort normierten Tatbestandes (Abwehr einer „gegenwärtigen Gefahr" für den Inhaber der Endeinrichtung) regelmäßig einen Fall von „Gefahr in Verzug" darstellen. Festzuhalten ist, dass in diesen Fällen nur ausnahmsweise überhaupt historische Standortdaten begehrt werden, nämlich nur dann, wenn eine live-Ortung (durch sog. „stummes SMS") erfolglos bleibt, etwa weil das Endgerät defekt oder ausgeschaltet ist. In Fällen von Gefahr im Verzug kann die Anfrage telefonisch übermittelt werden.

SPG Anfragen können bei Gefahr im Verzug entweder mündlich, schriftlich oder über die DLS zum Anbieter gelangen. Dabei ist jedoch festzuhalten, dass das Konzept der DLS auch darauf abzielt, die Abwicklung von Auskunftsbegehren im Vergleich zur bisherigen Praxis (Fax- und E-Mail- Anfragen) zu beschleunigen und den Verwaltungsaufwand sowohl auf Behörden- als auch auf Anbieterseite zu reduzieren. Es ist daher nicht generell davon auszugehen, dass eine Abwicklung abseits der DLS tatsächlich jene Beschleunigung mit sich bringt, welche die gesetzlichen Ausnahmen rechtfertigen soll. Die Praxis ab dem Vollbetrieb des neuen Konzepts ab 1.4.2012 wird zeigen, ob gerade in dringenden Fällen eine Abwicklung über die DLS nicht sogar vorteilhaft sein wird. Wenn keine Gefahr im Verzug vorliegt sind sowohl die Anfrage als auch die Antwort aber ausschließlich über die DLS zulässig. Darüber hinaus ist darauf hinzuweisen, dass selbst bei Anfragen von Notrufträgern gem. § 98 TKG, welche im Zuge eines Notfalles die Hilfeleistung bzw. die Abwehr von unmittelbarer Gefahr

[297] Vgl. dazu oben die Ausführungen zum EU Telekom-Reformpaket in Kapitel II.4.1; über die Planung der Schnittstelle zur Standortdatenfeststellung für Notrufträger wurde beim 6. Round Table diskutiert, vgl. dazu die BIM-Datensicherheitsstudie S 130.
[298] Vgl. die Erläuterungen zu § 3 Abs. 1 DSVO-Entwuf in der BIM-Datensicherheitsstudie S 149.
[299] Siehe die Erläuterungen zu § 3 Abs. 2 DSVO-Entwuf in der BIM-Datensicherheitsstudie S 149.

für Leib und Leben zum Ziel haben, eine schriftliche Darlegung der Notwendigkeit spätestens innerhalb von 24 Stunden nachgereicht werden muss.

Davon zu unterscheiden ist aber die Verpflichtung zur nachträglichen Dokumentation über die DLS. Die Dokumentation über die DLS ist dabei sinnvoll und notwendig, da teilweise (insbesondere bei Anfragen zu IP-Adressen und E-Mail Daten) auch Vorratsdaten betroffen sein werden und der Anbieter bei Zugriff auf Vorratsdaten die Protokolldaten gemäß § 102c TKG zu übermitteln hat und der besondere Rechtsschutz (Informationspflicht der Behörde) ausgelöst wird. Es soll daher jedenfalls eine Nachreichung der Anfrage über die DLS, wobei davon auszugehen ist, dass die Beantwortung der Anfrage bereits vor der Nachreichung der Anfrage erfolgt. Dies bedeutet, dass bei der technischen Spezifikation der DLS Festlegungen zur Unique-ID getroffen werden müssen.[300] Dazu könnte jedem Anbieter ein eigener Bereich von Referenznummern zugeteilt werden. Der Anbieter verwendet diese Referenznummern in aufsteigender Reihenfolge im Falle, dass die betreffende Anfrage noch nicht über die DLS eingelangt ist. In der Durchlaufstelle muss dann die Zuordnung zwischen Anfrage und (bereits erfolgter) Durchführung erfolgen. Zu berücksichtigen ist der Usecase "nachträgliche Anfragedokumentation" (Daten wurden bereits übermittelt) sowie die Übermittlung von Protokolldaten. Die technische Spezifikation sollte hierzu also jedenfalls einen Usecase "nachträgliche Anfragedokumentation" berücksichtigen und idealer weise auch eine Prioritäteninformation bei der Notifikation über die DLS vorsehen.[301]

In der Diskussion im Rahmen des 5. Round Table wurde seitens des BMJ argumentiert, dass es auch im Rahmen von StPO-Abfragen eng begrenzte Fälle geben könne, in denen zunächst eine mündliche Übermittlung der Anordnung erfolgen dürfe. Anordnungen von Zwangsmaßnahmen sind von der Staatsanwaltschaft grundsätzlich begründet und schriftlich auszufertigen und an die Kriminalpolizei zu richten. In dringenden Fällen könne aber eine solche Anordnung vorläufig mündlich übermittelt werden (§ 102 Abs. 1 StPO). Dies gelte auch für die Anordnung einer „Auskunft über Daten einer Nachrichtenübermittlung" (§ 134 Z 2 StPO) sowie künftig bei einer „Auskunft über Vorratsdaten" (§ 134 Z 2a StPO). In dringenden Fällen sollten nach Auffassung des BMJ mündliche Anordnung auch auf Grund einer mündlichen gerichtlichen Bewilligung (§ 105 StPO) erteilt werden. So könne etwa im Fall des § 135 Abs 2 Z 1 StPO (noch andauernde Entführung) eine Dringlichkeit vorliegen, die zumindest erfordert, dass die Übermittlung des Auskunftsbegehrens vorerst „auf kürzestem Weg" an den Anbieter gerichtet wird, während die Antwort über die sichere Verbindung gemäß § 94 Abs 4 TKG 2003 übermittelt werden muss, weil diesbezüglich keine gesetzliche Ausnahme vorgesehen ist. Der Wortlaut des TKG 2003 steht dem nicht entgegen, da § 94 Abs. 4 TKG 2003 ausdrücklich nur die Beantwortung, aber nicht die Übermittlung der Anordnung regelt. Diesbezüglich wäre gemäß § 102 Abs. 1 StPO die schriftliche und begründete Anordnung der Staatsanwaltschaft nachzureichen. Das Erfordernis einer gerichtlichen Bewilligung sage per se nichts über die Dringlichkeit und das auch über Entführungsfälle hinausgehende Erfordernis einer mündlichen Beauskunftung vorab aus. Die gerichtliche Bewilligung könne im Rahmen des Rufbereitschafts- und Journaldienstes fernmündlich binnen kürzester Zeit erteilt werden, gerade wenn eine unverzügliche Anordnung durch die Staatsanwaltschaft fallspezifisch nötig sei. § 102 Abs. 1 StPO sehe generell vor, dass Anordnungen und Genehmigungen in dringenden Fällen vorläufig mündlich übermittelt werden können. In der Praxis, so das BMJ, würden solche mündlichen Anordnungen von den meisten Anbietern akzeptiert–

[300] Vgl. dazu unten die Ausführungen zur Funktion der Unique-ID in Kapitel IV.2.3.4.
[301] Vgl. dazu unten die Ausführungen zu den Use-Cases in Kapitel IV.2.10.

wenn eine schriftliche Bestätigung der Exekutive über "mündliche Anordnung und Bewilligung" vorliege. Auch in diesen Fällen sei Vorkehrung dafür zu treffen, dass eine Beantwortung vor Übermittlung der Anfrage erfolgen könne.[302]

Im Rahmen der BIM-Datensicherheitsstudie wurde dieser Argumentation zunächst gefolgt, wobei diese Auslegung nicht ausdrücklich Eingang in den Text des Vorschlages für eine DSVO fand sondern nur in den Erläuterungen ausgeführt wurde. Zugleich wurde das Erfordernis herausgehoben, dass die schriftliche Anfrage über die DLS nachzureichen und zu dokumentieren ist.[303] Im Zuge der Stellungnahmen zum Begutachtungsverfahren wurde diese Argumentation allerdings von Seiten der Telekom- und Internetwirtschaft mit guten Gründen in Frage gestellt. Insbesondere die Stellungnahme der ISPA[304] (Internet Service Providers Austria, Dachverband) bringt hierzu beachtliche Argumente vor: Demzufolge sei schon in der Vergangenheit (nach einstimmiger Ansicht von Lehre und Praxis) klargestellt worden, dass mündliche (Betreiber-) Anordnungen nicht zulässig seien.[305] Einerseits sehen die Bestimmung der StPO (zB gem. § 138 Abs. 3 StPO) keine mündlichen Anordnungen vor. Andererseits beziehe sich § 102 StPO, auf welchen zB § 76a StPO[306] verweist, nur auf („an die Kriminalpolizei" gerichtete) sog. „Durchführungsverordnungen" und nicht auf (Betreiber) Anordnungen[307], die an Private bzw. Anbieter gerichtet werden. Ein Ausufern der Möglichkeit, mündliche Anordnungen zu erteilen, würde unweigerlich zu Rechtsunsicherheit und einer Reihe anderer Probleme (fehlende Authentifizierung der anfragenden Stelle, etc.[308]) führen, argumentiert die ISPA. Eine funktionierende Praxis der mündlichen Anordnungen, wie in den Erläuterungen angeführt, könne von Seiten der Anbieter nicht bestätigt werden. Auch jetzt würden derartige Anordnungen[309] nur eine in der StPO nicht vorgesehene Ausnahme darstellen. Von einer branchenweit anerkannten Praxis könne somit keinesfalls die Rede sein, da die StPO mündliche Anordnungen an Anbieter nicht vorsehe. Im Ergebnis wird nunmehr auch hier - im Gegensatz zu den Ausführungen in der BIM-Datensicherheitsstudie - die Kraft der Gegenargumente anerkannt und daher deren Position geteilt. Wenn also die von Seiten des BMJ gewünschten Ausnahmen im Zusammenhang mit Datenauskünften nach der StPO aufgenommen werden sollte, bedürfte es dafür einer ausdrücklichen gesetzlichen Grundlage, um diese ansonsten systemwidrige Konstellation in einer Datensicherheitsverordnung zu rechtfertigen.

---

[302] Vgl. die Zusammenfassung der Diskussion im 5. Round Table in der BIM-Datensicherheitsstudie S 120.

[303] Siehe die Erläuterungen zu § 3 Abs. 2 DSVO-Entwurf in der BIM-Datensicherheitsstudie S 121 sowie die Erläuterungen zu § 3 Abs. 2 DSVO-Begutachtungsentwurf im Anhang.

[304] ISPA Stellungnahme betreffend die Verordnung der Bundesministerin für Verkehr, Innovation und Technologie betreffend die Datensicherheit (Datensicherheitsverordnung TKG-DSVO), abrufbar auf der Website der ISPA unter http://www.ispa.at/stellungnahmen/bmvit-konsultation-datensicherheitsverordung/.

[305] EBRV 25 BlgNR XXII.GP 137; Bertel/Venier, Strafprozessrecht, Rz 195; Pilnacek/Peischl, Das neue Vorverfahren, RZ 419f.

[306] Tritt in Kraft mit 01.04.2012.

[307] Vgl. hierzu die in § 138 (3) StPO geregelte, an Anbieter gerichtete (Betreiber-) Anordnung.

[308] In Fußnote 7 der ISPA Stellungnahme wird dazu ausgeführt, die Erfahrungen der Anbieter in der Vergangenheit hätten gezeigt, dass die Nachreichung von Anordnungen in der Praxis zu erheblichen Problemen (zB keine Erteilung nachträglicher gerichtlicher Bewilligung, Weigerung der Staatsanwaltschaft Anordnung zu verfassen, Ziffernstürze, abweichende Zeiträume und -Umfänge, etc.) führte.

[309] ZB im Falle einer noch andauernden Entführung gem. § 135 Abs. 2 Z 1 StPO.

IV.2.1.2.2 VERPFLICHTUNG ZUR EINRICHTUNG EINES JOURNALDIENSTES?

Auch die TKG-Novelle zur Umsetzung der Vorratsdatenspeicherung enthält keine Pflicht zur Einrichtung eines Journaldienstes auf Seiten der Anbieter, um im Falle dringlich begehrter Datenauskünfte auch außerhalb der Geschäftszeiten in jedem Fall sofort reagieren zu können. Die Erläuterungen zu § 102b Abs. 2 TKG halten dazu knapp fest: „Die Wendung „unverzüglich" impliziert keinesfalls, dass Anbieter zur Einrichtung eines Journaldienstes zur Erteilung von Auskünften über Vorratsdaten verpflichtet sind. Eine Verpflichtung zur Beauskunftung außerhalb der Bürozeiten besteht daher nicht."[310]

Grundsätzlich werden Anfragen bei allen Anbietern umgehend beantwortet, am Wochenende ist jedoch generell kein juristischer Journaldienst verfügbar, um die Rechtmäßigkeit einer Anfrage zu prüfen. Zudem kommt es regelmäßig vor, dass die inneren organisatorischen Prozesse der Anbieter im Falle mehrerer gleichzeitiger Datenanfragen überlastet sind. Bei kleineren Providern dauert eine Auskunft generell länger, dies liegt vor allem an der rechtlichen Zulässigkeitsprüfung. Dennoch bieten in der Praxis einige (vor allem große) Anbieter die Möglichkeit, dass Anfragen außerhalb der Geschäftszeiten vor allem durch technisches Wartungspersonal rasch abgewickelt werden. Die sog. Network Operation Centers (NOC) sind allerdings nur dafür eingerichtet, auf betrieblich technische Daten zuzugreifen. Es wären also organisatorische Änderung notwendig, um hier auch einen Zugriff auf Vorratsdaten sicherzustellen, welcher nur nach dem 4-Augen-Prinzip erfolgen darf (wobei hier eine nachprüfende, wenngleich zeitlich nahe Kontrolle durch einen zweiten Mitarbeiter des Unternehmens ausreichen wird)[311]. Zu bedenken ist, dass in dringenden Auskunftsfällen wohl selten Daten zu Kommunikationsvorgängen benötigt werden, die länger zurück liegen und daher mit hoher Wahrscheinlichkeit nur noch als Vorratsdaten vorhanden sind. Relevant werden könnte die Frage aber vor allem bei IP-Adressen und Standortdaten, falls ein Anbieter schon nach kurzer Zeit keine betriebliche Rechtfertigung zur Speicherung mehr in seiner internen Speicher-Policy anführt.[312]

IV.2.1.2.3 LÖSUNGSVORSCHLÄGE FÜR EINE DSVO

Die eben ausgeführten Regel-Ausnahme Bestimmungen zur Klarstellung des Anwendungsbereichs könnten für eine Datensicherheitsverordnung wie folgt formuliert werden: [313]

§ 1 Regelungsgegenstand

(1) (1) Mit dieser Verordnung werden die näheren Bestimmungen des Formats, der Datenfelder und der Syntax der CSV-Datei bei der Übermittlung von Auskünften über Verkehrsdaten (§ 99 Abs. 5 TKG 2003) und Vorratsdaten (§ 102b TKG2003) sowie die näheren Bestimmungen zur Datensicherheit und zur Protokollierung bei der Übermittlung solcher Auskünfte getroffen.
(2) Ebenfalls Gegenstand dieser Verordnung sind die näheren Bestimmungen zur Datensicherheit bei der Speicherung und der Zugriffsprotokollierung von Vorratsdaten.

---

[310] EBRV zu § 102b Abs. 2 TKG, 1074 BLgNR XXIV. GP 27, abrufbar unter http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01074/fname_206854.pdf.
[311] Näher zum 4-Augen-Prinzip unten in Kapitel IV.2.8.1.
[312] Vgl. BIM-Datensicherheitsstudie S 122.
[313] Siehe den Entwurf für eine DSVO in der BIM-Datensicherheitsstudie S 138 f.

§ 2 Anwendungsbereich und Begriffsbestimmungen

(1) Erfasst vom Anwendungsbereich dieser Verordnung ist die Verwendung (§ 4 Z 8 des Datenschutzgesetzes 2000 - DSG 2000, BGBl. I Nr. 165/1999 in der Fassung BGBl. I Nr. 135/2009) von Verkehrsdaten, Zugangsdaten und Standortdaten sowie Stammdaten, soweit diese in Verbindung mit den eben genannten Datenkategorien gespeichert oder verarbeitet werden.
(2) Die in Absatz 1 genannten Daten werden nachfolgend bezeichnet als
    1. Betriebsdaten, soweit diese für den Anbieter für die in § 99 Abs. 2 und 3 TKG 2003 erfassten Zwecke notwendig sind;
    2. Vorratsdaten, soweit diese vom Anbieter ausschließlich aufgrund der Verpflichtung gemäß § 102a TKG 2003 für die in § 102b TKG 2003 genannten Zwecke vorrätig gespeichert werden (§ 92 Abs. 3 Z 6b TKG 2003).
(3) In dieser Verordnung bezeichnet der Begriff
    1. „Anbieter“ Anbieter von Kommunikationsdiensten,
    2. „Vorratsdatenbank“ eine Datenbank zur Speicherung von Vorratsdaten.

§ 3 Ausnahmen

(1) Die Bestimmungen zur Datensicherheit bei der Übermittlung von Daten nach dem III. Abschnitt dieser Verordnung sind gemäß § 94 Abs. 4 TKG nicht verbindlich
    1. in den Fällen des § 98 TKG 2003,
    2. in den Fällen des § 99 Abs. 5 Z 3 und 4 TKG 2003 bei Gefahr im Verzug,
    3. bei der Feststellung des aktuellen Standortes gemäß §§ 134 ff der Strafprozessordnung 1975 (StPO), BGBl. Nr. 631 in der Fassung BGBl. I Nr. 33/2011, und
    4. bei der Übermittlung von begleitenden Rufdaten im Rahmen einer Überwachung von Nachrichten.
(2) Anfragen zu Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, einschließlich Anfragen zu Vorratsdaten, die gemäß gesetzlicher Bestimmungen vorab mündlich erfolgen können, müssen mit Ausnahme der Anfragen gemäß § 98 TKG 2003 über die Durchlaufstelle (§ 9) nachgereicht und dokumentiert werden.

IV.2.1.2.3.1 Änderungen im Begutachtungsentwurf des BMVIT zur DSVO

Gegenstand und Anwendungsbereich

§ 1. (1) In dieser Verordnung werden die näheren Bestimmungen
1. des Formats, der Datenfelder und der Syntax der CSV-Datei bei der Übermittlung von Auskünften über Verkehrsdaten (§ 99 Abs. 5 TKG 2003) und Vorratsdaten (§ 102b TKG2003),
2. zur Datensicherheit und zur Protokollierung bei der Übermittlung der in Z 1 genannten Auskünfte sowie
3. zur Datensicherheit bei der Speicherung und der Zugriffsprotokollierung von Vorratsdaten getroffen

(2) Der Anwendungsbereich dieser Verordnung erstreckt sich auf die Verwendung von Verkehrsdaten, Zugangsdaten und Standortdaten sowie Stammdaten, soweit diese in Verbindung mit den eben genannten Datenkategorien verarbeitet werden.

Begriffsbestimmungen

§ 2. (1) Verkehrsdaten, Zugangsdaten und Standortdaten sowie – soweit sie in Verbindung mit den zuvor genannten Datenkategorien verarbeitet werden - Stammdaten werden bezeichnet als
1. „Betriebsdaten“, soweit diese für den Anbieter für die in § 99 Abs. 2 und 3 TKG 2003 erfassten Zwecke notwendig sind;
2. „Vorratsdaten“, soweit diese vom Anbieter ausschließlich aufgrund der Verpflichtung gemäß

§ 102a TKG 2003 für die in § 102b TKG 2003 genannten Zwecke vorrätig gespeichert werden (§ 92 Abs. 3 Z 6b TKG 2003).

(2) In dieser Verordnung bezeichnet der Begriff
1. „Anbieter“ Betreiber von öffentlichen Kommunikationsdiensten,
2. „Vorratsdatenbank“ eine Datenbank zur Speicherung von Vorratsdaten.

Ausnahmen

§ 3. (1) Die Bestimmungen des 3. Abschnittes sind nicht anzuwenden
1. in den Fällen des § 98 TKG 2003,
2. bei Gefahr in Verzug in den Fällen des § 99 Abs. 5 Z 3 und 4 TKG 2003,
3. bei der Feststellung des aktuellen Standortes gemäß §§ 134 ff der Strafprozessordnung 1975 (StPO), BGBl. Nr. 631 in der Fassung BGBl. I Nr. 33/2011, und
4. bei der Übermittlung von begleitenden Rufdaten im Rahmen einer Überwachung von Nachrichten.

(2) Anfragen über Verkehrsdaten, Standortdaten und Stammdaten, deren Beantwortung die Verarbeitung von Verkehrsdaten erfordert, einschließlich Anfragen über Vorratsdaten, deren Beantwortung gemäß gesetzlicher Bestimmungen vorab mündlich erfolgen können, müssen mit Ausnahme der Anfragen gemäß § 98 TKG 2003 über die Durchlaufstelle (§ 9) nachgereicht und dokumentiert werden.

Die Änderungen zwischen der Version in der BIM-Datensicherheitsstudie und der Begutachtungsversion des BMVIT in §§ 1 und 2 DSVO-Entwurf sind zunächst legistischer Natur ohne Auswirkungen auf den Bedeutungsgehalt. Der ursprünglich in § 1 DSVO genannte Regelungsgegenstand wurde für den Begutachtungsentwurf aus dem Normtext herausgezogen und in einer Promulgationsklausel formuliert.[314] Die formale Trennung von Anwendungsbereich und Begriffsdefinitionen in der Formulierung der Normtexte dient der Normenklarheit und bewirkt keine inhaltliche Änderung.

Dass im neuen § 1 Abs. 1 „Standortdaten“ nicht mehr ausdrücklich erwähnt werden, soll einer textökonomischen Formulierung dienen, weil Standortdaten in §§ 99 Abs. 5 und 102b TKG ausdrücklich enthalten sind und ohnehin ein Verweis auf diese Bestimmungen besteht. Dem ist grundsätzlich zuzustimmen, allerdings ist der Begutachtungsentwurf diesbezüglich inkonsequent, weil in § 2 DSVO Standortdaten doch wieder ausdrücklich angeführt werden.

In Absatz 1 wird bewusst die Formulierung „Verwendung“ normiert. Nach § 4 Z 8 DSG 2000 ist „Verwenden von Daten“ definiert wird als „ jede Art der Handhabung von Daten, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten“ und der Begriff „Verarbeiten von Daten“ gemäß § 4 Z 9 DSG 2000 auch die Speicherung umfasst. In der österreichischen datenschutzrechtlichen Terminologie ist dies der weiteste Begriff, der alle Fälle möglicher Datenverwendungen - insbesondere die Übermittlung von Daten - umfasst. Weil gerade im Regelungsbereich des § 94 Abs. 4 TKG 2003 die Übermittlung im Vordergrund steht, wird hier der Rechtsbegriff der Datenverwendung nutzbar gemacht. Aus dem Regelungsumfang der Verordnung ist zugleich klar, dass die weitere Verwendung der betreffenden Daten nach der Übermittlung über die DLS - insbesondere die weitere Verwendung der Daten für die Zwecke der Strafverfolgung - nicht

[314] Siehe DSVO-Begutachtungsentwurf im Anhang.

von dieser Verordnung bestimmt wird. Dass im Begutachtungsentwurf der ausdrückliche Klammerverweis auf § 4 Z 8 DSG 2000 entfallen ist, ändert in der Sache nichts. Ebenfalls keine inhaltliche Änderung bewirkt, dass bei der Definition des Anwendungsbereiches in § 1 Abs. 2 DSVO (ursprünglich § 2 Abs. 1) nur noch „verarbeitet" und nicht „gespeichert oder verarbeitet" formuliert wird, weil gemäß § 4 Z 9 DSG 2000 der Begriff „verarbeiten" auch „speichern" umfasst.

IV.2.2 Welche Funktionen soll die DLS bieten?

IV.2.2.1 Funktionen der DLS im Überblick[315]

Wichtig ist von vornherein die Klarstellung, dass der Durchlaufstelle nicht die Aufgabe zukommt, Auskunftsbegehren oder deren Beantwortung auf deren Rechtmäßigkeit zu prüfen. Die DLS ist keine Art neue Behörde[316] oder Dienststelle sondern vielmehr ein Modell für technische und organisatorische Abläufe im Zusammenhang mit Auskunftsbegehren von Sicherheits- und Strafverfolgungsbehörden gegenüber Anbietern von öffentlichen Kommunikationsdiensten. Vorwegzuschicken ist, dass im Rahmen einer Verordnung nicht alle technischen Details geregelt werden können. Vielmehr muss eine Datensicherheitsverordnung die Funktionen und die zu erreichenden Ziele (Sicherheitsniveau etc.) hinreichend klar vorgeben, sodass auf deren Basis eine technische Spezifikation zur Klarstellung aller Einzelheiten der Umsetzung erfolgen kann. Natürlich liegt auch die technische Spezifikation in der Verantwortung der zuständigen Ministerien[317], allerdings ist davon auszugehen, dass sich diese dafür eines Dienstleisters mit entsprechendem Fachwissen bedienen werden. Umso wichtiger ist es daher, dass bereits die Verordnung einen möglichst hohen Determinierungsgrad aufweist, damit die demokratiepolitischen Sicherungsmechanismen (öffentliche Begutachtung, Berichtspflicht an den Hauptausschuss des Nationalrats gemäß § 94 Abs. 4 TKG) nicht unterwandert werden.

Die primäre Funktion der DLS ist die eines Postfaches zum sicheren Datenaustausch. Hierfür muss sich in einer sicheren öffentlichen IT-Infrastruktur ein Server befinden, über den - technisch gesehen - alle Anfragen abgewickelt werden. Hier wird - wie schon im Rahmen der BIM-Datensicherheitsstudie - vorgeschlagen, den Auftrag zur Einrichtung und zum Betrieb der DLS an das Bundesrechenzentrum (BRZ) zu vergeben.[318] Für die Ausführung der Mailbox-Funktion der DLS kann es vorteilhaft sein, Webapplikationen und Webservices technisch zu kombinieren, da ein Webservice von der Clientseite flexibel angesprochen werden könnte und somit ein höheres Maß an Benutzerkomfort durch Ausgestaltung des Clients auf der jeweiligen Teilnehmerseite (Behörden oder Anbieter) gestaltbar wäre.[319] Die Abläufe der Zustellung von Auskunftsbegehren und Antworten in die Postfächer der jeweils Beteiligten sind in einer Datensicherheitsverordnung klar vorzuzeichnen und erfüllen auch eine wesentliche datenschutzrechtliche Funktion. Aus den Vorgaben für die

---

[315] Vgl. dazu oben die schematische Darstellung in Kapitel III.1.1.

[316] Gelegentlich tauchte in der Berichterstattung der jüngsten Zeit im Zusammenhang mit der DLS der Begriff „Clearingstelle" oder „Clearing-Instanz" auf, vlg. zB http://help.orf.at/stories/1687652/ (10.10.2011); dieser Begriff ist etwas irreführend, weil er eine inhaltliche Kontrolle der Auskunftsbegehren durch die DLS suggeriert.

[317] Konkret gemäß § 94 Abs. 4 TKG das BMVIT, das BMI und das BMJ gemeinsam, gemäß § 102c TKG das BMVIT.

[318] Zur Begründung, warum gerade das BRZ am besten dafür geeignet sein soll, vgl. unten Kapitel IV.2.11.1.

[319] Vgl. BIM-Datensicherheitsstudie S. 162 f und 166.

technische Konzeption muss eindeutig hervorgehen, dass die Auskunft über Daten, die vom Schutzbereich des DSG 2000 und des Kommunikationsgeheimnisses des § 93 TKG 2003 erfasst sind, immer in Form eines „push" aus der Sicht des Anbieters erfolgt, dass also Daten nicht von den Sicherheitsbehörden einfach abgerufen werden können sondern vom Anbieter aktiv gesendet werden müssen. Die Abholung der Anordnung durch den Anbieter einerseits und die Abholung der Antwort durch die Behörde andererseits könnte durch den Einsatz von Webservices teilautomatisiert werden. Dadurch entsteht aber keine vollautomatisierte Schnittstelle mit unmittelbarem Zugriff der Behörden auf die Datenbanken der Anbieter. Die Mediatisierung über die DLS als Postfachsystem stellt eine faktisch effektive und wichtige Begrenzung der staatlichen Kontrollmacht dar.[320] Um sicherzustellen, dass jede Behörde nur auf personenbezogene Daten im Rahmen ihrer gesetzlichen Aufgabenerfüllung zugreifen kann, soll ein Benutzer ausschließlich Zugriff auf jenes Postfach bei der DLS erhalten, welches seiner Dienststelle zugeordnet ist.

Die wichtigsten Funktionen der DLS und zugleich die Rechtfertigung für die Implementierung eines solchen Konzepts dienen der Datensicherheit im engeren Sinn. § 94 Abs. 4 TKG schreibt dazu vor, dass eine Übertragungstechnologie einzusetzen ist, „welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt". Ein Datenaustausch soll dabei nur möglich sein, wenn die beteiligten Stellen über eine Berechtigung verfügen. Damit ist die zweite wesentliche Funktion der DLS adressiert: Die Identifizierung und Authentifizierung der Teilnehmer am Datenaustausch. Datensicherheit kann nur gewährleistet werden, wenn von vornherein auf technischer Ebene zuverlässig abgesichert ist, dass nur jene Stellen an einem Datenaustausch teilnehmen können, denen auch eine gesetzliche Berechtigung dafür zukommt. Diese Stellen müssen daher zunächst als Benutzer an die DLS angebunden werden. Das System muss sodann für jeden einzelnen Kommunikationsfall sicherstellen, dass der jeweilige Teilnehmer Identifiziert wird und diese Identität auch authentisch ist.[321] Dem Themenkreis der Authentifizierung zuordnen lässt sich auch die Funktion der Integritätsprüfung. Dabei geht es darum, dass der Empfänger eines verschlüsselten Datensatzes feststellen kann, wenn die übermittelten Daten unterwegs in irgendeiner Weise verändert wurden. Eine solche Integritätsprüfung ist auch mit Hilfe einer elektronischen bzw. digitalen Signatur umsetzbar. Damit ist nachprüfbar, ob die elektronischen Informationen tatsächlich vom Signator stammen und ob sie im Originalzustand - also unverändert - sind. Elektronische Signaturen können weiters auch zur Identifikation verwendet werden. Die genannten Merkmale sind beim Empfänger elektronisch signierter Daten überprüfbar.[322]

Gemäß § 94 Abs. 4 TKG sind „die Daten (…) unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie als "Comma-Separated Value (CSV)" - Dateiformat zu übermitteln." Die dritte Funktion der DLS zur Erreichung eines hohen Datensicherheitsniveaus ist damit die Verschlüsselung, die technischen gesehen mit der Funktion der Authentifizierung regelmäßig zusammenhängt[323]. Um hohen Ansprüchen gerecht zu werden muss die Verschlüsselung auf zwei

---

[320] Siehe dazu oben die Ausführungen zum Urteil des dt. BVerfG in Kapitel II.3.1.1.

[321] Details zur Identifikation und Authentifizierung siehe unten in Kapitel IV.2.3.

[322] Vgl. dazu die Erklärungen des „Zentrum für sichere Informationstechnologie Austria" unter http://www.a-sit.at/de/signatur/index.php.

[323] Vgl. dazu den Überblick über die kryptographischen Grundziele in: Österreichisches Informationssicherheitshandbuch, Kapitel A.2.1.2, online abrufbar unter https://www.sicherheitshandbuch.gv.at/index.php?view=browse&chapter=712000&uid=712000&section=&topic=&noscroll=true (10.10.2011).

Ebenen stattfinden. Einerseits müssen bereits die Transportwege gesichert sein, über welche die Daten ausgetauscht werden. Diese Verschlüsselung kann und soll von der DLS selbst geleistet werden. Andererseits müssen auch die zu übertragenden Inhalte selbst verschlüsselt werden. Hierbei ist zu beachten, dass die DLS selbst keinen Zugang zu den Inhalten haben soll, also „blind" im Hinblick auf die übermittelten Daten sein soll. Dies hat zur Konsequenz, dass der Beitrag der DLS zur Inhaltsverschlüsselung beschränkt sein muss, um diese der Datensicherheit dienende Forderung zu erfüllen. Insofern ist maximal vorstellbar, dass im Rahmen eines asynchronen oder hybriden[324] Verschlüsselungsverfahrens jeweils der öffentliche Schlüssel eines Benutzers in der DLS hinterlegt wird.[325]

Schließlich ist aus Datenschutzrechtlicher Sicht von großer Bedeutung, dass alle Auskunftsvorgänge über die DLS protokolliert werden. Diese Protokollierung ist von jener Protokollierung zu unterscheiden, die alle Anbieter bei Zugriffen auf Vorratsdaten in den eigenen Systemen gemäß § 102c Abs. 2 TKG vorzunehmen haben. Die Protokollierung der DLS soll nämlich keinesfalls selbst personenbezogene Daten enthalten, weil ansonsten durch eine weitere (zwischen-)Speicherung der schutzwürdigen Daten, die Gegenstand der Datenauskunft sind, nur das Risiko eines Datenmissbrauchs erhöht und damit der Eingriff in die Grundrechte der Telekommunikationsteilnehmer verstärkt würde. Es geht vielmehr darum, dass die Abwicklung aller Datenauskünfte selbst unveränderlich dokumentiert wird, ohne dabei einen direkten Personenbezug herzustellen. Ein solcher Personenbezug existiert nur bei der internen Zugriffsprotokollierung des Anbieters sowie in der aktenmäßigen Dokumentation einer Datenauskunft auf Seiten der Behörden. Dennoch soll ein Bindeglied zwischen diesen Protokollierungen bestehen, nämlich in Form einer fortlaufenden Nummer die einmalig zu jedem Auskunftsfall automatisch durch die DLS vergeben wird (Unique-ID[326]).

Diese Unique-ID soll den zuständigen Behörden im Rechtsschutz- oder Kontrollfall - und zwar ausschließlich diesen, also der Datenschutzkommission und den Rechtsschutzbeauftragten - erleichtern, den Weg der schutzwürdigen personenbezogenen Daten nachzuvollziehen. Mit der Protokollierung verbunden ist die Funktion der DLS, automatisch eine Statistik über die Datenauskünfte zu erstellen. Im Hinblick auf Vorratsdaten ist eine solche Statistik schon aufgrund der Richtlinie 2006/24/EG jährlich an die EU-Kommission zu liefern. Die automatische Erfassung und Aufbereitung über die DLS bringt eine enorme Aufwandserleichterung, weil diese Daten sonst von allen Anbietern einzeln eingesammelt und danach aufbereitet werden müssten. Darüber hinaus sollten aber nicht Auskünfte betreffend Vorratsdaten sondern auch Betriebsdaten von der DLS-Protokollierung und von der Statistik erfasst werden. Denn abgesehen von dieser unionsrechtlichen Verpflichtung gebieten schon die Grundsätze des DSG 2000, dass ausreichende Vorkehrungen zur Wahrung der datenschutzrechtlichen Verantwortung getroffen werden.

[324] Zur Erklärung siehe oben Kapitel III.1.3.
[325] Für Details zum Thema Verschlüsselung siehe unten Kapitel IV.2.4.
[326] Genaueres zur Funktion der Unique-ID unten in Kapitel IV.2.3.4.

IV.2.2.1.1 LÖSUNGSVORSCHLÄGE FÜR EINE DSVO

Die soeben im Überblick dargestellten Funktionen bzw. die Grundstruktur der DLS könnten legistisch folgendermaßen erfasst werden:[327]

§ 8 Allgemeines

(1) Die Übermittlung der Daten erfolgt über eine zentrale Durchlaufstelle, die das Bundesministerium für Verkehr, Innovation und Technologie bei der Bundesrechenzentrum GmbH einzurichten hat.
(2) Die technische Spezifikation zur Durchlaufstelle hat einen verschlüsselten Übertragungsweg vorzusehen (Transportverschlüsselung).
(3) Zusätzlich ist eine Verschlüsselung der Inhalte sowohl der Anfrage als auch der Beantwortung von Absender zu Empfänger durch asymmetrische Verschlüsselungsverfahren vorzusehen (Inhaltsverschlüsselung). Asymmetrische Verschlüsselungsverfahren können als hybride Verfahren implementiert werden.
(4) Über die Durchlaufstelle werden die Teilnehmer des Datenaustausches über eine fortgeschrittene elektronische Signatur identifiziert und authentifiziert.

§ 9 Durchlaufstelle – Grundstruktur

(1) Die Durchlaufstelle ist ein elektronisches Postfachsystem zur sicheren Abwicklung von Anfragen und Auskünften im Sinne des § 94 Abs. 4 TKG 2003. Alle Beteiligten sind dabei über einen verschlüsselten Übertragungskanal an die Durchlaufstelle angebunden.
(2) Die Durchlaufstelle ist auf eine Weise einzurichten, dass für die Bundesrechenzentrum GmbH als Dienstleister der Durchlaufstelle im Sinne des DSG 2000 ein Zugang zu personenbezogenen Inhalten von Anfragen zu Datenauskünften so wie von deren Beantwortung nicht möglich ist.
(3) Über die Durchlaufstelle werden sowohl Auskünfte über Vorratsdaten als auch Auskünfte über Betriebsdaten abgewickelt. Ausnahmen sind nur in dem von § 3 normierten Ausmaß zulässig. Über die Durchlaufstelle werden alle Auskunftsfälle revisionssicher statistisch erfasst.
(4) In der Spezifikation zur Durchlaufstelle ist vorzusehen, dass die Integrität der Daten sowie die Identität des Senders durch den Empfänger überprüft werden kann (Signatur).

§ 12 Funktionen der Durchlaufstelle im Überblick

(1) Die Durchlaufstelle stellt für die Abwicklung von Auskünften im Sinne des § 94 Abs. 4 TKG 2003 elektronische Postfächer zur Verfügung, die unter Verwendung eines Webservice oder einer Webapplikation zu benutzen sind.
(2) Allen zur Abwicklung von Auskunftsbegehren ermächtigten Dienststellen auf Seiten der berechtigten Behörden sowie allen nach § 102a TKG 2003 speicherpflichtigen Anbietern wird jeweils eine Teilnehmerkennung und ein dazugehöriges Postfach von der Durchlaufstelle zugewiesen. Jeder Benutzer hat nur Zugriff auf das Postfach jenes Teilnehmers (Dienststelle oder Anbieter), dem der Benutzer zugehört.

[327] Die Formulierungen stammen aus der BIM-Datensicherheitsstudie S. 141 ff; diese Vorschläge wurden ohne Änderungen durch das BMVIT in öffentliche Begutachtung geschickt, vgl. dazu den Begutachtungsentwurf im Anhang.

(3) Die Authentifizierung der Benutzer erfolgt durch die Durchlaufstelle gemäß den Vorgaben des § 13.
(4) Die Verschlüsselung des Übertragungsweges ist über die Durchlaufstelle unter Verwendung einer geeigneten Technologie entsprechend dem Stand der Technik sicherzustellen.
(5) Zur Verschlüsselung der Anfragen und der Auskünfte verwaltet die Durchlaufstelle die öffentlichen Schlüssel aller ermächtigten Dienststellen und aller gemäß § 102a TKG 2003 speicherpflichtigen Anbieter. Nur authentifizierte Benutzer können den öffentlichen Schlüssel ihrer Organisation bei der Durchlaufstelle hinterlegen. Jeder Benutzer holt vor dem Absenden seiner Nachricht den öffentlichen Schlüssel des Empfängers zur Verschlüsselung des Inhalts bei der Durchlaufstelle ab.
(6) Alle Auskunftsfälle sind in der Durchlaufstelle revisionssicher zu protokollieren. Der Umfang dieser Protokollierung wird in § 22 geregelt.

§ 17 Postfächer und Zustellung

(1) Ein Auskunftsbegehren eines berechtigten Benutzers auf Behördenseite wird in das Postfach des über die Durchlaufstelle ausgewählten Anbieters zugestellt. Die Durchlaufstelle ermöglicht die Auswahl mehrerer Anbieter. Die Spezifikation zur Durchlaufstelle hat ein System der Notifikation über den Eingang eines Auskunftsbegehrens in das Postfach des Anbieters vorzusehen. Die Abholung des Auskunftsbegehrens erfolgt manuell durch Zugriff auf das Postfach des Anbieters nach entsprechender Authentifizierung des Benutzers. Eine Abholung des Auskunftsbegehrens per Webservice kann in der Spezifikation zur Durchlaufstelle vorgesehen werden.
(2) In der Spezifikation zur Durchlaufstelle muss sichergestellt werden, dass eine Beantwortung bereits vor der Übermittlung der Anfrage via Durchlaufstelle durchgeführt werden kann. Dazu wird ein anbieter-spezifischer Bereich von Referenzen (Unique-ID) definiert, der vom Anbieter in aufsteigender Reihenfolge vergeben wird. Gemäß § 3 Abs. 2 ist die nachträgliche Dokumentation der Anfrage über die Durchlaufstelle zu gewährleisten, wobei die Behörde die anbieter-spezifische Referenz anzugeben hat, die bei der Beantwortung verwendet wurde.
(3) Die Beantwortung eines Auskunftsbegehrens durch den Anbieter erfolgt durch Übermittlung einer verschlüsselten CSV-Datei gemäß der Schnittstellenspezifikation in der Anlage zu dieser Verordnung. Die Durchlaufstelle stellt automatisch sicher, dass die Antwort in das richtige Postfach der anfragenden Dienststelle zugestellt wird. In den Fällen des Abs. 2 muss die adressierte Dienststelle jedoch durch individuelle Auswahl über die Durchlaufstelle bestimmt werden.
(4) Die Durchlaufstelle versendet nach Eingang der Antwort in das Postfach der anfragenden Dienststelle eine Benachrichtigung über die Hinterlegung der Antwort an die Dienststelle.
(5) Die Abholung der Auskunft erfolgt manuell durch Zugriff auf das Postfach der Dienststelle nach entsprechender Authentifizierung des Benutzers. Eine Abholung der Auskunft per Webservice kann in der Spezifikation zur Durchlaufstelle vorgesehen werden.

IV.2.2.2 SOLL DIE DLS DETAILLIERTE FORMULARE FÜR ALLE ANFRAGEN VORGEBEN?

Für Anfragen nach dem SPG ist schon bisher eine Verwendung von einheitlichen Formularen gemäß einem Erlass des BIM vorgesehen[328]. Zu Anfragen nach der StPO gibt es zwar Formulare, denen jedoch kein zwingender Erlass zugrunde liegt und die in der Praxis auch nicht durchgehend verwendet werden.

Im Rahmen der BIM-Datensicherheitsstudie wurde in den Round Table Diskussionen darüber gesprochen, inwiefern über die DLS auch die jeweiligen Anfrageformulare für Datenauskünfte nach der StPO sowie nach dem SPG standardisiert werden sollten.[329] Für den Bereich des SPG wäre dies aufgrund der bereits bestehenden einheitlichen Formulare mit überschaubarem Aufwand zu erreichen. Etwas intensiver würde sich der Implementierungsprozess für den StPO-Bereich gestalten, weil hier zuerst eine bundesweite Vereinheitlichung festgelegt werden müsste. Anfragen nach der StPO enthalten nämlich als Beilage die Anordnung des Staatsanwalts mit der prosaischen Beschreibung des Auskunftsbegehrens, weshalb den Befugnissen nach der StPO durch eine Formalisierung nur eingeschränkt Rechnung getragen werden kann. Jedenfalls wurde auch seitens des BM.I und des BMJ das klare mittelfristige Ziel formuliert, für alle Datenanfragen auch im Interesse der Behörden an einer einheitlichen und geordneten Abwicklung eine Formalisierung über Eingabemasken anzustreben. Dabei sollte zugleich verhindert werden, dass Anbieter durch den Vergleich einer allenfalls per Webmaske ausgeführten Anordnung mit dem beiliegenden Original der StA Anordnung einen erhöhten Aufwand haben. Der wesentlichste Faktor bei dieser Frage ist jedoch nach aktuellem Stand der große Zeitdruck für die Einrichtung der DLS, weil mit 1.4.2012 sämtliche Bestimmungen zur Vorratsdatenspeicherung nach der Legisvakanz in Kraft treten und das System bis dahin den operativen Betrieb aufnehmen muss. Dass die angestrebte Vereinheitlichung daher zeitgerecht zu bewerkstelligen ist, wurde von allen Beteiligten ernsthaft angezweifelt. Für die erstmalige Implementierung der Durchlaufstelle bedeutet dies daher, dass vorerst jedenfalls StPO-Anordnungen wie bisher übermittelt werden können müssen, ohne dabei an bestimmte online-Formulare über die Webmaske gebunden zu sein.[330]

Diesem in der Praxis nicht zu ignorierenden Zeitdruck[331] Tribut zollend wurde daher im Zuge der BIM-Datensicherheitsstudie vorgeschlagen, dass bei der Übermittlung eines Auskunftsbegehrens via DLS zumindest auszuwählen ist, auf welcher Rechtsgrundlage eine Anordnung zur Datenauskunft ergeht. Dies dient der statistischen Erfassung über die DLS und beinhaltet keine Determinierung der

---

[328] Erlass des BM.I zu § 53 Abs 3a und 3b SPG, GZ 94762_101-GD_08 (abrufbar auf der Web-Seite der WKO unter http://portal.wko.at/wk/format_detail.wk?AngID=1&StID=386310&DstID=5000 (10.10.2011); vgl. dazu bereits oben Kapitel II.1.4.4.3.

[329] Siehe dazu die Zusammenfassung der Diskussion im 3. Round Table in der BIM-Datensicherheitsstudie S. 105 ff.

[330] Siehe dazu BIM-Datensicherheitsstudie S. 108 f.

[331] Der Druck geht dabei insbesondere vom Unionsrecht aus, zumal Österreich bereits durch den EuGH in einem Vertragsverletzungsverfahren mit Urteil vom 29.07.2010, C 189/09 Kommission/Österreich wegen Verletzung des EU Vertrages durch die Nichtumsetzung der Vorratsdatenspeicherungsrichtlinie 2006/24/EG verurteilt wurde und die EU-Kommission Österreich bereits die vorbereitenden Schritte für ein Bußgeldverfahren eingeleitet hat, für den Fall dass die endgültige Umsetzung nicht entsprechend rasch erfolgen sollte; siehe dazu Abl. C 246/8 vom 11.09.2010 unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:246:0008:0008:DE:PDF (10.10.2011); vgl. auch die Kommentierung der Verurteilung im bekannten Web-Blog von Hans Peter Lehofer, http://blog.lehofer.at/2010/08/aktives-abwarten-vorratsdatenspeicherun.html (10.10.2011).

Formulare oder Webmasken, die bei den Behörden für die Anordnungen verwendet werden. Eine Determinierung ergibt sich allerdings aus der Spezifikation der Felder der CSV-Datei gemäß der Branchenempfehlung EP020, die in den DSVO-Entwurf übernommen wurde.[332] Die Formulare, die für die Abfragen verwendet werden, müssen daher im Hinblick auf die Vorgaben zur CSV-Datei adaptiert werden. Die Formulare sind zunächst als Dateianhang verschlüsselt an die an die Anbieter via DLS zu übermitteln. Eine Automatisierung durch webbasierte Formulare in der DLS ist in weiteren Schritten möglich und würde eine Verarbeitung der Daten erleichtern.

IV.2.2.2.1 Lösungsvorschlag für eine DSVO

Im Rahmen der BIM-Datensicherheitsstudie wurde entsprechend den obigen Ausführungen folgender Formulierungsvorschlag unterbreitet:

§ 19 Eingabefelder

(1) Über die Durchlaufstelle ist bei jeder Anfrage auszuwählen, ob es sich um ein Auskunftsbegehren nach § 53 Abs. 3a SPG, nach § 53 Abs. 3b SPG, nach § 76a StPO, nach § 135 Abs. 2 StPO oder nach § 135 Abs. 2a StPO handelt. Eine allfällige Eingabemaske auf Behördenseite kann unter Beachtung der Schnittstellenspezifikation der Anlage frei gestaltet werden.
(2) Dies gilt sinngemäß auch für eine allfällige Eingabemaske auf Anbieterseite. Insbesondere besteht keine Verpflichtung zur automatisierten Befüllung der CSV-Datei.

Dieser Vorschlag wurde für den Begutachtungsentwurf des BMVIT wie folgt abgeändert:

Eingabefelder

§ 19. (1) Über die Durchlaufstelle ist bei jeder Anfrage auszuwählen, ob es sich um ein Auskunftsbegehren nach § 53 Abs. 3a SPG, nach § 53 Abs. 3b SPG, nach § 76a StPO, nach § 135 Abs. 2 StPO oder nach § 135 Abs. 2a StPO oder um eine Stammdatenauskunft nach § 21 handelt. In der Durchlaufstelle ist ein Feld für den Eintrag der einer Anordnung zu Grunde liegenden strafbaren Handlung für die Protokollierung gemäß § 7 Abs. 3 Z 8 vorzusehen. Eine allfällige Eingabemaske auf Behördenseite kann unter Beachtung der Schnittstellenspezifikation in der Anlage frei gestaltet werden.

(2) Dies gilt sinngemäß auch für eine allfällige Eingabemaske auf Anbieterseite. Insbesondere besteht keine Verpflichtung zur automatisierten Befüllung der CSV-Datei.

Die erste Änderung bezieht sich darauf, dass der Entwurf auch optional Stammdatenauskünfte über die DLS zulässt (dazu sogleich) und auch diese Art der Auskunft explizit ausgewiesen werden sollte. Die zweite Änderung im Begutachtungsentwurf wurde vom BMJ angeregt und bezieht sich auf ein Eingabefeld für die Dokumentation der einer Anfrage zugrunde liegenden strafbaren Handlung. Der Sinn dieser Ergänzung besteht darin, dass diese Informationen in der Statistik angeführt werden muss, welche die Republik Österreich gemäß § 10 RL 2006/24/EG jährlich an die EU-Kommission zu liefern hat. Beides wurde im Entwurf im Rahmen der BIM-Datensicherheitsstudie nicht bewusst ausgelassen sondern schlicht übersehen, die Änderungen werden daher hier befürwortet.

[332] Siehe dazu unten Kapitel IV.2.5 sowie den Begutachtungsentwurf zur DSVO im Anhang.

IV.2.2.3 STAMMDATENAUSKUNFT VIA DLS ALS OPTION FÜR DIE ANBIETER?

In den Diskussionen zur DLS im Rahmen der BIM-Datensicherheitsstudie wurde die Möglichkeit einer elektronischen Stammdatenauskunft im Bereich der Telefon-Anbieter als optionale Variante besprochen.[333] Dabei ging es aus Sicht des BMI nicht darum, eine unmittelbare Schnittstelle zur Kundendatenbank des Anbieters herzustellen. Vielmehr wurde der Wunsch nach einem elektronischen Hin- und Rückkanal geäußert, der zu einer möglichst raschen Abwicklung führen soll. In wie weit ein Anbieter solche Auskunftsvorgänge automatisiert, soll dem jeweiligen Anbieter überlassen bleiben - insbesondere im Hinblick auf kleine Anbieter, die nur wenig betroffen sind - solange die Auskunft in vertretbarer Zeit abgewickelt werden kann. Große Anbieter könnten durch eine (Teil-)Automatisierung in eigener Verantwortung die Auskünfte optimieren. Wesentlich ist, dass eine Anbindung an ein elektronisches System für Stammdatenauskünfte über die DLS nicht verpflichtend als ausschließliche Übermittlungsvariante für alle Anbieter eingerichtet werden muss. Durch die DSVO soll lediglich die optionale Möglichkeit einer solchen Anbindung normiert werden. Wenn zumindest die großen (insbesondere Mobilfunk-) Anbieter sich anschließen, würde der Zweck bereits erfüllt.[334]

Zum besseren Verständnis der Bedeutung solcher Stammdatenauskünfte hier eine kurze Erläuterung zur Praxisrelevanz von Stammdatenauskünften. In der bisherigen Praxis werden vor einer Anordnung zu einer Verkehrsdatenauskunft zunächst zu einer (oder mehreren) bestimmten Nummer Stammdatenauskünfte begehrt, wobei diese Auskunftsbegehren an alle in Frage kommenden Anbieter gerichtet werden, wobei im Bereich des Mobilfunks die Zahl der Anbieter überschaubar ist. Durch die Antworten erfährt die Behörde, für welche Zeiträume bei welchem Anbieter Verkehrsdaten vorhanden sein könnten und kann das Auskunftsbegehren zielgerichtet stellen. Die Stammdatenauskunft wird in der Praxis auch deshalb regelmäßig vorgelagert, weil die Kriminalpolizei damit bereits einen ersten Filter setzt, welche Teilnehmeranschlüsse ermittlungsrelevant sein könnten. Als Antwort werden Stammdaten, der entsprechende Zeitraum und die Information „aktiv“ oder „inaktiv“ übermittelt. Es können auch bei einem Anbieter zur gleichen Rufnummer während der letzten 6 Monate mehrere Stammdatensätze anfallen (z.B. bei einer Übertragung der Rufnummer).

Die Praxis der vorgelagerten Stammdatenauskünfte würde auch im System der DLS weiterhin relevant bleiben. Um solche Stammdatenabfragen zu erleichtern bzw. zu beschleunigen könnte eine DSVO beinhalten, dass Anbieter freiwillig für eine Abwicklung von Stammdaten-Auskünften via DLS optieren können. Eine Anbindung an ein elektronisches System für Stammdatenauskünfte über die DLS soll allerdings nicht verpflichtend als ausschließliche Übermittlungsvariante für alle Anbieter eingerichtet werden. Aus dem Vorschlag soll auch keine indirekte Verpflichtung zur Optierung für eine elektronische Stammdatenauskunft erwachsen, etwa indem die Forderung nach einer Auskunft „in vertretbarer Zeit“ an der Zeitspanne für elektronische Stammdatenauskünfte gemessen wird.[335] Außerdem soll keine unmittelbare Schnittstelle zur Kundendatenbank des Anbieters hergestellt werden, diese soll vielmehr über die DLS mediatisiert werden. Es soll lediglich einen elektronischen Hin- und Rückkanal geben, der zu einer möglichst raschen Abwicklung führt. In wie weit ein Anbieter

---

[333] Siehe die Zusammenfassung der Diskussion beim 2. Round Table, BIM-Datensicherheitsstudie S. 100

[334] Vgl. die Zusammenfassung der Diskussion beim 6. Round Table, BIM-Datensicherheitsstudie S. 132 f.

[335] Siehe die Formulierung entsprechender Bedenken in der Stellungnahme der ISPA im Begutachtungsverfahren, http://www.ispa.at/stellungnahmen/bmvit-konsultation-datensicherheitsverordung/.

solche Auskunftsvorgänge automatisiert, soll dem jeweiligen Anbieter überlassen bleiben - insbesondere im Hinblick auf kleine Anbieter, die nur wenig betroffen sind - solange die Auskunft in vertretbarer Zeit abgewickelt werden kann. Große Anbieter könnten durch eine (Teil-) Automatisierung in eigener Verantwortung die Auskünfte optimieren.[336]

IV.2.2.3.1 LÖSUNGSVORSCHLÄGE FÜR EINE DSVO

Legistisch könnte eine optionale Stammdatenauskunft im obigen Sinne folgendermaßen umgesetzt werden:[337]

§ 21 Optionale Stammdatenauskünfte über die Durchlaufstelle

(1) Anbieter können optieren, Stammdatenauskünfte über die Durchlaufstelle abzuwickeln. Die technischen Details solcher Auskünfte sind in der Spezifiktion zur Durchlaufstelle zu regeln.
(2) Der Anbieter ist dabei keinesfalls verpflichtet, die Stammdatenauswertung über eine Schnittstelle automatisiert verfügbar zu machen.

Dieser Vorschlag wurde für den Begutachtungsentwurf des BMVIT wie folgt abgeändert:

Optionale Stammdatenauskünfte über die Durchlaufstelle

§ 21. Anbieter und zugangsberechtigte Behörden können jeweils im Einvernehmen optieren, Stammdatenauskünfte über die Durchlaufstelle abzuwickeln. Die technischen Details solcher Auskünfte sind in der Spezifiktion zur Durchlaufstelle zu regeln.

Die erste Änderung bewirkt, dass nicht nur Anbieter sondern auch Behörden die Möglichkeit offen bleibt, für eine elektronische Stammdatenauskunft zu optieren. Das ist im Hinblick auf die freiwillige Natur dieser Möglichkeit nur konsequent und daher nicht zu beanstanden. Die zweite Änderung sieht eine vollständige Streichung des ursprünglich vorgeschlagenen Absatz 2 vor. Daraus ergibt sich zwar nicht, dass - im Falle eines Opt-in - eine automatisierte Schnittstelle zur Kundendatenbank des Anbieters zu schaffen ist. Allerdings wäre eine solche Möglichkeit datenschutzrechtlich äußerst bedenklich, weshalb die Streichung dieses Absatzes im Sinne der Rechtssicherheit zu kritisieren ist.

Angesichts des knappen Zeitplans für eine allfällige erste Implementierung des Systems der DLS ist zudem denkbar, diese Option an die Bedingung zu knüpfen, dass eine derartige Funktionalität von der DLS überhaupt zur Verfügung gestellt wird. Dadurch könnte man eine solche Funktionalität erst in einer 2. Phase (nach dem 1.4.2012) mit weniger Zeitdruck implementieren. In diesem Fall könnte man an den ersten Satz von § 21 anfügen: „ , sofern die Durchlaufstelle eine solche Funktionalität anbietet."

Seitens der Technischen Universität Wien wurde im Begutachtungsverfahren außerdem zu bedenken gegeben, dass die Formulierung nicht unproblematisch ist, wonach eine automatische Stammdatenabfrage nur im Einvernehmen zwischen Anbietern und Behörden erfolgen kann. Dies würde nämlich bedeuten, dass entsprechend viele bilaterale Verträge erforderlich sind. Die DLS

[336] Vgl. hierzu die Erläuterungen zu § 21 DSVO-Entwurf in der BIM-Datensicherheitsstudie S. 168 f.
[337] Siehe § 21 DSVO-Entwurf in der BIM-Datensicherheitsstudie S. 145.

müsste sodann all diese Vereinbarungen administrieren, da davon abhängig ist, ob die Oberfläche für eine abfragende Behörde und abhängig von dem vom Benutzer gewählten Anbieter überhaupt die entsprechende Auswahlgrundlage zur Stammdatenabfrage angezeigt wird.[338] Es erscheint daher sinnvoll, es dem Anbieter zu überlassen, ob dieser eine automatisierte Stammdatenabfrage „anbietet" und dies der DLS (besser gesagt dem BMVIT als verantwortliche Behörde) bekannt gibt. Der Behörde steht auch in diesem Fall noch immer frei, für eine Stammdatenabfrage den herkömmlichen Weg zu wählen. Diese Information wäre auch einfacher von der DLS zu administrieren, da nicht jeder einzelne bilaterale Vertrag berücksichtigt werden müsste, sondern nur bis zu (derzeit) maximal ca. 200 „Einwilligungen" der Anbieter. Die Abfragemaske seitens der Behörden könnte sich dann so gestalten, dass der Benutzer die Rechtsgrundlage für Stammdatenabfrage wählt und automatisiert auf die Liste jener Anbieter eingeschränkt wird, welche für eine automatische Stammdatenabfrage über die DLS optiert haben.

IV.2.3 Autorisierung, Identifizierung und Authentifizierung

IV.2.3.1 Ausgangslage und Probleme im status quo

In der bisherigen Praxis gestalten sich die von § 94 Abs. 4 TKG erfassten Datenauskünfte sehr uneinheitlich. Seitens des Bundeskriminalamts wurde in den Diskussionen angemerkt, dass bereits heute zwischen Bundeskriminalamt und A1 Telekom Austria ein verschlüsselter E-Mail Kanal zum Datenaustausch existiert, wobei zur Verschlüsselung die TLS-Technologie[339] zum Einsatz kommt.[340] Verschlüsselte elektronische Anfragen und Auskünfte stellen bisher aber nicht den Regelfall dar. So werden derzeit die meisten Datenauskünfte über unverschlüsselte E-Mail, Fax oder telefonisch abgewickelt.[341] Da die Sicherheitsbehörden teilweise gar nicht über die technischen Voraussetzungen verfügen, um z.B. verschlüsselte E-Mail Nachrichten zu entschlüsseln, ist eine Übertragung auf elektronischem Weg oft nicht möglich. In diesen Fällen erfolgt die Datenauskunft per Fax bzw. durch Übergabe von Datenträgern. Letztere Methode kommt derzeit vor allem bei großen Datenmengen zum Einsatz, wenn das Gegenüber keine Verschlüsselungstechnik unterstützt und der Anbieter nicht per Fax übermittelt.[342] Schwierig gestaltet sich die Kooperation mit den Behörden bei Datenauskünften bisher vor allem im Bereich der StPO. Die Rechtsansichten divergieren nicht selten, teilweise werden Beschlüsse seitens der Staatsanwaltschaft nicht übermittelt oder Hausdurchsuchungen angedroht, sollte ein Anbieter die Auskunft verweigern. Dabei ist auch im StPO-Anwendungsbereich die Kontaktstelle zum Datenaustausch immer eine Sicherheitsbehörde, die im Auftrag der Strafjustiz die Abwicklung vollzieht.[343] Im Hinblick auf die bestehenden

---

[338] Mit anderen Worten: Darf die konkrete Behörde für den konkret gewählten Anbieter eine solche Abfrage durchführen?

[339] Vgl. dazu zB die Ausführungen auf der Website des Microsoft online-Journals TechNet, http://technet.microsoft.com/de-de/library/cc759573%28WS.10%29.aspx (11.10.2011).

[340] Siehe die Zusammenfassung der Diskussion beim 1. Round Table, BIM-Datensicherheitsstudie S. 92.

[341] Zusammenfassung der Diskussion beim 1. Round Table, BIM-Datensicherheitsstudie S. 96.

[342] Diese Informationen über die derzeitige stammen aus den Diskussionsrunden mit der österreichischen Telekomwirtschaft im Rahmen des AK-TK, wobei die Protokolle zu den Diskussionen nicht öffentlich zugänglich sind.

[343] Zur rechtlichen Konstruktion und zur Abgrenzung der Anwendungsbereiche von SPG und StPO siehe oben Kapitel II.1.4.4.1.

Schwierigkeiten herrschte bereits beim 1. Round Table Einigkeit unter allen beteiligten Stellen, dass eine Änderung der bisherigen Auskunftspraxis dringend notwendig ist.[344] Abgesehen von den rein praktischen Abwicklungsschwierigkeiten ist eine ungesicherte Datenübermittlung per E-Mail, Fax oder telefonisch ohne jeden Zweifel keine sichere Form des Austausches schutzwürdiger personenbezogener Daten und damit schon aus der Gewährleistungspflicht[345] zum Datenschutzgrundrecht nicht länger hinzunehmen.

IV.2.3.2 WER SOLL ABFRAGEBERECHTIGT SEIN?

IV.2.3.2.1 ANBINDUNG DER BEHÖRDEN AN DIE DLS

Die Anzahl der anfrageberechtigten Dienststellen auf Seiten der Behörden wurde im Rahmen der BIM-Datensicherheitsstudie mehrfach im Hinblick auf die derzeitige Praxis diskutiert. Hierzu wurde vom BMI auch das Prinzip der „OSE" (zentrale interne Stellen, an welche die Anfrage zunächst polizeiintern geleitet werden) vorgestellt, welches jedoch nur verfügbar ist, sofern diese Stelle besetzt ist, was am Wochenende offenbar nicht der Fall ist. Nach Ausführungen der Anbieter kommen teilweise in der Praxis dennoch Anfragen direkt von den Polizeiinspektionen (PI). Die Anbieter sind in so einem Fall bisher gesetzlich auch zur Auskunft verpflichtet, weil die Beschränkung auf 12 berechtigte Stellen nur durch internen Erlass des BMI[346] geregelt, aber nach außen nicht verbindlich ist.

Der Wunsch nach einer Reduktion der abfrageberechtigten Stellen zur Vereinfachung der Abläufe wurde in der Diskussion auch von Seiten des Bundeskriminalamts geäußert.[347] Die Autorisierung auf der Seite der abfrageberechtigten Stellen liegt aber im Regelungsbereich des SPG bzw. der StPO und damit in der Verantwortung des BM.I und des BMJ. Da eine Einschränkung auf gesetzlicher Ebene derzeit politisch unwahrscheinlich ist, sollte die Einschränkung zumindest über eine DSVO erfolgen, in dem die Sicherheitsbehörden verpflichtet werden, eine endliche Zahl an abfrageberechtigten Stellen bekannt zu geben, welche sodann an die DLS angebunden werden.

Eine andere Form der Anbindung betrifft den Zugang zu den Protokolldaten und der Statistik der DLS. Zur Frage, welche Stellen im Hinblick auf einen solchen Zugang and die DLS angebunden werden sollen, siehe die ausführliche Darstellung unten in Kapitel IV.2.8.2.5.

---

[344] Zusammenfassung der Diskussion beim 1. Round Table, BIM-Datensicherheitsstudie S. 96.
[345] Siehe dazu die grundrechtsdogmatischen Ausführungen oben in Kapitel II.1.1.3.3.
[346] Erlass des BM.I zu § 53 Abs 3a und 3b SPG, GZ 94762_101-GD_08 (abrufbar auf der Web-Seite der WKO unter http://portal.wko.at/wk/format_detail.wk?AngID=1&StID=386310&DstID=5000 (10.10.2011); vgl. dazu bereits oben Kapitel II.1.4.4.3.
[347] Zusammenfassung der Diskussion beim 1. Round Table, BIM-Datensicherheitsstudie S. 95.

IV.2.3.2.1.1 LÖSUNGSVORSCHLÄGE FÜR EINE DSVO

Die soeben ausgeführten Grundsätze über die Anbindung von Behörden an die DLS könnten legistisch folgendermaßen erfasst werden:[348]

§ 14 Zugangsberechtigte Behörden

(1) Das Bundesministerium für Inneres sowie das Bundesministerium für Justiz geben der Bundesrechenzentrum GmbH für die Spezifikation der Durchlaufstelle eine begrenzte Anzahl von Dienststellen bekannt, die als Teilnehmer der Durchlaufstelle zur Abwicklung von Auskunftsbegehren berechtigt sind.
(2) Nachträgliche Änderungen der nach Abs. 1 bekannt gegebenen Dienststellen sind durch das Bundesministerium für Inneres sowie das Bundesministerium für Justiz der Bundesrechenzentrum GmbH für die Veranlassung der entsprechenden Änderungen in der Durchlaufstelle bekannt zu geben.
(3) Für die Datenschutzkommission, den Datenschutzrat und das Bundesministerium für Justiz sowie für die Rechtsschutzbeauftragten beim Bundesminister für Justiz und beim Bundesminister für Inneres ist in der Spezifikation zur Durchlaufstelle jeweils ein Zugang vorzusehen, der entsprechend der jeweiligen Aufgabe dieser Behörden einen Zugang zu den Protokolldaten gemäß § 22 Abs. 4 oder zur Statistik gemäß § 23 Abs. 3 ermöglicht.

Im Zuge des Begutachtungsverfahrens wurde vom Bundeskanzleramt-Verfassungsdienst Kritik an diesem - für den Begutachtungsentwurf unverändert übernommenen - Regelungsvorschlag geübt.[349] Die Kritik bezieht sich darauf, dass die Protokolldaten der DLS sehr wohl einen Personenbezug zulassen würden, nämlich insofern, als über die Unique-ID nachverfolgbar sei, von welchem Anbieter eine Datenauskunft an die Behörden gegeben wurde. Weil die Anbieter als juristische Personen ebenfalls vom Schutzbereich des Datenschutzgrundrechts gemäß § 1 DSG erfasst seien, erfordere der online-Zugriff auf die Protokolldaten der DLS eine ausdrückliche gesetzliche Grundlage im TKG.

Diese Kritik ist insofern ernst zu nehmen, als der Bezug zu einem bestimmten Anbieter tatsächlich eine schutzwürdige Information darstellen kann. Nämlich insofern, als diese Information wettbewerbsrelevant sein könnte. Man stelle sich etwa vor, welche Auswirkungen eine durch ein Medium veröffentlichte „Hitliste“ der Datenauskünfte durch heimische Telekom-Anbieter auf das Kundenverhalten und damit den Markt haben könnte.

Nicht geteilt wird hier jedoch die Ansicht, es mangle an einer hinreichend bestimmten gesetzlichen Grundlage. Die DLS wird in der Verantwortung des BMVIT betrieben, welches nach § 113 Abs. 5 TKG die oberste Fernmeldebehörde ist. In dieser Eigenschaft obliegt dem BMVIT gemäß § 18 Abs. 3 Z 3 KommAustria Gesetz auch die Aufsicht über die RTR-GmbH[350], soweit es sich um fachliche und unmittelbar zusammenhängende organisatorische Angelegenheiten im Telekommunikations- und Postbereich handelt. Die RTR-GmbH wiederum nimmt die Aufgaben der Regulierungsbehörde nach

[348] Die Formulierungen stammen aus der BIM-Datensicherheitsstudie S. 143; diese Vorschläge wurden ohne Änderungen durch das BMVIT in öffentliche Begutachtung geschickt, vgl. dazu den Begutachtungsentwurf im Anhang.
[349] Die an das BMVIT gerichteten Stellungnahmen im Begutachtungsverfahren wurden nicht veröffentlicht und können daher nicht mit Fundstelle zitiert werden. Diese wurden dem Autor jedoch zum Zwecke der Verarbeitung im Rahmen dieser Dissertation vom BMVIT zur Verfügung gestellt.
[350] Rundfunk und Telekom Regulierungs-GmbH“ (RTR-GmbH), eingerichtet gemäß § 16 KommAustria Gesetz.

dem Telekommunikationsgesetz wahr.[351] Insofern erscheint es nicht notwendig, dass für das BMVIT als Auftraggeberin der DLS eine zusätzliche gesetzliche Grundlage geschaffen werden muss, die das BMVIT berechtigt, wettbewerbsrelevante Informationen im eben beschriebenen Sinne einzusehen.

Im Hinblick auf den Zugang der Datenschutzkommission sowie der Rechtsschutzbeauftragten des BM.I und des BMJ ist die jeweilige gesetzliche Aufgabe - wie soeben in Kapitel IV.2.3.2.1 beschrieben - klar definiert, die diese Stellen berechtigen, die Zuordnung eines Anbieters zu einem bestimmten Auskunftsfall zu erheben. Als gesetzliche Grundlage, die die Verwendung von Daten durch staatliche Behörden rechtfertigt, kommen primär Gesetze in Betracht, in denen die Verwendung von Daten für einen bestimmten Zweck ausdrücklich geregelt ist. Nach der jüngeren Rechtsprechung der Datenschutzkommission können aber auch die in Betracht kommenden (einfachgesetzlichen) Regelungen der §§ 8 und 9 DSG unter Umständen Grundlage für die Verwendung von Daten durch staatliche Behörden sein[352], nämlich dann, wenn die Datenverwendung selbst eine notwendige Voraussetzung für die Erfüllung der jeweiligen gesetzlichen Aufgabe darstellt, aber dennoch im Gesetz nicht ausdrücklich genannt ist. Im Hinblick auf diese ständige Rechtssprechung der Datenschutzkommission erscheint eine weitere ausdrückliche gesetzliche Normierung des Zugangs zu den Protokolldaten verzichtbar.

Um der Kritik des BKA-VD Rechnung zu tragen, sollte aber der Zugang zu den Protokolldaten technisch so ausgestaltet sein, dass die Anbieterzuordnung sowie die Unique-ID auch für diese Kontrollinstanzen nur dann ersichtlich sind, wenn diese ihrerseits eine bestimmte Geschäftszahl zu deren Prüftätigkeit angeben. Klargestellt sollte in Absatz 3 außerdem werden, dass der Datenschutzrat ausschließlich Zugang zur Statistik haben soll, nicht jedoch zu den sonstigen Protokolldaten der DLS und insbesondere nicht zur Unique-ID und zur Anbieter-Zuordnung.[353]

IV.2.3.2.1.2 Anbindung der Anbieter an die DLS

Ebenfalls zu klären ist die Frage, welche Anbieter an die DLS zum Zwecke einer sicheren Datenübermittlung im Falle eines behördlichen Auskunftsbegehrens angebunden werden sollten. Ein erster Anhaltspunkt dafür bietet § 102a Abs. 6 TKG: „Die Speicherpflicht nach Abs. 1 besteht nicht für solche Anbieter, deren Unternehmen nicht der Verpflichtung zur Entrichtung des Finanzierungsbeitrages gemäß § 34 KommAustriaG unterliegen." Mit dieser Ausnahmeregelung sollen Anbieter ausgenommen werden, deren Größe im Hinblick auf Umsatz und Kundenzahl so gering erscheint, dass eine Pflicht zur Vorratsdatenspeicherung diese Unternehmen unverhältnismäßig hart treffen würde. Sog. „kleine Anbieter" sind daher nicht von der Vorratsdatenspeicherung betroffen.[354] Das hat zugleich den praktischen Vorteil, das jeder Anbieter eine gewisse Rechtssicherheit zur Frage vorfindet, ob er nun grundsätzlich überhaupt zur Vorratsdatenspeicherung verpflichtet ist. Diese Pflicht besteht grundsätzlich nämlich nur dann, wenn

[351] Vgl. dazu die Definition der Aufgaben gemäß § 17 KommAustriaG sowie die Beschreibung der Aufgaben auf der Website der RTR-GmbH, http://www.signatur.rtr.at/de/supervision/tkc.html.
[352] Vgl etwa K121.261/0024-DSK/2007.
[353] Vgl. dazu die oben formulierte Kritik zu § 102c Abs. 4 TKG in Kapitel IV.2.3.2.1.
[354] Vgl. dazu die EB der RV zu § 102a Abs. 6 TKG, BlgNR 1074. XXIV. GP.

die RTR-GmbH einem Anbieter bescheidmäßig die Beitragspflicht gemäß § 34 KommAustriaG vorgeschrieben hat. Nach Auskunft der RTR-GmbH sind dies in Österreich aktuell ca 200 Anbieter.[355]

Die zur Vorratsdatenspeicherung verpflichteten Anbieter sind gemäß § 94 Abs. 4 TKG jedenfalls an das System der DLS anzubinden, der dazu normiert: „Die Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, einschließlich der Übermittlung von Vorratsdaten, nach den Bestimmungen der StPO sowie des SPG, hat unter Verwendung einer Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt, zu erfolgen. Die Daten sind unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie als "Comma-Separated Value (CSV)" - Dateiformat zu übermitteln. (…)"

Allerdings bedeutet die Ausnahme von der Vorratsdatenspeicherpflicht gemäß § 102a TKG nicht automatisch, dass kleinere Anbieter nicht unter Umständen über Daten verfügen könnten, die Gegenstand eines behördlichen Auskunftsbegehrens werden. Es kann schließlich sein, dass ein solcher kleiner Anbieter noch aus betrieblichen Gründen Daten gespeichert hat, die von Ermittlern nach SPG oder StPO begehrt werden. Natürlich ist die Wahrscheinlichkeit einer solchen Anfrage viel geringer als für größere Anbieter, auszuschließen ist der Fall aber sicher nicht. Die Frage ist daher, ob aus § 94 Abs. 4 TKG resultiert, dass alle Anbieter öffentlicher Kommunikationsdienste an die DLS angebunden werden müssten, unabhängig davon, ob sie der Pflicht zur Vorratsdatenspeicherung unterliegen oder nicht.

Dass § 94 Abs. 4 TKG die „Verwendung einer Übertragungstechnologie fordert, welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt", heißt noch nicht zwingend, dass eine solche Technologie nur mit einem einzigen System realisiert werden darf. Das soll im Umkehrschluss jedoch nicht bedeuten, dass neben dem System der DLS noch andere, parallele Wege zur Abwicklung von Datenauskünften offen stehen sollen. Wenn ein Anbieter an die DLS angebunden ist, muss die Abwicklung auch zwingend über die DLS erfolgen - abgesehen von den in § 94 Abs. 4 ausdrücklich normierten Ausnahmen.[356] Im Sinne der schon zur Vorratsspeicherpflicht argumentierten Verhältnismäßigkeit erscheint es aber überschießend, auch alle nicht speicherpflichtigen, „kleinen Anbieter" in dieses System einzubinden. Der administrative und technische Aufwand stünde dabei sowohl für diese Anbieter als auch für den Staat in keinem angemessenen Verhältnis zum zu erwartenden Nutzen. Vielmehr sollte für den Fall, dass tatsächlich ein solcher Anbieter von einem Auskunftsbegehren betroffen ist, eine ad hoc Lösung gefunden werden, die den Anforderungen des § 94 Abs. 4 TKG auch ohne Abwicklung über die DLS gerecht zu werden vermag. Beispielsweise wäre in so einem Fall denkbar, dass ein Beamte der einem solchen Anbieter nächstgelegenen Polizeiinspektion persönlich vor Ort erscheint und die Daten auf einen - von der Behörde zur Verfügung zu stellenden - Datenträger speichern lässt. Die Daten könnten dann in der Folge über eine sichere polizei-interne Datenverbindung an die zuständige Stelle weitergeleitet werden. Da solche Fälle voraussichtlich zahlenmäßig in überschaubaren Grenzen bleiben werden, sollte dieses Problem in der Praxis auch ohne Einbußen beim Datenschutz zu bewältigen sein.

---

[355] Siehe dazu BIM-Datensicherheitsstudie S. 107.
[356] Zu den Ausnahmen siehe oben Kapitel IV.2.1.2.

Ein wesentlicher Vorteil des Konzepts der DLS ist jedenfalls die Verringerung der Kommunikationswege. In den Diskussionen ging man von 15 abfrageberechtigten Behörden und 200 auskunftspflichtigen Anbietern aus.[357] Daher ist es die effizienteste Vorgangsweise, nur über eine zentrale Stelle zu kommunizieren, als 15 mal 200 sichere Verbindungen zu Realisieren (n x m - Problem). Spezielle technische Voraussetzungen auf Anbieterseite werden für die Anbindung an die DLS keine nötig sein, da die DLS über eine sichere Verbindung (die wahrscheinlich über das Protokoll „https" realisiert werden wird) praktisch mit jedem gängigen Browserprogramm erreichbar wäre. Die Autorisierung auf Anbieterseite könnte durch die RTR-GmbH unterstützt werden, der die Identität jedes anbindungspflichtigen Anbieters aufgrund der bescheidmäßigen Erledigung gemäß § 34 KommAustriaG bekannt sein muss.

IV.2.3.2.2 Lösungsvorschläge für eine DSVO

Die soeben ausgeführten Grundsätze über die Anbindung der Anbieter an die DLS könnten legistisch folgendermaßen erfasst werden:[358]

§ 15 Anbindung der Anbieter

(1) Die Anbindung an die Durchlaufstelle ist für alle Anbieter verpflichtend, die gemäß § 102a Abs 6 TKG 2003 zur Vorratsdatenspeicherung verpflichtet sind. Die Erfassung aller speicherpflichtigen Anbieter zur erstmaligen Einrichtung des Stammportals der Anbieter gemäß § 13 Abs. 3 erfolgt durch die Rundfunk & Telekom Regulierungs-GmbH, welche der Bundesrechenzentrum GmbH eine Liste aller erfassten Anbieter zur Importierung und Freigabe zur Verfügung stellt.
(2) Entsteht ein neuer speicherpflichtiger Anbieter oder fällt ein bestehender weg, hat die Rundfunk & Telekom Regulierungs-GmbH alle notwendigen Informationen über diesen Anbieter der Bundesrechenzentrum GmbH für die Freigabe oder zur Deaktivierung der Anbindung an die Durchlaufstelle bekannt zu geben.

IV.2.3.3 Sicherheitsniveau der Anbindung - DLS im Portalverbund

IV.2.3.3.1 Anbindung der Behörden

Die Identifikation und die Authentifizierung des jeweiligen Partners sind wesentliche Anforderungen an eine hinreichende Datensicherheit. Die sichere Anbindung der Behördenseite über den Portalverbund bietet sich dabei an, weil hierzu beim Bundesrechenzentrum bereits die Infrastruktur und ein großer Erfahrungsschatz bestehen.

Der Portalverbund Österreich ist eine E-Government Anwendung und wird auf der Website „Digitales Österreich"[359] wie folgt beschrieben: „Der Portalverbund ist ein Zusammenschluss von

[357] Vgl. die Zusammenfassung der Diskussion beim 3. Round Table, BIM-Datensicherheitsstudie S. 107.
[358] Die Formulierungen stammen aus der BIM-Datensicherheitsstudie S. 143; diese Vorschläge wurden ohne Änderungen durch das BMVIT in öffentliche Begutachtung geschickt, vgl. dazu den Begutachtungsentwurf im Anhang.

Verwaltungsportalen zur gemeinsamen Nutzung von bestehender Infrastruktur. Grundsätzlich haben Portale den Vorteil, dass mehrere Applikationen über einen Punkt zugänglich werden. Die Identität der Benutzenden wird im Zuge des Anmeldevorganges am Portal nur einmal überprüft. Die Benutzenden müssen sich daher nur einmal "ausweisen" um auf mehrere Ressourcen zugreifen zu können. Betreibenden von Anwendungen wird es im Portalverbund ermöglicht, die Authentifizierung und Autorisierung zu Portalen in Vertrauensstellung auszulagern. Anstelle einer eigenen Benutzerverwaltung für jede Anwendung wird nur mehr eine Benutzerverwaltung am Stammportal benötigt. Dadurch wird die Benutzerverwaltung vereinfacht und ein Single Sign-On unterstützt. Die Benutzerverwaltung bleibt technisch und organisatorisch weiterhin im Verantwortungsbereich der personalführenden Stelle. Organisationen, die am Portalverbund teilnehmen, können ihre lokale Benutzerverwaltung nicht nur für interne Anwendungen, sondern auch für externe Applikationen und Anwendungen verwenden. Betreiber von Applikationsportalen bleibt somit die externe Benutzerverwaltung erspart.

Die Teilnahme am Portalverbund wird durch die Portalverbundvereinbarung geregelt. Diese enthält Rechte und Pflichten, die von den teilnehmenden Portalbetreibenden einzuhalten sind. Zwischen den Betreibenden von Stammportalen, welche die Benutzenden verwalten und Anwendungsbetreibenden wird so ein Vertrauensverhältnis hergestellt. Alle Vereinbarungen werden bei einem Depositar, das ist jenes Bundesministerium, das für die IT-Koordination des Bundes zuständig ist, aufbewahrt. Technisch und organisatorisch ist die Kommunikation im Portalverbund durch das Portalverbundprotokoll (PVP) und durch die Festlegung von Sicherheitsklassen geregelt. Die Definition von Sicherheitsklassen im Portalverbund ermöglicht es einer Anwendung zu prüfen, ob Benutzende die für die Nutzung der Anwendungsfunktion erforderlichen Sicherheitsauflagen erfüllen. Für Mitarbeitende von Institutionen, die am Portalverbund teilnehmen, ergeben sich keine Veränderungen.

Der Betreibende von Anwendungen bestimmt, welche Anwendungen über welches Anwendungsportal zugänglich sind. Der Betreibende legt unter Beachtung sämtlicher Datenschutzbestimmungen fest, welche Stellen beziehungsweise Kategorien von Stellen über ein Anwendungsportal zugriffsberechtigt sind und definiert für seine Anwendungen je nach Aufgabenstellungen der Benutzenden Rollen mit entsprechenden Rechteprofilen. Der Stammportalbetreibende muss unter anderem sicherstellen, dass über das eigene Portal nur berechtigte Benutzende ordnungsgemäß auf Anwendungen zugreifen. Der Anwendungsportalbetreiber muss sicherstellen, dass nur über ein Stammportal autorisierte Benutzende auf die durch das Portal erreichbaren Datenanwendungen zugreifen können. Die Übereinstimmung des Rechteprofils der Benutzenden mit den Zuständigkeiten der zugriffsberechtigten Stelle muss geprüft werden. Erforderliche Datensicherheitsmaßnahmen sind ebenfalls zu organisieren und umzusetzen. Betreiber von Stammportalen können sich für den technischen Betrieb eines Dienstleistenden bedienen. In diesem Fall ist vom Dienstleistenden eine Vereinbarung zu unterzeichnen, die gewährleistet, dass auch dieser alle technischen und organisatorischen Vorkehrungen einhält, auf denen das Vertrauensverhältnis der Portalverbund-Teilnehmenden beruht.“

---

[359] http://www.digitales.oesterreich.gv.at/site/5288/default.aspx.

Die Vorteile der DLS mit Eingliederung in den Portalverbund im Hinblick auf sichere Identifikation, Authentifizierung sowie der sicheren verschlüsselten Übermittlung von personenbezogenen Daten waren in der Diskussion unter allen Beteiligten unbestritten.[360]

Das Prozedere der internen Authentifizierung zur Sicherstellung der konkreten Berechtigung der handelnden Personen muss klar geordnet sein, kann aber im Konzept des Portalverbunds auch intern bei der jeweiligen Organisation (Behörden- oder Anbieterseite) erfolgen und muss nicht zwingend über die DLS technisch realisiert werden. Die Anbindung sollte aber den Anforderungen der Sicherheitsklasse 3 des Portalverbunds gerecht werden.[361] Es sind die Konventionen des Portalverbunds[362] einzuhalten, wobei die Bundesrechenzentrum GmbH Teilnehmer am Portalverbund ist. Die Stammportale werden von den einzelnen Institutionen betrieben (bzw. von deren Dienstleistern).

Die Sicherheitsklasse 3 im Rahmen der Portalverbundvereinbarung ist konzipiert für Transaktionen von „sensiblen Daten" iSd § 4 Z 2 DSG. Dieser Sicherheitsmaßstab ist im Hinblick auf die gegenständlichen Datenkategorien, nämlich den Verbindungs- und Zugangsdaten iSd § 102a Abs. 2 bis 4 TKG, jedenfalls gerechtfertigt, weil niemals auszuschließen ist, ob es sich um „sensible Daten" iSd § 4 Z 2 DSG handelt.[363] Die Authentifizierung kann nach dieser Sicherheitsklasse entweder durch Wissen und Eigenschaft an in einem geschützten Bereich betriebenen Gerät oder durch Wissen und Besitz an in einem geschützten Bereich betriebenen Gerät oder durch Wissen und Besitz an einem mobilen Endgerät mit erhöhtem Grundschutz erfolgen.

Das Signaturgesetz definiert in § 2 Z 3 SigG die Eigenschaften einer „fortgeschrittenen Signatur": „fortgeschrittene elektronische Signatur: eine elektronische Signatur, die

a) ausschließlich dem Signator zugeordnet ist,

b) die Identifizierung des Signators ermöglicht,

c) mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann, sowie

d) mit den Daten, auf die sie sich bezieht, so verknüpft ist, dass jede nachträgliche Veränderung der Daten festgestellt werden kann;"

Eine solche fortgeschrittene Signatur ist dann ausreichend im Sinne der Sicherheitsklasse 3 des Portalverbundes, wenn der Zugriff auf die Anwendung aus einem „geschützten Bereich" erfolgt, der dabei folgendermaßen definiert ist: „Die zugriffsberechtigte Stelle hat in ihrer Sicherheitsrichtline festzulegen, wie die physische und netzwerktechnische Kontrolle umzusetzen ist. Mit der physischen Kontrolle muss verhindert werden, dass unbekannte oder nicht vertrauenswürdige Personen Zutritt

---

[360] Siehe dazu die Zusammenfassung der Diskussion beim 2. Round Table, BIM-Datensicherheitsstudie S. 99 f.

[361] Im Detail vgl. "Spezifikation Sicherheitklassen für den Zugriff von Benutzern auf Anwendungen", Version 2.1.0, 8.2.2008, ["SecClass 2.1.0"; Anhang zur Portalverbundvereinbarung pvv 1.0, 21.11.2002], http://reference.e-government.gv.at/AG-IZ-PVV-pvv-1-0-Ergaenze.332.0.html; vgl. auch den letzten Diskussionsstand zur Erweiterung der Sicherheitsklassen in der Arbeitsversion SecClass 2.1.0 unter http://reference.e-government.gv.at/uploads/media/SecClass_2-1-0_2007-12-14.pdf.

[362] Siehe dazu die letzte Version des Vorschlages der Arbeitsgruppe zur Portalverbundsvereinbarung im Rahmen des PVP2 - Spezifikationspaket Portalverbundprotokoll Version 2.0.0, http://reference.e-government.gv.at/AG-IZ-PVP2-Version-2-0-0.2754.0.html.

[363] Beispielsweise im Falle eines E-Mails, dass ein Teilnehmer an die Adresse der Aidshilfe geschickt hat.

zum Gerät haben. Mit der netzwerktechnischen Kontrolle ist möglichst zu unterbinden, dass unerlaubte Zugriffe überhaupt das Gerät erreichen, etwa durch den Einsatz von Firewalls und Content-Filtern."[364] Das BM.I hat beispielsweise die fortgeschrittene Signatur im Portalverbund implementiert und verwendet diese zur Identifikation von Organisationseinheiten.

Erfolgt der Zugriff auf die Anwendung von einem Rechner außerhalb eines geschützten Bereichs, wird zur Entsprechung der Sicherheitsklasse 3 im Rahmen der Portalverbundvereinbarung eine „qualifizierte Signatur" iSd § 2 Z 3a SigG notwendig sein. Diese verlangt gemäß § 5 SigG eine Personenbindung, die beispielsweise durch elektronische Dienstausweise, aber auch durch die Bürgerkarte (§ 2 Z 10 E-GovG) realisiert werden kann.

IV.2.3.3.2 Anbindung der Anbieter

Für die Seite der Anbieter ist ein Portal zu schaffen, dass dem Portalverbund der Behörden nachgebildet ist und denselben Sicherheitsanforderungen entspricht. Auch hierzu besteht beim Bundesrechenzentrum bereits ein großer Erfahrungsschatz, etwa aus der Realisierung des Elektronischen Rechtsverkehrs (ERV) für die Kommunikation zwischen Gerichten und professionellen Parteienvertretern (Rechtsanwälte, Notare). Bei der Anbindung der Anbieter ist sicherzustellen, dass auf Anbieterseite möglichst flexibel auf die DLS zugegriffen werden kann, damit auch außerhalb der Geschäftszeiten eine möglichst rasche Beantwortung des Auskunftsbegehrens erfolgen kann.

Den Anforderungen der Sicherheitsklasse 3 des Portalverbundes würde hierzu die Sicherheitsstufe 3 aus der "Definition der Sicherheitsstufen in der Kommunikation Bürger – Behörde im Bereich E-Government" entsprechen. Diese ist ebenfalls über die Website „Digitales Österreich" des Bundeskanzleramts abrufbar[365] und dort wie folgt beschrieben:

„Die höchste Sicherheitsstufe im Bereich E-Government, die auch für die Kommunikation Verwaltung – Verwaltung angewendet werden kann, wenn dies die Vertraulichkeit erfordert, wurde darauf ausgelegt, dass sie kompromittierten Endgeräten stand hält. Bei Anwendung dieser Sicherheitsstufe haben Client und Server Klarheit darüber, wer kommuniziert und können auch von der Vertraulichkeit im Rahmen der Sicherheit der kryptographischen Schlüssel und Algorithmen ausgehen.

Die Sicherheit wird mit einer TLS-Verbindung erreicht und basiert auf Zertifikaten mit Verwaltungseigenschaft. Die Bindung der Zertifikate an Client und Server ist technisch so abzusichern, dass sie auch kompromittierten Endsystemen standhält. Die für den Ablauf notwendigen Zertifikate werden direkt vom Server bzw. Client in die sichere TLS-Verbindung eingebunden. Es wird somit, anders als bei Stufe II, eine automatische und in die Verbindungsprotokolle integrierte Überprüfung der Serveridentität möglich. Dieser Mechanismus kann nun auch automatisch man-in-the-middle Attacken erkennen.

Die Zertifikate des Clients und des Serves der TLS-Verbindung werden in vertrauenswürdigen Komponenten gehalten und sind technisch vor Modikation geschützt. Dies kann zum Beispiel durch

---

[364] Definition der Sicherheitsklassen im Portalverbund in der Version 2.1.0, http://reference.e-government.gv.at/uploads/media/SecClass_2-1-0_2007-12-14.pdf.

[365] http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=21832.

den Einsatz von hardware security modules (HSM), auch Kryptoboxen genannt, erreicht werden. Diese Sicherheitsmodule sind in verschiedenen Formaten (Box, Tischgerät, PC-Karte, Chipkarte) erhältlich und werden in der Regel als interne Karten, als periphere Geräte oder über einen Adapter (für die Chipkarte) an den Hostrechner (Zentralrechner, Server, PCs) angeschlossen. Eine weitere Möglichkeit zur Absicherung besteht im Schaffen einer vertrauenswürdigen Softwareumgebung, unter anderem mit sicherem boot - Prozess, zuverlässigem Betriebssystem und digital signierter Software. Diese Sicherheitsstufe ist für Transaktionen mit sensiblen Daten nach dem Datenschutzgesetz geeignet (analog zur Sicherheitsklasse 3 im Portalverbund)."

Wenn ein Anbieter innerhalb seiner IT-Infrastruktur entsprechend „geschützte Bereiche" verwendet, stellt auch hier die fortgeschrittene Signatur die praktikabelste Lösung dar und beinhaltet die Möglichkeit eines Zertifikats auf Unternehmensbasis. Die Zuordnung zu Einzelpersonen ist in den Protokolldateien ersichtlich und muss daher nicht unbedingt durch die Signatur erfolgen. Durch die Signatur wird auch ein Hashwert zur Wahrung der Datenintegrität überflüssig. Mit der Signatur kann im Gegensatz zum bloßen Hashwert auch die Identität des Signators überprüft werden. Man weiß dann nicht nur, dass die Daten korrekt sind, sondern dass sie auch tatsächlich vom Signator stammen. Bei der Verwendung eines bloßen Hashwerts könnte ein „Man-In-The-Middle" die Nachricht und den Hash abfangen, beides ändern, und die geänderten Versionen der Nachricht und des Hashwerts weiterschicken. Hashwerte (in diesem Kontext) alleine schützen nur vor zufälligen Veränderungen, Signaturen auch vor absichtlichen Manipulationen.[366]

IV.2.3.4 DIE FUNKTION DER UNIQUE-ID

Von Seiten des BMJ wurde in der Diskussion die Anforderung formuliert, dass lückenlos nachvollziehbar sein muss, welche Personen von Anfang bis Ende an einem Auskunftsvorgang beteiligt waren, um allfälligem Missbrauch effektiv begegnen zu können.[367] Dem ist aus datenschutzrechtlicher Sicht voll zuzustimmen. Diese Nachvollziehbarkeit lässt sich nur durch eine Lückenlose Protokollierung aller Auskunftsvorgänge über die DLS gewährleisten.[368]

Die Unique-ID ist dabei eine einmalige, eindeutig zuordenbare Transaktionsnummer und erfüllt die zentrale Funktion, zusammengehörige Transaktionen zu korrelieren, wobei jede spezifische Behördenanfrage an einen bestimmten Anbieter eine Transaktion darstellt. Beispiel: Eine Anfrage ergeht an zwei Anbieter. Die Unique-ID könnte aus einem einmaligen „Anfrageteil" sowie einer Anbieter-ID bestehen (1234567-1, 1234567-2). Alternativ müsste es eine eigene ID zu dieser Anfrage für jeden Anbieter geben (1234567, 1234568). Die konkrete Ausgestaltung ist in der technischen Spezifikation zur DLS zu klären. In dieser Hinsicht kommt der Unique-ID auch eine nicht unwesentliche technische Funktion zu, weil durch sie die Zustellung der Antwort eines Anbieters in das richtige Postfach der anfragenden Stelle einfacher realisiert werden kann.

Alle Anfragen über die DLS sollen mit einer Unique-ID versehen werden. Die vom Anbieter übermittelte Antwort ist über dieselbe Unique-ID verknüpft und kann so den Datensatz zur

---

[366] So auch die Erläuterungen zu § 18 DSVO-Entwurf in der BIM-Datensicherheitsstudie S. 166; zum legistischen Formulierungsvorschlag für eine DSVO jedoch erst unten zur Verschlüsselung in Kapitel IV.2.4.

[367] Siehe die Zusammenfassung der Diskussion beim 3. Round Table, BIM-Datensicherheitsstudie S. 106 f.

[368] Dazu bereits oben im Zusammenhang mit dem Zugang zu den Protokolldaten der DLS in Kapitel IV.2.3.2.1.

Protokollierung mit den weiteren benötigten Information ergänzen. Durch diese einmalige Transaktionsnummer jedes Auskunftsvorganges kann für den Fall einer Nachprüfenden Kontrolle beispielsweise die Datenschutzkommission den Ablauf über die DLS leichter nachvollziehen. Die Protokollierung der DLS beinhaltet jedoch rein statistische Werte ohne Personenbezug. Die Unique-ID kann lediglich eine nachprüfende Kontrolle (zB durch Datenschutzkommission, Rechtsschutzbeauftragten oder Gericht) erleichtern, der Personenbezug kann aber über die DLS selbst nicht hergestellt werden. Die personenbezogene Protokollierung ist daher innerhalb der betreffenden Organisationen (Behörden und Anbieter) zusätzlich erforderlich.

IV.2.3.5 LÖSUNGSVORSCHLAG FÜR EINE DSVO

Die soeben ausgeführten Grundsätze zum Sicherheitsniveau der Anbindung von Behörden und Anbietern an die DLS könnten legistisch folgendermaßen erfasst werden:[369]

§ 8 Allgemeines

(5) Die Übermittlung der Daten erfolgt über eine zentrale Durchlaufstelle, die das Bundesministerium für Verkehr, Innovation und Technologie bei der Bundesrechenzentrum GmbH einzurichten hat.
(6) Die technische Spezifikation zur Durchlaufstelle hat einen verschlüsselten Übertragungsweg vorzusehen (Transportverschlüsselung).
(7) Zusätzlich ist eine Verschlüsselung der Inhalte sowohl der Anfrage als auch der Beantwortung von Absender zu Empfänger durch asymmetrische Verschlüsselungsverfahren vorzusehen (Inhaltsverschlüsselung). Asymmetrische Verschlüsselungsverfahren können als hybride Verfahren implementiert werden.
(8) Über die Durchlaufstelle werden die Teilnehmer des Datenaustausches über eine fortgeschrittene elektronische Signatur identifiziert und authentifiziert.

§ 13 Authentifizierung – Einbindung über den Portalverbund und Unique-ID

(1) Die Durchlaufstelle vergibt zu jeder Anfrage eine einmalige Transaktionsnummer zur Prüfung der Authentizität der Anfrage und zur Nachverfolgung jeder Anfrage sowie deren Beantwortung (Unique-ID). Aus der Transaktionsnummer muss sowohl auf die zugrunde liegende konkrete Anfrage der Behörde als auch auf den angefragten Betreiber geschlossen werden können.
(2) Die Authentifizierung der Benutzer der berechtigten Behörden erfolgt durch das jeweilige Stammportal des Benutzers (Portalverbund).
(3) Für die Authentifizierung der Benutzer auf Seiten der Anbieter ist in der Spezifikation zur Durchlaufstelle ein Stammportal vorzusehen, das der Sicherheitsklasse 3 der Portalverbundvereinbarung entspricht.

[369] Die Formulierungen stammen aus der BIM-Datensicherheitsstudie S. 141 ff; diese Vorschläge wurden mit nur einer minimalen Änderungen in § 13 durch das BMVIT in öffentliche Begutachtung geschickt, die sogleich dargestellt wird; vgl. dazu den Begutachtungsentwurf im Anhang.

§ 16 Sicherheitsniveau der Anbindung

(1) Die Anbindung der Behörden an die Durchlaufstelle hat den Vorgaben der Sicherheitsklasse 3 in der Portalverbundvereinbarung zu entsprechen.
(2) Die Anbindung der Anbieter an die Durchlaufstelle hat den Vorgaben der Sicherheitsstufe 3 aus der Definition der Sicherheitsstufen in der Kommunikation Bürger – Behörde im Bereich E-Government zu entsprechen.

Die Einzige Änderung für den Begutachtungsentwurf zur DSVO betrifft § 13 Abs. 1:

Authentifizierung – Einbindung über den Portalverbund und Unique-ID

§ 13. (1) Die Durchlaufstelle vergibt zu jeder Anfrage eine einmalige, eindeutig zuordenbare Transaktionsnummer zur Prüfung der Authentizität der Anfrage und zur Nachverfolgung jeder Anfrage sowie deren Beantwortung (Unique-ID). Aus der Transaktionsnummer muss sowohl auf die zugrunde liegende konkrete Anfrage der Behörde als auch auf den angefragten Betreiber geschlossen werden können.

Hier wurde ergänzt, dass die Unique-ID eine einmalige, „eindeutig zuordenbare" Transaktionsnummer zur Prüfung der Authentizität der Anfrage und zur Nachverfolgung jeder Anfrage sowie deren Beantwortung darstellt. Diese Ergänzung bewirkt keine Änderung des Sinngehalts der Bestimmung, weil sich schon aus der Beschreibung der Funktion der Unique-ID unzweifelhaft ergibt, dass diese Transaktionsnummer „eindeutig zuordenbar" sein muss. Gleichzeitig ist aber auch nichts gegen diese Ergänzung einzuwenden, weil lediglich ausdrücklich klarstellt, was funktionell ohnehin notwendig ist.

Aus den Stellungnahmen im Begutachtungsverfahren ist im Zusammenhang mit der Eingliederung in den Portalverbund eine Anmerkung der IKT-Abteilung des Bundeskanzleramts beachtenswert.[370] Dort wird darauf hingewiesen, dass der Begriff „Portalverbund" gesetzlich bisher nicht definiert wurde sondern lediglich eine privatrechtliche Vereinbarung zwischen Bund, Ländern und Gemeinden darstellt. So würde auch in anderen Gesetzen, die an den „Portalverbund" anknüpfen wollten, bislang vermieden, diesen Begriff im Gesetz selbst zu verwenden. Vielmehr würde eine allgemeine Umschreibung gewählt und begleitend in den Erläuterungen klargestellt, dass damit der Portalverbund gemeint ist. Beispielhaft wird auf § 3 Abs. 6 Unternehmensserviceportalgesetz (USPG) und die zugehörigen Erläuterungen verwiesen. Es solle demzufolge eine Formulierung verwendet werden, die nicht etwa auf das „Stammportal" des Benutzers abstellt, sondern den Portalverbund im genannten Sinn umschreibt. Der konkrete Formulierungsvorschlag für § 13 Abs. 2 DSVO lautet dazu:

„(2) Die Identifizierung und Authentifizierung der Benutzer der berechtigten Behörden hat über technische Voraussetzungen zu erfolgen, die auch eine Einbeziehung von Anwendungen der Gebietskörperschaften, sonstiger Körperschaften des öffentlichen Rechts oder andere staatliche Aufgaben besorgender Institutionen ermöglichen."

Dem entsprechend solle auch in § 13 Abs. 2 DSVO nicht im Verordnungswege auf eine privatrechtliche Vereinbarung (Portalverbundvereinbarung) verwiesen werden. Vorgeschlagen wird

[370] Die an das BMVIT gerichteten Stellungnahmen im Begutachtungsverfahren wurden nicht veröffentlicht und können daher nicht mit Fundstelle zitiert werden. Diese wurden dem Autor jedoch zum Zwecke der Verarbeitung im Rahmen dieser Dissertation vom BMVIT zur Verfügung gestellt.

die ausdrückliche Normierung der Verwendung der Bürgerkarte bzw. ein Verweis auf § 2 Z 10 E-GovG, welches der Anforderung der Sicherheitsklasse 3 der Vereinbarung entspreche.

Sachlich ist dieser Einwand nachvollziehbar, weil eine Verweisung in einer Verordnung auf eine privatrechtliche Vereinbarung auch im Hinblick auf das verfassungsrechtliche Bestimmtheitsgebot nicht unproblematisch ist. Im Bereich technischer Standards ist dies allerdings häufiger der Fall, etwa wenn auf Standards von Normungsgremien verwiesen wird, die selbst nur privatrechtliche Zusammenschlüsse darstellen. So stellt etwa die Legaldefinition der „E-Mail" in § 92 Abs. 3 Z 12 TKG auf das „Simple Mail Transfer Protocol" (SMTP) ab, welches ebenfalls nur eine „private" Definition eines technischen Standards ohne jeden öffentlichrechtlichen Charakter darstellt. Aus Gründen der erhöhten Rechtsklarheit wird daher hier empfohlen, die ausdrückliche Nennung des Portalverbundes in der Verordnung beizubehalten und allenfalls auf einen bestimmten Stand der Vereinbarung abzustellen, um eine dynamische Verweisung zu vermeiden.

IV.2.4 Datensicherheit und Verschlüsselung

IV.2.4.1 Allgemeiner Datensicherheitsmaßstab

Die grundlegenden gesetzlichen Vorgaben zum Datensicherheitsmaßstab gemäß § 94 Abs. 4 und 102c TKG wurden bereits im Zusammenhang mit dem Anwendungsbereich einer Datensicherheitsverordnung oben in Kapitel IV.2.1.1 ausgeführt.

Ebenfalls beachtlich ist der erste Grundsatz zur Datensicherheit, den die Richtlinie 2006/24/EG in Art 7 lit a) aufstellt: „Die auf Vorrat gespeicherten Daten sind von der gleichen Qualität und unterliegen der gleichen Sicherheit und dem gleichen Schutz wie die im Netz vorhandenen Daten". Darüber hinausgehende Vorschläge für Sicherheitsvorschriften erfließen aus dem Spielraum der Mitgliedsstaaten, höhere Sicherheitsanforderungen zu erlassen (Art 7 Abs 1 RL 2006/24/EG, arg. „zumindest folgende Grundsätze") und sind unter anderem das Ergebnis intensiver Diskussion im Rahmen vieler Arbeitsgruppentreffen im Zuge der Umsetzung der Vorratsdatenspeicherung, die nicht zuletzt durch die Entscheidung des deutschen Bundesverfassungsgerichts (BVerfG, 1 BvR 256/08 Urteil vom 2.März 2010[371]) zur dortigen Aufhebung der deutschen Umsetzung der Vorratsdatenspeicherungs-Richtlinie motiviert und vorgezeichnet sind.

Die für den Sicherheitsmaßstab wesentlichsten Aussagen des BVerfG sollen hier auszugsweise wiederholt werden: Hinsichtlich der Datensicherheit fordert das Gericht „gesetzliche Regelungen, die einen solchen besonders hohen Sicherheitsstandard in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgeben"[372]. Dieser hat sich an dem Entwicklungsstand der Fachdiskussion zu orientieren, neue Erkenntnisse und Einsichten fortlaufend aufzunehmen und nicht unter dem Vorbehalt einer freien Abwägung mit allgemeinen wirtschaftlichen Gesichtspunkten zu stehen. Nur wenn diesbezüglich hinreichende anspruchsvolle und normenklare Regelungen getroffen

[371] Näheres zu den nachfolgenden Auszügen aus dem Urteil in den Entscheidungsbesprechungen bei *Schmidt*, Auswirkungen des Urteils zur Vorratsdatenspeicherung auf die Praxis, in: AnwZert ITR 5/2010, Anm. 2 (Publikation enthält keine Seitenzahlen); und *Gietl*, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 399; vgl. ausführlich oben die Kapitel II.2.1 sowie II.3.1.
[372] BVerfG, 1 BvR 256/08 Urteil vom 2.März 2010, Abs. 225.

sind, ist der in einer solchen Speicherung liegende Eingriff verhältnismäßig im engeren Sinne, so das deutsche Bundesverfassungsgericht[373]. Um in qualifizierter Weise dem Grunde nach den Schutzstandard konkretisieren zu können, muss der Gesetzgeber die Schutzmechanismen selbst benennen und nur deren Ausgestaltung auf Verordnungen oder Aufsichtsbehörden delegieren. Dem ist die Konzeption des § 94 Abs. 4 und 102c TKG 2003 auch gefolgt. Wo die allgemeinen Sicherheitsanforderungen an die Verarbeitung von Telekommunikationsdaten nicht ausreichend erscheinen, um dem speziellen Schutzbedürfnis zu begegnen, das aus der flächendeckenden und anlasslosen Vorratsspeicherung resultiert, werden besondere Anforderungen in Ausführung der Vorgaben des § 102c TKG nachfolgend sowie unten zur Protokollierung in Kapitel IV.2.8.1 beschrieben.[374]

Unter einer anspruchsvollen Verschlüsselung ist eine Verschlüsselung zu verstehen, die nach dem derzeitigen Stand der Technik ohne erheblichen Aufwand nicht zu überwinden ist. Dabei ist durch weitere organisatorische Maßnahmen sicherzustellen, dass die Schlüssel und gegebenenfalls das Passwort ebenfalls sicher aufbewahrt werden. Ausdrücklich vorgeschrieben werden sollte eine asymmetrische Verschlüsselung. Bei einem asymmetrischen Verschlüsselungsverfahren besitzt jede der kommunizierenden Parteien ein Schlüsselpaar, das aus einem geheimen Teil (private key) und einem nicht geheimen Teil (public key) besteht. Der öffentliche Schlüssel ermöglicht es jedem, Daten für den Inhaber des privaten Schlüssels zu verschlüsseln. Die kommunizierenden Parteien müssen keinen gemeinsamen geheimen Schlüssel kennen, das Verfahren wird daher auch als Public-Key-Verfahren bezeichnet. Dafür ist eine Public-Key-Infrastruktur erforderlich, über die (vereinfacht dargestellt) die Ausstellung vertrauenswürdiger digitaler Zertifikate zur sicheren Übertragung organisiert wird. Die zentrale Herausforderung liegt darin, sicherzustellen, dass der öffentliche Schlüssel wirklich echt ist. Der Vorteil ist eine deutliche Minimierung des Sicherheitsrisikos, da jeder Benutzer nur seinen eigenen privaten Schlüssel geheim halten muss. Im Gegensatz dazu muss bei einem symmetrischen Verschlüsselungssystem jeder Teilnehmer alle Schlüssel geheim halten, was mit steigendem Aufwand verbunden ist, je mehr Teilnehmer daran beteiligt sind (große Zahl an Schlüsseln).

Nachteilig ist, dass asymmetrische Kryptosysteme aufgrund der Verschlüsselungsalgorithmen im Vergleich zu den symmetrischen Verfahren eher langsam sind. Der Geschwindigkeitsnachteil asymmetrischer Verfahren wird in der Praxis durch die Verwendung hybrider Verschlüsselungsverfahren umgangen. Dabei werden die zu übertragenden Daten mit einem zufällig generierten Schlüssel (sog. „session key“) symmetrisch verschlüsselt (deutlich schneller) und der jeweils verwendete Schlüssel unter Verwendung einer asymmetrischen Verschlüsselung an die Teilnehmer verteilt. Diese Variante löst das Schlüsselverteilungsproblem und erhält dabei den Geschwindigkeitsvorteil der symmetrischen Verschlüsselung. Das Verfahren entspricht dem Stand der Technik und wird der Anforderung einer technisch anspruchsvollen Verschlüsselung jedenfalls gerecht. Es sollte jedoch der technischen Spezifikation zur DLS vorbehalten bleiben, wie das asymmetrische Verschlüsselungsverfahren der Inhaltsverschlüsselung ausgestaltet wird.[375]

---

[373] BVerfG, 1 BvR 256/08 Urteil vom 2.März 2010, Abs. 239.
[374] Vgl. die Erläuterungen zu § 4 DSVO-Entwurf in der BIM-Datensicherheitsstudie S. 151 f.
[375] Siehe dazu die weitgehend gleich formulierten Erläuterungen zu § 8 Abs. 2 und 3 DSVO-Entwurf in der BIM-Datensicherheitsstudie S. 159 f; vgl. auch die Ausführungen zu den verschiedenen Verschlüsselungssystemen im Zuge der Darstellung des Konzepts der DLS oben in Kapitel III.1.3.

Für die verschlüsselte Übermittlung von Auskunftsdaten wird der öffentliche Schlüssel (auch: public key) des jeweiligen Empfängers verwendet. Nur dieser kann dann mit seinem private Schlüssel (auch: private key) die Auskunft im Klartext lesen. Die bei der DLS angesiedelte Aufgabe der Schlüsselverwaltung bedeutet, dass die öffentlichen Schlüssel zur Verschlüsselung der Daten am DLS-Server technisch gesehen durch sog. „Zertifikate" hinterlegt werden. Die Verschlüsselung der Anfrage und der Antwort kann nur bei der Behörde bzw. beim Anbieter stattfinden. Für die Verschlüsselung wird der „private key" benötigt und dieser kann niemals von der DLS erzeugt oder gespeichert werden. Die DLS ist nur für die Transportverschlüsselung zuständig und kennt natürlich die dafür notwendigen Schlüssel.[376]

IV.2.4.2 Besondere Sicherheitsvorschriften betreffend Vorratsdaten[377]

Die österreichische Umsetzung der Vorratsdatenspeicherungsrichtlinie 2006/24/EG ist in einem Punkt weniger streng als das Urteil des deutschen Bundesverfassungsgerichts, wonach verlangt wird: „Die Daten sind getrennt von den weiteren IT-Systemen des Speicherverpflichteten zu speichern, und zwar hardwaremäßig getrennt und entkoppelt vom Internet." Es genügt also nicht den Anforderungen des Bundesverfassungsgerichts, die Daten, die zur Vorratsdatenspeicherung gedacht sind, durch eine Kennzeichnung in der Datenbank von denjenigen Daten zu trennen, die für Abrechnungszwecke gespeichert werden.[378]

Nach den Vorgaben des § 102c TKG 2003 ist eine physische Trennung bei der Speicherung von Vorratsdaten und Betriebsdaten nicht notwendig. Hintergrund dieser Entscheidung des Gesetzgebers ist die Tatsache, dass eine physische Trennung im Hinblick auf die Datensicherheit nur dann endgültig Sinn ergeben würde, wenn damit auch zwingend verbunden wäre, dass der physische und technische Zugang auf der Ebene der IT-Infrastruktur zu einem solcherart getrennten Speichersystem organisatorisch nur völlig unterschiedlichen Personen im Betrieb des Anbieters möglich ist. Das würde faktisch bedeuten, dass ein zur Speicherung verpflichtetes Unternehmen eine eigene und völlig abgegrenzte IT-Abteilung nur für die Vorratsdatenspeicherung schaffen müsste. Dies wurde in der Debatte zur Umsetzung als unverhältnismäßiger Eingriff in die Eigentumsfreiheit der Anbieter gesehen und hat daher keinen Eingang in die österreichische Umsetzung gefunden. Anzumerken ist, dass sich das deutsche Bundesverfassungsgericht mit dem Problem der flankierenden organisatorischen Trennung gar nicht auseinandergesetzt hat.

Gleichwohl sind die speicherpflichtigen Unternehmen gesetzlich verpflichtet, sicherzustellen, dass der Eingriff auf die Daten einem gesicherten Zugriffsregime unterliegt. Das BVerfG führt hier beispielhaft das Vier-Augen-Prinzip an. Der Zugriff soll nicht durch Einzelne, sondern nur durch zwei oder mehr Personen möglich sein. Darüber hinaus ist der Zugriff auf die Daten revisionssicher zu protokollieren. Damit verlangt das Bundesverfassungsgericht, dass einerseits ein Zugriff auf die Daten nur möglich ist, wenn der Zugriff auch protokolliert wird. Andererseits darf dieses Protokoll

---

[376] Siehe dazu die weitgehend gleich formulierten Erläuterungen zu § 18 DSVO-Entwurf in der BIM-Datensicherheitsstudie S. 166 f.

[377] Siehe dazu die weitgehend gleich formulierten Erläuterungen zu § 5 DSVO-Entwurf in der BIM-Datensicherheitsstudie S. 152 ff.

[378] Andreas Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 399.

nicht im Nachhinein zu verändern sein, muss also revisionssicher sein[379]. Um dieses getrennte Zugriffsregime effektiv zu verwirklichen, sind geeignete Maßnahmen sowohl auf technischer als auch organisatorischer Ebene beim Anbieter notwenig, die jedenfalls eine logische Trennung bei der Datenbankhaltung erfordern. Nicht hinreichend wäre dafür, dass die Daten einfach in den betrieblichen Datenbanken verbleiben und dort als Vorratsdaten markiert werden. Vorzuschreiben ist daher auch, dass diese Daten umgehend aus den betrieblichen Datenbanken zu löschen und in die Vorratsdatenbank zu überführen sind. Die konkret von einem Anbieter entwickelte Methode dieser Trennung muss für die Kontrolle durch die Datenschutzkommission nachvollziehbar sein und daher auch dokumentiert werden. Dies sollte der Datenschutzkommission ermöglichen, die tatsächliche Einhaltung der Standards jederzeit zu kontrollieren.

Eine völlige Harmonisierung, wie lange ein Anbieter im Detail welche Daten für betriebliche Zwecke speichern darf, ist kaum zu erreichen und wäre wohl ein unverhältnismäßiger Eingriff in die Erwerbsfreiheit. Die Schwierigkeit liegt nämlich darin, dass die betriebliche Notwendigkeit einer Datenspeicherung einerseits von den technischen Systemen und deren Wartung und andererseits von der Ausgestaltung verschiedener Tarif- und Geschäftsmodelle abhängt. Dabei ist zum Teil gar nicht möglich, dass ein Anbieter in Bezug auf bestimmte Datenkategorien (etwa der Unterscheidung gemäß § 102a Abs. 2 bis 4 TKG 2003 folgend) genau festlegen kann, wie lange diese Datenkategorien jeweils für betriebliche Zwecke aufbewahrt werden. Das Problem liegt nämlich darin, dass zur selben Datenkategorie in unterschiedlichen Tarifmodellen auch unterschiedliche Aufbewahrungszeiträume notwendig sind. Dieselben Daten können also in einem Fall noch Betriebsdaten und in einem anderen Geschäftsmodell bereits Vorratsdaten sein.

Der Anbieter muss jedoch betriebsintern Klarheit darüber schaffen, welche Daten im Hinblick auf die intern bestimmten technischen und geschäftlichen Notwendigkeiten wie lange gespeichert werden. Diese Klarheit ist schon deswegen notwendig, weil ansonsten eine Abgrenzung im Hinblick auf das geforderte erhöhte Sicherheitsregime bei Vorratsdaten nur schwer möglich ist. Obgleich ein Anbieter Spielraum zur Gestaltung seiner Geschäftsmodelle hat, ist die Unterscheidung von Vorratsdaten nicht völlig beliebig in der Hand des Anbieters. Vielmehr haben die internen Betriebsdaten-Richtlinien den Anforderungen an eine datenschutzrechtliche Rechtfertigung für die Verarbeitung personenbezogener Daten gerecht zu werden. Es muss für einen verständigen Beobachter nachvollziehbar sein, warum bestimmte Daten(Kategorien) für bestimmte Zwecke eine bestimmte Zeit lang aufbewahrt werden. Aus diesem Grund müssen die internen Betriebsdaten-Richtlinien auch der Datenschutzkommission zugänglich sein, damit sie im Falle einer objektiven Kontrolle die Nachvollziehbarkeit der Rechtfertigung prüfen kann.

Überdies muss der Anbieter schließlich in der Lage sein, seine Speicherpolitik gegenüber seinen Kunden zu rechtfertigen, insbesondere für den Fall, dass ein Kunde eine Auskunft gemäß § 26 DSG 2000 begehrt oder im gerichtlichen Verfahren gemäß § 32 DSG 2000 die Richtigstellung oder Löschung seiner Daten begehrt.

[379] Näher dazu unten zur Protokollierung in Kapitel IV.2.8.1.

IV.2.4.3 LÖSUNGSVORSCHLÄGE FÜR EINE DSVO

Die soeben ausgeführten Überlegungen zur Datensicherheit und zur Verschlüsselung könnten legistisch folgendermaßen erfasst werden:[380]

§ 4 Datensicherheitsmaßstab

(1) Der Sicherheitsmaßstab bei der Verwendung von Daten im Sinne des § 2 Abs. 1 hat den Vorgaben des § 95 TKG 2003 zu entsprechen.
(2) Über Abs. 1 hinaus sind die besonderen Vorschriften für einen erhöhten Sicherheitsmaßstab bei der Verarbeitung von Vorratsdaten in Ausführung des § 102c Abs. 1 TKG 2003 im 2. Abschnitt dieser Verordnung ausdrücklich geregelt.

2. Abschnitt – Datensicherheit beim Anbieter innerhalb des Betriebes

§ 5 Geeignete technische und organisatorische Maßnahmen zur Sicherheit von Vorratsdaten

(1) Vorratsdaten müssen vom Anbieter auf eine Weise gespeichert werden, dass deren logische Unterscheidung von Betriebsdaten bei jedem Zugriff und jeder Verarbeitung eindeutig ist.
(2) Eine physikalisch getrennte Datenspeicherung von Betriebsdaten und Vorratsdaten ist nicht notwendig. Der Anbieter hat durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass die Datenbank zur Speicherung von Vorratsdaten (in der Folge kurz: Vorratsdatenbank) auf eine Weise ausgestaltet ist, dass Zugriffe auf Vorratsdaten nur unter Einhaltung der besonderen Sicherheitsvorschriften gemäß § 7 möglich sind.
(3) Wenn keine betriebliche Rechtfertigung zur Speicherung als Betriebsdaten mehr vorliegt, sind diese Daten umgehend aus den betrieblichen Datenbanken zu löschen und in die Vorratsdatenbank zu überführen. Sollte die Speicherung in der Vorratsdatenbank bereits zuvor gemäß § 6 erfolgt sein, so ist die Kennzeichnung der gleichzeitigen betrieblichen Speicherung zeitgleich oder unmittelbar nach der Löschung aus den betrieblichen Datenbanken zu entfernen.
(4) Der Anbieter hat die Methode zur technischen und organisatorischen Trennung nachvollziehbar zu dokumentieren und diese Dokumentation für den Fall einer Prüfung durch die Datenschutzkommission gemäß § 102c Abs 1 TKG 2003 auf Anfrage der Datenschutzkommission zugänglich zu machen.
(5) Der Anbieter hat die tatsächliche Speicherdauer von Betriebsdaten sowie allfällige diesbezügliche interne Richtlinien (Betriebsdaten-Richtlinie) für den Fall einer Prüfung durch die Datenschutzkommission gemäß § 102c Abs 1 TKG 2003 oder auf Anfrage der Datenschutzkommission zu beauskunften.

§ 18 Verschlüsselung/Signatur der Antwort

(1) Die vertrauenswürdige Stelle zur Hinterlegung der Zertifikate ist das Bundesministerium für Verkehr, Innovation und Technologie, das diese Funktion über die Durchlaufstelle technisch wahrnimmt. Jeder Teilnehmer kann in der Durchlaufstelle nur zu seiner Institution zugehörige eindeutige Schlüssel hinterlegen.

---

[380] Die Formulierungen stammen aus der BIM-Datensicherheitsstudie S. 139 ff; diese Vorschläge wurden mit nur einer rein sprachlichen Änderungen in § 4 und § 5 durch das BMVIT in öffentliche Begutachtung geschickt, die sogleich dargestellt wird; vgl. dazu den Begutachtungsentwurf im Anhang.

(2) Die Echtheit der Software, die von der Durchlaufstelle zur Verschlüsselung durch den Client zur Verfügung gestellt wird, muss für einen Client-Administrator eindeutig verifizierbar sein. Die Verschlüsselung und die Signatur erfolgt auf Client Seite, nur der öffentliche Schlüssel wird bei der Durchlaufstelle abgeholt.
(3) In der Spezifikation zur Durchlaufstelle ist eine eindeutige Definition der Dateinamen für die Übermittlung der Antwort sowie der Signatur zur Verschlüsselung der Dateien vorzunehmen. Es ist eine fortgeschrittene elektronische Signatur im Sinne des § 2 Z 3 Signaturgesetzes, BGBl. I Nr. 190/1999 in der Fassung BGBl. I Nr. 75/2010, vorzusehen.
(4) Wenn die Antwort aus mehreren CSV-Dateien besteht, ist es optional möglich, alle Dateien zu einer Abfrage zu einer Gesamtdatei zusammenzufassen. Die Gesamtdatei kann optional komprimiert werden. Die komprimierte oder unkomprimierte Gesamtdatei ist für die Übermittlung zu verschlüsseln, nicht aber die einzelnen Dateien.

Für den Begutachtungsentwurf des BMVIT wurde § 4 wie folgt abgeändert:

Datensicherheitsmaßstab

§ 4. (1) Der Sicherheitsmaßstab bei der Verwendung von Daten im Sinne des § 2 Abs. 1 hat den Vorgaben des § 95 TKG 2003 zu entsprechen.
(2) Bei Verwendung von Vorratsdaten gelten in Ausführung des § 102 Abs. 1 TKG 2003 über Abs. 1 hinaus die im 2. Abschnitt dieser Verordnung ausdrücklich geregelten besonderen Vorschriften für einen erhöhten Sicherheitsmaßstab.

2. Abschnitt
Datensicherheit beim Anbieter innerhalb des Betriebes
Geeignete technische und organisatorische Maßnahmen zur Sicherheit von Vorratsdaten

§ 5. (1) Vorratsdaten müssen vom Anbieter auf eine Weise gespeichert werden, dass deren logische Unterscheidung von Betriebsdaten bei jedem Zugriff und jeder Verwendung eindeutig ist.
(2) Eine physikalisch getrennte Datenspeicherung von Betriebsdaten und Vorratsdaten ist nicht notwendig. Der Anbieter hat durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass die Vorratsdatenbank auf eine Weise ausgestaltet ist, dass Zugriffe auf Vorratsdaten
nur unter Einhaltung der besonderen Sicherheitsvorschriften gemäß § 7 möglich sind.
(3) Wenn keine betriebliche Rechtfertigung zur Speicherung als Betriebsdaten mehr vorliegt, sind diese Daten umgehend aus den betrieblichen Datenbanken zu löschen und in die Vorratsdatenbank zu überführen. Sollte die Speicherung in der Vorratsdatenbank bereits zuvor gemäß § 6 erfolgt sein, so ist die Kennzeichnung der gleichzeitigen betrieblichen Speicherung zeitgleich oder unmittelbar nach der Löschung aus den betrieblichen Datenbanken zu entfernen.
(4) Der Anbieter hat die Methode zur technischen und organisatorischen Trennung nachvollziehbar zu dokumentieren und diese Dokumentation für den Fall einer Prüfung durch die Datenschutzkommission gemäß § 102c Abs. 1 TKG 2003 auf Anfrage der Datenschutzkommission zugänglich zu machen.
(5) Der Anbieter hat die tatsächliche Speicherdauer von Betriebsdaten sowie allfällige diesbezügliche interne Richtlinien für den Fall einer Prüfung durch die Datenschutzkommission gemäß § 102c Abs. 1 TKG 2003 oder auf Anfrage der Datenschutzkommission zu beauskunften.

Die Änderungen in Abs. 2 sind zunächst lediglich eine Umstellung des Satzbaus ohne Veränderung des Sinngehalts. Eine inhaltliche Änderung ist jedoch der Austausch des Wortes „Verarbeitung“ durch das Wort „Verwendung“ von Vorratsdaten. Die „Verwendung“ von Daten ist gemäß § 4 Z 8 DSG der weitere Begriff und umfasst auch das „Verarbeiten“ sowie zusätzlich das „Übermitteln“ von Daten.

Diese Änderung ist zu begrüßen, zumal damit konsequent entsprechend § 1 Abs. 2 DSVO-Begutachtungsentwurf[381] der weitere Begriff der „Verwendung“ zum Einsatz kommt.

Auch in § 5 Abs. 1 wurde das Wort „Verarbeitung“ durch „Verwendung“ ersetzt, es gilt das soeben zu § 4 ausgeführte auch hier.

IV.2.4.4 WIE WIRD DIE DLS „BLIND“ GEGENÜBER DEN INHALTEN?

In der Diskussion beim 1. Round Table im Rahmen der BIM-Datensicherheitsstudie, also in einer relativ frühen Phase der Entwicklung des Konzepts der Durchlaufstelle, wurde zunächst vorgeschlagen, dass die DLS zugleich auch für die Erstellung der privaten Schlüssel zuständig ist. Dies stieß zu Recht auf Kritik und auf datenschutzrechtliche Bedenken, weil damit alle personenbezogenen Inhalte während der Zwischenspeicherung einer Auskunftsbeantwortung im Postfach der DLS theoretisch zentral zugänglich wären. Daher kamen alle an der Diskussion Beteiligten überein, dass die Erstellung der privaten Schlüssel von einer davon unabhängigen Stelle übernommen werden soll.

Bei der Übermittlung von Auskunftsdaten wird der öffentliche Schlüssel des jeweiligen Empfängers verwendet. Nur dieser kann dann mit seinem privaten Schlüssel die Auskunft im Klartext lesen. Nur die Protokolldaten, die alle Anfragen (ohne Personenbezug) dokumentieren, werden mit dem öffentlichen Schlüssel der Durchlaufstelle verschlüsselt und können somit von der Durchlaufstelle mit ihrem privaten Schlüssel gelesen und gesammelt werden.

Die Erstellung des privaten Schlüssels, mit dem die begehrten Verkehrsdaten entschlüsselt werden können, ist der DLS nicht bekannt. Die bei der DLS angesiedelte Aufgabe der Schlüsselverwaltung ist darauf reduziert, dass die öffentlichen Schlüssel zur Verschlüsselung der Daten am DLS-Server technisch gesehen durch sog. „Zertifikate“ hinterlegt werden.[382]

IV.2.4.4.1 LÖSUNGSVORSCHLAG FÜR EINE DSVO

Die soeben ausgeführten Überlegungen könnten legistisch folgendermaßen erfasst werden:[383]

§ 9 Durchlaufstelle – Grundstruktur

(1) (…)
(2) Die Durchlaufstelle ist auf eine Weise einzurichten, dass für die Bundesrechenzentrum GmbH als Dienstleister der Durchlaufstelle im Sinne des DSG 2000 ein Zugang zu personenbezogenen Inhalten von Anfragen zu Datenauskünften so wie von deren Beantwortung nicht möglich ist.

(…)

[381] Siehe dazu den Begutachtungsentwurf zur DSVO im Anhang.
[382] Vgl. die Zusammenfassung der Diskussion beim 2. Round Table, BIM-Datensicherheitsstudie S. 90 f.
[383] Die Formulierung stammt aus der BIM-Datensicherheitsstudie S. 141; der Vorschlag wurde durch das BMVIT unverändert in öffentliche Begutachtung geschickt; vgl. dazu den Begutachtungsentwurf im Anhang.

IV.2.5 DATENAUSKUNFT IM CSV-FORMAT - ZUSAMMENHANG MIT DER EP020

Die Verwendung des CSV-Dateiformats zur Übermittlung einer Antwort auf ein Auskunftsbegehren wird gesetzlich durch § 94 Abs. 4 TKG vorgeschrieben. Die Erläuterungen führen dazu aus: „Der Spielraum für eine nach dieser Bestimmung zu erlassenden Verordnung ist eng determiniert. Die technische Richtlinie soll für alle Anbieter einheitlich definieren, welche der zu beauskunftenden Werte an welcher Stelle innerhalb der CSV-Datei zu stehen haben und welche Zeichensätze dabei zu verwenden sind. (…)Kein Platz besteht für Vorschriften, bestimmte Programme zu verwenden oder gar eine komplexe Schnittstelle wie beispielsweise den ETSI-Standard zur Vorratsdatenspeicherung vollständig zu normieren.“ [384] Im Ergebnis bedeutet das, dass die Anbieter nicht determiniert werden, ob, inwieweit und wie die Beantwortung von Auskunftsbegehren (teil-)automatisiert wird. Per Verordnung nach § 94 Abs. 4 TKG ist lediglich einheitlich festzulegen, wie die CSV Datei aussehen muss. Wie die einzelnen Anbieter diese Datei „befüllen“ bleibt deren Entscheidung.[385] Die Entscheidung für eine Übermittlung im CSV-Format wurde ganz bewusst im Zuge der Erstellung des BIM Entwurfs zur TKG-Novelle als datenschutzrechtliche Maßnahme getroffen. Damit sollte nämlich sichergestellt werden, dass auf keinen Fall direkte Schnittstellen auf die Datenbanksysteme der Anbieter im Wege der technischen Umsetzung vorgeschrieben werden. Entsprechende Begehrlichkeiten wurden von Seiten des BM.I und auch des BMJ schon in den ersten Stakeholder-Diskussionen während der Ausarbeitung des BIM-Entwurfes zur TKG-Novelle artikuliert. Solche Schnittstellen, wie insbesondere die in den Erläuterungen genannte ETSI-Schnittstelle[386] zur Vorratsdatenspeicherung vermögen nämlich die Intensität des Eingriffes in das Datenschutzgrundrecht zu potenzieren. Diese ETSI-Schnittstelle ist nämlich so konzipiert, dass sie eine permanente Rasterfahndung innerhalb sämtlicher von der Vorratsdatenspeicherung erfasster Kommunikationsdaten ermöglicht, also sogenanntes Data-Mining. Die damit möglichen Datenverknüpfung und Analyse des Kommunikationsverhaltens geht weit über die EU-rechtlich oder gesetzlich Zulässigen Ermittlungsbefugnisse hinaus. Wenig verwunderlich ist, dass viele europäische Geheimdienstorganisationen prominent an der Entwicklung dieser Schnittstellt beteiligt waren.[387]

Zum CSV-Format selbst wird in den Erläuternden Bemerkungen zu § 94 Abs. 4 TKG weiters ausgeführt: „Das Dateiformat CSV beschreibt den Aufbau einer Textdatei zur Speicherung oder zum Austausch einfach strukturierter Daten. Die Dateiendung CSV ist eine Abkürzung für "Comma-Separated Values". Das Dateiformat CSV wird im RFC 4180 grundlegend beschrieben. Die Normierung dieses Dateiformats bei gleichzeitig eindeutiger Definition der Datenfelder in der technischen Richtlinie hat den großen Vorteil völliger Technikneutralität, das heißt, dass weder die Anbieter noch die staatlichen Stellen, an welche die Daten übermittelt werden, an besondere technische Voraussetzungen gebunden sind. CSV-Dateien können von allen gängigen Datenbanksystemen verwendet werden. Diese Lösung stellt daher überdies die geringste

---

[384] EB zur RV BlgNR 1074 XXIV. GP.

[385] Vgl. auch hierzu die EB zur RV zu § 94 Abs. 4 TKG, BglNR 1074. XXIV. GP.

[386] Die Schnittstelle trägt die Bezeichnung ETSI ES 201 671; das European Telecommunications Standards Institute (ETSI) ist dabei ein internationales aber nicht-staatliches Normungsgremium, das internationale Standards im Bereich der Informations- und Kommunikationstechnologie (IKT) produziert; siehe dazu den Web-Auftritt der ETSI unter http://www.etsi.org/WebSite/AboutETSI/AboutEtsi.aspx.

[387] Zum Schema der Schnittstelle sowie zum Hintergrund deren Entstehung siehe die Präsentation zum Vortrag des ehemaligen Chefredatkteurs der ORF-Futurezone, Erich Möchel, über die Vorratsdatenspeicherung vom 27.11.2008 an der Hochschule München unter http://moechel.com/doqs/missbrauchte_vorratsdaten.pdf.

Kostenbelastung dar."[388] Mit der Notwendigkeit, alle Datenfelder exakt zu definieren, geht eine weitere datenschutzrechtlich wichtige Beschränkung einher. Das bedeutet nämlich, dass definiert werden muss, welche Informationen bei einem Auskunftsbegehren als Suchkriterien mitgeliefert werden und welche Daten aufgrund dieser Suchkriterien zurückgeliefert werden können. Die Definition der Datenfelder hat sich sodann streng an die rechtlich zulässigen Abfragemöglichkeiten zu halten. Im Ergebnis werden damit auch auf technischer Ebene die rechtlich zulässigen Abfragemöglichkeiten festgelegt, wodurch für Data-Mining in der Gesamtheit aller gespeicherten Daten - anders als nach der ETSI-Schnittstelle - keine Möglichkeit besteht.

Wie bereits oben in Kapitel II.3.2.1 ausführlich dargestellt, wurde auf eine entsprechende Anregung des BIM in Eigeninitiative der Telekombranche im Rahmen des Arbeitskreis-Telekommunikation (AK-TK) durch die Arbeitsgruppe „Schnittstellendefinition" bereits während der Entstehung der TKG-Novelle zur Umsetzung der Vorratsdatenspeicherung Anfang 2010 eine Empfehlung für eine solche „Schnittstellendefinition" ausgearbeitet und dem BM.I sowie dem BMJ präsentiert. Diese Empfehlung trägt die Bezeichnung EP020. Sie wurde im Rahmen der insgesamt 6 Round Table Diskussionen im Zuge der BIM-Datensicherheitsstudie mit allen Beteiligten (insbesondere BMI und Bundeskriminalamt) diskutiert und abgestimmt.[389] Schließlich wurde ein allseitiger Konsens zur EP020 erzielt und die Freigabe der finalen Version der EP020 durch das Plenum des AK-TK am 29.6.2011 zur Veröffentlichung in der BIM-Datensicherheitsstudie (bzw. auch im Rahmen dieser Dissertation) sowie zur Verwendung für die Verordnung beschlossen.

IV.2.5.1.1 Lösungsvorschlag für eine DSVO

Weil die Schnittstellendefinition gemäß der EP020 bereits auf breiter Konsensbasis besteht, wird für die legistische Umsetzung vorgeschlagen, die EP020 aus Gründen der besseren Darstellung in Form einer Anlage in eine DSVO zu inkorporieren. Die Technische Richtlinie in der Anlage zum DSVO-Entwurf[390] enthält dabei all jene Teile der EP020, die sich unmittelbar auf die Definition der Syntax und Semantik der CSV Datei für die Übermittlung von Auskünften bezieht. Für die legistische Umsetzung werden aus der EP020 deren Kapitel 3.1 und das gesamte Kapitel 4 als Anhang A zur Verordnung beigelegt. In der DSVO selbst sollte ausdrücklich bestimmt werden, dass diesem Anhang die selbe normative Qualität wie den sonstigen Bestimmung der Verordnung zukommt.

Kapitel 1 und 2 der EP020 beschreiben den Gegenstand der Empfehlung und den Rahmen ihres Zustandekommens und sollen daher nicht Gegenstand der Verordnung sein. Die Kapitel 3.2 (Protokollierung), 3.3 (Verschlüsselung, Signatur und Datenintegrität) und 3.4 (Zusatzinformationen) enthalten nur kurze Beschreibungen, mit denen der Bezug zwischen der CSV-Datei und dem Konzept der Durchlaufstelle (DLS) erläutert wird. Der jeweilige Regelungsgegenstand ist aber unmittelbarer Bestandteil der Verordnung und wird daher im Anhang A zur Verordnung nicht wiedergegeben. Der Bezug in der DSVO könnte sodann aussehen wie folgt:

---

[388] EB zur RV BlgNR 1074 XXIV. GP.
[389] Vgl. dazu BIM-Datensicherheitsstudie S. 132.
[390] Siehe BIM-Datensicherheitsstudie S. 146.

4. Abschnitt – Definition Syntax und Semantik der CSV-Datei für Auskünfte

§ 25 Schnittstellendefinition EP020

Die Schnittstellendefinition ergibt sich aus der Anlage A.

Das Kapitel 5 der EP020 (Annex: Beispiele informativ und exemplarisch) dient nur dem besseren Verständnis der eigentlichen Schnittstellendefinition und wird in den Erläuterungen zur Verordnung Angehängt. In der Beilage zu den Erläuternden Bemerkungen werden für alle in der Anlage definierten Datenfelder Beispiele dargestellt. Die Aufzählung der Beispiele ist nicht abschließend und soll den Anbietern sowie den auskunftsberechtigten Behörden zur Hilfestellung bei der technischen Implementierung dienen. Entsprechend kommt dieser Beilage keine über die Anlage oder die sonstigen Bestimmungen dieser Verordnung hinausgehende Bedeutung zu.

Im Rahmen dieser Dissertation soll die EP020 jedoch Komplett im Anhang wiedergegeben werden.

IV.2.6 Unterscheidung von Vorratsdaten und Betriebsdaten

IV.2.6.1 Warum ist eine Unterscheidung zwischen Vorratsdaten und Betriebsdaten notwendig?

An die Unterscheidung zwischen Vorratsdaten und solchen Daten, die ein Anbieter noch für betriebliche Zwecke gespeichert hat (kurz: Betriebsdaten) sind einige rechtliche Konsequenzen geknüpft, die durch eine Konkretisierung und klare Formulierung der an sich schon im TKG 2003 vorgezeichneten Definitionen leichter normativ zu erfassen sind. So sollte in einer DSVO explizit der Begriff „Betriebsdaten“ eingeführt und definiert werden, weil in zahlreichen öffentlichen Diskussionen zum Thema Vorratsdatenspeicherung oft nur der Begriff der „Verrechnungsdaten“ verwendet wird, der jedoch zu kurz greift. Wohl bilden die Daten zum Zweck der Rechnungslegung (§ 99 Abs 2 TKG 2003) den praktisch wichtigsten Fall, doch auch jene Daten, die beim Anbieter zum Zweck der Aufrechterhaltung des Betriebes und insbesondere der technischen Wartung der Betriebsanlagen (§ 99 Abs 3 TKG 2003) verarbeitet und gespeichert werden, sind nach der bisherigen Rechtslage vor der Umsetzung der Vorratsdatenspeicherung regelmäßig Gegenstand von behördlichen Auskunftsersuchen. Zur leichteren Abgrenzung sollte eine DSVO dabei auch den Begriff der Vorratsdaten explizit wiedergeben, dabei natürlich auf die Legaldefinition des § 92 Abs. 3 Z 6b TKG 2003 abstellen und diese mit der Zweckwidmung des § 102b TKG 2003 verbinden. Damit soll lediglich die strenge Zweckbindung, die nur durch die Ausnahmen in § 99 Abs. 5 TKG 2003 durchbrochen wird, eindeutig klargestellt werden, ein über die Definition im TKG 2003 hinausgehender normativer Gehalt entsteht daraus nicht.[391]

Vom Anbieter muss jedenfalls eine Methode zur strikten Trennung von Vorratsdaten und betriebsnotwendigen Daten nachgewiesen werden. Damit muss verbunden sein, dass auf Vorratsdaten nur unter dem strengeren Sicherheitsregime des § 102c TKG zugegriffen werden kann (nur besonders ermächtigte Personen, Vier-Augen-Prinzip, revisionssichere Protokollierung). Eine

[391] Vgl. die Erläuterungen zu § 2 DSVO-Entwurf, BIM-Datensicherheitsstudie S. 148 f.

logische Trennung reicht dabei aus, eine physische Trennung der Daten ist in Österreich - anders als nach dem Urteil des deutschen Bundesverfassungsgerichts zur Vorratsdatenspeicherung - aber nicht vorgeschrieben.[392]

IV.2.6.1.1 Unterscheidung Aus der Sicht der abfrageberechtigten Behörden

Aus Sicht der abfrageberechtigten Stellen sollte die Unterscheidung zwischen Vorratsdaten und Verrechnungsdaten jedenfalls transparent gemacht werden. Seitens des BMJ wurde angeregt, durch die Branche eine "Richtlinie" bzw. einen Code of Conduct in dieser Beziehung zu erstellen, um den abfrageberechtigten Stellen die Unterscheidung zu erleichtern.[393] Zwar sollte nach diesem Wunsch des BMJ jedem Anbieter der Spielraum bleiben, die Definition entsprechend seiner Geschäftsmodelle und seiner technischen Infrastruktur vorzunehmen. Doch sollte diese Entscheidung dann nach Außen transparent gemacht werden. So ließe sich auch der Erwartung begegnen, dass nach Inkrafttreten der Vorratsdatenspeicherung viele Kunden entsprechende Anfragen nach § 26 DSG an ihren Anbieter stellen, was einen nicht geringen personellen Aufwand verursachen könnte. Die Transparenz liege also auch im Interesse der Anbieter. Aus Sicht der anfrageberechtigten Stellen wäre also gewünscht, schon vor der Abfrage der Daten zu wissen, ob es sich um Vorratsdaten oder Verkehrsdaten handelt. Bei E-Mail-Daten ist auch aus Sicht der Anbieter sofort der Status als Vorratsdaten gegeben, da E-Mail-Daten nicht für Verrechnungszwecke erforderlich sind. Bei IP-Adressen ist die Notwendigkeit einer Speicherung aus Sicht einiger Anbieter ebenfalls nicht gegeben. Allenfalls könnte eine IP-Adresse zur Verfolgung von Attacken im IP-Netz bis zu 14 Tagen aufbewahrt werden, wobei dies auch in den Diskussionen nicht einheitlich gesehen wurde. Für Telefoniedaten besteht nach Überlegungen des BIM bei der Erstellung der Gesetzesvorlage eine Notwendigkeit, die Daten etwa 3 Monate für Verrechnungszwecke aufzubewahren.[394]

Für die Praxis sollten möglichst Fälle vermieden werden, in denen eine Anfrage auf betrieblich gespeicherte Daten negativ beantwortet wird und dann eine zweite Anfrage auf Vorratsdaten erforderlich ist. Vielmehr sollte eine Anfrage auf Vorratsdaten auch dann beantwortet werden können, wenn der Anbieter die Daten tatsächlich noch als Betriebsdaten gespeichert hat. Es sollen zudem auch Fälle vermieden werden, in denen sich der Zeitraum einer negativen Anfrage auf betriebsnotwendige Daten und die darauf folgenden Anfrage auf Vorratsdaten genau mit jenem Zeitraum überschneidet, innerhalb dessen Daten nicht mehr für betriebsnotwendige Zwecke benötigt werden und somit zu Vorratsdaten werden. Ansonsten könnte es etwa sein, dass Vorratsdaten angefordert werden, zunächst aber nur Betriebsdaten vorliegen und zum Zeitpunkt der nochmaligen Übermittlung des Auskunftsbegehrens gerichtet auf Betriebsdaten (also gemäß § 135 Abs 2 StPO) diese Daten in der Zwischenzeit doch zu Vorratsdaten geworden sind, und der Anbieter die Antwort schließlich doch auf Basis der ersten Anfrage übermitteln müsste.

Um dieses Problem zu lösen, wurden verschiedene Optionen diskutiert. So sollen zudem auch Fälle vermieden werden, in denen sich der Zeitraum einer negativen Anfrage auf betriebsnotwendige Daten und die darauf folgenden Anfrage auf Vorratsdaten genau mit jenem Zeitraum überschneidet innerhalb dessen Daten nicht mehr für betriebsnotwendige Zwecke benötigt werden und somit

[392] Zur Begründung siehe oben Kapitel IV.2.4.2.
[393] Siehe die Zusammenfassung der Diskussion beim 4. Round Table, BIM-Datensicherheitsstudie S. 115 f.
[394] Vgl. dazu die Zusammenfassung der Diskussion beim 3. Round Table, BIM-Datensicherheitsstudie S. 110 ff.

Vorratsdaten sind. Ansonsten könnte etwa sein, dass Vorratsdaten angefordert werden, zunächst aber nur Billingdaten vorliegen, und zum Zeitpunkt der nochmaligen Übermittlung des Auskunftsbegehrens auf Billingdaten diese Daten in der Zwischenzeit doch zu Vorratsdaten geworden sind, und der Anbieter die Antwort schließlich doch auf Basis der ersten Anfrage übermittelt.[395] Diesem Problem - das primär durch die unterschiedlichen Rechtsschutzregime für Vorratsdaten- und Betriebsdatenauskünfte in der StPO entsteht - kann aber auch auf andere Weise begegnet werden, dazu sogleich unten in Kapitel IV.2.6.4.

Von Seiten der Anbieter wurde dem Wunsch des BMJ nach branchenweiten Richtlinien zur Vorab-Unterscheidung von Vorratsdaten und Betriebsdaten entgegnet, dass die internen Rechnungsläufe bis zu drei Monate betragen können, unterschiedliche Einspruchsfristen (ebenfalls bis zu drei Monaten) sowie betriebliche Gründe, die den Status der Daten beeinflussen können. Ein gemeinsamer Standard sei aus Sicht der Anbieter nicht erreichbar. Die Vorgangsweise könne z.B. auch von Produkten abhängig sein. Beispielsweise würden Daten für Produkte mit sogenannten „Flatrates“ früher zu Vorratsdaten werden, als Daten, die für Produkte aufgezeichnet werden müssen, die nach Volumen abgerechnet werden. Auch eine Abhängigkeit von Kunden im Einzelfall wurde argumentiert, weil sich diese unter Umständen ja vertraglich gesonderte Bestimmung zur Verwendung seiner personenbezogenen Daten ausbedingen könnten.[396] Abgesehen von diesen praktischen Problemen für eine Vereinheitlichung sprechen auch rechtliche Gründe dagegen, solche „Betriebsdatenrichtlinien“ im Rahmen einer DSVO vorzuschreiben. Damit würde nämlich schlicht die Verordnungsermächtigung der §§ 94 Abs. 4 und 102c TKG überschritten. Solche Vorschriften müsste der Gesetzgeber unmittelbar im TKG verankern.

IV.2.6.2 PRAKTISCHE RELEVANZ DER UNTERSCHEIDUNG IM RAHMEN DER STPO

Jedenfalls erforderlich im Rahmen der StPO wird eine ex-post Information sein, ob ein für die Auskunft übermittelter Datensatz Vorratsdaten enthält. Im Falle einer Auskunft über Vorratsdaten (§ 134 Z 2a StPO) ist gemäß der neuen Bestimmung des § 147 Abs 1 Z 2a iVm Abs 3 StPO[397] der Rechtsschutzbeauftragte der Justiz zu verständigen. Bisher war der RSB der Justiz bei einer „Auskunft über Daten einer Nachrichtenübermittlung“ gemäß § 147 Abs 1 Z 5 iVm Abs 3 StPO nur dann zu informieren, wenn eine entschlagungsberechtigte Person oder ein „Berufsgeheimnisträger“ von der Auskunft betroffen war (hier besteht in der Praxis eher die Schwierigkeit, dass regelmäßig im Voraus gar noch gar nicht beurteilt werden kann, ob die Datenauskunft solche Personen betrifft). Bedeutung erlangt die Unterscheidung aber auch für die Statistik, die vom BMJ zum Zweck der jährlichen Übermittlung an die EU Kommission zu führen ist – und die über die DLS automatisch generiert werden soll. Es ist nämlich zu erwarten, dass häufig eine „Auskunft über Vorratsdaten“ begehrt wird, die Daten beim Anbieter aber noch zu Verrechnungszwecken gespeichert sind und daher gar keine Vorratsdaten übermittelt werden. Denkbar ist auch, dass ein Auskunftsbegehren zu Daten einer Nachrichtenübermittlung (also zu Daten, die noch aus betrieblichen Gründen beim Anbieter

[395] Ibid, S. 117f.
[396] Siehe die Zusammenfassung der Diskussion beim 4. Round Table, BIM-Datensicherheitsstudie S. 115 f.
[397] Siehe dazu die Darstellung der neuen Rechtslage oben in Kapitel II.1.5.

gespeichert sind) ein Eventualbegehren zu Vorratsdaten enthält. Die Statistik sollte die Information, ob tatsächlich Vorratsdaten übermittelt wurden, aus Transparenzgründen jedenfalls enthalten.[398]

IV.2.6.3 Praktische Relevanz der Unterscheidung im Rahmen des SPG

Auf für Auskünfte nach dem SPG ist notwendig, die Information zu übermitteln, ob Vorratsdaten für die Beantwortung der Abfrage nach § 53 Abs. 3a und Abs. 3b SPG verwendet wurden. Gemäß § 53 Abs 3c SPG ist daran nämlich geknüpft, ob eine Information des Betroffenen zu erfolgen hat oder nicht. [399] Von der erfolgten Information des Betroffenen im Falle einer Auskunft über Vorratsdaten ist ausserdem der Rechtsschutzbeauftragte des BMI zu verständigen.

IV.2.6.4 Mögliche Lösungswege

Eine zuverlässige ex-ante Information gegenüber auskunftsberechtigten Behörden, ob Daten als Vorratsdaten oder als Betriebsdaten gespeichert sind, ist aus den oben beschriebenen Gründen nicht möglich. Zugleich ist aber zumindest eine ex-post Unterscheidung aus den soeben dargestellten Gründen erforderlich. In diesem Kapitel sollen mögliche Lösungswege dargestellt werden, wie insbesondere dem praktischen Bedürfnis nach Unterscheidung im Anwendungsbereich der StPO begegnet werden könnte. Zugleich sei aber nochmals darauf hingewiesen, dass dieses Problem im Rahmen der StPO vom BMJ gewissermaßen „hausgemacht" ist, weil erst durch die Unterscheidung in den Auskunfts- und Rechtsschutzregimen (Verständigung des Rechtsschutzbeauftragten nur bei Vorratsdaten) das Problem überhaupt existiert. Eine saubere Umsetzung der Vorratsdatenspeicherung auf Seiten der StPO hätte dieses Problem von vornherein vermeiden können. Das selbe gilt auch für die neuen Bestimmungen in § 53 SPG. Dass die Änderungen zu beiden Gesetzen niemals in öffentliche Begutachtung vor der Umsetzung geschickt wurden, war bei der Erfassung der nachfolgenden Probleme natürlich nicht hilfreich.

IV.2.6.4.1 Ist eine Doppelte Speicherung als Vorratsdaten und zugleich als Betriebsdaten rechtlich zulässig?

Relevant ist zunächst die Frage des Zeitpunkts der Vorratsspeicherung. Daten werden gemäß § 92 Abs. 3 Z 6b TKG dann zu Vorratsdaten, wenn sie der Anbieter für betriebliche Zwecke nicht mehr benötigt und die Daten nur noch aufgrund der Verpflichtung des § 102a TKG gespeichert werden. Dann müssen diese Daten gemäß § 102c TKG so gespeichert werden, dass sie logisch streng von den betrieblich benötigten Daten unterschieden werden. Für diesen Zweck wird daher erforderlich sein, eine eigene „Vorratsdatenbank" zu halten. Nun stellt sich aber die Frage, ob in eine solche Vorratsdatenbank auch schon Daten übertragen werden dürfen, die zugleich auch noch in den betrieblichen Systemen der Anbieter vorhanden sind. Der Sinn einer solchen Lösung würde darin liegen, dass der Anbieter im Falle eines Auskunftsbegehrens der Strafverfolgungsbehörden gemäß § 135 Abs. 2a StPO nur in dieser Datenbank suchen müsste, ob die begehrten Informationen

[398] Vgl.BIM-Datensicherheitsstudie S. 121.
[399] Zur Kritik dieser sachlich nicht nachvollziehbaren Unterscheidung im Rechtsschutz siehe oben Kapitel II.1.5.

vorhanden sind, und keine zusätzliche Abfrage in seinen betrieblichen Datenbanken durchführen müsste. Streng nach dem Wortlaut von § 135 Abs. 2 (Betriebsdatenauskunft) und § 135 Abs. 2a StPO (Vorratsdatenauskunft) müsste nämlich für eine Nachschau in den Betriebsdatenbanken ein neuerliches Auskunftsbegehren gemäß § 135 Abs. 2 StPO gestellt werden, wenn die Anfrage ursprünglich auf § 135 Abs. 2a StPO gestützt wurde.

Zu bedenken ist in diesem Zusammenhang das Doppelspeicherungsverbot. Ein solches ist zwar im normativen Teil der EU-Richtlinie 2006/24/EG nicht ausdrücklich enthalten. Allerdings enthält Erwägungsgrund 13 der RL die Vorgabe: „Die Vorratsspeicherung von Daten sollte so erfolgen, dass vermieden wird, dass Daten mehr als einmal auf Vorrat gespeichert werden. Das muss aber nicht zwingend bedeuten, dass eine Speicherung von Daten als Billingdaten und Vorratsdaten verboten ist.

Eine solche doppelte Speicherung könnte die operative Abwicklung sowohl für die Anbieter als auch für die auskunftsberechtigten Behörden erleichtern. Die Anbieter könnten nämlich alle Daten schon bei der ersten Verarbeitung aus dem Live-System „abgreifen“ und in die Vorratsdatenbank überführen. Aus den betrieblichen Datenbanken würden die Daten dann ohne Weiteres gelöscht, sobald die betriebliche Notwendigkeit nicht mehr gegeben ist. Aus Sicht der Behörden würde dies bedeuten, dass eine Anfrage auf Vorratsdaten in jedem Fall erfolgreich wäre, auch wenn diese Daten zugleich noch zu betrieblichen Zwecken gespeichert wären. Der Anbieter müsste dann jedenfalls in der Vorratsdatenbank über ein „Flag“ pro Datensatz (unterschieden nach den Datenkategorien des § 102a Abs 2 bis 4 TKG) markieren, ob das Datum zugleich noch im betrieblichen System vorhanden ist oder nicht. Bei der Löschung im betrieblichen System müsste dieses „Flag“ dann den Status ändern. Diese Information (zB: Vorratsdatum J/N) müsste bei der Übermittlung der Antwort zu einem Auskunftsbegehren dann für die Statistik und zur Kenntnis der Behörden mitgeliefert werden. Sollte ein Auskunftsbegehren nur die Übermittlung von betriebsnotwendigen Daten, nicht aber die Übermittlung von Vorratsdaten erlauben, wäre die Auskunft aus der Vorratsdatenbank nur zulässig, wenn markiert ist, dass die Daten auch in den betrieblichen Systemen noch vorhanden sind.[400]

Dazu normiert § 92 Abs. 3 Z 6b des TKG: "*Vorratsdaten sind Daten, die ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a gespeichert werden.*" Zur Bestätigung oder Widerlegung der Hypothese geht es also vor allem um die Auslegung des Wortes "ausschließlich".

IV.2.6.4.2 Argumente pro doppelte Speicherung

Für die Zulässigkeit einer gleichzeitigen Speicherung als Vorrats- und Betriebsdaten könnte sprechen, „ausschließlich“ aus der Perspektive der Vorratsdatenbank zu verstehen. Daten in dieser Datenbank dienen allein dem in § 102a Abs 1 TKG normierten (und eingeschränkt von § 99 Abs 5 TKG mit Ausnahmen durchbrochenen) Zweck der „Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt.“ Zugriffe auf diese Datenbank sind stets nur unter den strengeren Voraussetzungen der §§ 102b und 102c TKG zulässig, selbst wenn diese Daten zugleich im betrieblichen System des Anbieters vorhanden sind. Insofern wären die Daten in dieser Datenbank tatsächlich „ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a“ gespeichert. Diese Datenbank würde ab dem Ende der Kommunikation stets alle Daten enthalten, die für Auskünfte gegenüber den berechtigten Behörden zur Verfügung stehen müssen.

[400] Vgl. BIM-Datensicherheitsstudie S. 123 ff.

Falls Daten auch in den betrieblichen Systemen des Anbieters noch vorhanden sind, müsste dies für die Richtigkeit der Statistik sowie allfällige prozedurale Folgen (Informationspflicht nach SPG) in der Vorratsdatenbank jeweils markiert sein. Auskunftsbeantwortungen könnten dann immer einheitlich über den (protokollierten) Zugriff auf diese Datenbank abgewickelt werden. Eine Stütze für diese Lesart findet sich in den Erläuterungen zur Regierungsvorlage:[401] „Der Begriff „Vorratsdaten" verdeutlicht explizit, dass die Speicherung der Daten für die in § 102a Abs 1 festgelegte Dauer ab ihrer Entstehung deshalb flächendeckend und vorrätig erfolgt, damit sie später den Strafverfolgungsbehörden zur Verfügung stehen, falls die Auskunft zu bestimmten Daten einer Nachrichtenübermittlung in einem bestimmten Verfahren zur Ermittlung, Feststellung und Verfolgung einer bestimmten Straftat, deren Schwere eine Auskunft nach § 135 Abs 2a rechtfertigt, notwendig ist." [402]

IV.2.6.4.3 Argumente contra doppelte Speicherung

Gegen diese Auslegung spricht jedoch die Erklärung in den Erläuterungen unmittelbar davor:[403] „Bei der Beurteilung, ob es sich bei einem Datum um ein Vorratsdatum handelt, ist vielmehr darauf abzustellen, ob es von Anbietern der in § 102a genannten Dienste ausschließlich aufgrund der Speicherverpflichtung des § 102a gesammelt bzw. bespeichert wird. Dabei ist zu beachten, dass auch beim Anbieter zunächst zu anderen Zwecken vorhandene Daten zu Vorratsdaten werden können, wenn alle anderen zulässigen Speicherzwecke (insbesondere die Betriebsnotwendigkeit der Speicherung) wegfallen. Die Einordnung der Daten als Vorratsdaten ist also durch den Zweck determiniert, zu dem die Daten gespeichert werden (dürfen)." Nach der Legaldefinition in § 134 Z 2a StPO ist eine Auskunft über Vorratsdaten, „die Erteilung einer Auskunft über Daten, die Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe des § 102a Abs. 2 bis 4 TKG zu speichern haben, und die nicht nach § 99 Abs. 2 TKG einer Auskunft nach Z 2 (Anm.: „Auskunft über Daten einer Nachrichtenübermittlung") unterliegen." Wenn Daten aber sowohl aus betrieblichen Gründen als auch als Vorratsdaten gleichzeitig gespeichert würden, würden erstere zugleich einer Auskunft nach § 134 Z 2 StPO unterliegen. Diese Definition spricht daher gegen die Zulässigkeit einer Überlappung von Vorratsdaten und betriebsnotwendigen Daten.[404]

IV.2.6.4.4 Veranschaulichung beider Varianten

Zur Veranschaulichung der eben dargestellten Varianten wurde von der ISPA im Anschluss an die Diskussion[405] eine graphische Darstellung ausgearbeitet, die hier zum besseren Problemverständnis abgebildet wird (Abbildung 3):

---

[401] EB zur RV, 2. Absatz zu § 92 Abs 3 Z 6b TKG, BglNR. 1074 XXIV. GP.
[402] Vgl. BIM-Datensicherheitsstudie S. 123 f.
[403] EB zur RV, 1. Absatz zu § 92 Abs 3 Z 6b TKG, BglNR. 1074 XXIV. GP.
[404] Vgl. BIM-Datensicherheitsstudie S. 124 f.
[405] Siehe die Zusammenfassung der Diskussion beim 5. Round Table, BIM-Datensicherheitsstudie S. 125.

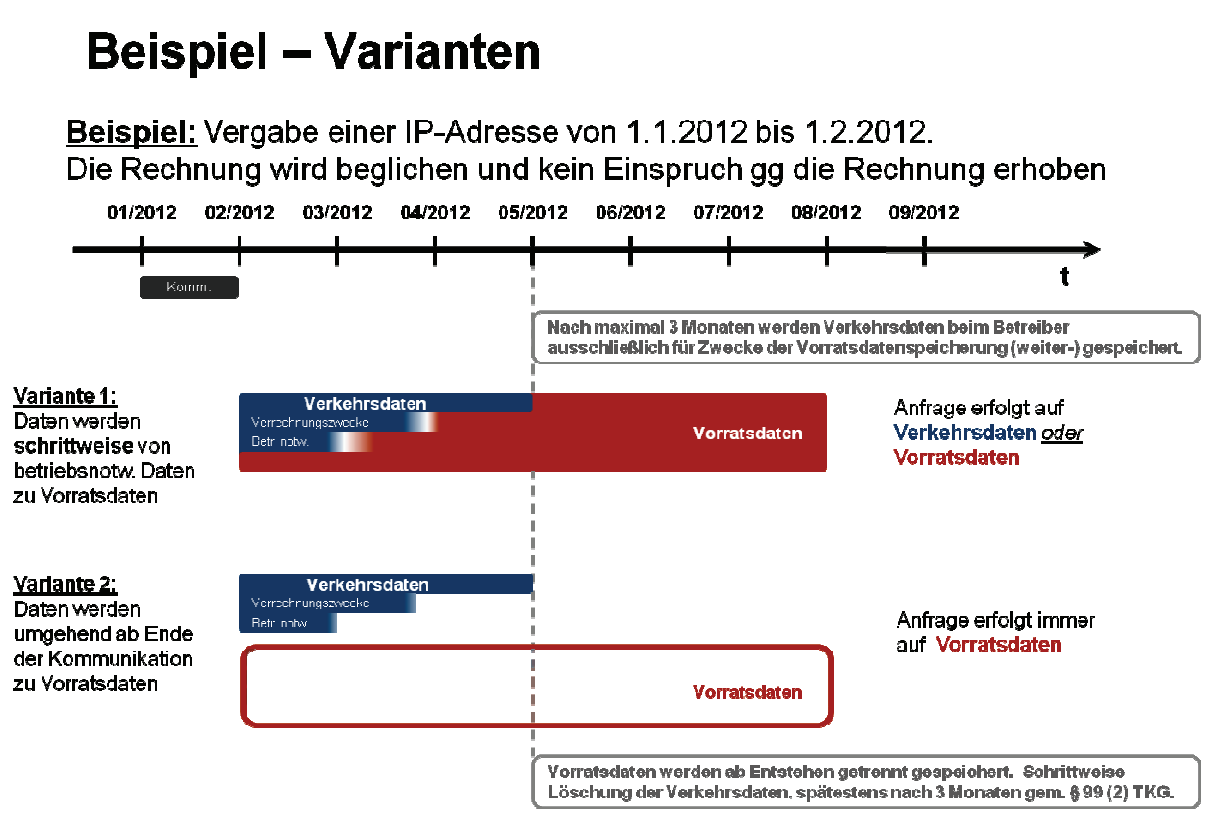

Abbildung 3: Doppelte Speicherung als Vorratsdaten und als Betriebsdaten

Variante 1: Eigenschaft als Vorratsdatum oder betriebsnotwendiges Datum schließt sich aus, manche Datenarten (grundsätzlich E-Mail Verkehrsdaten) werden immer ab der Kommunikation zu Vorratsdaten, weil keine betriebliche Notwendigkeit für diese Daten besteht.

Variante 2: Eigenschaft als Vorratsdatum und betriebsnotwendiges Datum schließt sich nicht aus, Datensätze müssen in der Vorratsdatenbank die Information enthalten, ob dieselben Daten aktuell auch noch in den betrieblichen Systemen des Anbieters vorhanden sind (Flag).

Abschließend festzuhalten ist, dass die Zulässigkeit einer sofortigen Speicherung in der Vorratsdatenbank keine Nachteile im Hinblick auf das Schutzniveau brächte. Vielmehr hätte es Vorteile, wenn Auskunftsbegehren grundsätzlich unter Zugriff auf die Vorratsdatenbank abgewickelt würden, weil dort (im Gegensatz zu den betrieblichen Systemen) ein Zugriff stets nur nach dem Vier-Augen-Prinzip unter revisionssicherer Protokollierung erfolgen darf - auch wenn die Daten zugleich noch in den betrieblichen Systemen des Anbieters vorhanden sein sollten.[406] Daher wird hier jene Auslegung bevorzugt, die eine gleichzeitige Speicherung als Vorratsdaten und Betriebsdaten zulässt. Allerdings wird diese Möglichkeit in der Praxis nicht von allzu großer Bedeutung sein. Die ursprüngliche Intention dieser Möglichkeit aus den Diskussionen zur Umsetzung lag nämlich wie bereits dargestellt in der Absicherung, dass Anfragen auf Vorratsdaten auf jeden Fall (wenn

[406] Ibid, S. 119.

überhaupt Daten vorhanden sind) erfolgreich sind, auch wenn dafür Betriebsdaten ausgewertet werden müssen. Dies kann aber deutlich leichter durch die Normierung des Größenschlusses erreicht werden, wie sogleich gezeigt wird.[407] Die Bedeutung kann aber für kleinere Anbieter bestehen bleiben, wenn gerade mit wenigen Mitarbeitern ein einheitliches Konzept für die Abwicklung von Auskünften gestaltet wird. Große Anbieter werden dies in der Praxis wohl nicht in Erwägung ziehen, weil sich ja auch der benötigte Speicherplatz im Hinblick auf noch betrieblich vorhandene Daten verdoppelt. Vielmehr wird die Abfragelogik (unter Vermeidung von Doppelspeicherung) sowohl Betriebsdaten als auch die Vorratsdatenbank abfragen – letzteres allerdings nur, wenn potentiell Daten in der Vorratsdatenbank vorhanden sein könnten.

IV.2.6.4.5 Rechtfertigt eine Anfrage nach Vorratsdaten eine Auskunft über Betriebsdaten (Größenschluss)?

Am einfachsten zu lösen ist das oben beschriebene Problem über einen Größenschluss, wonach eine Abfrage nach Vorratsdaten jedenfalls auch eine Abfrage nach Billingdaten rechtfertigen würde. Dessen Zulässigkeit ergibt sich aus den gesetzlichen Voraussetzungen für die Auskunft über Vorratsdaten gemäß § 135 Abs. 2a StPO ergibt. Dieser verweist nämlich auf die Fälle des § 135 Abs. 2 Z 2 bis 4 StPO, woraus sich ergibt, dass immer dann, wenn die Voraussetzungen für eine Auskunft über Vorratsdaten vorliegen, zugleich auch die Vorraussetzungen für eine Auskunft über „Betriebsdaten“ nach § 135 Abs. 2 StPO gegeben sind.

Ergänzend ist dazu klarzustellen, dass strengere Protokollierungsverpflichtungen bei Vorratsdatenabfragen nur dann ausgelöst werden, wenn eine Anfrage über Vorratsdaten erfolgt, die auch einen Zugriff auf (potentiell vorhandene) Vorratsdaten beim Anbieter auslöst, weil es ansonsten in der Statistik auch keine sinnvolle Auswertung zu negativen Beantwortungen geben würde. Wenn beim Anbieter nicht einmal zur Nachschau auf die Vorratsdatenbank zugegriffen wird, etwa weil aufgrund der internen Betriebsdaten-Richtlinie klar ist, dass alle angeforderten Daten noch in den betrieblichen Systemen vorhanden sind, würde eine Protokollierung als Fall der Verwendung von Vorratsdaten nur die Statistik verfälschen.

Das heißt eine Anfrage nach § 135 Abs. 2a StPO soll nur dann von der Protokollierung erfasst sein, wenn der Anbieter diese nicht allein durch Abfrage der betriebsnotwendigen Daten beantworten kann, sondern tatsächlich gezielt (allenfalls zusätzlich) Vorratsdaten abfragen muss. Umgekehrt reicht allerdings schon aus, dass der Anbieter eine Abfrage in der Vorratsdatenbank vornehmen muss, um die strengere Protokollierungspflicht auszulösen, auch wenn diese Abfrage zu keinem Ergebnis führt. Dieser Fall muss in die Statistik als erfolglose Anfrage nach Vorratsdaten Eingang finden. Außerdem muss in der Antwort klargestellt werden, ob Vorratsdaten oder Betriebsdaten verwendet wurden, da im SPG Bereich unterschiedliche Rechtsschutzfolgen an die Antwort geknüpft sind und (auch) für den StPO Bereich sonst die Statistik verfälscht wird.[408]

[407] Sie sogleich in Kapitel IV.2.6.4.5.
[408] Vgl. BIM-Datensicherheitsstudie S. 126 f.

IV.2.6.4.6 MÖGLICHKEIT EINER ZWEISTUFIGEN VORGEHENSWEISE

Eine weitere Option wäre, einen zweistufigen Prozess einzuführen. Im ersten Schritt würde eine Anfrage an die Anbieter übermittelt werden, mit der Bitte festzustellen, ob die erforderlichen Daten Billingdaten, Vorratsdaten oder allenfalls sowohl Billing- als auch Vorratsdaten sind. In einem zweiten Schritt würde dann die konkrete Antwort übermittelt.[409] Angesichts der eben beschriebenen Möglichkeit, die Zulässigkeit eines Größenschlusses in einer DSVO ausdrücklich zu normieren, stellt diese Möglichkeit aber keine gute Alternative dar, weil sie den operativen Aufwand enorm steigert.

IV.2.6.5 LÖSUNGSVORSCHLÄGE FÜR EINE DSVO

Die soeben ausgeführten Überlegungen zur Datensicherheit und zur Verschlüsselung könnten legistisch folgendermaßen erfasst werden:[410]

§ 5 Geeignete technische und organisatorische Maßnahmen zur Sicherheit von Vorratsdaten

(1) Vorratsdaten müssen vom Anbieter auf eine Weise gespeichert werden, dass deren logische Unterscheidung von Betriebsdaten bei jedem Zugriff und jeder Verwendung eindeutig ist.
(2) Eine physikalisch getrennte Datenspeicherung von Betriebsdaten und Vorratsdaten ist nicht notwendig. Der Anbieter hat durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass die Datenbank zur Speicherung von Vorratsdaten (in der Folge kurz: Vorratsdatenbank) auf eine Weise ausgestaltet ist, dass Zugriffe auf Vorratsdaten nur unter Einhaltung der besonderen Sicherheitsvorschriften gemäß § 7 möglich sind.
(3) Wenn keine betriebliche Rechtfertigung zur Speicherung als Betriebsdaten mehr vorliegt, sind diese Daten umgehend aus den betrieblichen Datenbanken zu löschen und in die Vorratsdatenbank zu überführen. Sollte die Speicherung in der Vorratsdatenbank bereits zuvor gemäß § 6 erfolgt sein, so ist die Kennzeichnung der gleichzeitigen betrieblichen Speicherung zeitgleich oder unmittelbar nach der Löschung aus den betrieblichen Datenbanken zu entfernen.
(4) Der Anbieter hat die Methode zur technischen und organisatorischen Trennung nachvollziehbar zu dokumentieren und diese Dokumentation für den Fall einer Prüfung durch die Datenschutzkommission gemäß § 102c Abs 1 TKG 2003 auf Anfrage der Datenschutzkommission zugänglich zu machen.
(5) Der Anbieter hat die tatsächliche Speicherdauer von Betriebsdaten sowie allfällige diesbezügliche interne Richtlinien (Betriebsdaten-Richtlinie) für den Fall einer Prüfung durch die Datenschutzkommission gemäß § 102c Abs 1 TKG 2003 oder auf Anfrage der Datenschutzkommission zu beauskunften.

---

[409] Ibid, S. 126 f.

[410] Die Formulierungen stammen aus der BIM-Datensicherheitsstudie S. 139 f; diese Vorschläge wurden mit nur einer rein sprachlichen Änderungen in § 5 durch das BMVIT in öffentliche Begutachtung geschickt, die bereits oben in Kapitel IV.2.3.5 dargestellt wurde und daher hier nicht wiederholt wird; die Änderung in § 5 Abs. 1, nämlich die Ersetzung des Wortes „Verarbeitung“ durch „Verwendung“ wurde hier vorweggenommen; vgl. dazu den Begutachtungsentwurf im Anhang.

§ 6 Unterscheidung von Betriebsdaten und Vorratsdaten

(1) Eine Anordnung der Staatsanwaltschaft gemäß § 135 Abs. 2a StPO zur Auskunft über Vorratsdaten berechtigt den Anbieter in jedem Fall, zur Erfüllung seiner Auskunftsverpflichtung auch Betriebsdaten zu verarbeiten und zu übermitteln. Die Verpflichtung zur Protokollierung gemäß § 7 Abs. 3 besteht nur dann, wenn der Anbieter zur Erfüllung der Auskunftsverpflichtung tatsächlich eine Abfrage in der Vorratsdatenbank durchführen muss.
(2) Wenn eine Auskunft Vorratsdaten enthält, hat der Anbieter diesen Umstand als Zusatzinformation gemäß der Schnittstellenspezifikation in der Anlage (Kapitel 1.4) zu übermitteln.
(3) Zur Vereinfachung des operativen Betriebes im Hinblick auf Datenauskünfte gemäß § 99 Abs 5 TKG 2003 oder § 102b TKG 2003 darf der Anbieter die in § 2 Abs 1 genannten Daten auch dann bereits in der Vorratsdatenbank speichern, wenn diese Daten zugleich noch als Betriebsdaten gespeichert sind. In diesem Fall ist in der Vorratsdatenbank für jede Datenkategorie kenntlich zu machen, dass diese Daten auch in den betrieblich notwendigen Datenbanken des Anbieters vorhanden sind.

Zu § 6 Abs. 1 DSVO-Entwurf wurde vom BMJ in einer Stellungnahme zum Begutachtungsentwurf angeregt, dass die Protokollierungsverpflichtung nach dieser Bestimmung auch auf Auskünfte über Betriebsdaten ausgeweitet werden sollte, weil jede staatsanwaltliche Anordnung nach § 135 Abs. 2a StPO der Kontrolle des Rechtsschutzbeauftragen gem. § 147 Abs. 1 StPO unterliege und daher seitens der Strafverfolgungsbehörden als Auskunft über Vorratsdaten (§ 135 Abs. 2a StPO) zu erfassen sei. Es solle daher aus Gründen der statistischen Einheitlichkeit auch in Fällen, in welchen der Anbieter auf Basis einer Anordnung nach § 135 Abs. 2a StPO lediglich Betriebsdaten verarbeite oder übermittle, eine Verpflichtung zur Protokollieren bestehen. Konkret wird in der Stellungnahme daher vorgeschlagen, den zweiten Satz des § 6 Abs. 1 des Entwurfs der DSVO folgendermaßen zu formulieren: „Die Verpflichtung zur Protokollierung gemäß § 7 Abs. 3 besteht in allen Fällen einer Anordnung der Staatsanwaltschaft gemäß § 135 Abs. 2a StPO zur Auskunft über Vorratsdaten."

Im Hinblick auf eine rechtsschutzfreundliche Gestaltung erscheint dieser Vorschlag auf den ersten Blick zunächst begrüßenswert. Allerdings ist hierbei Vorsicht und eine nähere Betrachtung geboten. Es ist nämlich zu unterscheiden, ob eine Datenverwendung beim Anbieter allgemein zu protokollieren ist, oder ob das speziell für Vorratsdaten konzipierte, strenge, revisionssicher zu protokollierende Zugriffsregime des § 7 DSVO-Entwurf gemeint ist. Das bedeutet nicht, dass der Auskunftsvorgang bei Verwendung von Betriebsdaten gar nicht protokolliert werden soll. Ganz im Gegenteil wäre eine solche allgemeine Protokollierungspflicht wünschenswert. Allerdings sollte eine solche Protokollierungsvorschrift wohl im TKG durch den Gesetzgeber normiert werden. Im Rahmen einer DSVO basierend auf § 94 Abs. 4 und § 102c TKG würde eine solche Pflicht wahrscheinlich die Verordnungsermächtigung überschreiten. Die Gelegenheit dazu hätte der Gesetzgeber aktuell im Zuge der derzeit im Parlament zu beratenden TKG-Novelle zur Umsetzung des neuen EU Telekom-Rechtsrahmens.[411]

Eine Protokollierung erfolgt in der Praxis außerdem schon im eigenen Interesse des Anbieters grundsätzlich, weil die Auskunft nach den Bestimmungen der Überwachungskostenverordnung dem Bund in Rechnung gestellt werden kann. Es muss sich dabei aber eben nicht um die spezielle

[411] Näher dazu oben in Kapitel II.4.1.

revisionssichere Protokollierung nach den strengeren Regeln der Vorratsdatenverwendung handeln. Der Grund dafür ist, dass Anbieter zur Aufrechterhaltung ihres Betriebes in der Lage sein müssen, auf ihre eigenen betrieblich notwendigen Daten im alltäglichen Betrieb zugreifen zu können, ohne dabei jedes Mal die Autorisierung durch eine zweite Person zu benötigen. Ansonsten würde nämlich der Personalaufwand für die Abwicklung des üblichen Betriebes eines öffentlichen Kommunikationsdienstes dermaßen unverhältnismäßig steigen, dass den österreichischen Anbietern am europäischen Markt schwere Wettbewerbsnachteile drohen würden. Ein hinreichender Sorgfaltsmaßstab bei der betrieblichen Verarbeitung von Daten sollte sich in Bezug auf Betriebsdaten auch auf andere Weise erreichen lassen.

IV.2.7 Datenschutzrechtliche Rollenverteilung[412]

IV.2.7.1 Sind die Anbieter bei der Verwendung von Vorratsdaten als Auftraggeber des privaten oder des öffentlichen Bereichs im Sinne des DSG zu sehen?

Ebenfalls von Bedeutung ist die Frage, ob die Anbieter bei der Verarbeitung von Vorratsdaten als Auftraggeber des öffentlichen oder des privaten Bereichs zu sehen sind. Der BIM-Entwurf zur TKG-Novelle[413] hatte dazu in § 102a Abs. 9 folgenden Vorschlag vorgesehen: „(9) Im Hinblick auf Vorratsdaten gilt jener Anbieter, der die Daten den vorstehenden Absätzen entsprechend zu speichern hat, als Auftraggeber des öffentlichen Bereichs gemäß § 4 Z 4 in Verbindung mit § 5 Abs. 2 Z 2 DSG 2000. Im Hinblick auf Vorratsdaten, die gemäß § 102b übermittelt werden, richten sich die Ansprüche auf Information oder Auskunft über diese Datenverwendung ausschließlich nach den Bestimmungen der StPO."

Die Erläuterungen im BIM-Entwurf TKG-Novelle 2010 beschreiben das Problem und erklären den Lösungsansatz: „Diese rechtliche Klarstellung ist notwendig, weil sich allein aufgrund der Kriterien des DSG 2000 nur schwer abschließend beantworten lässt, wer datenschutzrechtlicher Auftraggeber der Datenanwendung im Hinblick auf Vorratsdaten ist. Denn einerseits stehen die Daten, sobald sie allein aufgrund §102a gespeichert sind, nur mehr der Strafverfolgung für schwere Straftaten zur Verfügung - und damit auch nicht mehr zur beliebigen Verwendung durch die Anbieter selbst. Dies würde rechtfertigen, das BMJ als Auftraggeber zu sehen. Andererseits stehen die Daten auch der Justiz nur im Einzelfall bei Vorliegen der entsprechenden Voraussetzungen zur Verfügung, und auch in diesem Fall müssen sie erst vom Anbieter übermittelt werden. Letztlich sind es aber die Anbieter, die faktisch die Kontrolle über diese Daten ausüben und damit auch für ihre Sicherheit und rechtmäßige Verwendung verantwortlich sind. Weil sie dies aber allein aufgrund der gegenständlichen Norm tun (müssen), handeln sie in Vollziehung der Gesetze und sind damit Auftraggeber des öffentlichen Bereichs iSd § 5 Abs. 2 Z 2 DSG 2000. Im Hinblick auf Daten, die noch bzw. auch für betriebliche Zwecke des Anbieters nach § 99 vorhanden sind, gelten diese entsprechend § 5 Abs. 3 DSG 2000 als Auftraggeber des privaten Bereichs. Die entscheidende Konsequenz dieser gesetzlichen Klarstellung ist die ausschließliche Zuständigkeit der

[412] Details zu den rechtlichen Grundlagen siehe oben in Kapitel II.4.3. Hier sollen nur einige Fragen behandelt werden, die im Rahmen der Round Tables besonders diskutiert wurden.
[413] Fundstelle siehe Literaturverzeichnis.

Datenschutzkommission (DSK) für den Rechtsschutz nach dem DSG 2000. Für die Kunden der Anbieter bedeutet dies einen erleichterten Zugang zum Rechtsschutz ohne das Kostenrisiko eines Zivilprozesses. Nur in Bezug auf personenbezogene Daten, die beim Anbieter (auch) für eigene betriebliche Zwecke vorhanden sind, bleibt die Zuständigkeit der ordentlichen Gericht nach § 1 Abs. 5 DSG 2000 bestehen. Allfällige Schadenersatzansprüche, die aus einer rechtswidrigen Verwendung von Vorratsdaten durch den Anbieter resultieren, sind somit nach dem Regime des Amtshaftungsgesetzes zu beurteilen, ebenso allenfalls in weiterer Folge erwachsende Regressansprüche des Bundes gegenüber dem Anbieter. Hinsichtlich des Rechts auf Information (§ 24 DSG 2000) bzw. des Rechts auf Auskunft (§ 26 DSG 2000) besteht aber das Problem, dass die Anbieter praktisch nicht beurteilen können, wann eine Information/Auskunft die Ermittlungen gefährden würde und damit eine Ausnahme von der Informationspflicht gemäß § 24 Abs. 4 iVm § 17 Abs. 3 Z 5 DSG 2000 vorliegt, weil dies "zur Verwirklichung des Zweckes der Datenanwendung notwendig ist". Aus diesem Grund stellt der Verweis auf die Auskunft bzw. Information nach der StPO (gegenwärtig §139) als lex specialis die entsprechende Rechtssicherheit für die Adressaten des TKG her.“[414]

Der Verfassungsdienst des Bundeskanzleramts (BKA-VD) vertrat in seiner Stellungnahme im Begutachtungsverfahren zur TKG-Novelle die Ansicht, dass Anbieter (entgegen dem Vorschlag im Begutachtungsentwurf) auch bzgl. Vorratsdaten jedenfalls als Anbieter des privaten Bereichs gelten sollen. Das Argument, die Daten seien bei Anbietern nur noch deshalb vorhanden, weil der Staat die Aufbewahrung der (sonst zu löschenden) Daten für Zwecke der Strafverfolgung gesetzlich anordnet, ändere daran nichts. Denn auch in anderen Fällen, in denen das Gesetz bestimmte Datenverarbeitungen für Private vorschreibe, würden laut BKA-VD der Private dadurch nicht zum datenschutzrechtlichen Auftraggeber, der „in Vollziehung der Gesetze“ tätig werde. Für die Eigenschaft als Auftraggeber des öffentlichen Bereichs trotz Einrichtung in Form des Privatrechts komme es vielmehr darauf an, dass eine ausdrückliche gesetzliche Zuweisung von Hoheitsaufgaben und insofern einer Stellung als beliehene Organe vorliege.[415] Die im BIM-Entwurf zur TKG-Novelle vorgeschlagene Bestimmung des § 102a Abs. 9 TKG wurde folglich in der Umsetzung der TKG-Novelle auch nicht beschlossen. Umgekehrt wurde aber auch keine ausdrückliche Normierung der Gegenteiligen Ansicht des BKA-VD beschlossen. Da diese Frage ohne ausdrückliche Regelung einer Auslegung zugänglich ist, bleibt es den Gerichten vorbehalten, über diese Zuständigkeitsfrage selbst zu entscheiden. Interessant könnte dieselbe Frage auch werden, wenn ein Kunde eines Anbieters im Falle eines Datenmissbrauchs nur den Anbieter belangt und dennoch einen Amtshaftungsanspruch geltend machen will.

Die Position zu dieser Frage die der Autor dieser Arbeit bereits bei der Konzeption des Lösungsvorschlag im BIM Entwurf zur TKG-Novelle vertreten hat, wird grundsätzlich auch hier weiter aufrecht erhalten. Hier werden zudem ergänzende Argumente angeführt, die auf einer differenzierten Sichtweise unter Beachtung eines funktionellen Rollenverständnisses basieren: „Wenn die Frage aufgeworfen wird, wer von mehreren Rechtssubjekten rechtmäßiger Auftraggeber einer Datenanwendung sei (sein könne), dann ist zunächst der Zweck der Datenanwendung zu

---

[414] BIM-Entwurf TKG-Novelle 2010, S. 61; Die gesamten Erläuterungen zum besonderen Teil des BIM-Entwurf TKG-Novelle 2010 wurden vom Autor der vorliegenden Dissertation eigenverantwortlich verfasst.

[415] Siehe dazu die Stellungnahme des BKA-VD im Begutachtungsverfahren zum Ministerialentwurf einer TKG-Novelle 117/ME, XXIV GP., S. 13,
http://www.parlinkom.gv.at/PAKT/VHG/XXIV/ME/ME_00117_E3/fname_177948.pdf.

definieren. Rechtmäßiger Auftraggeber kann dann jedes Rechtssubjekt sein, das eine ausreichende Berechtigung bzw. eine gesetzliche Zuständigkeit zur Verfolgung dieses Zwecks besitzt.

Zweck der Vorratsdatenspeicherung als eigene, separate Datenanwendung ist die Strafverfolgung. Diesen Zweck kann ein Kommunikationsdienstebetreiber nicht rechtmäßigerweise verfolgen. Er könnte in diesem Bereich nur Dienstleister derjenigen Behörden sein, die den Zweck „Strafverfolgung" zu vollziehen haben. Ausgehend von den generellen Bestimmungen des DSG 2000 müssten die Strafverfolgungsbehörden als Auftraggeber begriffen werden und die Betreiber als deren Dienstleister mit der speziellen Funktion des hosting der Daten und der Durchsuchung der Daten im jeweiligen Auftrag einer Strafverfolgungsbehörde.

Der Gesetzentwurf möchte von der sich aus dem DSG 2000 ergebenden Rollenverteilung offensichtlich durch besondere Gesetzesbestimmungen abgehen. Soweit dies angesichts des § 1 DSG 2000 durch einfaches Gesetz überhaupt möglich ist, sollte die sich aus dem DSG 2000 ergebende grundsätzliche Rollenverteilung jedoch nicht völlig außer Acht gelassen werden, da sonst die Gefahr der mangelnden Ausgewogenheit - insbesondere auch im Hinblick auf den Rechtsschutz - besteht. Wenn die Betreiber NICHT als Dienstleister im üblichen Sinn fungieren sollen, sondern im Interesse eines „Vieraugenprinzips" den Strafverfolgungsbehörden quasi auf gleicher Augenhöhe gegenüberstehen und daher einen „Quasi-Auftraggeberstatus" erhalten sollen, so ist dies aufgrund besonderer gesetzlicher Bestimmungen bis u einem gewissen Grad wohl möglich. Doch darf darüber nicht vergessen werden, dass sie auch in dieser – außergewöhnlichen – Stellung jeweils nur Teil einer hoheitlichen Verwendung von personenbezogenen Daten sind. Welche datenschutzrechtliche Sonder-Rollenverteilung im vorliegenden Gesetzentwurf daher auch geschaffen werden sollte, wäre zu beachten, dass die *gesamte* Datenanwendung dem öffentlichen Bereich zuzuordnen ist, und daher alle Entitäten, denen hier eine Rolle zugeschrieben wird, sich in diesem Bereich zu bewegen haben."[416]

IV.2.7.1.1 KONSEQUENZEN FÜR DIE RECHTSDURCHSETZUNG FÜR BETROFFENE?

Nicht leicht fällt die rechtliche Beurteilung zur Frage, welchen Rechtsschutzweg ein Betroffener einschlagen müsste, wenn zB ein Datensatz seiner „Vorratsdaten" in falsche Hände gelangen würde. Ob er dann den Zivilrechtsweg gegenüber dem Anbieter wählen müsste oder ob er auch gegenüber dem Anbieter wie gegenüber einer Behörde bei der DSK vorgehen sollte, ist nicht klar geregelt. Die Übermittlung durch den Anbieter könnte dabei eine Zäsur darstellen. Wenn zu den statistischen Daten die jeweilige „Unique-ID" zum Auskunftsfall gespeichert bleibt - wenngleich nur den Rechtsschutzorganen zugänglich - ließe sich zumindest die Nachvollziehbarkeit solcher Vorgänge besser sichern.[417]

Eine Folge der Auslegung des BKA-VD ist, dass die DSK als Kontrollbehörde bei Beschwerden gegenüber Anbietern niemals zuständig wäre. Falls die Anbieter Auftraggeber des privaten Bereiches

---

[416] Waltraut Kotschy, unveröffentlichtes Memo, welches dem Autor vom ehemaligen langjährigen geschäftsführenden Mitglied der österreichischen Datenschutzkommission zum Zweck der Verwendung in dieser Dissertation anlässlich einer aufschlussreichen Diskussion bei einem gemeinsamen EU-Twinning Projekteinsatz in Montenegro zur Verfügung gestellt wurde.

[417] Vgl. BIM-Datensicherheitsstudie S. 102 f.

sind, liegt die Zuständigkeit im Falle von Datenschutzverletzungen bei den Gerichten. Die Zuständigkeit für die Geltendmachung auf Richtigstellung und Löschung von Vorratsdaten müsste demzufolge immer bei den Zivilgerichten liegen, egal ob Vorratsdaten oder Betriebsdaten betroffen sind. [418] Diese Konsequenz ist nachteilig für den Rechtsschutz, weil der Rechtsschutzsuchende im Einzelfall mit dem vollen Prozesskostenrisiko eines Zivilprozesses belastet wird, was die Hemmschwelle zweifellos erhöht, den Rechtsschutz allenfalls in Anspruch zu nehmen.

IV.2.7.1.2 INFORMATION DES BETROFFENEN

Voraussetzung dafür, dass der Betroffene einen Rechtsweg beschreiten kann ist, dass dieser von der Abfrage seiner Daten auch Kenntnis hat. Der Auskunftsanspruch nach § 26 DSG bleibt aber jedenfalls in der Zuständigkeit der Datenschutzkommission, insofern bleiben die gesamten Protokoll-Daten (nicht nur die anbieterinterne Protokollierung) auch für die Erfüllung der Aufgaben der DSK von Interesse. Denn allenfalls müsste die DSK auch prüfen können, ob die vom Anbieter intern dokumentierte Anfrage einer Behörde auch tatsächlich gestellt wurde. Schwierig gestaltet sich jedoch für den Anbieter die Entscheidung, ob er einen von einer Vorratsdatenabfrage betroffenen Kunden im Falle eines Auskunftsbegehrens gemäß § 26 DSG über die erfolgte Auskunft (oder auch die bloße Anfrage) informieren darf. Es besteht nämlich das bereits in den Erläuterungen zu § 102a Abs. 9 BIM-Entwurf TKG-Novelle ausgeführte Problem, „dass die Anbieter praktisch nicht beurteilen können, wann eine Information/Auskunft die Ermittlungen gefährden würde und damit eine Ausnahme von der Informationspflicht gemäß § 24 Abs. 4 iVm § 17 Abs. 3 Z 5 DSG 2000 vorliegt, weil dies "zur Verwirklichung des Zweckes der Datenanwendung notwendig ist".“ Daher wurde in diesem Entwurf konsequenterweise auch die Auskunft bzw. Information nach § 139 StPO als lex specialis zur Herstellung entsprechender Rechtssicherheit vorgeschlagen.

Anders ist die Rechtslage nach § 98 Abs. 2 TKG, wonach den Anbieter die Pflicht trifft, den Betroffenen frühestens nach 48 Stunden, aber spätestens nach 30 Tagen über die Tatsache zu informieren, dass sein Standort ermittelt wurde. Diese Information hat wenn möglich mittels Kurzmitteilung (SMS) zu erfolgen. Es wurde diskutiert, dass es Fälle geben kann, bei denen diese Kurznachricht die kriminalpolizeiliche Ermittlung behindern kann. Diese Konstellation ist allerdings nur dann denkbar, wenn zuvor ein Notruf abgesetzt wurde und sich der Inhaber der Endeinrichtung, von der der Notruf abgesetzt wurde, in der Gewalt einer anderen Person befindet. Dann könnte nämlich sein, dass die Verständigung über die Ortung auf das Endgerät der gefährdeten Person dem Entführer zur Kenntnis gelangt. Es wurde diskutiert, nach welchen Kriterien von den Netzanbietern diese Frist gewählt wird. Nach Aussagen vom BMI würde es ausreichend sein, wenn diese Bestimmung erst ab 1. April 2012 umgesetzt wird. Allerdings gehört die betreffende gesetzliche Bestimmung im TKG aber zu jenen Teilen, die sofort in Kraft getreten sind. Es wird hier wohl erforderlich sein, eine Information von der Polizei an die Netzanbieter zu übermitteln, für den Fall, dass eine Information des Betroffenen erst zu einem späteren Zeitpunkt unter Ausnutzung der vollen 30 Tage Frist erfolgen soll.[419]

[418] Vgl. BIM-Datensicherheitsstudie S. 45f.
[419] Ibid, S. 116.

IV.2.8 PROTOKOLLIERUNG DER DATENVERWENDUNG

Die DLS soll nicht nur dem Datenaustausch dienen, sondern auch Protokollierungaufgaben erfüllen. Europarechtlich besteht eine Pflicht zur Protokollierung soweit Vorratsdaten von einer Datenauskunft betroffen sind. Die Protokollierung hat derartig zu erfolgen, dass die Bundesregierung jedenfalls über jene Rohdaten verfügt, welche sie zur Erfüllung ihrer Verpflichtung nach Art. 10 RL 2006/24/EG, der Kommission jährlich eine Statistik zu übermitteln, benötigt.[420] Gleichzeitig soll damit auch eine wesentliche Rechtsschutzaufgabe erfüllt werden. Die Aufbereitung der Statistik für die EU-Kommission obliegt dem Justizministerium, welchem die Protokolldaten daher nach Abs. 4 zu übermitteln sind.[421]

IV.2.8.1 REVISIONSSICHERE PROTOKOLLIERUNG UND 4-AUGEN-PRINZIP

Auseinanderzuhalten sind die Protokollierung der Auskunftsvorgänge, die über die DLS erfolgen soll und dabei insbesondere die Rohdaten für die Erstellung einer Statistik liefern soll einerseits und die Protokollierung, die ein Anbieter innerhalb seiner Systeme intern gemäß § 102c TKG vorzunehmen hat, wenn er auf Vorratsdaten zugreift.

Der Regelungsbedarf zu diesem Themenkreis steht unmittelbar unter dem Eindruck des Urteils des deutschen Bundesverfassungsgerichts.[422] Dort wird ausgeführt: „Wenn der Gesetzgeber eine flächendeckende Speicherung der Telekommunikationsverkehrsdaten ausnahmslos vorschreibt, gehört es zu den erforderlichen Voraussetzungen, dass die betroffenen Anbieter nicht nur ihre Pflicht zur Speicherung, sondern auch die korrespondierenden Anforderungen zur Datensicherheit erfüllen können. Anknüpfend an die sachverständigen Stellungnahmen liegt es nahe, dass nach dem gegenwärtigen Stand der Diskussion grundsätzlich eine getrennte Speicherung der Daten, eine anspruchsvolle Verschlüsselung, ein gesichertes Zugriffsregime unter der Nutzung etwa des Vier-Augen-Prinzips sowie eine revisionssichere Protokollierung sichergestellt sein müssen, um die Sicherheit der Daten verfassungsrechtlich hinreichend zu gewährleisten (1 BvR 256/08, Absatz 224). Erforderlich sind gesetzliche Regelungen, die einen solchen besonders hohen Sicherheitsstandard in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgeben. Dabei steht es dem Gesetzgeber frei, die technische Konkretisierung des vorgegebenen Maßstabs einer Aufsichtsbehörde anzuvertrauen. Der Gesetzgeber hat dabei jedoch sicherzustellen, dass die Entscheidung über Art und Maß der zu treffenden Schutzvorkehrungen nicht letztlich unkontrolliert in den Händen der jeweiligen Telekommunikationsanbieter liegt. Die zu stellenden Anforderungen sind entweder durch differenzierte technische Vorschriften – möglicherweise gestuft auf verschiedenen Normebenen – oder in allgemein- genereller Weise vorzugeben und dann in transparenter Weise durch verbindliche Einzelentscheidung der Aufsichtsbehörden gegenüber den einzelnen Unternehmen zu konkretisieren. Verfassungsrechtlich geboten sind weiterhin eine für die

[420] Synergien könnten sich auch ergeben, wenn die Protokollierung im Zusammenhang mit der Verrechnung der einzelnen Auskunft nach der Überwachungskostenverordnung erfolgen kann.
[421] BIM Entwurf TKG Novelle 2010, S. 31.
[422] BVerfG, 1 BvR 256/08 Urteil vom 2. März 2010.

Öffentlichkeit transparente Kontrolle (…) sowie ein ausgeglichenes Sanktionensystem, das auch Verstößen gegen die Datensicherheit ein angemessenes Gewicht beimisst.“[423]

Diesen Anforderungen wird die österreichische Umsetzung im ersten Schritt gerecht, indem sie in § 102c TKG 2003 die Notwendigkeit der Unterscheidung von Vorratsdaten und Betriebsdaten, des Vier-Augen-Prinzips beim Zugriff sowie die revisionssichere Protokollierung solcher Zugriffe schon im Gesetz normiert, während die genaueren technischen Vorgaben mit dieser Verordnung geregelt werden. Auch was die Kontrolle durch die Datenschutzkommission betrifft, wird diese abgestufte Regelungstechnik den Anforderungen gerecht. Die für die Öffentlichkeit transparente Kontrolle kann insbesondere dadurch hergestellt werden, dass die statistischen Daten aus der Protokollierung über die DLS (siehe § 22) gemäß § 102c Abs. 4 TKG 2003 auch dem Nationalrat und dem Datenschutzrat zugänglich sein müssen. Was das ausgeglichene Sanktionensystem betrifft, so greifen hier die bereits bestehenden ausdifferenzierten Haftungsvorschriften des DSG 2000, insbesondere durch § 1 Abs. 5, der im Verfassungsrang die Drittwirkung des Grundrechts normiert und den Rechtsweg an die Zivilgerichte eröffnet.[424]

Wesentlich für den gegenständlichen Themenkreis ist, dass jeder Zugriff auf Vorratsdaten durch zwei Personen mit einer besonderen Ermächtigung hierzu autorisiert sein muss. Außerdem müssen Zugriffe auf Vorratsdaten beim Anbieter revisionssicher protokolliert werden. Die wichtigsten Kriterien sind dabei der Schutz vor Veränderung und Verfälschung, die Vollständigkeit, die Ordnungsmäßigkeit, die Sicherung vor Verlust, die Einhaltung der Aufbewahrungsfristen sowie die Dokumentation, Nachvollziehbarkeit und Prüfbarkeit des Verfahrens, wozu etwa bei Anordnungen der Staatsanwaltschaft auch die Angabe der Geschäftszahl der ermittelnden Kriminalpolizei zählt.[425] Bisher ist bei den Anbietern lediglich ein Zugriffsmanagement vorhanden. Aufgezeichnet wird, wer zum Zugriff autorisiert ist, sowie die Zugriffe selbst. Dem Zugriffsmanagement liegt ein „Prozess des Misstrauens“ zugrunde. Wenn es einen Verdacht gibt, hebt die Revision die entsprechenden Daten aus und die Zugreifenden müssen belegen, warum sie auf die Daten zugegriffen haben.[426] Dies ist in Bezug auf Vorratsdaten nicht ausreichend.

Das Ziel des Vier-Augen Prinzips ist, dass nicht eine einzelne Person unbemerkt und unkontrolliert auf diese Daten zugreifen kann. Der Zugriff muss dabei nicht durch zwei autorisierte Mitarbeiter des Unternehmens gleichzeitig erfolgen, die Autorisierung durch die zweite Person kann auch nachträglich erfolgen. „Zeitnah zum Zugriff durch die erste Person“ gibt dabei keine absolute Zeitschranke vor, diese Formulierung indiziert vielmehr, dass zwischen dem Zugriff und der Autorisierung des Zugriffs durch eine zweite Person nicht mehr Zeit vergeht, als im Sinne der arbeitsökonomischen Ausgestaltung der betrieblichen Abläufe noch zumutbar erscheint. Die Anbieter sind zwar nicht verpflichtet, einen „Journaldienst“ zur Beantwortung von Auskunftsersuchen einzurichten, dennoch bieten in der Praxis einige (vor allem große) Anbieter die Möglichkeit, dass Anfragen außerhalb der Geschäftszeiten vor allem durch technisches

---

[423] Ibid Rn. 225.
[424] Im Detail dazu oben in Kapitel II.4.3.
[425] Aus der Ausschussfeststellung anlässlich der Umsetzung der Vorratsdatenspeicherung im Ausschuss für Forschung, Innovation und Technoloige (FIT Ausschuss) des Nationalrats, siehe dazu den Ausschussbericht BlgNR 1157 XXIV. GP, zitiert nach BIM-Datensicherheitsstudie S. 147.
[426] Aus den unveröffentlichen Protokollen der Arbeitssitzungen im Rahmen der ”Arbeitsgruppe Schnittstellendefinition” des AK-TK.

Wartungspersonal rasch abgewickelt werden, wobei hier regelmäßig nur eine nachträgliche zweite Autorisierung erfolgen kann. Insgesamt muss aber jedenfalls systematisch sichergestellt sein, dass der Anbieter intern über ein effektives Kontrollsystem zur Sicherstellung der Verantwortung verfügt. Dies kann etwa dadurch erreicht werden, dass der Anbieter in kurzen Abständen eine regelmäßige Überprüfung von Zugriffen ohne zweite Autorisierung auch durch technische Ausgestaltung (zB automatische Notifikation) institutionalisiert. Die unmittelbare verfassungsrechtliche Pflicht der Anbieter aufgrund der Drittwirkung des § 1 Abs. 5 DSG 2000 gebietet auch eine entsprechende Dokumentation schon durch die Anbieter selbst, und nicht nur durch die Strafverfolgungsbehörden, denen die Daten im Auskunftsfall übermittelt werden.

Der Begriff der Revisionssicherheit orientiert sich dabei an den Grundsätzen einer ordnungsgemäßen Buchführung in den unternehmensrechtlichen Vorschriften (insbesondere dem UGB) und dient dem Ziel, die Nutzung nur durch Berechtigte und die Einhaltung der Verfahrensvorschriften sicherzustellen. Die Einhaltung der oben formulierten Kriterien ist dabei durch die technische Ausgestaltung des Zugriffsregimes auf die Datenbank sicherzustellen.

Der Inhalt der Protokollierung ist bereits durch § 102c Abs. 2 TKG 2003 detailliert vorgegeben, sollte aber in einer DSVO einerseits zur Rechtsklarheit wiederholt, andererseits im Sinne der Eindeutigkeit der zu protokollierenden Informationen, allenfalls um Verweise auf Bestimmungen innerhalb der Verordnung im Zusammenhang mit der Durchlaufstelle ergänzt. Ergänzungen sind insbesondere im Hinblick auf die Erfassung von Speicherzeiträumen bzw. des Datums notwendig. So sollte das Datum der Anfrage sich auf die jeweilige Hinterlegung in der Durchlaufstellte beziehen. Diese Daten sind für den Anbieter überdies nur sehr schwer automatisiert zu erfassen (bzw. zu verpacken, da z.B. die Zustellung in das Postfach der DLS nach Erstellung des Protokollfiles beim Anbieter geschieht). Daher sollte hierzu normiert werden, dass diese Informationen über die DLS direkt protokolliert und an den Anbieter weitergeleitet werden. Der Anbieter kann sodann diese Protokollinformationen von der DLS für seine interne Protokollierung automatisiert weiterverwenden.

Klarzustellen ist, dass das Datum zur Aufschlüsselung der abgefragten Datensätze sich auf den Beginn des Kommunikationsvorgangs bezieht, zumal dieser Wert auch im Rahmen der Vorratsdatenspeicherungspflicht gemäß § 102a Abs. 2 bis 4 TKG 2003 relevant ist. Zu berücksichtigen ist dabei, dass dem Anbieter nur das Datum der Anordnung gemäß § 138 Abs. 3 StPO (sog. Anbieterausfertigung) bzw. das Datum der Anordnung nach § 53 Abs. 3a oder 3b SPG bekannt ist. Für die Berechnung der Speicherdauer muss der Zeitpunkt der Anordnung der Übermittlung mit dem Zeitpunkt der Speicherung als Vorratsdatensatz verglichen werden. Da die Anordnung nur ein Datum aber keinen genauen Zeitpunkt enthält, ist für die Berechnung auch nur das Datum der Speicherung als Vorratsdatum relevant. Die Verordnung sollte daher – im Gegensatz zu § 102c Abs. 2 Z 5 TKG – nur das Datum und nicht der Zeitpunkt nennen, um Klarheit für die Protokollierung zu schaffen.

Jeder Zugriff auf Vorratsdaten – darunter fallen bereits Zugriffe zur Nachschau, ob Daten vorhanden sind, auch wenn schließlich keine Daten beauskunftet werden[427] - muss protokolliert werden. Dies hat unabhängig davon zu erfolgen, wer der Anfragende ist. Dabei muss die Protokollierung entsprechend der Verordnung ausgeführt werden, die wiederum die Protokollierungsvorschriften des § 102c TKG konkretisieren soll.

[427] ZB weil gar keine Daten vorhanden sind.

Bei einer Anfrage nach § 135 Abs. 2 StPO ist keine interne Protokollierung beim Anbieter notwendig, da keine Vorratsdaten angegriffen werden. Eine Auskunft, dass keine betriebsnotwendigen Daten vorhanden sind, jedoch Vorratsdaten (auch nur die bloße Information über das Vorhandensein) ist laut Gesetz nicht vorgesehen. Bei einer Anfrage nach § 135 Abs. 2a StPO ist auf jeden Fall nach den strengen Vorschriften des § 102c TKG zu protokollieren. Die Verordnung sollte dazu ausdrücklich festhalten, dass eine Anfrage nach Daten, die durch Zugriff auf die Betriebsdaten völlig erfüllt werden kann, keine Protokollierungspflicht nach den Regelungen der (Anbieter-internen) Zugriffsprotokollierung zu Vorratsdaten auslöst. [428]

Ob tatsächlich Vorratsdaten von der Auskunft betroffen sind bzw. ob ein Zugriff auf die Vorratsdatenbank für die Bearbeitung des Auskunftsbegehrens notwendig war, soll vom Anbieter als Zusatzinformation über die DLS übermittelt werden. Dies ist in der technischen Spezifikation zur DLS entsprechend zu berücksichtigen.[429]

IV.2.8.1.1 Lösungsvorschlag für eine DSVO

Die soeben ausgeführten Überlegungen zur revisionssicheren Protokollierung und zum 4-Augen-Prinzip könnten legistisch folgendermaßen erfasst werden:[430]

§ 7 Revisionssichere Protokollierung und Vier-Augen-Prinzip bei Zugriffen auf Vorratsdaten

(1) Der Anbieter hat seine Systeme auf technischer und organisatorischer Ebene so auszugestalten, dass Zugriffe auf Vorratsdaten nur durch besonders ermächtigte Mitarbeiter unter Einhaltung des Vier-Augen-Prinzips möglich sind. Jeder Zugriff auf Vorratsdaten muss durch zwei Personen mit einer besonderen Ermächtigung hierfür autorisiert sein. Die Autorisierung durch die zweite Person kann auch zeitnah zum Zugriff durch die erste Person nachträglich erfolgen, wenn dabei die effektive Wahrung des Vier-Augen-Prinzips sichergestellt ist.
(2) Zugriffe auf Vorratsdaten müssen beim Anbieter so protokolliert werden, dass die Protokolldaten vor Veränderung und Verfälschung geschützt sind und die Vollständigkeit, die Ordnungsmäßigkeit, die Sicherung vor Verlust, die Einhaltung der Aufbewahrungsfristen sowie die Dokumentation, Nachvollziehbarkeit und Prüfbarkeit des Verfahrens gewahrt sind (revisionssichere Protokollierung).
(3) Die Protokollierung umfasst
    1. die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Referenz zur staatsanwaltschaftlichen oder gerichtlichen Anordnung gemäß den Bestimmungen der StPO, die der Übermittlung der Daten zugrunde liegt,

    2. in den Fällen des § 99 Abs. 5 Z 3 und 4 TKG 2003 die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Aktenzahl der Sicherheitsbehörde,

---

[428] Siehe dazu aber oben die Anmerkung zur Stellungnahme des BMJ im Begutachtungsverfahren zu § 6 Abs. 1 DSVO-Entwurf in Kapitel IV.2.6.5.
[429] Vgl. zum Ganzen Thema die Erläuterungen zu § 7 DSVO-Entwurf in der BIM-Datensicherheitsstudie S. 157 ff.
[430] Die Formulierungen stammen aus der BIM-Datensicherheitsstudie S. 140 f; diese Vorschläge wurden mit einer Ergänzung in Abs. 3 Z 5 und der Ergänzung einer neuen Z 8 durch das BMVIT in öffentliche Begutachtung geschickt, die nachfolgend dargestellt und besprochen werden; vgl. dazu den Begutachtungsentwurf im Anhang.

3. das Datum der Anfrage (Zustellung in das Postfach des Anbieters in der Durchlaufstelle gemäß § 18 Abs. 1) sowie das Datum und den genauen Zeitpunkt der erteilten Auskunft (Zustellung der Antwort in das Postfach der Behörde in der Durchlaufstelle gemäß § 18 Abs. 3), wobei diese Daten von der Durchlaufstelle als Zusatzinformation an den Anbieter zu übermitteln sind,

4. die nach dem Datum des Beginns des Kommunikationsvorganges und den Kategorien gemäß § 102a Abs. 2 bis 4 TKG 2003 (Einteilung der Kategorien gemäß der Anlage, Kapitel 1.1.2) aufgeschlüsselte Anzahl der übermittelten Datensätze,

5. die Speicherdauer der übermittelten Daten ab dem Datum, seit dem die Daten als Vorratsdaten gemäß § 2 Abs. 2 Z 2 gespeichert wurden, zum Zeitpunkt der Anordnung der Übermittlung (Datum der staatsanwaltschaftlichen Anordnung gemäß § 138 Abs. 3 StPO oder Datum der Anfrage nach § 53 des Sicherheitspolizeigesetzes – SPG, BGBl. Nr. 566/1991 in der Fassung BGBl. I Nr. 33/2011),

6. den Namen und die Anschrift des von der Auskunft über Vorratsdaten betroffenen Teilnehmers, soweit der Anbieter über diese Daten verfügt sowie

7. eine eindeutige Kennung, welche eine Zuordnung der Personen ermöglicht, die im Unternehmen des Anbieters auf Vorratsdaten zugegriffen haben.

Für den Begutachtungsentwurf des BMVIT wurde § 4 wie folgt abgeändert:

Revisionssichere Protokollierung und Vier-Augen-Prinzip bei Zugriffen auf Vorratsdaten
§ 7. (1) (…)

(3) Die Protokollierung umfasst
(…)
5. die Speicherdauer der übermittelten Daten ab dem Datum, seit dem die Daten *als Betriebsdaten (§ 2 Abs. 2 Z 1) und* als Vorratsdaten gemäß § 2 Abs. 2 Z 2 gespeichert wurden, zum Zeitpunkt der Anordnung der Auskunft (Datum der staatsanwaltschaftlichen Anordnung gemäß § 138 Abs. 3 StPO oder Datum der Anfrage nach § 53 des Sicherheitspolizeigesetzes – SPG, BGBl. Nr. 566/1991 in der Fassung BGBl. I Nr. 33/2011),
(…)
8. im Fall von Auskünften über Vorratsdaten (§ 135 Abs. 2a StPO) die der Anordnung zu Grunde liegende strafbare Handlung.

Beide Ergänzungen wurden für den Begutachtungsentwurf von Seiten des BMJ vorgeschlagen. Nach der Änderung in Z 3 sollte für die Protokollierung auf den Speicherbeginn als Betriebs- und Vorratsdatum abgestellt werden, da ansonsten auf Grund der unterschiedlichen Geschäftsmodelle vergleichbare Daten bei unterschiedlichen Anbietern unterschiedlich lange als Vorratsdatum gespeichert sind. Sollte tatsächlich nur auf die Speicherdauer als Vorratsdatum abgezielt werden, ergäbe sich auch regelmäßig ein Zugriff auf „jüngere“ Daten als tatsächlich der Fall sei.

Seitens der Wirtschaftskammer Österreich (WKO) wurde in der Stellungnahme zum Begutachtungsverfahren[431] zu dieser Änderung argumentiert, dass Art 10 der RL 2006/24/EG nur auf die Dauer der Vorratsdatenspeicherung abstelle und die Bestimmung zur Angabe der Speicherdauer von Betriebsdaten daher aus Z 5 gestrichen werden sollte. In der Stellungnahme von T-Mobile wird zu diesem Argument ergänzt, dass die Speicherdauer von Betriebsdaten auch in der Protokollierungsvorschrift des § 102c Abs. 2 TKG nicht gefordert werde. Dem ist zu entgegnen, dass die Richtlinie 2006/24/EG nicht eindeutig Aufschluss gibt, welche Information für die Statistik tatsächlich benötigt wird. Es ist verständlich, dass diese Ergänzung seitens der Anbieter kritisiert wird, weil für die Anbieter nicht einfach ist, den jeweils richtigen Zeitpunkt festzustellen und auf die Speicherdauer zurückzurechnen. Allerdings ist die Vorschrift des Art 10 der RL 2006/24/EG nur als Mindestanforderung aus unionsrechtlicher Perspektive zu sehen, welche den Mitgliedsstaat jedoch nicht daran hindert, ein strengeres Protokollierungsregime vorzusehen. Ernst zu nehmen ist das Argument, dass die Ergänzung nicht von der einschlägigen gesetzlichen Bestimmung des § 102c Abs. 2 TKG gedeckt ist, weil damit angedeutet wird, dass die Verordnung insofern überschießend und daher gesetzwidrig sein könnte. Zu prüfen ist allenfalls, ob die Erweiterung ihre gesetzliche Deckung in einer anderen Norm des TKG finden könnte, etwa in der allgemeinen Anforderung an die Datensicherheit gemäß § 94 Abs. 4 TKG, um diesem Einwand zu begegnen.

Die Ergänzung der Z 8 beruht darauf, dass Art 10 der RL 2006/24/EG auch statistische Daten über die Fälle fordert, in welchen Vorratsdaten beauskunftet werden. Diesbezüglich wäre auf das der Anordnung zu Grunde liegende Delikt abzustellen. Das ist richtig und sollte insofern in der DSVO ergänzt werden, als diese Daten im Ergebnis in den Rohdaten für die Statistik enthalten sein müssen. Damit ist aber nicht zwingend verbunden, dass diese Informationen im Zusammenhang mit der internen Protokollierung des Anbieters an die DLS geliefert werden müssen. Ebenso gut könnte die Abfragemaske der DLS die Eingabe dieser Informationen bereits bei der Anfrage auf Behördenseite verlangen. Insofern ist geradezu verwunderlich, dass dieser Vorschlag in den Stellungnahmen seitens der Anbieter nicht kritisiert wurde.

In mehreren Stellungnahmen von Seiten der Anbieter wurde im Begutachtungsverfahren darauf hingewiesen, dass die Anforderungen an das 4-Augen-Prinzip gemäß § 7 Abs. 1 DSVO-Entwurf näher konkretisiert werden soll. Diese Kritik sollte ernst genommen und die Möglichkeiten für eine nähere Determinierung nochmals diskutiert werden.

IV.2.8.2 WAS SIND DIE PROTOKOLLDATEN DER DLS?

Einerseits müssen wie im vorherigen Unterkapitel dargestellt die sog. anbieter-internen Protokolldaten vorliegen (vgl. § 102c Abs 1 TKG). Anbieter müssen intern revisionssicher protokollieren, dass Zugriffe auf Vorratsdaten unter Einhaltung des 4-Augen-Prinzips nur durch speziell ermächtigte und bestimmte Personen und nur aufgrund einer entsprechenden behördlichen bzw. gerichtlichen Anfrage erfolgt sind.

Dem gegenüber stehen jene Protokoll bzw Statistik-Aufzeichnung über erfolgte Vorratsdaten-Abfragen (vgl. § 102c Abs 1 TKG): Die Kontrolle über die Einhaltung dieser Vorschriften obliegt der für

[431] Wie bereits mehrfach erwähnt, wurden die Stellungnahmen nicht veröffentlicht, aber dem Autor zur Verwendung für diese Dissertation vom BMVIT zur Verfügung gestellt.

die Datenschutzkontrolle gemäß § 30 DSG 2000 zuständigen Datenschutzkommission. Diese beiden Protokollverpflichtungen überschneiden sich allerdings im Hinblick auf den Informationsgehalt. Die Protokollierung für die Statistik muss diese anbieter-internen Informationen (also welche Mitarbeiter wann zugegriffen haben) allerdings nicht enthalten.[432]

Welche Informationen der Anbieter bei der Abwicklung von behördlichen Auskunftsbegehren zu protokollieren hat, ist bereits detailliert in § 102c Abs. 2 TKG 2003 geregelt, sollte aber im Sinne der Rechtsklarheit in einer DSVO mit ergänzenden Verweisen auf relevante Bestimmungen dieser Verordnung wiederholt werden. Die Protokolldaten der DLS beziehen sich indes auf jene Protokoll-Informationen, die der Anbieter gemäß § 102c Abs. 4 TKG 2003 an die dort genannten Stellen (Datenschutzkommission, Datenschutzrat, BMJ) zu übermitteln hat. Bei der Entwicklung des Konzepts der Durchlaufstelle wurde dabei bedacht, dass die zentrale Sammlung der für die Statistik notwendigen Protokollinformationen für diese Zwecke in der DLS eine enorme Verfahrens- und Verwaltungsvereinfachung darstellt. Dabei werden jene – nicht personenbezogenen – Informationen aus der Protokollierung beim Anbieter mit der (verschlüsselten) Auskunft unverschlüsselt mitgeliefert, sodass diese in der DLS für die Aufbereitung der Statistik gespeichert werden können. Diese Methode ist zugleich ein wertvoller Beitrag zur Datensicherheit, weil damit zugleich eine revisionssichere Protokollierung aller Auskunftsfälle in der DLS selbst erfolgt. Für den Fall, dass die Rechtsschutzbeauftragten, die Datenschutzkommission oder ein Gericht im Verfahren gemäß § 32 DSG 2000 für die Überprüfung der Rechtmäßigkeit eines bestimmten Falles der Datenübermittlung die exakten personenbezogenen Daten benötigt, die auf der Seite der Anbieter gemäß § 7 DSVO-Entwurf gespeichert werden und auch auf Seiten der Behörden nach den für diese einschlägigen (internen) Verfahrensvorschriften zu erfassen und aufzubewahren sind, kann die statistische Erfassung über die DLS äußerst hilfreich sein. Über die Unique-ID (§ 13 DSVO-Entwurf) kann nämlich im Rechtsschutzfall der gesamte Ablauf vom Auskunftsbegehren bis zur Beantwortung lückenlos nachvollzogen werden und die richtigen Protokolldaten werden so auf der jeweils überprüften Seite (Anbieter oder Behörden) leichter auffindbar.

Deutlich vereinfacht wird dabei auch das Verfahren für die Aufbereitung der Statistik, die das BMJ jährlich an die EU-Kommission gemäß Art 10 der Richtlinie 2006/24/EG zu übermitteln hat. Über die DLS sollen alle Rohdaten automatisch gesammelt werden, die für die Statistik notwendig sind.[433] Hier ist darauf hinzuweisen, dass in der TKG Novelle zur Umsetzung der Vorratsdatenspeicherung ein Redaktionsversehen unterlaufen ist, das dazu führen würde, dass die notwendigen Rohdaten zur Erfüllung dieser gemeinschaftsrechtlichen Verpflichtung unmöglich machen würde. § 102c Abs. 4 Z 2 ordnet nämlich an, dass die Anbieter die Protokolldaten gemäß § 102c Abs. 2 Z 2 bis 4 an das BMJ zu übermitteln haben. Damit würden die Anbieter für die Statistik die Aktenzahlen zu den Auskunftsfällen nach SPG (Z 2 leg cit) übermitteln, nicht aber die Information zur Speicherdauer der übermittelten Daten (Z 5 leg cit), die nach Art 10 Abs. 1 zweiter Spiegelstrich RL 2006/24/EG ausdrücklich gefordert sind. Dieses Versehen entstand dadurch, dass die Z 2 in § 102c Abs. 2 TKG 2003 im Zuge der Entstehung der Regierungsvorlage erst nachträglich eingefügt wurde, die entsprechende Anpassung im Absatz 4 aber unterblieb. In einer DSVO sollte daher die unverzügliche Korrektur dieses Redaktionsversehens durch den Gesetzgeber antizipiert werden.[434] Um zu

[432] Vgl. BIM-Datensicherheitsstudie S. 171.
[433] Zur automatischen Aufbereitung der Statistik in der DLS siehe unten Kapitel IV.2.9.
[434] Konkret durch einen Verweis auf die „richtigen" Protokolldaten gemäß § 7 Abs. 3 Z 3 bis 5 DSVO-Entwurf.

vermeiden, dass die Verordnung aus rein formalistischen Gründen wegen Gesetzwidrigkeit beim Verfassungsgerichtshof angefochten und möglicherweise in diesem Punkt für nichtig erklärt wird, sollte der Gesetzgeber daher schnellstmöglich die Richtigstellung im Gesetz selbst vornehmen, zugleich zur Vermeidung, dass die europarechtlichen Verpflichtung zur Übermittlung der Statistik aufgrund eines bloßen Versehens nicht erfüllt werden kann.

IV.2.8.2.1 WAS WIRD PROTOKOLLIERT: NUR VORRATSDATEN ODER AUCH BETRIEBSDATEN?

Die Protokollierung von Verkehrsdatenauskünften ist nur bzgl. Vorratsdaten europarechtlich zwingend. Nicht nur für einen höheren Rechtsschutzstandard sondern schon aus praktischen Gründen sollte jedoch überlegt werden, diese innerstaatlich auf alle Verkehrsdatenauskünfte auszudehnen. Überwiegend werden nämlich in ein und demselben Auskunfts-Datensatz gleichzeitig sowohl Vorratsdaten als auch Betriebsdaten enthalten sein. Als Beispiel sei ein Mobiltelefon-Gespräch angeführt: während die Information, wer mit wem wie lange telefoniert hat (Telefoniedaten) beim Anbieter noch für die Rechnungslegung gespeichert ist, benötigt dieser die Standortinformation nicht mehr für eigene Zwecke. Die Standortdaten in diesem Datensatz wären dann Vorratsdaten.[435]

Nach § 90 Abs. 1 Z 7 des jüngsten Vorschlags für eine TKG-Novelle zur Umsetzung des neuen EU Telekom-Rechtsrahmens[436] ist die Zahl der Anfragen nach § 94 Abs. 4 dieses Entwurfs zur TKG-Novelle zu erheben. Das bedeutet im Klartext, dass nach diesem Vorschlag eine gesetzliche Verpflichtung entstehen soll, sämtliche Auskunftsvorgänge über Verkehrsdaten zu protokollieren, egal ob es sich um Vorratsdaten oder „Billingdaten" handelt. Es ist daher notwendig, die Protokollierungspflicht nach der Umsetzung des neuen Rechtsrahmens mit den Protokollierungsverpflichtungen gemäß der TKG-Novelle zur Vorratsdatenspeicherung und einer umsetzenden DSVO abzugleichen.[437]

IV.2.8.2.2 SOLLTEN DIE PROTOKOLL-DATEN ZENTRAL BEI DER DLS GESPEICHERT WERDEN?

Im Rahmen der Protokollierung stellt sich zunächst die Frage, inwiefern eine zentrale Speicherung erforderlich bzw. sinnvoll ist.

Das BMJ schlägt ein dezentrales Modell vor: Die Übermittlung dieser Protokolldaten durch die einzelnen Anbieter im jährlichen Abstand an z.B. das BMJ wäre eine Alternative zu dieser Vorgangsweise, die auch nur unwesentlich mehr Aufwand verursachen würde.[438]

Folgende Argument sprechen dagegen für ein zentrales Modell: Es besteht eine Verpflichtung zur jährlichen Berichterstattung gegenüber der Europäischen Kommission. Die Erfassung der Protokolldaten im Rahmen der Durchlaufstelle könnte diese Erfassung der Protokolldaten für Anbieter sowie Behörden deutlich vereinfachen. Denn ansonsten müssen die Protokolldaten von

---

[435] Vgl. BIM-Datensicherheitsstudie S. 89.
[436] Näher dazu oben in Kapitel II.4.1.
[437] Vgl. BIM-Datensicherheitsstudie S. 87.
[438] Ibid, S. 87.

allen Anbietern eingesammelt und in einheitlicher Struktur zusammengeführt werden. Die Harmonisierung der Protokoll-Struktur müsste also jedenfalls geregelt werden.[439]

IV.2.8.2.3 Erfassung von Protokolldaten direkt bei der Anfrage

Von Beginn der Entwicklung des Konzepts der DLS an war ein beachtliches Argument für eine zentrale Abwicklung von Datenauskünften, dass direkt bei der Anfrage von der DLS die entsprechende Protokollierung angefertigt werden kann, um so den Protokoll-Datensatz zu einer Anfrage zu „eröffnen“. Alle Anfragen über die DLS sollen mit einer "*Unique-ID*" versehen werden. Die vom Anbieter übermittelte Antwort ist über dieselbe "*Unique-ID*" verknüpft und kann so den Datensatz zur Protokollierung mit den weiteren benötigten Information ergänzen.

Dazu die Veranschaulichung in der Grafik:

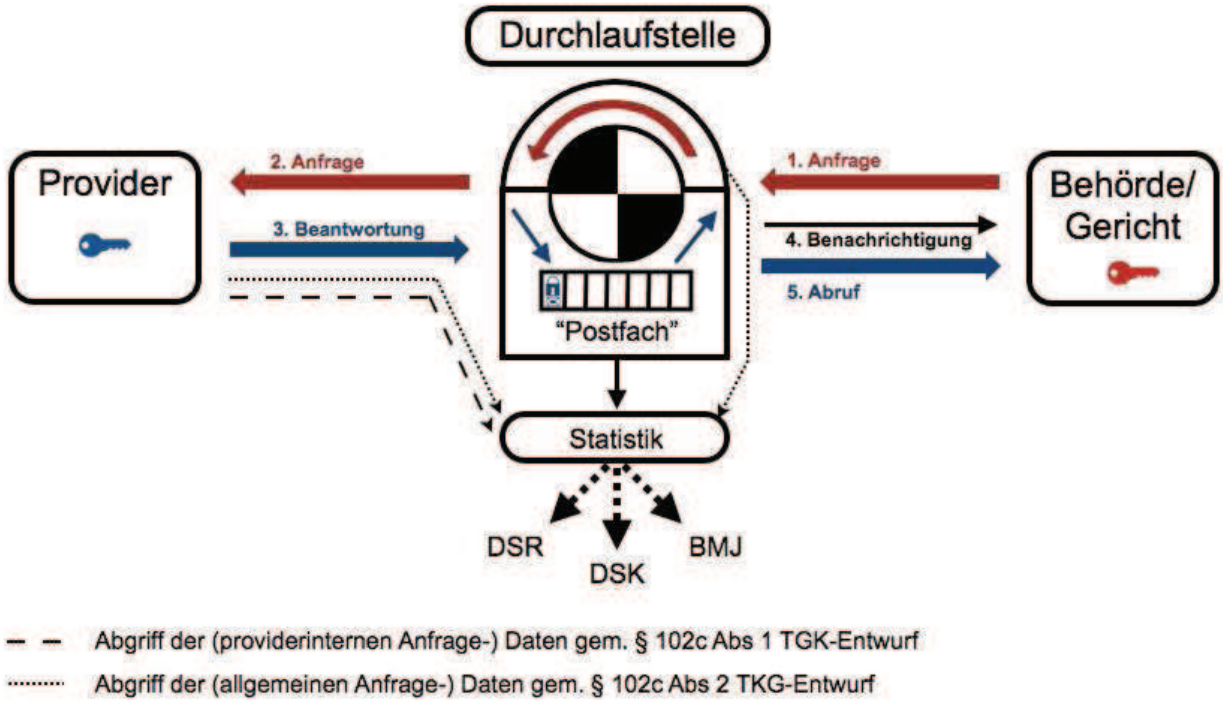

Abbildung 4: Abgriff von Protokolldaten im Zuge der Auskunftsabwicklung über die DLS

IV.2.8.2.4 Wird dabei ein Informationsverbundsystem geschaffen?

Ein „Informationsverbundsystem“ ist gemäß der Legaldefinition des § 4 Z 13 DSG „die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, daß jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden“. Gemäß § 18 DSG unterliegt ein Informationsverbundsystem der verpflichtenden Vorabkontrolle durch die Datenschutzkommission, vor die Datenanwendung rechtmäßig betrieben werden darf. Diese

[439] Ibid, S. 87.

Vorabkontrollpflicht entfällt dann, wenn die Datenanwendung einer Musteranwendung nach § 19 Abs. 2 entspricht. In § 50 DSG sind sodann spezielle Auflagen für den Betrieb eines Informationsverbundsystems vorgeschrieben. Beispiele für solche Informationsverbundsysteme finden sich sowohl im privatwirtschaftlichen (Buchungs- und Reservierungssysteme) als auch im öffentlichen Bereich (Zentrales Melderegister).[440]

Ob die DLS als Informationsverbundsystem zu sehen ist, hängt primär von der konkreten Ausgestaltung des Systems ab, die natürlich durch eine DSVO entsprechend zu determinieren ist. Konkret soll die Eigenschaft als Informationsverbundsystems primär dadurch vermieden werden, dass jeder Benutzer der DLS – sowohl auf Seiten der Behörden als auch auf Seiten der Anbieter – jeweils nur Zugang auf das Postfach seiner Organisationseinheit haben darf. Ein entsprechender Vorschlag zur Ausgestaltung wurde bereits oben zu § 12 Abs. 2 DSVO-Entwurf dargestellt.[441] Außerdem ist unter anderem auch aus diesem Grund wichtig, dass die DLS selbst keinen Zugang zu den Inhalten der Datenauskünfte haben darf, also „blind" gegenüber den Inhalten ist.[442]

Bleibt zu prüfen, ob die Protokolldaten der DLS die Eigenschaft eines Informationsverbundsystems begründen, weil diese im Zuge der Aufbereitung der Statistik jedenfalls zusammengeführt werden. Diese Protokolldaten sind jedoch nur statistischer Natur ohne Personenbezug, sodass kein schutzwürdiges Geheimhaltungsinteresse iSd § 1 DSG besteht. Auch über die Unique-ID ist aus Sicht der DLS keine Rückführung auf den Personenbezug möglich, lediglich die gesetzlich Zuständigen Rechtsschutzorgane (Datenschutzkommission, Rechtsschutzbeauftragte) können durch weitere Ermittlungen bei den Anbietern oder den Behörden personenbezogene Protokolldaten einsehen, wobei die Unique-ID auch hier nur ein Hilfsmittel zur leichteren Nachvollziehbarkeit des gesamten Auskunftsablaufs darstellt und dabei aus Sicht der DLS die Protokolldaten höchstens zu „indirekt personenbezogenen Daten" iSd § 4 Z 1 DSG macht. Dabei gelten bei nur indirekt personenbezogenen Daten schutzwürdige Geheimhaltungsinteressen gemäß § 8 Abs. 2 DSG sowie gemäß § 9 Z 2 DSG als nicht verletzt. Darüber hinaus ist nach der Konzeption der DLS unklar, ob die Protokolldaten überhaupt als „indirekt personenbezogene Daten" zu sehen sind oder gar nur statistische Daten iSd § 46 DSG darstellen.

Im Ergebnis ist daher auszuschließen, dass die in dieser Arbeit[443] vorgeschlagene Konzeption der DLS die Eigenschaft eines Informationsverbundsystems begründet.

IV.2.8.2.5 Wer soll Zugriff auf die DLS Protokollierung haben?

§ 102c Abs. 4 TKG regelt zwar den Zugang zu Protokolldaten im Zusammenhang mit der Vorratsdatenspeicherung, allerdings betrifft diese Regelung die Protokollierung beim Anbieter intern, die von der Protokollierung der Auskunftsfälle über die DLS zu unterscheiden ist.[444] Dennoch bietet die Regelung einen Anhaltspunkt dafür, welche Behörden Zugang zu den Protokolldaten der DLS und zur Statistik haben sollten. Demnach wären die Datenschutzkommission, der Datenschutzrat und das

---

[440] Aus der Beschreibung des Begriffes Informationsverundsystem auf der Website der ARGE Daten, http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=86661381.
[441] Siehe oben Kapitel IV.2.2.1.1.
[442] Dazu näher oben in Kapitel IV.2.4.4.
[443] Sowie auch in der BIM-Datensicherheitsstudie.
[444] Siehe dazu schon oben zu den Grundfunktionen der DLS in Kapitel IV.2.2.1.

BMJ zu berücksichtigen. Festzuhalten ist hier nochmals, dass diese Protokollierung zunächst keinen Personenbezug enthält sondern rein statistische Werte. Ein Bezug zu einem bestimmten Kommunikationsteilnehmer lässt sich erst herstellen, wenn die Protokolldaten aus der internen Protokollierung der Anbieter oder Behörden eingesehen werden. Dies ist über die DLS nicht möglich, durch die Unique-ID wird es im Rechtsschutzfall aber vereinfacht, die entsprechende vollständige Protokollierung auf der jeweiligen Seite aufzufinden. Allerdings darf diese personenbezogene Protokollierung - und auch bereits die Hilfsinformation über die Unique-ID nur zugänglich sein, wenn einer Behörde auch eine entsprechende gesetzliche Befugnis dafür zusteht.

Hinsichtlich der Datenschutzkommission (DSK) ist das ohne Zweifel zu bejahen, weil die Datenschutzkommission darüber hinaus auch klare gesetzliche Befugnisse bzw. Pflichten hat, die einen Zugang zu den Protokolldaten der DLS rechtfertigen. Zuständig ist die DSK im Fall eines datenschutzrechtlichen Auskunftsverfahrens gemäß § 26 DSG oder im Fall einer präventiven Systemprüfung gemäß § 14 DSG und § 102c Abs. 1 TKG. Eine Zuständigkeit im Rahmen eines Beschwerdeverfahrens gemäß § 31 DSG kann ebenfalls bestehen, sicher allerdings nur dann, wenn sich die Beschwerde eines Betroffenen gegen eine staatliche Behörde richtet. Richtet sich eine Beschwerde eines betroffenen Teilnehmers eines öffentlichen Kommunikationsdienstes nämlich gegen einen Anbieter, sind gemäß § 1 Abs. 5 DSG iVm § 32 DSG die ordentlichen Gerichte zuständig, weil in Österreich sämtliche Anbieter in Formen des Privatrechts eingerichtet sind.[445]

Theoretisch rechtfertigt dies daher auch einen Zugang für ein Zivilgerichte, die im Streitfall zwischen Kunden und Anbieter im Verfahren gemäß § 32 DSG den Verlauf einer Datenauskunft nachverfolgen können sollten. Einen unmittelbaren Zugang der Zivilgerichte zu den Protokolldaten der DLS vorzusehen erscheint aber unverhältnismäßig im Hinblick auf den Aufwand einer solchen Anbindung. Der Grund dafür ist, dass solche Verfahren schon an sich sehr selten sind, ein Zugang aber theoretisch für alle Zivilgerichte in Österreich einzurichten wäre. In der Praxis lässt sich das Problem wohl mit einem Rechtshilfeersuchen des zuständigen Gerichts an die Datenschutzkommission problemlos lösen, sodass ein direkter Zugang der Zivilgerichte entbehrlich erscheint. Ausserdem ist ein Gericht in einem solchen Verfahren nicht unbedingt auf die Protokollierung der DLS angewiesen, weil der Betroffene ja einen Beklagten benennen muss und das Gericht damit den betroffenen Anbieter schon kennt, sodass das Gericht zuerst die interne Protokollierung beim Anbieter prüfen wird.

Ähnlich gestaltet sich das Problem auch im Hinblick auf Strafgerichte. Auch diese können theoretisch in ihrer Zuständigkeit Verfahren zu führen haben, für welche die DLS-Protokollierung einen Beweiswert haben könnte, zB in einem Verfahren wegen “Mißbrauch der Amtsgewalt” gemäß § 302 StGB oder wegen “Verletzung des Telekommunikationsgeheimnisses“ gemäß § 119 StGB. Auch hier sollte das Problem mit einem Rechtshilfeersuchen an die Datenschutzkommission in der Praxis ohne große Schwierigkeiten zu bewältigen sein.

Aus der Perspektive des Datenschutzgrundrechts äußerst problematisch erscheint die Regelung des § 102c Abs. 4 Z 1 TKG, wonach dem Datenschutzrat sämtliche in Abs. 2 leg cit genannten Protokolldaten zugänglich sein sollen. Diese Regelung war im ursprünglichen Begutachtungsentwurf zur TKG-Novelle[446] noch nicht enthalten, dort war der Zugang zu den Protokolldaten ausschließlich

[445] Siehe dazu oben die theoretischen Grundlagen in Kapitel II.1.1.3.3.
[446] BIM-Entwurf TKG Novelle 2010, Fundstelle und ausführliche Zitierung siehe Literaturverzeichnis.

für die Datenschutzkommission vorgesehen. Dass der Datenschutzrat vollen Zugang zu sämtlichen personenbezogenen Protokolldaten haben soll ist schlechterdings unverständlich, weil dieser gemäß § 41 DSG als ein beratendes Organ der Bundesregierung und (auf Ersuchen) der Landesregierungen eingerichtet ist, der sich mit rechtspolitischen Fragen des Datenschutzes auseinandersetzt. Insbesondere hat der Datenschutzrat keine gesetzlichen Aufgaben im Zusammenhang mit konkreten Beschwerden wegen Datenschutzverletzungen. Dass der Datenschutzrat daher Zugang zu personenbezogenen Daten von Kommunikationsteilnehmern haben soll, scheint für sich ein unzulässiger Eingriff in das Datenschutzgrundrecht der Betroffenen zu sein. Zur Wahrnehmung seiner Aufgaben als rechtspolitisches Beratungsorgan in Datenschutzfragen scheint es aber - abseits der eben formulierten Kritik - ausreichend und auch sinnvoll, wenn der Datenschutzrat Zugang zu den Statistischen Daten der DLS hat. Zugang zur Information über die Unique-ID zur Weiterverfolgung einer bestimmten Datenauskunft soll der Datenschutzrat dabei aber nicht erhalten, weil solche Ermittlungshandlungen von seinen gesetzlich Definierten Aufgaben nicht erfasst sein werden.

Unzweifelhaft ist demgegenüber, dass das BMJ Zugang zur Statistik der DLS haben muss, denn diesem Bundesministerium obliegt die Pflicht zur Berichterstattung gegenüber der EU-Kommission gemäß Art. 10 RL 2006/24/EG. Dies ist auch in § 102c Abs. 4 Z 2 TKG ausdrücklich normiert, wobei das BMJ nach dieser Bestimmung darüber hinaus auch die Pflicht zur Berichterstattung über die Statistik an den Nationalrat trifft. Hier sieht jedoch schon § 102c Abs. 4 Z 2 TKG ausdrücklich vor, dass die dem BMJ zugänglichen Protokolldaten auf die in § 102c Abs. 2 Z 2 bis 4 TKG genannten Daten beschränkt sind - also auf solche, die keinen Personenbezug enthalten.

Nicht in § 102c Abs. 4 TKG genannt sind die Rechtsschutzbeauftragten des Innenministeriums und des Justizministeriums. Diese haben aber gemäß § 91c SPG bzw. § 147 StPO Kontrolltätigkeiten zu erfüllen, die einen Zugang zu den Protokolldaten der DLS rechtfertigen. Der Mehrwert einer statistischen Erfassung aller Auskunftsvorgänge lässt sich am Beispiel des Rechtsschutzbeauftragten (RSB) des BM.I gut veranschaulichen. Dieser ist gemäß § 91c SPG durch die Sicherheitsbehörden über Auskunftsverlangen gemäß § 53 Abs. 3a Z 2 und 3, Abs. 3a zweiter Satz und 3b SPG zu informieren. Ob diese Information durch die Sicherheitsbehörden allerdings tatsächlich erfolgt, ist für den RSB in der Realität schwer nachvollziehbar, weil er keine objektivierte Vergleichsgrundlage hat sondern vielmehr von der Meldedisziplin der Behörden abhängig ist.

Wenn der RSB nun künftig anhand der objektiven statistischen Werte aus der DLS vergleichen kann, wie viele Datenauskünfte aufgrund einer bestimmten Rechtsgrundlage stattgefunden haben und wie viele ihm andererseits durch die Sicherheitsbehörden gemeldet wurden, kann er Maßnahmen ergreifen, falls diese Zahlen nicht übereinstimmen. Durch stichprobenartige Kontrollen kann er mit Hilfe der Unique-ID zu bestimmten Auskünften - etwa wenn zB besonders viele Auskünfte zu IP-Adressen gemäß § 53 Abs. 3a SPG nicht gemeldet wurden - weiter ermitteln, ob eine Meldung erfolgte bzw. ob das Auskunftsbegehren rechtmäßig war. Die statistische, nicht personenebezogene Protokollierung dient auf diese Weise der Missbrauchsprävention.[447] Wie die Datenschutzkommission sollen aber auch die Rechtsschutzbeauftragten erst dann die Providerzuordnung sehen können, wenn sie in einem konkreten Fall nähere Prüfschritte unternehmen.

[447] Für Details zur Protokollierung und zur Statistik über die DLS siehe unten Kapitel IV.2.8.

IV.2.8.3 LÖSUNGSVORSCHLÄGE FÜR EINE DSVO

Die soeben ausgeführten Überlegungen zur Protokollierung über die DLS könnten legistisch folgendermaßen erfasst werden:[448]

§ 22 Protokollierung über die Durchlaufstelle

(1) Die Protokollierung der Durchlaufstelle enthält keine personenbezogenen Daten. Durch die Unique-ID jeder Anfrage wird der Zusammenhang zwischen jeder Anfrage und deren Beantwortung ohne Personenbezug hergestellt.
(2) Bei der Übermittlung der Antwort zu einem Auskunftsbegehren hat der Anbieter die Protokollinformationen gemäß § 7 Abs. 3 Z 4 und 5 für die in Absatz 4 genannten Zwecke an die Durchlaufstelle zu übermitteln.
(3) Die Protokolldaten werden in einer Protokolldatei unverschlüsselt über die sichere Transportverbindung zur Durchlaufstelle übermittelt. Das Format der Datei und der Dateiname sind in der Spezifikation zur Durchlaufstelle festzulegen.
(4) Die Protokolldaten sind ausschließlich für die definierten Protokolldatenempfänger zugänglich und werden innerhalb der Durchlaufstelle in einer gesonderten Datenbank archiviert. Für die Datenschutzkommission sowie für die Rechtsschutzbeauftragten beim Bundesminister für Justiz und beim Bundesminister für Inneres sind in der Spezifikation zur Durchlaufstelle gesonderte Berechtigungen für den Zugang zu den Protokolldaten vorzusehen.

IV.2.9 STATISTIK ZUR DATENVERWENDUNG GEMÄß ART 10 RL 2006/24/EG

Es besteht eine Verpflichtung zur jährlichen Berichterstattung gegenüber der Europäischen Kommission gemäß Art 10 RL 2006/24/EG, die vom BMJ wahrzunehmen ist:

„Art 10 Statistik

(1) Die Mitgliedstaaten sorgen dafür, dass der Kommission jährlich eine Statistik über die Vorratsspeicherung von in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder eines öffentlichen Kommunikationsnetzes erzeugten oder verarbeiteten Daten übermittelt wird. Aus dieser Statistik muss hervorgehen:

— in welchen Fällen im Einklang mit dem innerstaatlichen Recht Daten an die zuständigen Behörden weitergegeben worden sind;

— wie viel Zeit zwischen dem Zeitpunkt der Vorratsspeicherung der Daten und dem Zeitpunkt, zu dem sie von der zuständigen Behörde angefordert wurden, vergangen ist und

— in welchen Fällen die Anfragen nach Daten ergebnislos geblieben sind.

(2) Die Statistik darf keine personenbezogenen Daten enthalten.“

---

[448] Die Formulierungen stammen aus der BIM-Datensicherheitsstudie S. 144; diese Vorschläge wurden unverändert durch das BMVIT in öffentliche Begutachtung geschickt; vgl. dazu den Begutachtungsentwurf im Anhang.

Zur Erstellung einer solchen Statistik sind die entsprechenden Rohdaten über alle Auskunftsfälle notwendig, wobei diese von vornherein keine personenbezogenen Daten enthalten müssen. Die Erfassung der Protokolldaten im Rahmen der Durchlaufstelle soll diese Erfassung der statistischen Rohdaten für die Anbieter sowie das BMJ deutlich vereinfachen. Denn ansonsten müssten die Protokolldaten von allen Anbietern eingesammelt und in einheitlicher Struktur zusammengeführt werden. Gemäß § 102c Abs. 4 Z 2 TKG obliegt es weiters auch dem BMJ, dem Nationalrat über die Statistik zu berichten. Darüber hinaus sollte die Statistik auch den gesetzlich zuständigen Rechtsschutzorgangen (Datenschutzkommission, Rechtsschutzbeauftragte) zugänglich sein. Darüber hinaus kommt auch dem Datenschutzrat das Recht zu, „von Auftraggebern des öffentlichen Bereichs Auskünfte und Berichte sowie die Einsicht in Unterlagen zu verlangen, soweit dies zur datenschutzrechtlichen Beurteilung von Vorhaben mit wesentlichen Auswirkungen auf den Datenschutz in Österreich notwendig ist“[449]. Zur Vereinfachung des Vervahrensaufwands und im Hinblick auf dessen rechtspolitische Beratungsfunktion in Datenschutzangelegenheiten sollte daher auch dem Datenschutzrat ein direkter online-Zugang zur Statistik über die DLS gewährt werden.

Grundsätzlich sollten alle Rohdaten für die Statistik soweit möglich bereits bei der DLS abgegriffen werden, um die Vorteile einer Arbeitsreduktion in dieser Hinsicht auch effektiv zu nutzen. Diesem Zweck dient (auch) die Erfassung der Protokolldaten der DLS wie oben in Kapitel IV.2.8.2.3 dargestellt. Allerdings ist das nur im Hinblick auf jene Informationen möglich, die für die DLS ohne Verschlüsselung zugänglich sein dürfen, weil sie keinen Personenbezug enthalten und nicht Teil der zu übertragenden Inhalte sind. Konkret betrifft dies die Informationen über das Datum der Anfrage und der erteilten Auskunft, die gemäß § 7 Abs. 3 Z 3 DSVO-Entwurf erfasst werden sollen.[450] Die Informationen über die nach den Kategorien des § 102a Abs. 2 bis 4 TKG aufgeschlüsselten Datensätze[451] sowie über das Alter der Daten[452] sind demgegenüber zunächst nur erfassbar, wenn Zugang zu den Inhalten einer tatsächlich übermittelten Auskunft besteht. Aus diesem Grund müssen diese Daten bei der Beantwortung eines Auskunftsbegehrens vom Anbieter aus dem (verschlüsselten) Inhalt extrahiert und ohne Personenbezug an die DLS übergeben werden, sodass die DLS diese Daten für die Statistik weiterverarbeiten kann. Diese Informationen müssen als Zusatzinformationen[453] zur verschlüsselten CSV-Datei mit der Antwort vom Anbieter übermittelt werden.

IV.2.9.1 LÖSUNGSVORSCHLAG FÜR EINE DSVO

Die soeben ausgeführten Überlegungen zur Generierung der Statistik über die DLS könnten legistisch folgendermaßen erfasst werden:[454]

---

[449] § 41 Abs. 2 Z 4 DSG.
[450] Siehe den Lösungsvorschlag zu den Protokolldaten der DLS oben in Kapitel IV.2.8.3.
[451] Die Erfassung dieser Informationen dient nicht primär der unionsrechtlichen Statistik-Pflicht sondern stellt eine innerstaatliche Erweiterung dar, die im weiteren Sinn dem Rechtsschutz dienen soll; vgl. § 7 Abs. 3 Z 4 DSVO-Entwurf.
[452] Siehe § 7 Abs. 3 Z 5 DSVO-Entwurf.
[453] Dazu sogleich in Kapitel IV.2.10.2.
[454] Die Formulierungen stammen aus der BIM-Datensicherheitsstudie S. 145 f; diese Vorschläge wurden mit einer Ergänzung - als Konsequenz der Ergänzungen in § 7 Abs. 3 DSVO-Entwurf - durch das BMVIT in öffentliche Begutachtung geschickt, dazu sogleich; vgl. dazu den Begutachtungsentwurf im Anhang.

§ 23 Statistik aus den Protokolldaten

(1) Die Statistik zur Erfüllung der Verpflichtung aus Art 10 der Richtlinie 2006/24/EG soll in der Durchlaufstelle automatisch aufbereitet werden. Die genaue Definition der zu erstellenden Statistik ist in der Spezifikation zur Durchlaufstelle vorzunehmen.
(2) Für die Erstellung der Statistik sind die Protokoll-Informationen gemäß § 7 Abs. 3 Z 3 bis 5 erforderlich. Die Informationen gemäß § 7 Abs. 3 Z 3 sind von der Durchlaufstelle automatisch zu jedem Auskunftsfall zu erfassen. Die Informationen gemäß § 7 Abs. 3 Z 4 und 5 hat der Anbieter gemäß § 22 Abs. 2 gemeinsam mit der Beantwortung des Auskunftsbegehrens an die Durchlaufstelle zu übermitteln.
(3) Zugang zur Statistik der Durchlaufstelle erhalten gemäß § 102c Abs. 4 TKG 2003 das Bundesministerium für Justiz, der Datenschutzrat, und die Datenschutzkommission. Darüber hinaus ist in der Spezifikation zur Durchlaufstelle ein elektronischer Zugang für die Rechtsschutzbeauftragten beim Bundesminister für Justiz und beim Bundesminister für Inneres vorzusehen.

Die einzige Änderung, die zu diesem Vorschlag für den Begutachtungsentwurf erfolgte, betrifft § 23 Abs. 2 DSVO-Entwurf und ist die Konsequenz aus dem Änderungsvorschlag des BMJ, dem § 7 Abs. 3 DSVO-Entwurf eine Z 8 anzufügen, nach welcher die Informationen über die zugrunde liegende strafbare Handlung zu Erheben ist. Weil es hier um Daten geht, die aufgrund der Statistik-Pflicht des Art 10 RL 2006/24/EG zu erfassen sind, erschließt sich der Sinn dieser Ergänzung erst durch die Erweiterung, diese Daten auch in die Statistik aufzunehmen. Insofern ist der Änderungsvorschlag zu Abs. 2 nur konsequent und nicht zu beanstanden. Zur Frage, ob diese Informationen nun durch den Anbieter oder die Behörden ergänzt werden sollen siehe oben Kapitel IV.2.8.1.1.

Statistik aus den Protokolldaten

§ 23. (1) (…)
(2) Für die Erstellung der Statistik sind die Protokoll-Informationen gemäß § 7 Abs. 3 Z 3 bis 5 *und Z 8* erforderlich. Die Informationen gemäß § 7 Abs. 3 Z 3 sind von der Durchlaufstelle automatisch zu jedem Auskunftsfall zu erfassen. Die Informationen gemäß § 7 Abs. 3 Z 4 und 5 hat der Anbieter gemäß § 23 Abs. 2 gemeinsam mit der Beantwortung des Auskunftsbegehrens an die Durchlaufstelle zu übermitteln.
(3) (…)

IV.2.10 Anwendungs-Fälle (Use-Cases) aus Sicht der DLS

Aus technischer Sicht stellen die bisher behandelten Funktionen der DLS Anwendungsfälle (Use-Cases) dar, die für die technische Realisierung der DLS zu berücksichtigen sind. Mit den Kernfunktionen sind darüber hinaus Hilfsfunktionen zu berücksichtigen, die eine Abwicklung von Datenauskünften entsprechend den verfahrensrechtlichen Vorgaben und den Sicherheitsanforderungen ermöglichen. Diese Hilfsfunktionen sollen im Folgenden verdeutlicht werden.

IV.2.10.1 Rückfragen seitens der anfrageberechtigten Stelle ?

In der Praxis wird sich auch durch eine stärker formalisierte Auskunftsabwicklung über die DLS nicht vermeiden lassen, dass ein Anbieter im Einzelfall Rückfragen zum Auskunftsbegehren an die

anfragende Behörde hat. Um die DLS als einheitlichen Kommunikationskanal für Datenauskünfte zu etablieren und parallele Kommunikationswege im Sinne der Datensicherheit zu vermeiden, sollte die DLS daher einen zusätzlichen Kommunikationskanal bieten.

Auch umgekehrt kann nach einer Anfragebeantwortung der Fall auftreten, dass eine Behörde Rückfragen zur Auskunft an den Anbieter hat, die allenfalls sogar zu einer neuerlichen Datenübermittlung führen können. Die Behandlung von Rückfragen kann durch einen "Spielraum" bei der Implementierung erleichtert werden. Die DLS sollte zulassen, dass im Falle notwendiger Ergänzungen eine neuerliche Übermittlung problemlos möglich ist, die dann entweder als eigener Auskunftsfall dokumentiert werden könnte (wenn zB nach einer Rückfrage neue Datensätze hinzukommen) oder dem zugrunde liegenden Auskunftsfall zugeordnet werden können.[455]

IV.2.10.2 Übertragung von Zusatzinformationen

Die eben beschriebene Notwendigkeit, einen zusätzlichen Kommunikationskanal über die DLS zu bieten, heißt mit anderen Worten, es müssen zusätzlich zur eigentlichen Datenauskunft auch Informationen übermittelt werden können, zB wenn der Anbieter die Gründe ausführt, warum zu einer Anfrage keine Datensätze vorhanden sind (Leer-Meldung). Sofern es sich um personenbezogene Informationen handelt, muss die DLS auch hier „blind“ sein. Informationen, die keinen Aufschluss über bestimmte Personen geben, können aber Durchaus in einer Weise übertragen werden, die für die DLS zugänglich ist. Im Falle der vom Anbieter an die DLS zu übermittelnden Statistik-Informationen ist diese Zugänglichkeit sogar funktionelle Voraussetzung.

Die CSV-Dateien werden mittels sicherem Datentransfer und inhaltsverschlüsselt an die Durchlaufstelle übermittelt. Zusatzinformationen könnten allenfalls über ein Web-Interface zu der entsprechenden Abfrage eingegeben werden. Diese Zusatzinformationen könnten etwa Gründe für eine Leer-Meldung beschreiben. Ob und in welchem Ausmaß ein Web-Interface auf Seiten der DLS zur Verfügung gestellt werden soll, wird Gegenstand der Diskussion zur Spezifikation der DLS sein. Jedenfalls ist dabei zu bedenken, dass die DLS gegenüber Inhalten der Auskünfte "blind" sein soll, personenbezogene Informationen sollten also nicht als Zusatzinformation übermittelt werden, weil diese gegenüber der DLS nicht inhaltsverschlüsselt werden, sondern nur durch die Transportverschlüsselung vor Zugriffen von außen sicher sind. Alternativ ist auch möglich nach dem sonstigen Aufbau der EP 020 die möglichen Dateiformate und Dateinamen für Zusatzinformationen zu definieren. Auf diese Weise könnten auch personenbezogene Zusatzinformationen mit Inhaltsverschlüsselung übertragen werden, die aus Sicht der DLS nicht zugänglich sind. Für Anfragen, die nicht zwischen Vorratsdaten und betriebsnotwendigen Daten unterscheiden (z.B. nach § 53 Abs. 3a und 3b SPG) muss jedenfalls die Information übermittelt werden, ob Vorratsdaten für die Beantwortung dieser Anfrage verwendet wurden. Diese Information wird von den Anbietern als "Zusatzinformation" übermittelt (siehe § 6 Abs. 2).

[455] Vgl. BIM-Datensicherheitsstudie S. 111.

Allenfalls könnte für die Übertragung von Zusatzinformationen eine Textdatei (.doc/.txt) zum Einsatz kommen, welches leicht wie eine "reale Antwort" mit dem Schlüssel der Behörde verschlüsselt wird. In diesem Fall hier wäre die Benennung dieser Datei in der Spezifikation zur DLS zu regeln[456].

IV.2.10.2.1 LÖSUNGSVORSCHLAG FÜR EINE DSVO

Die soeben ausgeführten Überlegungen zur Protokollierung über die DLS könnten legistisch folgendermaßen erfasst werden:[457]

§ 20 Zusatzinformationen

> Die Durchlaufstelle hat die Übertragung von Zusatzinformationen zu unterstützen. Zusatzinformationen können allenfalls über ein Web-Interface zu der entsprechenden Abfrage eingegeben werden. Diese Zusatzinformationen könnten auch Gründe für eine Leer-Meldung beschreiben. Ob und in welchem Ausmaß ein Web-Interface auf Seiten der Durchlaufstelle zur Verfügung gestellt werden soll, ist in der Spezifikation zur Durchlaufstelle zu regeln. Voraussetzung ist in jedem Fall, dass die Durchlaufstelle keinen Zugang zu personenbezogenen Inhalten der Auskünfte hat.

IV.2.10.3 IST EINE ANFRAGE AN MEHRERE ANBIETER ZUGLEICH MÖGLICH?

In der Praxis ist häufig notwendig, dass ein Auskunftsbegehren nicht nur an einen sondern an mehrere oder sogar sämtliche Anbieter gestellt wird, was häufig etwa bei Funkzellenauswertungen zur Ermittlung von Standortdaten oder bei der IMEI-Rasterung vorkommt.[458] Hierfür sollten jedoch die (derzeit ca 200) gem. § 102a TKG speicherpflichtigen Anbieter entsprechend der angebotenen Dienste klassifiziert werden, zB in „Internet-Zugangsanbieter", „Mobilfunkanbieter", etc, um nur die relevanten Anbieter im Rahmen einer Anfrage zu adressieren. So könnten unnötige Ressourcenbelastung vermieden werden, wie zum Beispiel eine Anfrage für eine Funkzellenauswertung an alle 200 Anbieter zu übermitteln, obwohl es nur 5 Mobilfunkanbieter gibt, die eine solche Anfrage tatsächlich beantworten können.

Es wurde auch das konkrete Problem erwähnt, den Netzanbieter zu einer portierten Nummer feststellen zu können. Angeblich existiert dazu bei zumindest einem der 5 Mobilfunkanbieter – als reine Serviceleistung ohne rechtliche Verpflichtung – eine Liste, welche die Zuteilung von portierten Mobil-Rufnummern zu den jeweiligen Anbietern enthält. Falls eine Datenbank mit der Zuordnung von Rufnummern zu Netzanbietern für eine automatisierte Abfrage tatsächlich zur Verfügung steht, würde dies die operative Arbeit bei den abfrageberechtigten Stellen erleichtern.[459]

---

[456] Ibid, S. 168.
[457] Die Formulierungen stammen aus der BIM-Datensicherheitsstudie S. 145; dieser Vorschlag wurde unverändert durch das BMVIT in öffentliche Begutachtung geschickt; vgl. dazu den Begutachtungsentwurf im Anhang.
[458] Zur Funktion solcher Auskünfte siehe oben Kapitel II.1.4.2.2.
[459] Ibid, S. 114.

IV.2.10.3.1 SONDERPROBLEM PORTIERTE RUFNUMMERN

Im 6. Round Table wurde in diesem Zusammenhang das praktische Problem der portierten Rufnummern diskutiert.[460] Dieses besteht darin, dass die anfragende Behörde zunächst überhaupt wissen will, an welchen Anbieter sie das Auskunftsbegehren richten soll, was bei portierten Rufnummern anhand der Nummer nicht identifizierbar ist. In der Diskussion wurde festgehalten, dass diesbezüglich keine gesetzlichen Verpflichtungen der Anbieter zum Führen einer Liste besteht, obwohl solche Listen in der Praxis in Verwendung sind.

Derzeit hat jeder Anbieter seine eigene Lösung, mit der Nummernportierung umzugehen (zB beim technischen Routing von Anrufen) und es gibt keine zentrale Stelle, die alle Informationen hält. Die Anbieter haben aktuelle Informationen über die aktiven Rufnummern in ihrem Netz, können aber in der Regel keine historischen Daten abfragen. Insbesondere existieren keine Datenbanken, die eine Feststellung erlauben, bei welchem Anbieter eine bestimmte Rufnummer geschaltet ist oder in der Vergangenheit war. Für Rufnummernportierungen sind diese Daten bei Mobilfunk in den Vermittlungsstellen für Routingzwecke enthalten. Diese Systeme sind nicht für online Abfragen eingerichtet und enthalten auch keine historischen Daten. Die Anbieterlisten enthalten also keine Gewähr, dass sie tatsächlich aktuell und vollständig sind. Da bei Fest- und Mobilnummern nur eine begrenzte Anzahl von Anbietern in Frage kommt, scheint es sinnvoll, die Anfrage an alle in Frage kommenden Anbieter zu schicken.

IV.2.10.3.2 LÖSUNGSVORSCHLAG FÜR EINE DSVO

Die soeben ausgeführten Überlegungen könnten legistisch folgendermaßen erfasst werden:[461]

§ 17 Postfächer und Zustellung

(1) Ein Auskunftsbegehren eines berechtigten Benutzers auf Behördenseite wird in das Postfach des über die Durchlaufstelle ausgewählten Anbieters zugestellt. Die Durchlaufstelle ermöglicht die Auswahl mehrerer Anbieter(…).

(…)

IV.2.11VERANTWORTUNGSZUSAMMENHANG IM KONZEPT DER DLS?

Zur Erlassung einer Datensicherheitsverordnung ist gemäß §§ 94 (4) und 102c (1) TKG die Bundesministerin für Verkehr, Innovation und Technologie (BMVIT) im Einvernehmen mit der Bundesministerin für Inneres und der Bundesministerin für Justiz ermächtigt. Davon getrennt ist aber die Frage zu klären, welche Behörde für den Betrieb der DLS verantwortlich ist.

---

[460] Siehe die Zusammenfassung der Diskussion zum 6. Round Table, BIM-Datensicherheitsstudie S. 129.

[461] Die Formulierung stammt aus der BIM-Datensicherheitsstudie S. 143 f; dieser Vorschlag wurde unverändert durch das BMVIT in öffentliche Begutachtung geschickt; vgl. dazu den Begutachtungsentwurf im Anhang; zum vollständigen Vorschlag des § 17 DSVO-Entwurf siehe oben Kapitel IV.2.2.1.1.

Die sauberste Lösung für die datenschutzrechtlichen Problemstellungen, die mit der zentralen Abwicklung aller Datenauskünfte nach § 94 Abs. 4 TKG 2003 verbunden sind, wäre, wenn das BMVIT die Verantwortung für den Betrieb der Durchlaufstelle übernimmt. Der Betrieb der DLS und die Beauftragung zur technischen Spezifikation und Umsetzung sollte in der Verantwortung des BMVIT liegen. Damit wären die Bedarfsträger vom Auftraggeber getrennt, weil dem BMVIT keine Aufgaben obliegen, für die eine Verarbeitung von Vorratsdaten notwendig wäre, dieses ist hier vielmehr eine neutrale Stelle ohne eigenes Interesse an den zu übermittelnden Inhalten. Das Interesse des BMVIT am Betrieb der DLS ist darin zu sehen, dass diesem Bundesministerium obliegt, über die Einhaltung der Bestimmungen des TKG 2003 zu wachen, wozu insbesondere auch das Kommunikationsgeheimnis des § 93 TKG 2003 zählt.[462] Hiervon getrennt zu beurteilen ist aber die Frage, wem die Eigenschaft eines datenschutzrechtlichen Auftraggebers zukommt (dazu sogleich in Unterkapitel IV.2.11.2.

IV.2.11.1 Muss der Auftrag zur Errichtung und zum Betrieb der DLS ausgeschrieben werden? Oder: Warum das BRZ?

Mit der Einrichtung und dem Betrieb der DLS sollte das BMVIT die Bundesrechenzentrum GmbH (BRZ) beauftragen. Das BRZ kann im Wege einer sogenannten In-House-Vergabe gemäß §10 Z 7 Bundesvergabegesetz 2006 (BVerG) durch den Bund (hier konkret vertreten durch das BMVIT) sowohl mit der Entwicklung als auch dem Betrieb der DLS beauftragt werden. Wenn die Anwendung gesetzlich oder per Verordnung vorgesehen ist und der Auftrag aus einem Bundesministerium kommt, würde damit das „Ausschreibungsprivileg" des BRZ greifen, der Auftrag müsste also unabhängig vom Volumen nicht öffentlich ausgeschrieben werden.[463] Dies begründet das erste Argument, warum gerade das BRZ hier vorgeschlagen wird. Faktisch besteht nämlich das Problem, dass sämtliche Bestimmungen zur Vorratsdatenspeicherung am 1.4.2012 in Kraft treten und bis dahin ein sicheres Datenübertragungssystem iSd § 94 Abs. 4 TKG in vollem operativen Betrieb stehen muss. Müsste ein Auftrag für die Einrichtung eines solchen Systems erst unter Einhaltung aller Regeln des BVerG ausgeschrieben werden, ließe sich dieser Zeitplan sicher nicht einhalten. Dazu kommt der von der EU-Kommission ausgehende Druck eines drohenden Strafzahlungsverfahrens wegen Nichtumsetzung der RL 2006/24/EG.[464]

Aber auch auf der Sachebene bestehen gute Gründe, die DLS durch das BRZ betreiben zu lassen. Insbesondere besteht dort bereits eine umfassende Infrastruktur, um die Eingliederung der DLS in den Portalverbund zu bewerkstelligen. Auch die diesbezüglichen Erfahrungen, eine große Zahl von privaten Teilnehmern an eine Anwendung im Rahmen des Portalverbunds einzubinden, stellen ein gutes Argument für die Heranziehung des BRZ dar. Ganz abgesehen davon verfügt das BRZ über eine ausreichende Infrastruktur, um den Sicherheitsanforderungen an die DLS gerecht zu werden, wenngleich dies wohl nicht als Alleinstellungsmerkmal des BRZ zu sehen ist.

---

[462] Vgl. BIM-Datensicherheitsstudie S. 110 und 162.
[463] Ibid, S. 95.
[464] Dazu oben in Kapitel IV.2.2.2.

IV.2.11.2 WER IST DATENSCHUTZRECHTLICHER AUFTRAGGEBER?

Durch die Eigenschaft als Auftraggeber der DLS wird das BMVIT nicht automatisch zum datenschutzrechtlichen Auftraggeber iSd § 4 Z 4 DSG im Hinblick auf die übermittelten Daten. Einerseits besteht nämlich die „Dienstleistung" der DLS nur darin, allen Beteiligten Postfächern für den Datenaustausch zu bieten und bestimmte Aufgaben zur sicheren Übertragung der Daten zu übernehmen. Darüber hinaus müssen die Daten auf eine Weise verschlüsselt werden, dass die DLS gar keine Möglichkeit hat, die Inhalte einzusehen. Die Protokollierung der DLS beinhaltet rein statistische Werte ohne Personenbezug. Die fortlaufende einmalige Nummer jedes Auskunftsvorgang („Unique-ID") kann lediglich eine nachprüfende Kontrolle (zB durch Datenschutzkommission, Rechtsschutzbeauftragten oder Gericht) erleichtern, der Personenbezug kann aber über die DLS selbst nicht hergestellt werden, weil die Daten in der DLS nur verschlüsselt vorhanden und damit aus der Perspektive der DLS nur indirekt personenbezogen sind.

Im Hinblick auf diese Rollenverteilung lässt sich die Konstruktion der datenschutzrechtlichen Verantwortung wohl am besten so beschreiben: Das BMVIT ist als verantwortliche Stelle (gesetzlicher) Dienstleister iSd § 4 Z 5 DSG jeweils für den Auftraggeber, für dessen Anwendung Daten an die DLS übergeben oder von der DLS übernommen werden. Das heißt wenn die DLS eine Anordnung der Staatsanwaltschaft in das Postfach des Anbieters zustellt, geschieht dies im Dienst der Behörde, von welcher die Anordnung stammt. Nur in einer einzigen Hinsicht ist das BMVIT selbst als unmittelbarer datenschutzrechtlich verantwortlicher Auftraggeber zu sehen, nämlich in Bezug auf die Verarbeitung der Information, welche Benutzer überhaupt Auskunftsbegehren über die DLS abwickeln.

Das Bundesrechenzentrum ist überhaupt funktionell nur Sub-Dienstleister im Sinne des § 4 Z 5 DSG, der die notwendige technische Infrastruktur (also die DLS an sich) implementiert und betreibt. Das BRZ wäre somit dem BMVIT verantwortlich und das BMVIT seinerseits den Behörden, in deren Auftrag die Daten übermittelt werden. Die Stellung eines datenschutzrechtlichen Auftraggebers kommt dem Bundesrechenzentrum im Hinblick auf den Betrieb der DLS in keiner Phase zu. Die Grundlage dafür bildet dann die (zu erlassende) Verordnung (DSVO) sowie ein auf Basis dieser Verordnung abzuschließender Vertrag zwischen dem BMVIT und dem BRZ.

Festzuhalten ist, dass auch ein Anbieter bei der Übermittlung einer Antwort auf ein Auskunftsbegehren einer Behörde nicht selbst zum datenschutzrechtlichen Auftraggeber wird. Rechtmäßiger Auftraggeber kann dann jedes Rechtssubjekt sein, das eine ausreichende Berechtigung bzw. eine gesetzliche Zuständigkeit zur Verfolgung dieses Zwecks besitzt. Der Zweck der Datenübermittlung ist die Strafverfolgung oder die Gefahrenabwehr. Diesen Zweck kann ein Anbieter nicht rechtmäßigerweise verfolgen. Er kann in diesem Bereich nur Dienstleister derjenigen Behörden sein, die diesen Zweck zu vollziehen haben. Ausgehend von den generellen Bestimmungen des DSG 2000 müssen daher die Strafverfolgungsbehörden bzw. die Sicherheitsbehörden als Auftraggeber begriffen werden und die Anbieter als deren Dienstleister, mit der Funktion, im Fall eines Auskunftsbegehrens die entsprechenden Daten zu ermitteln und zu übermitteln.[465]

[465] Siehe dazu ausführlich die Argumentation schon oben zur datenschutzrechtlichen Rolle bei der Speicherung der Daten in Kapitel IV.2.7.1.

IV.2.11.3 LÖSUNGSVORSCHLÄGE FÜR EINE DSVO

Die soeben ausgeführten Überlegungen könnten legistisch folgendermaßen erfasst werden:[466]

§ 8 Allgemeines

(1) Die Übermittlung der Daten erfolgt über eine zentrale Durchlaufstelle, die das Bundesministerium für Verkehr, Innovation und Technologie bei der Bundesrechenzentrum GmbH einzurichten hat.
[…]

§ 9 Durchlaufstelle – Grundstruktur

(1) […]
(2) Die Durchlaufstelle ist auf eine Weise einzurichten, dass für die Bundesrechenzentrum GmbH als Dienstleister der Durchlaufstelle im Sinne des DSG 2000 ein Zugang zu personenbezogenen Inhalten von Anfragen zu Datenauskünften so wie von deren Beantwortung nicht möglich ist.
[…]

§ 10 Einrichtung und Betrieb der Durchlaufstelle – Auftraggeber und Durchführung

(1) Die Einrichtung der Durchlaufstelle sowie die Zertifikatsverwaltung und die Datensicherheit liegen in der Verantwortung des Bundesministeriums für Verkehr, Innovation und Technologie.
(2) Die Einrichtung und der Betrieb der Durchlaufstelle erfolgt durch die Bundesrechenzentrum GmbH. Die Bundesrechenzentrum GmbH ist funktionell Dienstleister im Sinne des § 4 Z 5 DSG 2000 jeweils für den Auftraggeber, für dessen Anwendung Daten an die Durchlaufstelle übergeben oder von der Durchlaufstelle übernommen werden.
[…]

IV.2.12 AUDITIERUNG

Das BMVIT muss auf Basis einer DSVO die Spezifikation vornehmen, mit der die näheren technischen Anforderungen an die DLS beschrieben werden. Auf Basis dieser Spezifikation hat das Bundesrechenzentrum die DLS sodann einzurichten und zu betreiben. Der Zweck einer Auditierung besteht sodann in der Sicherstellung, dass im BRZ auch tatsächlich das implementiert wurde, was in der technischen Spezifikation vorgegeben war. Diese Überprüfung ist im Sinne der Datensicherheit essentiell. Sofern von der DLS für die Behörden und die Anbieter auch eine Client-Software zur Verfügung gestellt wird, muss diese als „Standardsoftware“ zur Kommunikation mit der DLS ebenfalls auditiert werden. Eine auditierte Client-Software muss aber nicht der einzige Kommunikationsweg mit der DLS sein, weil auch die Möglichkeit bestehen sollte, dass Anbieter und Behörden über ein

[466] Die Formulierungen stammen aus der BIM-Datensicherheitsstudie S. 141 ff; diese Vorschläge wurden unverändert durch das BMVIT in öffentliche Begutachtung geschickt; vgl. dazu den Begutachtungsentwurf im Anhang.

Webservice mit der DLS kommunizieren können. Die Auditierung betrifft nur die Datensicherheit bei der Durchlaufstelle, nicht aber die Betreiberimplementierungen.[467]

IV.2.12.1 LÖSUNGSVORSCHLAG FÜR EINE DSVO

Die soeben ausgeführten Überlegungen könnten legistisch folgendermaßen erfasst werden:[468]

§ 10 Einrichtung und Betrieb der Durchlaufstelle – Auftraggeber und Durchführung

(1) […]
(2) […]
(3) Das Bundesministerium für Verkehr, Innovation und Technologie kann sich zur Auditierung der tatsächlichen Umsetzung der technischen Spezifikation durch die Bundesrechenzentrum GmbH eines Dienstleisters bedienen.

§ 11 Auditierung der Durchlaufstellen-Funktionen

Der Bundesminister für Verkehr, Innovation und Technologie stellt sicher, dass

1. die tatsächliche Umsetzung der Durchlaufstelle durch die Bundesrechenzentrum GmbH den Spezifikationen zur Durchlaufstelle entspricht,
2. jene Dienste, die von der Durchlaufstelle für die Ausführung in der Client-Software der jeweiligen Benutzer zur Verfügung gestellt werden, für einen Client-Administrator verifizierbar ist (Signatur) und der Schnittstellendefinition zur Durchlaufstelle entspricht,
3. nur eine auditierte schnittstellenkonforme Software der Durchlaufstelle eine richtige Datenübertragung ermöglicht,
4. nur authentifizierte Anwender ihre öffentlichen Schlüssel in der Durchlaufstelle eindeutig zu ihrer jeweiligen Institution zugehörig hinterlegen können und
5. jede Änderung der Durchlaufstelle einer Re-Auditierung zum Zweck der Sicherstellung der Verifizierbarkeit der Echtheit der Software durch die Endnutzer unterliegt.

Im Begutachtungsverfahren wurde zu dieser Regelung in einer Stellungnahme vom Verein der Internetbenutzer Österreichs (VIBE.AT)[469] kritisiert, dass die Regelung des § 10 Abs. 3 DSVO-Entwurf die Formulierung „…kann sich zur Auditierung (…) eines Dienstleisters bedienen“ verwendet. „Um die Sicherheit der DLS zu gewährleisten, muss das BMVIT einen externen, unabhängigen Dienstleister mit dem Audit beauftragen“[470], wird diesbezüglich gefordert. Weiters wird gefordert, dass die Audits regelmäßig durchgeführt werden sollten, um sicherzugehen, dass die DLS auf dem aktuellen Stand der Technik bleibt. Außerdem sollten die Ergebnisse dieser Audits der Öffentlichkeit oder zumindest dem Datenschutzrat vorgelegt werden, bevor die DLS in Betrieb genommen wird.

Grundsätzlich sind diese Anregungen zu begrüßen. Aus der Formulierung „kann“ in § 10 Abs. 3 DSVO-Entwurf sollte jedoch nicht geschlossen werden, dass die Durchführung einer Auditierung im Belieben des BMVIT stehen würde. Die Verpflichtung zur Auditierung ergibt sich unmittelbar aus §

---

[467] Vgl. die Zusammenfassung der Diskussion beim 4. Round Table, BIM-Datensicherheitsstudie S. 114.
[468] Die Formulierungen stammt aus der BIM-Datensicherheitsstudie S. 142; der Vorschlag wurde unverändert durch das BMVIT in öffentliche Begutachtung geschickt; vgl. dazu den Begutachtungsentwurf im Anhang.
[469] http://wiki.vibe.at/Hauptseite.
[470] Stellungnahme veröffentlicht unter http://wiki.vibe.at/Begutachtung_DatensicherheitsVerordnung.

11. Die kann-Bestimmung bezieht sich auf das Heranziehen eines externen Dienstleisters. Theoretisch ist denkbar, dass das BMVIT nämlich selbst über die Ressourcen verfügt, eine solche Auditierung vorzunehmen. Tatsächlich ist dies derzeit aber nicht der Fall. Gleichwohl, auch die Verpflichtung zur Beauftragung eines externen Dienstleisters mit der Autidierung wird im Sinne einer höheren Datensicherheit und Transparenz hier gutgeheißen. Was die Frage nach dem „Stand der Technik" betrifft, ist das Anliegen berechtigt und auch im Sinne der Rechtssprechung des deutschen Bundesverfassungsgericht grundrechtlich geboten.

IV.2.13 Kosten und Kostentragung einer Umsetzung der DLS

Die Frage der Kostentragung stellt zwar keine unmittelbare Frage der Datensicherheit dar. Allerdings war die Klärung dieser Frage in den Round Table Diskussionen zum Konzept der DLS von großer Bedeutung für die Entscheidung, ob ein solches System tatsächlich umgesetzt werden sollte. Mit anderen Worten war der Kostenfaktor wesentlich für die Entscheidung, welches Ausmaß an Datensicherheit sich die Republik Österreich im Zuge der Umsetzung der Vorratsdatenspeicherung leisten kann und will. Aus diesem Grund werden die wesentlichen Argumente nachfolgend behandelt.

IV.2.13.1 Kostenschätzung der Einrichtung und des Betriebs der DLS?

Das Bundesrechenzentrum (BRZ) hatte für den 3. Round Table auf Basis der bisherigen Diskussion eine Kostenschätzung für eine Umsetzung des Konzepts der Durchlaufstelle (DLS) unternommen.[471] Die Umsetzung der Durchlaufstelle würde nach dieser ersten Schätzung 288.000 Euro an initialem Aufwand verursachen, die monatlichen Betriebskosten für Hard- und Software wurden auf etwa 4.500 Euro geschätzt. Die Schätzung ist sehr vorsichtig angelegt, damit nicht zu befürchten ist, dass sich im Falle einer tatsächlichen Umsetzung die Kosten dann als deutlich höher erweisen. Dieser Kostenschätzung liegen folgende Annahmen zugrunde:

Authentifizierung mittels qualifizierter Signatur

Nutzung vorhandener Infrastruktur des BRZ (bestehende Serversysteme)

Maximale Größe der zu übermittelnden Daten 15 MB

Die Schätzung enthält ein Portal für Netzanbieter ähnlich dem Portalverbund.

Die Funktion eines Help-desk ist nicht enthalten.

Aufwendungen für erhöhte Sicherheit sind in der Kostenschätzung nicht enthalten.

[471] Vgl. die Zusammenfassung der Diskussion beim3. Round Table, BIM-Datensicherheitsstudie S. 105 ff.

IV.2.13.2 KOSTENERSPARNIS BEI EINRICHTUNG EINER DLS?

Auf den ersten Blick entsteht zunächst der Anschein, die DLS verursacht zusätzliche Investitionskosten für den Bund in Höhe von rund 300.000,-- Euro, die beispielsweise bei der verschlüsselten Übermittlung per E-Mail (ursprünglich im Begutachtungsentwurf zur TKG-Novelle vorgesehenes „S/MIME Konzept“) nicht anfallen. Die Relation zu den - zu 80% zu erstattenden - Investitionskosten der Anbieter erschließt sich bei näherer Betrachtung wie folgt: Ohne die zentrale Variante der DLS müssten schon in der Implementierungsphase zwischen ca. 200 Anbietern (nach Angaben der RTR derzeit speicherpflichtig gemäß § 102a TKG) und mindestens 15 auskunftsberechtigten Stellen auf Seiten der Sicherheitsbehörden dezentral sichere Wege zur Datenübermittlung und zur Authentifizierung geschaffen werden. Das würde erfordern, dass die technische Implementierung mit allen Anbietern jeweils definiert und implementiert werden müsste, allein der dezentrale Austausch der Sicherheits-Zertifikate würde dabei schon beträchtlichen Aufwand verursachen. Demgegenüber muss die Spezifikation zur DLS nur einmal ausgearbeitet werden (unter Beteiligung der Telekom Branche, die dabei teilweise auch über die Interessenvertretungen erfolgt und nicht für alle - vor allem kleinere - Anbieter unmittelbar Aufwand verursacht). Die zentrale Architektur und vor allem die zentrale Hinterlegung der public keys vereinfachen diese Prozesse enorm, der einzelne Anbieter benötigt für die Abwicklung nur noch einen herkömmlichen Internet-Browser für eine sicher Verbindung (per https) zur Durchlaufstelle.

Es herrschte daher in den Round Table Diskussionen Konsens darüber, dass der Aufwand für die Spezifikation der Schnittstelle beim dezentralen S/MIME Konzept deutlich höher wäre als bei der zentralen Variante der DLS. Wenn dieser Mehraufwand auf Seiten aller Anbieter insgesamt Kosten in Höhe von 375.000 Euro verursachte (wovon 80% - also 300.000 Euro - vom Bund zu erstatten wären), wäre die DLS auch vom Investitionskostenaufwand her günstiger als eine verschlüsselte Übermittlung per E-Mail. Bei 200 Anbietern wird diese Schwelle erreicht, wenn im Durchschnitt Mehrkosten in Höhe von 1.875 Euro pro Anbieter entstehen. Bei üblichen Tagsätzen für qualifizierte IT Techniker würde diese Schwelle wohl leicht überschritten, weil ein durchschnittlicher Mehraufwand von zwei Arbeitstagen pro Unternehmen selbst bei vorsichtiger Schätzung von allen Beteiligten als realistisch eingeschätzt wurde.[472]

Ein wesentlicher Kostenvorteil des Modells der DLS im operativen Ablauf ist die Verringerung der Kommunikationswege. Es ist die effizienteste Vorgangsweise, nur mit einer Stelle zu kommunizieren. Auf Seiten der Anbieter wären keine speziellen technischen Voraussetzungen nötig, da die DLS über eine sichere „https“-Verbindung praktisch mit jedem gängigen Browserprogramm erreichbar wäre. In welchem Ausmaß ein Anbieter seine Prozesse bis zur Erstellung der „CSV-Datei“ mit den begehrten Daten automatisiert, bleibt ihm selbst überlassen, was insbesondere für kleinere Anbieter wichtig ist, bei denen eine teure Automatisierung in keinem Verhältnis zur Zahl der jährlichen Auskünfte steht. Auf Seiten der Anbieter wird allerdings keine Kostenersparnis in wesentlichem Ausmaß erwartet. Es muss auf jeden Fall die „CSV-Datei“ gemäß § 94 Abs. 4 TKG-Entwurf befüllt und übermittelt werden. Ob die Sicherung der Übermittlung über eine (ohnehin vom Bund einzurichtende) Public-Key-Infrastructure und S/MIME oder über eine Durchlaufstelle erfolgt, macht für die Anbieter kostenmäßig keinen großen Unterschied. Die höhere Zuverlässigkeit bei der Authentifizierung und der Umstand, dass es nur eine Stelle gäbe, an die zu übermitteln wäre, würde aber jedenfalls

[472] Vgl. BIM-Datensicherheitsstudie S. 107 ff.

mögliche Fehlerquellen minimieren und damit Vorteile bringen, die sich schwer quantifizieren lassen.[473]

Am stärksten spürbar wird eine Ersparnis für die Sicherheitsbehörden im operativen Betrieb sein. Durch stärkere Automatisierung und die zentrale Kommunikation über die DLS wird bei den Auskunftsbegehren von Seiten des Bundeskriminalamts eine beträchtliche Aufwandsersparnis erwartet. Die größte Aufwandsreduzierung besteht vor allem darin, dass im Vergleich zur E-Mail-Variante die laufende Erneuerung der Sicherheitszertifikate zentral erfolgt und damit massiv erleichtert wird. Die Erfahrung aus der Europol Kooperation zeigt, dass dies bei einer dezentralen sicheren Kommunikation zwischen vielen Stellen ein enormer Aufwands- und damit Kostensteigerungsfaktor ist. Eine unverbindliche Einschätzung seitens der IT-Abteilung des BMI geht davon aus, dass die „S/MIME Variante" hier einen Mehraufwand im Ausmaß einer vollen Planstelle bedeuten würde. Stellt man dem die geschätzten Betriebskosten der DLS in Höhe von rund 4.500 Euro entgegen, zeigt sich auch für den operativen Betrieb die DLS als die kostengünstigere Variante.[474]

IV.2.13.3 KOSTENTRAGUNG UND VERHÄLTNISMÄßIGKEIT AUS SICHT DER ANBIETER

Die Grundlagen zur Kostenerstattung für Anbieter bei der Umsetzung der Vorratsdatenspeicherung wurden in den Erläuterungen zu § 94 Abs. 1 des BIM-Entwurf zur TKG-Novelle 2010 formuliert: „Da die Vorratsdatenspeicherung (zwangsläufig) nur durch die Anbieter von Kommunikationsdiensten vorgenommen werden kann, bei denen die speicherpflichtigen Daten erzeugt bzw. verarbeitet werden, wird durch die Normierung der Speicherpflicht eine Inpflichtnahme Privater durch den Staat begründet. Im konkreten Fall wird dadurch in verfassungsrechtlich geschützte Rechtspositionen der betroffenen Anbieter, nämlich die durch Art. 5 StGG und Art. 1 1. ZProtMRK verfassungsgesetzlich normierte Eigentumsfreiheit, eingegriffen, da die Anbieter zur Erfüllung ihrer Verpflichtung erhebliche Investitionen vornehmen müssen, die sich aus Erstinvestitions- sowie laufenden Kosten zusammensetzen. Der Verfassungsgerichtshof hat (beginnend mit VfSlg 6884/1972; 7234/1972) im Hinblick auf derartige Eigentumseingriffe aus dem Gleichheitsgrundsatz Pflichten zur Enteignungsentschädigung abgeleitet, um das Erfordernis der Verhältnismäßigkeit bei Eigentumseinschränkung zu erfüllen. Insbesondere dürfen „auch im besonderen öffentlichen Interesse gelegene Verpflichtungen, die mit einer erheblichen Vermögensbelastung verbunden sind, […] nur auferlegt werden […], wenn dies unter Bedachtnahme auf das Prinzip der Verhältnismäßigkeit wirtschaftlich zumutbar ist"[475].

Die derzeit geltende Rechtslage verpflichtet Anbieter einerseits zur Bereitstellung von Einrichtungen zur Überwachung einer Telekommunikation (soweit diese nach der StPO erforderlich sind), andererseits zur Mitwirkung im erforderlichen Ausmaß (§ 94 Abs 1 und 2 TKG 2003, BGBl I 70/2003 idgF). Dabei ist allerdings zu berücksichtigen, dass die daraus resultierenden zugemuteten Aufwendungen verhältnismäßig sein müssen. Insbesondere ist eine wirtschaftliche Belastung der Telekommunikationsbetreiber bzw. die Bereithaltung aufwändiger Vorkehrungen nur bei Vorliegen besonderer Umstände nach Maßgabe einer Interessensabwägung gerechtfertigt: „Mag auch die

[473] Ibid, S. 101.
[474] Ibid, S. 108.
[475] VfSlg 13.587/1993.

Inpflichtnahme privater Betreiber von Telekommunikationsdiensten für die Überwachung des Fernmeldeverkehrs und die Bereitstellung entsprechender Einrichtungen eine sachlich gerechtfertigte und daher verfassungsmäßige Mitwirkungspflicht Privater an einer staatlichen Aufgabe darstellen, so ist dennoch auch bei der Regelung der Kostentragung der Verhältnismäßigkeitsgrundsatz zu beachten (VfSlg 16.808)."[476]

Der Kostenersatz sollte daher sichergestellt sein für die Implementierung der Durchlaufstelle im Bundesrechenzentrum, für die Implementierung durch die Anbieter und mittels ÜKVO auch für den Betrieb. Zu den laufenden Kosten gemäß Überwachungskostenverordnung (ÜKVO) wurde diskutiert, dass sich die Kosten zwischen Abfrage von Vorratsdaten und Abfrage von Verkehrsdaten nicht unterscheiden sollten. Dabei wurde auch diskutiert, ob die Betriebskosten der Durchlaufstelle im Zusammenhang mit der ÜKVO geregelt werden könnten. Damit verbunden ist die Frage, ob diese Betriebskosten (indirekt) anteilig von den Anbietern mitfinanziert werden sollten. Dies wird Gegenstand von Verhandlungen im Zusammenhang mit der Überarbeitung der ÜKVO anlässlich der TKG Novelle sein.[477]

IV.2.13.4 KOSTENTRAGUNGSREGELN IM TKG

Grundsätzlich ist zunächst von Bedeutung, dass die „DLS" einen Teil der Umsetzung der Richtlinie zur Vorratsdatenspeicherung 2006/24/EG darstellt, weil die besonderen Anforderungen an die Datensicherheit ihre Grundlage in Art 7 Lit. c) der RL haben: „in Bezug auf die Daten werden geeignete technische und organisatorische Maßnahmen getroffen, um sicherzustellen, dass der Zugang zu den Daten ausschließlich besonders ermächtigten Personen vorbehalten ist." Denselben Standard auf die Abwicklung aller Datenauskünfte (auch „Betriebsdaten", nicht nur „Vorratsdaten") anzuwenden ist dabei nicht nur konsequent sondern auch aus rein praktischen Gründen notwendig. Viele Auskünfte werden nämlich künftig wohl „gemischte" Datensätze enthalten, also in derselben Auskunft „Vorratsdaten" und „Betriebsdaten". Diese Annahme ist deshalb wesentlich, weil es bzgl. der Vorratsdatenspeicherung in der Regierungsvorlage zum TKG klare Regeln zur Kostentragung gibt. Investitionskosten die dabei auf Anbieterseite anfallen, müssen dabei gem. § 94 TKG-Entwurf zu 80% vom Bund ersetzt werden. Eine Deckelung auf einen absoluten Höchstbetrag ist gesetzlich nicht vorgesehen und wäre vom Gesetzeswortlaut auch nicht gedeckt.[478]

IV.2.13.5 KOSTENVERTEILUNG UNTER DEN BETEILIGTEN MINISTERIEN?

In diesem Zusammenhang stellt sich die Frage, in welchem Verhältnis zu der eben beschriebenen Regelung jene Kosten stehen, die auf Behördenseite für die Umsetzung der Vorratsdatenspeicherung anfallen. Die Einrichtungskosten der DLS fallen zwar direkt beim Bund an, stehen aber in unmittelbarem Zusammenhang zu den Investitionskosten der Anbieter. Wie oben gezeigt wurde, reduzieren sich durch die Implementierung der DLS jene Kosten deutlich, die ansonsten auf Anbieterseite als Aufwand zur Schnittstellenspezifikation anfallen und vom Bund zu 80% ersetzt würden. Daher lässt sich folgerichtig argumentieren, dass die Implementierungskosten der DLS

[476] Siehe dazu den BIM-Entwurf zur TKG-Novelle 2010, Erläuterungen zu § 94 Abs. 1, S. 40f.
[477] Siehe die Zusammenfassung der Diskussion zum 3. Round Table, BIM-Datensicherheitsstudie S. 109.
[478] Ibid, S. 116.

sachlich von dem mit insgesamt 15.000.000 Euro bezifferten Budgetvolumen[479] erfasst sind, die der Bund für die gesamten Investitionskosten zur Umsetzung der Vorratsdatenspeicherung veranschlagt hat. Diese Annahme ist deshalb wesentlich, weil bei der Verabschiedung der gemeinsamen Regierungsvorlage zur TKG-Novelle auch eine Vereinbarung zur Aufteilung dieser Kosten auf die Ministerien BMI (33%), BMJ (Fixbetrag von € 360.000,--) und BMVIT (67%) getroffen wurde. [480]

IV.2.13.6 LÖSUNGSVORSCHLÄGE FÜR EINE DSVO

Die soeben ausgeführten Überlegungen zur Kostentragung könnten legistisch folgendermaßen erfasst werden:[481]

§ 24 Kostentragung der Durchlaufstelle

(1) Die Investitionskosten der Durchlaufstelle sind gemäß § 94 Abs. 1 TKG 2003 entsprechend dem dort festgelegten Aufteilungsschlüssel vom Bundesministerium für Inneres, dem Bundesministerium für Justiz und dem Bundesministerium für Verkehr, Innovation und Technologie zu tragen.
(2) Die laufenden Kosten der Durchlaufstelle sind gemäß § 94 Abs. 2 TKG 2003 vom Bundesministerium für Inneres und vom Bundesministerium für Justiz zu tragen.

Für den Begutachtungsentwurf des BMVIT wurde diese Bestimmung folgendermaßen abgeändert:

Kostentragung der Durchlaufstelle

§ 24. (1) Die Investitionskosten.für die Durchlaufstelle sind Investitionskosten gemäß § 94 Abs. 1 TKG 2003.

Die knappe Formulierung im geänderten Abs. 1 beschränkt sich bzgl. der Investitionskosten auf einen Verweis auf § 94 Abs. 1 TKG. In Zusammenschau mit den Ausführungen zu den finanziellen Auswirkungen im Vorblatt zum Begutachtungsentwurf[482] wird aber klar, dass sich daraus keine Veränderung des Regelungsgehalts gegenüber dem Vorschlag aus der BIM-Datensicherheitsstudie ergibt. Dort werden nämlich die Ausführungen zum Aufteilungsschlüssel wiedergegeben, die im Rahmen der BIM-Datensicherheitsstudie als Erläuterungen zu § 24 formuliert wurden.

Die Streichung des Abs. 1 bewirkt demgegenüber eindeutig eine Veränderung des Regelungsgehalts gegenüber der Version aus der BIM-Datensicherheitsstudie. Er bewirkt schlicht, dass die Frage der Aufteilung der Betriebskosten der DLS offen bleibt. Im Vorblatt wird darauf hingewiesen, dass aus die Bedeckung der laufenden Kosten (Betriebskosten) der DLS mit vorhandenen Budgetmitteln der beteiligten Ressorts erfolgt. Die Aufteilung der laufenden Kosten bleibt aber ausdrücklich einer interministeriellen Vereinbarung vorbehalten. Diese Frage stellt, um nach dem Stand der

---

[479] Zur Argumentation dieser Kosten siehe das Vorblatt der Regierungsvorlage zur TKG Novelle, BlgNR 1074. XXIV. GP, http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01074/fname_206854.pdf.
[480] Vgl. die Zusammenfassung der Diskussion beim 2. Round Table sowie beim3. Round Table, BIM-Datensicherheitsstudie S. 98 ff.
[481] Die Formulierung stammt aus der BIM-Datensicherheitsstudie S. 146; dieser Vorschlag wurde für den Begutachtungsentwurf deutlich verändert, dazu sogleich; vgl. dazu den Begutachtungsentwurf im Anhang.
[482] Siehe den Begutachtungsentwurf zur DSVO im Anhang.

Diskussionen und den Ergebnissen des Begutachtungsverfahrens zu urteilen, die letzte dar, deren Klärung für die Herstellung des notwendigen Einvernehmens zwischen BMVIT, BM.I und BMJ noch eine eher schwierigere Diskussion mit sich bringen wird.

IV.3 Schlusswort - der Beitrag des Datensicherheitskonzepts zum Grundrechtsschutz

Der wissenschaftliche Fokus dieser Arbeit und das zugrunde liegenden Forschungsprojekts im Rahmen der BIM-Datensicherheitsstudie war von Beginn an darauf ausgerichtet, ausgehend vom Rahmen der grundrechtlichen Anforderungen, insbesondere im Hinblick auf die Achtung der informationellen Selbstbestimmung, ein Referenzkonzept zur Datensicherheit im Rahmen der Vorratsdatenspeicherung zu entwickeln, an dem sich die aktuellen Umsetzungsvorhaben orientieren können. Datensicherheit und Informationssicherheitsmanagement werden dabei nicht als Selbstzweck betrachtet sondern sind vielmehr ein Instrument, um den grundrechtlichen Schutzbedürfnissen so weit wie nur möglich zu begegnen.

Der neuartige Ansatz besteht eben darin, die Perspektive des Grundrechtsschutzes ins Zentrum einer Entwicklungsaufgabe zu setzen, die primär auf technischer Ebene umgesetzt werden soll. Der erste Schritt dafür ist die Erforschung der durch die Grundrechte vorgegebenen Determinanten. Sodann werden die einfachgesetzliche Rechtslage in Beziehung zum eher grobmaschigen Raster der Grundrechte gesetzt und dabei die wesentlichen Anknüpfungspunkte für ein Datensicherheitskonzept identifiziert. Bedeutung erlangen diese vor allem durch den Umstand, dass der Gestaltungsspielraum letztlich in das Korsett einer Verordnungsermächtigung mündet, in deren Umsetzung die eigentliche Aufgabe der Konkretisierung der Sorgfaltspflichten zu erfüllen ist. Und genau hier beginnt das Kernstück der Arbeit: Die rechtswissenschaftliche Formulierung der Anforderungen auf einer tiefen Abstraktionsebene, die so nahe wie möglich an der technischen Ausgestaltung eines umfassenden Datensicherheitskonzeptes liegen soll. Auf diese weise werden die (grund-)rechtlichen Analysen mit konkreten praktischen Problemstellungen und ebenso konkreten Lösungsvorschlägen verbunden.

Das Konzept der Durchlaufstelle (DLS) und der dazugehörigen legistischen Lösungsvorschläge für eine Datensicherheitsverordnung, die dieses Konzept umsetzen könnte, ist in dieser Hinsicht ein Novum, weil Gesetze und Verordnungen üblicherweise keine so hohe technische Determinierungsdichte aufweisen. Damit geht einher, dass das grundrechtliche Schutzniveau nicht allein vom guten Willen oder dem grundrechtlichen Feingefühl jener abhängig ist, die letzten Endes ein Pflichtenheft in technischer Sprache zu verfassen haben. Im modernen Datenschutz ist diese Figur seit einiger Zeit unter dem Begriff „privacy by design“ bekannt. Die Etablierung dieses Ansatzes auch auf der Ebene der Gesetz- und Verordnungsgebung hat noch beträchtliches Entwicklungspotential, zu dessen Entfaltung diese Arbeit ein Beitrag sein soll.

Die Durchlaufstelle zeigt dabei konkret, dass die Beachtung der Anforderungen des Datenschutzes und der dahinter zu schützenden Grundrechtspositionen weder eine Einbuße an Benutzerfreundlichkeit noch Zugeständnisse an die Funktionalität mit sich bringen muss. Durch die Adressierung und Zusammenschau aller für die Praxis wesentlichen Fragen ist das Konzept ausgewogen im Hinblick auf die Notwendigkeiten und Bedürfnisse aller Beteiligten. Die Abwicklung von Datenauskünften wird stärker als bisher automatisiert, ohne dabei den staatlichen Behörden

einen freien Zutritt zur Rasterfahndung in der Gesamtheit aller Kommunikationsdaten zu geben. Die Einhaltung der gesetzlich zulässigen Datenermittlungen und Verknüpfungen ist schon auf der technischen Ebene fixiert und reduziert damit die Gefahr von Missbrauch, wenngleich diese niemals völlig unterbunden werden kann. Des Weiteren schafft die Durchlaufstelle ein effektiveres System zur Kontrolle der Rechtmäßigkeit, in dem die unumgängliche Protokollierung aller Datenauskünfte automatisiert und vom Willen der Beteiligten unabhängig gemacht wird. Dass im Konzept der DLS in Hinkunft alle am Datenaustausch Beteiligten zuverlässig identifiziert und authentifiziert werden, ist im Vergleich zum Status Quo geradezu eine Revolution. Dabei ist die sichere Anbindung mit verhältnismäßig geringem Aufwand verbunden, weil durch die Einbindung in die bestehenden Strukturen und Standards des Portalverbundes Synergien genutzt werden.

Ein wesentliches Element der Datensicherheit ist, dass mit der DLS trotz der zentralisierten Abwicklung aller Auskunftsvorgänge keine zusätzliche „Datenkrake“ geschaffen wird, weil die schützenswerten Inhalte einerseits so verschlüsselt sind, dass sie der DLS selbst gar nicht zugänglich sind, und andererseits auch die verschlüsselten Inhalte nur so lange zentral gelagert werden, bis sie vom Empfänger abgeholt werden. Dadurch wird vermieden, dass die eigentlich zur Sicherheitsoptimierung gedachte Schnittstelle ihrerseits zum schwer kontrollierbaren Sicherheitsrisiko wird. Allerdings muss man sich der Tatsache bewusst sein, dass es keine absolute Sicherheit geben kann. Die Rechtsschutzvorkehrungen sind daher ein Fehlerkalkül, um zumindest leichter nachvollziehen zu können, wo eine Fehlerquelle gelegen sein könnte, falls doch ein unerwünschtes Ereignis eintritt. Verbunden mit den Protokollierungsvorschriften für die Anbieter und den entsprechenden Richtlinien auf Behördenseite hilft die Protokollierung über die DLS im Schadensfall bei der Rekonstruktion der Ereignisse, was in seiner präventiven Wirkung nicht zu unterschätzen ist. Dadurch, dass die DLS-Protokollierung selbst keine personenbezogenen Daten enthält, wird wiederum vermieden, dass das eigentlich für die Datensicherheit gedachte System selbst zum Risikofaktor wird.

Die automatisierte Aufbereitung der Statistik zu den Auskunftsfällen erfüllt eine wesentliche gesellschaftspolitische Funktion, weil damit Transparenz geschaffen wird und ein ausufernder Gebrauch der Überwachungsinstrumente durch Sicherheits- und Strafverfolgungsbehörden möglicherweise schon von vornherein im Zaum gehalten wird. Daneben bringt die automatisierte statistische Aufbereitung enorme Aufwandserleichterungen mit sich und bietet zugleich tagesaktuelle Werte.

Auch wenn dies nicht primär eine Frage der Datensicherheit ist, so ist doch auch hervorzuheben, dass das Konzept der DLS nicht nur mittelfristig sondern schon im Zuge der Implementierung kostengünstiger als alle diskutierten Alternativmodelle (ETSI-Standard, S/MIME) ist. Dies ist insofern bedeutsam, als dadurch deutlich wird, dass ein höheres Schutzniveau nicht zwingend immer auch mit höheren Kosten verbunden ist. Und im Hinblick auf die Akzeptanz war diese Frage letzten Endes das Zünglein an der Waage.

Obwohl das Konzept der DLS zum Zeitpunkt des Abschlusses dieser Arbeit noch nicht definitiv Eingang in den Rechtsbestand gefunden hat, lässt der Stand der Diskussion nach dem Begutachtungsverfahren zur Datensicherheitsverordnung die Vermutung zu, dass die tatsächliche Umsetzung in nicht allzu ferner Zeit erfolgen wird. Dies allein schon deshalb, weil der Zeitrahmen für den Abschluss der Umsetzung der Vorratsdatenspeicherung bis 1.4.2012 keinen großen Spielraum lässt, mit der Diskussion zu einem völlig anderen Konzept noch einmal zurück an den Start zu gehen.

Dass die DLS also aller Wahrscheinlichkeit nach in die Realität finden wird, ist nach dem Entstehungsverlauf bemerkenswert. Noch im Februar dieses Jahres erweckte die Stimmungslage in den Round Table Diskussionen im Rahmen der BIM-Datensicherheitsstudie eher den Anschein, als würde die DLS als theoretisches Referenzkonzept allerhöchstens am Papier dieser Arbeit existieren. Aus wissenschaftlicher Sicht wäre dies nicht weiter schlimm gewesen, weil die Diskussionen der praktisch Relevanten Fragen in jedem Fall aufschlussreich und einer wissenschaftlichen Aufarbeitung zugänglich waren. Aus der Sicht des betroffenen Grundrechtsträgers ist der nunmehrige Ausgang des parallel verlaufenen rechtspolitischen Diskurses aber jedenfalls ein „happy End“.

V LITERATURVERZEICHNIS

V.1 MONOGRAPHIEN:

Albrecht, Hans-Jörg./ Grafe, A/ Kilchling, Michael. (2008): Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsdaten nach §§ 100g, 100h StPO; Forschungsbericht im Auftrag des deutschen Bundesministeriums der Justiz, Max Planck Institut.

Bertel, Christian /Venier, Andreas (2008): Strafprozessrecht, 2. Auflage, Wien: Manz.

Beulke, Werner (2010): Strafprozessordnung, 11. Auflage, Heidelberg: C.F. Müller.

Chadoian, Satenig (2011), Das Fernmeldegeheimnis im Zeitalter der Internet- und Mobilfunküberwachung. Eine rechtsvergleichende Untersuchung des schweizerischen und österreichischen Grundrechtsverständnisses im Hinblick auf neuartige technische Überwachungsmaßnahmen und unter besonderer Berücksichtigung der Prinzipientheorie, Dissertation Wien, Einreichung voraussichtlich Ende 2011.

Daum, Alexandra (1998): Drittwirkung und Fiskalgeltung der Grundrechte. Innsbruck, Univ., Diss.

Dohr, Walter / Pollirer, Hans / Weiss, Ernst (2008): DSG Kommentar, 8.Er.-Lfg., Wien: Manz.

Egli, Patricia (2002): Drittwirkung von Grundrechten. zugleich ein Beitrag zur Dogmatik der grundrechtlichen Schutzpflichten im Schweizer Recht / Zugl.: Zürich, Univ., Diss., Zürich: Schulthess (Zürcher Studien zum öffentlichen Recht, 147).

Fleury-Steiner, Benjamin; Nielsen, Laura Beth (2006): The new civil rights research. A constitutive approach. Aldershot, Hants, England, Burlington, VT: Ashgate (Law, justice, and power).

Grabenwarter, Christoph (2009): Europäische Menschenrechtskonvention, 4. Auflage, München: Beck.

Häberle, Peter (1972): Grundrechte im Leistungsstaat, in: Martens/Häberle/Bachof/Brohm (Hrsg.), Berlin - New York: Gruyter (Veröffentlichung der Vereinigung der deutschen Staatsrechtslehrer, 30).

Häberle, Peter (2008): Das Menschenbild im Verfassungsstaat. 4., aktualisierte u. erw. Aufl. Berlin: Duncker & Humblot (Schriften zum Öffentlichen Recht, 540).

Holoubek, Michael (1997): Grundrechtliche Gewährleistungspflichten. ein Beitrag zu einer allgemeinen Grundrechtsdogmatik / Zugl.: Wien, Wirtschaftsuniv., Habil.-Schr., 1996. Wien u.a.: Springer (Forschungen aus Staat und Recht, 114).

Holoubek, Michael (2004): Rechtliche Grundlagen der Informationswirtschaft. Wien u.a.: Springer.

Höpfel, Frank /Ratz, Eckart (2011): Wiener Kommentar zum Strafgesetzbuch, 2. Auflage, 1.-80. Lieferung und Austauschlieferungen 2005-2011, Wien: Manz [=WK].

Maunz, Theodor/Dürig, Günter (2011), Grundgesetz, 62. Ergänzungslieferung, München: Beck.

Münch, Ingo von (1998): Zur Drittwirkung der Grundrechte. Frankfurt am Main, Wien u.a.: Lang.

Pilnacek, Christian /Pleischl, Werner (2005): Das neue Vorverfahren, Wien: Manz.

Resch, Günter (1990): Entwicklung der Grundrechte in Österreich, Wien, Univ., Dipl. Arb. Wien.

Schneider-Danwitz, Klaus (1993): Datenschutz gegen private Branchenwarndienste. zur Auslegung des Bundesdatenschutzgesetzes und zur Drittwirkung der Grundrechte im Konflikt zwischen Informations- und Geheimhaltungsinteressen / Berlin, Freie Univ., Diss., 1994.

Spindler, Gerald /Schuster, Fabian (2011), Recht der elektronischen Medien, 2. Auflage, München: Beck.

Stelzer, Manfred (1991): Das Wesensgehaltsargument und der Grundsatz der Verhältnismäßigkeit. Wien u.a.: Springer (Forschungen aus Staat und Recht, 94).

Stelzer, Manfred (2004): Datenschutz im Gentechnikrecht. Studie über den allfälligen Anpassungsbedarf der datenschutzrechtlichen Bestimmungen des Gentechnikgesetzes. Wien: Bundesministerium für Gesundheit u. Frauen Sektion IV (Forschungsberichte der Sektion IV / Bundesministerium für Gesundheit und Frauen, 2004,1).

Suhr, Dieter/ Trautmann, Armin (2001): Gleiche Freiheit. Allgemeine Grundlagen und Reziprozitätsdefizite in der Geldwirtschaft. Bad Boll (Fragen der Freiheit, 259/260).

Taudes, Katharina (2005): Die mittelbare Drittwirkung der Grundrechte. Salzburg, Univ., Dipl.-Arb., 2006.

Thanner, Theodor/Vogl, Mathias (2010): Sicherheitspolizeigesetz, 4. Auflage, Wien – Gratz: NWV – Neuer Wiss. Verl..

Walter, Robert/Mayer, Heinz (2000): Grundriß des österreichischen Bundesverfassungsrechts, 9. Auflage, Wien: Manz.

Weber-Fas, Rudolf (2002): Der Verfassungsstaat des Grundgesetzes, Tübingen: Mohr Siebeck.

V.2 Aufsätze in Zeitschriften und Sammelbänden:

Albers, Marion / Reinhardt, Jörn (2010), Entscheidungsbesprechung – Vorratsdatenspeicherung im Mehrebenensystem: Die Entscheidung des BVerfG vom 2.3.2010, ZJS 2010, S. 767.

Badura, Art 10 GG, Bonner Kommentar, 136. Aktualisierung, Oktober 2008.

Boka, Manuel /Feiler, Lukas, die Vorratsdatenspeicherung von Verkehrs- und Standortdaten, in: Zankl (Hg.) Auf dem Weg zum Überwachungsstaat? Neue Überwachungsmaßnahmen im Bereich der Informations- und Kommunikationstechnologie (2009), 157ff.

Eisenberger, Iris (2010): Technik der Grundrechte - Grundrechte der Technik, in: Holoubek/Martin/Schwarzer (Hrsg.), Die Zukunft der Verfassung - Die Verfassung der Zukunft? Festschrift für Karl Korinek zum 70. Geburtstag, Wien - New York: Springer, 115 - 128.

Feiler, Lukas /Stahov, Ana (2011): Die Einführung der Vorratsdatenspeicherung in Österreich, Medien und Recht 3/11, 111 ff.

Fleury-Steiner, Benjamin/ Nielsen, Laura Beth (2006): A constitutive perspective of rights. Introduction, in: The new civil rights research, S. 1-6.

Funk, Bernd-Christian/ Krejci, Heinz/ Schwarz,Walter (1984): Zur Registrierung von Ferngesprächsdaten durch den Dienstgeber, in: DRdA, S. 285.

Hammer, Stefan; Lukas, Karin (2005): Internationale Menschenrechte als Schutzansprüche gegenüber wirtschaftlicher Macht. In: JRP, S. 173.

Heißl, Gregor (2009): Recht auf die Achtung des Privatlebens, des Hausrechts sowie des Breif- und Fernmeldegeheimnisses, in: Heißl (Hrsg.), Handbuch der Menschenrechte, Wien: Facultas. WUV, S.160-175.

Heißl, Gregor (2010): Happy End einer unendlichen Geschichte? Der Beitritt der EU zur EMRK und seine Auswirkungen auf Österreich, in: Holoubek/Martin/Schwarzer (Hrsg.), Die Zukunft der Verfassung - Die Verfassung der Zukunft? Festschrift für Karl Korinek zum 70. Geburtstag, Wien - New York: Springer, S. 129-148.

Helmreich, Markus (2005): Auskunftspflicht des Access-Providers bei Urheberrechtsverletzungen? ecolex, S.379.

Hofmann, Hans (2008): Art 10 GG in: Schmidt-Bleibtreu, Bruno (Hrsg.), Grundgesetz Kommentar, 11. Auflage, S. 340.

Kotschy, Waltraut (2011): Datenschutzrechtliche Fragen im Zusammenhang mit dem neuen Verbraucherkreditrecht, Österreichisches Bankenarchiv 2011, S. 307-312.

Ladeur, Karl-Heinz (2009): Das Recht auf informationelle Selbstbestimmung. Eine juristische Fehlkonstruktion? In: Die öffentliche Verwaltung, Jg. 62, H. 2, S. 45–55.

Laurer, René H. (1983): Der Geheimnisschutz im österreichischen Grundrechtssystem, in: EuGRZ 1983, S.29.

Lehner, Andreas (2009): Recht auf Datenschutz, in: Heißl (Hrsg.), Handbuch Menschenrechte, Wien: Facultas. WUV, S. 211-227.

Leutheusser-Schnarrenberger, Sabine (2007): Vorratsdatenspeicherung – Ein vorprogrammierter Verfassungskonflikt, in: ZRP, S. 9.

Liebwald, Doris (2006): The New Data Retention Directive, in: MR-Int, S.49.

Möstl, Markus (2010), Das Bundesverfassungsgericht und das Polizeirecht – Zwischenbilanz aus Anlass des Urteils der Vorratsdatenspeicherung, DVBl. 2010, S. 808.

Reindl, Susanne (2002): Telefonüberwachung zweimal neu?, in: JBl, S. 69.

Reindl, Susanne (1999): Die nachträgliche Offenlegung der Vermittlungsdaten im Fernmeldeverkehr („Rufdatenrückerfassung“), in: JBl, S. 791.

Schlink, Bernhard (1984): Freiheit durch Eingriffsabwehr - Rekonstruktion der klassischen Grundrechtsfunktion. In: EuGRZ, Jg. 11, H. 17, S. 457–468.

Schmölzer, Gabrielle(1997): Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr, in: JBl, S. 211.

Singer, Christian (2003): Kommentar zu § 93 TKG in: Stratil(u.a.), Telekommunikationsgesetz 2003, 297.

Suhr, Dieter (1984): Freiheit durch Geselligkeit. Institut, Teilhabe, Verfahren und Organisation im systematischen Raster eines neuen Paradigmas. In: EuGRZ, Jg. 11, H. 20, S. 529–546.

Tretter, Hannes (2010): Österreich: Aktuelle datenschutzrechtliche Herausforderungen, in: Zukunft. Die Diskussionszeitschrift für Politik, Gesellschaft und Kultur, 01/2010.

Tretter, Hannes (2009): Grundrechtliche Probleme der Verwendung personenbezogener Daten durch die Sicherheitsbehörden, in: Österreichische Juristenkommission (Hg.), Alles unter Kontrolle? Überwachung - Privatsphäre - Datenschutz [= Kritik und Fortschritt im Rechtsstaat, Band 34], Wien - Graz 2009, 55ff

Tschohl, Christof (2011), Der Europäische Vorrat an Daten über Kommunikationsverhalten, in: Bielefeld ua. (Hrsg.), Jahrbuch Menschenrechte (2011), Nothing to hide - nothing to fear? Datenschutz - Transparenz - Solidarität, Wien/Köln/Weimar: Böhlauverlag, 74ff.

Wessely, Wolfgang (1999): Das Fernmeldegeheimnis – ein unbekanntes Grundrecht?, in: ÖJZ, S. 491.

Wiederin, Ewald (1999): Art. 10a StGG, in: Korenik, Karl/Holoubek, Michael (Hrsg.), Österreichisches Bundesverfassungsrecht, Bd. III, Wien u.a.: Springer

Wolff, Heinrich Amadeus (2010), Vorratsdatenspeicherung – Der Gesetzgeber gefangen zwischen Europarecht und Verfassung?, NVwZ 2010, S. 751.

V.3 Online verfügbare Literatur und Informationen:

ARGE Daten, Website mit zahlreichen Informationen zu datenschutzrechtlichen Fragestellungen http://www.argedaten.at/ (13.10.2011).

BIM-Entwurf TKG-Novelle 2010, ausgearbeitet vom Ludwig Boltzmann Institut für Menschenrechte (BIM) im Auftrag des Bundesministeriums für Verkehr, Innovation und Technologie (BMVIT), 11.09.2009, zum Download unter http://bim.lbg.ac.at/de/informationsgesellschaft/bimentwurf-zur-vorratsdatenspeicherung-begutachtung [= BIM-Entwurf TKG-Novelle 2010] (13.10.2011).

Bundeskanzleramt Österreich, Österreichisches Informationssicherheitshandbuch, https://www.sicherheitshandbuch.gv.at/index.php?view=browse&chapter=712000&uid=712000&section=&topic=&noscroll=true (13.10.2011).

Deutscher Arbeitskreis Vorratsdaten: http://www.vorratsdatenspeicherung.de (13.10.2011).

Epping, Volker /Hillgruber, Christian, Beck'scher Onlinekommentar GG, Stand: 1.07.2011 Edition: 11, www.beck-online.de (13.10.2011).

Europarat, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, 28.1.1981., SEV Nr. 108, abrufbar auf der Web-Seite des Europarat-Vertragsdienstes unter http://conventions.coe.int/Treaty/ger/Treaties/Html/108.htm (13.10.2011).

European Telecommunications Standards Institute (ETSI), http://www.etsi.org/WebSite/AboutETSI/AboutEtsi.aspx (13.10.2011).

EU Kommission, Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24/EG), http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_de.pdf (13.10.2011).

European Digital Rigts (EDRi), „Schattenbericht" zur Evaluierung der Richtlinie zur Vorratsdatenspeicherung, http://www.edri.org/files/shadow_drd_report_110417.pdf (13.10.2011).

Internet Service Providers Austria (ISPA), Stellungnahme betreffend die Verordnung der Bundesministerin für Verkehr, Innovation und Technologie betreffend die Datensicherheit (Datensicherheitsverordnung TKG-DSVO), http://www.ispa.at/stellungnahmen/bmvit-konsultation-datensicherheitsverordung/ (13.10.2011).

Lehofer, Hans Peter, Aktives Abwarten? Vorratsdatenspeicherung in Österreich nach EuGH-Urteil und neuem Entwurf, Web-Blog des Autors unter http://blog.lehofer.at/2010/08/aktives-abwarten-vorratsdatenspeicherun.html (13.10.2011).

Microsoft online-Journal TechNet, http://technet.microsoft.com/de-de (13.10.2011).

Möchel, Erich, Präsentation zum Vortrag über die Vorratsdatenspeicherung und zur ETSI-Schnittstelle ETSI ES 201 671, vom 27.11.2008 an der Hochschule München, http://moechel.com/doqs/missbrauchte_vorratsdaten.pdf (13.10.2011).

Österreichischer Arbeitskreis Vorratsdaten: http://www.akvorrat.at/ (13.10.2011).

Portalverbundvereinbarung, pvv 1.0, 21.11.2002, http://reference.e-government.gv.at/AG-IZ-PVV-pvv-1-0-Ergaenze.332.0.html (13.10.2011).

Rechtshistorische Dokumentation österreichischer Verfassungsentwürfe: http://www.verfassungen.de/at/verfassungsentwurf49-i.htm, (13.10.2011).

Schmidbauer, Franz: http://www.internet4jurists.at/glossar/glossar.htm (13.10.2011).

Tschohl, Christof (2011), Studie zur Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung in Österreich, Wien 14.07.2011, http://bim.lbg.ac.at/de/digital-rights/studie-zur-datensicherheit-umsetzung-vorratsdatenspeicherung (10.10.2011) [= BIM-Datensicherheitsstudie].

Tschohl, Christof, Stellungnahme des BIM zur TKG-Novelle 2010 im Rahmen des parlamentarischen Begutachtungsverfahrens, 15.1.2010, http://www.parlinkom.gv.at/PG/DE/XXIV/ME/ME_00117_B9/pmh.shtml (13.10.2011).

Zentrum für sichere Informationstechnologie Austria (A-SIT), http://www.a-sit.at (13.10.2011).

V.4 Parlamentarische Materialien:

Begutachtungsentwurf des Bundesministeriums für Verkehr, Innovation und Technologie (BMVIT), ausgearbeitet vom Ludwig Boltzmann Institut für Menschenrechte (BIM) im Auftrag des BMVIT, von 15.11.2009 bis 15.1.2010 in öffentlicher Begutachtung: <http://www.parlinkom.gv.at/PG/DE/XXIV/ME/ME_00117/pmh.shtml> (13.10.2011) [entspricht inhaltlich dem BIM-Entwurf TKG Novelle 2010, aber in anderer Form aufbereitet, insbesondere durch Trennung von Gesetzestext und Erläuterungen in verschiedene Dokumente].

Regierungsvorlage zur TKG Novelle zur Umsetzung der Vorratsdatenspeicherungsrichtlinie 2006/24/EG (TKG-Novelle 2010), BlgNR 1074, XXIV GP, http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01074/index.shtml (13.10.2011).

Regierungsvorlage zu den Änderungen der Strafprozessordnung 1975 (StPO) und des Sicherheitspolizeigesetzes (SPG) im Rahmen der Umsetzung der Vorratsdatenspeicherungsrichtlinie 2006/24/EG, BlgNR 1075, XXIV GP, http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01075/ (13.10.2011).

V.5 RECHTSPRECHUNG:

OGH 13.4.2011, 15 Os 172/10y, EvBl 2011/62

OGH 19. 10. 2010, 14 Os 105/10p

OGH 15. 06. 2010, Gz 14 Os 64/10h

OGH 12. 08. 2010, Gz 12 Os 28/10z

OGH 14.7.2009, 4 Ob 41/09x

OGH 26.03.2009, 12Os2/09z

OLG Linz 23.2.2005, 9Bs35/05v

OGH 26.7.2005, 11 Os 57/05Z, JBl 2006, 130

OGH 1.10.2002, 11 Os 64/02.

OGH 17.6.1998, 13 Os 68/98, EvBl 1998/191

OGH 14. 12. 1998, Gz 18Bs272/98

OGH 6.12.1995, 13 Os 161/95, JBl 1997, 260

OGH 09.06.1992, 1Ob16/92

EuGH 29.1.2007, C-275/06.

VfGH 16.12.2010, G259/09 ua.

VfGH 1.7.2009, G 31/08

VfGH 1. 7.2009, G 147, 148/08

VfGH 23.01.2004, G 363/02 VfSlg 17.102/2004

VfGH 14.10.1993, B 1633/92, VfSlg 13.587/1993

BVerfG, 1 BvR 256_08 vom 02.03.2010, http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html (13.10.2011), [VDS Urteil des BVerfG].

BVerfG, 2 BvR 902/06 vom 16.6.2009, http://www.bverfg.de/entscheidungen/rs20090616_2bvr090206.html (13.10.2011).

EGMR Urteil Amann gg. die Schweiz, Appl. 27798/95 vom 16.02.2000 (ÖJZ 2001, S. 71 ff).

EGMR Urteil Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien, Appl. 62540/00 vom 28.6.2007.

EGMR Urteil Valenzuela Contreras gg. Spanien, Reports 1998-V, Abs. 47 vom 30.07.1998.

EGMR Urteil Copland gg. das Vereinigte Königreich, Appl. 62617/00 vom 03.07.2007 (EuGRZ 2007, S. 415 ff).

EGMR Urteil Craxi gg. Italien, Appl. 25337/94 vom 17.07.2003.

EGMR Urteil Halford gg. das Vereinigte Königreich, Appl. 20605/92 vom 25.06.1997 (ÖJZ 1998, S. 311 ff).

EGMR Urteil Huvig gg. Frankreich, Appl. 11105/84 vom 24.04.1990

EGMR Urteil Klass u.a. gg. Deutschland, Appl. 5029/71 vom 06.09.1978 (NJW 1979 S. 1755 ff)

EGMR Urteil Khan gg. das Vereinigte Königreich, Appl. 35394/97 vom 12.05.2000 (JZ 2000, S. 993 ff).

EGMR Urteil Kopp gg. die Schweiz, Appl. 23224/94 vom 25.03.1998 (ÖJZ 1999 S. 115 ff).

EGMR Urteil Kruslin gg. Frankreich, Appl. 11801/85 vom 24.04.1990.

EGMR Urteil Lambert gg. Frankreich, Reports 1998-V, §§ 15, 28 vom 24.08.1998 (ÖJZ 1999 S. 570 ff)

EGMR Urteil Leander gg. Schweden, Appl. 9248/81 vom 26.03.1987.

EGMR Urteil Malone gg. das Vereinigte Königreich, Appl. 8691/79 vom 02.08.1984 (EuGRZ 1985 S. 17 ff).

EGMR Urteil Niemietz gg. Deutschland, Appl. 13710/88 vom 16.12.1992 (NJW 1993 S. 718).

EGMR Urteil Rotaru gg. Rumänien, Appl. 28341/95 vom 04.05.2000 (ÖJZ 2001, S. 74 ff).

EGMR Urteil Silver gg. das Vereinigte Königreich, Ser. A Nr. 61 § 84 vom 25.03.1983. (EuGRZ 1984, S. 147 ff).

EGMR Urteil Taylor–Sabori gg. das Vereinigte Königreich, Appl. 47114/99 vom 22.10.2002.

ff).

EGMR Urteil Weber und Saravia gg. Deutschland, Appl. 54934/00 vom 29.06.2006 (NJW 2007, S. 1433 ff).

EGMR Urteil W. gg. das Vereinigte Königreich, Appl. 9348/81 vom 28.02.1983.

VI ABKÜRZUNGSVERZEICHNIS

1. BVRBG	Erstes Bundesverfassungsrechtsbereinigungsgesetz BGBl I 2008/2
Abl	Amtsblatt der Europäischen Union
Abs	Absatz
Anbieter	Anbieter von öffentlichen Kommunikationsdiensten, die iSd § 102a TKG zur Vorratsspeicherung von Kommunikationsdaten verpflichtet sind.
AnwZert ITR	AnwaltZertifikatOnline IT-Recht
Art	Artikel
Bd	Band
BGBl	Bundesgesetzblatt
BIM	Ludwig Boltzmann Institut für Menschenrechte
BKA	Bundeskriminalamt
BlgNR	Beilage zu den stenographischen Protokollen des Nationalrates
BM.I	Bundesministeriums für Inneres
BMJ	Bundesministerium für Justiz
BMVIT	Bundesministerium für Verkehr Innovation und Technologie
BVerfG	Bundesverfassungsgericht (Deutschland)
BVerfGE	Entscheidungen des Bundesverfassungsgerichts, amtliche Sammlung (Deutschland)
B-VG	Bundes-Verfassungsgesetz BGBl 1930/1 zuletzt idF BGBl I 2010/15
BVT	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
CSV	Comma-Separated Values
dBGBl	deutsches Bundesgesetzblatt
DLS	Durchlaufstelle
dRGBl	deutsches Reichsgesetzblatt
DSG	Datenschutzgesetz 2000 BGBl I 1999/165 zuletzt idF BGBl I 2009/135
DSK	Datenschutzkommission
dStPO	deutsche Strafprozeßordnung dRGBl 1877, S. 253 zuletzt idF dBGBl. I 2011

	S. 1266, 1269
DSVO	Datensicherheitsverordnung gemäß §§ 94 Abs. 4 und 102c TKG
dTKG	deutsches Telekommunikationsgesetz dBGBl I 1996, S. 1120 zuletzt idF dBGBl I 2011, S. 506, 509 f.
DuD	Datenschutz und Datensicherheit
DVBl	Deutsches Verwaltungsblatt
EBRV	erläuternde Bemerkungen zur Regierungsvorlage
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention BGBl 1958/210 zuletzt idF BGBl III 2002/79
etc	etcetera
EuGH	Europäischer Gerichtshof
EUV	Vertrag über die Europäische Union Abl 1997 C 340/1 (BGBl III 1999/85) zuletzt idF Abl 2009 C 290/1
GG	Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949 (dBGBl 1949, S.1), zuletzt idF dBGBl I 2010, S. 944
GRC	Charta der Grundrechte der Europäischen Union Abl 2000 C 364/1 zuletzt idF Abl 2007 303/1
HSM	hardware security modules
idF	in der Fassung
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
insb	insbesondere
IP	Internet Protokoll
iSd	im Sinne des (in Verbindung mit einer zitierten Rechtsnorm)
iVm	in Verbindung mit
JBl	Justizblatt
KommAustria-G	KommAustria-Gesetz BGBl. I Nr. 32/2001 zuletzt idF BGBl. I Nr. 111/2010
LKA	Landeskriminalamt
NJW	Neue Juristische Wochenschrift

NVwZ	Neue Zeitschrift für Verwaltungsrecht
OGH	Oberster Gerichtshof
ÖJZ	Österreichische Juristenzeitung
OLG	Oberlandesgericht
PI	Polizeiinspektion
PIN	Personal Identification Number
PUK	PIN Unlock Key
RGBl	Reichsgesetzblatt
RL	Richtlinie
Rn	Randnummer
Rz	Randziffer
S	Seite
SMTP	Simple Mail Transfer Protocol
SPG	Sicherheitspolizeigesetz BGBl 1991/566 zuletzt idF BGBl I 2009/131
StGG	Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger für die im Reichsrate vertretenen Königreiche und Länder RGBl 132 idF BGBl 1920/1 (BVG), zuletzt idF BGBl 1988/684
StPO	Strafprozeßordnung 1975 BGBl 631 zuletzt idF BGBl I 2011/67
TKG	Telekommunikationsgesetz 2003 BgBl I 70 zuletzt idF BGBl I 2009/65
UrHRG	Urheberrechtsgesetz
usw	und so weiter
vgl	vergleiche
WKO	Wirtschaftskammer Österreich
Z	Ziffer
ZJS	Zeitschrift für das Juristische Studium
ECG	E-Commerce-Gesetz BGBl. I Nr. 152/2001

ANHANG A) BEGUTACHTUNGSENTWURF DES BMVIT FÜR EINE DATENSICHERHEITSVERORDNUNG GEM. §§ 94 (4) UND 102C TKG (DSVO)

Vorblatt

Probleme und Ziele:

Mit § 94 Abs. 4 Telekommunikationsgesetz 2003 (TKG 2003) wird der Bundesminister für Verkehr, Innovation und Technologie ermächtigt, die näheren Bestimmungen zur einheitlichen Definition der Syntax, der Datenfelder und der Verschlüsslung, zur Speicherung und Übermittlung der Daten sowie die näheren Bestimmungen betreffend die Speicherung der gemäß § 102c angefertigten Protokolle festzusetzen.

Mit § 102c TKG 2003 wird der Bundesminister für Verkehr, Innovation und Technologie ermächtigt, eine nähere Beschreibung des Sorgfaltsmaßstabs zur Gewährleistung der Datensicherheit festschreiben.

Von diesen beiden Verordnungsermächtigungen soll nun Gebrauch gemacht und mit der vorliegenden Verordnung die Bestimmungen festgesetzt werden, die einerseits als Grundlage zur Einrichtung einer Durchlaufstelle (DLS) dienen und deren Aufgaben und deren Funktionsweise beschreiben sowie andererseits den von Anbietern von Kommunikationsdiensten einzuhaltenden Sicherheitsmaßstab regeln.

Die Grundlagen für diese Verordnung bilden die Studie zur „Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung", welche das Ludwig Boltzmann Institut für Menschenrechte (BIM) im Auftrag des BMVIT ausgearbeitet hat, sowie die Diskussionen der insgesamt 6 Round Table Veranstaltungen des BIM im ersten Halbjahr 2011 zur Entwicklung der Schnittstellenbeschreibung und eines sicheren Systems der Datenübermittlung.

Inhalt:

- Konkretisierung der Datensicherheitsmaßnahmen innerhalb des Betriebs von Anbietern
- Konkretisierung der Datensicherheitsmaßnahmen bei Übermittlung der Daten
- Darstellung der Grundstruktur und der Funktionen der Durchlaufstelle (DLS)
- Einrichtung und Betrieb der DLS
- Auditierung der DLS-Funktionen
- Einbindung in den Portalverbund
- Erstellung der und Zugang zur Zugriffsstatistik

Alternativen:

Keine.

Auswirkungen des Regelungsvorhabens:

– Finanzielle Auswirkungen:

Für die Erfassung der Kosten der DLS ist zunächst von Bedeutung, dass die DLS einen Teil der Umsetzung der Richtlinie zur Vorratsdatenspeicherung 2006/24/EG darstellt, weil die besonderen Anforderungen an die Datensicherheit ihre Grundlage in Art 7 Lit. c) dieser Richtlinie haben: „in Bezug auf die Daten werden geeignete technische und organisatorische Maßnahmen getroffen, um sicherzustellen, dass der Zugang zu den Daten ausschließlich besonders ermächtigten Personen vorbehalten ist." Denselben Standard auf die Abwicklung aller Datenauskünfte (auch Daten, die zu Verrechnungszwecken vorhanden sind, nicht nur „Vorratsdaten") anzuwenden ist dabei nicht nur konsequent sondern auch aus rein praktischen Gründen notwendig. Viele Auskünfte werden nämlich künftig wohl „gemischte" Datensätze enthalten, also in derselben Auskunft Vorratsdaten und Betriebsdaten. Diese Annahme ist deshalb wesentlich, weil es bzgl. der Vorratsdatenspeicherung in der Regierungsvorlage zum TKG 2003 klare Regeln zur Kostentragung gibt. Der initiale Investitionsaufwand (Investitionskosten) zur Schaffung der für die Umsetzung der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung notwendigen Infrastruktur wird für die gesamte österreichische Telekommunikationsbranche geschätzte 15 Millionen Euro betragen und wird gem. § 94 Abs. 1 TKG 2003 zu 80% vom Bund ersetzt. Dafür ist ein Aufteilungsschlüssel zwischen den Ministerien (BMVIT, BMI und BMJ) vorgesehen. Bei der Verabschiedung der gemeinsamen Regierungsvorlage zur TKG-Novelle wurde nämlich eine Vereinbarung zur Aufteilung dieser Kosten auf die Ministerien BMI (34%), BMJ (Fixbetrag von Euro 360.000,--) und BMVIT (63%) getroffen.

Die Einrichtungskosten der DLS für die Umsetzung der Vorratsdatenspeicherung fallen zwar direkt beim Bund an, stehen aber in unmittelbarem Zusammenhang zu den Investitionskosten der Anbieter, da im Gegensatz zu einer dezentralen S/MIME, wo die Kosten direkt bei den Anbietern anfielen und dem Investitionskostenersatz nach § 94 abs. 1 TKG 2003 unterlägen, wesentlich günstiger sind.

Die Bundesrechenzentrum GmbH (BRZ) schätzt die Investitionskosten auf knapp unter 500.000,- Euro, die monatlichen Betriebskosten wurden mit 7.000,- Euro beziffert. Die Schätzung ist vorsichtig angelegt, damit nicht zu befürchten ist, dass sich im Falle einer tatsächlichen Umsetzung die Kosten dann als deutlich höher erweisen.

Dieser Kostenschätzung liegen folgende Annahmen zugrunde:

Authentifizierung mittels qualifizierter Signatur

Nutzung vorhandener Infrastruktur des BRZ (bestehende Serversysteme)

Maximale Größe der zu übermittelnden Daten 15 MB

Die Schätzung enthält ein Portal für Netzbetreiber ähnlich dem Portalverbund.

Die Funktion eines Help-desk ist nicht enthalten.

Aufwendungen für erhöhte Sicherheit sind in der Kostenschätzung nicht enthalten.

Die Kosten für die Auditierung der tatsächlichen Umsetzung durch die BRZ, die durch einen Dienstleister erfolgen muss, werden auf 49.500,- Euro geschätzt.

Die durch die Einrichtung der DLS verursachten Investitionskosten für den Bund in Höhe von rund 500.000,-- Euro, die beispielsweise bei der verschlüsselten Übermittlung per E-Mail (ursprünglich im Begutachtungsentwurf zur TKG-Novelle vorgesehenes „S/MIME Konzept") nicht anfallen, sind in die Investitionskosten nach § 94 Abs. 1 TKG 2003 einzuberechnen. Die Einrechnung dieser Kosten in die zu 80% zu erstattendenden Investitionskosten der Anbieter ist gerechtfertigt, da bei der Implementierung eines dezentralen S/MIME Konzepts die Anbieter (nach Angaben der RTR sind dzt. ca 200 Anbieter gemäß § 102a TKG 2003 speicherpflichtig) und mindestens 15 anfrageberechtigte Stellen auf Seiten der Sicherheitsbehörden dezentral sichere Wege zur Datenübermittlung und zur Authentifizierung schaffen müssten. Das würde erfordern, dass die technische Implementierung mit allen Anbietern einzeln definiert und implementiert werden müsste. Allein der dezentrale Austausch der Sicherheits-Zertifikate würde dabei schon einen beträchtlichen Aufwand verursachen. Demgegenüber muss die Spezifikation zur DLS nur einmal ausgearbeitet werden (unter Beteiligung der Telekom Branche, die dabei teilweise auch über die Interessenvertretungen erfolgt und nicht für alle - vor allem kleinere - Anbieter unmittelbar Aufwand verursacht). Die zentrale Architektur und vor allem die zentrale Hinterlegung der „publickeys" vereinfachen diese Prozesse enorm. Der einzelne Anbieter benötigt für die Abwicklung nur noch einen herkömmlichen Internet-Browser für eine sicher Verbindung (per https) zur Durchlaufstelle.

Der Entwicklungsaufwand für die Spezifikation der Schnittstelle stellt bei den Anbietern Investitionskosten dar, die im Sinne des § 94 Abs. 1 TKG dem Investitionskostenersatz unterliegen. Der Aufwand für die Spezifikation der Schnittstelle eines dezentralen S/MIME Konzepts wäre deutlich höher als jener einer zentralen DLS. Unter der Annahme, dass der Aufwand für die Spezifikation eines dezentralen Konzepts auf Seiten aller Anbieter insgesamt Kosten in Höhe von 625.000,- Euro verursacht (wovon 80% - also 500.000,- Euro - vom Bund zu erstatten wären), ist die DLS auch vom Investitionskostenaufwand her günstiger als eine verschlüsselte Übermittlung per E-Mail. Bei 200 Anbietern wird diese Schwelle erreicht, wenn im Durchschnitt Mehrkosten in Höhe von 3.125,- Euro pro Anbieter entstehen. Bei marktüblichen Stundensätzen für qualifizierte IT Techniker würde diese Schwelle wohl erheblich überschritten werden, weil ein durchschnittlicher Mehraufwand von zwei bis drei Arbeitstagen pro Unternehmen selbst bei vorsichtiger Schätzung von allen Beteiligten als realistisch bezeichnet wurde.

Die Implementierungskosten der DLS sind sachlich von dem mit etwa 15.000.000 Euro bezifferten Budgetvolumen erfasst, die der Bund für die Investitionskosten zur Umsetzung der Vorratsdatenspeicherung veranschlagt hat. Die Implementierung der DLS bedeutet auf Seiten der Sicherheitsbehörden eine Effizienzerhöhung und damit eine deutliche Kostenersparnis. Der geringere Aufwand für die Spezifikation der Schnittstelle bei der zentralen DLS Lösung wird dabei vor allem beim Innenministerium / Bundeskriminalamt spürbar sein, wo die faktische Abwicklung der Auskunftsvorgänge implementiert werden muss. Dementsprechend ist - in der Relation der Investitionskosten der DLS zu den Investitionskosten der Anbieter - auch hier eine Kostenteilung zwischen den Ressorts sachgerecht.

Am stärksten spürbar sein wird die Erleichterung für die Sicherheitsbehörden im operativen Betrieb. Durch stärkere Automatisierung und die zentrale Kommunikation über die DLS wird bei den Auskunftsbegehren von Seiten des Bundeskriminalamts eine Aufwandsersparnis erwartet. Die größte Aufwandsreduzierung besteht vor allem darin, dass im Vergleich zum dezentralen S/MIMe Konzept die laufende Erneuerung der Sicherheitszertifikate zentral erfolgt und damit massiv erleichtert wird. Die Erfahrung aus der Europol Kooperation zeigt, dass dies bei einer dezentralen sicheren Kommunikation

zwischen vielen Stellen ein enormer Aufwands- und damit Kostensteigerungsfaktor ist. Eine unverbindliche Einschätzung seitens der IT-Abteilung des BMI geht davon aus, dass die „S/MIME Variante" hier einen Mehraufwand im Ausmaß einer vollen Planstelle bedeuten würde. Stellt man dem die geschätzten laufenden monatlichen Kosten der DLS in Höhe von rund 7.000,- Euro entgegen, zeigt sich auch für den operativen Betrieb die DLS als die kostengünstigere Variante.

Die Bedeckung der laufenden Kosten (Betriebskosten) der DLS erfolgt aus vorhandenen Budgetmitteln der beteiligten Ressorts. Die Aufteilung der laufenden Kosten bleibt einer interministeriellen Vereinbarung vorbehalten.

– Wirtschaftspolitische Auswirkungen:

– – Auswirkungen auf die Beschäftigung und den Wirtschaftsstandort Österreich:

Keine.

– – Auswirkungen auf die VerwaltungskostenfürBürger/innen und für Unternehmen:

Für Bürger/innen fallen keine Kosten an.

Die sich durch die Einführung der Verpflichtung zur Vorratsdatenspeicherung für Unternehmen ergebenden Kosten wurden bereits im Vorblatt zur Novelle des TKG 2003, BGBl. I Nr. 27/2011 (1074 der Beilagen XXIV. GP) dargelegt. Es darf hierauf verwiesen werden.

– Auswirkungen in umweltpolitischer Hinsicht, insbesondere Klimaverträglichkeit:

Es sind keine umweltpolitischen Auswirkungen zu erwarten.

Das Regelungsvorhaben ist nicht klimarelevant.

– Auswirkungen in konsumentenschutzpolitischer sowie sozialer Hinsicht:

Es sind weder konsumentenschutzpolitische noch soziale Auswirkungen zu erwarten.

– Geschlechtsspezifische Auswirkungen:

Genderspezifische Auswirkungen sind nach dem Inhalt des vorliegenden Entwurfes nicht zu erwarten, da die Normadressaten ausschließlich Unternehmen und Behörden sind.

Verhältnis zu Rechtsvorschriften der Europäischen Union:

Gegeben. Der Entwurf dient stellenweise der Umsetzung von Gemeinschaftsrecht. Die darüber hinaus vorgesehenen Regelungen fallen nicht in den Anwendungsbereich des Rechts der Europäischen Union.

Entwurf

Verordnung des Bundesministers für Verkehr, Innovation und Technologie betreffend die Datensicherheit (Datensicherheitsverordnung TKG-DSVO)

Auf Grund der §§ 94 Abs. 4 und 102c des Bundesgesetzes, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003-TKG 2003), BGBl. I Nr. 70/2003, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 27/2011, wird, hinsichtlich der §§ 1 bis 4 und 8 bis 25 im Einvernehmen mit dem Bundesministerium für Inneres und dem Bundesministerium für Justiz, verordnet:

1. Abschnitt

Allgemeines

Gegenstand und Anwendungsbereich

§ 1. (1) In dieser Verordnung werden die näheren Bestimmungen

1. des Formats, der Datenfelder und der Syntax der CSV-Datei bei der Übermittlung von Auskünften über Verkehrsdaten (§ 99 Abs. 5 TKG 2003) und Vorratsdaten (§ 102b TKG2003),
2. zur Datensicherheit und zur Protokollierung bei der Übermittlung der in Z 1 genannten Auskünfte sowie
3. zur Datensicherheit bei der Speicherung und der Zugriffsprotokollierung von Vorratsdaten

getroffen

(2) Der Anwendungsbereich dieser Verordnung erstreckt sich auf die Verwendung von Verkehrsdaten, Zugangsdaten und Standortdaten sowie Stammdaten, soweit diese in Verbindung mit den eben genannten Datenkategorien verarbeitet werden.

Begriffsbestimmungen

§ 2. (1) Verkehrsdaten, Zugangsdaten und Standortdaten sowie – soweit sie in Verbindung mit den zuvor genannten Datenkategorien verarbeitet werden - Stammdaten werden bezeichnet als

1. „Betriebsdaten", soweit diese für den Anbieter für die in § 99 Abs. 2 und 3 TKG 2003 erfassten Zwecke notwendig sind;
2. „Vorratsdaten", soweit diese vom Anbieter ausschließlich aufgrund der Verpflichtung gemäß § 102a TKG 2003 für die in § 102b TKG 2003 genannten Zwecke vorrätig gespeichert werden (§ 92 Abs. 3 Z 6b TKG 2003).

(2) In dieser Verordnung bezeichnet der Begriff

1. „Anbieter" Betreiber von öffentlichen Kommunikationsdiensten,
2. „Vorratsdatenbank" eine Datenbank zur Speicherung von Vorratsdaten.

Ausnahmen

§ 3. (1) Die Bestimmungen des 3. Abschnittes sind nicht anzuwenden

1. in den Fällen des § 98 TKG 2003,
2. bei Gefahr in Verzug in den Fällen des § 99 Abs. 5 Z 3 und 4 TKG 2003,
3. bei der Feststellung des aktuellen Standortes gemäß §§ 134 ff der Strafprozessordnung 1975 (StPO), BGBl. Nr. 631 in der Fassung BGBl. I Nr. 33/2011, und

4. bei der Übermittlung von begleitenden Rufdaten im Rahmen einer Überwachung von Nachrichten.

(2) Anfragen über Verkehrsdaten, Standortdaten und Stammdaten, deren Beantwortung die Verarbeitung von Verkehrsdaten erfordert, einschließlich Anfragen über Vorratsdaten, deren Beantwortung gemäß gesetzlicher Bestimmungen vorab mündlich erfolgen können, müssen mit Ausnahme der Anfragen gemäß § 98 TKG 2003 über die Durchlaufstelle (§ 9) nachgereicht und dokumentiert werden.

Datensicherheitsmaßstab

§ 4. (1) Der Sicherheitsmaßstab bei der Verwendung von Daten im Sinne des § 2 Abs. 1 hat den Vorgaben des § 95 TKG 2003 zu entsprechen.

(2) Bei Verwendung von Vorratsdaten gelten in Ausführung des § 102 Abs. 1 TKG 2003 über Abs. 1 hinaus die im 2. Abschnitt dieser Verordnung ausdrücklich geregelten besonderen Vorschriften für einen erhöhten Sicherheitsmaßstab.

2. Abschnitt

Datensicherheit beim Anbieter innerhalb des Betriebes

Geeignete technische und organisatorische Maßnahmen zur Sicherheit von Vorratsdaten

§ 5. (1) Vorratsdaten müssen vom Anbieter auf eine Weise gespeichert werden, dass deren logische Unterscheidung von Betriebsdaten bei jedem Zugriff und jeder Verwendung eindeutig ist.

(2) Eine physikalisch getrennte Datenspeicherung von Betriebsdaten und Vorratsdaten ist nicht notwendig. Der Anbieter hat durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass die Vorratsdatenbank auf eine Weise ausgestaltet ist, dass Zugriffe auf Vorratsdaten nur unter Einhaltung der besonderen Sicherheitsvorschriften gemäß § 7 möglich sind.

(3) Wenn keine betriebliche Rechtfertigung zur Speicherung als Betriebsdaten mehr vorliegt, sind diese Daten umgehend aus den betrieblichen Datenbanken zu löschen und in die Vorratsdatenbank zu überführen. Sollte die Speicherung in der Vorratsdatenbank bereits zuvor gemäß § 6 erfolgt sein, so ist die Kennzeichnung der gleichzeitigen betrieblichen Speicherung zeitgleich oder unmittelbar nach der Löschung aus den betrieblichen Datenbanken zu entfernen.

(4) Der Anbieter hat die Methode zur technischen und organisatorischen Trennung nachvollziehbar zu dokumentieren und diese Dokumentation für den Fall einer Prüfung durch die Datenschutzkommission gemäß § 102c Abs. 1 TKG 2003 auf Anfrage der Datenschutzkommission zugänglich zu machen.

(5) Der Anbieter hat die tatsächliche Speicherdauer von Betriebsdaten sowie allfällige diesbezügliche interne Richtlinien für den Fall einer Prüfung durch die Datenschutzkommission gemäß § 102c Abs. 1 TKG 2003 oder auf Anfrage der Datenschutzkommission zu beauskunften.

Unterscheidung von Betriebsdaten und Vorratsdaten

§ 6. (1) Eine Anordnung der Staatsanwaltschaft gemäß § 135 Abs. 2a StPO zur Auskunft über Vorratsdaten berechtigt den Anbieter in jedem Fall zur Erfüllung seiner Auskunftsverpflichtung auch Betriebsdaten zu verarbeiten und zu übermitteln. Die Verpflichtung zur Protokollierung gemäß § 7 Abs. 3 besteht nur dann, wenn der Anbieter zur Erfüllung der Auskunftsverpflichtung tatsächlich eine Abfrage in der Vorratsdatenbank durchführen muss.

(2) Wenn eine Auskunft Vorratsdaten enthält, hat der Anbieter diesen Umstand als Zusatzinformation gemäß der Schnittstellenspezifikation in der Anlage (Kapitel 1.4) zu übermitteln.

(3) Zur Vereinfachung des operativen Betriebes im Hinblick auf Datenauskünfte gemäß § 99 Abs. 5 TKG 2003 oder § 102b TKG 2003 darf der Anbieter die in § 2 Abs. 1 genannten Daten auch dann bereits in der Vorratsdatenbank speichern, wenn diese Daten zugleich noch als Betriebsdaten gespeichert sind. In diesem Fall ist in der Vorratsdatenbank für jede Datenkategorie kenntlich zu machen, dass diese Daten auch in den betrieblich notwendigen Datenbanken des Anbieters vorhanden sind.

Revisionssichere Protokollierung und Vier-Augen-Prinzip bei Zugriffen auf Vorratsdaten

§ 7. (1) Der Anbieter hat seine Systeme auf technischer und organisatorischer Ebene so auszugestalten, dass Zugriffe auf Vorratsdaten nur durch besonders ermächtigte Mitarbeiter unter Einhaltung des Vier-Augen-Prinzips möglich sind. Jeder Zugriff auf Vorratsdaten muss durch zwei Personen mit einer besonderen Ermächtigung hierfür autorisiert sein. Die Autorisierung durch die zweite Person kann auch zeitnah zum Zugriff durch die erste Person nachträglich erfolgen, wenn dabei die effektive Wahrung des Vier-Augen-Prinzips sichergestellt ist.

(2) Zugriffe auf Vorratsdaten müssen beim Anbieter so protokolliert werden, dass die Protokolldaten vor Veränderung und Verfälschung geschützt sind und die Vollständigkeit, die Ordnungsmäßigkeit, die Sicherung vor Verlust, die Einhaltung der Aufbewahrungsfristen sowie die Dokumentation, Nachvollziehbarkeit und Prüfbarkeit des Verfahrens gewahrt sind.

(3) Die Protokollierung umfasst

1. die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Referenz zur staatsanwaltschaftlichen oder gerichtlichen Anordnung gemäß den Bestimmungen der StPO, die der Übermittlung der Daten zugrunde liegt,
2. in den Fällen des § 99 Abs. 5 Z 3 und 4 TKG 2003 die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Aktenzahl der Sicherheitsbehörde,
3. das Datum der Anfrage (Zustellung in das Postfach des Anbieters in der Durchlaufstelle gemäß § 18 Abs. 1) sowie das Datum und den genauen Zeitpunkt der erteilten Auskunft (Zustellung der Antwort in das Postfach der Behörde in der Durchlaufstelle gemäß § 18 Abs. 3), wobei diese Daten von der Durchlaufstelle als Zusatzinformation an den Anbieter zu übermitteln sind,
4. die nach dem Datum des Beginns des Kommunikationsvorganges und den Kategorien gemäß § 102a Abs. 2 bis 4 TKG 2003 (Einteilung der Kategorien gemäß der Anlage, Kapitel 1.1.2) aufgeschlüsselte Anzahl der übermittelten Datensätze,
5. die Speicherdauer der übermittelten Daten ab dem Datum, seit dem die Daten als Betriebsdaten (§ 2 Abs. 2 Z 1) und als Vorratsdaten gemäß § 2 Abs. 2 Z 2 gespeichert wurden, zum Zeitpunkt der Anordnung der Auskunft (Datum der staatsanwaltschaftlichen Anordnung gemäß § 138 Abs. 3 StPO oder Datum der Anfrage nach § 53 des Sicherheitspolizeigesetzes – SPG, BGBl. Nr. 566/1991 in der Fassung BGBl. I Nr. 33/2011),
6. den Namen und die Anschrift des von der Auskunft über Vorratsdaten betroffenen Teilnehmers, soweit der Anbieter über diese Daten verfügt,
7. eine eindeutige Kennung, welche eine Zuordnung der Personen ermöglicht, die im Unternehmen des Anbieters auf Vorratsdaten zugegriffen haben sowie
8. im Fall von Auskünften über Vorratsdaten (§ 135 Abs. 2a StPO) die der Anordnung zu Grunde liegende strafbare Handlung.

3. Abschnitt

Datensicherheit bei der Übermittlung von betriebsnotwendigen Verkehrs- und Standortdaten und Vorratsdaten zu Auskunftszwecken an Strafverfolgungs- und Sicherheitsbehörden

Allgemeines

§ 8. (1) Die Übermittlung der Daten erfolgt über eine zentrale Durchlaufstelle, die das Bundesministerium für Verkehr, Innovation und Technologie bei der Bundesrechenzentrum GmbH einzurichten hat.

(2) Die technische Spezifikation zur Durchlaufstelle hat einen verschlüsselten Übertragungsweg vorzusehen (Transportverschlüsselung).

(3) Zusätzlich ist eine Verschlüsselung der Inhalte sowohl der Anfrage als auch der Beantwortung von Absender zu Empfänger durch asymmetrische Verschlüsselungsverfahren vorzusehen (Inhaltsverschlüsselung). Asymmetrische Verschlüsselungsverfahren können als hybride Verfahren implementiert werden.

(4) Über die Durchlaufstelle werden die Teilnehmer des Datenaustausches über eine fortgeschrittene elektronische Signatur identifiziert und authentifiziert.

Durchlaufstelle – Grundstruktur

§ 9. (1) Die Durchlaufstelle ist ein elektronisches Postfachsystem zur sicheren Abwicklung von Anfragen und Auskünften im Sinne des § 94 Abs. 4 TKG 2003. Alle Beteiligten sind dabei über einen verschlüsselten Übertragungskanal an die Durchlaufstelle angebunden.

(2) Die Durchlaufstelle ist auf eine Weise einzurichten, dass für die Bundesrechenzentrum GmbH als Dienstleister der Durchlaufstelle im Sinn des DSG 2000 ein Zugang zu personenbezogenen Inhalten von Anfragen zu Datenauskünften so wie von deren Beantwortung nicht möglich ist.

(3) Über die Durchlaufstelle werden sowohl Auskünfte über Vorratsdaten als auch Auskünfte über Betriebsdaten abgewickelt. Ausnahmen sind nur in dem von § 3 normierten Ausmaß zulässig. Über die Durchlaufstelle werden alle Auskunftsfälle revisionssicher statistisch erfasst.

(4) In der Spezifikation zur Durchlaufstelle ist vorzusehen, dass die Integrität der Daten sowie die Identität des Senders durch den Empfänger überprüft werden kann (Signatur).

Einrichtung und Betrieb der Durchlaufstelle – Auftraggeber und Durchführung

§ 10. (1) Die Einrichtung der Durchlaufstelle sowie die Zertifikatsverwaltung und die Datensicherheit liegen in der Verantwortung des Bundesministeriums für Verkehr, Innovation und Technologie.

(2) Die Einrichtung, die Zertifikatsverwaltung und der Betrieb der Durchlaufstelle erfolgen durch die Bundesrechenzentrum GmbH. Die Bundesrechenzentrum GmbH ist funktionell Dienstleister im Sinne des § 4 Z 5 DSG 2000 jeweils für den Auftraggeber, für dessen Anwendung Daten an die Durchlaufstelle übergeben oder von der Durchlaufstelle übernommen werden.

(3) Der Bundesminister für Verkehr, Innovation und Technologie kann sich zur Auditierung der tatsächlichen Umsetzung der technischen Spezifikation durch die Bundesrechenzentrum GmbH eines Dienstleisters bedienen.

Auditierung der Durchlaufstellen-Funktionen

§ 11. Der Bundesminister für Verkehr, Innovation und Technologie stellt sicher, dass

1. die tatsächliche Umsetzung der Durchlaufstelle durch die Bundesrechenzentrum GmbH den Spezifikationen zur Durchlaufstelle entspricht,
2. jene Dienste, die von der Durchlaufstelle für die Ausführung in der Client-Software der jeweiligen Benutzer zur Verfügung gestellt werden, für einen Client-Administrator verifizierbar ist (Signatur) und der Schnittstellendefinition zur Durchlaufstelle entspricht,
3. nur eine auditierte schnittstellenkonforme Software der Durchlaufstelle eine richtige Datenübertragung ermöglicht,
4. nur authentifizierte Anwender ihre öffentlichen Schlüssel in der Durchlaufstelle eindeutig zu ihrer jeweiligen Institution zugehörig hinterlegen können und
5. jede Änderung der Durchlaufstelle einer Re-Auditierung zum Zweck der Sicherstellung der Verifizierbarkeit der Echtheit der Software durch die Endnutzer unterliegt.

Funktionen der Durchlaufstelle im Überblick

§ 12. (1) Die Durchlaufstelle stellt für die Abwicklung von Auskünften im Sinne des § 94 Abs. 4 TKG 2003 elektronische Postfächer zur Verfügung, die unter Verwendung eines Webservice oder einer Webapplikation zu benutzen sind.

(2) Allen zur Abwicklung von Auskunftsbegehren ermächtigten Dienststellen auf Seiten der berechtigten Behörden sowie allen nach § 102a TKG 2003 speicherpflichtigen Anbietern wird jeweils eine Teilnehmerkennung und ein dazugehöriges Postfach von der Durchlaufstelle zugewiesen. Jeder Benutzer hat nur Zugriff auf das Postfach jenes Teilnehmers (Dienststelle oder Anbieter), dem der Benutzer zugehört.

(3) Die Authentifizierung der Benutzer erfolgt durch die Durchlaufstelle gemäß den Vorgaben des § 13.

(4) Die Verschlüsselung des Übertragungsweges ist über die Durchlaufstelle unter Verwendung einer geeigneten Technologie entsprechend dem Stand der Technik sicherzustellen.

(5) Zur Verschlüsselung der Anfragen und der Auskünfte verwaltet die Durchlaufstelle die öffentlichen Schlüssel aller ermächtigten Dienststellen und aller gemäß § 102a TKG 2003 speicherpflichtigen Anbieter. Nur authentifizierte Benutzer können den öffentlichen Schlüssel ihrer Organisation bei der Durchlaufstelle hinterlegen. Jeder Benutzer holt vor dem Absenden seiner Nachricht den öffentlichen Schlüssel des Empfängers zur Verschlüsselung des Inhalts bei der Durchlaufstelle ab.

(6) Alle Auskunftsfälle sind in der Durchlaufstelle revisionssicher zu protokollieren. Der Umfang dieser Protokollierung wird in § 23 geregelt.

Authentifizierung – Einbindung über den Portalverbund und Unique-ID

§ 13. (1) Die Durchlaufstelle vergibt zu jeder Anfrage eine einmalige, eindeutig zuordenbare Transaktionsnummer zur Prüfung der Authentizität der Anfrage und zur Nachverfolgung jeder Anfrage sowie deren Beantwortung (Unique-ID). Aus der Transaktionsnummer muss sowohl auf die zugrunde liegende konkrete Anfrage der Behörde als auch auf den angefragten Betreiber geschlossen werden können.

(2) Die Authentifizierung der Benutzer der berechtigten Behörden erfolgt durch das jeweilige Stammportal des Benutzers (Portalverbund).

(3) Für die Authentifizierung der Benutzer auf Seiten der Anbieter ist in der Spezifikation zur Durchlaufstelle ein Stammportal vorzusehen, das der Sicherheitsklasse 3 der Portalverbundvereinbarung entspricht.

Zugangsberechtigte Behörden

§ 14. (1) Das Bundesministerium für Inneres sowie das Bundesministerium für Justiz geben der Bundesrechenzentrum GmbH für die Spezifikation der Durchlaufstelle eine begrenzte Anzahl von Dienststellen bekannt, die als Teilnehmer der Durchlaufstelle zur Abwicklung von Auskunftsbegehren berechtigt sind.

(2) Nachträgliche Änderungen der nach Abs. 1 bekannt gegebenen Dienststellen sind durch das Bundesministerium für Inneres sowie das Bundesministerium für Justiz der Bundesrechenzentrum GmbH für die Veranlassung der entsprechenden Änderungen in der Durchlaufstelle bekannt zu geben.

(3) Für die Datenschutzkommission, den Datenschutzrat und das Bundesministerium für Justiz sowie für die Rechtsschutzbeauftragten beim Bundesminister für Justiz und beim Bundesminister für Inneres ist in der Spezifikation zur Durchlaufstelle jeweils ein Zugang vorzusehen, der entsprechend der jeweiligen Aufgabe dieser Stellen einen Zugang zu den Protokolldaten gemäß § 22 Abs. 4 oder zur Statistik gemäß § 23 Abs. 3 ermöglicht.

Anbindung der Anbieter

§ 15. (1) Die Anbindung an die Durchlaufstelle ist für alle Anbieter verpflichtend, die gemäß § 102a Abs. 6 TKG 2003 zur Vorratsdatenspeicherung verpflichtet sind. Die Erfassung aller speicherpflichtigen Anbieter zur erstmaligen Einrichtung des Stammportals der Anbieter gemäß § 13 Abs. 3 erfolgt durch die Rundfunk und Telekom Regulierungs-GmbH, welche der Bundesrechenzentrum GmbH eine Liste aller erfassten Anbieter zur Importierung und Freigabe zur Verfügung stellt.

(2) Entsteht ein neuer speicherpflichtiger Anbieter oder fällt ein bestehender weg, hat die Rundfunk und Telekom Regulierungs-GmbH alle notwendigen Informationen über diesen Anbieter der Bundesrechenzentrum GmbH für die Freigabe oder zur Deaktivierung der Anbindung an die Durchlaufstelle bekannt zu geben.

Sicherheitsniveau der Anbindung

§ 16. (1) Die Anbindung der Behörden an die Durchlaufstelle hat den Vorgaben der Sicherheitsklasse 3 in der Portalverbundvereinbarung zu entsprechen.

(2) Die Anbindung der Anbieter an die Durchlaufstelle hat den Vorgaben der Sicherheitsstufe 3 aus der Definition der Sicherheitsstufen in der Kommunikation Bürger – Behörde im Bereich E-Government zu entsprechen.

Postfächer und Zustellung

§ 17. (1) Ein Auskunftsbegehren eines berechtigten Benutzers auf Behördenseite wird in das Postfach des über die Durchlaufstelle ausgewählten Anbieters zugestellt. Die Durchlaufstelle ermöglicht die Auswahl mehrerer Anbieter. Die Spezifikation zur Durchlaufstelle hat ein System der Notifikation über den Eingang eines Auskunftsbegehrens in das Postfach des Anbieters vorzusehen. Die Abholung des Auskunftsbegehrens erfolgt manuell durch Zugriff auf das Postfach des Anbieters nach entsprechender Authentifizierung des Benutzers. Eine Abholung des Auskunftsbegehrens per Webservice kann in der Spezifikation zur Durchlaufstelle vorgesehen werden.

(2) In der Spezifikation zur Durchlaufstelle muss sichergestellt werden, dass eine Beantwortung bereits vor der Übermittlung der Anfrage via Durchlaufstelle durchgeführt werden kann. Dazu wird ein anbieterspezifischer Bereich von Referenzen (Unique-ID) definiert, der vom Anbieter in aufsteigender Reihenfolge vergeben wird. Gemäß § 3 Abs. 2 ist die nachträgliche Dokumentation der Anfrage über die Durchlaufstelle zu gewährleisten, wobei die Behörde die anbieterspezifische Referenz anzugeben hat, die bei der Beantwortung verwendet wurde.

(3) Die Beantwortung eines Auskunftsbegehrens durch den Anbieter erfolgt durch Übermittlung einer verschlüsselten CSV-Datei gemäß der Schnittstellenspezifikation in der Anlage zu dieser Verordnung. Die Durchlaufstelle stellt automatisch sicher, dass die Antwort in das richtige Postfach der anfragenden Dienststelle zugestellt wird. In den Fällen des Abs. 2 muss die adressierte Dienststelle jedoch durch individuelle Auswahl über die Durchlaufstelle bestimmt werden.

(4) Die Durchlaufstelle versendet nach Eingang der Antwort in das Postfach der anfragenden Dienststelle eine Benachrichtigung über die Hinterlegung der Antwort an die Dienststelle.

(5) Die Abholdung der Auskunft erfolgt manuell durch Zugriff auf das Postfach der Dienststelle nach entsprechender Authentifizierung des Benutzers. Eine Abholung der Auskunft per Webservice kann in der Spezifikation zur Durchlaufstelle vorgesehen werden.

Verschlüsselung/Signatur der Antwort

§ 18. (1) Die vertrauenswürdige Stelle zur Hinterlegung der Zertifikate ist das Bundesministerium für Verkehr, Innovation und Technologie, das diese Funktion über die Durchlaufstelle technisch wahrnimmt. Jeder Teilnehmer kann in der Durchlaufstelle nur zu seiner Institution zugehörige eindeutige Schlüssel hinterlegen.

(2) Die Echtheit der Software, die von der Durchlaufstelle zur Verschlüsselung durch den Client zur Verfügung gestellt wird, muss für einen Client-Administrator eindeutig verifizierbar sein. Die Verschlüsselung und die Signatur erfolgt auf Client Seite, nur der öffentliche Schlüssel wird bei der Durchlaufstelle abgeholt.

(3) In der Spezifikation zur Durchlaufstelle ist eine eindeutige Definition der Dateinamen für die Übermittlung der Antwort sowie der Signatur zur Verschlüsselung der Dateien vorzunehmen. Es ist eine fortgeschrittene elektronische Signatur im Sinne des § 2 Z 3 des Signaturgesetzes, BGBl. I Nr. 190/1999 in der Fassung BGBl. I Nr. 75/2010, vorzusehen.

(4) Wenn die Antwort aus mehreren CSV-Dateien besteht, ist es optional möglich, alle Dateien zu einer Abfrage zu einer Gesamtdatei zusammenzufassen. Die Gesamtdatei kann optional komprimiert werden. Die komprimierte oder unkomprimierte Gesamtdatei ist für die Übermittlung zu verschlüsseln, nicht aber die einzelnen Dateien.

Eingabefelder

§ 19. (1) Über die Durchlaufstelle ist bei jeder Anfrage auszuwählen, ob es sich um ein Auskunftsbegehren nach § 53 Abs. 3a SPG, nach § 53 Abs. 3b SPG, nach § 76a StPO, nach § 135 Abs. 2 StPO oder nach § 135 Abs. 2a StPO oder um eine Stammdatenauskunft nach § 21 handelt. In der Durchlaufstelle ist ein Feld für den Eintrag der einer Anordnung zu Grunde liegenden strafbaren Handlung für die Protokollierung gemäß § 7 Abs. 3 Z 8 vorzusehen. Eine allfällige Eingabemaske auf Behördenseite kann unter Beachtung der Schnittstellenspezifikation in der Anlage frei gestaltet werden.

(2) Dies gilt sinngemäß auch für eine allfällige Eingabemaske auf Anbieterseite. Insbesondere besteht keine Verpflichtung zur automatisierten Befüllung der CSV-Datei.

Zusatzinformationen

§ 20. Die Durchlaufstelle hat die Übertragung von Zusatzinformationen zu unterstützen. Zusatzinformationen können allenfalls über ein Web-Interface zu der entsprechenden Abfrage eingegeben werden. Diese Zusatzinformationen könnten auch Gründe für eine Leer-Meldung beschreiben. Ob und in welchem Ausmaß ein Web-Interface auf Seiten der Durchlaufstelle zur Verfügung gestellt werden soll, ist in der Spezifikation zur Durchlaufstelle zu regeln. Voraussetzung ist in jedem Fall, dass die Durchlaufstelle keinen Zugang zu personenbezogenen Inhalten der Auskünfte hat.

Optionale Stammdatenauskünfte über die Durchlaufstelle

§ 21. Anbieter und zugangsberechtigte Behörde können jeweils im Einvernehmen optieren, Stammdatenauskünfte über die Durchlaufstelle abzuwickeln. Die technischen Details solcher Auskünfte sind in der Spezifiktion zur Durchlaufstelle zu regeln.

Protokollierung über die Durchlaufstelle

§ 22. (1) Die Protokollierung der Durchlaufstelle enthält keine personenbezogenen Daten. Durch die Unique-ID jeder Anfrage wird der Zusammenhang zwischen jeder Anfrage und deren Beantwortung ohne Personenbezug hergestellt.

(2) Bei der Übermittlung der Antwort zu einem Auskunftsbegehren hat der Anbieter die Protokollinformationen gemäß § 7 Abs. 3 Z 4 und 5 für die in Abs. 4 genannten Zwecke an die Durchlaufstelle zu übermitteln.

(3) Die Protokolldaten werden in einer Protokolldatei unverschlüsselt über die sichere Transportverbindung zur Durchlaufstelle übermittelt. Das Format der Datei und der Dateiname sind in der Spezifikation zur Durchlaufstelle festzulegen.

(4) Die Protokolldaten sind ausschließlich für die definierten Protokolldatenempfänger zugänglich und werden innerhalb der Durchlaufstelle in einer gesonderten Datenbank archiviert. Für die Datenschutzkommission sowie für die Rechtsschutzbeauftragten beim Bundesminister für Justiz und

beim Bundesminister für Inneres sind in der Spezifikation zur Durchlaufstelle gesonderte Berechtigungen für den Zugang zu den Protokolldaten vorzusehen.

Statistik aus den Protokolldaten

§ 23. (1) Die Statistik zur Erfüllung der Verpflichtung aus Art. 10 der Richtlinie 2006/24/EG soll in der Durchlaufstelle automatisch aufbereitet werden. Die genaue Definition der zu erstellenden Statistik ist in der Spezifikation zur Durchlaufstelle vorzunehmen.

(2) Für die Erstellung der Statistik sind die Protokoll-Informationen gemäß § 7 Abs. 3 Z 3 bis 5 und Z 8 erforderlich. Die Informationen gemäß § 7 Abs. 3 Z 3 sind von der Durchlaufstelle automatisch zu jedem Auskunftsfall zu erfassen. Die Informationen gemäß § 7 Abs. 3 Z 4 und 5 hat der Anbieter gemäß § 23 Abs. 2 gemeinsam mit der Beantwortung des Auskunftsbegehrens an die Durchlaufstelle zu übermitteln.

(3) Zugang zur Statistik der Durchlaufstelleerhalten gemäß § 102c Abs. 4 TKG 2003 das Bundesministerium für Justiz, der Datenschutzrat, und die Datenschutzkommission. Darüber hinaus ist in der Spezifikation zur Durchlaufstelle ein elektronischer Zugang für die Rechtsschutzbeauftragten beim Bundesminister für Justiz und beim Bundesminister für Inneres vorzusehen.

Kostentragung der Durchlaufstelle

§ 24. Die Investitionskosten für die Durchlaufstelle sind Investitionskosten gemäß § 94 Abs. 1 TKG 2003.

4. Abschnitt

Definition Syntax und Semantik der CSV-Datei für Auskünfte

Schnittstellendefinition EP020

§ 25. Die Schnittstellendefinition ergibt sich aus der Anlage.

Erläuterungen

Allgemeiner Teil

Die Verordnungsermächtigungen der §§ 94 Abs. 4 und 102c TKG 2003 werden gegenständlich mit einer einheitlichen Verordnung geregelt. Diese Verordnung wird von der Bundesministerin für Verkehr, Innovation und Technologie erlassen, wobei jene Teile der Verordnung, die in Ausführung des § 94 Abs. 4 TKG 2003 ergehen, im Einvernehmen mit dem Bundesminister für Inneres und dem Bundesminister für Justiz zu erlassen sind, während ein solches Einvernehmen in Bezug auf die § 102c TKG ausführenden Bestimmungen nicht erforderlich ist. Letzteres betrifft die Bestimmungen im 2. Abschnitt (§§ 5 bis 7), wobei auch zu diesen in der Vorbreitung grundsätzliches Einvernehmen hergestellt wurde.

Besonderer Teil

Zu § 1:

In den Erläuterungen zu § 94 Abs. 4 TKG 2003 wird der Spielraum abstrakt beschrieben, den der Verordnungsgeber bei der Ausgestaltung dieser Bestimmung hat: „Die Bestimmung identifiziert die maßgeblichen Indikatoren zur Datensicherheit bei der Übermittlung von Verkehrsdaten. Die Übertragungstechnologie, welche durch eine Verordnung („Technische Richtlinie") nach dieser Bestimmung zu konkretisieren ist, soll durch sichere „Identifikation und Authentifizierung von Sender Empfänger" sicherstellen, dass die durch das Kommunikationsgeheimnis geschützten Verkehrsdaten tatsächlich nur Behörden, Staatsanwaltschaften und Gerichten zugänglich sind, denen eine gesetzliche Auskunftsbefugnis zusteht. Dabei muss auf technischer Ebene die Datenintegrität gewahrt sein. Das bedeutet, dass jede allfällige Veränderung der übermittelten Daten auf dem Übertragungsweg für den Empfänger sofort identifizierbar wäre und dieser sich damit auf die Richtigkeit der Daten nicht mehr verlassen darf. Die Formulierung „unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie" (im Gegensatz zur Fassung im ursprünglichen Begutachtungsentwurf vom Dezember 2009 „Übertragung per E-Mail") ist eine Ergänzung zur Erfüllung anspruchsvoller Datensicherheitsstandards, wie sie insbesondere im Urteil des deutschen Bundesverfassungsgerichts zu BVerfG, 1 BvR 256/08 vom 2.3.2010 beschrieben werden. Die Formulierung lässt genügend Spielraum, die nähere technische Ausgestaltung durch Verordnung zu regeln und stellt gleichzeitig einen Auftrag an den Verordnungsgeber dar. Die gesetzlich vorgezeichneten Indikatoren sind dabei technologieneutral formuliert. Wesentlich ist, dass die eingesetzte Technologie den Zielvorgaben entspricht.

Am 7.4.2011 wurde die TKG Novelle zur Umsetzung der Vorratsdatenspeicherung im Ausschuss für Forschung, Innovation und Technologie (FIT Ausschuss) des Nationalrats diskutiert (siehe dazu den Ausschussbericht: 1157 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXIV. GP). In diesem Rahmen wurde ein Antrag für eine Ausschussfeststellung zum Thema Datensicherheit eingebracht, der eine Grundsatzerklärung für die Implementierung der Durchlaufstelle enthält. Diese Ausschussfeststellung wurde mit den Stimmen der Regierungsfraktionen angenommen und lautet wie folgt: „Für die Datensicherheit und die Nachvollziehbarkeit der Zugriffe auf den Datenvorrat ist das Zusammenspiel der Bestimmungen der §§ 94 Abs. 4 und 102c TKG von besonderer Bedeutung. Während § 94 Abs. 4 TKG 2003 den Aspekt der technischen Datenintegrität und der Determinierung der Verordnungsermächtigung über die Art der Verschlüsselung betrifft und die maßgeblichen Indikatoren zur Datensicherheit bei der Übermittlung von Verkehrsdaten identifiziert, um durch sichere ‚Identifikation und Authentifizierung von Sender und Empfänger' sicherzustellen, dass die durch das Kommunikationsgeheimnis geschützten Verkehrsdaten tatsächlich nur Behörden, Staatsanwaltschaften und Gerichten zugänglich sind, denen eine gesetzliche Auskunftsbefugnis zusteht, regelt § 102c TKG 2003 Zugriffs- und Sicherheitsbestimmungen. Einerseits muss jeder Zugriff auf Vorratsdaten durch zwei Personen mit einer besonderen Ermächtigung hierzu autorisiert sein, um zu gewährleisten, dass nicht eine einzelne Person unbemerkt und unkontrolliert auf diese Daten zugreifen kann. Andererseits müssen Zugriffe auf Vorratsdaten beim Anbieter revisionssicher protokolliert werden. Die wichtigsten Kriterien sind dabei der Schutz vor Veränderung und Verfälschung, die Vollständigkeit, die Ordnungsmäßigkeit, die Sicherung vor Verlust, die Einhaltung der Aufbewahrungsfristen sowie die Dokumentation, Nachvollziehbarkeit und Prüfbarkeit des Verfahrens, wozu etwa bei Anordnungen der Staatsanwaltschaft auch die Angabe der Geschäftszahl der ermittelnden Kriminalpolizei zählt. Der Ausschuss geht davon aus, dass sämtliche Zugriffe und Übermittlungen von wem auch immer auf Vorratsdaten gemäß § 94 Abs. 4 TKG lückenlos protokolliert werden. Der Ausschuss geht weiters davon aus, dass ein automatisches zentrales System der Protokollierung solcher Abfragen und Übermittlungen notwendig ist, wobei unter dieser Protokollierung nicht die in § 102c Abs. 2 TKG 2003genannte zu verstehen ist. Sie wird vielmehr

nur jene Daten umfassen, die zur statistischen Auswertung und zur Verknüpfung mit der gemäß § 102c Abs. 2 TKG 2003 erfolgenden Protokollierung dient. Wünschenswert ist die Einrichtung einer ‚Datendrehscheibe' (‚Durchlaufstelle', kurz: DLS). Da jeder Auskunftsfall über die DLS mit einer fortlaufenden einmaligen Nummer versehen wird, kann im Falle einer Nachprüfenden Kontrolle über die Protokollierung bei der DLS zur Protokollierung beim Anbieter gemäß § 102c Abs. 2 TKG 2003 verknüpft werden. Zugang zu den übermittelten personenbezogenen Daten soll die DLS selbst nicht bieten, die Daten liegen dort nur verschlüsselt bis zur Abholung bereit und werden bei der Abholung automatisch gelöscht."

Festzuhalten ist, dass diese Ausschussfeststellung sachlich auf der gemeinsamen Arbeit zur Entwicklung der Schnittstellenbeschreibung und eines sicheren Systems der Datenübermittlung in den Round Table Diskussionen basiert, die das Ludwig Boltzmann Institut für Menschenrechte (BIM) im Rahmen einer Studie zur Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung im Auftrag des BMVIT ausgearbeitet hat. Die Ausschussfeststellung bezieht sich auf den Diskussions- und Einigungsstand beim 3. von insgesamt 6 Round Table Veranstaltungen am 24.3.2011, bei dem die Grundsatzeinigung auf das Konzept der Durchlaufstelle (siehe § 10) bereits Konsens unter allen Beteiligten war.

Zu § 1 Abs. 2:

Zunächst wird klargestellt, dass diese Verordnung nicht ausschließlich Vorratsdaten betrifft. Soweit es nämlich um die Übermittlung von Verkehrsdaten, Zugangsdaten und Standortdaten für Auskünfte gegenüber Sicherheits- und Strafverfolgungsbehörden geht, die beim Anbieter für betriebliche Zwecke gespeichert sind, sind die Datensicherheitsvorschriften auch für diese Daten relevant. Hinsichtlich jener Bestimmungen, die Datensicherheitsmaßen innerhalb des Betriebes des Anbieters betreffen, ist die Verordnung allerdings nur für Vorratsdaten maßgeblich, denn nur für diese gelten gemäß § 102c TKG 2003 die strengen Zugriffsbestimmungen. Ansonsten gilt der allgemeine Sicherheitsmaßstab, den das TKG 2003 und das DSG 2000 vorgeben (siehe dazu die Erläuterungen zu § 4).

Schließlich wird bewusst die Formulierung „Verwendung" normiert. Nach § 4 Z 8 DSG 2000 ist „Verwenden von Daten" definiert wird als „ jede Art der Handhabung von Daten, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten" und der Begriff „Verarbeiten von Daten" gemäß § 4 Z 9 DSG 2000 auch die Speicherung umfasst. In der österreichischen datenschutzrechtlichen Terminologie ist dies der weiteste Begriff, der alle Fälle möglicher Datenverwendungen - insbesondere die Übermittlung von Daten - umfasst. Weil gerade im Regelungsbereich des § 94 Abs. 4 TKG 2003 die Übermittlung im Vordergrund steht, wird hier der Rechtsbegriff der Datenverwendung nutzbar gemacht. Aus dem Regelungsumfang der Verordnung ist zugleich klar, dass die weitere Verwendung der betreffenden Daten nach der Übermittlung über die DLS - insbesondere die weitere Verwendung der Daten für die Zwecke der Strafverfolgung - nicht von dieser Verordnung bestimmt wird.

Zu § 2 Abs. 1:

Diese Bestimmung definiert die Bezeichnung der beiden Datenarten, deren Unterscheidung vom Zweck der Verarbeitung und Speicherung abhängt. An diese Unterscheidung sind einige rechtliche Konsequenzen geknüpft, die durch eine Konkretisierung und klare Formulierung der an sich schon im TKG 2003 vorgezeichneten Definitionen leichter normativ zu erfassen sind. In Z 1 wird bewusst der Begriff „Betriebsdaten" eingeführt, weil in zahlreichen öffentlichen Diskussionen zum Thema Vorratsdatenspeicherung oft nur der Begriff der „Verrechnungsdaten" verwendet wird, der jedoch zu kurz greift. Wohl bilden die Daten zum Zweck der Rechnungslegung (§ 99 Abs. 2 TKG 2003) den praktisch wichtigsten Fall, doch auch jene Daten, die beim Anbieter zum Zweck der Aufrechterhaltung des Betriebes und insbesondere der technischen Wartung der Betriebsanlagen (§ 99 Abs. 3 TKG 2003) verarbeitet und gespeichert werden, sind nach der bisherigen Rechtslage vor Umsetzung der Vorratsdatenspeicherung regelmäßig Gegenstand von behördlichen, staatsanwaltschaftlichen und gerichtlichen Auskunftsersuchen. Z 2 gibt die Legaldefinition des § 92 Abs. 3 Z 6b TKG 2003 wieder und verbindet diese mit der Zweckwidmung des § 102b TKG 2003. Damit soll lediglich die strenge Zweckbindung, die nur durch die Ausnahmen in § 99 Abs. 5 TKG 2003 durchbrochen wird, eindeutig klargestellt werden, ein über die Definition im TKG 2003 hinausgehender normativer Gehalt entsteht daraus nicht.

Zu § 3 Abs. 1:

Absatz 1 nimmt jene Fälle vom Datensicherheitsregime des 3. Abschnitts dieser Verordnung aus, die bereits durch die gesetzliche Regelung des § 94 Abs. 4 TKG 2003 als Ausnahmen vorgesehen sind. Aufgezählt werden jene Fälle, in denen eine Beantwortung von Auskunftsbegehren durch den Anbieter nach einem anderen Regime vorgesehen oder zumindest zulässig ist und keine Verschlüsselung nach dem 3. Abschnitt zwingend durchzuführen ist. Die auf § 98 TKG 2003 bezogene Ausnahme bezieht sich auf die Identifizierung und Lokalisierung von Anschlüssen bzw. Endgeräten, von denen ein Notruf abgesetzt

wurde. Für diese Fälle wird es künftig nach der Umsetzung des neuen Telekom Rechtsrahmens eine eigene Schnittstelle geben, um eine sofortige Reaktion der Notrufträger zu ermöglichen, wobei damit eine automatische nachträgliche Information der Betroffenen verbunden ist. Die Umsetzung dieser gemeinschaftsrechtlichen Verpflichtung steht unmittelbar bevor, daher ist dieser Fall aus dem Anwendungsbereich dieser Verordnung ausgeklammert.

Die Fälle des § 99 Abs. 5 Z 3 und 4 TKG 2003 bei Gefahr im Verzug gemäß Z 2 bezieht sich auf Anfragen nach § 53 Abs. 3a und 3b SPG, wenn aufgrund der besonderen Umstände des Falles der Zweck der Auskunft (zB die Abwehr einer gegenwärtigen oder unmittelbar drohenden Gefahr) dadurch gefährdet wäre, dass die Abwicklung der Auskunft über das System der DLS zu lange dauern würde und daher eine schnellere Form der Beauskunftung unerlässlich ist, zB eine telefonische Auskunft über die Standortdaten des Endgerätes einer akut gefährdeten Person. Die Übermittlung von begleitenden Rufdaten im Rahmen einer Überwachung von Nachrichten erfolgt über die ETSI Schnittstelle zur Inhaltsüberwachung durch Übergabe der sogenannten „S-Records".

Zu § 3 Abs. 2:

Absatz 2 dieser Bestimmung regelt die gesetzlich definierten Ausnahmefälle für Anfragen abseits der DLS sowie die Verpflichtung zur nachträglichen Dokumentation über die DLS. Ganz generell ist hier voraus zu schicken, dass das Konzept der DLS auch darauf abzielt, die Abwicklung von Auskunftsbegehren im Vergleich zur bisherigen Praxis (Fax- und E-Mail- Anfragen) zu beschleunigen und den Verwaltungsaufwand sowohl auf Behörden- als auch auf Anbieterseite zu reduzieren. Es ist daher nicht generell davon auszugehen, dass eine Abwicklung abseits der DLS tatsächlich jene Beschleunigung mit sich bringt, welche die gesetzlichen Ausnahmen rechtfertigen soll. Die Praxis ab dem Vollbetrieb des neuen Konzepts ab 1.4.2012 wird zeigen, ob gerade in dringenden Fällen eine Abwicklung über die DLS nicht sogar vorteilhaft sein wird. Die technische Spezifikation sollte hierzu also jedenfalls den Usecase "nachträgliche Anfragedokumentation" berücksichtigen und idealer weise auch eine Prioritäteninformation bei der Notifikation über die DLS vorsehen. Bereits die Erläuterungen zu § 94 Abs. 4 TKG 2003 führen zu den Ausnahmen aus: „Ausdrücklich gesetzlich gefordert ist eine Verschlüsselung bei der Übermittlung. Davon ausgenommen sein soll die Übermittlung von Daten in Notfällen. In diesen Fällen soll daher die bisher praktizierte Übermittlungsform beibehalten werden, also Auskünfte per Telefon oder Fax. Die weiteren Ausnahmen vom Grundsatz der Übermittlung in einem CSV-File berücksichtigen die in der Praxis wichtigen Fälle, in denen aufgrund der besonderen Dringlichkeit (insbesondere bei Standortdatenauskünften, etwa zur Lebensrettung oder bei zeitkritischen Observationen) dieses Verfahren nicht zweckmäßig wäre. Außerdem sind die sogenannten „S-Records" (das sind die begleitenden Verkehrsdaten bei einer Inhaltsüberwachung von Telefongesprächen) berücksichtigt, welche über eine besondere technische Schnittstelle gemeinsam mit der Inhaltsüberwachung abgewickelt werden."

Die in den Ausnahmen genannten Fälle des § 99 Abs. 5 Z 3 und 4 TKG 2003 betreffen Auskünfte nach § 53 Abs. 3a und Abs. 3b SPG, bei denen eine Anfrage bzw. Beantwortung via DLS bei Gefahr in Verzug unterbleiben kann. Standortdatenanfragen nach § 53 Abs. 3b SPG werden dabei schon aufgrund des dort normierten Tatbestandes (Abwehr einer „gegenwärtigen Gefahr" für den Inhaber der Endeinrichtung) regelmäßig einen Fall von „Gefahr in Verzug" darstellen. Festzuhalten ist, dass in diesen Fällen nur ausnahmsweise überhaupt historische Standortdaten begehrt werden, nämlich nur dann, wenn eine live-Ortung (durch sog. „stummes SMS") erfolglos bleibt, etwa weil das Endgerät defekt oder ausgeschaltet ist. In Fällen von Gefahr im Verzug kann die Anfrage telefonisch übermittelt werden. Es erfolgt eine Nachreichung der Anfrage über die DLS, wobei davon auszugehen ist, dass die Beantwortung der Anfrage bereits vor der Nachreichung der Anfrage erfolgt. Dies bedeutet, dass bei der technischen Spezifikation der DLS Festlegungen zur Unique-ID getroffen werden müssen. Dazu könnte jedem Anbieter ein eigener Bereich von Referenznummern zugeteilt werden. Der Anbieter verwendet diese Referenznummern in aufsteigender Reihenfolge im Falle, dass die betreffende Anfrage noch nicht über die DLS eingelangt ist. In der Durchlaufstelle muss dann die Zuordnung zwischen Anfrage und (bereits erfolgter) Durchführung erfolgen. Es ist hier nur der Usecase "nachträgliche Anfragedokumentation" zu berücksichtigen (Daten wurden bereits übermittelt) + Übermittlung von Protokolldaten bei Zugriff auf Vorratsdaten.

SPG Anfragen können

a) bei Gefahr im Verzug

- mündlich
- lt. SPG von jeder Sicherheitsbehörde
- schriftlich

- oder über die DLS

b) wenn keine Gefahr im Verzug vorliegt

- durch Anfrage (und Antwort) über die DLS

zum Anbieter gelangen.

Die Dokumentation über die DLS ist dabei sinnvoll und notwendig, da teilweise (insbesondere bei Anfragen zu IP-Adressen und E-Mail Daten) auch Vorratsdaten betroffen sein werden und der Anbieter bei Zugriff auf Vorratsdaten die Protokolldaten gemäß § 7 Abs. 3 Z 3 bis 5 zu übermitteln hat und der besondere Rechtsschutz (Informationspflicht der Behörde) ausgelöst wird.

Auch im Rahmen von StPO-Abfragen kann es - eng begrenzte - Fälle geben, in denen eine mündliche Übermittlung der Anordnung erfolgt. Anordnungen von Zwangsmaßnahmen sind von der Staatsanwaltschaft begründet und schriftlich auszufertigen und an die Kriminalpolizei zu richten. In dringenden Fällen kann aber eine solche Anordnung vorläufig mündlich übermittelt werden (§ 102 Abs. 1 StPO). Dies gilt auch für die Anordnung einer „Auskunft über Daten einer Nachrichtenübermittlung" (§ 134 Z 2 StPO) sowie künftig bei einer „Auskunft über Vorratsdaten" (§ 134 Z 2a StPO). In dringenden Fällen kann eine solche mündliche Anordnung auch auf Grund einer mündlichen gerichtlichen Bewilligung (§ 105 StPO) erteilt werden. So kann im Fall des § 135 Abs. 2 Z 1 StPO (noch andauernde Entführung) eine Dringlichkeit vorliegen, die zumindest erfordert, dass die Übermittlung des Auskunftsbegehrens vorerst „auf kürzestem Weg" an den Anbieter gerichtet wird, während die Antwort über die sichere Verbindung gemäß § 94 Abs. 4 TKG 2003 übermittelt werden muss, weil diesbezüglich keine gesetzliche Ausnahme vorgesehen ist. Aus Sicht des TKG 2003 ist dies rechtlich zulässig, da § 94 Abs. 4 TKG 2003 ausdrücklich nur die Beantwortung, aber nicht die Übermittlung der Anordnung regelt. Diesbezüglich wäre gemäß § 102 Abs. 1 StPO die schriftliche und begründete Anordnung der Staatsanwaltschaft nachzureichen. Das Erfordernis einer gerichtlichen Bewilligung sagt per se nichts über die Dringlichkeit und das auch über Entführungsfälle hinausgehende Erfordernis einer mündlichen Beauskunftung vorab aus. Die gerichtliche Bewilligung kann im Rahmen des Rufbereitschafts- und Journaldienstes fernmündlich binnen kürzester Zeit erteilt werden, gerade wenn eine unverzügliche Anordnung durch die Staatsanwaltschaft fallspezifisch nötig ist. § 102 Abs. 1 StPO sieht generell vor, dass Anordnungen und Genehmigungen in dringenden Fällen vorläufig mündlich übermittelt werden können. In der Praxis werden solche mündlichen Anordnungen von den Anbietern akzeptiert– wenn eine schriftliche Bestätigung der Exekutive über "mündliche Anordnung und Bewilligung" vorliegt. Auch in diesen Fällen ist Vorkehrung dafür zu treffen, dass eine Beantwortung vor Übermittlung der Anfrage erfolgen kann, wobei gerade hier erforderlich ist, dass die schriftliche Anfrage über die DLS nachzureichen und zu dokumentieren ist.

Zu § 4:

Absatz 1 folgt zunächst dem ersten Grundsatz, den die Richtlinie 2006/24/EG in Art 7 lit a) aufstellt: „Die auf Vorrat gespeicherten Daten sind von der gleichen Qualität und unterliegen der gleichen Sicherheit und dem gleichen Schutz wie die im Netz vorhandenen Daten".

Die darüber hinausgehenden Sicherheitsvorschriften, die im 2. Abschnitt geregelt werden und auf die Absatz 2 in diesem Zusammenhang nur verweist, erfließen aus dem Spielraum der Mitgliedsstaaten, höhere Sicherheitsanforderungen zu erlassen (Art 7 Abs. 1 RL 2006/24/EG, arg. „zumindest folgende Grundsätze") und sind das Ergebnis einer intensiven Diskussion im Rahmen vieler Arbeitsgruppentreffen im Zuge der Umsetzung der Vorratsdatenspeicherung, die nicht zuletzt durch die Entscheidung des deutschen Bundesverfassungsgerichts (BVerfG, 1 BvR 256/08 Urteil vom 2.März 2010) zur dortigen Aufhebung der deutschen Umsetzung der Vorratsdatenspeicherungs-Richtlinie motiviert und vorgezeichnet sind.

Die für die Ausarbeitung des Konzepts hinter dieser Verordnung wesentlichsten Aussagen des BVerfG sollen hier auszugsweise wiedergegeben werden: Hinsichtlich der Datensicherheit fordert das Gericht „gesetzliche Regelungen, die einen solchen besonders hohen Sicherheitsstandard in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgeben" (BVerfG, 1 BvR 256/08 Urteil vom 2.März 2010, Abs. 225). Dieser hat sich an dem Entwicklungsstand der Fachdiskussion zu orientieren, neue Erkenntnisse und Einsichten fortlaufend aufzunehmen und nicht unter dem Vorbehalt einer freien Abwägung mit allgemeinen wirtschaftlichen Gesichtspunkten zu stehen. Nur wenn diesbezüglich hinreichende anspruchsvolle und normenklare Regelungen getroffen sind, ist der in einer solchen Speicherung liegende Eingriff verhältnismäßig im engeren Sinne, so das Gericht (BVerfG, 1 BvR 256/08 Urteil vom 2.März 2010, Abs. 239). Um in qualifizierter Weise dem Grunde nach den Schutzstandard konkretisieren zu können, muss der Gesetzgeber die Schutzmechanismen selbst benennen und nur deren Ausgestaltung auf Verordnungen oder Aufsichtsbehörden delegieren. Dem ist die Konzeption des § 94

Abs. 4 und 102c TKG 2003 auch gefolgt. Wo die allgemeinen Sicherheitsanforderungen an die Verarbeitung von Telekommunikationsdaten nicht ausreichend sind, um dem speziellen Schutzbedürfnis zu begegnen, das aus der flächendeckenden und anlasslosen Vorratsspeicherung resultiert, werden die besonderen Anforderungen in Ausführung der Vorgaben des § 102c TKG 2003 im nachfolgenden 2. Abschnitt normiert, auf den Absatz 2 klarstellend verweist.

Zu § 5 Abs. 1 bis 4:

Die österreichische Umsetzung ist in einem Punkt weniger streng als das Urteil des deutschen Bundesverfassungsgerichts vorzeichnet, wonach verlangt wird: „Die Daten sind getrennt von den weiteren IT-Systemen des Speicherverpflichteten zu speichern, und zwar hardwaremäßig getrennt und entkoppelt vom Internet." Es genügt also nicht den Anforderungen des Bundesverfassungsgerichts, die Daten, die zur Vorratsdatenspeicherung gedacht sind, durch eine Kennzeichnung in der Datenbank von denjenigen Daten zu trennen, die für Abrechnungszwecke gespeichert werden (Andreas Gietl, Die Zukunft der Vorratsdatenspeicherung – Anmerkung zum Urteil des BVerfG vom 2. März 2010, in: DuD 6/2010, S. 399).

Nach den Vorgaben des § 102c TKG 2003 und der Konkretisierung durch § 5 ist eine physische Trennung bei der Speicherung von Vorratsdaten und Betriebsdaten nicht notwendig. Hintergrund dieser Entscheidung des Gesetzgebers und in weiterer Folge des Verordnungsgebers ist die Tatsache, dass eine physische Trennung im Hinblick auf die Datensicherheit nur dann endgültig Sinn ergeben würde, wenn damit auch zwingend verbunden wäre, dass der physische und technische Zugang auf der Ebene der IT-Infrastruktur zu einem solcherart getrennten Speichersystem organisatorisch nur völlig unterschiedlichen Personen im Betrieb des Anbieters möglich ist. Das würde faktisch bedeuten, dass ein zur Speicherung verpflichtetes Unternehmen eine eigene und völlig abgegrenzte IT-Abteilung nur für die Vorratsdatenspeicherung schaffen müsste. Dies wurde in der Debatte zur Umsetzung als unverhältnismäßiger Eingriff in die Eigentumsfreiheit der Anbieter gesehen und hat daher keinen Eingang in die österreichische Umsetzung gefunden. Anzumerken ist, dass sich das deutsche Bundesverfassungsgericht mit dem Problem der flankierenden organisatorischen Trennung gar nicht auseinandergesetzt hat.

Gleichwohl sind die speicherpflichtigen Unternehmen gesetzlich verpflichtet, sicherzustellen, dass der Eingriff auf die Daten einem gesicherten Zugriffsregime unterliegt. Das BVerfG führt hier beispielhaft das Vier-Augen-Prinzip an. Der Zugriff soll nicht durch Einzelne, sondern nur durch zwei oder mehr Personen möglich sein. Darüber hinaus ist der Zugriff auf die Daten revisionssicher zu protokollieren. Damit verlangt das Bundesverfassungsgericht, dass einerseits ein Zugriff auf die Daten nur möglich ist, wenn der Zugriff auch protokolliert wird. Andererseits darf dieses Protokoll nicht im Nachhinein zu verändern sein, muss also revisionssicher sein (siehe dazu die Erläuterungen zu § 7). Um dieses getrennte Zugriffsregime effektiv zu verwirklichen, sind geeignete Maßnahmen sowohl auf technischer als auch organisatorischer Ebene beim Anbieter notwenig, die jedenfalls eine logische Trennung bei der Datenbankhaltung erfordern. Nicht hinreichend wäre dafür, dass die Daten einfach in den betrieblichen Datenbanken verbleiben und dort als Vorratsdaten markiert werden. Daher ordnet Absatz 3 auch an, dass diese Daten umgehend aus den betrieblichen Datenbanken zu löschen und in die Vorratsdatenbank zu überführen sind. Die konkret von einem Anbieter entwickelte Methode dieser Trennung muss für die Kontrolle durch die Datenschutzkommission nachvollziehbar sein und daher auch dokumentiert werden. Dies sollte der Datenschutzkommission ermöglichen, die tatsächliche Einhaltung der Standards jederzeit zu kontrollieren.

Zu § 5 Abs. 5:

Eine völlige Harmonisierung, wie lange ein Anbieter im Detail welche Daten für betriebliche Zwecke speichern darf, ist kaum zu erreichen und wäre wohl ein unverhältnismäßiger Eingriff in die Erwerbsfreiheit. Die Schwierigkeit liegt nämlich darin, dass die betriebliche Notwendigkeit einer Datenspeicherung einerseits von den technischen Systemen und deren Wartung und andererseits von der Ausgestaltung verschiedener Tarif- und Geschäftsmodelle abhängt. Dabei ist zum Teil gar nicht möglich, dass ein Anbieter in Bezug auf bestimmte Datenkategorien (etwa der Unterscheidung gemäß § 102a Abs. 2 bis 4 TKG 2003 folgend) genau festlegen kann, wie lange diese Datenkategorien jeweils für betriebliche Zwecke aufbewahrt werden. Das Problem liegt nämlich darin, dass zur selben Datenkategorie in unterschiedlichen Tarifmodellen auch unterschiedliche Aufbewahrungszeiträume notwendig sind. Dieselben Daten können also in einem Fall noch Betriebsdaten und in einem anderen Geschäftsmodell bereits Vorratsdaten sein.

Der Anbieter muss jedoch betriebsintern Klarheit darüber schaffen, welche Daten im Hinblick auf die intern bestimmten technischen und geschäftlichen Notwendigkeiten wie lange gespeichert werden. Diese Klarheit ist schon deswegen notwendig, weil ansonsten eine Abgrenzung im Hinblick auf das geforderte

erhöhte Sicherheitsregime bei Vorratsdaten nur schwer möglich ist. Obgleich ein Anbieter Spielraum zur Gestaltung seiner Geschäftsmodelle hat, ist die Unterscheidung von Vorratsdaten nicht völlig beliebig in der Hand des Anbieters. Vielmehr haben die internen Betriebsdaten-Richtlinien den Anforderungen an eine datenschutzrechtliche Rechtfertigung für die Verarbeitung personenbezogener Daten gerecht zu werden. Es muss für einen verständigen Beobachter nachvollziehbar sein, warum bestimmte Daten(Kategorien) für bestimmte Zwecke eine bestimmte Zeit lang aufbewahrt werden. Aus diesem Grund müssen die internen Betriebsdaten-Richtlinien auch der Datenschutzkommission zugänglich sein, damit sie im Falle einer objektiven Kontrolle die Nachvollziehbarkeit der Rechtfertigung prüfen kann.

Überdies muss der Anbieter schließlich in der Lage sein, seine Speicherpolitik gegenüber seinen Kunden zu rechtfertigen, insbesondere für den Fall, dass ein Kunde eine Auskunft gemäß § 26 DSG 2000 begehrt oder im gerichtlichen Verfahren gemäß § 32 DSG 2000 die Richtigstellung oder Löschung seiner Daten begehrt.

Zu § 6 Abs. 1:

Absatz 1 normiert einen für die Praxis wichtigen Größenschluss, dessen Zulässigkeit sich aus den gesetzlichen Voraussetzungen für die Auskunft über Vorratsdaten gemäß § 135 Abs. 2a StPO ergibt. Dieser verweist nämlich auf die Fälle des § 135 Abs. 2 Z 2 bis 4 StPO, woraus sich ergibt, dass immer dann, wenn die Voraussetzungen für eine Auskunft über Vorratsdaten vorliegen, zugleich auch die Vorraussetzungen für eine Auskunft über „Betriebsdaten" nach § 135 Abs. 2 StPO gegeben sind. Für die Praxis sollen möglichst Fälle vermieden werden, in denen eine Anfrage auf betrieblich gespeicherte Daten negativ beantwortet wird und dann eine zweite Anfrage auf Vorratsdaten erforderlich ist. Es sollen zudem auch Fälle vermieden werden, in denen sich der Zeitraum einer negativen Anfrage auf betriebsnotwendige Daten und die darauf folgenden Anfrage auf Vorratsdaten genau mit jenem Zeitraum überschneidet, innerhalb dessen Daten nicht mehr für betriebsnotwendige Zwecke benötigt werden und somit zu Vorratsdaten werden. Ansonsten könnte es etwa sein, dass Vorratsdaten angefordert werden, zunächst aber nur Betriebsdaten vorliegen und zum Zeitpunkt der nochmaligen Übermittlung des Auskunftsbegehrens gerichtet auf Betriebsdaten (also gemäß § 135 Abs. 2 StPO) diese Daten in der Zwischenzeit doch zu Vorratsdaten geworden sind, und der Anbieter die Antwort schließlich doch auf Basis der ersten Anfrage übermitteln müsste.

Ergänzend erfolgt in Absatz 1 die Klarstellung, dass Protokollierungsverpflichtungen nur dann ausgelöst werden, wenn eine Anfrage über Vorratsdaten erfolgt, die auch einen Zugriff auf (potentiell vorhandene) Vorratsdaten beim Anbieter auslöst, weil es ansonsten in der Statistik auch keine sinnvolle Auswertung zu negativen Beantwortungen geben würde. Wenn beim Anbieter nicht einmal zur Nachschau auf die Vorratsdatenbank zugegriffen wird, etwa weil aufgrund der internen Betriebsdaten-Richtlinie klar ist, dass alle angeforderten Daten noch in den betrieblichen Systemen vorhanden sind, würde ein Protokollierung als Fall der Verwendung von Vorratsdaten nur die Statistik verfälschen. D.h. eine Anfrage nach § 135 Abs. 2a StPO soll nur dann von der Protokollierung erfasst sein, wenn der Anbieter diese nicht allein durch Abfrage der betriebsnotwendigen Daten beantworten kann, sondern tatsächlich gezielt zusätzlich Vorratsdaten abfragen muss. Umgekehrt reicht allerdings schon aus, dass der Anbieter eine Abfrage in der Vorratsdatenbank vornehmen muss, um die Protokollierungspflicht auszulösen, auch wenn diese Abfrage zu keinem Ergebnis führt. Dieser Fall muss in die Statistik als erfolglose Anfrage nach Vorratsdaten Eingang finden.

Zu § 6 Abs. 2:

Aus Sicht der anfrageberechtigten Behörden, Staatsanwaltschaften und Gerichte ist eine Information darüber, ob die abzufragenden Daten betriebsnotwendige Daten oder Vorratsdaten sind, erforderlich. Daher ist hier die Frage relevant, wann einem Datum (besser: einem Datensatz) die rechtliche Qualifikation als „Vorratsdatum" zukommt. An diese Qualifikation sind nämlich in weiterer Folge erhöhte Konsequenzen im Rechtsschutz geknüpft, beispielsweise die verpflichtende Information der Betroffenen bei Auskünften nach SPG, sowie die besonderen Zugriffs- und Protokollierungsbestimmungen beim Anbieter intern. Für diese Qualifikation findet sich eine Erklärung in den Erläuterungen (GP XXIV, Nr. 1074, 1. Absatz zu § 92 Abs 3 Z 6b TKG 2003): „Bei der Beurteilung, ob es sich bei einem Datum um ein Vorratsdatum handelt, ist vielmehr darauf abzustellen, ob es von Anbietern der in § 102a genannten Dienste ausschließlich aufgrund der Speicherverpflichtung des § 102a gesammelt bzw. gespeichert wird. Dabei ist zu beachten, dass auch beim Anbieter zunächst zu anderen Zwecken vorhandene Daten zu Vorratsdaten werden können, wenn alle anderen zulässigen Speicherzwecke (insbesondere die Betriebsnotwendigkeit der Speicherung) wegfallen. Die Einordnung der Daten als Vorratsdaten ist also durch den Zweck determiniert, zu dem die Daten gespeichert werden (dürfen)." Nach der Legaldefinition in § 134 Z 2a StPO ist eine Auskunft über Vorratsdaten, „die Erteilung einer Auskunft über Daten, die Anbieter von öffentlichen Kommunikationsdiensten nach

Maßgabe des § 102a Abs. 2 bis 4 TKG 2003 zu speichern haben, und die nicht nach § 99 Abs. 2 TKG 2003 einer Auskunft nach Z 2 (Anm.: „Auskunft über Daten einer Nachrichtenübermittlung") unterliegen."

Für Anfragen, die nicht zwischen Vorratsdaten und betriebsnotwendigen Daten unterscheiden (z.B. nach § 53 Abs. 3a und 3b SPG), muss die Information übermittelt werden, ob Vorratsdaten für die Beantwortung dieser Anfrage verwendet wurden. Umgekehrt kann es sein, dass Anfragen der Staatsanwaltschaft zunächst auf Vorratsdaten gemäß § 135 Abs. 2a StPO gerichtet sind, aufgrund des in Absatz 1 normierten zulässigen Größenschlusses aber tatsächlich keine Vorratsdaten übermittelt werden. In diesen Fällen ist ebenfalls relevant, ob Vorratsdaten verwendet wurden, weil davon die Befassung des Rechtsschutzbeauftragten der Justiz abhängt. Aus diesen Gründen hat der Anbieter bei jeder Übermittlung von Vorratsdaten diesen Umstand als Zusatzinformation (gemäß Anlage, Kapitel 1.4) über die DLS zu übermitteln.

Zu § 6 Abs. 3:

Zu unterscheiden von der rechtlichen Qualifikation als „Vorratsdatum" ist die Frage nach dem Zeitpunkt der Vorratsspeicherung und der Datenhaltung in der „Vorratsdatenbank". Hier ist zunächst das Doppelspeicherungsverbot für Vorratsdaten zu beachten. Ein solches ist zwar im normativen Teil der EU-Richtlinie 2006/24/EG nicht ausdrücklich enthalten. Allerdings enthält Erwägungsgrund 13 der RL die Vorgabe: „Die Vorratsspeicherung von Daten sollte so erfolgen, dass vermieden wird, dass Daten mehr als einmal auf Vorrat gespeichert werden." Das heißt aber nicht, dass eine gleichzeitige Speicherung von Daten als Betriebsdaten und Vorratsdaten dadurch ausgeschlossen ist. Eine gleichzeitige Speicherung von Daten sowohl in der Vorratsdatenbank als auch in den betrieblichen Datenbanken der Anbieter kann die operative Abwicklung für die Anbieter erleichtern. Die Anbieter könnten nämlich alle Daten schon bei der ersten Verarbeitung aus dem Live-System „abgreifen" und in die Vorratsdatenbank überführen. Aus den betrieblichen Datenbanken müssen die Daten dann gelöscht werden, sobald die betriebliche Notwendigkeit nicht mehr gegeben ist.

Dazu normiert § 92 Abs. 3 Z 6b des TKG 2003: "Vorratsdaten sind Daten, die ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a gespeichert werden." Für die Beurteilung der Rechtmäßigkeit der in Absatz 3 vorgeschlagenen (nicht verpflichtenden) Zulässigkeit zur gleichzeitigen Speicherung von Betriebsdaten in der Vorratsdatenbank geht es dabei vor allem um die Auslegung des Begriffes "ausschließlich", der aus der Perspektive der Vorratsdatenbank zu verstehen ist. Daten in dieser Datenbank dienen allein dem in § 102a Abs 1 TKG 2003 normierten (und eingeschränkt von § 99 Abs. 5 TKG 2003 mit Ausnahmen durchbrochenen) Zweck der „Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs. 2a StPO rechtfertigt." Zugriffe auf diese Datenbank sind stets nur unter den strengeren Voraussetzungen der §§ 102b und 102c TKG 2003 zulässig, selbst wenn diese Daten zugleich im betrieblichen System des Anbieters vorhanden sind. Insofern wären die Daten in dieser Datenbank – auch bei gleichzeitiger Speicherung in den betrieblichen Systemen des Anbieters – tatsächlich „ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a" gespeichert. Diese Datenbank würde ab dem Ende der Kommunikation stets alle Daten enthalten, die für Auskünfte gegenüber den berechtigten Behörden, Staatsanwaltschaften und Gerichten zur Verfügung stehen müssen. Dies geht konform mit der Formulierung in § 102a Abs. 1 TKG 2003, derzufolge „nach Maßgabe der Abs. 2 bis 4 Daten ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern" sind.

Außerdem findet sich in den Erläuterungen zur Regierungsvorlage dazu (GP XXIV, Nr. 1074, 2. Absatz zu § 92 Abs. 3 Z 6b TKG 2003): „Der Begriff „Vorratsdaten" verdeutlicht explizit, dass die Speicherung der Daten für die in § 102a Abs. 1 festgelegte Dauer ab ihrer Entstehung deshalb flächendeckend und vorrätig erfolgt, damit sie später den Strafverfolgungsbehörden zur Verfügung stehen, falls die Auskunft zu bestimmten Daten einer Nachrichtenübermittlung in einem bestimmten Verfahren zur Ermittlung, Feststellung und Verfolgung einer bestimmten Straftat, deren Schwere eine Auskunft nach § 135 Abs. 2a rechtfertigt, notwendig ist."

Festzuhalten ist, dass die Zulässigkeit einer sofortigen Speicherung in der Vorratsdatenbank keine Nachteile im Hinblick auf das Schutzniveau nach sich zieht. Vielmehr hätte es Vorteile aus der Sicht des Rechtsschutzes, wenn Auskunftsbegehren beim Anbieter grundsätzlich unter Zugriff auf die Vorratsdatenbank abgewickelt würden, weil dort (im Gegensatz zu den betrieblichen Systemen) ein Zugriff stets nur nach dem Vier-Augen-Prinzip unter revisionssicherer Protokollierung erfolgen darf – auch wenn die Daten zugleich noch in den betrieblichen Systemen des Anbieters vorhanden sein sollten.

Falls Daten, die also auch in den betrieblichen Systemen des Anbieters noch vorhanden sind, beauskunftet werden, muss dies für die Richtigkeit der Statistik sowie allfällige prozedurale Folgen (Informationspflicht nach SPG) in der Vorratsdatenbank jeweils markiert sein. Auskunftsbeantwortungen

könnten dann immer einheitlich über den (protokollierten) Zugriff auf diese Datenbank abgewickelt werden. Der Anbieter muss dann aber jedenfalls in der Vorratsdatenbank über ein „Flag" pro Datensatz (unterschieden nach den Datenkategorien des § 102a Abs 2 bis 4 TKG 2003) markieren, ob das Datum zugleich noch im betrieblichen System vorhanden ist oder nicht. Bei der Löschung im betrieblichen System müsste dieses „Flag" dann den Status ändern. Diese Information in der Datenbank (zB: Vorratsdatum J/N) muss dann auch bei der Übermittlung der Antwort zu einem Auskunftsbegehren für die Statistik und zur Kenntnis der Behörden Staatsanwaltschaften und Gerichten mitgeliefert werden (siehe Absatz 2). Sollte ein Auskunftsbegehren nur die Übermittlung von betriebsnotwendigen Daten, nicht aber die Übermittlung von Vorratsdaten erlauben, wäre die Auskunft aus der Vorratsdatenbank nur zulässig, wenn markiert ist, dass die Daten auch in den betrieblichen Systemen noch vorhanden sind.

Zu bemerken ist, dass die durch Absatz 3 eröffnete Möglichkeit in der Praxis nicht von allzu großer Bedeutung sein wird. Die ursprüngliche Intention dieser Möglichkeit aus den Diskussionen zur Umsetzung lag nämlich in der Absicherung, dass Anfragen auf Vorratsdaten auf jeden Fall (wenn überhaupt Daten vorhanden sind) erfolgreich sind, auch wenn dafür Betriebsdaten ausgewertet werden müssen. Dies wird aber nun durch die Normierung des Größenschlusses in Absatz 1 grundsätzlich klargestellt. Die Bedeutung kann aber für kleinere Anbieter bestehen bleiben, wenn gerade mit wenigen Mitarbeitern ein einheitliches Konzept für die Abwicklung von Auskünften gestaltet wird. Große Anbieter werden dies in der Praxis wohl nicht in Erwägung ziehen, weil sich ja auch der benötigte Speicherplatz im Hinblick auf noch betrieblich vorhandene Daten verdoppelt. Vielmehr wird die Abfragelogik (unter Vermeidung von Doppelspeicherung) sowohl Betriebsdaten als auch die Vorratsdatenbank abfragen – letzteres allerdings nur, wenn potentiell Daten in der Vorratsdatenbank vorhanden sein könnten.

Zu § 7 Abs. 1 und 2:

Absatz 1 und 2 dieser Bestimmung sind unmittelbar unter dem Eindruck des Urteils des deutschen Bundesverfassungsgerichts (BVerfG, 1 BvR 256/08 Urteil vom 2. März 2010) entstanden. Dort wird ausgeführt: „Wenn der Gesetzgeber eine flächendeckende Speicherung der Telekommunikationsverkehrsdaten ausnahmslos vorschreibt, gehört es zu den erforderlichen Voraussetzungen, dass die betroffenen Anbieter nicht nur ihre Pflicht zur Speicherung, sondern auch die korrespondierenden Anforderungen zur Datensicherheit erfüllen können. Anknüpfend an die sachverständigen Stellungnahmen liegt es nahe, dass nach dem gegenwärtigen Stand der Diskussion grundsätzlich eine getrennte Speicherung der Daten, eine anspruchsvolle Verschlüsselung, ein gesichertes Zugriffsregime unter der Nutzung etwa des Vier-Augen-Prinzips sowie eine revisionssichere Protokollierung sichergestellt sein müssen, um die Sicherheit der Daten verfassungsrechtlich hinreichend zu gewährleisten (1 BvR 256/08, Absatz 224). Erforderlich sind gesetzliche Regelungen, die einen solchen besonders hohen Sicherheitsstandard in qualifizierter Weise jedenfalls dem Grunde nach normenklar und verbindlich vorgeben. Dabei steht es dem Gesetzgeber frei, die technische Konkretisierung des vorgegebenen Maßstabs einer Aufsichtsbehörde anzuvertrauen. Der Gesetzgeber hat dabei jedoch sicherzustellen, dass die Entscheidung über Art und Maß der zu treffenden Schutzvorkehrungen nicht letztlich unkontrolliert in den Händen der jeweiligen Telekommunikationsanbieter liegt. Die zu stellenden Anforderungen sind entweder durch differenzierte technische Vorschriften – möglicherweise gestuft auf verschiedenen Normebenen – oder in allgemein-genereller Weise vorzugeben und dann in transparenter Weise durch verbindliche Einzelentscheidung der Aufsichtsbehörden gegenüber den einzelnen Unternehmen zu konkretisieren. Verfassungsrechtlich geboten sind weiterhin eine für die Öffentlichkeit transparente Kontrolle (...) sowie ein ausgeglichenes Sanktionensystem, das auch Verstößen gegen die Datensicherheit ein angemessenes Gewicht beimisst (1 BvR 256/08, Absatz 225)."

Diesen Anforderungen wird die österreichische Umsetzung gerecht, indem sie in § 102c TKG 2003 die Notwendigkeit der Unterscheidung von Vorratsdaten und Betriebsdaten, des Vier-Augen-Prinzips beim Zugriff sowie die revisionssichere Protokollierung solcher Zugriffe schon im Gesetz normiert, während die genaueren technischen Vorgaben mit dieser Verordnung geregelt werden. Auch was die Kontrolle durch die Datenschutzkommission betrifft, wird diese abgestufte Regelungstechnik den Anforderungen gerecht. Die für die Öffentlichkeit transparente Kontrolle wird insbesondere dadurch hergestellt, dass die statistischen Daten aus der Protokollierung über die DLS (siehe § 22) gemäß § 102c Abs. 4 TKG 2003 auch dem Nationalrat und dem Datenschutzrat zugänglich sein müssen. Was das ausgeglichene Sanktionensystem betrifft, so greifen hier die bereits bestehenden ausdifferenzierten Haftungsvorschriften des DSG 2000, insbesondere durch § 1 Abs. 5, der im Verfassungsrang die Drittwirkung des Grundrechts normiert und den Rechtsweg an die Zivilgerichte eröffnet. Das Ziel des Vier-Augen Prinzips ist, dass nicht eine einzelne Person unbemerkt und unkontrolliert auf diese Daten zugreifen kann. Der Zugriff muss dabei nicht durch zwei autorisierte Mitarbeiter des Unternehmens gleichzeitig erfolgen, die

Autorisierung durch die zweite Person kann auch nachträglich erfolgen. „Zeitnah zum Zugriff durch die erste Person" gibt dabei keine absolute Zeitschranke vor, diese Formulierung indiziert vielmehr, dass zwischen dem Zugriff und der Autorisierung des Zugriffs durch eine zweite Person nicht mehr Zeit vergeht, als im Sinne der arbeitsökonomischen Ausgestaltung der betrieblichen Abläufe noch zumutbar erscheint. Die Anbieter sind zwar nicht verpflichtet, einen „Journaldienst" zur Beantwortung von Auskunftsersuchen einzurichten, dennoch bieten in der Praxis einige (vor allem große) Anbieter die Möglichkeit, dass Anfragen außerhalb der Geschäftszeiten vor allem durch technisches Wartungspersonal rasch abgewickelt werden, wobei hier regelmäßig nur eine nachträgliche zweite Autorisierung erfolgen kann. Insgesamt muss aber jedenfalls systematisch sichergestellt sein, dass der Anbieter intern über ein effektives Kontrollsystem zur Sicherstellung der Verantwortung verfügt. Dies kann etwa dadurch erreicht werden, dass der Anbieter in kurzen Abständen eine regelmäßige Überprüfung von Zugriffen ohne zweite Autorisierung auch durch technische Ausgestaltung (zB automatische Notifikation) institutionalisiert. Die unmittelbare verfassungsrechtliche Pflicht der Provider aufgrund der Drittwirkung des § 1 Abs. 5 DSG 2000 gebietet auch eine entsprechende Dokumentation schon durch die Anbieter selbst, und nicht nur durch die Strafverfolgungsbehörden, denen die Daten im Auskunftsfall übermittelt werden.

Der Begriff der Revisionssicherheit orientiert sich dabei an den Grundsätzen einer ordnungsgemäßen Buchführung in den unternehmensrechtlichen Vorschriften (insbesondere dem UGB) und dient dem Ziel, die Nutzung nur durch Berechtigte und die Einhaltung der Verfahrensvorschriften sicherzustellen. Die Einhaltung der in Absatz 2 normierten Kriterien ist dabei durch die technische Ausgestaltung des Zugriffsregimes auf die Datenbank sicherzustellen.

Zu § 7 Abs. 3:

Der Inhalt der Protokollierung ist bereits durch § 102c Abs. 2 TKG 2003 detailliert vorgegeben und wird in dieser Verordnung einerseits zur Rechtsklarheit wiederholt, andererseits im Sinne der Eindeutigkeit der zu protokollierenden Informationen um Verweise auf Bestimmungen innerhalb der Verordnung im Zusammenhang mit der Durchlaufstelle ergänzt. Ergänzungen sind insbesondere im Hinblick auf die Erfassung von Speicherzeiträumen bzw. des Datums notwendig. So soll das Datum der Anfrage gemäß Z 3 sich auf die jeweilige Hinterlegung in der Durchlaufstellte beziehen. Diese Daten sind für den Anbieter überdies nur sehr schwer automatisiert zu erfassen (bzw. zu verpacken, da z.B. die Zustellung in das Postfach der DLS nach Erstellung des Protokollfiles beim Anbieter geschieht). Daher wird hierzu in § 23 normiert, dass diese Informationen über die DLS direkt protokolliert und an den Anbieter weitergeleitet werden. Der Anbieter kann sodann diese Protokollinformationen von der DLS für seine interne Protokollierung automatisiert weiterverwenden.

Zu Z 4 wird konkretisiert, dass das Datum zur Aufschlüsselung der abgefragten Datensätze sich auf den Beginn des Kommunikationsvorgangs bezieht, zumal dieser Wert auch im Rahmen der Vorratsdaten gemäß § 102a Abs. 2 bis 4 TKG 2003 relevant ist. Die Ergänzung zu Z 5 basiert auf dem Umstand, dass dem Anbieter nur das Datum der Anordnung gemäß § 138 Abs. 3 StPO (sog. Anbieterausfertigung) bzw. das Datum der Anordnung nach § 53 Abs. 3a oder 3b SPG bekannt ist. Für die Berechnung der Speicherdauer muss der Zeitpunkt der Anordnung der Auskunft mit dem Zeitpunkt der Speicherung als Vorratsdatensatz bzw als Betriebsdatensatz verglichen werden. Da die Anordnung nur ein Datum aber keinen genauen Zeitpunkt enthält, ist für die Berechnung auch nur das Datum der Speicherung als Vorratsdatum relevant, weshalb in Z 5 im Gegensatz zu § 102c Abs. 2 Z 5 TKG 2003 nur das Datum und nicht der Zeitpunkt genannt ist, um Klarheit für die Protokollierung zu schaffen.

Durch Z 8 soll ermöglicht werden, der Forderung von Art 10 der RL 2006/24/EG nachzukommen und auch statistische Daten über die Fälle in welchen Vorratsdaten beauskunftet werden, zu erheben. Die Angabe des zugrundeliegenden Straftatbestands soll bereits beim Auskunftsbegehren auf Seiten der Behörde bzw. der Staatsanwaltschaft oder des Gerichts eingetragen werden. Ein entsprechendes Eingabefeld dafür ist in § 19 vorgesehen, das automatische Abgreifen dieser Information über die DLS für die Statistik ist in § 23 Abs. 2 geregelt.

Zu § 8 Abs. 1:

Siehe die Ausführung zur grundsätzlichen Einigung über das System der DLS und insbesondere die Feststellungen aus dem FIT-Ausschuss bei den Erläuterungen zu § 1.

Zu § 8 Abs. 2 und 3:

Die Vorgaben zur sicheren Übertragung der Daten im Schutzbereich des Telekommunikationsgeheimnisses macht § 94 Abs. 4 TKG 2003: „Die Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, einschließlich der Übermittlung von Vorratsdaten, nach den Bestimmungen der StPO sowie des SPG, hat unter Verwendung einer Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender

und Empfänger sowie die Datenintegrität sicherstellt, zu erfolgen. Die Daten sind unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie als "Comma-Separated Value (CSV)" - Dateiformat zu übermitteln." Die Erläuternden Bemerkungen zu § 94 Abs. 4 TKG 2003 (1074 der Beilagen XXIV. GP) führen dazu aus: „Der Spielraum für eine nach dieser Bestimmung zu erlassenden Verordnung ist eng determiniert. Die technische Richtlinie soll für alle Anbieter einheitlich definieren, welche der zu beauskunftenden Werte an welcher Stelle innerhalb der CSV-Datei zu stehen haben und welche Zeichensätze dabei zu verwenden sind. Klar festgelegt ist auch, dass eine Übermittlung der Daten unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie zu erfolgen hat. Zur weiteren Verbesserung des Sicherheitsstandards kann eine asymmetrische Verschlüsselung vorgeschrieben werden. Hier sind allenfalls die näheren technischen Details zur Public Key Infrastructure zu definieren."

Unter einer anspruchsvollen Verschlüsselung ist eine Verschlüsselung zu verstehen, die nach dem derzeitigen Stand der Technik ohne erheblichen Aufwand nicht zu überwinden ist. Dabei ist durch weitere organisatorische Maßnahmen sicherzustellen, dass die Schlüssel und gegebenenfalls das Passwort ebenfalls sicher aufbewahrt werden. Absatz 2 ordnet daher ausdrücklich eine asymmetrische Verschlüsselung an. Bei einem asymmetrischen Verschlüsselungsverfahren besitzt jede der kommunizierenden Parteien ein Schlüsselpaar, das aus einem geheimen Teil (private key) und einem nicht geheimen Teil (public key) besteht. Der öffentliche Schlüssel ermöglicht es jedem, Daten für den Inhaber des privaten Schlüssels zu verschlüsseln. Die kommunizierenden Parteien müssen keinen gemeinsamen geheimen Schlüssel kennen, das Verfahren wird daher auch als Public-Key-Verfahren bezeichnet. Dafür ist eine Public-Key-Infrastruktur erforderlich, über die (vereinfacht dargestellt) die Ausstellung vertrauenswürdiger digitaler Zertifikate zur sicheren Übertragung organisiert wird. Die zentrale Herausforderung liegt darin, sicherzustellen, dass der öffentliche Schlüssel wirklich echt ist. Der Vorteil ist eine deutliche Minimierung des Sicherheitsrisikos, da jeder Benutzer nur seinen eigenen privaten Schlüssel geheim halten muss. Im Gegensatz dazu muss bei einem symmetrischen Verschlüsselungssystem jeder Teilnehmer alle Schlüssel geheim halten, was mit steigendem Aufwand verbunden ist, je mehr Teilnehmer daran beteiligt sind (große Zahl an Schlüsseln). Nachteilig ist, dass asymmetrische Kryptosysteme aufgrund der Verschlüsselungsalgorithmen im Vergleich zu den symmetrischen Verfahren eher langsam sind.

Hybride Verschlüsselungssysteme: Der Geschwindigkeitsnachteil asymmetrischer Verfahren wird in der Praxis durch die Verwendung hybrider Systeme umgangen. Dabei werden die zu übertragenden Daten mit einem zufällig generierten Schlüssel (sog. „session key") symmetrisch verschlüsselt (deutlich schneller) und der jeweils verwendete Schlüssel unter Verwendung einer asymmetrischen Verschlüsselung an die Teilnehmer verteilt. Diese Variante löst das Schlüsselverteilungsproblem und erhält dabei den Geschwindigkeitsvorteil der symmetrischen Verschlüsselung. Das Verfahren entspricht dem Stand der Technik und wird der Anforderung einer technisch anspruchsvollen Verschlüsselung jedenfalls gerecht. Es bleibt jedoch der technischen Spezifikation zur DLS vorbehalten, wie das asymmetrische Verschlüsselungsverfahren der Inhaltsverschlüsselung ausgestaltet wird.

Zu § 8 Abs. 4:

Eine wesentliche Forderung zur Datensicherheit sind die Identifikation und die Authentifizierung des jeweiligen Partners. Das Signaturgesetz kennt dazu die Funktionalität der qualifizierten Signatur, die eine Personenbindung enthält, und der fortgeschrittenen Signatur, die für Unternehmen besser geeignet ist. Das Bundesministerium für Inneres hat die fortgeschrittene Signatur im Portalverbund implementiert und verwendet diese zur Identifikation von Organisationen. Die fortgeschrittene Signatur sollte durch die begleitenden Sicherheitskriterien im Rahmen des Portalverbunds datenschutzrechtlichen Standards genügen. Generell ist es sinnvoll, den Portalverbund, das ist eine Kommunikationsplattform für Bundesdienststellen, auch für die Übermittlung von Anfragen zur Vorratsdatenspeicherung einzusetzen. Die Vorteile der DLS mit Eingliederung in den Portalverbund im Hinblick auf sichere Identifikation, Authentifizierung sowie der sicheren verschlüsselten Übermittlung von personenbezogenen Daten waren in der Diskussion von Beginn an unbestritten. Näheres dazu siehe in den Erläuterungen zu § 13.

Zu § 9:

Am 7.4.2011 wurde die TKG Novelle zur Umsetzung der Vorratsdatenspeicherung im FIT Ausschuss des Nationalrats diskutiert (siehe dazu den Ausschussbericht: 1157 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXIV. GP). In diesem Rahmen wurde von Ausschussfeststellung beschlossen, in der die grundsätzlichen Annahmen zur DLS wie folgt beschrieben werden: „Für die Datensicherheit und die Nachvollziehbarkeit der Zugriffe auf den Datenvorrat ist das Zusammenspiel der Bestimmungen der §§ 94 Abs. 4 und 102c TKG 2003 von besonderer Bedeutung. Während § 94 Abs. 4 den Aspekt der technischen Datenintegrität und der Determinierung der Verordnungsermächtigung über

die Art der Verschlüsselung betrifft und die maßgeblichen Indikatoren zur Datensicherheit bei der Übermittlung von Verkehrsdaten identifiziert, um durch sichere ‚Identifikation und Authentifizierung von Sender und Empfänger' sicherzustellen, dass die durch das Kommunikationsgeheimnis geschützten Verkehrsdaten tatsächlich nur Behörden, Staatsanwaltschaften und Gerichten zugänglich sind, denen eine gesetzliche Auskunftsbefugnis zusteht, regelt § 102c Zugriffs- und Sicherheitsbestimmungen. Einerseits muss jeder Zugriff auf Vorratsdaten durch zwei Personen mit einer besonderen Ermächtigung hierzu autorisiert sein, um zu gewährleisten, dass nicht eine einzelne Person unbemerkt und unkontrolliert auf diese Daten zugreifen kann. Andererseits müssen Zugriffe auf Vorratsdaten beim Anbieter revisionssicher protokolliert werden. Die wichtigsten Kriterien sind dabei der Schutz vor Veränderung und Verfälschung, die Vollständigkeit, die Ordnungsmäßigkeit, die Sicherung vor Verlust, die Einhaltung der Aufbewahrungsfristen sowie die Dokumentation, Nachvollziehbarkeit und Prüfbarkeit des Verfahrens, wozu etwa bei Anordnungen der Staatsanwaltschaft auch die Angabe der Geschäftszahl der ermittelnden Kriminalpolizei zählt. Der Ausschuss geht davon aus, dass sämtliche Zugriffe und Übermittlungen von wem auch immer auf Vorratsdaten gemäß § 94 Abs. 4 TKG 2003 lückenlos protokolliert werden. Der Ausschuss geht weiters davon aus, dass ein automatisches zentrales System der Protokollierung solcher Abfragen und Übermittlungen notwendig ist, wobei unter dieser Protokollierung nicht die in § 102c Abs. 2 genannte zu verstehen ist. Sie wird vielmehr nur jene Daten umfassen, die zur statistischen Auswertung und zur Verknüpfung mit der gemäß § 102c Abs. 2 erfolgenden Protokollierung dient. Wünschenswert ist die Einrichtung einer ‚Datendrehscheibe' (‚Durchlaufstelle', kurz: DLS). Da jeder Auskunftsfall über die DLS mit einer fortlaufenden einmaligen Nummer versehen wird, kann im Falle einer nachprüfenden Kontrolle über die Protokollierung bei der DLS zur Protokollierung beim Anbieter gemäß § 102c Abs. 2 verknüpft werden. Zugang zu den übermittelten personenbezogenen Daten soll die DLS selbst nicht bieten, die Daten liegen dort nur verschlüsselt bis zur Abholung bereit und werden bei der Abholung automatisch gelöscht."

Die Abwicklung der Anfragen und Auskünfte soll über die DLS erleichtert werden, insbesondere die Einbindung über den Portalverbund bringt Synergie-Effekte, weil damit auf Seiten des BMI bereits gute Erfahrungen bestehen. Die DLS ist zugleich die ökonomischste Art der Umsetzung, weil eine sichere Anbindung unter Transport- und Inhaltsverschlüsselung zwischen voraussichtlich 15 anfrageberechtigten Behörden und ca. 200 speicher- und auskunftspflichtigen Anbietern (nach aktuellen Angaben der RTR) über eine zentrale Lösung beim Datenaustausch wesentlich einfacher zu garantieren ist als bei einer dezentralen Kommunikation, zB per E-Mail. Mit der zentralen Lösung der DLS werden sowohl das Fehler- als auch das Sicherheitsrisiko minimiert.

Zu § 10:

Dass das BMVIT die Verantwortung für den Betrieb der Durchlaufstelle übernimmt, ist die sauberste Lösung für die datenschutzrechtlichen Problemstellungen, die mit der zentralen Abwicklung aller Datenauskünfte nach § 94 Abs. 4 TKG 2003 verbunden sind. Der Vorschlag, den Betrieb der DLS und die Beauftragung zur technischen Spezifikation und Umsetzung durch das BMVIT durchzuführen, hat den Grund, dass damit die Bedarfsträger vom Auftraggeber getrennt werden. Weil dem BMVIT keine Aufgaben obliegen, für die eine Verarbeitung von Vorratsdaten notwendig wäre, ist es eine neutrale Stelle ohne eigenes Interesse an den zu übermittelnden Inhalten. Das Interesse des BMVIT am Betrieb der DLS ist darin zu sehen, dass diesem Bundesministerium obliegt, über die Einhaltung der Bestimmungen des TKG 2003 zu wachen, wozu insbesondere auch das Kommunikationsgeheimnis des § 93 TKG 2003 zählt.

Durch die Eigenschaft als Auftraggeber der DLS wird das BMVIT jedoch nicht zum datenschutzrechtlichen Auftraggeber im Hinblick auf die übermittelten Daten. Einerseits besteht nämlich die „Dienstleistung" der DLS nur darin, allen Beteiligten Postfächern für den Datenaustausch zu bieten und bestimmte Aufgaben zur sicheren Übertragung der Daten zu übernehmen. Darüber hinaus müssen die Daten auf eine Weise verschlüsselt werden, dass die DLS gar keine Möglichkeit hat, die Inhalte einzusehen. Die Protokollierung der DLS beinhaltet rein statistische Werte ohne Personenbezug. Die fortlaufende einmalige Nummer jedes Auskunftsvorgang („Unique ID") kann lediglich eine nachprüfende Kontrolle (zB durch Datenschutzkommission, Rechtsschutzbeauftragten oder Gericht) erleichtern, der Personenbezug kann aber über die DLS selbst nicht hergestellt werden.

Nur in einer einzigen Hinsicht ist das BMVIT als datenschutzrechtlich verantwortlicher Auftraggeber zu sehen, nämlich in Bezug auf die Verarbeitung der Information, welche Benutzer überhaupt Auskunftsbegehren über die DLS abwickeln. Ansonsten sind alle personenbezogenen Informationen in der DLS nur verschlüsselt vorhanden, damit sind sie aus der Perspektive der DLS nur indirekt personenbezogen.

Das Bundesrechenzentrum ist überhaupt funktionell Dienstleister im Sinne des § 4 Z 5 DSG, dies jeweils für den Auftraggeber, für dessen Anwendung Daten an die DLS übergeben oder von der DLS übernommen werden. Das heißt, wenn die DLS beispielsweise eine Anordnung der Staatsanwaltschaft in das Postfach des Anbieters zustellt, geschieht dies im Dienst der Behörde, Staatsanwaltschaft oder des Gerichts, von welcher/m die Anordnung stammt. Die Stellung eines datenschutzrechtlichen Auftraggebers kommt dem Bundesrechenzentrum im Hinblick auf den Betrieb der DLS in keiner Phase zu.

Zu § 11:

Die Auditierung betrifft nur die Datensicherheit bei der Durchlaufstelle, nicht aber die Anbieterimplementierungen. Siehe ansonsten die Erläuterungen zu § 18.

Zu § 12:

Die DLS ist ein Modell für technische und prozedurale Abläufe, nicht jedoch eine Art neue Behörde oder Dienststelle. Hierfür muss sich in einer sicheren öffentlichen Infrastruktur (wie jener des Bundesrechenzentrum) ein Server befinden, über den - technisch gesehen - die Anfragen abgewickelt werden. Eine Kommunikation über diesen Server ist dabei nur möglich, wenn die entsprechenden Stellen über eine Berechtigung (Authentifizierung) verfügen.

Für die Ausführung der Mailbox-Funktion der DLS kann es vorteilhaft sein, Webapplikationen und Webservices technisch zu kombinieren, da ein Webservice von der Clientseite flexibel angesprochen werden könnte und somit ein höheres Maß an Benutzerkomfort durch Ausgestaltung des Clients auf der jeweiligen Teilnehmerseite (Behörden oder Anbieter) gestaltbar wäre.

Zu § 13:

Die Unique-ID erfüllt die zentrale Funktion, zusammengehörige Transaktionen zu korrelieren, wobei jede spezifische Behördenanfrage an einen bestimmten Anbieter eine Transaktion darstellt. Beispiel: Eine Anfrage ergeht an zwei Anbieter. Die Unique-ID könnte aus einem einmaligen „Anfrageteil" sowie einer Anbieter-ID bestehen (1234567-1, 1234567-2); alternativ müsste es eine eigene ID zu dieser Anfrage für jeden Anbieter geben (1234567, 1234568). Die konkrete Ausgestaltung ist in der technischen Spezifikation zur DLS zu klären.

Von Seiten des BMJ wurde in der Diskussion die Anforderung formuliert, dass lückenlos nachvollziehbar sein muss, welche Personen von Anfang bis Ende an einem Auskunftsvorgang beteiligt waren, um allfälligem Missbrauch effektiv begegnen zu können. Die sichere Anbindung der Behördenseite über den Portalverbund bietet sich dabei an, weil hierzu beim Bundesrechenzentrum bereits die vollständige Infrastruktur und ein reicher Erfahrungsschatz besteht. Für die Seite der Anbieter ist ein Portal zu schaffen, dass dem Portalverbund der Behörden nachgebildet ist und denselben Sicherheitsanforderungen entspricht. Auch hierzu besteht beim bereits ein großer Erfahrungsschatz, etwa aus der Realisierung des Elektronischen Rechtsverkehrs (ERV) für die Kommunikation zwischen Gerichten und professionellen Parteienvertretern (Rechtsanwälte, Notare).

Das Prozedere der internen Authentifizierung zur Sicherstellung der konkreten Berechtigung der handelnden Personen muss klar geordnet sein, kann aber im Konzept des Portalverbunds auch intern bei der jeweiligen Organisation (Behörden- oder Anbieterseite) erfolgen und muss nicht zwingend über die DLS technisch realisiert werden, sofern die Anforderungen der Sicherheitsklasse 3 des Portalverbunds erreicht werden; Im Detail vgl. "Spezifikation Sicherheitklassen für den Zugriff von Benutzern auf Anwendungen", Version 2.1.0, 8.2.2008, ["SecClass 2.1.0"; Anhang zur Portalverbundvereinbarung pvv 1.0, 21.11.2002]. Es sind die Konventionen des Portalverbunds einzuhalten, wobei die Bundesrechenzentrum GmbH Teilnehmer am Portalverbund ist. Die Stammportale werden von den einzelnen Institutionen betrieben (oder von deren Dienstleistern).

Der Portalverbund Österreich ist eine E-Government Anwendung und wird auf der Website „Digitales Österreich" (http://www.digitales.oesterreich.gv.at/site/5288/default.aspx) wie folgt beschrieben: „Der Portalverbund ist ein Zusammenschluss von Verwaltungsportalen zur gemeinsamen Nutzung von bestehender Infrastruktur. Grundsätzlich haben Portale den Vorteil, dass mehrere Applikationen über einen Punkt zugänglich werden. Die Identität der Benutzenden wird im Zuge des Anmeldevorganges am Portal nur einmal überprüft. Die Benutzenden müssen sich daher nur einmal "ausweisen" um auf mehrere Ressourcen zugreifen zu können. Betreibenden von Anwendungen wird es im Portalverbund ermöglicht, die Authentifizierung und Autorisierung zu Portalen in Vertrauensstellung auszulagern. Anstelle einer eigenen Benutzerverwaltung für jede Anwendung wird nur mehr eine Benutzerverwaltung am Stammportal benötigt. Dadurch wird die Benutzerverwaltung vereinfacht und ein Single Sign-On unterstützt. Die Benutzerverwaltung bleibt technisch und organisatorisch weiterhin im Verantwortungsbereich der personalführenden Stelle. Organisationen, die am Portalverbund teilnehmen,

können ihre lokale Benutzerverwaltung nicht nur für interne Anwendungen, sondern auch für externe Applikationen und Anwendungen verwenden. Betreiber von Applikationsportalen bleibt somit die externe Benutzerverwaltung erspart.

Die Teilnahme am Portalverbund wird durch die Portalverbundvereinbarung geregelt. Diese enthält Rechte und Pflichten, die von den teilnehmenden Portalbetreibenden einzuhalten sind. Zwischen den Betreibenden von Stammportalen, welche die Benutzenden verwalten und Anwendungsbetreibenden wird so ein Vertrauensverhältnis hergestellt. Alle Vereinbarungen werden bei einem Depositar, das ist jenes Bundesministerium, das für die IT-Koordination des Bundes zuständig ist, aufbewahrt. Technisch und organisatorisch ist die Kommunikation im Portalverbund durch das Portalverbundprotokoll (PVP) und durch die Festlegung von Sicherheitsklassen geregelt. Die Definition von Sicherheitsklassen im Portalverbund ermöglicht es einer Anwendung zu prüfen, ob Benutzende die für die Nutzung der Anwendungsfunktion erforderlichen Sicherheitsauflagen erfüllen. Für Mitarbeitende von Institutionen, die am Portalverbund teilnehmen, ergeben sich keine Veränderungen.

Der Betreibende von Anwendungen bestimmt, welche Anwendungen über welches Anwendungsportal zugänglich sind. Der Betreibende legt unter Beachtung sämtlicher Datenschutzbestimmungen fest, welche Stellen beziehungsweise Kategorien von Stellen über ein Anwendungsportal zugriffsberechtigt sind und definiert für seine Anwendungen je nach Aufgabenstellungen der Benutzenden Rollen mit entsprechenden Rechteprofilen. Der Stammportalbetreibende muss unter anderem sicherstellen, dass über das eigene Portal nur berechtigte Benutzende ordnungsgemäß auf Anwendungen zugreifen. Der Anwendungsportalbetreiber muss sicherstellen, dass nur über ein Stammportal autorisierte Benutzende auf die durch das Portal erreichbaren Datenanwendungen zugreifen können. Die Übereinstimmung des Rechteprofils der Benutzenden mit den Zuständigkeiten der zugriffsberechtigten Stelle muss geprüft werden. Erforderliche Datensicherheitsmaßnahmen sind ebenfalls zu organisieren und umzusetzen. Betreiber von Stammportalen können sich für den technischen Betrieb eines Dienstleistenden bedienen. In diesem Fall ist vom Dienstleistenden eine Vereinbarung zu unterzeichnen, die gewährleistet, dass auch dieser alle technischen und organisatorischen Vorkehrungen einhält, auf denen das Vertrauensverhältnis der Portalverbund-Teilnehmenden beruht."

Zu § 14:

Die Anzahl der zugangsberechtigen Dienststellen der Sicherheitsbehörden wird durch Erlass der Bundesministerin für Inneres festgelegt jener im Bereich der Justizbehörden wird durch das Bundesministerium für Justiz festgelegt und der Bundesrechenzentrum GmbH für die Spezifikation der Durchlaufstelle bekanntgegeben.

Zu § 15:

Ein wesentlicher Vorteil des Konzepts der DLS ist die Verringerung der Kommunikationswege. In den Diskussionen ging man von 15 anfrageberechtigten Behörden und 200 auskunftspflichtigen Netzen (alle die der Verpflichtung zur Entrichtung des Finanzierungsbeitrages zur RTR unterliegen) aus. Insbesondere kleinere Anbieter haben geringere Ressourcen. Daher ist es die effizienteste Vorgangsweise, nur mit einer Stelle zu kommunizieren. Spezielle technische Voraussetzungen auf Anbieterseite sind keine nötig, da die DLS über eine sichere Verbindung (die wahrscheinlich über das Protokoll „https" realisiert werden wird) praktisch mit jedem gängigen Browserprogramm erreichbar wäre. In welchem Ausmaß ein Anbieter seine Prozesse bis zur Erstellung des „CSV-Files" mit den begehrten Daten automatisiert, bleibt ihm selbst überlassen, was insbesondere für kleinere Anbieter wichtig ist, bei denen eine teure Automatisierung in keinem Verhältnis zur Zahl der jährlichen Auskünfte steht.

Zu § 16:

Bei der Anbindung der Anbieter ist sicherzustellen, dass auf Anbieterseite möglichst flexibel auf die DLS zugegriffen werden kann, damit auch außerhalb der Geschäftszeiten eine möglichst rasche Beantwortung des Auskunftsbegehrens erfolgen kann.

Die Sicherheitsstufe 3 aus der "Definition der Sicherheitsstufen in der Kommunikation Bürger – Behörde im Bereich E-Government" ist abrufbar unter http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=21832 und dort wie folgt beschrieben:

„Die höchste Sicherheitsstufe im Bereich E-Government, die auch für die Kommunikation Verwaltung – Verwaltung angewandt werden kann, wenn dies die Vertraulichkeit erfordert, wurde darauf ausgelegt, dass sie kompromittierten Endgeräten stand hält. Bei Anwendung dieser Sicherheitsstufe haben Client und Server Klarheit darüber, wer kommuniziert und können auch von der Vertraulichkeit im Rahmen der Sicherheit der kryptographischen Schlüssel und Algorithmen ausgehen.

Die Sicherheit wird mit einer TLS-Verbindung erreicht und basiert auf Zertifikaten mit Verwaltungseigenschaft. Die Bindung der Zertifikate an Client und Server ist technisch so abzusichern,

dass sie auch kompromittierten Endsystemen standhält. Die für den Ablauf notwendigen Zertifikate werden direkt vom Server bzw. Client in die sichere TLS-Verbindung eingebunden. Es wird somit, anders als bei Stufe II, eine automatische und in die Verbindungsprotokolle integrierte Überprüfung der Serveridentität möglich. Dieser Mechanismus kann nun auch automatisch man-in-the-middle Attacken erkennen.

Die Zertifikate des Clients und des Serves der TLS-Verbindung werden in vertrauenswürdigen Komponenten gehalten und sind technisch vor Modikation geschützt. Dies kann zum Beispiel durch den Einsatz von hardware security modules (HSM), auch Kryptoboxen genannt, erreicht werden. Diese Sicherheitsmodule sind in verschiedenen Formaten (Box, Tischgerät, PC-Karte, Chipkarte) erhältlich und werden in der Regel als interne Karten, als periphere Geräte oder über einen Adapter (für die Chipkarte) an den Hostrechner (Zentralrechner, Server, PCs) angeschlossen. Eine weitere Möglichkeit zur Absicherung besteht im Schaffen einer vertrauenswürdigen Softwareumgebung, unter anderem mit sicherem boot - Prozess, zuverlässigem Betriebssystem und digital signierter Software. Diese Sicherheitsstufe ist für Transaktionen mit sensiblen Daten nach dem Datenschutzgesetz geeignet (analog Sicherheitsklasse 3 im Portalverbund)."

Zu § 17:

Die in § 17 klar vorgezeichneten Abläufe der Zustellung von Auskunftsbegehren und Antworten in die Postfächer der jeweils Beteiligten sind zentral für die Architektur der DLS und erfüllen auch eine wesentliche datenschutzrechtliche Funktion. Damit ist nämlich auch von der technischen Konzeption her eindeutig, dass die Auskunft über Daten, die vom Schutzbereich des DSG 2000 und des Kommunikationsgeheimnisses des § 93 TKG 2003 erfasst sind, immer in Form eines „push" aus der Sicht des Anbieters erfolgt. Lediglich die Abholung der Anordnung durch den Anbieter einerseits und die Abholung der Antwort durch die Behörde andererseits kann durch den Einsatz von Webservices teilautomatisiert werden. Dadurch entsteht aber keine vollautomatisierte Schnittstelle mit unmittelbarem Zugriff der Behörden auf die Datenbanken der Anbieter. Die Mediatisierung über die DLS als Postfachsystem stellt eine faktisch effektive Begrenzung der staatlichen Kontrollmacht dar.

Zu § 18:

Die fortgeschrittene Signatur stellt die praktikabelste Lösung dar und beinhaltet die Möglichkeit eines Zertifikats auf Unternehmensbasis. Die Zuordnung zu Einzelpersonen ist in den Protokolldateien ersichtlich und muss daher nicht unbedingt durch die Signatur erfolgen. Durch die Signatur wird auch ein Hashwert zur Wahrung der Datenintegrität überflüssig. Mit der Signatur kann im Gegensatz zum bloßen Hashwert auch die Identität des Signators überprüft werden. Man weiß dann nicht nur, dass die Daten korrekt sind, sondern dass sie auch tatsächlich vom Signator stammen. Bei der Verwendung eines bloßen Hashwerts könnte ein „Man-In-The-Middle" die Nachricht und den Hash abfangen, beides ändern, und die geänderten Versionen der Nachricht und des Hashwerts weiterschicken. Hashwerte (in diesem Kontext) alleine schützen nur vor zufälligen Veränderungen, Signaturen auch vor absichtlichen Manipulationen.

Für die verschlüsselte Übermittlung von Auskunftsdaten wird der öffentliche Schlüssel (auch: public key) des jeweiligen Empfängers verwendet. Nur dieser kann dann mit seinem private Schlüssel (auch: private key) die Auskunft im Klartext lesen. Die bei der DLS angesiedelte Aufgabe der Schlüsselverwaltung bedeutet, dass die öffentlichen Schlüssel zur Verschlüsselung der Daten am DLS-Server technisch gesehen durch sog. „Zertifikate" hinterlegt werden. Die Verschlüsselung der Anfrage und der Antwort kann nur bei der Behörde bzw. beim Anbieter stattfinden. Für die Verschlüsselung wird der „private key" benötigt und dieser kann niemals von der DLS erzeugt oder gespeichert werden. Die DLS ist nur für die Transportverschlüsselung zuständig und kennt natürlich die dafür notwendigen Schlüssel.

Zu § 19:

Im Zuge der Diskussion zum zeitlichen und finanziellen Rahmen der Umsetzung eines Datensicherheitskonzepts wurde die so genannte "Implementierung Light" der Durchlaufstelle diskutiert. Darunter sind jene Änderungen im Konzept zu verstehen, die sich seit der ersten Vorstellung des Konzepts der Durchlaufstelle aus der Diskussion ergeben haben. Dazu gehört einerseits die Implementierung im Rahmen des Portalverbundes. Damit kann die interministerielle Seite und die Anbieterseite der Implementierung getrennt werden. Für die Spezifikation und Implementierung der interministeriellen Seite ist keine Einbindung der Netzbetreiber mehr erforderlich. Die zweite Eigenschaft der "Durchlaufstelle Light" betrifft die Formalisierung der Anfragen. Für Anfragen nach dem SPG ist heute bereits eine Verwendung von normierten Formularen gemäß Erlass des BIM vorgesehen. Bei Anfragen nach der StPO gibt es zwar Formulare, denen jedoch kein zwingender Erlass zugrunde liegt und die in der Praxis auch nicht durchgehend verwendet werden. Anfragen nach der StPO enthalten als Beilage die Anordnung des Staatsanwalts mit der prosaischen Beschreibung des Auskunftsbegehrens.

Mittelfristig wurde in der Diskussion das Ziel formuliert, auch für Datenanfragen nach der StPO eine Formalisierung über Eingabemasken zu erreichen. Es sollte allerdings zugleich verhindert werden, dass Anbieter durch den Vergleich einer allenfalls per Webmaske ausgeführten Anordnung mit dem beiliegenden Original der StA Anordnung einen erhöhten Aufwand haben. Zur Optimierung der Betriebsabläufe ist jedenfalls ein Rückkanal vorzusehen. Das heißt etwa, dass bei Differenzen zwischen den begehrten Daten und der beiliegenden Anordnung der StA eine Antwort an die abfrageberechtigte Stelle zu schicken ist, mit der darauf hingewiesen wird, dass diese Fehler zu korrigieren sind. Zu diesem Zweck regelt die Verordnung in § 20 die Möglichkeit von „Zusatzinformationen". Für die Implementierung der Durchlaufstelle bedeutet dies, dass in der Phase der ersten Implementierung jedenfalls StPO-Anordnungen übermittelt werden können müssen, ohne dabei an bestimmte online-Formulare über die Webmaske gebunden zu sein.

Zusammengefasst bedeutet das:

Die DLS ist zwingend die Drehscheibe zur Kommunikation für alle Auskunftsfälle. Kern ist dabei, dass die jeweilige Seite ihre Anforderung/Antwort sicher über die DLS samt dem notwendigen Anhang (Anbieter-Anordnung nach § 139 Abs. 3 StPO, CSV-Datei mit den begehrten Daten) übermittelt.

Die Spezifikation der DLS muss jedoch nicht enthalten, wie auf Seiten der Behörden die jeweiligen Web-Formulare aussehen. Eine Formalisierung wird jedoch auf Behördenseite aus eigenem Interesse einer einheitlichen und geordneten Abwicklung angestrebt.

Auch auf der Seite der Anbieter muss nicht spezifiziert werden, ob, inwieweit und wie die Beantwortung von Auskunftsbegehren (teil-)automatisiert wird. Durch die Anlage zu dieser Verordnung wird einheitlich festgelegt, wie die CSV-Datei aussehen muss. Wie die einzelnen Anbieter diese Datei „befüllen" bleibt deren Entscheidung.

Der Vorschlag enthält lediglich, dass bei der Übermittlung eines Auskunftsbegehrens via DLS ausgewählt werden muss, auf welcher Rechtsgrundlage die Anordnung ergeht. Dies dient der statistischen Erfassung über die DLS und beinhaltet keine Determinierung der Formulare oder Webmasken, die bei den Behörden für die Anordnungen verwendet werden. Eine Determinierung ergibt sich allerdings aus der Spezifikation der Felder der CSV-Datei gemäß dem Vorschlag in der Anlage.

Zu § 20:

Die CSV-Dateien werden mittels sicherem Filetransfer und Inhaltsverschlüsselt an die Durchlaufstelle übermittelt. Zusatzinformationen könnten allenfalls über ein Web-Interface zu der entsprechenden Abfrage eingegeben werden. Diese Zusatzinformationen könnten etwa Gründe für eine Leer-Meldung beschreiben. Ob und in welchem Ausmaß ein Web-Interface auf Seiten der DLS zur Verfügung gestellt werden soll, wird Gegenstand der Diskussion zur Spezifikation der DLS sein. Jedenfalls ist dabei zu bedenken, dass die DLS gegenüber Inhalten der Auskünfte "blind" sein soll, personenbezogene Informationen sollten also nicht als Zusatzinformation übermittelt werden, weil diese gegenüber der DLS nicht inhaltsverschlüsselt werden, sondern nur durch die Transportverschlüsselung vor Zugriffen von außen sicher sind. Alternativ ist auch möglich nach dem sonstigen Aufbau der EP 020 die möglichen Dateiformate und Dateinamen für Zusatzinformationen zu definieren. Auf diese Weise könnten auch personenbezogene Zusatzinformationen mit Inhaltsverschlüsselung übertragen werden, die aus Sicht der DLS nicht zugänglich sind. Für Anfragen, die nicht zwischen Vorratsdaten und betriebsnotwendigen Daten unterscheiden (z.B. nach § 53 Abs. 3a und 3b SPG) muss jedenfalls die Information übermittelt werden, ob Vorratsdaten für die Beantwortung dieser Anfrage verwendet wurden. Diese Information wird von den Anbietern als "Zusatzinformation" übermittelt (siehe § 6 Abs. 2).

Allenfalls könnte für die Übertragung von Zusatzinformationen eine Textdatei (.doc/.txt) zum Einsatz kommen, welches leicht wie eine "reale Antwort" mit dem Schlüssel der Behörde verschlüsselt wird. In diesem Fall hier wäre die Benennung dieser Datei in der Spezifikation zur DLS zu regeln.

Zu § 21:

In den Grundsatzdiskussionen zur DLS wurde die Möglichkeit einer elektronischen Stammdatenauskunft im Bereich der Telefon-Anbieter als optionale Variante besprochen. Festgehalten wird aus dieser Diskussion, dass es aus Sicht des BMI nicht darum geht, eine unmittelbare Schnittstelle zur Kundendatenbank des Anbieters herzustellen. Vielmehr besteht der Wunsch nach einem elektronischen Hin- und Rückkanal, der zu einer möglichst raschen Abwicklung führt. In wie weit ein Anbieter solche Auskunftsvorgänge automatisiert, soll dem jeweiligen Anbieter überlassen bleiben - insbesondere im Hinblick auf kleine Anbieter, die nur wenig betroffen sind - solange die Auskunft in vertretbarer Zeit abgewickelt werden kann. Große Anbieter könnten durch eine (Teil-)Automatisierung in eigener Verantwortung die Auskünfte optimieren. Wesentlich ist, dass eine Anbindung an ein elektronisches System für Stammdatenauskünfte über die DLS nicht gesetzlich verpflichtend als ausschließliche

Übermittlungsvariante für alle Anbieter eingerichtet werden muss. Durch die Verordnung soll lediglich die optionale Möglichkeit einer solchen Anbindung normiert werden. Wenn zumindest die großen (insbesondere Mobilfunk-) Anbieter sich anschließen, würde der Zweck erfüllt.

In einer solchen Anfrage würde eine Rufnummer übermittelt. Dazu sind vom Anbieter die zugehörigen Stammdaten für den Anfragezeitraum, längstens aber 6 Monate zurück, zu ergänzen. In der bisherigen Praxis werden vor einer Anordnung zu einer Verkehrsdatenauskunft zunächst zu einer (oder mehreren) bestimmten Nummer Stammdatenauskünfte begehrt, wobei diese Auskunftsbegehren an alle in Frage kommenden Anbieter gerichtet werden (bei Mobilfunk ist die Zahl dabei überschaubar, weil es nicht so viele Anbieter gibt). Aufgrund der Antworten weiß die Behörde dann, für welche Zeiträume bei welchem Anbieter Verkehrsdaten vorhanden sein könnten, und kann das Auskunftsbegehren zielgerichtet stellen. Die Stammdatenauskunft wird in der Praxis auch deshalb regelmäßig vorgelagert, weil die Kriminalpolizei damit bereits einen ersten Filter setzt, welche Teilnehmeranschlüsse ermittlungsrelevant sein könnten. Als Antwort werden Stammdaten, der entsprechende Zeitraum und die Information „aktiv" oder „inaktiv" übermittelt. Es können auch bei einem Anbieter zur gleichen Rufnummer während der letzten 6 Monate mehrere Stammdatensätze anfallen (z.B. bei einer Übertragung der Rufnummer).

Die Praxis der vorgelagerten Stammdatenauskünfte wird auch im zukünftigen Auskunftsregime über die DLS weiterhin relevant bleiben. Um solche Stammdatenabfragen zu erleichtern bzw. zu beschleunigen sieht der Entwurf zur Verordnung vor, dass Anbieter im Einvernehmen mit den abfrageberechtigten Behörden für eine Abwicklung von Stammdaten-Auskünften via DLS optieren können. Eine Abwicklung von Stammdatenauskünften über die DLS soll nicht verpflichtend als ausschließliche Übermittlungsvariante für alle Anbieter eingerichtet werden. Außerdem soll keine unmittelbare Schnittstelle zur Kundendatenbank des Anbieters hergestellt werden, diese soll vielmehr über die DLS mediatisiert werden. Es soll lediglich einen elektronischen Hin- und Rückkanal geben, der zu einer möglichst raschen Abwicklung führt. In wie weit ein Anbieter solche Auskunftsvorgänge automatisiert, soll dem jeweiligen Anbieter überlassen bleiben - insbesondere im Hinblick auf kleine Anbieter, die nur wenig betroffen sind - solange die Auskunft in vertretbarer Zeit abgewickelt werden kann. Große Anbieter könnten durch eine (Teil-)Automatisierung in eigener Verantwortung die Auskünfte optimieren.

Zu § 22:

Welche Informationen der Anbieter bei der Abwicklung von behördlichen Auskunftsbegehren zu protokollieren hat, ist bereits detailliert in § 102c Abs. 2 TKG 2003 geregelt und wird im Sinne der Rechtsklarheit in § 7 Abs. 3 mit ergänzende Verweisen auf relevante Bestimmungen dieser Verordnung wiederholt. Diese Bestimmung zur Protokollierung bezieht sich indes auf jene Protokoll-Informationen, die der Anbieter gemäß § 102c Abs. 4 TKG 2003 an die dort genannten Stellen (Datenschutzkommission, Datenschutzrat, BMJ) zu übermitteln hat. Bei der Entwicklung des Konzepts der Durchlaufstelle wurde dabei bedacht, dass die zentrale Sammlung der für die Statistik notwendigen Protokollinformationen für diese Zwecke in der DLS eine enorme Verfahrens- und Verwaltungsvereinfachung darstellt. Dabei werden jene – nicht personenbezogenen – Informationen aus der Protokollierung beim Anbieter mit der (verschlüsselten) Auskunft unverschlüsselt mitgeliefert, sodass diese in der DLS für die Aufbereitung der Statistik gespeichert werden können. Diese Methode ist zugleich ein wertvoller Beitrag zur Datensicherheit, weil damit zugleich eine revisionssichere Protokollierung aller Auskunftsfälle in der DLS selbst erfolgt. Für den Fall, dass die Rechtsschutzbeauftragten, die Datenschutzkommission oder ein Gericht im Verfahren gemäß § 32 DSG 2000 für die Überprüfung der Rechtmäßigkeit eines bestimmten Falles der Datenübermittlung die exakten personenbezogenen Daten benötigt, die auf der Seite der Anbieter gemäß § 7 gespeichert werden und auch auf Seiten der Behörden nach den für diese einschlägigen (internen) Verfahrensvorschriften zu erfassen und aufzubewahren sind, kann die statistische Erfassung über die DLS äußerst hilfreich sein. Über die Unique-ID (§ 13) kann nämlich im Rechtsschutzfall der gesamte Ablauf vom Auskunftsbegehren bis zur Beantwortung lückenlos nachvollzogen werden und die richtigen Protokolldaten werden so auf der jeweils überprüften Seite (Anbieter oder Behörden) leichter auffindbar.

Deutlich vereinfacht wird dabei auch das Verfahren für die Aufbereitung der Statistik, die das BMJ jährlich an die EU-Kommission gemäß Art 10 der Richtlinie 2006/24/EG zu übermitteln hat. Über die DLS werden nach dieser Bestimmung alle Rohdaten automatisch gesammelt, die für die Statistik notwendig sind. Die automatische Aufbereitung der Statistik in der DLS richtet sich nach § 23. Hier ist darauf hinzuweisen, dass in der TKG Novelle zur Umsetzung der Vorratsdatenspeicherung ein Redaktionsversehen unterlaufen ist, das dazu führen würde, dass die notwendigen Rohdaten zur Erfüllung dieser gemeinschaftsrechtlichen Verpflichtung unmöglich machen würde. § 102c Abs. 4 Z 2 ordnet nämlich an, dass die Anbieter die Protokolldaten gemäß § 102c Abs. 2 Z 2 bis 4 an das BMJ zu übermitteln haben. Damit würden die Anbieter für die Statistik die Aktenzahlen zu den Auskunftsfällen nach SPG (Z 2 leg cit) übermitteln, nicht aber die Information zur Speicherdauer der übermittelten Daten

(Z 5 leg cit), die nach Art 10 Abs. 1 zweiter Spiegelstrich RL 2006/24/EG ausdrücklich gefordert sind. Dieses Versehen entstand dadurch, dass die Z 2 in § 102c Abs. 2 TKG 2003 im Zuge der Entstehung der Regierungsvorlage erst nachträglich eingefügt wurde, die entsprechende Anpassung im Absatz 4 aber unterblieb. In Absatz 2 dieser Bestimmung erfolgt daher durch den Verweis auf § 7 Abs. 3 Z 3 bis 5 die Korrektur dieses Redaktionsversehens. Um zu vermeiden, dass die Verordnung aus rein formalistischen Gründen wegen Gesetzwidrigkeit beim Verfassungsgerichtshof angefochten und möglicherweise in diesem Punkt für nichtig erklärt wird, sollte der Gesetzgeber daher schnellstmöglich die Richtigstellung im Gesetz selbst vornehmen, um zu vermeiden, dass die europarechtlichen Verpflichtung zur Übermittlung der Statistik aufgrund eines bloßen Versehens nicht erfüllt werden kann.

Zu § 23:

Einerseits müssen die sog. provider-internen Protokolldaten vorliegen (vgl. § 102c Abs 1 TKG 2003). Anbieter müssen intern revisionssicher protokollieren, dass Zugriffe auf Vorratsdaten unter Einhaltung des Vier-Augen-Prinzips nur durch speziell ermächtigte und bestimmte Personen und nur aufgrund einer entsprechenden behördlichen, staatsanwaltschaftlichen bzw. gerichtlichen Anfrage erfolgt sind. Diesen Zugriffen muss immer ein behördlicher, staatsanwaltschaftlicher bzw. gerichtlicher Auftrag zugrunde liegen, insofern besteht ein Zusammenhang zu den Protokoll-Daten über die Auskunftsfälle. Dem gegenüber stehen jene Protokoll bzw Statistik-Aufzeichnung über erfolgte Vorratsdaten-Abfragen (vgl. § 102c Abs 2 TKG 2003), die einmal jährlich an die Europäische Kommission zu übermitteln sind.

Diese beiden Protokollverpflichtungen überschneiden sich allerdings im Hinblick auf den Informationsgehalt. Die Protokollierung für die Statistik muss diese provider-internen Informationen (also welche Mitarbeiter wann zugegriffen haben) allerdings nicht enthalten."

Es besteht eine Verpflichtung zur jährlichen Berichterstattung gegenüber der Europäischen Kommission, die vom BMJ wahrzunehmen ist. Die Erfassung der Protokolldaten im Rahmen der Durchlaufstelle soll diese Erfassung der Protokolldaten für die Anbieter sowie das BMJ deutlich vereinfachen. Denn ansonsten müssen die Protokolldaten von allen Providern eingesammelt und in einheitlicher Struktur zusammengeführt werden. Die Harmonisierung der Protokoll-Struktur müsste also jedenfalls geregelt werden. Gemäß § 102c Abs. 4 Z 2 TKG 2003 obliegt es weiters auch dem BMJ, dem Nationalrat über die Statistik zu berichten.

Es macht jedenfalls Sinn, die Information zum Zeitpunkt der Zustellung der Anordnung in das Postfach des Anbieters gemäß § 7 Abs. 3 Z 3 schon bei der Anfrage zu protokollieren und damit den Protokoll-Datensatz zu einer Anfrage zu „eröffnen". Alle Anfragen über die DLS sind mit einer "Unique-ID" versehen. Die vom Anbieter übermittelte Antwort ist über dieselbe "Unique_ID" verknüpft und kann so den Datensatz zur Protokollierung mit den weiteren benötigten Informationen ergänzen. Gleichermaßen wird der Zeitpunkt der Zustellung der Antwort in das Postfach des Anbieters von der DLS selbständig protokolliert.

Zu § 24:

Diese Bestimmung dient der Klarstellung der Kostentragung der Investitionskosten für die Durchlaufstelle. Nähere Ausführungen über die finanziellen Auswirkungen sind im Vorblatt dargestellt.

Die Aufteilung der laufenden Kosten der DLS (Betriebskosten) bleibt einer interministeriellen Vereinbarung vorbehalten.

Zur Anlage (Schnittstellendefinition EP020):

Die Schnittstellendefinition erfolgt aus Gründen der besseren Darstellung in Form einer Anlage. In der Beilage zu den Erläuternden Bemerkungen werden für alle in der Anlage definierten Datenfelder Beispiele dargestellt. Die Aufzählung der Beispiele ist nicht abschließend und soll den Anbietern sowie den auskunftsberechtigten Behörden zur Hilfestellung bei der technischen Implementierung dienen. Entsprechend kommt dieser Beilage keine über die Anlage oder die sonstigen Bestimmungen dieser Verordnung hinausgehende Bedeutung zu.

Aus den EB zur RV (1074 der Beilagen XXIV. GP - Regierungsvorlage - Vorblatt und Erläuterungen): „Der Spielraum für eine nach dieser Bestimmung zu erlassenden Verordnung ist eng determiniert. Die technische Richtlinie soll für alle Anbieter einheitlich definieren, welche der zu beauskunftenden Werte an welcher Stelle innerhalb der CSV-Datei zu stehen haben und welche Zeichensätze dabei zu verwenden sind."

Die Technische Richtlinie in der Anlage basiert auf einer Empfehlung (EP020), die innerhalb der Telekom-Branche im Rahmen des Arbeitskreis-Telekommunikation (AK-TK) durch die Arbeitsgruppe „Schnittstellendefinition" bereits während der Entstehung der TKG-Novelle zur Umsetzung der Vorratsdatenspeicherung ausgearbeitet wurde. Die EP020 wurde im Rahmen der insgesamt 6 Round

Table Diskussionen des BIM im Zuge der Studie zur Datensicherheit (im Auftrag des BMVIT) mit allen Beteiligten (insbesondere BMI und Bundeskriminalamt) diskutiert und abgestimmt (siehe dazu ausführlich die EB zu § 1). Die Technische Richtlinie in der Anlage enthält all jene Teile der EP020, die sich unmittelbar auf die Definition der Syntax und Semantik der CSV Datei für die Übermittlung von Auskünften bezieht. Die EP020 als ganzes ist in der Datensicherheitsstudie abgebildet und in diesem Rahmen auch zur Veröffentlichung freigegeben.

ANHANG B) EP 020 AUSGABE 3 - EMPFEHLUNG DES AK-TK FÜR EINE SCHNITTSTELLENDEFINITION GEM. § 94 (4) TKG

Geschäftsstelle: ÖFEG, Postfach 147, 1103 Wien, E-Mail: ak-tk@oefeg.at

E M P F E H L U N G

Schnittstelle gemäß TKG § 94 (4)

Zuordnung: AG-Schnittstellendefinition

Ausgabenübersicht

Ausgabe Nr.	1	2	3		
Ausgabe Datum	26.1.2010	3.2.2010	29.6.2011		
Editor	W. Reichl	W. Reichl	W. Reichl		
AK-TK Geschäftsstelle					

Inhaltsverzeichnis

1 Allgemeines

1.1 Einleitung

Diese Empfehlung wird vom Arbeitskreis für Technische Koordination für öffentliche Kommunikationsnetze und -dienste (AK-TK) herausgegeben und von der Arbeitsgruppe Schnittstellendefinition für das Thema „Schnittstellendefinition gemäß TKG § 94 (4)" erstellt.

Leiter der Arbeitsgruppe und Editor für diese Empfehlung ist Dipl.-Ing. Wolfgang Reichl.

Die vorliegende Empfehlung beschreibt den von der Industrie im Rahmen des AK-TK abgestimmten Vorschlag für die Schnittstelle zur Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, einschließlich der Übermittlung von Vorratsdaten, nach den Bestimmungen der StPO sowie des SPG.

Diese Schnittstelle ist im Kontext zum Konzept der Durchlaufstelle zu sehen. Referenzen zur Durchlaufstelle sind in der EP 020 durch gelb hinterlegten Text gekennzeichnet. Nach Stabilisierung der Spezifikationen der Durchlaufstelle sind diese zu aktualisieren.

1.2 Mandat der Arbeitsgruppe

Die Arbeitsgruppe erhielt vom AK-TK Ende 2009 folgendes Mandat:

> *"Im Rahmen des AK-TK wird eine Arbeitsgruppe mit dem Titel „Schnittstellendefinition zur Vorratsdatenspeicherung" (kurz „Schnittstellendefinition") eingesetzt. In dieser Arbeitsgruppe soll eine technische Richtlinie erarbeitet werden, welche die Erfordernisse nach TKG Entwurf § 94 (4) erfüllt und in der Arbeitsgruppe abgestimmt wird. Die für diese Arbeiten erforderlichen Experten können im Rahmen der Arbeitsgruppe beigezogen werden. Die Arbeiten sind ehestens zu beginnen. Ziel ist es, eine in der Arbeitsgruppe abgestimmte Empfehlung zum Plenum des AK-TK Ende Januar 2010 vorzulegen."*

Dieses Mandats wurde mit der Erstellung und Abstimmung der Ausgabe 2 der EP 020 erfüllt.

Das Mandat wurde im 32. Plenum des AK-TK wie folgt erweitert:

> *Die Arbeitsgruppe Vorratsdatenspeicherung des AK-TK soll die Schnittstellendefinition EP 020 überarbeiten. Insbesondere ist diese Schnittstellendefinition den geänderten Rahmenbedingungen anzupassen und weiters sind Klarstellungen im Zusammenhang mit offenen Fragen zu ergänzen.*
>
> *Im Zusammenhang mit der Überarbeitung der Schnittstellendefinition soll die Arbeitsgruppe auch eine Plattform für die Diskussion mit dem Boltzmann Institut für Menschenrechte und anderen Experten darstellen. Diese Diskussion soll aktuelle Themen im Zusammenhang mit der Umsetzung der Vorratsdatenspeicherung unter Berücksichtigung der bis Mai 2011 notwendigen Umsetzung der Rahmenrichtlinie ermöglichen. Hier geht es um die Aufbereitung politischer Grundlagen und die Möglichkeit, den Branchenstandpunkt gegenüber dem Boltzmann Institut für Menschenrechte zu artikulieren.*

Nach Beschluss der Novellen zum TKG 2003, StPO und SPG am 28. April 2011 in zweiter Lesung im Nationalrat wurde mit der Überarbeitung der EP 020 begonnen. Die Ausgabe 3 der EP 020 enthält die mit BMI, BMJ diskutierte Version auf Basis der aktuellen Gesetzeslage.

1.3 Mitglieder der Arbeitsgruppe

A1 Telekom Austria AG
Colt Telecom Austria GmbH
Ericsson Austria GesmbH
Fachverband Telekom/Rundfunk
Hutchison 3G Austria GmbH
Orange Austria Telecommunication GmbH
Rundfunk und Telekom Regulierungs-GmbH
Tele2 Telecommunication Services GmbH
T-Mobile Austria GmbH
UPC Telekabel Wien GmbH

Als Experten im Rahmen der Arbeitsgruppe haben Herr Ing. Mag. Christof Tschohl, Ludwig Boltzmann Institut für Menschenrechte, Herr Dr. Martin Heigl, Herr Mag. Maximilian Schubert, Herr Dr. Andreas Wildberger, ISPA und Herr Prof. Dr. Franz Schönbauer, TU Wien teilgenommen.

2 Gegenstand dieser Empfehlung

2.1 Rechtliche Grundlagen

Mit 20. November 2009 wurde vom Bundesministerium für Verkehr, Innovation und Technologie, Sektion III, ein Entwurf einer Novelle des TKG zur Begutachtung ausgesandt. Dieser Entwurf setzt die Richtlinie 2006/24/EG über die Vorratsdatenspeicherung um.

Der Fachverband der Telekommunikations- und Rundfunkunternehmungen hat angeregt, Vorbereitungsarbeiten zu einer technischen Richtlinie zur einheitlichen Definition der Syntax, der Datenfelder und der Verschlüsselung zur Übermittlung der Daten gemäß § 94 (4), TKG-Entwurf im Rahmen des AK-TK zu beginnen.

Diesem Vorschlag folgend hat der AK-TK eine Schnittstellendefinition zur Umsetzung des TKG-Entwurfs § 94 (4) in EP 020 – Ausgabe 2 erarbeitet.

Die Novellen zu TKG 2003, StPO und SPG wurde am 28. April 2011 in zweiter Lesung im Nationalrat beschlossen. Danach wurde die Schnittstellendefinition angepasst.

Alle zitierten Textstellen des TKG, der StPO und des SPG beziehen sich auf Bundesgesetzblatt Nr. 28 vom 18. Mai 2011 und Bundesgesetzblatt Nr. 33 vom 20. Mai 2011. Der § 94 (4) des TKG lautet nunmehr:

> *Die Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, einschließlich der Übermittlung von Vorratsdaten, nach den Bestimmungen der StPO sowie des SPG, hat unter Verwendung einer Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt, zu erfolgen. Die Daten sind unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie als "Comma-Separated Value (CSV)" - Dateiformat zu übermitteln. Ausgenommen davon ist die Übermittlung von Daten in den Fällen des § 98, von Daten in den Fällen von § 99 Abs. 5 Z 3 und 4 bei Gefahr in Verzug, von Standortdaten in den Fällen der Feststellung des aktuellen Standortes gemäß §§ 134 ff StPO sowie die Übermittlung von begleitenden Rufdaten im Rahmen einer Überwachung von Nachrichten. Durch Verordnung kann der Bundesminister für Verkehr, Innovation und Technologie im Einvernehmen mit den Bundesministern für Inneres und für Justiz die näheren Bestimmungen zur einheitlichen Definition der Syntax, der Datenfelder und der Verschlüsselung, zur Speicherung und Übermittlung der Daten sowie die näheren Bestimmungen betreffend die Speicherung der gemäß § 102c angefertigten Protokolle festsetzen. Nach Erlass der Verordnung ist unmittelbar dem Hauptausschuss des Nationalrates zu berichten."*

2.2 Durchlaufstelle

In § 94 (4) TKG sind Anforderungen bezüglich Übertragungstechnologie, Datenintegrität und Verschlüsselung enthalten. Zur Umsetzung der Datenübermittlung zwischen den Netzbetreibern und den abfrageberechtigten Stellen wurde das Konzept der Durchlaufstelle (DLS) erarbeitet. Im FIT-Ausschuss des Nationalrats wurde eine Ausschussfeststellung verabschiedet, die eine Grundsatzerklärung zur Durchlaufstelle enthält. Demnach scheint nunmehr unter allen Stakeholdern der Konsens zu herrschen, dass die Durchlaufstelle dem Grunde nach jenes Konzept ist, welches in Hinkunft eine sichere Übermittlung im Zusammenhang mit Datenauskünften nach dem TKG gewährleisten soll.

Das Konzept der Durchlaufstelle wurde in Round Tables, welche vom BIM organisiert wurden, diskutiert. Diese Durchlaufstelle ist eine zentrale Verteilstelle für Anfragen und Antworten. Die DLS kann an dieser zentralen Stelle die Funktionen der Protokollierung und Statistik zuverlässig und effizient erfüllen. Die DLS wird in den Portalverbund des Bundes integriert. Für die Provider gibt es daher eine Ansprechstelle, von der Anfragen erhalten werden und die Antworten gesendet werden.

Die folgende Abbildung zeigt das Prinzip der Durchlaufstelle. Die Schlüsselsymbole bei den abfrageberechtigten Stellen und bei den Providern weisen auf die Implementierung der "anspruchsvollen Verschlüsselungstechnologie" hin. Bei den vorgesehenen Public Key Verfahren werden die Daten mit dem öffentlichen Schlüssel des Empfängers verschlüsselt (d.h. das rote Schlüsselsymbol bezeichnet den öffentlichen Schlüssel der abfrageberechtigten Stellen). Nur der Besitzer des zugehörigen privaten Schlüssels kann die Daten lesen. Dies bedeutet auch dass die Durchlaufstelle für die gemäß § 94 (4) TKG zu übermittelnden Daten "blind" ist.

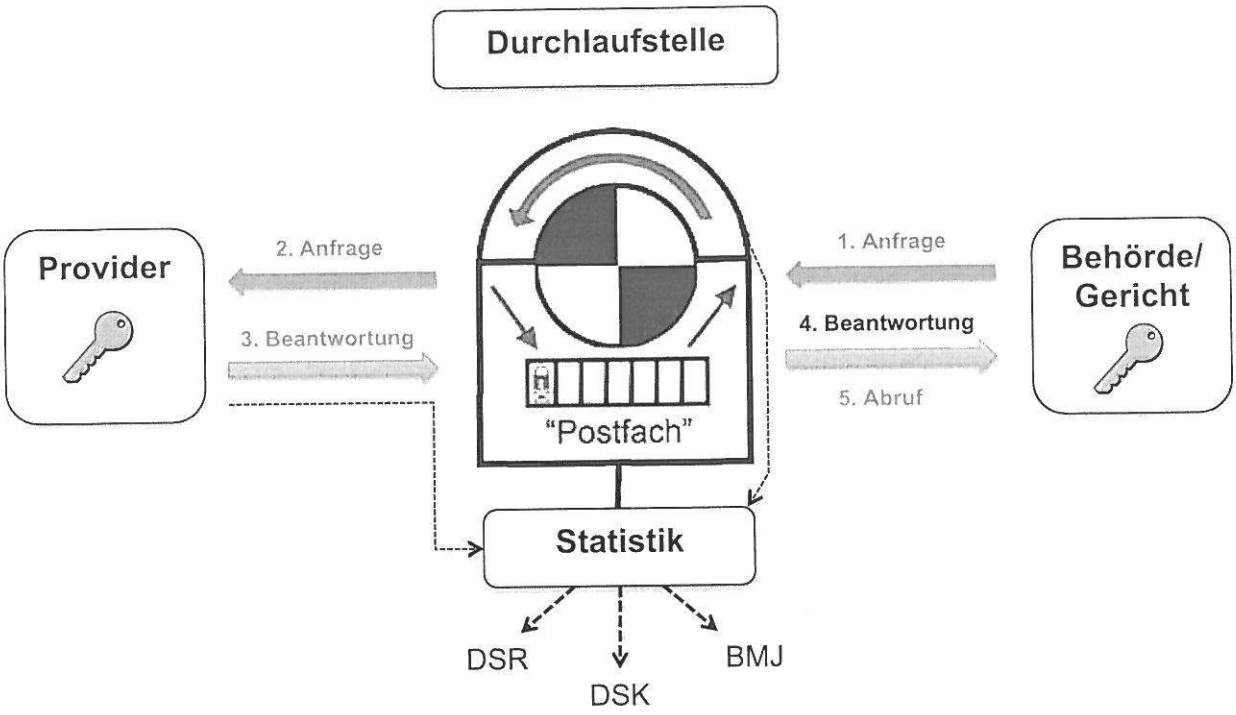

Abbildung 1: Konzept der Durchlaufstelle

Die Schnittstellenbeschreibung nach EP 020 gilt ausschließlich für die Schnittstelle nach Ziffer "3" bzw. "5" der obigen Abbildung.

3 Schnittstelle nach TKG § 94 (4)

Diese Empfehlung definiert die Syntax, die Semantik und die Übergabe der Daten, die einer Behörde im Rahmen einer Beauskunftung übermittelt werden.

3.1 Datenformat

Gemäß § 94 (4) TKG wird das CSV („Comma-Separated Values") Format nach IETF RFC 4180 verwendet.

Grundsätzlich besteht das CSV Format demnach aus Records, die durch Zeilenschaltung getrennt sind. Jeder Record enthält Datenfelder, welche durch Komma (Hexadezimal 2C) getrennt sind. Alle Datenfelder werden durch Anführungszeichen (double quote - Hexadezimal 22) begrenzt. Wenn Anführungszeichen Inhalt eines Datenfeldes sind, wird ein weiteres Anführungszeichen vorgesetzt. Metadaten wie n.a. oder # (siehe Kapitel 3.1.17.) werden nicht unter Anführungszeichen gesetzt. Jeder Record wird durch CRLF (Carriage Return - Hexadezimal 0D, Line Feed - Hexadezimal 0A) abgeschlossen.

Beispiel für einen Record: "aaaa","bbbb","cccc" CRLF
Beispiel für ein Datenfeld mit double quote: "aaaa","b""bb","cccc" CRLF
Beispiel für nicht nachgefragte Datenfelder: "aaaa",#,#,# CRLF

Jedes "csv"-File bildet die Auskunft zu einem bestimmten Indikator und einer bestimmten Datenart ab.

Die optionalen Parameter des CSV Formats gemäß RFC 4180 und die Kodierung der Datenfelder werden wie folgt festgelegt:

3.1.1 Zeichensatz

Als Zeichensatz wird UTF-8 (RFC 3629) verwendet.

Die Kodierung in UTF-8 hat eine variable Länge von 1 – 4 Byte. Die ersten 128 Zeichen (US-ASCII) werden in einem Byte kodiert. Für Umlaut, Akzent, griechische, arabische und andere Schriftsätze werden zwei Bytes verwendet. Mit drei und vier Bytes können praktisch alle weltweit geläufigen Zeichen dargestellt werden.

3.1.2 Header

Die Vorratsdaten gemäß § 102a Z 2 bis 4 TKG können in fünf Datenarten unterteilt werden (siehe folgende Tabelle):

Nummer	Datenart	gesetzliche Grundlage
1	Internetzugangsdienste	§ 102a (2) Z 1 - 4 TKG
2	Öffentliche Telefondienste	§ 102a (3) Z 1 - 6 TKG
3	Erstaktivierung	§ 102a (3) Z 6c TKG
4	E-Mail Verkehrsdaten	§ 102a (4) Z 1 - 4 TKG
5	E-Mail An-/Abmeldung	§ 102a (4) Z 5 TKG

Diese Datenarten haben jeweils unterschiedliche Strukturen, die in Kapitel 4 im Detail dargestellt werden. Use Cases, welche die konkrete Anwendung beschreiben, sind in Kapitel 5 zusammengefasst.

Als erste Zeile jeder Datei wird ein Header eingefügt. Dieser Header enthält die Namen der Datenfelder in dieser Datei. Für jede Datenart gibt es eine spezifische Kopfzeile. In einer Datei dürfen nur Records ein und derselben Datenart enthalten sein. Jeder Datensatz einer Datei hat daher die gleiche Struktur.

Die ersten Felder jeder Datei und jedes Records geben Auskunft über Referenz und Abfragekriterium (in dieser Richtlinie als "Indikator" bezeichnet). Danach kommen die datenartspezifischen Felder. Datenfelder werden im folgenden Text in der Schriftart `Courier New` dargestellt.

3.1.3 Datenfeld "Referenz"

Das erste Datenfeld jeder Datei ist die `Referenz`, die eine eindeutige Referenz zum Auskunftsbegehren ("unique Id") und einem bestimmten Betreiber enthält. Diese wird von der Durchlaufstelle vergeben. Die "unique Id" ist Inhalt des ersten Datenfeldes in jeder Dateiart und jedem Record. Bezieht sich ein Auskunftsbegehren auf mehrere Betreiber, so sind mehrere Bezeichungen zu vergeben.

Es kann Fälle geben, bei denen die Übermittlung des Auskunftsbegehrens wegen hoher Dringlichkeit nicht über die DLS (i.a. telefonisch) erfolgt. Eine Nachreichung der Anfrage über die DLS ist vorgesehen. Es muss aber sichergestellt werden, dass eine Beantwortung bereits vor der Übermittlung der Anfrage via DLS durchgeführt werden kann. Dazu wird ein Betreiber-spezifischer Bereich von Referenzen definiert, der vom Betreiber in aufsteigender Reihenfolge vergeben wird.

3.1.4 Datenfeld "IndikatorArt" und "Indikator"

Nach der Referenz wird bei jeder Dateiart in jedem Record die Art des Indikators und der Indikator selbst angeführt. Damit sind in jeder „csv"-kodierten Datei alle Informationen zur Zuordnung zu einer bestimmten Abfrage enthalten. Der Indikator ist jenes Datum, welches von der abfrageberechtigten Stelle übermittelt wird und zu dem die entsprechenden Vorratsdaten gesucht werden. Ein Indikator ist typischerweise eine IP-Adresse, zu dem die Stammdaten des Teilnehmers gesucht werden.

3.1.5 Indikator, Anschlusskennung und Teilnehmerkennung

Indikator, Anschlusskennung und Teilnehmerkennung zeigen auf Identifikationsmerkmale, die betreiber- und anlassspezifisch eingesetzt werden. In der folgenden Tabelle sind die Identifikationsmerkmale und deren Kodierung zusammengefasst. Der Code ist Inhalt der Felder `IndikatorArt`, `AnschlusskennungArt` und `TeilnehmerArt`.

Identifikationsmerkmal	Code	Beschreibung
Festnetznummer	NR	E.164 Nummer eines Festnetzbetreibers
MSISDN	MSIS	E.164 Nummer eines Mobilfunkbetreibers
Zielrufnummer	ZIEL	E.164 Rufnummer
IMSI	IMSI	Kennung einer Mobilfunk Subskription nach E.212
IMEI	IMEI	Identifikation eines Mobilfunkendgerätes
Öffentliche IP-Adresse	IP	Identifikation eines Endpunktes in einem Datennetz
Betreiberspezifische Kennung	KENN	Kennung, die nur innerhalb eines Betreibers eindeutig ist. Diese Kennung kann, aber muss nicht, dem Kunden bekannt sein
Cell-Id	CELL	betreiberspezifische Kennung einer Funkzelle
E-Mail Adresse	MAIL	Identifikation eines E-Mail Postfaches

Die folgende Tabelle beschreibt, bei welcher Datenart welche Identifikationsmerkmale als Indikator zur Anwendung kommen können.

Identifikationsmerkmal als Indikator	Datenart				
	1	2	3	4	5
Festnetznummer	X	X			
MSISDN	X	X	X		
Zielrufnummer		X			
IMSI		X			
IMEI		X			
Öffentliche IP-Adresse	X				
Betreiberspezifische Kennung	X				
Cell-Id		X			
E-Mail Adresse				X	X

Bei der Datenart Internetzugangsdienste ist gemäß § 102a. (2) Ziffer 4 die eindeutige Kennung des Anschlusses, über den der bestimmte Internetzugang erfolgt ist, aufzuzeichnen. Die Art dieser Anschlusskennung hängt vom Betreiber ab. Im Datensatz werden die Datenfelder `Anschlusskennung` und `AnschlusskennungArt` verwendet. Mögliche Identifikationsmerkmale für die Anschlusskennung sind Festnetznummer, MSISDN, öffentliche IP-Adresse und betreiberspezifische Kennung.

Bei den Datenarten E-Mail Verkehrsdaten und E-Mail An-/Abmeldung ist gemäß § 102a (2) Ziffer 1 und (4) Ziffer 1 die Teilnehmerkennung aufzuzeichnen. Die Art dieser Teilnehmerkennung hängt vom Betreiber ab. Im Datensatz werden die Datenfelder `Teilnehmerkennung` und `TeilnehmerkennungArt` verwendet. Mögliche Identifikationsmerkmale für die Teilnehmerkennung sind Festnetznummer, MSISDN und betreiberspezifische Kennung.

3.1.6 Quelle und Ziel öffentlicher Telefondienste

Im Datensatz für öffentliche Telefondienste werden Quelle und Ziel der Verbindung aufgezeichnet. Bei Abfragen von Mobilfunkanschlüssen werden die jeweils fehlenden Daten IMSI, IMEI oder MSISDN zum Indikator ergänzt. Wird also nach Indikator `MSISDN` abgefragt, so werden `IndikatorIMSI` und `IndikatorIMEI` ergänzt.

In den Datensätzen wird jeweils der Partner der Verbindung (der Anrufer bei ankommenden oder das Ziel bei abgehenden Verbindungen) angegeben. Hier werden die Datenfelder `PartnerIMSI`, `PartnerIMEI` und `PartnerMSISDN` verwendet.

Bemerkung: Die Kodierung von IMSI und IMEI sind den aktuellen ETSI 3GPP Spezifikationen zu entnehmen.

Anrufumleitungen können etweder in einem Datensatz oder in zwei Datensätzen dargestellt werden. Wird ein Datensatz verwendet, so enthält das Feld `Anrufumleitung` die Festnetznummer oder die MSISDN des Umleiteziels. Werden zwei Datensätze verwendet, so enthält der zweite Datensatz (Richtung = Aktiv) die Eintragung JA im Datenfeld `Anrufumleitung`.

3.1.7 Ruftyp

Der Ruftyp bei öffentlichen Telefondiensten wird im Datenfeld `Ruftyp` kodiert:

Ruftyp	`Ruftyp`
Telefonie	T
SMS	S
MMS	M

3.1.8 Richtung

Die Richtung des Verbindungsaufbaues wird bei öffentlichen Telefondiensten im Feld `Richtung` angegeben.

Richtung	`Richtung`
Aktiv	A
Passiv	P

3.1.9 Datumsformate

Datum, Uhrzeit und Zeitzone werden in einem Datenfeld dargestellt und nach ISO 8601 kodiert. Folgende Felder sind auf diese Art kodiert: `Zeit`, `Anmeldung` und `Abmeldung`.

Beispiel: Bei Verwendung des Kalendertages und der Uhrzeit mit Winterzeit in Österreich wird der 7. Januar 2010, 9:00 Uhr wie folgt dargestellt: 2010-01-07T09:00:00+01

3.1.10 Rufnummernformate

Rufnummern (nach E.164) werden im Format

"CC NDC Teilnehmernummer"

angegeben. Diese Kodierung wird für die Felder `Festnetznummer`, `MSISDN`, `IndikatorMSISDN`, `Zielrufnummer` und `PartnerMSISDN` verwendet.

CC ... Country Code (für Österreich "43")

NDC ... National Destination Code ("1" für Wien)

Beispiel für die Darstellung einer Mobilfunknummer: 43664xxxxxxx

Bemerkung: Es gibt auch betreiberinterne Servicerufnummern, die nicht E.164 konform sind. Eine gesonderte Kennzeichnung dieser betreiberinternen Servicerufnummern erfolgt vorerst nicht.

3.1.11 Geografische Koordinaten

Die Darstellung geografischer Koordinaten für den Standort des Senders erfolgt nach dem World Geodetic System 1984 (WGS 84).

Bemerkung: Ob die Darstellung in Graddezimal oder GradMinutenSekunden erfolgt, wird im Einvernehmen mit den Behörden festgelegt.

3.1.12 BetreiberId und CellId

Zur Kennzeichnung von Funkzellen wird das Datenfeld `CellId` verwendet. Die Kodierung dieses Datenfeldes ist netzbetreiberspezifisch. Innerhalb eines Netzbetreibers ist die CellId eindeutig. Die BetreiberId besteht aus Mobile Country Code (MCC) und Mobile Network Code (MNC) gemäß dem Nummerierungsplan nach E.212.

Beispiel: BetreiberId in Österreich:

MCC	MNC	Brand	Netzbetreiber
232	01	A1	A1 Telekom Austria
232	03	T-Mobile	T-Mobile Austria
232	05	Orange	Orange Austria
232	07	tele.ring	T-Mobile Austria
232	10	3	Hutchison 3G
232	11	bob	A1 Telekom Austria
232	12	yesss	yesss
232	15	Barablu	Barablu Mobile Ltd.

Bemerkung: die aktuelle Liste der vergebenen Betreiber-ID ist bei der RTR-GmbH abrufbar.

3.1.13 E-Mail Adresse

E-Mail Adressen haben die Struktur "local-part@domain". Die Syntax ist in RFC 5322 und 5321 beschrieben. Das betrifft die Felder `Indikator`, wenn `IndikatorArt` = "MAIL" ist und die Felder `GesendetAbsender`, `GesendetEmpfänger`, `EmpfangAbsender` und `EmpfangZiel`.

3.1.14 IP-Adresse

IPv4-Adressen werden im Format x.x.x.x angegeben, wobei x eine Zahl zwischen 0 und 255 sein kann. IPv6-Adressen hingegen werden im Format x:x:x:x:x:x:x:x angegeben, wobei x eine hexadezimale Zahl zwischen 0 und FFFF sein kann. Die verkürzte Darstellungsvariante bei mehreren aufeinander folgenden 0 mit "::" gem. IETF RFC 1924 wird nicht verwendet. Die Unterscheidung der Adressformate (IPv4 und IPv6) erfolgt an Hand der unterschiedlichen Darstellungsformen.

Dies betrifft die Datenfelder `Indikator`, `Anschlusskennung`, falls die `IndikatorArt` bzw. `AnschlusskennungArt` = "IP" ist. Weiters werden IP-Adressen bei E-Mail Verkehr aufgezeichnet: `GesendetAbsenderIP_Adresse`, `EmpfangIP_Adresse` und `IP_Adresse`.

3.1.15 Stammdaten

Stammdaten (Vorname, Familienname und Adresse) sind frei beschreibbare Felder. Das betrifft folgende Datenfelder:

- `Vorname`, `Familienname`, `Adresse`
- `IndikatorVorname`, `IndikatorFamilienname`, `IndikatorAdresse`
- `PartnerVorname`, `PartnerFamilienname`, `PartnerAdresse`

Bemerkung: Die in der Datenstruktur der "csv"-Files enthaltenen Stammdaten sind immer historisch, d.h. stimmen für den Zeitpunkt des Kommunikationsvorganges. Die Stammdaten des Indikators sind entweder bereits bekannt oder Gegenstand gesonderter Abfragen. Die korrekte Korrelation von Indikator und dazugehörigen (historischen) Stammdaten ist Aufgabe der abfragenden Behörde. Dazu ist es wichtig, bei reinen Stammdatenabfragen, die aber nicht Gegenstand dieser Empfehlung sind, den Zeitpunkt oder Zeitraum genau zu spezifizieren.

3.1.16 Dateiname

Der Dateiname besteht aus dem Datenfeld `Referenz` und ist mit der Dateierweiterung ".csv" versehen. Werden bei einer Anfrage mehrere Antwort-Files zur gleichen Referenz erstellt, so werden die einzelnen "csv"-Files durchnummeriert (Referenz_1.csv, Referenz_2.csv, etc.).

Zur Zusammenfassung aller zu übermittelnden Dateien sowie deren Verschlüsselung siehe Kapitel 3.3.

3.1.17 Nicht ausgefüllte Felder

Je Datenart wird eine Struktur definiert. Allerdings werden in einem Auskunftsbegehren nur bestimmte Datenfelder angefragt. Andererseits müssen bei einem Betreiber nicht alle Datenfelder vorhanden sein. Um diese beiden Fälle im "csv" File kennzeichnen und unterscheiden zu können, wird festgelegt:

- Datenfelder, die für die Abfrage nicht relevant sind oder nicht nachgefragt wurden, werden mit "#" (Hexadezimal 23) gefüllt. Dies gilt auch für Daten, die der Betreiber nicht haben kann (z.B. Stammdaten einer Zielrufnummer in einem Fremdnetz).
- Datenfelder, die angefragt wurden, aber beim Betreiber nicht verfügbar sind, werden mit "n.a." (für "not available") gefüllt.

Um Dateninhalte von den Kennzeichen zu unterscheiden, werden diese nicht unter Hochkomma gesetzt.

Mit dieser Festlegung wird erreicht, dass der Datenbestand je Datenart einheitlich und daher die Verarbeitung einfacher ist.

Datenfelder werden insbesondere dann mit "n.a." gefüllt, wenn die betreffenden Daten vom Betreiber nicht erzeugt oder verarbeitet wurden. Im Folgenden werden Beispiele dazu aufgezählt:

- Die CellId sowie die geografischen Koordinaten werden beim Ruftyp MMS (Multimedia Messaging Service) bei allen Netzbetreibern nicht aufgezeichnet.
- Falls die Erstaktivierung direkt in der Verkaufsstelle ohne Einbuchen der MSISDN im Netz erfolgt, werden keine geografischen Koordinaten aufgezeichnet.
- Bei Abfragen nach Kapitel 4.5 E-Mail – An-/Abmeldung wird bei einigen Betreibern das Abmeldedatum nicht aufgezeichnet.

3.2 Protokollierung

Die Durchlaufstelle soll auch Funktionen zur Protokollierung übernehmen. § 102c (4) Z 2 normiert: "zum Zweck der Berichterstattung an die Europäische Kommission und an den Nationalrat die Protokolldaten gemäß Abs. 2 Z 2 bis 4[1] an den Bundesminister für Justiz zu übermitteln." Die Protokollierung umfasst daher:

- das Datum der Anfrage sowie das Datum und den genauen Zeitpunkt der erteilten Auskunft,
- die nach Datum und Kategorien gemäß § 102a Abs. 2 bis 4 aufgeschlüsselte Anzahl der übermittelten Datensätze und

[1] Dieser Verweis ist ein Redaktionsversehen. Es soll Z 3 bis Z 5 heißen.

- die Speicherdauer der übermittelten Daten zum Zeitpunkt der Anordnung der Übermittlung.

Diese Daten werden in einem Protokollfile im csv Format unverschlüsselt über die sichere https-Verbindung an die DLS übermittelt. Format der Datei und Dateiname sind noch festzulegen. Protokolldaten haben andere Adressaten als die jene CSV Dateien, welche die begehrten Auskünte enthalten und müssen daher auch nicht mit dem Key der Behörde/des Gerichts verschlüsselt werden. Die Protokolldaten werden ausschließlich für die definierten Protokolldatenempfänger zugänglich sein und werden innerhalb der DLS in einer gesonderten Datenbank archiviert, wobei der Kreis der Zugangsberechtigten und die Art des Zugangs sich nach der Spezifikation der DLS richtet und daher auch nicht Gegenstand der EP 020 ist.

3.3 Verschlüsselung, Signatur und Datenintegrität

Die Verschlüsselung der Daten erfolgt sowohl auf Transportebene als auch end-to-end. Zur Verschlüsselung auf Transportebene wird HTTPS[2] verwendet. Als Mechanismus zur end-to-end Verschlüsselung wird Public Key Infrastruktur mit Client- und Server-Zertifikaten verwendet.

Um die Datenintegrität end-to-end sicherzustellen, wird vom Absender ein SHA-1[3] Hash berechnet und in einem eigenen File (Dateiname gemäß Kapitel 3.1.16 und zusätzliche Dateierweiterung ".sha1", also Referenz_1.csv.sha1, Referenz_2.csv.sha1, etc.) gespeichert. Dieses File wird gemeinsam mit den "csv" Files übermittelt. Der Empfänger kann die Datenintegrität des jeweiligen "csv" Files durch Berechnung und Vergleich des SHA-1 Hash prüfen.

Es ist optional möglich, alle Dateien (csv und Hash Files) zu einer Abfrage zu einer zip-Datei mit dem Namen Referenz.zip zusammenzufassen. Für die Übermittlung wird nur die zip-Datei verschlüsselt, nicht aber die einzelnen Dateien.

Die Übermittlung und Benennung der Protokolldaten richtet sich nach Kapitel 3.2.

Die Definition der Dateinamen für die Übermittlung verschlüsselter Dateien sowie der Signaturen sind Gegenstand der Spezifikation zur Durchlaufstelle und werden von der EP 020 nicht berührt. Die Bildung eines Hash-Wertes zur Sicherung der Datenintegrität wurde in dieser Fassung der EP 020 losgelöst von der public/private-key infrastructure diskutiert. Diese Funktion soll über die Signatur erfüllt werden und ist im Rahmen der Spezifikation zur DLS gesondert zu regeln.

[2] HTTP Secure (RFC 2818)
[3] Secure Hash Algorithm 1 (RFC 3174)

3.4 Zusatzinformationen

Die csv-Dateien (und Hash Files) werden mittels sicherem Filetransfer an die Durchlaufstelle übermittelt. Zusatzinformationen könnten allenfalls über ein Web-Interface zu der entsprechenden Abfrage eingegeben werden. Diese Zusatzinformationen könnten auch Gründe für eine Leer-Meldung beschreiben. Ob und in welchem Ausmaß ein Web-Interface auf Seiten der DLS zur Verfügung gestellt werden soll, wird Gegenstand der Diskussion zur Spezifikation der DLS sein. Jedenfalls ist dabei zu bedenken, dass die DLS gegenüber Inhalten der Auskünfte "blind" sein soll. Alternativ sind nach dem sonstigen Aufbau der EP 020 die möglichen Dateiformate und Dateinamen für Zusatzinformationen zu definieren.

Für Anfragen, die nicht zwischen Vorratsdaten und betriebsnotwendigen Daten unterscheiden (z.B. nach § 53 Abs. 3a und 3b SPG) muss die Information übermittelt werden, ob Vorratsdaten für die Beantwortung dieser Anfrage verwendet wurden. Diese Information wird von den Betreibern als "Zusatzinformation" übermittelt.

4 Datenarten

Zur Übermittlung der Daten nach § 94 (4) werden fünf unterschiedliche Datenarten und Datenstrukturen definiert. Damit können alle Auskunftsbegehren beantwortet werden. Diese Datenstrukturen sind die Maximalausprägung der Daten für die jeweiligen Datenarten. Use Cases der konkreten Verwendung werden in Kapitel 5 beschrieben.

Zu jeder Datenart wird für jedes Abfragekriterium ("Indikator") ein konkreter Anwendungsfall definiert. In Abhängigkeit von diesen Anwendungsfällen werden die möglichen Parameter in den Datenfeldern und die auszufüllenden Felder festgelegt.

4.1 Internetzugangsdienste

Abfragen im Zusammenhang von Internetzugangsdiensten sind vorgesehen um den Zusammenhang zwischen öffentlichen IP-Adressen und Teilnehmern herzustellen. Eine Abfrage nach öffentlichen IP-Adressen liefert jenen Teilnehmer, dem diese IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war. Umgekehrt kann auch abgefragt werden, welche öffentliche IP-Adresse einem bestimmten Teilnehmer zu einem bestimmten Zeitpunkt zugeordnet war.

Grundlage:

§ 92 (3) 3. "Stammdaten" alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind:

a) Name (Familienname und Vorname bei natürlichen Personen, Name bzw. Bezeichnung bei juristischen Personen),

b) akademischer Grad bei natürlichen Personen,

c) Anschrift (Wohnadresse bei natürlichen Personen, Sitz bzw. Rechnungsadresse bei juristischen Personen).

§ 92 (3) 6b. "Vorratsdaten" Daten, die ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a gespeichert werden;

§ 92. (3) 14. "Internet-Zugangsdienst" einen Kommunikationsdienst im Sinne von § 3 Z 9, der in der Bereitstellung von Einrichtungen oder Diensten zur Erbringung von Zugangsleistungen zum Internet besteht;

§ 92. (3) 16. "Öffentliche IP-Adresse" eine einmalige numerische Adresse aus einem Adressblock, der durch die Internet Assigned Numbers Authority (IANA) oder durch eine regionale Vergabestelle (Regional Internet Registries) einem Anbieter eines Internet-Zugangsdienstes zur Zuteilung von Adressen an seine Kunden zugewiesen wurde, die einen

Rechner im Internet eindeutig identifiziert und im Internet geroutet werden kann. Öffentliche IP-Adressen sind Zugangsdaten im Sinne des § 92 Abs 3 Z 4a. Wenn eine konkrete öffentliche IP-Adresse einem Teilnehmer für die Dauer des Vertrages zur ausschließlichen Nutzung zugewiesen ist, handelt es sich zugleich um ein Stammdatum im Sinne des § 92 Abs 3 Z 3.

§ 102a. (2) Anbietern von Internet-Zugangsdiensten obliegt die Speicherung folgender Daten:

1. Name, Anschrift und Teilnehmerkennung des Teilnehmers, dem eine öffentliche IP-Adresse zu einem bestimmten Zeitpunkt unter Angabe der zugrunde liegenden Zeitzone zugewiesen war;
2. Datum und Uhrzeit der Zuteilung und des Entzugs einer öffentlichen IP-Adresse bei einem Internetzugangsdienst unter Angabe der zugrundeliegenden Zeitzone;
3. die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss;
4. die eindeutige Kennung des Anschlusses über den der Internet-Zugang erfolgt ist.

Das Datenformat für die Abfrage von Vorratsdaten zu Internetzugangsdiensten wird wie folgt festgelegt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 3.1.3
IndikatorArt	NR, MSIS, IP, KENN	siehe Kapitel 3.1.4
Indikator	Festnetznummer, MSISDN, IP-Adresse, betreiberspezifische Kennung	
AnschlusskennungArt	NR, MSIS, IP, KENN	siehe Kapitel 3.1.5
Anschlusskennung	Festnetznummer, MSISDN, IP-Adresse, betreiberspezifische Kennung	
Vorname	optional: akademischer Grad vorangesetzt	siehe Kapitel 3.1.15
Familienname	optional: akademischer Grad vorangesetzt	
Adresse	Präferiert ist die Wohnadresse. Falls diese nicht zur Verfügung steht, wird die Rechnungsadresse eingetragen.	

Falls der Provider aus Mangel an öffentlichen IP-Adressen eine NAT[4] anbietet (d.h. zu einer öffentlichen IP-Adresse kann nur eine Menge von möglichen Teilnehmern ermittelt werden), so wird an den Auftraggeber ausschließlich die Information übermittelt, dass eine Einschränkung auf eine bestimmte Person nicht möglich ist.

[4] Mit einer NAT (Network Address Translation) wird die öffentliche IP-Adresse dynamisch Adressen eines privaten Adressraumes zugeordnet.

4.1.1 Indikator IP-Adresse

Bei Abfrage nach IP-Adresse wird der Datensatz wie folgt ausgefüllt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 3.1.3
IndikatorArt	IP	siehe Kapitel 3.1.4
Indikator	IP Adresse	
AnschlusskennungArt	KENN, NR, MSIS	siehe Kapitel 3.1.5
Anschlusskennung	betreiberspezifische Kennung, Festnetznummer, MSISDN	
Vorname	optional: akademischer Grad vorangesetzt	siehe Kapitel 3.1.15
Familienname	optional: akademischer Grad vorangesetzt	
Adresse	Präferiert ist die Anschlussadresse. Falls diese nicht zur Verfügung steht, wird die Rechnungsadresse eingetragen.	

Die Abfrage gibt Auskunft darüber, wem eine bestimmte öffentliche IP-Adresse zu einem bestimmten Zeitpunkt zugeteilt war. Die Art der Anschlusskennung hängt vom Betreiber ab (Mobilfunk – MSISDN, Festnetzbetreiber/Kabelnetzbetreiber/ISP – betreiberspezifische Kennung oder Telefonnummer bzw. Dial-up Nummer). Jeder Anschlusskennung werden – falls möglich – die betreffenden Stammdaten zugeordnet.

4.1.2 Indikator Teilnehmerkennung

Bei Abfrage nach Teilnehmerkennung wird der Datensatz wie folgt ausgefüllt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 3.1.3
IndikatorArt	KENN, NR, MSIS	siehe Kapitel 3.1.4
Indikator	betreiberspezifische Kennung, Festnetznummer, MSISDN	
AnschlusskennungArt	IP	siehe Kapitel 3.1.5
Anschlusskennung	IP-Adresse	
Vorname	#	
Familienname	#	
Adresse	#	

Die Abfrage gibt Auskunft darüber, welche IP-Adresse einem bestimmten Teilnehmer zu einem bestimmten Zeitpunkt zugeordnet war. Die Art des Indikators hängt vom Betreiber ab und wird in den meisten Fällen eine Telefonnummer (Festnetznummer oder MSISDN) sein. In diesem Fall werden Stammdaten nicht ausgefüllt.

4.2 Öffentliche Telefondienste

Die Vorratsdatenspeicherung für öffentliche Telefondienste umfasst aktive und passive Gespräche sowie Informationen über Gesprächspartner. Besondere Abfragen können nach Cell-Id und Zielrufnummer gestellt werden.

Grundlage:

§ 92. (3) 6a. "Standortkennung" die Kennung einer Funkzelle, über welche eine Mobilfunkverbindung hergestellt wird (Cell-Id);

§ 92. (3) 8. "Anruf" eine über einen öffentlichen Telefondienst aufgebaute Verbindung, die eine zwei- oder mehrseitige Echtzeit-Kommunikation ermöglicht;

§ 92. (3) 8a. "erfolgloser Anrufversuch" einen Telefonanruf, bei dem die Verbindung erfolgreich aufgebaut wurde, der aber unbeantwortet bleibt oder bei dem das Netzwerkmanagement eingegriffen hat;

§ 92. (3) 10. "elektronische Post" jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird;

§ 92. (3) 13. "Internet-Telefondienst" einen öffentlichen Telefondienst im Sinne des § 3 Z 16, der auf paketvermittelter Nachrichtenübertragung über das Internet-Protokoll basiert;

§ 102a. (3) Anbietern öffentlicher Telefondienste einschließlich Internet-Telefondiensten obliegt die Speicherung folgender Daten:

1. Teilnehmernummer oder andere Kennung des anrufenden und des angerufenen Anschlusses;
2. bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Teilnehmernummer, an die der Anruf geleitet wird;
3. Name und Anschrift des anrufenden und des angerufenen Teilnehmers;
4. Datum, Uhrzeit des Beginns und Dauer eines Kommunikationsvorganges unter Angabe der zugrundeliegenden Zeitzone;
5. die Art des in Anspruch genommenen Dienstes (Anrufe, Zusatzdienste und Mitteilungs- und Multimediadienste);
6. Betreibern von Mobilfunknetzen obliegt zudem die Speicherung
    a. der internationalen Mobilteilnehmerkennung (IMSI) des anrufenden und des angerufenen Anschlusses;

b. der internationalen Mobilfunkgerätekennung (IMEI) des anrufenden und des angerufenen Anschlusses;

c. Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Standortkennung (Cell-ID), an dem der Dienst aktiviert wurde, wenn es sich um vorbezahlte anonyme Dienste handelt;

d. der Standortkennung (Cell-ID) bei Beginn einer Verbindung;

Das Datenformat für die Abfrage von Vorratsdaten zu öffentlichen Telefondiensten wird wie folgt festgelegt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 3.1.3
IndikatorArt	NR, MSIS, ZIEL, IMSI, IMEI, CELL	siehe Kapitel 3.1.4
Indikator	Festnetznummer, MSISDN, Zielrufnummer, IMSI, IMEI, Cell-Id	
IndikatorMSISDN		siehe Kapitel 3.1.6
IndikatorIMSI		
IndikatorIMEI		
IndikatorVorname		siehe Kapitel 3.1.15
IndikatorFamilienname		
IndikatorAdresse		
BetreiberId	diese Information bezieht sich auf den Indikator und ist nur für Mobilfunkbetreiber relevant	siehe Kapitel 3.1.12
CellId	die CellId ist Netzbetreiber-spezifisch	
GeoKoordinaten	das sind die geografischen Koordinaten des Senderstandortes	siehe Kapitel 3.1.11
Zeit	Datum und Uhrzeit nach ISO 8601	siehe Kapitel 3.1.9
Dauer	in Sekunden	Zahl
Ruftyp	Telefonie (T), SMS (S) oder MMS (M)	siehe Kapitel 3.1.7
Richtung	aktiv (A) oder passiv (P)	siehe Kapitel 3.1.8
PartnerMSISDN		siehe Kapitel 3.1.6
PartnerIMSI	IMSI und IMEI werden nur angegeben, wenn sich der Partner im eigenen (Mobilfunk-) Netz befindet.	
PartnerIMEI		
PartnerVorname	Die Stammdaten können nur ermittelt werden, wenn sich der Partner im eigenen Netz befindet.	siehe Kapitel 3.1.15
PartnerFamilienname		
PartnerAdresse		
Anrufumleitung	gibt an, ob es sich um eine Anrufumleitung handelt (JA) oder enthält die Zielrufnummer der Anrufumleitung	siehe Kapitel 3.1.6

Wird das Auskunftsbegehren für einen Namen oder eine Adresse gestellt, so erhebt der Betreiber die in Frage kommenden Indikatoren und führt die Abfrage nach diesen Indikatoren durch.

Nicht erfolgreiche Verbindungen werden nur in dem Ausmaß erfasst, als der Betreiber dies auch bisher durchgeführt hat. Eine separate Kennzeichnung zur Unterscheidung von erfolgreichen und nicht erfolgreichen Verbindungen gibt es nicht.

Anrufumleitung bezieht sich auf eine aktivierte Anrufumleitung durch den Indikator. Für Anrufumleitung können zwei Gesprächsdatensätze im „csv" File enthalten sein. Die erste Verbindung geht vom Partner zum Indikator und die zweite vom Indikator zum Umleiteziel. Der zweite Datensatz ist als umgeleitete Verbindung gekennzeichnet (Anrufumleitung = ja).

Optional besteht auch die Möglichkeit, nur einen Datensatz aufzuzeichnen und das Umleiteziel im Feld Anrufumleitung einzutragen.

Die Information, ob es sich um ein Fax oder Datentransfer via Modem handelt, kann aus technischen Gründen nicht inkludiert werden.

Ein Internet-Telefondienst ist gemäß § 92 (3) Z 13 ein „öffentlicher Telefondienste" iSd § 3 Z 16 TKG. Im Sinne dieser Bestimmung ist VoIP Klasse A iSd Richtlinien für Anbieter von VoIP Diensten der RTR zu verstehen. Diese Internet-Telefondienste werden in der gleichen Form beauskunftet wie andere öffentliche Telefondienste.

4.2.1 Indikator Festnetznummer

Bei Abfrage nach Festnetznummer wird der Datensatz wie folgt ausgefüllt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 3.1.3
IndikatorArt	NR	siehe Kapitel 3.1.4
Indikator	Festnetznummer	
IndikatorMSISDN	#	
IndikatorIMSI	#	
IndikatorIMEI	#	
IndikatorVorname	#	
IndikatorFamilienname	#	
IndikatorAdresse	#	
BetreiberId	#	
CellId	#	
GeoKoordinaten	#	
Zeit	Datum und Uhrzeit nach ISO 8601	siehe Kapitel 3.1.9
Dauer	in Sekunden	Zahl
Ruftyp	Telefonie (T), SMS (S) oder MMS (M)	siehe Kapitel 3.1.7
Richtung	aktiv (A) oder passiv (P)	siehe Kapitel 3.1.8
PartnerMSISDN	die Rufnummer des Partners	siehe Kapitel 3.1.6
PartnerIMSI	#	
PartnerIMEI	#	
PartnerVorname	Die Stammdaten können nur ermittelt werden, wenn sich der Partner im eigenen Netz befindet.	siehe Kapitel 3.1.15
PartnerFamilienname		
PartnerAdresse		
Anrufumleitung	gibt an, ob es sich um eine Anrufumleitung handelt oder enthält optional die Zielrufnummer der Anrufumleitung	siehe Kapitel 3.1.6

4.2.2 Indikator MSISDN, IMEI oder IMSI

Bei Abfrage nach MSISDN, IMSI oder IMEI wird der Datensatz wie folgt ausgefüllt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 3.1.3
IndikatorArt	MSIS, IMSI, IMEI	siehe Kapitel 3.1.4
Indikator	MSISDN, IMSI oder IMEI	
IndikatorMSISDN	Die jeweils fehlenden Daten zum Indikator werden eingetragen.	siehe Kapitel 3.1.6
IndikatorIMSI		
IndikatorIMEI		
IndikatorVorname	#	
IndikatorFamilienname	#	
IndikatorAdresse	#	
BetreiberId	Id des Netzbetreibers, in dem sich der Indikator befindet	siehe Kapitel 3.1.12
CellId	CellId, in dem sich der Indikator bei Beginn der Verbindung befindet	
GeoKoordinaten	geografische Koordinaten des Senderstandortes, in dem sich der Indikator zu Beginn der Verbindung befindet	siehe Kapitel 3.1.11
Zeit	Datum und Uhrzeit nach ISO 8601	siehe Kapitel 3.1.9
Dauer	in Sekunden	Zahl
Ruftyp	Telefonie (T), SMS (S) oder MMS (M)	siehe Kapitel 3.1.7
Richtung	aktiv (A) oder passiv (P)	siehe Kapitel 3.1.8
PartnerMSISDN	die Rufnummer des Partners	siehe Kapitel 3.1.6
PartnerIMSI	Diese Daten werden nur eingetragen, wenn sich der Partner im eigenen Netz befindet.	
PartnerIMEI		
PartnerVorname	Die Stammdaten können nur ermittelt werden, wenn sich der Partner im eigenen Netz befindet.	siehe 3.1.15
PartnerFamilienname		
PartnerAdresse		
Anrufumleitung	gibt an, ob es sich um eine Anrufumleitung handelt oder enthält optional die Zielrufnummer der Anrufumleitung	siehe 3.1.6

Bei Roaming in anderen Netzen wird die jeweilige BetreiberId angegeben. In diesen Fällen sind die Felder `CellId` und `GeoKoordinaten` nicht ausgefüllt (#).

Bei Roaming werden die Gesprächsdaten von jenem Betreiber aufgezeichnet, in dessen Netz sich der Teilnehmer aufhält. Die Übermittlung dieser Gesprächdaten zum Heimatnetzbetreiber kann einige Zeit in Anspruch nehmen. Bei der Abfrage werden daher nur jene Daten erfasst, die zum Zeitpunkt der Abfrage vorliegen. Es ist nicht sichergestellt, dass alle Roamingdaten enthalten sind.

Bei Network Sharing, MVNO und nationalem Roaming schickt die Behörde das Auskunftsbegehren an alle involvierten Netzbetreiber, um eine vollständige Datenerfassung sicherzustellen.

4.2.3 Indikator CellId

Bei Abfrage nach CellId wird der Datensatz wie folgt ausgefüllt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 3.1.3
IndikatorArt	CELL	siehe Kapitel 3.1.4
Indikator	Cell-Id	
IndikatorMSISDN	Hier werden Informationen über die Teilnehmer eingetragen, die sich in der abgefragten Zelle in dem abgefragten Zeitraum aufgehalten haben und/oder Verbindungen aufgebaut haben.	siehe Kapitel 3.1.6
IndikatorIMSI		
IndikatorIMEI		
IndikatorVorname		siehe Kapitel 3.1.15
IndikatorFamilienname		
IndikatorAdresse		
BetreiberId	Id des Netzbetreibers, in dem sich der Indikator befindet	siehe Kapitel 3.1.12
CellId	CellId, in dem sich der Teilnehmer bei Beginn der Verbindung befindet	
GeoKoordinaten	geografische Koordinaten des Senderstandortes, in dem sich der Teilnehmer zu Beginn der Verbindung befindet	siehe Kapitel 3.1.11
Zeit	Datum und Uhrzeit nach ISO 8601	siehe Kapitel 3.1.9
Dauer	in Sekunden	Zahl
Ruftyp	Telefonie (T), SMS (S) oder MMS (M)	siehe Kapitel 3.1.7
Richtung	aktiv (A) oder passiv (P)	siehe Kapitel 3.1.8
PartnerMSISDN	die Rufnummer des Partners	siehe Kapitel 3.1.6
PartnerIMSI	Diese Daten werden nur eingetragen, wenn sich der Partner im eigenen Netz befindet.	
PartnerIMEI		
PartnerVorname	Die Stammdaten können nur ermittelt werden, wenn sich der Partner im eigenen Netz befindet.	siehe Kapitel 3.1.15
PartnerFamilienname		
PartnerAdresse		
Anrufumleitung	gibt an, ob es sich um eine Anrufumleitung handelt oder enthält optional die Zielrufnummer der Anrufumleitung	siehe Kapitel 3.1.6

Mit dieser Abfrage soll festgestellt werden, welche Mobilfunkteilnehmer/-geräte zu einer bestimmten Zeit in einem bestimmten geografischen Bereich Verbindungen aufgebaut haben.

Falls verfügbar, werden die Stammdaten sowohl des Teilnehmers in dieser Zelle als auch des Partners angegeben. Für Teilnehmer aus fremden Netzen (Visitor Roaming) können Stammdaten nicht inkludiert werden.

Falls sich das Auskunftsbegehren an einen bestimmten geografischen Bereich richtet, erhebt der Netzbetreiber, welche Zellen dafür in Frage kommen und führt die Abfrage je CellId durch.

4.2.4 Indikator Zielrufnummer

Bei Abfrage nach Zielrufnummer wird der Datensatz wie folgt ausgefüllt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 3.1.3
IndikatorArt	ZIEL	siehe Kapitel 3.1.4
Indikator	Zielrufnummer	
IndikatorMSISDN	#	siehe Kapitel 3.1.6
IndikatorIMSI	#	
IndikatorIMEI	#	
IndikatorVorname	#	siehe Kapitel 3.1.15
IndikatorFamilienname	#	
IndikatorAdresse	#	
BetreiberId	#	
CellId	#	
GeoKoordinaten	#	
Zeit	Datum und Uhrzeit nach ISO 8601	siehe Kapitel 3.1.9
Dauer	in Sekunden	Zahl
Ruftyp	Telefonie (T), SMS (S) oder MMS (M)	siehe Kapitel 3.1.7
Richtung	aktiv (A) oder passiv (P)	siehe Kapitel 3.1.8
PartnerMSISDN	Hier werden Informationen über die Teilnehmer eingetragen, die Verbindungen zu dieser Zielrufnummer aufgebaut haben.	
PartnerIMSI		
PartnerIMEI		
PartnerVorname		
PartnerFamilienname		
PartnerAdresse		
Anrufumleitung	#	

Zweck dieser Abfrage ist es, festzustellen, welche Teilnehmer diese Zielrufnummer gerufen haben. Es handelt sich dabei immer um eine Zielrufnummer in einem Fremdnetz (sonst würde eine Abfrage nach Kapitel 4.2.1 oder 4.2.2 gestellt werden).

Die Abfrage kann an Festnetz- oder an Mobilfunkbetreiber gestellt werden. Es sind die jeweils relevanten Daten auszufüllen. Die jeweilige Rufnummer ist im Feld `PartnerMSISDN` einzutragen.

Standortdaten werden bei dieser Abfrage nicht inkludiert. Diese müssten in einem zweiten Schritt nach Kapitel 4.2.2 abgefragt werden.

4.3 Erstaktivierung

Diese Datenstruktur erlaubt die Übermittlung von Datum und Uhrzeit der Erstaktivierung bei vorbezahlten anonymen Diensten.

Grundlage:

§ 102a. (3) Anbietern öffentlicher Telefondienste obliegt die Speicherung folgender Daten:

6. Betreibern von Mobilfunknetzen obliegt zudem die Speicherung
    c. Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Standortkennung (Cell-ID), an dem der Dienst aktiviert wurde, wenn es sich um vorbezahlte anoynme Dienste handelt;

Das Datenformat für die Abfrage von Vorratsdaten zur Erstaktivierung wird wie folgt festgelegt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 3.1.3
IndikatorArt	MSIS	siehe Kapitel 3.1.4
Indikator	MSISDN	
BetreiberId	Id des Netzbetreibers	siehe Kapitel 3.1.12
CellId	CellId, in dem der Teilnehmer die Erstaktivierung durchgeführt hat	
GeoKoordinaten	geografische Koordinaten des Senderstandortes, in dem der Teilnehmer die Erstaktivierung durchgeführt hat	siehe Kapitel 3.1.11
Zeit	Datum und Uhrzeit der Erstaktivierung	siehe Kapitel 3.1.9

Die Beauskunftung darf nur erfolgen, wenn die Erstaktivierung nicht länger als 6 Monate zurückliegt.

4.4 E-Mail – Verkehrsdaten

Zweck dieses Datenformates ist Auskunft über E-Mail Verkehr. Dabei werden zu einer bestimmten E-Mail Adresse die Absender ankommender E-Mails und die Zieladressen gesendeter E-Mails angegeben.

Grundlage:

§ 92. (3) 2b "E-Mail Adresse" die eindeutige Kennung, die einem elektronischen Postfach von einem Internet E-Mail Anbieter zugewiesen wird;

§ 92. (3) 10. "elektronische Post" jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird;

§ 92. (3) 11. "elektronisches Postfach" ein elektronisches Ablagesystem, das einem Teilnehmer eines E-Mail Dienstes zugeordnet ist;

§ 92. (3) 12. "E-Mail" elektronische Post, die über das Internet auf Basis des "Simple Mail Transfer Protokoll" (SMTP) versendet wird;

§ 92. (3) 15. "E-Mail Dienst" einen Kommunikationsdienst im Sinne von § 3 Z 9, welcher den Versand und die Zustellung von E-Mails auf Basis des "Simple Mail Transfer Protokoll" (SMTP) umfasst;

§ 102a. (4) Anbietern von E-Mail Diensten obliegt die Speicherung folgender Daten:

1. die einem Teilnehmer zugewiesene Teilnehmerkennung;
2. Name und Anschrift des Teilnehmers, dem eine E-Mail Adresse zu einem bestimmten Zeitpunkt zugewiesen war;
3. bei Versenden einer E-Mail die E-Mail Adresse und die öffentliche IP-Adresse des Absenders sowie die E-Mail Adresse jedes Empfängers der E-Mail;
4. beim Empfang einer E-Mail und deren Zustellung in ein elektronisches Postfach die E-Mail Adresse des Absenders und des Empfängers der Nachricht sowie die öffentliche IP-Adresse der letztübermittelnden Kommunikationsnetzeinrichtung;

Das Datenformat für die Abfrage von Vorratsdaten bezüglich E-Mail Verkehr wird wie folgt festgelegt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 3.1.3
IndikatorArt	MAIL	siehe Kapitel 3.1.4
Indikator	E-Mail Adresse	
TeilnehmerkennungArt	NR, MSIS, KENN	siehe Kapitel 3.1.5
Teilnehmerkennung	Festnetznummer, MSISDN, betreiberspezifische Kennung	
Zeit	Datum, Uhrzeit und Zeitzone nach ISO 8601	siehe Kapitel 3.1.9
GesendetAbsender	Bei gesendeten E-Mails wird je Adressat ein Datensatz aufgenommen.	siehe Kapitel 3.1.13
GesendetAbsenderIP_Adresse		siehe Kapitel 3.1.14
GesendetEmpfänger		siehe Kapitel 3.1.13
EmpfangAbsender	Bei empfangenen E-Mails wird die E-Mail Adresse des Absenders und jene des Empfängers angegeben.	siehe Kapitel 3.1.13
EmpfangZiel		siehe Kapitel 3.1.13
EmpfangIP_Adresse	öffentliche IP-Adresse der letztübermittelnden Kommunikationseinrichtung	siehe Kapitel 3.1.14

Es wird nur die jeweils im Auskunftsbegehren angegebene E-Mail Adresse abgefragt. Für Aliases müssen eigene Auskunftsbegehren gestellt werden.

Falls ein Betreiber nur einen Server für abgehende E-Mails anbietet, sind nur Informationen über diese E-Mails in die Abfrage aufzunehmen. Der vollständige E-Mail Verkehr kann in diesem Fall nur durch Abfrage bei beiden Betreibern (dem, in dessen Zuständigkeitsbereich

der Server für abgehende E-Mails steht und jener, in dessen Zuständigkeitsbereich der Server für ankommend E-Mails steht) ermittelt werden.

Datum/Uhrzeit wird aus den Log-Einträgen des Mail-Servers entnommen. Bei gesendeten E-Mails gibt dieser Zeitstempel an, wann die E-Mail vom Client im E-Mail Server erhalten wurde. Bei empfangenen E-Mails gibt der Zeitstempel den Zeitpunkt des Einlangens beim E-Mail-Server an ("received").

Die E-Mail Adressdaten des Absenders und der Empfänger stammen vom "MAIL" und "RCPT" command der E-Mail iSd RFC 5321.

Spam E-Mails, die bereits vor Zustellung in das Postfach vom Betreiber ausgefiltert wurden, werden nicht aufgezeichnet.[5]

E-Mail Alias Adressen, die zum Zeitpunkt der Abfrage nicht mehr aktiv sind, können nicht rückwirkend einem bestimmten Teilnehmer zugeordnet werden. Diese Historisierung wird von den österreichischen Anbietern nicht durchgeführt.[6]

Stammdaten zum E-Mail Verkehr sind in der „csv"-Datei nicht enthalten. Zur Abfrage dieser Daten müsste eine gesonderte Stammdatenabfrage erfolgen. Es wird darauf hingewiesen, dass Absenderinformation (wie bei einem Brief) kein gesichertes Datum darstellt. Eine Manipulation bzw. Verfälschung durch den Teilnehmer ist in einfacher Weise möglich.

Die öffentliche IP-Adresse des Absenders einer E-Mail kann eine NAT bezeichnen und damit keinen eindeutigen Rückschluss auf den Teilnehmer zulassen.

[5] siehe auch Erläuterungen zu § 102a Abs. 5

[6] siehe auch Erläuterungen zu § 102a Abs. 4 Z 1 und 2

4.5 E-Mail – An-/Abmeldung

Zweck dieses Datenformates ist Auskunft über An- und Abmeldung des Teilnehmers beim E-Mail Server.

Grundlage:

§ 102a. (4) Anbietern von E-Mail Diensten obliegt die Speicherung folgender Daten:

5. bei An- und Abmeldung beim E-Mail Dienst Datum, Uhrzeit, Teilnehmerkennung und öffentliche IP-Adresse des Teilnehmers unter Angabe der zugrundeliegenden Zeitzone.

Das Datenformat für die Abfrage von An-/Abmeldedaten beim E-Mail Server wird wie folgt festgelegt:

Feldname	Beschreibung	Syntax
Referenz		siehe Kapitel 3.1.3
IndikatorArt	MAIL	siehe Kapitel 3.1.4
Indikator	E-Mail Adresse	
TeilnehmerkennungArt	NR, MSIS, KENN	siehe Kapitel 3.1.5
Teilnehmerkennung	Festnetznummer, MSISDN, betreiberspezifische Kennung	
Anmeldung	Datum, Uhrzeit und Zeitzone der Anmeldung	siehe Kapitel 3.1.9
Abmeldung	Datum, Uhrzeit und Zeitzone der Abmeldung	siehe Kapitel 3.1.9
IP_Adresse		siehe Kapitel 3.1.14

Es gibt für die Kunden mehrere Methoden, E-Mails abzurufen. Bei Webmail-Zugang melden sich Kunden üblicherweise nicht explizit ab. Daher ist der Zeitpunkt der Abmeldung in den meisten Fällen das Time-out des E-Mail Servers, nicht aber das Schließen des Browser-Fensters.[7] Bei E-Mail Push Services (z.B. Blackberry) muss der Blackberry Server nicht im Einflussbereich des E-Mail Anbieters stehen. Es ist davon auszugehen, dass der Blackberry Server permanent beim E-Mail Server eingeloggt ist.

Die öffentliche IP-Adresse des Absenders einer E-Mail kann eine NAT bezeichnen und damit keinen eindeutigen Rückschluss auf den Teilnehmer zulassen.

[7] siehe auch Erläuterungen zu § 102a Abs. 4 Z 5

5 Annex Beispiele (informativ und exemplarisch)

Dieser Annex enthält Beispiele für Anwendungsfälle je Datenart und Indikator. Dazu werden jeweils der Header und ein Beispiel für einen Datensatz angegeben. Alle Beispieldaten sind fiktiv (der Wiener Rufnummernbereich 991 sowie die Mobilfunkkennzahlen 663 und 665 sind dzt. nicht zugeteilt, als Domain Namen wurde lt. RFC 2606 example.com verwendet, IP-Adressen wurden aus dem reservierten Bereich 192.0.2.00/24 gemäß RFC 3330 entnommen, Namen und Adressen sind fiktiv).

In Kapitel 5.1 werden die rechtlichen Grundlagen für Anfragen nach TKG, StPO und SPG zusammengefasst. Kapitel 5.2 beschreibt die Auskünfte über Vorratsdaten. Auskünfte über Daten einer Nachrichtenübermittlung haben dieselbe Struktur wie Vorratsdaten (Kapitel 5.3.). In Kapitel 5.4 ff werden diese Anfragen für die Anwendung gemäß § 76a (2) StPO und § 53 (3a) und (3b) SPG spezifiziert.

Generell stellen die Use Cases den Maximalumfang der übermittelten Daten dar. Wenn in der Anfrage eine weitere Einschränkung erfolgt, kann auch die Antwort auf die angefragten Felder eingeschränkt werden.

5.1 Rechtliche Grundlagen für Beauskunftung

Die Schnittstelle nach § 94 (4) TKG dient zur Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, einschließlich der Übermittlung von Vorratsdaten, nach den Bestimmungen der StPO sowie des SPG. Daher werden zunächst die rechtlichen Grundlagen für die Beauskunftung dieser Daten zusammengefasst.

5.1.1 TKG 2003

Nach § 90 (6) sind Anbieter von Kommunikationsdiensten verpflichtet, Verwaltungsbehörden auf deren schriftliches und begründetes Verlangen Auskunft über Stammdaten im Sinne von § 92 Abs. 3 Z 3 lit. a bis e von Teilnehmern zu geben, die in Verdacht stehen, durch eine über ein öffentliches Telekommunikationsnetz gesetzte Handlung eine Verwaltungsübertretung begangen zu haben, soweit dies ohne Verarbeitung von Verkehrsdaten möglich ist.

Nach § 90 (7) sind Anbieter von Kommunikationsdiensten auf schriftliches Verlangen der zuständigen Gerichte, Staatsanwaltschaften oder der Kriminalpolizei (§ 76a Abs. 1 StPO) verpflichtet, diesen zur Aufklärung und Verfolgung des konkreten Verdachts einer Straftat Auskunft über Stammdaten (§ 92 Abs. 3 Z 3) von Teilnehmern zu geben. Dies gilt sinngemäß für Verlangen der Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a Z 1 SPG. In dringenden Fällen können aber solche Ersuchen vorläufig mündlich übermittelt werden.

5.1.2 StPO – Auskunft über Daten einer Nachrichtenübermittlung und Auskunft über Vorratsdaten auf Grund einer richterlichen Bewilligung

Nach § 134 StPO ist die "Auskunft über Daten einer Nachrichtenübermittlung" die Erteilung einer Auskunft über Verkehrsdaten (§ 92 Abs. 3 Z 4 TKG), Zugangsdaten (§ 92 Abs. 3 Z 4a TKG) und Standortdaten (§ 92 Abs. 3 Z 6 TKG) eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes).

"Auskunft über Vorratsdaten" ist die Erteilung einer Auskunft über Daten, die Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe des § 102a Abs. 2 bis 4 TKG zu speichern haben und die nicht nach § 99 Abs. 2 TKG einer Auskunft nach Z 2 (Auskunft über Daten einer Nachrichtenübermittlung) unterliegen.

In § 135 (2) und (2a) StPO ist die Zulässigkeit der Auskunft über Daten einer Nachrichten-übermittlung und Vorratsdaten normiert.

5.1.3 StPO – Auskunft über Stamm- und Zugangsdaten auf Anordnung der Staatsanwaltschaft

Nach § 76a (2) StPO sind Anbieter von Telekommunikationsdiensten auf Anordnung der Staatsanwaltschaft zur Auskunft über folgende Daten nach § 99 Abs. 5 Z 2 TKG verpflichtet:

1. Name, Anschrift und Teilnehmerkennung des Teilnehmers, dem eine öffentliche IP-Adresse zu einem bestimmten Zeitpunkt unter Angabe der zugrunde liegenden Zeitzone zugewiesen war, es sei denn, dass diese Zuordnung eine größere Anzahl von Teilnehmern erfassen würde;

2. die bei Verwendung von E-Mail Diensten dem Teilnehmer zugewiesene Teilnehmer-kennung;

3. Name und Anschrift des Teilnehmers, dem eine E-Mail-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, und

4. die E-Mail-Adresse und die öffentliche IP-Adresse des Absenders einer E-Mail.

5.1.4 SPG - Stammdatenabfrage (Telefonie, IP-Adressen)

Nach § 53 (3a) SPG sind die Sicherheitsbehörden berechtigt, von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 - TKG 2003, BGBl. I Nr. 70) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz - ECG, BGBl. I Nr. 152/2001) Auskunft zu verlangen:

1. über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses, wenn dies zur Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben erforderlich ist,

2. über die Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung, wenn sie diese Daten als wesentliche Voraussetzung zur Abwehr
   a. einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht (§ 19),
   b. eines gefährlichen Angriffs (§ 16 Abs. 1 Z 1) oder
   c. einer kriminellen Verbindung (§ 16 Abs.1 Z 2) benötigen,
3. über Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, wenn sie diese Daten als wesentliche Voraussetzung zur Abwehr,
   a. einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht (§ 19),
   b. eines gefährlichen Angriffs (§ 16 Abs. 1 Z 1) oder
   c. einer kriminellen Verbindung (§ 16 Abs.1 Z 2) benötigen,

auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 4 iVm § 102a TKG 2003 erforderlich ist,

4. über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer, wenn dies zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder zur Abwehr gefährlicher Angriffe erforderlich ist.

5.1.5 SPG – Standortdaten, Vorratsdaten

Nach § 53 (3b) SPG gilt: "Ist auf Grund bestimmter Tatsachen anzunehmen, dass eine gegenwärtige Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen besteht, sind die Sicherheitsbehörden zur Hilfeleistung oder Abwehr dieser Gefahr berechtigt, von Betreibern öffentlicher Telekommunikationsdienste Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der von dem gefährdeten Menschen mitgeführten Endeinrichtung zu verlangen, auch wenn hiefür die Verwendung von Vorratsdaten gemäß § 99 Abs. 5 Z 3 iVm § 102a TKG 2003 erforderlich ist, sowie technische Mittel zur Lokalisierung der Endeinrichtung zum Einsatz zu bringen."

5.2 Use Cases für Auskunft über Vorratsdaten nach § 135 StPO

„Auskunft über Vorratsdaten" ist die Erteilung einer Auskunft über Daten, die Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe des § 102a Abs. 2 bis 4 TKG zu speichern haben und die nicht nach § 99 Abs. 2 TKG einer Auskunft nach Z 2 (Auskunft über Daten einer Nachrichtenübermittlung) unterliegen".

Die Daten nach Maßgabe des § 102a wurden in folgende fünf Datenarten unterteilt:

Nummer	Datenart	gesetzliche Grundlage
1	Internetzugangsdienste	§ 102a (2) Z 1 - 4 TKG
2	öffentliche Telefondienste	§ 102a (3) Z 1 - 6
3	Erstaktivierung	§ 102a (3) Z 6 c
4	E-Mail Verkehrsdaten	§ 102a (4) Z 1 - 4
5	E-Mail An-/Abmeldung	§ 102a (4) Z 5

Zur Auskunft über diese Daten sind folgende Use Cases vorgesehen:

5.2.1 Datenart Internetzugangsdienste

5.2.1.1 Indikator IP-Adresse

Anforderung: Auskunft über Vorratsdaten/Internetzugangsdienste zur IP Adresse 192.0.2.0 zu einem bestimmten Zeitpunkt

Dateiname: 100001.csv

```
"Referenz","IndikatorArt","Indikator","AnschlusskennungArt",
"Anschlusskennung","Vorname","Familienname","Adresse" CRLF

"100001","IP","192.0.2.0","KENN","45672000","Max","Mustermann",
"1030 Wien, Landstrasse 27" CRLF
```

5.2.1.2 Indikator betreiberspezifische Kennung

Anforderung: Auskunft über Vorratsdaten/Internetzugangsdienste zur Anschlusskennung 45672000 und zu einem bestimmten Zeitpunkt

Dateiname: 100002.csv

```
"Referenz","IndikatorArt","Indikator","AnschlusskennungArt",
"Anschlusskennung","Vorname","Familienname","Adresse" CRLF

"100002","KENN","45672000","IP","192.0.2.0","Max","Mustermann",
"1030 Wien, Landstrasse 27" CRLF
```

5.2.1.3 Indikator Festnetznummer

Anforderung: Auskunft über Vorratsdaten/Internetzugangsdienste zur Festnetznummer Wien 991 65 98 und zu einem bestimmten Zeitpunkt

Dateiname: 100003.csv

```
"Referenz","IndikatorArt","Indikator","AnschlusskennungArt",
"Anschlusskennung","Vorname","Familienname","Adresse" CRLF

"100003","NR","4319916598","IP","192.0.2.0","Max","Mustermann",
"1020 Wien, Landstrasse 27" CRLF
```

5.2.1.4 Indikator MSISDN

Anforderung: Auskunft über Vorratsdaten/Internetzugangsdienste zur Mobilnummer 0665 312 65 65 und zu einem bestimmten Zeitpunkt

Dateiname: 100004.csv

```
"Referenz","IndikatorArt","Indikator","AnschlusskennungArt",
"Anschlusskennung","Vorname","Familienname","Adresse" CRLF

"100004","MSIS","436653126565","IP","192.0.2.10","Max","Mustermann",
"1010 Wien, Landstrasse 27" CRLF
```

5.2.2 Datenart öffentliche Telefondienste

5.2.2.1 Indikator Festnetznummer

Anforderung: Auskunft über Vorratsdaten/öffentliche Telefondienste zur Festnetznummer Wien 991 8002 während eines bestimmten Zeitraums

Dateiname: 100005.csv

```
"Referenz","IndikatorArt","Indikator","IndikatorMSISDN","IndikatorIMSI",
"IndikatorIMEI","IndikatorVorname","IndikatorFamilienname",
"IndikatorAdresse","BetreiberId","CellId","GeoKoordinaten","Zeit","Dauer",
"Ruftyp","Richtung","PartnerMSISDN","PartnerIMSI","PartnerIMEI",
"PartnerVorname","PartnerFamilienname","PartnerAdresse","Anrufumleitung" CRLF

"100005","NR","4319918002",#,#,#,#,#,#,#,#,#,
"2010-01-12T21:23:00+01","412","T","A","436655126543",#,#,#,#,#,# CRLF
```

Bemerkung: In diesem Beispiel wird eine aktive Telefonverbindung zu einer Mobilfunknummer aufgelistet. Die Zielnummer befindet sich nicht im eigenen Netz des Festnetz-

betreibers. Daher können Stammdaten zur Zielrufnummer in diesem Beispiel nicht ermittelt werden.

5.2.2.2 Indikator MSISDN[8]

Anforderung: Auskunft über Vorratsdaten/öffentliche Telefondienste zur Mobilrufnummer 0665 98 75634 während eines bestimmten Zeitraums

Dateiname: 100006.csv

```
"Referenz","IndikatorArt","Indikator","IndikatorMSISDN","IndikatorIMSI",
"IndikatorIMEI","IndikatorVorname","IndikatorFamilienname",
"IndikatorAdresse","BetreiberId","CellId","GeoKoordinaten","Zeit","Dauer",
"Ruftyp","Richtung","PartnerMSISDN","PartnerIMSI","PartnerIMEI",
"PartnerVorname","PartnerFamilienname","PartnerAdresse","Anrufumleitung" CRLF

"100006","MSIS","436659875634",#,"232031234567890",
"35-209900-176148-1",#,#,#,"T-Mobile","87543","16.151715/45.758972",
"2010-01-12T21:23:00+01","42","T","P","436655126543",#,#,#,#,#,# CRLF
```

Bemerkung: In diesem Beispiel wird eine passive Telefonverbindung zu einer anderen Mobilfunknummer inkl. IMSI, IMEI, Cell-Id und geografische Koordinaten aufgelistet. Die Zielnummer befindet sich nicht im eigenen Netz des Mobilfunknetzbetreibers. Daher können Stammdaten zur Zielrufnummer in diesem Beispiel nicht ermittelt werden.

5.2.2.3 Indikator IMEI

Anforderung: Auskunft über Vorratsdaten/öffentliche Telefondienste zur IMEI 35-209900-176148-1 während eines bestimmten Zeitraums

Dateiname: 100007.csv

```
"Referenz","IndikatorArt","Indikator","IndikatorMSISDN","IndikatorIMSI",
"IndikatorIMEI","IndikatorVorname","IndikatorFamilienname",
"IndikatorAdresse","BetreiberId","CellId","GeoKoordinaten","Zeit","Dauer",
"Ruftyp","Richtung","PartnerMSISDN","PartnerIMSI","PartnerIMEI",
"PartnerVorname","PartnerFamilienname","PartnerAdresse","Anrufumleitung" CRLF

"100007","IMEI","35-209900-176148-1",
"436769875634","232031234567890",#,#,#,#,"T-Mobile","87543",
"16.151715/45.758972","2010-01-12T21:23:00+01","42","T","P",
"436655126543",#,#,#,#,#,# CRLF
```

[8] GeoKoordinaten werden in den Beispielen in Graddezimal kodiert.

Bemerkung: In diesem Beispiel wird eine passive Telefonverbindung zu einer anderen Mobilfunknummer inkl. MSISDN, IMSI, Cell-Id und Geo Koordinaten aufgelistet. Die Zielnummer befindet sich nicht im eigenen Netz des Mobilfunknetzbetreibers. Daher können Stammdaten zur Zielrufnummer in diesem Beispiel nicht ermittelt werden.

5.2.2.4 Indikator IMSI

Anforderung: Auskunft über Vorratsdaten/öffentliche Telefondienste zur IMSI 232031234567890 während eines bestimmten Zeitraums

Dateiname: 100008.csv

```
"Referenz","IndikatorArt","Indikator","IndikatorMSISDN","IndikatorIMSI",
"IndikatorIMEI","IndikatorVorname","IndikatorFamilienname",
"IndikatorAdresse","BetreiberId","CellId","GeoKoordinaten","Zeit","Dauer",
"Ruftyp","Richtung","PartnerMSISDN","PartnerIMSI","PartnerIMEI",
"PartnerVorname","PartnerFamilienname","PartnerAdresse","Anrufumleitung" CRLF

"100008","IMSI","232031234567890","436659875634",#,
"35-209900-176148-1",#,#,#,"T-Mobile","87543","16.151715/45.758972",
"2010-01-12T21:23:00+01","42","T","P","436635126543",#,#,#,#,#,# CRLF
```

Bemerkung: In diesem Beispiel wird eine passive Telefonverbindung zu einer anderen Mobilfunknummer inkl. MSISDN, IMEI, Netzbetreiber, Cell-Id und Geo Koordinaten aufgelistet. Die Zielnummer befindet sich nicht im eigenen Netz des Mobilfunknetzbetreibers. Daher können Stammdaten zur Zielrufnummer in diesem Beispiel nicht ermittelt werden.

5.2.2.5 Indikator Cell-Id

Anforderung: Auskunft über Vorratsdaten/öffentliche Telefondienste zur Cell-Id 76465 während eines bestimmten Zeitraums

Dateiname: 100009.csv

```
"Referenz","IndikatorArt","Indikator","IndikatorMSISDN","IndikatorIMSI",
"IndikatorIMEI","IndikatorVorname","IndikatorFamilienname",
"IndikatorAdresse","BetreiberId","CellId","GeoKoordinaten","Zeit","Dauer",
"Ruftyp","Richtung","PartnerMSISDN","PartnerIMSI","PartnerIMEI",
"PartnerVorname","PartnerFamilienname","PartnerAdresse","Anrufumleitung" CRLF

"100009","CELL","76465","436654527634",
"232031234567890","35-209900-176148-1","Max","Mustermann",
"2020 Graz, Wohnstrasse 45","T-Mobile","76465","16.151715/45.758972",
"2010-01-12T21:23:00+01","42","T","P","436635126543",#,#,#,#,#,# CRLF
```

Bemerkung: In diesem Beispiel wird eine Telefonverbindung zwischen zwei Mobilfunkteilnehmern aufgezeichnet. Zu aktiven Teilnehmer werden MSISDN, IMSI, IMEI, Stammdaten und Geo Koordinaten aufgelistet. Die Zielnummer befindet sich nicht im eigenen Netz des Mobilfunknetzbetreibers. Daher können Stammdaten zur Zielrufnummer in diesem Beispiel nicht ermittelt werden.

5.2.2.6 Indikator Zielrufnummer

Anforderung: Auskunft über Vorratsdaten/öffentliche Telefondienste zur Zielrufnummer Wien 991 5432 während eines bestimmten Zeitraums

Dateiname: 100010.csv

```
"Referenz","IndikatorArt","Indikator","IndikatorMSISDN","IndikatorIMSI",
"IndikatorIMEI","IndikatorVorname","IndikatorFamilienname",
"IndikatorAdresse","BetreiberId","CellId","GeoKoordinaten","Zeit","Dauer",
"Ruftyp","Richtung","PartnerMSISDN","PartnerIMSI","PartnerIMEI",
"PartnerVorname","PartnerFamilienname","PartnerAdresse","Anrufumleitung" CRLF

"100010","ZIEL","4319915432",#,#,#,#,#,#,#,#,#,#,
"2010-01-12T21:23:00+01","22","T","A","4319914534",#,#,"Max","Mustermann",
"2322 Baden, Wohnstrasse 45",# CRLF
```

Bemerkung: In diesem Beispiel wird eine Telefonverbindung zu dieser Zielrufnummer von der Wiener Rufnummer 991 4534 aufgezeichnet. Zu dieser Rufnummer sind auch die Stammdaten enthalten. Es handelt sich um ein Aktivgespräch aus Sicht der Rufnummer 991 4534. Die Zielrufnummer befindet sich in einem Fremdnetz.

5.2.3 Datenart Erstaktivierung

Anforderung: Auskunft über Vorratsdaten/Erstaktivierung zur MSISDN 06637543234

Dateiname: 100011.csv

```
"Referenz","IndikatorArt","Indikator","BetreiberId","CellId",
"GeoKoordinaten","Zeit" CRLF

"100011","MSIS","436637543234","Orange","76543",
"16.151715/45.758972","2010-01-12T21:23:00+01" CRLF
```

5.2.4 Datenart E-Mail Verkehrsdaten

Anforderung: Auskunft über Vorratsdaten/E-Mail Verkehrsdaten zur E-Mail Adresse max@example.com während eines bestimmten Zeitraums

Dateiname: 100012.csv

```
"Referenz","IndikatorArt","Indikator","TeilnehmerkennungArt",
"Teilnehmerkennung","Zeit","GesendetAbsender","GesendetAbsenderIP_Adresse",
"GesendetEmpfaenger","EmpfangAbsender","EmpfangZiel","EmpfangIP_Adresse" CRLF
```

Gesendete E-Mail:

```
"100012","MAIL","max@example.com","NR","4319918767",
"2010-01-12T21:23:00+01","max@example.com","192.0.2.20",
"mona@example.com",#,#,# CRLF
```

Empfangene E-Mail:

```
"100012","MAIL","max@example.com","NR","4319918767",
"2010-01-12T21:23:12+01",#,#,#,"mona@example.com","max@example.com",
"192.0.2.10" CRLF
```

5.2.5 Datenart E-Mail An-/Abmeldung

Anforderung: Auskunft über Vorratsdaten/E-Mail An-/Abmeldung zur E-Mail Adresse max@example.com während eines bestimmten Zeitraums

Dateiname: 100013.csv

```
"Referenz","IndikatorArt","Indikator","TeilnehmerkennungArt",
"Teilnehmerkennung","Anmeldung","Abmeldung",IP_Adresse" CRLF

"100013","MAIL","max@example.com","NR","4319918767",
"2010-01-12T21:23:00+01",#,"192.0.2.5" CRLF
```

5.2.6 Beispiel für Auskunft über mehrere Daten

Am 2. Februar 2010 wird unter der Referenz 100014 eine Anfrage nach den Indikatoren MSISDN 0663 8752368 sowie 0665 7646893 und der Datenart Internetzugangsdienste gestellt.

Als Ergebnis werden zwei "csv"-Files mit folgenden Dateinamen erzeugt:

Dateiname 1: 100014_1.csv
Dateiname 2: 100014_2.csv

5.3 Auskunft über Daten einer Nachrichtenübermittlung

Nach § 134 StPO gehören dazu Verkehrsdaten, Zugangsdaten und Standortdaten:

§ 92 (3) Z 4 TKG: "Verkehrsdaten" Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;

§ 92 (3) Z 4a TKG: "Zugangsdaten" jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind;

§ 92 (3) Z 6 TKG: "Standortdaten" Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben;

Die Auskunft über Daten einer Nachrichtenübermittlung betrifft eine Untermenge der Daten, die als Vorratsdaten erfasst werden Daher kommen für die Beauskunftung die gleichen Use Cases zur Anwendung wie auch für Vorratsdaten. Dabei sind allerdings die Bestimmungen über die Zulässigkeit der Datenspeicherung zu beachten.

Nach § 99 (1) TKG dürfen Verkehrsdaten außer in den gesetzlich geregelten Fällen nicht gespeichert werden und sind vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren. Nach § 99 (2) TKG gilt: *"Sofern dies für Zwecke der Verrechnung von Entgelten, einschließlich der Entgelte für Zusammenschaltungen, erforderlich ist, hat der Betreiber Verkehrsdaten bis zum Ablauf jener Frist zu speichern, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht werden kann. Diese Daten sind im Streitfall der entscheidenden Einrichtung sowie der Schlichtungsstelle unverkürzt zur Verfügung zu stellen. Wird ein Verfahren über die Höhe der Entgelte eingeleitet, dürfen die Daten bis zur endgültigen Entscheidung über die Höhe der Entgelte nicht gelöscht werden. Der Umfang der gespeicherten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken."*

Die konkrete Speicherdauer hängt vom Geschäftsmodell und den betrieblichen Notwendigkeiten des jeweiligen Netzbetreibes ab.

5.4 Auskunft nach § 76a (2) Z 1 StPO

Es sind nach § 76a (2) Z 1 StPO zu beauskunften: Name, Anschrift und Teilnehmerkennung des Teilnehmers, dem eine öffentliche IP-Adresse zu einem bestimmten Zeitpunkt unter Angabe der zugrunde liegenden Zeitzone zugewiesen war, es sei denn dass diese Zuordnung eine größere Anzahl von Teilnehmern erfassen würde.

Use Case Internetzugangsdienste, Indikator IP-Adresse

Anforderung: Auskunft gemäß § 76a (2) Z 1 StPO nach der IP Adresse 192.0.2.6 zum Zeitpunkt 13.1.2010, 01:00:00 Uhr.

Dateiname: 200001.csv

```
"Referenz","IndikatorArt","Indikator","AnschlusskennungArt",
"Anschlusskennung","Vorname","Familienname","Adresse" CRLF

"200001","IP","192.0.2.6","KENN","45672000","Max","Mustermann",
"2343 Wr. Neustadt, Landstrasse 27" CRLF
```

5.5 Abfrage nach § 76a (2) Z 2 StPO

Anforderung: Auskunft über die bei Verwendung von E-Mail Diensten dem Teilnehmer zugewiesene Teilnehmerkennung.

Use Case E-Mail Verkehrsdaten

Anforderung: Auskunft gemäß § 76a (2) Z 2 StPO nach der E-Mail Adresse max@example.com

Bemerkung: Bei dieser Abfrage werden die aktuellen Daten übermittelt.

Dateiname: 200002.csv

```
"Referenz","IndikatorArt","Indikator","TeilnehmerkennungArt",
"Teilnehmerkennung","Zeit","GesendetAbsender","GesendetAbsenderIP_Adresse",
"GesendetEmpfaenger","EmpfangAbsender","EmpfangZiel","EmpfangIP_Adresse" CRLF

"200002","MAIL","max@example.com","NR","4319918767",#,#,#,#,#,#,# CRLF
```

5.6 Abfrage nach § 76a (2) Z 3 StPO

Anforderung: Auskunft über Name und Anschrift des Teilnehmers, dem eine E-Mail-Adresse zu einem bestimmten Zeitpunkt zugewiesen war.

Diese Anfrage entspricht zunächst jener nach Kapitel 5.5., wobei historische Daten erhoben werden. Im zweiten Schritt erfolgt die Zuordnung zu den damals gültigen Stammdaten.

5.7 Abfrage nach § 76a (2) Z 4 StPO

Anforderung: Auskunft über die E-Mail-Adresse und die öffentliche IP-Adresse des Absenders einer E-Mail.

Use Case E-Mail Verkehrsdaten

Anforderung: Auskunft gemäß § 76a (2) Z 4 StPO nach der E-Mail Adresse max@example.com

Dateiname: 200003.csv

```
"Referenz","IndikatorArt","Indikator","TeilnehmerkennungArt",
"Teilnehmerkennung","Zeit","GesendetAbsender","GesendetAbsenderIP_Adresse",
"GesendetEmpfaenger","EmpfangAbsender","EmpfangZiel","EmpfangIP_Adresse" CRLF
```

Empfangene E-Mail:

```
"200003","MAIL","max@example.com","NR","4319918767",
```

```
"2010-01-12T21:23:12+01",#,#,#,"mona@example.com","max@example.com",
"192.0.2.10" CRLF
```

5.8 Auskunft nach § 53 (3a) Z 2 SPG

Anforderung: Auskunft über die Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung.

Bemerkung: Die Schnittstellendefinition gemäß § 94 (4) TKG richtet sich schon aufgrund der Normenadressaten ausschließlich an Anbieter im Sinne des TKG, nicht jedoch an Anbieter von "Diensten der Informationsgesellschaft" im Sinne des § 3 Z 2 E-Commerce-Gesetz, auf den § 53 (3a) Z 2 SPG ebenfalls verweist. In dieser Schnittstellendefinition sind daher nur jene Use-Cases erfasst, welche einen Anbieter im Sinne des TKG überhaupt betreffen können. Im Hinblick auf den Regelungsgehalt des § 53 (3a) Z 2 SPG (siehe oben) kann dies nur Anbieter von E-Mail Diensten betreffen, während beispielsweise Logfiles zu Webshops, Foren, Chatrooms, etc. sich ausschießlich nach dem ECG richten und daher nicht von dieser Schnittstellendefinition erfasst sind. Die Übermittlung von Auskünften solcher Anbieter wird durch die gegenständlichen Rechtsänderungen nicht berührt.

Arbeitshypothese ist, dass die Nachricht durch E-Mail Adresse von Sender und Empfänger sowie den Zeitpunkt der Übermittlung identifiziert wird. Dementsprechend kann der Use Case E-Mail Verkehrsdaten für Sende- oder Empfangsadresse herangezogen werden. Im folgenden Beispiel wird die Sendeadresse ausgewertet. Die IP-Adresse bezieht sich auf den Sender. In gleicher Weise kann eine Abfrage der Empfänger E-Mail Adresse erfolgen, welche dann die IP-Adresse des Empfängers liefert.

Use Case E-Mail Verkehrsdaten

Anforderung: Auskunft nach § 53 (3a) Z 2 SPG zur E-Mail Sendeadresse max@example.com und Empfangsadresse Mona@example.com, Zeitpunkt

Dateiname: 300001.csv

```
"Referenz","IndikatorArt","Indikator","TeilnehmerkennungArt",
"Teilnehmerkennung","Zeit","GesendetAbsender","GesendetAbsenderIP_Adresse",
"GesendetEmpfaenger","EmpfangAbsender","EmpfangZiel","EmpfangIP_Adresse" CRLF
```

Gesendete E-Mail:

```
"300001","MAIL","max@example.com","NR","4319918767",
"2010-01-12T21:23:00+01","max@example.com","192.0.2.20",
"mona@example.com",#,#,# CRLF
```

5.9 Abfrage nach § 53 (3a) Z 3 SPG

Anforderung: Auskunft über Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war.

Use Case Internetzugangsdienste, Indikator IP-Adresse

Anforderung: Auskunft nach § 53 (3a) Z 3 SPG zur IP Adresse 112.64.33.121 zum Zeitpunkt 13.1.2010, 01:00:00 Uhr.

Bemerkung: Die Teilnehmerkennung wird für diese Abfrage nicht übermittelt.

Dateiname: 300002.csv

```
"Referenz","IndikatorArt","Indikator","AnschlusskennungArt",
"Anschlusskennung","Vorname","Familienname","Adresse" CRLF

"300002","IP","112.64.33.121",#,#,"Max","Mustermann",
"1234 Stockerau, Landstrasse 27" CRLF
```

5.10 Anfrage nach § 53 (3a) Z 4 SPG

Anforderung: Auskunft über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer.

Use Case Öffentliche Telefondienste, Indikator Festnetznummer bzw. MSISDN

Bemerkung: Für diese Auswertung sind zunächst die Verkehrsdaten der vorgegebenen passiven Teilnehmernummer abzufragen. Dabei werden sich u.U. mehrere A-Rufnummern ergeben, weil die Anfrage lediglich unter Angabe eines möglichst genauen Zeitraumes zu erfolgen hat, der gemäß Erlass des BMI maximal eine Stunde betragen darf. Je stärker dieser Zeitraum bei der Anfrage eingeschränkt wird, desto zielgenauer kann die Auskunft erfolgen und damit der Verfahrensaufwand reduziert werden. Die Ermittlung der zugehörigen Stammdaten kann allerdings nur durch den jeweiligen Netzbetreiber erfolgen. Daher ist für diese Auswertung u.U. eine zweistufige Vorgangsweise erforderlich.

Anforderung: Auskunft gemäß § 53 (3a) Z 4 SPG zur Zielrufnummer Wien 991 5432 zwischen 12.1.2010, 23:00 und 24:00 Uhr.

Dateiname: 300003.csv

```
"Referenz","IndikatorArt","Indikator","IndikatorMSISDN","IndikatorIMSI",
"IndikatorIMEI","IndikatorVorname","IndikatorFamilienname",
"IndikatorAdresse","BetreiberId","CellId","GeoKoordinaten","Zeit","Dauer",
"Ruftyp","Richtung","PartnerMSISDN","PartnerIMSI","PartnerIMEI",
"PartnerVorname","PartnerFamilienname","PartnerAdresse","Anrufumleitung" CRLF

"300003","ZIEL","4319915432",#,#,#,#,#,#,#,#,#,#,
"2010-01-12T21:23:30+01","22","T","A","4319914534",#,#,#,#,#,# CRLF
```

Bemerkung: In diesem Beispiel wird eine Telefonverbindung zu dieser Zielrufnummer von der Wiener Rufnummer 991 4534 aufgezeichnet. Zu dieser Rufnummer sind keine Stammdaten enthalten, da sich diese in einem Fremdnetz befindet.

Zur Ermittlung der Stammdaten muss eine Anfrage an den Betreiber gestellt werden, in dessen Netz die Wiener Rufnummer 991 4534 angeschaltet ist.

5.11 Anfrage nach § 53 (3b) SPG

Anforderung: Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der von dem gefährdeten Menschen mitgeführten Endeinrichtung.

Use Case Öffentliche Telefondienste, Indikator MSISDN

Anforderung: Auskunft nach § 53 (3b) SPG zur MSISDN 0665 98 75634 zur Ermittlung des aktuellen Aufenthaltsorts

Bemerkung: Die Beauskunftung wird im Regelfall wegen Gefahr im Verzug formlos telefonisch erfolgen. Die Anfrage muss aber über die DLS nachgereicht werden.

Dateiname: 300004.csv

```
"Referenz","IndikatorArt","Indikator","IndikatorMSISDN","IndikatorIMSI",
"IndikatorIMEI","IndikatorVorname","IndikatorFamilienname",
"IndikatorAdresse","BetreiberId","CellId","GeoKoordinaten","Zeit","Dauer",
"Ruftyp","Richtung","PartnerMSISDN","PartnerIMSI","PartnerIMEI",
"PartnerVorname","PartnerFamilienname","PartnerAdresse","Anrufumleitung" CRLF

"300004","MSIS","436659875634",#,"232031234567890",#,#,#,#,"T-Mobile",
"87543","16.151715/45.758972",#,#,#,#,#,#,#,#,#,#,# CRLF
```

Abstract zur Dissertation **Christof Tschohl / Matrikelnummer 0207311**

„Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung in Österreich“

Die vorliegende Arbeit ist eine rechtswissenschaftliche Untersuchung der Datensicherheit im Rahmen der österreichischen Umsetzung der Vorratsdatenspeicherung gemäß der Richtlinie 2006/24/EG, welche die flächendeckende vorrätige Speicherung von Telekommunikationsverbindungs- und Zugangsdaten durch alle Anbieter öffentlicher elektronischer Kommunikationsnetze und -Dienste innerhalb der EU vorschreibt. Die Bereitstellung solcher Dienste beinhaltet regelmäßig die Verarbeitung von personenbezogenen Daten der Nutzer. Die österreichische Umsetzung der Richtlinie erfolgte durch eine Novelle zum Telekommunikationsgesetz (TKG 2003) und wurde am 18. Mai 2011 im Bundesgesetzblatt kundgemacht (BGBl. I Nr. 27/2011), wobei die Speicherverpflichtung für die Anbieter erst mit 1.4.2012 in Kraft treten wird. Das Gesetz enthält jedoch zur Datensicherheit nur relativ grobe Vorgaben, die detaillierte Ausgestaltung bleibt einer Verordnung in Ausführung der §§ 94 Abs. 4 und 102c TKG vorbehalten. Um dem Datenschutzgesetz und dem Telekommunikationsgeheimnis sowie den Vorgaben der Europäischen Menschenrechtskonvention, insbesondere dessen Artikel 8 zum Schutz des Privatlebens und der Korrespondenz zu entsprechen, müssen diese Daten geheim gehalten werden, wozu insbesondere auch Maßnahmen auf der technischen Ebene notwendig sind, die auf der rechtlichen Ebene erfasst und beschrieben werden müssen. Die Verpflichtung zur effektiven Wahrung der Grundrechte aller Nutzer erfordert dabei auch, ein System einer revisionssicheren Protokollierung zu etablieren und so eine ausreichende Nachvollziehbarkeit für den Rechtsschutz zu gewährleisten.

Die Zielsetzung dieser Dissertation ist, im ersten Teil (Kapitel II) ausgehend von den Grundrechten und dem Europarecht bis hin zur innerstaatlichen Umsetzung den normativen Unterbau zu evaluieren, der für die Beschreibung eines Sorgfaltsmaßstabs auf rechtlicher und technischer Ebene bei der Verarbeitung und Übermittlung von Verkehrsdaten relevant ist, unter besonderer Beachtung eines hohen Niveaus an Datensicherheit und Grundrechtsschutz. Die Arbeit behandelt sowohl das Thema der Datensicherheit bei den Anbietern unternehmensintern, als auch im Zusammenhang mit der Übermittlung von personenbezogenen Daten im Falle einer Auskunft an Sicherheits- und Strafverfolgungsbehörden. Da in der Praxis der Schwerpunkt der Datensicherheitsprobleme eindeutig bei der sicheren Übermittlung der Daten liegt, steht im Zentrum des zweiten Teils ein Konzept einer zentralen Datendrehscheibe (Kapitel III). Die sogenannte „Durchlaufstelle“ (DLS) wird in der Arbeit als Referenzmodell entwickelt und dargestellt. Personenbezogene Inhalte werden nach diesem Konzept verschlüsselt zwischen Absender und Empfänger ausgetauscht und sind der DLS nicht zugänglich. Die Beteiligten sind über gesicherte Transportverbindungen mit fortgeschrittenen Signaturen angebunden, identifiziert und authentifiziert. Das System wirkt durch die zentrale Protokollierung aller Auskunftsvorgänge auch auf die Datensicherheit beim Anbieter und die Rechtsschutzmöglichkeiten zurück.

Im Dritten Teil werden im Speziellen insgesamt 13 wesentliche Problemkreise und deren Fragestellungen diskutiert, die für die Praxis mit den Anforderungen an eine sichere Datenübermittlung einhergehen. Die Behandlung jedes Problemkreises schließt mit einem konkreten Vorschlag, wie den jeweiligen Fragen im Rahmen einer Umsetzungsverordnung zur Datensicherheit begegnet werden könnte, um den Vorgaben aus der normativen Analyse des ersten Teils zu entsprechen. Technische Anforderungen werden dabei normativ formuliert, um die wesentlichen Funktionen technischer Hilfsmittel rechtlich hinreichend zu determinieren.

Abstract of dissertation **Christof Tschohl / Matrikelnummer 0207311**

„Data security in the implementation of data retention in Austria“

This paper is a jurisprudential dissertation on data security within the framework of the Austrian transposition of data retention in accordance with Directive 2006/24/EC, which requires the coverage of stock retention of telecommunications connectivity and access by all providers of public electronic communications networks and services within the EU. The provision of such services regularly includes the processing of personal data of users. The Austrian implementation of the directive through an amendment to Telecommunication Law (TKG 2003) was promulgated in the Federal Law Gazette on 18 May 2011 (BGBl. I Nr. 27/2011), the obligation on the side of the providers to store data will enter into force until 1 April 2012. The Act contains relatively crude specifications regarding data security standards. Data security standards will be included in a detailed manner by a regulation to § § 94 para 4 and 102c TKG. To comply with the Data Protection Act and the secrecy of telecommunications as well as the European Convention on Human Rights, particularly Article 8 concerning the private life and correspondence, this data must be kept secret. In this regard, there are in particular measures necessary at the technical level. The demand for effective protection of fundamental rights of all users requires establishing a system of tamper-proof logging and thus ensuring adequate accountability for the legal protection.

The objective of this dissertation in its first part (chapter II) is to evaluate technical solutions based on the legal requirements from Fundamental Rights and European Law to the national implementation with relevance for the description of the standard of care for the transmission of traffic data on legal and technical level. A special focus is put on the high standard of data protection and the protection of Fundamental Rights. The work deals with both the issues of data security for the provider internally, as well as the transfer of personal data and information in context of requests for disclosure by security and law enforcement authorities. In practice the emphasis focuses on problems of data security linked to the transmission of data. Therefore the second part (chatpter III) of the dissertation will mainly deal with the concept of a data-hub. The so called „Durchlaufstelle“ (DLS), a special mailbox-system, is developed and explained as reference model in this work. According to this concept personal data will be encrypted and exchanged through the DLS between sender and receiver but can’t be seen from the point of the DLS. Those involved will be connected, identified and authenticated through a secured communication channel using an advanced electronic signature. The system will also perform the central record of all requests and will hereby play an important role in data security on the side of the supplier and in the possibility of appeals.

In the third part the most relevant practical problems that arise are divided into 13 fields of topics and discussed in detail. This discussion will emphasize the requirements on a secure data transmission. Every covered topic is followed by a definite proposal, which points out how the certain question could be solved in an implementing regulation on data security in order to match the normative analysis from the first part. Technical requirements will be verbalized in a normative way in order to determine technical equipments legally.

Lebenslauf

Ing. Mag. Christof Tschohl

Ausbildung

• Doktoratsstudium der Rechtswissenschaften (Universität Wien, seit 09/2006)
Spezialisierung Grund- und Menschenrechte/Datenschutzrecht

• Magisterstudium der Rechtswissenschaften (Universität Wien, 09/2002 - 06/2006)
Spezialisierung Europarecht, Grund- und Menschenrechte

• Höhere Technische Lehranstalt für Elektronik und Nachrichtentechnik
(HTL Rankweil 09/1992 - 06/1997), Spezialisierung Nachrichtentechnik und Digitaltechnik

Berufserfahrung

• Wissenschaftlicher Mitarbeiter am Ludwig Boltzmann Institut für Menschenrechte (BIM), Wien
(seit 09/2007)

• juristischer Mitarbeiter in der Rechtsanwaltskanzlei Mag. Franz Paul, Wien
(01/2006 - 12/2007)

• Wissenschaftlicher Mitarbeiter in der Rechtsanwaltskanzlei Galla & Herget Rechtsanwälte, Wien
(01/2006 - 06/2007)

• System Engineer für Telefon- und IT-Systeme bei Fa. Kapsch Business Com, Wien
(09/2002 - 12/2005)

• Service- und Inbetriebnahmetechniker für Telefon- und IT-Systeme bei Fa Ericsson, Dornbirn
(09/1998 - 08/2002)

Kernkompetenzen

• Forschungstätigkeit im Bereich Menschenrechte, insbesondere im Zusammenhang mit Datenschutzrecht, Sicherheitspolizeirecht, Strafrecht und Strafprozessrecht

• Entwicklung und Implementierung des Grundrechtsmoduls für die Österreichische RichterInnenausbildung (Schulungsunterlagen, Seminare, Trainings)

• Tätigkeit als Trainer im Rahmen des Grundrechtsmoduls für RichteramtsanwärterInnen

• Expertise im Bereich Menschenrechtsbildung (Lehrveranstaltungen, Vorträge)

• Koordination und inhaltliche Betreuung von Projekten zum Datenschutz im Hinblick auf elektronische Kommunikation (Vorratsdatenspeicherung, gerichtliche und polizeiliche Überwachungsbefugnisse)

• Konzeption und Ausarbeitung von Projektanträgen/Veranstaltungen