Evaluation und Lösungsvorschläge zu den Auswirkungen der Datenschutz-Grundverordnung auf Kleinunternehmen und Einzelpersonen

Bachelorarbeit zur Erlangung des Bachelor-Grades
Bachelor of Science im Studiengang Informatik
an der Fakultät für Informatik und Ingenieurwissenschaften
der Technischen Hochschule Köln

vorgelegt von:	Alexander Chrysanth Kosmehl
Matrikel-Nr.:	1111 0545
Adresse:	La-Roche-Sur-Yon-Str. 9
	51643 Gummersbach
	Alexander_Chrysanth.Kosmehl@smail.th-koeln.de

eingereicht bei:	Prof. Dr. Birgit Bertelsmeier
Zweitgutachter/in:	Prof. Dr. Heide Faeskorn-Woyke

Gummersbach, 02.08.2018

Technology
Arts Sciences
TH Köln

Kurzfassung

Ziel dieser Arbeit ist die Entwicklung eines Leitfadens für die Anpassung von Webseiten und unternehmensinternen Prozessen an die Vorgaben der neuen Datenschutz-Grundverordnung. Die Zielgruppen dieses Leitfadens sind in erster Linie Einzelpersonen und Kleinunternehmen, die keine eigene Rechtsabteilung oder Arbeitsgemeinschaften haben, die sich mit der Umsetzung der Datenschutz-Grundverordnung befassen können. Die erarbeiteten Erkenntnisse sind jedoch auch für mittelständische Unternehmen, Vereine und gemeinnützige Institutionen interessant.

Nach einer Erläuterung der technischen und rechtlichen Grundlagen, werden die wichtigsten Neuerungen durch die Verordnung zusammengefasst. Anschließend werden die wesentlichen Probleme der Zielgruppen erläutert, leitfadenartig verschiedene Lösungsansätze vorgestellt und ein Fazit zur aktuellen Situation gezogen.

Inhalt

1 Einleitung

1.1 Aktuelle Situation und Problemstellung

Zu Beginn dieser Arbeit waren es noch wenige Wochen, bis die Datenschutz-Grundverordnung in Kraft treten würde. Zu dieser Zeit gab es verschiedenste Meldungen in der Zeitung, im Radio und im Internet, die die schlechte Vorbereitung auf die neue Datenschutzverordnung kritisierten. Die Webseite IT-Business schrieb hier beispielsweise:

> ***Mittelständler tun sich schwer***
>
> *44 Prozent der befragten Unternehmen geben an, dass sie noch keine konkreten technologischen oder organisatorischen Maßnahmen zur Vorbereitung auf die DSGVO getroffen haben. […]*
>
> ***Der Überblick fehlt***
>
> *[…] Umso erschreckender, dass 23 Prozent der Befragten nicht wissen, wo ihre Daten gespeichert werden. 27 Prozent können nicht genau sagen, wer Zugriff auf personenbezogene Daten hat und 34 Prozent sind die Löschfristen nicht bekannt. Darüber hinaus geben 37 Prozent der Studienteilnehmer an, dass Dokumente unkontrolliert auf den Fileservern unter der Obhut der Mitarbeiter liegen. […]*[1]

Inzwischen sind wenige Monate seit dem Inkrafttreten der Verordnung vergangen und Zeitungen beziehungsweise Onlineplattformen wie die "Zeit" schreiben von einer Überforderung für Blogger und Vereine[2], "Heise" berichtet von einer ganzen „Abmahn-Maschinerie“[3] und die "Bild-Zeitung" trägt Schlagzeilen zum „Datenschutz-Wahnsinn“[4].

Interessant ist hier insbesondere, dass sich ausgerechnet große Datengiganten wie Google und Facebook vollständig auf die neue Datenschutz-Grundverordnung umgestellt haben und Leitfäden bieten, wie Nutzer beispielsweise von Google bereitgestellte Werbung datenschutzkonform in ihre Webseite einbinden können.

Von Abmahnungen bedroht werden hingegen hauptsächlich

- kleine und mittelständige Unternehmen, die eigene Webseiten besitzen,
- Vereine, die ihre Mitglieder verwalten wollen,
- sowie Einzelpersonen, die Blogs oder ähnliches führen,

[1] (Schuster, 2017)

[2] (Hegemann, 2018)

[3] (Bleich, 2018)

[4] (Bild, 2018)

da diese meist nicht die menschlichen/technischen/finanziellen Ressourcen besitzen, um eine eigene Abteilung oder Arbeitsgemeinschaft zu gründen, die sich mit einer Umsetzung der Datenschutzverordnung befasst, wie es die großen Unternehmen können.

1.2 Ziel der Arbeit

Diese Arbeit hat also nun das Ziel, zunächst die neue Verordnung zu untersuchen und die wichtigsten Grundlagen und Neuerungen zusammenzufassen.

Anschließend soll anhand eines Leitfadens insbesondere Kleinunternehmen und Einzelpersonen die Möglichkeit geboten werden, die eigene Situation zunächst zu analysieren, dann die eigene Webseite oder Dienstleistungen anzupassen und außerdem die größten Fallen zu umgehen.

Zudem wird beschrieben, welche Maßnahmen getroffen werden können, um eine gesetzeskonforme Absicherung im Sinne der Verordnung – und damit auch gegen Abmahnungen gefeit zu sein – zu erreichen.

Abschließend wird rückblickend ein Fazit zur neuen Datenschutz-Grundverordnung und ihren Auswirkungen gegeben.

2 Grundlagen

2.1 Was ist die Datenschutz-Grundverordnung?

Die Datenschutz-Grundverordnung, kurz DSGVO, ist eine Verordnung der Europäischen Union, die dazu dienen soll, personenbezogene Daten innerhalb der EU zu schützen und einen freien Datenverkehr innerhalb dieser sicherzustellen. Des Weiteren werden mit ihr die verschiedenen lokalen Gesetze der einzelnen Mitgliedsstaaten unter einer Verordnung zusammengefasst und vereinheitlicht.

In Kraft getreten ist die Datenschutz-Grundverordnung am 24. Mai 2016, allerdings handelte es sich in den ersten zwei Jahren um eine Übergangsphase, weshalb sie erst ab dem 25. Mai 2018 anzuwenden war.

Die Verordnung ersetzt die „Richtlinie 94/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ aus dem Jahre 1995. Hierbei ist anzumerken, dass es sich nicht mehr um eine Richtlinie, sondern um eine Verordnung handelt. Richtlinien sind nicht unmittelbar wirksam, sondern müssen nach ihrer Festlegung erst durch nationale Rechtsakte umgesetzt werden. Verordnungen hingegen sind unmittelbar in allen Mitgliedsstaaten wirksam und allgemein gültig.

Auf das zeitgleich in Kraft getretene Bundesdatenschutzgesetz-neu, das die Datenschutz-Grundverordnung auf Bundesebene ergänzt und konkretisiert, wird zusätzlich eingegangen, wenn eine Relevanz für die betroffenen "Kleinunternehmen und Einzelpersonen" gegeben ist.

2.2 Ziele der Datenschutz-Grundverordnung

Die DSGVO hat verschiedene Ziele:

1. Den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihr Recht auf Schutz personenbezogener Daten[5]
2. Den freien Verkehr personenbezogener Daten in der Union[6]

[5] Vgl. Art. 1 Abs. 2 DSGVO Gegenstand und Ziele

[6] Vgl. Art. 1 Abs. 3 DSGVO Gegenstand und Ziele

2.3 Grundsätze der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung basiert auf folgenden Prinzipien[7]:

2.3.1 Rechtmäßigkeit

Alle verarbeiteten Daten müssen in einer für die betroffene Person nachvollziehbaren und rechtmäßigen Weise verarbeitet werden. Des Weiteren gilt der Grundsatz von Treu und Glauben.

2.3.2 Zweckbindung

Alle erhobenen Daten dürfen ausschließlich für die festgelegten und eindeutigen Zwecke verwendet werden. Eine wichtige Ausnahme dieser Regel gilt, wenn die Daten für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke verwendet werden. Hierzu müssen jedoch zusätzliche Maßnahmen wie beispielsweise eine Anonymisierung angewendet werden.

2.3.3 Datenminimierung

Die erhobenen Daten müssen dem Zweck angemessen und erheblich sein. Außerdem müssen sie auf das für den Zweck der Verarbeitung notwendige Maß beschränkt sein.

2.3.4 Richtigkeit

Die erhobenen Daten müssen sachlich richtig und, falls es erforderlich sein sollte, auch auf dem neuesten Stand sein. Hierzu sind angemessene Maßnahmen zu treffen, um unrichtige Daten unverzüglich zu löschen oder zu berichtigen.

2.3.5 Speicherbegrenzung

Die erhobenen Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für den Zweck, für den sie verarbeitet werden, erforderlich ist. Sie dürfen länger gespeichert werden, solange sie für die in 2.3.2 angesprochenen Zwecke verwendet werden.

2.3.6 Integrität und Vertraulichkeit

Die erhobenen Daten müssen so verarbeitet werden, dass eine angemessene Sicherheit der Daten gewährleistet wird. Des Weiteren müssen die Daten durch geeignete Maßnahmen vor unbefugtem Zugriff und Verlust geschützt werden.

2.3.7 Rechenschaftspflicht

Der Verarbeiter ist für die Einhaltung der vorhergehenden Aspekte verantwortlich und muss diese Einhaltung nachweisen können.

[7] Vgl. Art. 5 Abs. 1 DSGVO Grundsätze für die Verarbeitung personenbezogener Daten

2.4 Rechtliche Grundlagen

2.4.1 Personenbezogene Daten

Personenbezogene Daten sind definiert als alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Dies schließt nicht nur Daten ein, die sich auf eine Person beziehen, sondern auch alle Daten, über die ein Bezug zu einer bestimmten Person hergestellt werden kann.[8]

Personenbezogene Daten sind beispielsweise:

- Name und Adresse
- E-Mailadresse
- Angaben über die Person wie Geschlecht, Aussehen, Größe oder Titel
- Personalausweisnummer
- IP-Adresse, das im Internet wohl wichtigste Datum

Neben den genannten personenbezogenen Daten gibt es außerdem noch die sogenannten "besonderen Arten von personenbezogenen Daten", für die das Gesetz einen besonderen Schutz vorsieht.[9]

Diese sind beispielsweise:

- Rassische oder ethnische Herkunft
- Politische Meinung
- Religiöse oder weltanschauliche Überzeugung
- Gewerkschaftszugehörigkeit
- Angaben zur Gesundheit oder Sexualleben

2.4.2 Rechtmäßigkeit der Verarbeitung

Für die Verarbeitung von personenbezogenen Daten gilt in erster Linie ein sogenanntes Verbot mit Erlaubnisvorbehalt. Dieses besagt, dass jede Erhebung oder Verarbeitung von personenbezogenen Daten grundsätzlich verboten ist. Sie ist nur rechtmäßig, wenn die betroffene Person vorweg in die Verarbeitung einwilligt oder die Erhebung für die Erfüllung eines Vertrags zwischen dem Nutzer und Verarbeiter oder einer Anfrage der betroffenen Person erforderlich ist und der Betroffene damit eine indirekte Einwilligung abgibt.[10]

[8] Vgl. Art. 4 Abs 1 DSGVO Begriffsbestimmungen

[9] Vgl. Art. 9 DSGVO Verarbeitung besonderer Kategorien personenbezogener Daten

[10] Vgl. Art. 6 Abs 1 DSGVO Rechtmäßigkeit der Verarbeitung

Zusätzlich ist die Verarbeitung auch rechtmäßig, wenn die Verarbeitung zur Wahrung des berechtigten Interesses des Verantwortlichen oder eines Dritten erforderlich ist, solange dieses Interesse die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person an dem Schutz ihrer Daten überwiegt. Dies ist eine Klausel von enormer Wichtigkeit, da sie als Grundlage für eine Speicherung von personenbezogenen Daten ohne die Einwilligung des Betroffenen dient. Ob die Interessen des Verarbeiters die des Nutzers überwiegen, muss für den konkreten Fall sorgfältig abgewogen werden. Hier sind insbesondere Gerichtsurteile in der näheren Zukunft interessant zu beobachten, um konkrete Beispiele zu erhalten, was nun erlaubt ist und was nicht.

Außerdem ist wichtig zu erwähnen, dass selbst wenn eine Verarbeitung letztendlich doch für unrechtmäßig erklärt wird, keine zu hohen Strafen bevorstehen sollten, solange sorgfältig dokumentiert wurde, inwiefern eine rechtmäßige Verarbeitung vorliegt und warum die eigenen Interessen überwiegen.

Weitere Rechtmäßigkeitsgründe sind der Schutz von lebenswichtigen Interessen der betroffenen Person, oder die Erfüllung einer Aufgabe, die im öffentlichen Interesse oder durch öffentliche Gewalt erfolgt.

2.4.3 Einwilligung

Bei jeder Verarbeitung, die auf einer Einwilligung beruht, muss der Verantwortliche diese nachweisen können. Des Weiteren müssen die einzelnen Sachverhalte, denen zugestimmt wird, in klarer und einfacher Sprache erläutert werden und leicht voneinander zu unterscheiden sein.

Außerdem hat die betroffene Person das Recht, jederzeit ihre Einwilligung zu widerrufen. Die Möglichkeit des Widerrufs muss der betroffenen Person vor Abgabe ihrer Einwilligung mitgeteilt werden, und muss so einfach durchzuführen sein, wie die Einwilligung selbst. Hierbei ist jedoch anzumerken, dass bei einem Widerruf die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung unberührt bleibt.[11]

2.4.4 Einwilligung eines Kindes

Einwilligungen von Minderjährigen sind nur dann rechtmäßig, wenn diese das sechzehnte Lebensjahr vollendet haben. Ist dies nicht der Fall, muss die Einwilligung durch die Eltern des Kindes erteilt werden. Hierfür muss der für die Verarbeitung Verantwortliche den Umständen angemessene Anstrengungen unternehmen, um sich zu vergewissern, dass die Einwilligung des Kindes die elterliche Unterstützung hat. Verschiedene Onlinedienste verlangen hier beispielsweise eine E-Mailadresse der Eltern, über die die Einwilligung eingeholt werden kann.

[11] Vgl. Art. 7 DSGVO Bedingungen für die Einwilligung

2.5 Technische Grundlagen

2.5.1 Sicherheit der Verarbeitung

Um ein angemessenes Schutzniveau sicherzustellen, müssen die Verantwortlichen verschiedene Maßnahmen anwenden.

Diese Maßnahmen sind die drei klassischen Schutzziele der IT-Sicherheit:

- die Anonymisierung und Verschlüsselung der Daten, um die Vertraulichkeit sicherzustellen
- Backups und andere Möglichkeiten einer Wiederherstellung der Daten nach einem technischen Zwischenfall für eine ausreichende Verfügbarkeit dieser Daten
- Prüfsummen oder Quittierungen, die sicherstellen, dass die Integrität der Daten ebenfalls gewährleistet ist

Mit der Datenschutz-Grundverordnung kommt noch das Ziel der Belastbarkeit hinzu, mit dem sichergestellt werden soll, dass Systeme und Dienste stets abrufbereit sind, um die Datenverfügbarkeit zu sichern.

Wichtig ist, dass die in den vorgenannten Grundsätzen der Datenschutz-Grundverordnung aufgeführte Rechenschaftspflicht eingehalten wird und die Erfüllung aller Schutzziele auch nachgewiesen werden kann. [12]

2.5.2 Data protection by design and default

Mit der Datenschutz-Grundverordnung ist der Begriff „Data Protection By Design and Default“[13] hinzugekommen. Hierbei handelt es sich um die Kombination der bereits bekannten Prinzipien „Privacy By Design“ und „Privacy By Default“. Die Umsetzung dieser beiden Prinzipien wird zukünftig fest vorgeschrieben, weshalb sie erheblich an Bedeutung gewonnen haben.

a) Privacy By Design

Das sogenannte „Privacy By Design“-Prinzip ist ein Paradigma, welches vorschreibt, dass schon bei dem Entwurf („Design“) des Gesamtsystems und der einzelnen Geschäftsprozesse auf den Datenschutz geachtet werden soll. Zudem müssen dem Nutzer grundsätzlich Möglichkeiten gegeben werden, um seine Daten zu schützen.

b) Privacy By Default

„Privacy By Default” hingegen besagt, dass Einstellungen, die die Privatsphäre des Nutzers schützen, voreingestellt sein sollen. Dies würde beispielsweise bedeuten, dass ein

[12] (Bayerisches Landesamt für Datenschutzaufsicht, 2018)

[13] (Information Commissioner's Office)

neuer Facebook Account mit den schärfsten Sicherheitseinstellungen eröffnet wird und erst vom Nutzer auf das gewünschte Niveau herabgesetzt werden kann.

2.5.3 Technische und organisatorische Maßnahmen („TOM“)

Bei dem Datenschutz durch technische und organisatorische Maßnahmen handelt es sich um ein weiteres großes Schutzparadigma, das bereits aus dem Bundesdatenschutzgesetz bekannt war, jedoch mit der neuen Datenschutz-Grundverordnung an Bedeutung gewonnen hat.

Für Unternehmen wird es zukünftig besonders wichtig sein, bezüglich der technischen und organisatorischen Maßnahmen gut aufgestellt zu sein, da dies bei einem Datenschutzverstoß maßgeblich die Strafe beeinflusst. Nach Art. 83 Abs. 2d DSGVO sind die getroffenen Sicherheitsmaßnahmen entscheidend darüber, wie hoch verhängte Bußgelder sein werden und ob diese überhaupt verhängt werden.

Beispiele für diese Maßnahmen sind unter anderem Änderungen/Anpassungen der internen Prozessabläufe, betriebsinterne Richtlinien, Vertretungsregeln für abwesende Mitarbeiter, Implementierung automatischer Sperr- und Löschmaßnahmen, Anonymisierung sowie die Protokollierung von Zugriffen.

2.6 Rechte der Endnutzer

2.6.1 Recht auf Löschung („Recht auf Vergessenwerden“)

Die für Endnutzer womöglich interessanteste Neuerung durch die Datenschutz-Grundverordnung ist das Recht auf Löschung. Demzufolge können Betroffene nun von den für ihre Daten Verantwortlichen verlangen, dass ihre Daten unverzüglich gelöscht werden, woraufhin der Verantwortliche verpflichtet ist, dieser Forderung nachzukommen.

Es gibt verschiedene Gründe, die die Löschung begründen oder verhindern können:

- sollten die Daten nicht mehr für ihren ursprünglichen Zweck notwendig sein, müssen sie unverzüglich gelöscht werden
- sollten sie hingegen noch genutzt werden, muss der Betroffene von dem neuen Widerrufsrecht Gebrauch machen
- sollten die Daten allerdings nachweislich für zwingende schutzwürdige Gründe oder für Rechtsansprüche des Datenverarbeitenden benötigt werden, müssen sie wiederum nicht gelöscht werden
- sollten die Daten allerdings nur für Werbezwecke verarbeitet werden, kann jederzeit Widerspruch dagegen eingelegt werden[14]

[14] Vgl. Art. 17 DSGVO Recht auf Löschung ("Recht auf Vergessenwerden")

2.6.2 Recht auf Auskunft

Durch die Datenschutz-Grundverordnung haben Betroffene künftig das Recht, von dem Verantwortlichen eine Bestätigung zu verlangen, ob dieser sie betreffende personenbezogene Daten verarbeitet.

Sollte dies der Fall sein, haben sie zusätzlich ein Recht auf Auskunft über diese personenbezogenen Daten. Dies bedeutet, dass der Verantwortliche eine Kopie folgender Informationen den Betroffenen bereitstellen muss[15]:

- die Verwendungszwecke
- die Kategorien personenbezogener Daten, die verarbeitet werden
- die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden
- falls möglich die geplante Dauer der Speicherung der personenbezogenen Daten, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder auf Widerspruch gegen diese Verarbeitung
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling

Des Weiteren hat die betroffene Person das Recht, Auskunft über getroffene Schutzmaßnahmen der Übermittlung zu erhalten, falls ihre Daten an ein Drittland oder eine internationale Organisation übertragen werden.

2.6.3 Recht auf Datenübertragbarkeit

Betroffene haben nun das Recht, ihre erfassten Daten mitnehmen zu können, zum Beispiel zu alternativen Unternehmen mit gleichem Dienstleistungsangebot. Die Verantwortlichen müssen einer entsprechenden Aufforderung der Herausgabe oder Weiterleitung der Daten nachkommen.[16]

2.6.4 Haftung und Recht auf Schadensersatz

Das bisher im Bundesdatenschutzgesetz verankerte Recht, Haftungsansprüche gegenüber Unternehmen geltend zu machen, falls bei einer Datenübertragung ein Schaden

[15] Vgl. Art. 15 DSGVO Auskunftsrecht der betroffenen Person

[16] Vgl. Art. 20 DSGVO Recht auf Datenübertragbarkeit

entstand, oder falls die Verarbeitung unzulässig war, wird übernommen und um die Haftung im Falle von moralischen Schäden erweitert.

2.6.5 Haftungserstreckung auf ausländische Unternehmen

Künftig können bei einem unzureichenden Datenschutzniveau Haftungsansprüche auch gegen Unternehmen geltend gemacht werden, die keinen Sitz in der EU haben. Voraussetzung hierfür ist, dass auf der Webseite eine Amtssprache eines EU-Mitgliedsstaates verwendet wird. Dies umfasst also beispielsweise alle Webseiten, die die englische Sprache unterstützen.

2.6.6 Recht auf Berichtigung

Sollten Daten einer Person fehlerhaft sein, kann die betroffene Person von dem Verantwortlichen eine unverzügliche Berichtigung verlangen. Des Weiteren hat die Person das Recht auf eine Vervollständigung unvollständiger personenbezogener Daten.[17]

2.6.7 Recht auf Einschränkung der Verarbeitung

Betroffene Personen haben grundsätzlich das Recht, eine Einschränkung der Verarbeitung zu verlangen, falls beispielsweise

- die Richtigkeit von Daten bestritten wird,
- die Verarbeitung der Daten unrechtmäßig ist, die betroffene Person jedoch nicht möchte, dass ihre Daten gelöscht werden,
- der Verarbeiter die Daten eigentlich nicht mehr verwendet, die betroffene Person sie jedoch für gewisse Rechtsansprüche benötigt.

Im Falle einer Einschränkung der Verarbeitung werden die Daten komplett gesperrt, gegebenenfalls auf ein anderes System übertragen oder von einer Webseite entfernt. Damit soll sichergestellt werden, dass die Daten in keiner Weise weiterverarbeitet oder verändert werden können, bis feststeht, wie weiter mit ihnen verfahren werden soll.[18]

2.6.8 Widerspruchsrecht

In den meisten Fällen kann die Einwilligung jederzeit widerrufen werden, wodurch die Verarbeitung aufgrund der mangelnden Rechtmäßigkeit abgebrochen werden muss. Der verantwortliche Verarbeiter ist verpflichtet, die betroffene Person spätestens zum Zeitpunkt der ersten Kommunikation auf ihr Widerspruchsrecht hinzuweisen.

Sollte die Verarbeitung jedoch aus Gründen erfolgen, die im öffentlichen Interesse liegen, oder die Verarbeitung dient der Wahrung der berechtigten Interessen des Verantwortlichen, können die Daten weiterverarbeitet werden. Letzteres erfordert als Ausgleich

[17] Vgl. Art. 16 DSGVO Recht auf Berichtigung

[18] Vgl. Erwägungsgrund 67 DSGVO Beschränkung der Verarbeitung

allerdings zusätzlich, dass die Interessen des Verantwortlichen die Grundrechte oder Grundfreiheiten des Betroffenen überwiegen, was insbesondere bei Kindern nur selten der Fall sein dürfte.

Zusätzlich zu dem grundsätzlichen Schutz auf Basis der Grundrechte und Grundfreiheiten gibt es noch ein zusätzliches Widerspruchsrecht, mit dessen Hilfe gegen die oben genannte Weiterverarbeitung bei fehlender Einwilligung widersprochen werden kann. Hierfür müssen jedoch von der betroffenen Person selbst besondere Gründe genannt werden, aufgrund derer sie im Vergleich zu anderen Personen besonders schützenswert ist.

Sollte die Verarbeitung nur zu Werbezwecken erfolgen, kann dieser jederzeit ohne Voraussetzungen widersprochen werden.[19]

2.7 Verpflichtungen der Anbieter

2.7.1 Bestellung des Datenschutzbeauftragten[20]

Durch die Datenschutz-Grundverordnung wird nun europaweit vorgegeben, wann Datenschutzbeauftragte zu bestellen sind. In Deutschland ist bei dieser Thematik zusätzlich das Bundesdatenschutzgesetz-neu zu berücksichtigen. Insgesamt sind folgende Bereiche zu prüfen:

a) Unternehmensgröße

Arbeiten mehr als 10 Mitarbeiter regelmäßig mit personenbezogenen Daten oder automatischer Datenverarbeitung – hierzu zählt sowohl die Erhebung als auch die Nutzung – so besteht gemäß Bundesdatenschutzgesetz-neu die Pflicht, einen Datenschutzbeauftragten zu bestellen.

b) Detailgrad der Daten

Sollten Daten verarbeitet werden, welche Informationen unter anderem über die Rasse, die ethnische Herkunft, die politische Meinung, die religiösen Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben einer Person enthalten, so besteht ebenfalls eine Verpflichtung, unabhängig von der Anzahl der Mitarbeiter einen Datenschutzbeauftragten zu bestellen.

c) Geschäftsfeld

Ist die Kerntätigkeit des Unternehmens die geschäftsmäßige Verarbeitung oder Erhebung von personenbezogenen Daten, so besteht ebenfalls eine Verpflichtung, unabhängig von der Anzahl der Mitarbeiter einen Datenschutzbeauftragten zu bestellen.

[19] Vgl. Art. 21 DSGVO Widerspruchsrecht

[20] Vgl. Art. 37 DSGVO Benennung eines Datenschutzbeauftragten

2.7.2 Aufgaben des Datenschutzbeauftragten

Ist der Datenschutzbeauftragte erst einmal ernannt, fallen ihm viele verschiedene Aufgaben zu. Die wichtigsten sind im Folgenden aufgezählt. [21]

- die Beratung des Verantwortlichen, des Auftragsverarbeiters und der beschäftigten Verarbeiter hinsichtlich ihrer Pflichten entsprechend der gültigen Gesetzeslage,
- die Überwachung der Einhaltung der Gesetze, sowie die Einweisung der beteiligten Mitarbeiter.
- die Zusammenarbeit mit Aufsichtsbehörden, insbesondere als Anlaufstelle für Fragen zur Verarbeitung der personenbezogenen Daten.

2.7.3 Verzeichnis von Verarbeitungstätigkeiten

Mit der Datenschutz-Grundverordnung sind Unternehmen und Auftragsverarbeiter sowie deren Vertreter von nun an verpflichtet, schriftliche Verzeichnisse von Verarbeitungstätigkeiten, in denen wesentliche Angaben zur Datenverarbeitung aufgeführt werden müssen, zu führen. In diesen Verzeichnissen sind aufzuführen[22]:

- der Name und Kontaktdaten des Verantwortlichen für die Verarbeitung
- der Zweck der Verarbeitung
- die Kategorien der betroffenen Personen und ihrer Daten
- die Kategorien der Empfänger der Daten
- übermittlungen der Daten in Drittländer
- wenn möglich die vorgesehenen Fristen für die Löschung
- wenn möglich eine Beschreibung der technischen und organisatorischen Maßnahmen zum Schutz der Verarbeitung

a) Befreiung von der Pflicht zur Erstellung eines Verzeichnisses

Für die Pflicht, ein Verzeichnis von Verarbeitungstätigkeiten anzulegen, gibt es eine bedeutsame Ausnahme für kleine und mittelständische Unternehmen sowie Einzelpersonen. Sie gilt nämlich nicht für Unternehmen oder Einrichtungen mit weniger als 250 Mitarbeitern, es sei denn:

[21] Vgl. Art. 39 DSGVO Aufgaben des Datenschutzbeauftragten

[22] Vgl. Art. 30 Abs. 1-2 DSGVO Verzeichnis von Verarbeitungstätigkeiten

- die Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der Betroffenen
- es erfolgt eine Verarbeitung besonderer Arten personenbezogener Daten
- die Verarbeitung erfolgt öfter als „nur gelegentlich“.[23]

Allerdings ist das letzte Kriterium so vage formuliert, dass der Vorteil für diese Zielgruppe hinfällig sein könnte und auf ein konkretes Gerichtsurteil gewartet werden sollte.

2.7.4 Datenschutz-Verpflichtung von Beschäftigten

Die Datenschutz-Grundverordnung erwartet zudem von den für eine Verarbeitung verantwortlichen Stellen, dass diese sicherstellen, dass ihnen unterstellte Personen, die Zugang zu den personenbezogenen Daten haben, diese nur auf Anweisung verarbeiten und diese Verarbeitung den Pflichten zur Verarbeitung, wie beispielsweise dem Einhalten der Prinzipien der Datenminimierung oder der Zweckbindung, genügen.[24]

Hierbei empfiehlt es sich, allen Mitarbeitern sowie Auszubildenden, Praktikanten oder ähnlichen so früh wie möglich die Einhaltung der Pflichten, die für die Verarbeitung für das Unternehmen gelten, aufzuerlegen, um so die Verantwortung an die entsprechenden Stellen weiterzureichen.

2.7.5 Informations- und Auskunftspflichten[25]

a) Informationspflichten bei Direkterhebung

Es müssen von nun an die Kontaktdaten der für die Verarbeitung zuständigen Person beziehungsweise deren Stellvertreter und die eines etwaig vorhandenen Datenschutzbeauftragten angegeben werden. Künftig sind zudem das berechtigte Interesse, die Rechtsgrundlage und der Verarbeitungszweck, die zur Erhebung der Daten ermächtigen, anzugeben.

Falls eine Übermittlung der personenbezogenen Daten stattfindet, muss dem Betroffenen der eindeutige Empfänger mitgeteilt werden. Sollte dies nicht möglich sein, müssen Informationen über die Kategorie des Empfängers ausgewiesen werden.

Sollten Daten in Drittländer oder an internationale Organisationen übertragen werden, so ist dies mitzuteilen. Dem Betroffenen muss zudem mitgeteilt werden, welche Bedingungen die Rechtmäßigkeit der Übertragung begründen.

Außerdem muss klar werden, welche Maßnahmen ein angemessenes Datenschutzniveau gewährleisten und Einsicht in diese ermöglicht werden.

[23] Vgl. Art. 30 Abs. 5 DSGVO Verzeichnis von Verarbeitungstätigkeiten

[24] Vgl. Art. 32 Abs. 4 DSGVO Sicherheit der Verarbeitung

[25] Vgl. Art. 12-14 DSGVO

Des Weiteren müssen zudem folgende Punkte (siehe auch Ziffer 2.6.2 Recht auf Auskunft) mitgeteilt werden:

- Dauer der Speicherung
- Rechte über Auskunft
- Möglichkeit einer Berichtigung
- Möglichkeit einer Löschung
- Einschränkung und Widerspruch
- die zuständige Aufsichtsbehörde für Beschwerden
- vertragliche Pflichten für die Bereitstellung der Daten sowie Folgen, falls diese nicht erfolgt
- Informationen zur verwendeten Logik im Falle einer automatischen Entscheidung wie beispielsweise Profiling

b) Informationspflichten bei Dritterhebung

Analog zur Direkterhebung müssen die verschiedenen Kategorien der erhobenen personenbezogenen Daten genannt werden. Darüber hinaus muss ebenfalls das Interesse an einer Verarbeitung der Daten begründet darzulegen sein. Zusätzlich zu einer einfachen Direkterhebung muss jedoch auch die Quelle, aus der die personenbezogenen Daten stammen, genannt werden.

c) Einschränkungen der Informationspflicht

Die Bereitstellung der Informationen hat schriftlich zu erfolgen. Dies kann elektronisch, beispielsweise auf einem öffentlichen Bereich einer Webseite geschehen. Findet eine Erhebung von Daten direkt statt, so besteht eine unmittelbare Informationspflicht. Im Falle einer Dritterhebung ist eine Frist von maximal einem Monat einzuhalten.

2.7.6 Auftragsverarbeitung

Die Auftragsverarbeitung ist die Verarbeitung von personenbezogenen Daten im Auftrag des Verantwortlichen durch eine zusätzliche Stelle. Die Verantwortung der korrekten Verarbeitung der Daten kann jedoch nicht an den Auftragsverarbeiter übertragen werden, sondern ist durch den Verantwortlichen sicherzustellen und muss von ihm in regelmäßigen Abständen überprüft werden.[26]

[26] (Bayerisches Landesamt für Datenschutzaufsicht, 2016)

2.7.7 Datenschutzverletzungen

Mit der Datenschutz-Grundverordnung wird eine Benachrichtigungspflicht im Falle einer Datenschutzverletzung vorgeschrieben. Die Betroffenen sind unmittelbar in Kenntnis zu setzen, die Aufsichtsbehörde innerhalb von 72 Stunden.

Dem Betroffenen ist mitzuteilen, welche Art von Verletzung vorliegt und an wen er sich für weitere Informationen wenden kann (Datenschutzbeauftragter). Außerdem müssen die Folgen der Datenschutzverletzung aus der Mitteilung hervorgehen.

2.7.8 Datenschutz-Folgenabschätzung

Sollte eine Datenverarbeitung ein besonders hohes Risiko für die betroffenen Personen darstellen, sei es aufgrund ihrer Art, ihres Umfangs oder sonstiger Gründe der Daten, muss der Verantwortliche eine Abschätzung der möglichen Folgen durchführen.[27]

Diese Folgenabschätzung ist außerdem immer erforderlich, wenn:

- es sich um eine systematische und umfassende Bewertung persönlicher Aspekte von Personen handelt, wie beispielsweise Profiling, die wiederum als Grundlage für rechtswirksame Entscheidungen dient,
- es sich um eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten handelt oder Daten über Straftaten oder strafrechtliche Verurteilungen enthalten sind,
- es sich um eine Überwachung öffentlich zugänglicher Bereiche handelt.

2.7.9 Verbot der Weiterverarbeitung

Aufgrund des Grundsatzes der Zweckbindung muss im Vorfeld festgelegt werden, für welchen Zweck erhobene Daten verwendet werden dürfen. Eine zweckentfremdete Weiterverarbeitung der Daten ist somit prinzipiell verboten. Allenfalls kann eine Erweiterung des Zwecks vorgenommen werden, die jedoch nur zulässig ist, wenn sie mit dem ursprünglichen Zweck vereinbar ist. Dies muss vor jeder Weiterverarbeitung geprüft werden.[28]

2.7.10 Vorgaben zur Webseite-Compliance

a) Datenschutzerklärung

Die bisher geltende Notwendigkeit, Seitenbesucher in einer Datenschutzerklärung über datenschutzrelevante Aktivitäten, wie beispielsweise Cookies, Social Media oder Kontaktformulare, zu informieren, bleibt bestehen und wird um einige neue Aspekte erweitert. So muss nun zum Zeitpunkt einer Erfassung von personenbezogenen Daten auf

[27] Vgl. Art. 35 DSGVO Datenschutz-Folgenabschätzung

[28] Vgl. Erwägungsgrund 50 DSGVO Weiterverarbeitung

diese Erfassung hingewiesen werden und der Zweck und die Rechtsgrundlage der Erfassung kenntlich gemacht werden.

b) Recht auf Vergessenwerden

Außerdem muss die Webseite den Besucher dabei unterstützen, sein Recht auf Vergessenwerden geltend zu machen. Sollten die Daten an einen Dritten weitergeleitet worden sein, so muss die Löschanweisung ebenfalls weitergeleitet werden.[29]

2.7.11 Risikoanalyse der Verarbeitung

Es ist künftig eine Risikoanalyse durchzuführen, die die Risiken einer Verarbeitung und Übertragung und deren Eintrittswahrscheinlichkeit abschätzt. Außerdem muss diese Analyse schriftlich dokumentiert werden.

2.7.12 Datenschutzfreundliche Voreinstellungen

Prozesse müssen so gestaltet werden, dass sie als datenschutzfreundlich gelten. Es sollen also nur Daten erhoben werden, die tatsächlich notwendig sind. Von Anfang an soll durch Maßnahmen wie Privacy By Design sichergestellt werden, dass die verarbeiteten Daten geschützt werden.

2.7.13 Werbliche Ansprache und Direktmarketing

Im Vorfeld einer Werbung muss bewertet werden, wie es um die Interessen des Betroffenen steht und ob eine Werbemaßnahme zugemutet werden kann. Außerdem besteht nun eine Dokumentationspflicht für jede einzelne Werbemaßnahme einschließlich der Interessenabwägung.

a) Postalische Werbung und E-Mails

Hier ist eine Einwilligung des Betroffenen erforderlich, eine Ausnahme gilt bei der Verwendung von Listendaten. Darunter fallen die Berufs-, Branchen-, oder Geschäftsbezeichnung, Titel, Name, akademischer Grad, Anschrift und Geburtsjahr. E-Mailadressen dürfen unter bestimmten Bedingungen ebenfalls gespeichert werden.[30] Außerdem muss erkennbar sein, wer für die Werbung verantwortlich ist. Sollten die Daten von einer dritten Quelle stammen, ist diese zu nennen.

b) Telefon

Hierbei wird zwischen Verbrauchern und Unternehmen unterschieden. Für Verbraucher ist eine Einwilligung zwingend erforderlich, für Unternehmen entscheidet die Interessen-

[29] (Herold Unternehmensberatung GmbH, kein Datum)

[30] (Hiddemann, 2017)

abwägung. Der Betroffene kann jederzeit unabhängig von der Form der Werbung formlos widersprechen. Ein Widerspruch hat ein Verarbeitungsverbot der personenbezogenen Daten zur Folge.

2.8 Zertifizierungen

Um die vollständige und korrekte Umsetzung der Datenschutz-Grundverordnung zu fördern, sollen unionsweit Zertifizierungsverfahren und Datenschutzsiegel eingeführt werden. mit denen Unternehmen nachweisen und werben können, dass sie in besonderem Maße datenschutzkonform arbeiten. Diese Zertifizierungen sind allerdings rein freiwillig und mindern zudem nicht die Verantwortung der Einhaltung der Gesetze und Vorschriften zum Datenschutz.[31]

2.9 Bußgelder und Sanktionen

Bislang wurden Verstöße gegen den Datenschutz mit einer Strafe von bis zu 300.000 Euro geahndet. Dies wurde mit einer Erhöhung auf bis zu 20 Mio. Euro bedeutend verschärft. Außerdem ist es nun möglich, die Strafe an den Jahresumsatz zu koppeln, wodurch Strafen von bis zu 4 Prozent des Unternehmensumsatzes verhängt werden können.[32]

Hierbei ist zu beachten, dass die EU-Definition eines Unternehmens das gesamte Unternehmen beziehungsweise den Konzern als eine wirtschaftliche Einheit umfasst. Für Verstöße eines Tochterunternehmens kann also der Konzernumsatz zum Strafmaß herangezogen werden.

Außerdem besteht die Möglichkeit, dass die Verarbeitung von personenbezogenen Daten vollständig verboten werden kann, falls ein Unternehmen den Anordnungen, den Verstoß zu beenden, nicht nachkommt.

[31] Vgl. Art. 42 DSGVO Zertifizierung

[32] Vgl. Art. 83 DSGVO Allgemeine Bedingungen für die Verhängung von Geldbußen

3 Leitfaden für Datenverarbeiter

Im Folgenden wird nun ein Ablauf dargestellt, mit dessen Hilfe überprüft werden kann, welche Anforderungen der Datenschutz-Grundverordnung erfüllt werden müssen. Die Struktur lehnt sich in Ansätzen an die Publikationen[33] des Bayerischen Landesamtes für Datenschutzaufsicht an, geht jedoch tiefer in die Materie ein und erläutert die Hintergründe der einzelnen Punkte, die in der genannten Quelle nur aus einer Checkliste bestehen.

3.1 Bestandsanalyse

Als Vorbereitung sollte jedes Unternehmen und jeder, der eine eigene Internetpräsenz besitzt, eine Bestandsanalyse durchführen, um herauszufinden, ob Anpassungen nötig sind. Dabei sind alle wesentlichen Verarbeitungstätigkeiten von personenbezogenen Daten aufzuführen.

Es geht dabei um eine erste Prüfung, ob und was zu tun ist. Die Bestandsanalyse ist insofern nicht mit dem Verzeichnis von Verarbeitungstätigkeiten gleichzusetzen, welches angefertigt werden muss, wenn eine regelmäßige Verarbeitung von personenbezogenen Daten vorliegt.

Bei der Bestandsanalyse muss geprüft werden, ob in einer beliebigen Form mit personenbezogenen Daten interagiert wird. Es spielt keine Rolle, ob es sich hierbei um eine Excel-Liste mit Kundendaten, eine externe Lohnabrechnung oder ein Kontaktformular auf einer Internetseite handelt. Sobald personenbezogene Daten im Unternehmen existieren, ist Handlungsbedarf gegeben.

3.2 Zuweisung der Datenschutzaufgaben

Durch die neue Datenschutz-Grundverordnung werden sich, auch nach einer guten Vorbereitung, viele Fragen ergeben, die beantwortet werden müssen.

Sofern Kleinunternehmen nicht auf die für die Bestellung eines Datenschutzbeauftragten verpflichtende Mindestanzahl von 10 Personen mit regelmäßigem Kontakt zu personenbezogenen Daten kommen, ist dessen Aufgabe durch die Geschäftsleitung wahrzunehmen.

Insbesondere in der ersten Zeit der Datenschutz-Grundverordnung und bei jedem neuen zu prüfenden Geschäftsprozess werden sich viele Aufgaben häufen. Da diese aber in übersichtlichen Zeitfenstern auftreten, kann die Beschäftigung eines externen Datenschutzbeauftragten sinnvoll sein. Auch würde dieser eher über das erforderliche Maß an juristischer und technischer Expertise verfügen, als ein Mitarbeiter, der die Aufgaben

[33] (Bayerisches Landesamt für Datenschutzaufsicht, 2018)

nach erforderlicher Schulung „nebenbei“ übernimmt. Ohnehin wäre dies eine kostengünstigere Alternative gegenüber einer zusätzlichen Spezialisten-Vollzeitstelle.

3.3 Anpassung der Datenerfassung

Bei der anschließenden Auswertung der Bestandsanalyse sollte evaluiert werden, ob die zu erfassenden Daten angepasst werden müssen, um die Prinzipien der Zweckbindung und der Datenminimierung zu wahren. Falls bisher erhobene Daten sich als nicht für den eigentlichen Zweck der Verarbeitung notwendig herausstellen, sollte ausgewertet werden, ob diese weiterhin erfasst werden müssen.

Insbesondere Werbezwecke können eine valide Rechtfertigung für die Speicherung verschiedener Nutzerdaten sein, die nicht unbedingt mit der ursprünglichen Verwendung zusammenhängen, an deren Weiterverarbeitung gleichwohl ein berechtigtes Interesse besteht.

3.4 Implementieren der Lösch-Funktionalitäten

Ein wichtiger Aspekt der Datenschutz-Grundverordnung sind die neuen Rechte der Personen, deren Daten verarbeitet werden. Es sollte damit gerechnet werden, dass viele Nutzer von ihrem Widerrufsrecht oder dem Recht auf Löschung Gebrauch machen werden. Insofern sind Möglichkeiten, darauf einfach reagieren zu können, einzuführen.

Hierfür kommen verschiedene Maßnahmen, wie beispielsweise die automatische Löschung nach Erfüllung des Zwecks, für den die Daten erhoben wurden, oder zumindest eine algorithmische Verarbeitung einer Löschanfrage in Betracht.

Niemand sollte von Hand Exceltabellen nach einem zu löschenden Kunden absuchen oder einzelne Datensätze aus der Datenbank löschen müssen. Auch wenn ersteres vielleicht noch bei kleineren Datenmengen möglich sein sollte, ist es ein vermeidbarer Mehraufwand und insbesondere bei Backups – die für die von der Datenschutz-Grundverordnung geforderte Absicherung gegen einen Verlust der Daten ohnehin verwendet werden – wächst der Aufwand enorm.

Und auch das Löschen von einzelnen Datensätzen aus Datenbanken kann, aufgrund der verschiedenen Abhängigkeiten der Daten untereinander, zu Schwierigkeiten führen, wie beispielsweise fehlende Fremdschlüsselbeziehungen zu den gelöschten, für die Integrität der Datenbank jedoch notwendigen Datensätze.

3.5 Anpassung der Webseite

Viele Webseiten verwenden Funktionalitäten, die zwar sehr beliebt, aber nun nicht mehr datenschutzkonform sind. Im Folgenden werden die Probleme einiger Funktionen beschrieben und Lösungen vorgeschlagen.

3.5.1 Überarbeiten von veralteter Datenerfassung

Durch die neuen Sicherheitsanforderungen der Datenschutz-Grundverordnung wird vorausgesetzt, dass angemessene Sicherheitsmaßnahmen verwendet werden, um personenbezogene Daten zu schützen. Dies bedeutet allerdings auch, dass die in Deutschland bereits seit Januar 2016 geltende Pflicht, bei Erhebung personenbezogener Daten eine SSL-Verbindung zu verwenden, an Bedeutung zunimmt und nun sehr wahrscheinlich auch international gelten wird.

3.5.2 Kommentarfunktionen

Nahezu alle Blogs im Internet verwenden eine Kommentarfunktion. Grundsätzlich sind Kommentare weiterhin möglich, allerdings muss für die meisten Implementierungen eine E-Mailadresse und ein Name angegeben werden. Zusätzlich wird oftmals noch die IP-Adresse gespeichert. Da es sich hierbei um personenbezogene Daten handelt, kommt auch hier die Datenschutz-Grundverordnung zum Tragen.

Da Kommentare rechtswidrige Inhalte haben können, ist es aus Haftungsgründen zwingend notwendig, die Person identifizieren zu können, die den Kommentar abgegeben hat, da der Betreiber des Blogs sonst dem Risiko der Haftung ausgesetzt wäre. Somit besteht ein berechtigtes Interesse des Betreibers, Personen langfristig identifizieren zu können.

Ob nun das berechtigte Interesse des Betreibers das Interesse des Kommentators auf Datenschutz überwiegt, ist größtenteils Auslegungssache. Somit sollte sich ein Betreiber über eine entsprechende Einverständniserklärung absichern. Hierzu gibt es beispielsweise in WordPress das Plugin „WP GDPR Compliance“[34], welches eine Checkbox mit einer hinterlegten Einverständniserklärung einfügt.

3.5.3 Newsletter

Hinsichtlich Newsletter oder auch E-Mail-Werbung ändert sich zukünftig fast nichts. Wie bereits unter dem Telemediengesetz gilt das Verbot mit Erlaubnisvorbehalt, welches eine informierte Einwilligung erfordert. Hierfür sorgt ein Standard Double-Opt-In Verfahren sowie der Nachweis über dessen Durchführung.

Wichtig anzumerken ist, dass Opt-Out-Verfahren zu vermeiden sind, da die Einwilligung durch eine „eindeutige bestätigende Handlung“[35] erfolgen soll. Es soll also beispielsweise ein Kästchen beim Besuch einer Internetseite angeklickt werden müssen. Bereits vorangekreuzte Kästchen hingegen sollen demnach keine Einwilligung darstellen.

[34] (Oexman, Visser, Molenaar, van Tulder, & Van, 2018)

[35] Vgl. Erwägungsgrund 32 DSGVO Einwilligung

Eine neue Verpflichtung ist die Einhaltung des Simplizitätsgebots bei dem Widerruf einer Einwilligung, also einer hinreichend einfachen Möglichkeit, zum Beispiel einen Newsletter abzubestellen. In der Regel geschieht dies bereits jetzt über einen Link am Ende des Newsletters, was auch in Zukunft ausreichen wird.[36]

3.5.4 **Traffic Analyse** am Beispiel „Google Analytics“

Google Analytics ist ein Analyseservice, der den Verkehr einer Webseite speichert und auswertet.

In der Standardkonfiguration sendet Google Analytics hierzu die IP-Adressen der Nutzer an Google in den USA mit dem Risiko, dass diese dort gespeichert und für Profiling verwendet werden. Da die IP-Adresse zu den personenbezogenen Daten gehört, muss zum einen auf die Verwendung des Analysetools in der Datenschutzerklärung hingewiesen werden und dem Nutzer die Möglichkeit gegeben werden, per „Opt-Out“ von seinem Widerrufsrecht Gebrauch zu machen. Zum anderen benötigt man zusätzlich einen Auftragsdatenverarbeitungsvertrag mit Google.

Da für die Auswertung der Webseitenbesuche nicht wichtig ist, wer genau sie besucht hat, kann die IP-Adresse des Nutzers auch vorher anonymisiert werden. Google stellt hierzu eine „AnonymizeIP“-Funktion bereit, die diese Aufgabe übernimmt.

Sollen Datenweitergabe in die USA und zusätzlicher Verarbeitungsvertrag mit Google vermieden werden, bietet es sich alternativ an, ein open source Analysetool wie zum Beispiel „Matomo“ zu verwenden, welches auf dem eigenen Server läuft. Aber auch hier ist darauf zu achten, eine entsprechende Einwilligung vom Nutzer einzuholen.

3.5.5 Web Fonts

Viele Webseiten reduzieren ihre Netzwerkauslastung, indem sie keine eigenen Schriftarten verwenden, die jeweils zum Nutzer geschickt werden müssen, sondern stattdessen Web Fonts einbinden. Diese werden beim Aufruf der Seite von einem zusätzlichen Server abgerufen, der diese bereitstellt. Hierzu wird jedoch die IP-Adresse des Nutzers an den jeweiligen Server geschickt, wodurch diese beispielsweise im Falle der sehr häufig genutzten Google Fonts in die USA gesendet wird und wiederum das Risiko einer dortigen Speicherung und Verarbeitung sowie Verwendung für Profiling besteht.

Auch hier gibt es den Einwand, dass bei der Verwendung von Web Fonts ein berechtigtes Interesse des Anbieters besteht und dieses das Datenschutzinteresse des Nutzers überwiegt. Daher muss in der Datenschutzerklärung auf die Verwendung hingewiesen werden. Ein Beispiel hierzu wäre folgender Ausschnitt aus der Datenschutzerklärung der Webseite der SKM-Rechtsanwälte:

[36] (Brünnen, 2018)

> *[…] Die Nutzung von Google Web Fonts erfolgt im Interesse einer einheitlichen und ansprechenden Darstellung unserer Online-Angebote. Dies stellt ein berechtigtes Interesse im Sinne von Art. 6 Abs. 1 lit. f DSGVO dar*.[37]

Um dieses Problem auszuschalten, müssen die Schriftarten auf dem eigenen Server liegen. Hierzu gibt es verschiedene Quellen im Internet, die Web Fonts zum Download anbieten.

3.5.6 **Einbindung von Onlinekarten** am Beispiel „Google Maps“

Bei der Einbindung von Google Maps besteht die gleiche Thematik wie bei den Google Analytics und Google Fonts, insbesondere da letztere automatisch in Google Maps mit eingebunden werden. Im Gegensatz zu Web Fonts gibt es jedoch keine Onlinekarten, die auf dem eigenen Server laufen, weshalb eine andere Lösung nötig ist.

Es bieten sich mehrere Möglichkeiten der Lösung an. Zusätzlich zu einer ähnlichen, auf dem berechtigten Interesse basierenden Lösung wie bei den Web Fonts, also dem Verweis in der Datenschutzerklärung auf die Nutzung von Google Maps und der daraus resultierenden Versendung von Daten, können alternative Karten wie „OpenStreetMap“ verwendet werden, deren Server unter anderem auch in der EU liegen.

Zusätzlich bietet sich mit der Verwendung eines Plugins wie „Borlabs Cookie“[38], welches eingebettete Elemente auf einer Webseite erst lädt, wenn der Nutzer dies per Klick bestätigt, eine weitere interessante Lösung an. Hiermit kann direkt an der zu bestätigenden Stelle, analog der Kommentarfunktion, eine Einverständniserklärung hinterlegt werden, der erst zugestimmt werden muss, bevor die Daten versendet und die Karte geladen wird.

3.5.7 **Einbettung von personalisierter Werbung** am Beispiel „Google AdSense“

Google AdSense ist ein Service von Google, mit dessen Hilfe Werbung auf Webseiten angezeigt werden kann. Google erhält für die angezeigte Werbung eine Gebühr, von der dann ein Teil an den Betreiber der Webseite ausgezahlt wird.

Um möglichst relevante Werbung anzuzeigen, personalisiert Google diese Werbung, indem es sie an das Thema der Webseite und die Interessen des Nutzers anpasst. Dies geschieht größtenteils über Cookies, aber wie auch schon bei den anderen Google Diensten mittels Übertragung und Speicherung der IP-Adressen. [39]

Webseitenbetreiber werden diesbezüglich sowohl von Google als auch der Datenschutz-Grundverordnung dazu verpflichtet, verständliche und umfassende Informationen in der Datenschutzerklärung bereitzustellen, sowie zusätzlich die Einwilligung des Seitenbesuchers bezüglich der Erhebung personenbezogener Daten und dem Einsatz von Cookies

[37] (SKM Rechtsanwälte, kein Datum)

[38] (Borlabs, kein Datum)

[39] (Siebert, 2017)

einzuholen. Außer dem Verzicht auf personalisierte Werbung oder einer vorgeschalteten Seite, auf der der Nutzer einwilligt, Werbung quasi "im Tausch gegen seine IP-Adresse" zu erhalten, gibt es kaum Alternativen, da auch der Einbau von unpersonalisierter Werbung mit der Thematik der Übertragung von IP-Adressen behaftet sein kann.[40]

3.5.8 Cookies

Cookies sind kleine Datensätze, die von einer Webseite auf dem Rechner eines Besuchers gespeichert werden. In den meisten Fällen dienen sie zur Identifikation des Besuchers, entweder für die Umsetzung eines Logins oder zur Verfolgung des Nutzers über mehrere Seiten hinweg, um personalisierte Werbung anzuzeigen. Da sie zur eindeutigen Identifikation einer Person dienen, sind Cookies als personenbezogene Daten anzusehen.

Auch hier gibt es also wieder die beiden Möglichkeiten, die eindeutige Einwilligung des Besuchers einzuholen, oder auf das berechtigte Interesse des Anbieters zu verweisen. Um sich hier bestmöglich abzusichern, empfiehlt beispielsweise die "IT-Recht Kanzlei München":

> *[…] den Nutzer der Webseite durch einen Banner auf die Verwendung von Cookies hinzuweisen, und ihn darüber zu informieren, dass bei weiterem Besuch der Webseite von der Einwilligung des Nutzers in die Verwendung von Cookies ausgegangen wird.*[41]

3.5.9 Impressum

Grundsätzlich gilt für jede nicht private Webseite eine Informations- beziehungsweise Impressumspflicht. Hierbei ist zu beachten, dass der Einsatz von Werbeprogrammen oder sogenannten „Affiliate“-Links zur Folge hat, dass eine Webseite nicht mehr als privat eingestuft wird und der Betreiber als Unternehmer handelt und vor allem als solcher haftet. Dies wurde bereits im bisherigen Telemediengesetz behandelt, wird aber durch die neue Datenschutz-Grundverordnung insbesondere im Hinblick auf die möglichen Strafen deutlich verschärft.

In ein solches Impressum gehören unter anderem Name, Anschrift und Kontaktdaten des Unternehmens oder des Betreibers, sowie die rechtliche Vertretung und das entsprechende Handelsregister. Für die Erstellung eines vollständigen und korrekten Impressums gibt es wie auch für die Datenschutzerklärung Generatoren oder Checklisten, die zur Unterstützung herangezogen werden sollten.

[40] (Google, kein Datum)

[41] (Keller, 28)

3.5.10 Erstellung oder Anpassung der Datenschutzerklärung

Zusätzlich zum Impressum gibt es weitere Informationspflichten, die den Seitenbetreiber verpflichten, die Nutzer über die Erhebung und Verarbeitung von personenbezogenen Daten aufzuklären. Wie bereits bei der Impressumspflicht gab es die Pflicht zu einer Datenschutzerklärung bereits durch das Telemediengesetz, es sind allerdings einige Neuerungen hinzugekommen, wie beispielsweise die Pflicht, bei der Datenschutzerklärung eine „präzise, transparente, verständliche, klare und einfache Sprache“ zu benutzen.

Darüber hinaus muss die Datenschutzerklärung um den Umfang und die Rechtsgrundlage der Datenverarbeitung erweitert werden, um die Betroffenen auf ihre Rechte, beispielsweise zur Beschwerde über eine unrechtmäßige Datenverarbeitung oder zum Widerspruch gegen die Verarbeitung, hinzuweisen.

Aufgrund der enormen Bedeutung der Datenschutzerklärung für eine Webseite unter der neuen Datenschutz-Grundverordnung, ist hier angemessene Vorsicht geboten. Nicht nur fehlende, sondern auch falsche Angaben in der Datenschutzerklärung sind abmahnfähig, somit sollte darauf geachtet werden, dass alle datenverarbeitenden Prozesse korrekt aufgelistet werden und für jeden einzelnen dieser Prozesse eine Rechtsgrundlage vorliegt.

Eine gute Grundlage für vollständige und korrekte Datenschutzerklärungen kann ein Datenschutzerklärungs-Generator bieten. Das Ergebnis sollte allerdings individualisiert und vom Datenschutzbeauftragten, gegebenenfalls von einem Anwalt kontrolliert werden, um gegen eventuelle Abmahnungen gefeit zu sein.

a) Datenschutzerklärungs-Generatoren

Datenschutzerklärungs-Generatoren, wie der der Deutschen Gesellschaft für Datenschutz[42], fragen checklistenartig verschiedene informationspflichtige Seitenelemente ab und erzeugen aus Nutzerangaben zum Unternehmen und den abgegebenen Informationen eine Datenschutzerklärung.

Es ist jedoch wichtig anzumerken, dass diese aufgrund ihrer Natur nur Funktionen einbeziehen können, die in der Checkliste aufgeführt werden. Dies sind also in erster Linie webseitenübergreifende Aspekte wie Cookies, Kontaktformulare, Werbeeinblendungen und Traffic-Analysen. Viele unternehmensspezifische Datenverarbeitungen müssen nachträglich eingepflegt werden, sodass am Ende tatsächlich jede einzelne Funktion, die personenbezogene Daten erhebt oder verarbeitet, ausgewiesen ist.

[42] (Deutsche Gesellschaft für Datenschutz, kein Datum)

Prinzipiell erzeugen die meisten Datenschutzerklärungs-Generatoren gute und rechtssichere Formulierungen, die eine solide Grundlage bilden, falls man die Erstellung nicht an einen externen Spezialisten auslagern möchte.

3.5.11 NOINDEX Absicherung gegen automatische Abmahnskripte

Durch die NOINDEX-Direktive ist es technisch möglich, sich gegen automatische Abmahnungen zu schützen und Abmahnvereinen und Kanzleien die Arbeit etwas schwerer zu machen. Sie bewirkt, dass einzelne Teilseiten, wie beispielsweise die Datenschutzerklärung und das Impressum, nicht mehr von Suchmaschinen indexiert werden. Sie bietet jedoch keinen Schutz gegen manuelle Abmahnungen bei fehlerhaften Datenschutzerklärungen und anderen Abmahngründen.

Die NOINDEX-Direktive kann entweder direkt im Header einer Webseite eingetragen werden, oder von Suchmaschinen-Optimierungs-Plugins auf Seiten wie WordPress eingestellt werden. Neben der Verhinderung von Abmahnskripten, die mithilfe verschiedener Suchmaschinen nach Schwachstellen in Datenschutzerklärungen und Impressen suchen, bietet die NOINDEX-Direktive eine zusätzliche Suchmaschinen-Optimierung, da die meisten Suchmaschinen doppelte Inhalte, wie Texte, die von anderen Seiten kopiert wurden, als „Duplicate Content“ werten und die Qualität der Seite herabstufen.[43]

3.6 Einholen und Verwalten von Einwilligungen

Da die Einwilligung mit der Datenschutz-Grundverordnung an Wichtigkeit gewonnen hat, sollte auf eine korrekte Einholung von Einwilligungen große Sorgfalt gelegt werden. Hierzu gibt es verschiedene Möglichkeiten, die jedoch alle auf der gleichen Grundlage aufbauen:

> *Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.*[44]

Hier bieten sich folgende Verfahren an:

3.6.1 Direkte Einwilligung

Mit einer direkten Einwilligung, bei der der Nutzer einer Seite ein „Ich stimme zu“-Feld anklickt oder ein „Ich habe die Erklärung gelesen und bin einverstanden“-Häkchen setzt, ist ein Anbieter grundsätzlich auf der sicheren Seite. Wichtig ist hier, dass die Daten-

[43] (IT Logic GmbH, 2017)

[44] Vgl. Erwägungsgrund 32 DSGVO Einwilligung

schutzerklärung oder ein Hinweis auf die konkrete Verwendung personenbezogener Daten an der zu bestätigenden Stelle hinterlegt ist, damit sichergestellt ist, dass die Handlung informiert durchgeführt wurde.

Durch die direkte Natur der Einwilligung sind die Ansprüche der Eindeutigkeit und Unmissverständlichkeit ebenfalls gedeckt. Ein „Ich stimme der Verarbeitung meiner Daten zu“-Button ist eindeutig und auch bestätigend. Der Button darf nicht vorausgefüllt sein, da es sich anderenfalls nicht mehr um eine "eindeutige bestätigende Handlung" handelt und damit keine rechtswirksame Einwilligung vorliegt.

3.6.2 Konkludente Einwilligung

Anstelle einer direkten Einwilligung verwenden viele Seiten eine Art der konkludenten Einwilligung. Bei dieser wird bei dem ersten Besuch einer Seite auf die Verarbeitung von personenbezogenen Daten hingewiesen, welcher der Nutzer durch die Nutzung der Webseite zustimmt. Eine konkludente Einwilligung ist prinzipiell legal, es ist jedoch darauf zu achten, dass auch hier die Anforderungen an eine gültige Einwilligung erfüllt werden:

- keine Daten beim ersten Besuch der Seite verarbeitet werden
- die Einwilligung freiwillig erfolgt und der Nutzer nicht etwa durch versehentliches scrollen automatisch auf eine andere Seite navigiert wird
- der Nutzer auch hier über die Verwendung von seinen Daten, den Zweck der Verarbeitung und sein Widerrufsrecht informiert wird.

Da die Rechtswirksamkeit von konkludenten Einwilligungen letztlich Auslegungssache ist, sollte im Zweifelsfall eine direkte Einwilligung verwendet werden, um ausreichend abgesichert zu sein.

3.6.3 Speicherung der Einwilligung

Außerdem ist es erforderlich, die Einwilligung langfristig zu speichern und auch ausdrucken zu können, falls sie beispielsweise vor Gericht vorgelegt werden muss. Gemäß Art. 7 Abs. 1 DSGVO trägt hier der Verantwortliche die Beweislast. Das Vorliegen einer einwandfreien Einwilligung spielt demnach eine entscheidende Rolle, ob datenschutzkonform gehandelt wurde oder nicht.

3.6.4 Widerruf der Einwilligung

Zudem ist es nicht nur wichtig, die Einwilligung leicht ausdrucken zu können, sondern auch auf einen möglichen Widerruf der Einwilligung zu reagieren. Für eine unkomplizierte Ausübung sollte dem Nutzer eine technisch einfache Möglichkeit bereitgestellt werden, diese Einwilligung beispielsweise innerhalb seines Profils, am Ende der Seite, oder unter der Datenschutzerklärung widerrufen zu können.

Im Falle eines Widerrufs muss dies auf alle zukünftigen Interaktionen angewendet werden. Alle bisherigen Verarbeitungen bleiben von dem Widerruf unberührt, da sie auf der vorangegangenen rechtmäßigen Einwilligung beruhten.

3.6.5 Verarbeitung ohne Einwilligung

Zusätzlich zur Einwilligung gibt es noch weitere Fälle, in denen ein Erlaubnistatbestand nach Art. 6 DSGVO vorliegt, ohne dass eine tatsächliche Einwilligung gegeben wurde. Hierfür führt der Rechtsanwalt Dr. Carsten Ulbricht folgende Beispiele zu den verschiedenen Unterabschnitten des Art. 6 DSGVO in seinem Blog[45] auf:

a) Erfüllung eines Vertrages

Wenn die Datenverarbeitung zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist (Art.6 Abs.1 lit. b DSGVO). Wer im Onlineshop Daten zur Abwicklung der Bestellung (z.B. Name, Adresse, Kontoverbindung) oder Beantwortung einer Produktanfrage (z.B. über ein Kontaktformular) verarbeitet, braucht hierfür keine Einwilligung, weil Art.6 Abs.1 lit. b DSGVO dies eben bereits erlaubt.

b) Erfüllung einer rechtlichen Verpflichtung

Wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung der verarbeitenden Stelle erforderlich ist (Art.6 Abs.1 lit. c DSGVO). So sind Unternehmen z.B. nach 257 Abs. 1 HGB verpflichtet, verschiedene geschäftliche Unterlagen für 6 Jahre aufzubewahren. Wer zu etwas gesetzlich verpflichtet ist, braucht für eine entsprechende Datenverarbeitung natürlich auch keine Einwilligung.

c) Wahrung berechtigter Interessen des Verarbeiters oder eines Dritten

Wenn die Verarbeitung zur Wahrung berechtigter Interessen der verarbeitenden Stelle oder Dritter erforderlich ist und die Interessen des Betroffen nicht überwiegen (Art.6 Abs.1 lit. f DSGVO). Über die im Rahmen dieses Erlaubnistatbestandes vorzunehmende Interessenabwägung legitimiert eine Vielzahl üblicher und alltäglicher Datenverarbeitungsvorgänge in Unternehmen (z.B. Speicherung von Visitenkartendaten im CRM) ohne dass es hier einer Einwilligung bedürfte.

Diese Erlaubnistatbestände sind einer Einwilligung gleichgestellt, so dass eine gesonderte Einwilligung nicht erforderlich ist.

3.7 Überprüfung der Auftragsdatenverarbeitung

Die Auftragsverarbeitung wurde in den Grundlagen bereits angesprochen, sie verdient jedoch einen eigenen Absatz. Grundsätzlich stellt sie kein Problem bei der Verarbeitung von personenbezogenen Daten dar, es ist jedoch auf folgende zusätzliche Punkte zu achten:

[45] (Dr. Ulbricht, 2018)

- der Nutzer hat eine Einwilligung zu dieser besonderen Form der Verarbeitung seiner Daten abzugeben
- zwischen dem Webseitenbetreiber und dem Auftragsverarbeiter muss ein Datenverarbeitungsvertrag vorliegen
- darüber hinaus liegt die Verantwortung der Datenverarbeitung unverändert bei dem eigentlichen Anbieter, also beispielsweise dem Webseitenbetreiber. Im Falle eines Verstoßes sind die Betroffenenrechte gegenüber diesem geltend zu machen
- außerdem obliegen dem eigentlichen Anbieter zusätzliche Kontrollpflichten, wonach er bei Vertragsbeginn und während der Vertragslaufzeit regelmäßig die technischen und organisatorischen Schutzmaßnahmen des Verarbeiters zu prüfen und diese Prüfung zu dokumentieren hat

3.8 Datenschutz innerhalb eines Unternehmens

Die Datenschutz-Grundverordnung betrifft nicht nur Anbieter von Internetseiten. Sämtliche, auch unternehmensinterne Prozesse, in denen personenbezogene Daten verarbeitet werden, sind von den neuen Regelungen betroffen. Demnach kann es sich neben den bereits angesprochenen Internetseiten auch um interne Mitarbeiterlisten oder Entgeltabrechnungen der Personalabteilung handeln.[46]

3.8.1 Der Umgang mit alten Daten

Da in Zukunft alle nicht mehr benötigten Daten ein „Verfallsdatum“ haben müssen, entsteht für viele Unternehmen ein Problem, über das sie bisher wahrscheinlich nicht nachgedacht haben. Viele Daten von ehemaligen Mitarbeitern müssen künftig mit deren Austritt aus der Firma gelöscht werden und auch Backups und Sicherungsdateien müssen jedes Mal nach zu löschenden Datensätzen abgesucht werden.

Erschwert wird dieses Problem durch eine anfängliche Unsicherheit in der Auslegung der neuen Gesetze, was die Kategorisierung und die jeweiligen Aufbewahrungsfristen der einzelnen Daten betrifft.

Hier sollte also, wie schon bei der Auswahl des Einwilligungsverfahrens, eine begründete Entscheidung für eine konkrete Lösung hinsichtlich Erfassung, Verwendung und Aufbewahrung der Daten getroffen werden, um sich im Ernstfall rechtfertigen zu können und der Rechenschaftspflicht Genüge zu tun. Schließlich ist die Rechenschaftspflicht einer der wichtigsten Kernbestandteile der neuen Datenschutz-Grundverordnung und indiziert, ob im Zweifelsfall ein schuldhaftes Handeln vorliegt oder nicht.

[46] (Schmitz, 2018)

3.8.2 Die Probleme der Visitenkarten

Die Sammlung von Visitenkarten und insbesondere die Übertragung der Daten von der Visitenkarte in eine Unternehmensdatenbank ist hinsichtlich der Behandlung im Sinne der Datenschutz-Grundverordnung noch nicht abschließend geklärt. Da es sich hierbei um personenbezogene Daten handelt, finden auch hierfür die neuen Regelungen Anwendung. Somit müsste also bei der Übergabe der Visitenkarte bereits ein Zweck der Verwendung bekannt gemacht und eine Einwilligung eingeholt werden, was im täglichen Geschäftsleben kaum praktikabel ist.

Die Geschäftsleiterin von Bitkom empfiehlt hier beispielsweise, dass bei Übertragung der Daten von der Visitenkarte in die Unternehmensdatenbank eine E-Mail an den Betroffenen geschickt werden sollte, in der er auf die Verwendung seiner Daten und insbesondere seine Möglichkeiten zum Widerspruch gegen eine Verarbeitung aufgeklärt wird.[47]

Andererseits könnte man auch anführen, dass es sich hier um eine Verarbeitung zur Wahrung berechtigter Interessen der verarbeitenden Stelle handelt, die die Interessen der Betroffenen überwiegen. Es bleibt insofern abzuwarten, wie eventuelle Gerichtsurteile hierüber befinden.

3.9 Erstellung der Datenschutz-Dokumentation

Abschließend geht es nun zu der Erfüllung der Rechenschaftspflichten. Darunter fällt insbesondere die Erstellung der Datenschutz-Dokumentation, die die verschiedenen Punkte, zu denen Rechenschaft abgelegt werden muss, auflistet und erläutert. Es handelt sich hierbei um das Verzeichnis der Verarbeitungstätigkeiten, die Liste der verwendeten organisatorischen und technischen Maßnahmen, die Erläuterung der verwendeten Schutzprinzipien des Unternehmens und gegebenenfalls eine Folgenabschätzung im Falle einer besonderen Gefährdung der Rechte und Freiheiten der betroffenen Nutzer.

Wichtig ist, dass diese Dokumentation jederzeit vorgelegt werden kann, da schon bereits das Fehlen dieser Dokumentation als Verstoß gewertet wird, auch wenn die Datenverarbeitung selbst gesetzeskonform abläuft.

Im Folgenden werden die einzelnen Abschnitte der zu erstellenden Dokumentation aufgelistet und erläutert. Hierzu wurde die von der „DSGVO-Vorlagen“-Webseite veröffentlichte Beispieldokumentation[48] erweitert und anschließend erläutert.

[47] (Seibel, 2018)

[48] (DeinData UG, kein Datum)

3.9.1 Hauptteil der Dokumentation

Im Hauptteil werden die wesentlichen Informationen über die Webseite, den Blog, oder das Unternehmen erläutert. Dieser sollte den Anfang der Dokumentation bilden und folgende Bestandteile aufweisen:

- Kontaktdaten der für die Verarbeitung verantwortlichen Stelle und des entsprechenden Vertreters
- Unternehmen beziehungsweise die zuständige Niederlassung
- Informationen zum Datenschutzbeauftragten und dessen Kontaktdaten
- das grundsätzlich verwendete Löschungskonzept, welches für alle Verfahren verwendet wird
- das grundsätzliche Vorgehen bei einer Übermittlung an Drittländer, insbesondere an Länder außerhalb der EU, wie beispielsweise eine Verschlüsselung der Übertragung

3.9.2 Verzeichnis der Verarbeitungstätigkeiten

Auf den einleitenden Hauptteil folgt das Verzeichnis der Verarbeitungstätigkeiten. Prinzipiell könnten viele Unternehmen von der Pflicht, dieses Verzeichnis zu erstellen, befreit werden, allerdings sind die erforderlichen Kriterien so vage formuliert, dass entweder auf einen konkreten Gerichtsfall gewartet oder bis dahin auf jeden Fall ein solches Verzeichnis angelegt werden sollte.

Die Struktur dieses Verzeichnisses kann der Einfachheit halber mit den Erklärungen in der Datenschutzerklärung übereinstimmen, da alle Funktionen, die dort aufgelistet werden, hier noch einmal detailliert dokumentiert werden müssen.

Dieses Verzeichnis besteht aus einem für alle verwendeten Verfahren gleichen, an Art. 30 DSGVO und § 70 BDSG angelehnten Formular. Hierbei ist wichtig, dass wirklich alle Verarbeitungstätigkeiten aufgelistet sind:

- die Bezeichnung der jeweiligen Verarbeitungstätigkeit
- der Name von gegebenenfalls eingesetzten Tools oder Dienstleistungen
- das Datum des Beginns der Nutzung des Verfahrens
- das Datum der letzten Überprüfung des Verfahrens
- die verantwortliche Stelle innerhalb des Unternehmens
- der Name und die Kontaktdaten des Verantwortlichen
- der Zweck der Verarbeitungstätigkeit
- die Kategorie der betroffenen Personen
- die Kategorien der verarbeiteten Daten
- die Kategorien der Empfänger der Daten

- die Rechtsgrundlage der Datenerhebung, -verarbeitung und -nutzung
- gegebenenfalls die Angabe einer Übermittlung an Drittstaaten
- spezielle Abweichungen der Löschfristen und -konzepte
- spezielle technische und organisatorische Maßnahmen

3.9.3 Verwendete technische und organisatorische Maßnahmen

Hier sind die vom Unternehmen verwendeten Maßnahmen aufzulisten, wobei insbesondere Rücksicht auf die zentralen Aspekte der Datensicherheit zu nehmen ist:

- **Der Vertraulichkeit**
  Werden die Daten vor dem Zugriff Unberechtigter geschützt?
- **Der Verschlüsselung**
  Werden die Daten verschlüsselt um sie zu schützen?
- **Der Anonymisierung**
  Werden Daten, beispielsweise vor der Analyse, anonymisiert?
- **Der Datenintegrität**
  Können Daten aktualisiert oder zuverlässig gelöscht werden?
- **Der Absicherung gegen Datenverluste**
  Werden zur Absicherung bei Systemabstürzen Backups der Daten angelegt?
- **Der Kontrolle der Systeme und Drittanbieter**
  Wie und wie regelmäßig wird die Funktionalität der Systeme und der Drittanbieter überprüft?

Es geht an dieser Stelle noch nicht darum, diese konkreten Fragen zu beantworten, sondern vielmehr darum, die vom Unternehmen gewählten Konzepte darzustellen.

3.9.4 Datenschutz-Folgenabschätzung

Sollte durch die Verarbeitung ein besonders hohes Risiko für Betroffene vorliegen, oder eine systematische und umfassende Bewertung wie Profiling oder eine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten durchgeführt werden, muss zudem eine Datenschutz-Folgenabschätzung vorgenommen werden.

Diese Folgenabschätzung sollte durch den Datenschutzbeauftragten erfolgen und enthält mindestens:

- eine Beschreibung der geplanten Verarbeitungsvorgänge
- der Zweck der Verarbeitung
- eine Bewertung der Notwendigkeit der Verarbeitung
- eine Bewertung der Risiken für die betroffenen Personen
- eine Liste an Maßnahmen zur Abwendung der Risiken

Zusätzlich zu der Folgenabschätzung muss in diesem Falle außerdem noch eine vorherige Konsultation mit der entsprechenden Aufsichtsbehörde erfolgen. Diese kann im Falle eines noch nicht einschätzbaren oder unzureichend eingedämmten Risikos Empfehlungen zur Verarbeitung oder sogar Verbote aussprechen.

4 Fazit

Die neue Verordnung bringt viele wichtige Neuerungen und Absicherungen für Internetnutzer und alle Kunden, die persönliche Daten zur Verfügung stellen, sei es bei Social Media, Versandshops oder Banken. Den Einzelnen wird ermöglicht, zu wissen, was mit ihren Daten passiert, und einer Verarbeitung zu widersprechen. Gerade den Nutzern von Onlinediensten sollte der Anblick von neuen Bestätigungsformularen auf Internetseiten die Beruhigung bieten, dass sie nun selbst in der Hand haben, was mit ihren Daten passiert.

Natürlich bringt dies auch neue Aufgaben und Herausforderungen für die Anbieter der verschiedenen Dienstleistungen. Prozesse müssen überarbeitet, Datenschutzerklärungen umgeschrieben und Dokumentationen angefertigt werden, aber für die meisten Unternehmen und Webseitenbetreiber sollte dies durchaus zu bewältigen sein. Mittlerweile gibt es zahlreiche Möglichkeiten der Unterstützung bei diesen Aufgaben. Von einschlägigen Internetseiten über die Möglichkeit der Einbindung von externen Datenschutzbeauftragten bis hin zu einer professionellen Beratung durch einen Anwalt kann dem individuellen Sicherheitsbedürfnis und den jeweiligen finanziellen Möglichkeiten Rechnung getragen werden.

Solange die Verarbeitung von Daten rechtmäßig ist und hierfür ein Erfordernis besteht - und davon ist, wenn Anbieter und Kunde zusammenkommen, in den überwiegenden Fällen auszugehen - kann nahezu alles erfragt und verarbeitet werden. Und selbst wenn einmal Zweifel bei einer Verarbeitung bestehen, können diese im Normalfall mit einer entsprechenden Einwilligung ausgeräumt werden.

Auch die Angst vor Abmahnungen relativiert sich, da grundsätzlich einfache Anpassungen von Webseiten und Geschäftsprozessen sowie eine solide Datenschutzerklärung ausreichen, um jegliche Abmahnungen zu verhindern. Verschiedene Veröffentlichungen berichten zwar immer von möglichen Millionenstrafen, da diese allerdings von dem Unternehmensumsatz und der Art der Datenschutzverletzung abhängen, sollte es insbesondere bei kleinen und mittelständischen Unternehmen nicht einmal zu einem Bruchteil davon kommen. Solange in der Datenschutz-Dokumentation eine besonnene Abwägung der Risiken und der verwendeten Schutzmaßnahmen sowie eine umfassende Klärung der Rechtmäßigkeit der Verarbeitung stattgefunden hat und nicht grob fahrlässig gehandelt wird, sollten die meisten Unternehmen gut gewappnet sein.

Alles in allem wird kein Unternehmen Probleme mit der Datenschutz-Grundverordnung haben, wenn es sich mit der Thematik angemessen beschäftigt. Das zunächst propagierte Ende aller Blogs oder die befürchteten Abmahnfallen für kleine und mittelständische Unternehmen haben sich mit der Einführung der Datenschutz-Grundverordnung nicht bewahrheitet.

5 Literaturverzeichnis

Bayerisches Landesamt für Datenschutzaufsicht. (2018. Januar 2016). *Kurzpapier Auftragsverarbeitung.* Abgerufen am 30. Juli 2018 von https://www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf

Bayerisches Landesamt für Datenschutzaufsicht. (09. Juni 2018). *EU-Datenschutz-Grundverordnung.* Abgerufen am 30. Juli 2018 von https://www.lda.bayern.de/media/baylda_ds-gvo_1_security.pdf

Bayerisches Landesamt für Datenschutzaufsicht. (2018). *Handreichungen für kleine Unternehmen*. Abgerufen am 30. 07 2018 von https://www.lda.bayern.de/de/kleine-unternehmen.html

Bild. (26. Mai 2018). *Datenschutz-Wahnsinn - DSGVO-Chaos führt zu Handy-Verbot beim Arzt*. Abgerufen am 30. Juli 2018 von https://www.bild.de/bild-plus/digital/internet/datenschutzvorschriften/dgsvo-total-verrueckt-55802426

Bleich, H. (30. Mai 2018). *DSGVO: Die Abmahn-Maschinerie ist angelaufen*. Abgerufen am 30. Juli 2018 von https://www.heise.de/newsticker/meldung/DSGVO-Die-Abmahn-Maschinerie-ist-angelaufen-4061044.html

Borlabs. (kein Datum). *Borlabs Cookie - IFrame Demo*. Abgerufen am 30. Juli 2018 von https://de.borlabs.io/borlabs-cookie-iframe-demo/

Brünnen, B. (2018). *E-Mail-Marketing 2018: Was ändert sich durch die DSGVO in Bezug auf Newsletter?* Abgerufen am 30. Juli 2018 von https://www.it-recht-kanzlei.de/newsletter-datenschutzgrundverordnung-dsgvo.html

Datenschutz-Grundverordnung. (kein Datum). *Online Gesetzestext der Datenschutz-Grundverordnung*. Abgerufen am 30. Juli 2018 von https://dsgvo-gesetz.de/

DeinData UG. (kein Datum). *Bestandteile eines Verfahrensverzeichnisses nach DSGVO*. Abgerufen am 30. Juli 2018 von https://dsgvo-vorlagen.de/bestandteile-muessen-in-verfahrensverzeichnis-dsgvo

Deutsche Gesellschaft für Datenschutz. (kein Datum). *Ihre DSGVO-Konforme Datenschutzerklärung per Klick*. Abgerufen am 30. Juli 2018 von https://dsgvo-muster-datenschutzerklaerung.dg-datenschutz.de

Dr. Ulbricht, C. (02. Mai 2018). *Zu viele Mythen und gefährliches Halbwissen zum neuen europäischen Datenschutzrecht*. Abgerufen am 30. Juli 2018 von http://www.rechtzweinull.de/archives/2558-mein-erster-dgsvo-rant-zu-viele-mythen-und-gefaehrliches-halbwissen-zum-neuen-europaeischen-datenschutzrecht.html

Google. (kein Datum). *Richtlinie zur Einwilligung der Nutzer in der EU*. Abgerufen am 30. Juli 2018 von https://www.google.com/about/company/user-consent-policy.html

Hegemann, L. (18. Mai 2018). *Keine Website ist auch keine Lösung*. Abgerufen am 30. Juli 2018 von https://www.zeit.de/digital/datenschutz/2018-05/dsgvo-blogger-websites-datenschutz-umsetzung-tipps

Herold Unternehmensberatung GmbH. (kein Datum). *Datenschutz-Grundverordnung: Die Uhr tickt - wo Unternehmen handeln müssen*. Abgerufen am 30. Juli 2018 von https://www.mein-datenschutzbeauftragter.de/eu-datenschutz-grundverordnung/

Hiddemann, N. (04. August 2017). *Datenschutzgrundverordnung: Was ändert sich im Bereich Direktwerbung per E-Mail?* Abgerufen am 30. Juli 2018 von https://www.anwalt.de/rechtstipps/datenschutzgrundverordnung-was-aendert-sich-im-bereich-direktwerbung-per-e-mail_112661.html

Information Commissioner's Office. (kein Datum). *Data protection by design and default .* Abgerufen am 30. Juli 2018 von https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

IT Logic GmbH. (23. Dezember 2017). *Impressum und Datenschutzerklärung: NOINDEX gegen Abmahnungen*. Abgerufen am 30. Juli 2018 von https://www.webseitenschutzpaket.de/artikel/impressum-datenschutzerklaerung-noindex/

Keller, M.-L. (28. November 28). *Verwendung von Cookies nach Datenschutzgrundverordnung nur noch bei vorheriger ausdrücklicher Einwilligung des Nutzers?* Abgerufen am 30. Juli 2018 von https://www.it-recht-kanzlei.de/cookies-eu-datenschutz-grundverordnung.html

Oexman, D., Visser, J., Molenaar, M., van Tulder, M., & Van, O. (2018). *WP GDPR Compliance*. Abgerufen am 30. Juli 2018 von https://wordpress.org/plugins/wp-gdpr-compliance/

Schmitz, P. (20. Juni 2018). *DSGVO betrifft auch den Datenschutz in HR und Payroll*. Abgerufen am 30. Juli 2018 von https://www.security-insider.de/dsgvo-betrifft-auch-den-datenschutz-in-hr-und-payroll-a-723807/

Schuster, H. (19. Oktober 2017). *Schlecht vorbereitet auf die DSGVO*. Abgerufen am 30. Juli 2018 von https://www.it-business.de/schlecht-vorbereitet-auf-die-dsgvo-a-654325/

Seibel, K. (18. Mai 2018). *Jetzt werden sogar Visitenkarten zur Datenschutz-Falle*. Abgerufen am 30. Juli 2018 von https://www.welt.de/wirtschaft/article176468214/DSGVO-Visitenkarten-werden-durch-neue-EU-Regel-zum-Datenschutz-Problem.html

Siebert, S. (11. Oktober 2017). *Datenschutz: Was Sie zu Google AdSense wissen müssen*. Abgerufen am 30. Juli 2018 von https://www.e-

recht24.de/artikel/datenschutz/6635-datenschutz-rechtliche-risiken-bei-der-nutzung-von-google-analytics-und-googleadsense.html

SKM Rechtsanwälte. (kein Datum). *Datenschutzerklärung der SKM Rechtsanwälte*. Abgerufen am 30. Juli 2018 von https://www.skm-rechtsanwaelte.de/datenschutz/

Eidesstaatliche Erklärung

Ich versichere, die von mir vorgelegte Arbeit selbstständig verfasst zu haben. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder nicht veröffentlichten Arbeiten anderer oder der Verfasserin/des Verfassers selbst entnommen sind, habe ich als entnommen kenntlich gemacht. Sämtliche Quellen und Hilfsmittel, die ich für die Arbeit benutzt habe, sind angegeben. Die Arbeit hat mit gleichem Inhalt bzw. in wesentlichen Teilen noch keiner anderen Prüfungsbehörde vorgelegen.

Ort, Datum

Rechtsverbindliche Unterschrift