Masterthesis

Eingereicht an der ZHAW – School of Managment and Law

Datenschutzverzeichnisse nach EU-DSGVO

Modelle zum Verzeichnis von Verarbeitungstätigkeiten

Vorgelegt von

Valérie Thommen

Neuwiesenstrasse 33, 8400 Winterthur

thommval@students.zhaw.ch

Matrikelnummer: 10-276-368

Betreuer/Erstgutachter

Dr. Nico Ebert

Zweitgutachter

Dr. Peter Heinrich

Abgabe

Winterthur, 25. Mai 2018

Wahrheitserklärung

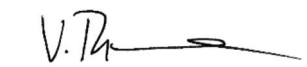
„Ich erkläre hiermit, dass ich die vorliegende Arbeit selbständig, ohne Mithilfe Dritter und nur unter Benützung der angegebenen Quellen verfasst habe und dass ich ohne Zustimmung des Betreuers keine Kopien dieser Arbeit an Dritte aushändigen werde."

Gleichzeitig werden sämtliche Rechte am Werk an die Zürcher Hochschule für angewandte Wissenschaften (ZHAW) abgetreten. Das Recht auf Nennung der Urheberschaft bleibt davon unberührt.

Name der / des Studierenden (Druckbuchstaben)

Valérie Thommen

Unterschrift der / des Studierenden



……..

Danksagung

Hiermit bedanke ich mich bei allen, die mich bei der Masterthesis unterstützt haben. Allen voran bedanke ich mich bei den drei Experten, die mir im Rahmen der durchgeführten Interviews wertvollen Input für die Erarbeitung der Resultate geliefert haben.

Ein besonderer Dank gilt auch Nico Ebert, der meine Masterthesis betreut hat. Vielen Dank, Nico, dass ich während der gesamten Zeit auf deine Unterstützung zählen durfte. Die Zusammenarbeit habe ich als sehr angenehm empfunden.

Abstract

Seit dem 25. Mai 2018 gilt die Europäische Datenschutzgrundverordnung (EU-DSGVO) für alle Mitgliedstaaten der Europäischen Union. Sie beinhaltet Vorschriften, die organisatorische Änderungen in den betroffenen Unternehmen erfordern. Ein zentraler Teil der DSGVO ist ein Datenschutzverzeichnis, das eine Übersicht über Verfahren, bei denen personenbezogene Daten verarbeitet werden, beinhaltet. Bis auf wenige Ausnahmen sind alle Unternehmen, die personenbezogene Daten von Personen, die sich in der EU befinden, verarbeiten, verpflichtet, das in der Verordnung als «Verzeichnis von Verarbeitungstätigkeiten» bezeichnete Datenschutzverzeichnis zu führen und auf Anfrage der zuständigen Aufsichtsbehörde zur Verfügung zu stellen.

Die vorliegende Masterthesis beschäftig sich damit, wie die gesetzlich geforderten Bestandteile sowie Anforderungen aus der Praxis in einem formalen Modell (Ontologie) dargestellt werden können, um Zusammenhänge zu verdeutlichen und ein einheitliches Verständnis zu schaffen.

Die Herleitung des Modells erfolgt anhand eines iterativen Prozesses auf Grundlage der Ausführungen in der DSGVO, Ansätzen zum Verzeichnis von Verarbeitungstätigkeiten sowie Experteninterviews. Sie beruht auf einer Methodologie zur Erstellung von Ontologien. Entstanden sind letztendlich zwei Artefakte in Form von Ontologien, die ein schnelles Verständnis für die Anforderungen an die Datenschutzverzeichnisse nach DSGVO ermöglichen. Die Artefakte können als Grundlage für die Entwicklung einer Methodologie zur Umsetzung eines Verzeichnisses von Verarbeitungstätigkeiten, für Wikis oder Softwaresysteme dienen.

Inhaltsverzeichnis

I Tabellenverzeichnis

II Abbildungsverzeichnis

III Abkürzungsverzeichnis

BvD	Berufsverband der Datenschutzbeauftragten Deutschlands
CPP	Commission for the protection of privacy
CRM	Customer-Relationship-Management
DSGVO	Datenschutzgrund-Verordnung
DSK	Datenschutzkonferenz
DSRM	Desing Science Research Methodology
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
E-DSG	Entwurf Datenschutzgesetz
GDD	Gesellschaft für Datenschutz und Datensicherheit
ISO	International Organization for Standardisation
SQS	Schweizerischen Vereinigung für Qualitäts- und Management-Systeme
TOM	Technische und organisatorische Massnahmen
UML	Unified Modeling Language
VV	Verzeichnis von Verarbeitungstätigkeiten
	Verzeichnis der Bearbeitungstätigkeiten
VVA	Verzeichnis von Verarbeitungstätigkeiten für Auftragsverarbeiter
	Verzeichnis der Bearbeitungstätigkeiten für Auftragsbearbeiter
VVU	Verzeichnis von Verarbeitungstätigkeiten für Unternehmen
	Verzeichnis der Bearbeitungstätigkeiten für Unternehmen
WKO	Wirtschaftskammern Österreichs

1 Einleitung

In der Einleitung wird zunächst die Ausgangslage beschrieben, die als Grundlage für die darauffolgende Problemstellung dient. Darauf folgen die Zielsetzung zusammen mit der Definition der zu beantwortenden Forschungsfragen sowie deren Abgrenzung. Abschliessend wird der Aufbau der Masterthesis erläutert.

1.1 Ausgangslage

Am 27. April 2016 wurde die Verordnung 2016/679 des Europäischen Parlaments und Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG veröffentlicht und trat 20 Tage später in Kraft. Die sogenannte Datenschutz-Grundverordnung (DSGVO) (Art. 99) gilt seit dem 25. Mai 2018 für alle Mitgliedstaaten der Europäischen Union. Was dies explizit bedeutet und welche Vorschriften aus der Verordnung hervorgehen, wird im Folgenden erläutert.

1.1.1 Geltungsbereich DSGVO

Gemäss DSGVO, Artikel 3 findet die Verordnung Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Unternehmens in der EU erfolgt, unabhängig davon, wo die Verarbeitung stattfindet. Weiter findet die Verordnung Anwendung auf die Verarbeitung personenbezogener Daten von Personen, die sich in der EU befinden, durch ein nicht in der EU niedergelassenes Unternehmen. Dies ist der Fall, wenn die Datenverarbeitung damit im Zusammenhang steht, Personen in der EU Waren oder Dienstleistungen anzubieten oder das Verhalten von Personen zu beobachten.

Rechtsanwältin Dr. Ursula Widmer von Dr. Widmer & Partner, Rechtsanwälte (2017) beschreibt die Geltung der DSGVO für Schweizer Unternehmen zusammengefasst wie folgt:

> «Die Verordnung findet Anwendung für Schweizer Unternehmen mit Niederlassung in der EU (Niederlassungsprinzip). Dies trifft zu für Schweizer Unternehmen, die Personendaten für Tochtergesellschaften verarbeiten oder IT-Dienstleistungen für Kunden in der EU erbringen. Das Marktortprinzip (Angebot von Waren oder Dienstleistungen an Personen in der EU) kommt dann zum

> Tragen, wenn der Produktekauf im Online-Shop oder eine Online-Buchung für Personen aus der EU möglich ist. Darunter fällt auch der Direktvertrieb in Form von Telefonmarketing oder Inseratewerbung an Verbraucher in der EU. Unter Verhaltensbeobachtungen fallen zum Beispiel Dienstleistungen wie Besucherstrom- und Frequenzanalysen, die für ein Unternehmen in der EU ausgeführt werden.»

Analoge Schlüsse ziehen Raoul Egeli, Geschäftsführer des Schweizerischen Gläubigerverbands Creditreform (2016), und Rechtsanwalt Dr. Martin Eckert vom Beratungsunternehmen MME (2016). Das EU-Recht gilt somit für alle Schweizer Exporteure, Versandhändler, Betreiber von Onlineplattformen für Onlinebestellungen und Dienstleister, die ihre Leistungen Kunden in der EU anbieten (Widmer, 2016).

1.1.2 Bevorstehende Erneuerung des Schweizer Datenschutzgesetzes

Schweizer Unternehmen, die nicht dem EU-Recht unterstehen, sind indirekt ebenfalls von der DSGVO betroffen, da die Verordnung in der laufenden Revision des Schweizerischen Datenschutzrechts berücksichtigt werden muss, um die Gleichwertigkeit des schweizerischen Datenschutzgesetzes mit demjenigen der EU weiterhin zu gewährleisten (Widmer, 2016). Nur so ist ein reibungslos funktionierender Datenaustausch mit EU-Ländern auch zukünftig möglich, was aus gesamtwirtschaftlicher Sicht von grosser Wichtigkeit ist (Bühlmann, 2017). Zudem hat sich die Schweiz gemäss dem Schengen-Assoziierungsabkommen grundsätzlich verpflichtet, jede Weiterentwicklung des Schengen-Besitzstandes zu akzeptieren, umzusetzen und anzuwenden (Schweizerische Eidgenossenschaft, die Europäische Union und die Europäische Gemeinschaft, 2008, Art. 2, Abs. 3).

1.1.3 Neue gesetzliche Vorschriften

Aus den neuen Gesetzen gehen insbesondere für Personen, deren Daten in Unternehmen bearbeitet werden, neue Rechte hervor. So müssen Unternehmen bereits bei der Erhebung von Daten die betroffene Person umfangreich informieren (DSGVO, Art. 13). Darüber hinaus hat dieser Personen jederzeit das Recht von einem Unternehmen zu erfahren, ob sie betreffende personenbezogene Daten verarbeitet werden und haben ausserdem das Recht auf Informationen bezüglich der Bearbeitung. Dazu zählen die Verarbeitungszwecke, die Kategorien personenbezogener Daten, die von der Person bearbeitet werden,

Empfänger sowie mögliche Empfänger der Daten. Zusätzlich muss über die Rechte informiert werden, die mit den Daten im Zusammenhang stehen (DSGVO, Art. 15). Darunter fallen das Recht auf Berichtigung (DSGVO, Art. 16), das Recht auf Löschung (DSGVO, Art. 17) und das Recht auf Einschränkung der Bearbeitung von Daten, wenn die Richtigkeit bestritten wird oder die Bearbeitung unrechtmässig ist (DSGVO, Art. 18). Analoge Formulierungen gehen aus dem Entwurf zum neuen Schweizer Datenschutzgesetz hervor (E-DSG, Art. 23 und 28). Auch Anwälte und Datenschützer sehen die Informationspflicht und die Rechte von betroffenen Personen als einen der wesentlichen Punkte der neuen Gesetze an (vgl. Datenschutzbeauftragter INFO, 2016a; Polenz, 2018; Seidl-Nussbaumer, 2017; Wirtschaftskammern Österreichs, 2018c).

Neben den Rechten der Personen stellen der Datenschutz durch Technikgestaltung (Privacy-by-Design) sowie datenschutzfreundliche Voreinstellungen (Privacy-by-Default) in den Systemen wesentliche Punkte in den neuen Gesetzen dar (DSGVO, Art. 25; E-DSG Art. 19 und 20). Zu diesem Schluss kommen auch Polenz (2018), Widmer (2017) und die Wirtschaftskammern Österreichs (WKO) (2018c). Unterliegt eine Form der Verarbeitung beispielsweise durch die Verwendung neuer Technologien oder aufgrund der Zwecke der Verarbeitung einem hohen Risiko, so sind Datenschutz-Folgeabschätzungen vorzunehmen. Dies bedeutet, dass vorab Abschätzungen der Folgen der vorgesehenen Bearbeitungen durchgeführt werden müssen (DSGVO, Art. 35; E-DSG Art. 20). Die Datenschutz-Folgeabschätzung betrachten auch Widmer (2017), Seidl-Nussbaumer (2017) und Balthasar (2018) als eine wesentliche Erneuerung.

Die neuen Gesetze sehen eine Auszeichnungspflicht in Form eines Datenschutzverzeichnisses vor, das jedes Unternehmen führen muss. Dieses Verzeichnis dient als Grundlage, um anderen gesetzlichen Anforderungen nachzukommen. Auch Anwälte und Datenschützer sind sich einig, dass das sogenannte Verzeichnis der Verarbeitungstätigkeiten (DSGVO, Art. 30) beziehungsweise das Verzeichnis der Bearbeitungstätigkeiten (E-DSG, Art. 11) einer der wichtigsten Aspekte der neuen Gesetze ist (vgl. Balthasar, 2018; Polenz, 2018; Seidl-Nussbaumer, 2017; Widmer, 2017; Wirtschaftskammern Österreichs, 2018c).

Die Einhaltung und Umsetzung der Anforderungen der neuen Gesetze ist insbesondere aufgrund der vor allem nach DSGVO (Art. 83) hohen Bussen von bis zu 20 Millionen Euro beziehungsweise bis zu vier Prozent des Jahresumsatzes ratsam. Die im E-DSG

(Art. 54ff) aktuell vorgesehenen Bussen von bis zu 250'000 Franken sind vergleichsweise niedrig, wobei die persönliche Strafbarkeit im Vordergrund steht. Bussen für Unternehmen können nur bis zu einer Höhe von 50'000 Franken betragen. Das Strafmass wird auch von Balthasar (2018), Widmer (2017), Datenschutzbeauftragter INFO (2016a), Seidl-Nussbaumer (2017) sowie den WKO (2018c) als entscheidend angesehen.

1.2 Problemstellung

Für Unternehmen, die der DSGVO, beziehungsweise in Kürze auch für Unternehmen, die dem neuen Schweizer Datenschutzgesetz (vgl. E-DSG) unterstellt sind, stellt sich die Frage, wie vorgegangen werden soll, um den neuen gesetzlichen Vorgaben gerecht zu werden.

Ein zentraler Bestandteil der DSGVO ist Artikel 30, der ein ‚Verzeichnis von Verarbeitungstätigkeiten' vorschreibt. Bei diesem Verzeichnis handelt es sich um eine Dokumentation und Übersicht über Verfahren, bei denen personenbezogene Daten verarbeitet werden (Datenschutzbeauftragter INFO, 2016b). Es geht im Wesentlichen darum, Verantwortliche für die Verfahren in einem Unternehmen zu definieren und aufzuzeigen, wozu die Verarbeitung dient und welche Kategorien von Personen und Daten im jeweiligen Verfahren bearbeitet werden (DSGVO, Art. 30). Das Gleiche gilt für Auftragsverarbeiter, die im Auftrag eines Verantwortlichen personenbezogene Daten verarbeiten.

Der aktuelle Entwurf des neuen Schweizerischen Datenschutzgesetzes (E-DSG) (Art. 11) sieht ein analoges Verzeichnis vor, das als ‚Verzeichnis der Bearbeitungstätigkeiten' bezeichnet wird. Eine detaillierte Übersicht über die gesetzlich geforderten Bestandteile der besagten Verzeichnisse ist im Anhang v zu finden.

Aus der Literatur geht hervor, dass das Verzeichnis von Verarbeitungstätigkeiten beziehungsweise das Verzeichnis der Bearbeitungstätigkeiten ein zentrales Element des Datenschutzrechts bildet (Bitcom, 2017, S. 6). Voigt und von dem Bussche (2017, S. 248) betrachten das Verzeichnis als ein zentrales Element bei der Implementierung der DSGVO. Bestärkt werden diese Aussagen durch die Ergebnisse der Experteninterviews, die im Rahmen der vorliegenden Masterthesis durchgeführt wurden. Die befragten Experten sehen das Verzeichnis als einen der ersten Schritte bei der Umsetzung der DSGVO und als Voraussetzung für die Einhaltung der anderen Verpflichtungen an, die aus der DSGVO hervorgehen (Interview A und C). Um die weiterführenden Ausführungen zu

vereinfachen, folgt nun zunächst eine Begriffsklärung sowie eine Erläuterung bezüglich der Frage, welche Unternehmen verpflichtet sind, das besagte Verzeichnis zu führen.

1.2.1 Begriffsklärung: Verarbeitungstätigkeiten und Bearbeitungstätigkeiten

In der DSGVO wird von einem ‚Verzeichnis von Verarbeitungstätigkeiten' gesprochen, im E-DSG wird das Verzeichnis mit dem gleichen Zweck jedoch als ‚Verzeichnis der Bearbeitungstätigkeiten' bezeichnet.

Im Sinne der DSGVO versteht der Gesetzgeber unter dem Ausdruck ‚Verarbeitung' folgendes:

> «jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung»

(DSGVO, Art. 4)

Anstelle des Begriffs des ‚Verarbeitens' verwendet das Schweizer Recht den Begriff des ‚Bearbeitens'. Aus Praktikabilitätsgründen wird darauf verzichtet, das Schweizer Recht in dieser Hinsicht anzupassen, zumal inhaltlich kein Unterschied besteht (E-DSG, Art. 4). Daraus geht hervor, dass zwischen den beiden Bezeichnungen nicht unterschieden werden muss. In der Folge wird deshalb der Begriff ‚Verzeichnis von Verarbeitungstätigkeiten' verwendet, der als ‚VV' abgekürzt wird. Daraus folgt ebenfalls, dass der Ausdruck ‚Auftragsverarbeiter' (DSGVO, Art. 4) dem Ausdruck ‚Auftragsbearbeiter' (E-DSG, Art. 4) weitgehend entspricht. Deshalb wird in allen folgenden Ausführungen der Begriff ‚Auftragsverarbeiter' verwendet.

1.2.2 Verpflichtete Unternehmen

Von den in DGSVO, Artikel 30 genannten Pflichten sind Unternehmen ausgenommen, die weniger als 250 Mitarbeitende beschäftigen. Dies ist unter der Bedingung der Fall, dass die von ihnen vorgenommene Verarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nur gelegentlich erfolgt sowie keine

besonderen Datenkategorien enthält (DSGVO, Art. 30, Abs. 5). Darunter fallen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszughörigkeit hervorgehen. Ebenfalls zählen hierzu die Verarbeitung von genetischen und biometrischen Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung (DSGVO, Art. 9, Abs. 1). Weiter sind Unternehmen, die personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten verarbeiten, unabhängig von ihrer Grösse dazu verpflichtet, ein Verzeichnis von Verarbeitungstätigkeiten zu führen (DSGVO, Art. 30, Abs. 5). Eine Befreiung von der Pflicht zum Führen eines VV wird es damit nur für wenige Unternehmen geben, insbesondere, da eine «gelegentliche Verarbeitung» unterschiedlich ausgelegt werden kann (Datenschutzbeauftragter INFO, 2016b).

Der aktuelle Entwurf des neuen Schweizerischen Datenschutzgesetzes sieht Ausnahmen für Unternehmen vor, die weniger als 50 Mitarbeitende beschäftigen. Jede Ausnahme muss vom Bundesrat bewilligt werden. Dabei wird neben der Grösse des Unternehmens berücksichtigt, welche Risiken von der Datenbearbeitung ausgehen (E-DSG, Art. 11, Abs. 5).

Faktisch bedeutet dies, dass mit dem Inkrafttreten beziehungsweise der Gültigkeit des neuen Schweizerischen Datenschutzgesetzes (DSG) grundsätzlich alle Schweizer Unternehmen verpflichtet sind, ein Verzeichnis von Verarbeitungstätigkeiten beziehungsweise Bearbeitungstätigkeiten zu führen. Ein Termin ist gemäss den Erläuterungen im E-DSG (2017, S. 238) noch nicht bekannt. Aktuell wir davon ausgegangen, dass das E-DSG im besten Fall Anfang 2019 rechtskräftig wird und danach nach einer Übergangsfrist von zwei Jahren Gültigkeit erlangt (Israel & Carli, 2018).

1.2.3 Umsetzung des Verzeichnisses von Verarbeitungstätigkeiten

Da das VV als zentraler und fundamentaler Teil bei der Umsetzung der neuen gesetzlichen Anforderungen gilt, stehen die betroffenen Unternehmen vor der Herausforderung, dieses umzusetzen. Umfragen zeigen, dass bei den Unternehmen im Bereich des VV Handlungsbedarf besteht. So haben gemäss einer Umfrage des Verbands der Internetwirtschaft (ECO Verband) (2018) unter 500 Unternehmen, wovon 335 mehr als 500 Mitarbeitende beschäftigen, erst sechs Prozent ein VV umgesetzt. Etwas entschärft wird dieses Umfrageergebnis durch eine Umfrage des Bitcoms (2017) unter mehr als 500 Unterneh-

men, wonach 14 Prozent ein VV umgesetzt haben. Ausserdem nennen in derselben Umfrage über 43 Prozent der Unternehmen die «Rechtsunsicherheit» neben dem «schwer abschätzbaren Umsetzungsaufwand» als eine der grössten Herausforderungen. Eine Umfrage von Deloitte (2017) unter mehr als 250 Unternehmen in Österreich ergab, dass knapp die Hälfte unzureichend auf die Anforderungen der DSGVO vorbereitet ist.

Aus den Experteninterviews geht hervor, dass auch vielen Schweizer Unternehmen die Wichtigkeit des Themas noch nicht bewusst ist (Interview A). Bewusstsein zu schaffen ist ein zentraler Aspekt und Voraussetzung für die Umsetzung, ebenso die Überzeugung des Managements (Interview B). Um dies zu erreichen, bedarf es zunächst des Verständnisses, worum es effektiv geht (Interview A und B). Dazu gehört das Finden einer gemeinsamen Sprache der operativen Bereiche, der Zuständigen von rechtlicher Seite und der Zuständigen seitens der Informatik. Da die neuen Datenschutzgesetze in hohem Masse auf Informatik bezogen sind, gilt dies insbesondere für die Zuständigen von rechtlicher Seite und die Zuständigen seitens der Informatik. Einerseits gilt es, Verständnis für Informationssysteme zu schaffen, und anderseits, ein Verständnis für die Rechtssprache zu erlangen. Teilweise geht es dabei um zunächst einfach klingende Begriffe wie ‚personenbezogene Daten', die sich bei näherer Betrachtung als komplexer herausstellen (Interview A). Ausserdem ist noch keine Rechtsprechung bekannt, die Hinweise auf die exakte Bedeutung dieser Begriffe geben könnte (Interview C).

Gelingt es, das Bewusstsein zu schaffen, so gilt es zu identifizieren, wo sich die relevanten Daten im Unternehmen befinden (Interview C). Dies gestaltet sich komplex, da beinahe alle Geschäftsprozesse betroffen sind (Interview A). Dabei besteht die Herausforderung darin, den Fokus auf das Wesentliche zu legen (Interview C). Eine weitere Herausforderung entsteht aufgrund heterogener Unternehmensarchitekturen, in denen die Verarbeitungen durchgeführt werden.

1.3 Zielsetzung

Aus der Problemstellung geht hervor, dass für die Umsetzung der DSGVO als einer der ersten Schritte die Umsetzung des VV in Angriff genommen werden sollte. Nachdem erkannt wurde, dass das eigene Unternehmen ein VV umsetzen muss, gilt es, Bewusstsein zu schaffen, indem ein Verständnis für die relevanten Begriffe, Bestandteile und Zusammenhänge erreicht wird.

Bekräftigt durch aktuelle Umfragen sowie die Experteninterviews zeichnet sich in diesem Bereich eine Lücke ab. Die vorliegende Masterthesis hat deshalb zum Ziel, die relevanten Begriffe zu erläutern und die Bestandteile des VV aufzuzeigen, um es Unternehmen zu erleichtern, Verarbeitungen und Bestände von personenbezogenen Daten innerhalb des Unternehmens zu erfassen. Ein Verzeichnis ist eine «nach einem bestimmten System geordnete schriftliche Aufstellung mehrerer unter einem Gesichtspunkt zusammengehörender Dinge o. Ä.» (Duden) und somit ein sehr formales Konstrukt. Dies gilt auch für das VV, weshalb die Aufbereitung der Thematik in Form eines formalen Modells erfolgt.

Zu diesem Zweck werden folgende Forschungsfragen definiert:

Q: Wie lassen sich bestehende Verarbeitungen und Bestände in Unternehmen mit einem Modell beschreiben, das den gesetzlichen Vorgaben und spezifischen Anforderungen entspricht?

Q1: Wie kann ein gemeinsames Verständnis für die Anforderungen aller Beteiligten geschaffen werden?

Q2: Wie stehen die Verarbeitungen und Bestände im Zusammenhang?

1.4 Abgrenzung

Im formalen Modell beziehungsweise in den formalen Modellen (Erläuterung dazu siehe Kapitel 5.4) werden nur Bestandteile der Gesetze, die sich direkt auf das VV beziehen, berücksichtigt. Daraus folgt, dass Zusammenhänge, die sich aus den Ausführungen teilweise ergeben, sich jedoch nicht direkt auf das VV beziehen, nicht in den Modellen enthalten sind.

1.5 Aufbau

Aus der folgenden Abbildung 1 wird der Aufbau der vorliegenden Arbeit ersichtlich. Die Arbeit gliedert sich in sieben Kapitel. Nach der Einleitung erfolgen nun im Kapitel 2 die Erläuterungen zum Forschungsdesign, wobei der zugrundeliegende Forschungsprozess spezifiziert wird und die verwendeten Methoden erläutert werden. Im Kapitel 3 werden daraufhin bekannte Ansätze und Konzepte erläutert, die im Zusammenhang mit der Thematik stehen.

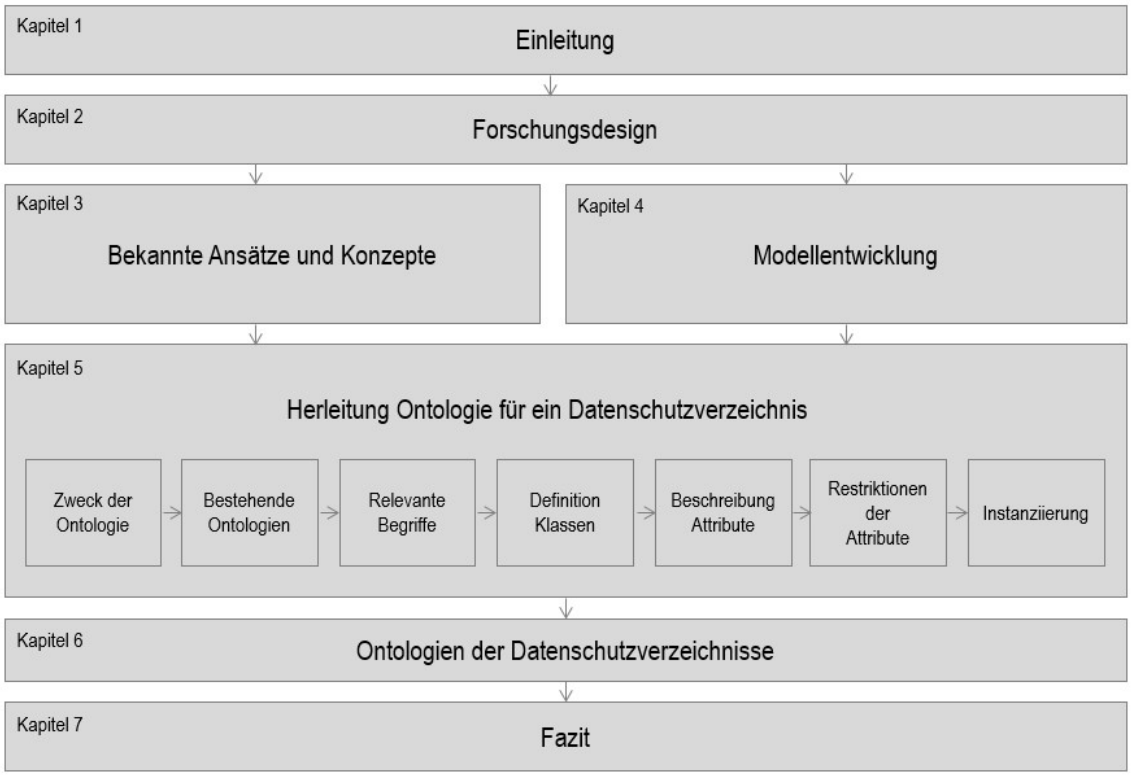


Abbildung 1: Aufbau der Arbeit

Unabhängig davon erfolgen im Kapitel 4 Ausführungen zu Grundlagen der Modellentwicklung sowie zur Methodologie, die für die Herleitung der Ontologie verwendet wird, sowie die Spezifizierung der später verwendeten UML-Elemente. Kapitel 5 bildet den Hauptteil der Arbeit. In diesem Kapitel erfolgen die Erläuterungen zur Herleitung der Ontologie, die darauf in Kapitel 6 präsentiert wird. Abschliessend folgt im Kapitel 7 das Fazit zu den gewonnenen Erkenntnissen.

2 Forschungsdesign

In der Wirtschaftsinformatik kommen hauptsächlich die Forschungsparadigmen ‚Behavioral Science' und ‚Design Science' zur Anwendung. Das Paradigma der ‚Behavioral Science' versucht, Theorien zu entwickeln, die menschliches und organisatorisches Verhalten erklären oder vorhersagen. Das Paradigma der «Desing Science» verfolgt den Ansatz, Probleme der Wirtschaftsinformatik mit der Entwicklung von innovativen Artefakten anzugehen (Hevner, March, Park, & Ram, 2004).

Die in Kapitel 1.3 formulierten Forschungsfragen legen einen «Design Science» Forschungsansatz nahe. Hevner et al. (2004) beschreiben mit dem «Information Systems Research Framework» ein Vorgehensmodell für das Bilden von Artefakten, die sowohl praktische Relevanz (Relevance) als auch Relevanz für die Forschung (Rigor) haben (vgl. Anhang i). Der Artikel «Design Science in Information Systems Research» (Hevner et al., 2004) definiert Prinzipien, Ziele und Regeln, die als Orientierungshilfe während dem Forschungsprozess dienen (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007).

Peffers et al. (2007) beschreiben darauf basierend mit der «Design Science Research Methodology (DSRM)» einen generischen Forschungsprozess für den «Design Science» Forschungsansatz (vgl. Anhang ii). Er berücksichtigt implizit die Design Science Research Guidelines von Hevner (2004) (vgl. Anhang iii).

2.1 Forschungsprozess

Der Forschungsprozess der geplanten Masterthesis leitet sich aus dem von Peffers et al. (2007) beschriebenen generischen Forschungsprozess für ‚Design Science' ab. Der definierte Forschungsprozess besteht aus fünf Phasen (vgl. Abbildung 2), die jeweils mit einem Zwischenziel abgeschlossen werden. Das Vorgehen in den Forschungsphasen wird im Folgenden erläutert.

Phase 1 – Problem definieren beinhaltet die Formulierung der Ausgangslage (vgl. Kapitel 1), die anhand einer Literaturanalyse ermittelt wird. Dabei stehen die aktuellen Gesetzesanpassungen im Fokus. Zudem wird das Problem, das sich aus den Gesetzesanpassungen ergibt, formuliert und daraus die Forschungsfragen abgeleitet (vgl. Kapitel 1.2 & 1.3).

Darauf wird die vermutete Forschungslücke bestätigt. Dies geschieht anhand einer Literaturanalyse, in der relevante Gesetze und bestehende Konzepte betrachtet werden. Nach

Abschluss der Phase 1 wird das erste Zwischenziel erreicht und somit die Forschungslücke definiert.

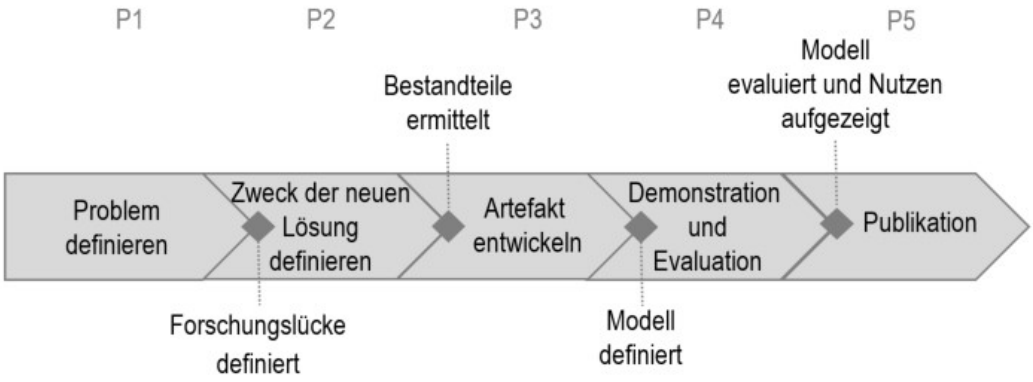


Abbildung 2: Forschungsprozess (in Anlehnung an Peffers et al., 2007, S. 54)

Ist die Forschungslücke definiert, beginnt **Phase 2 – Zweck der neuen Lösung definieren**. In dieser Phase wird definiert, was ein besseres Modell beinhalten müsste. Die Identifikation der fehlenden Bestandteile in möglicherweise bestehenden Modellen geschieht anhand einer Literaturanalyse. Am Ende der Phase 2 sind die Bestandteile für das neue Modell ermittelt.

In **Phase 3 – Artefakt entwickeln** ist die Erstellung des Modells zur Abbildung bestehender Vorgehen und Bestände in einem Unternehmen vorgesehen. Das Modell wird in Form einer Ontologie in der Unified Modeling Language (UML) dargestellt.

Ist eine erste Version des Modells erstellt, so wird das Modell durch Experteninterviews in einem iterativen Prozess evaluiert und der Nutzen anhand eines Prototyps für ein VV in Form einer Access-Datenbank aufgezeigt (**Phase 4 – Demonstration und Evaluation**).

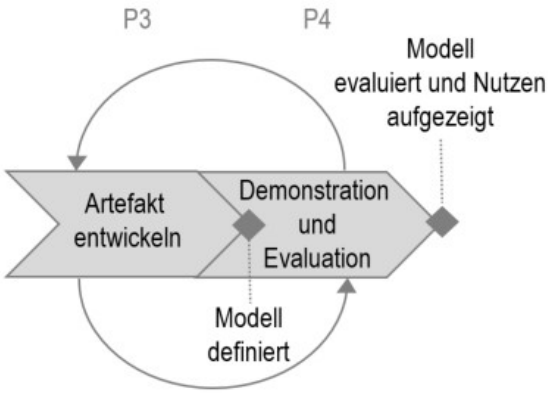


Abbildung 3: Iterative Evaluationsphase – Ausschnitt aus dem Forschungsprozess (vgl. Abbildung 2)

Nach Abschluss der Phasen 3 und 4 ist ein Modell vorhanden, das die Bestandteile eines VV, das den gesetzlichen sowie spezifischen Anforderungen entspricht, verdeutlicht.

Phase 5 – Publikation sieht die Veröffentlichung der gewonnenen Erkenntnisse vor. Guideline 7 (Hevner et al., 2004) besagt, dass die Erkenntnisse sowohl einem technologie-orientierten als auch einem management-orientierten Publikum präsentiert werden müssen. Bislang ist, neben der vorliegenden Masterthesis, eine Publikation vorgesehen, die die gewonnenen Erkenntnisse für ein management-orientiertes Publikum zusammenfasst.

2.2 Forschungsmethoden

Die während des Forschungsprozesses angewendeten Forschungsmethoden werden aus Tabelle 1 ersichtlich. Ausserdem zeigt Tabelle 1 auf, in welchen Phasen des Forschungsprozesses die Design Science Research Guidlines berücksichtigt werden. Die Anwendung der Methoden wird in den folgenden Abschnitten beschrieben.

Phase	**Methode (n)**	**DSR Guidelines**
Phase 1: Problem definieren	Literaturanalyse	2, 6
Phase 2: Ziele der neuen Lösung definieren	Literaturanalyse	-
Phase 3: Artefakt entwickeln	Ontologie-/Modellbildung	1, 4, 5
Phase 4: Demonstration und Evaluation	Experteninterviews, Ontologie-/Modellbildung, Instanziierung	3, 5
Phase 5: Publikation	-	7

Tabelle 1: Forschungsmethoden

2.2.1 Vorgehen Literaturanalyse

Die geplante Masterthesis ist im Themenbereich der DSGVO und insbesondere dem Artikel 30 DSGVO – Verzeichnis von Verarbeitungstätigkeiten – zu verorten. Mit folgendem Rechercheprozess wird die relevante Literatur identifiziert:

1) Ermittlung von relevanten Begriffen mit Hilfe von Einstiegsliteratur und dem zugrundeliegenden Gesetz

2) Identifikation der relevanten Literatur über Datenbankrecherchen

3) Ergänzende Quellen berücksichtigen: Webseiten von Softwareherstellern, Consulting-Unternehmen und Verbänden

Die aus der Einstiegsliteratur und dem zugrundeliegenden Gesetz identifizierten Begriffe haben bei der Datenbankrecherche zu den in Abbildung 4 ersichtlichen Ergebnissen geführt. Die Datenbasis hierzu ist dem Anhang vi zu entnehmen. Der Literaturrechercheprozess orientiert sich am Vorgehen von Eberle (2017, S. 3ff). Wie Abbildung 4 zeigt, wurden im Themenbereich der DSGVO schon tausende Publikationen veröffentlicht. Die Menge an Publikationen zum VV ist verglichen dazu sehr klein.

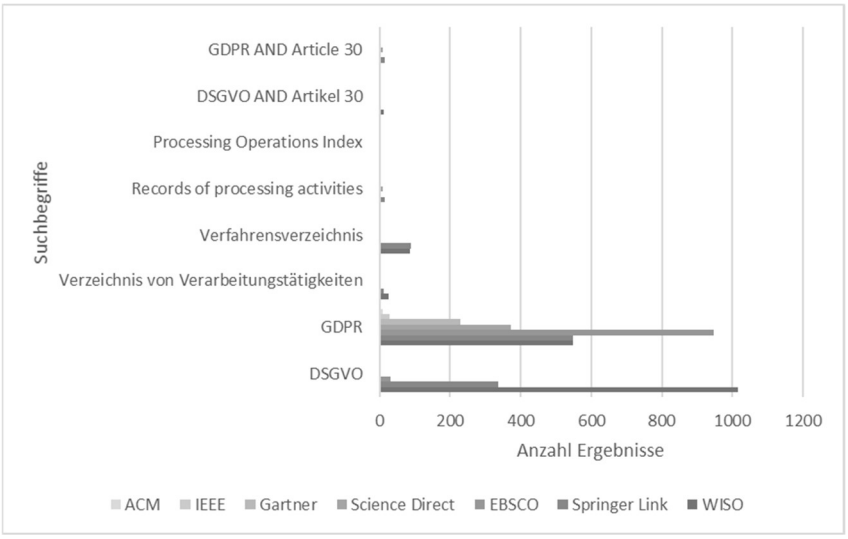


Abbildung 4: Ergebnisse der Datenbankrecherche

2.2.2 Experteninterviews

Die Evaluation des entwickelten Artefakts erfolgt anhand systematisierender Experten-Interviews. Diese Methode wird eingesetzt, um im Rahmen eines Forschungsprojekts bereits dokumentiertes Wissen zu vertiefen und weitere Zusammenhänge herauszuarbeiten. Die interviewende Person nimmt die Rolle des Experten eines anderen Fachgebiets ein (Kruse, 2015, S. 167).

Die Interviewpartner und -partnerinnen wurden über Organisationen angefragt oder direkt recherchiert und aufgrund ihrer Erfahrung auf dem Fachgebiet (vgl. Tabelle 2) ausgewählt (Kruse, 2015, S. 250ff). Aktuell gibt es auf dem Fachgebiet erst wenige Experten und Expertinnen, daher wurde nach jedem Interview reflektiert, ob ein weiteres Interview zusätzliche Erkenntnisse bringen könnte. Nach drei durchgeführten Interviews hat sich gezeigt, dass noch viele Unklarheiten bestehen und weitere Interviews nur wenige zusätz-

liche Erkenntnisse bringen würden. Neben der Erfahrung auf dem Fachgebiet ist aus Tabelle 2 die Rolle der Interviewpartner und -partnerinnen in den jeweiligen Unternehmen ersichtlich. Ausserdem ist ein Verweis definiert, der in der Folge für die Kennzeichnung von Aussagen aus den Interviews verwendet wird.

Interviewpartner/in	**Erfahrung auf dem Fachgebiet**	**Verweis**
Rechtsanwalt in einer international vernetzten Schweizer Kanzlei	Der Experte beschäftigt sich seit Mai 2016 mit der DSGVO und hat im Rahmen seiner Beratungstätigkeit verschiedene Firmen bei der Umsetzung von VV unterstützt. Dabei hat er schon verschiedene Ausprägungen von VV gesehen. Erste Erfahrungen mit dem Datenschutzrecht hat er 2011 gemacht (Interview A).	Interview A
Leitende Rechtsanwältin eines global tätigen Industrie Unternehmens	Die Expertin beschäftigt sich seit Mai 2016 mit der DSGVO und befasst sich zusammen mit vier anderen Juristen im Unternehmen seit sechs Monaten mit der Umsetzung der Verordnung und dabei auch intensiv mit dem VV (Interview B).	Interview B
Rechtsanwalt in einem global führenden Wirtschaftsprüfungs- und Beratungsunternehmen	Der Experte befasst sich im Rahmen seiner Tätigkeit als Berater im Bereich Datenschutzrecht seit 2017 mit der DSGVO (Interview C).	Interview C

Tabelle 2: Übersicht Interviewpartner/innen

2.2.3 Ontologie-/Modellbildung

Für die Bildung von Ontologien werden in der Literatur verschiedene Methodologien beschrieben. In der vorliegenden Masterthesis wird auf eine prozessbasierte Entwicklung von Ontologien gesetzt. Dazu werden die Methodologien von Uschold und King (1995, S. 2) sowie Noy und McGuiness (2001, S. 4ff) berücksichtigt. Das Vorgehen nach diesen Methodologien bezieht sich auf die Phasen zwei bis vier des Forschungsprozesses (vgl. Kapitel 4.2).

3 Bekannte Ansätze und Konzepte

Bevor mit der Entwicklung des Modells begonnen wurde, wurden bereits bekannte Konzepte von Datenschutzverzeichnissen sowie Ansätze zum VV betrachtet. Die Erkenntnisse hieraus werden im Folgenden erläutert.

3.1 Bisher bekannte Datenschutzverzeichnisse

Die bisherige EU-Gesetzgebung legt anstelle des VV eine Meldepflicht von Verarbeitungstätigkeiten im Zusammenhang mit personenbezogenen Daten fest. Zusätzliche Bestimmungen sind den Mitgliedstaaten überlassen (Richtlinie 95/46/EG, Art. 18). Länder wie Italien, Österreich und Schweden haben die Meldepflicht in ihre nationalen Gesetze übernommen und spezifiziert. Von zusätzlichen Bestimmungen sehen sie ab (activeMind, o. J.). Ähnlich gestaltet sich die Situation in der Schweiz. Für Bundesorgane besteht eine Meldepflicht für Datensammlungen, die personenbezogene Daten enthalten. Private Unternehmen müssen ein Register der Datensammlungen führen, das über das Internet zugänglich ist (DSG, Art 11a). Vorgaben zu den Datensammlungen sind im DSG nicht enthalten.

Anders ist die Situation in Deutschland. Das BDSG (Art. 4c) schreibt ein internes und ein öffentliches Verfahrensverzeichnis vor. Das interne Verfahrensverzeichnis dient dazu, eine betriebsinterne Selbstkontrolle zu ermöglichen (Datenschutzbeauftragter INFO, o. J.). Es erfordert ähnliche Angaben, wie sie die DSGVO und das E-DSG beschreiben (vgl. Anhang v). Das öffentliche Verfahrensverzeichnis soll nach aussen Transparenz über die Datenverarbeitungsvorgänge schaffen. Es besteht aus einer reduzierten Aufstellung von Angaben (Datenschutzbeauftragter INFO, o. J.).

Ein weiteres Konzept eines Datenschutzverzeichnisses beschreibt die International Organization for Standardisation (ISO; 2017) in der Norm ISO27001, die Anforderungen an Informationstechnik-Sicherheitsverfahren und Informationssicherheitssysteme in Unternehmen auflistet. Sie sieht vor, dass die Werte, die mit Informationen in Zusammenhang stehen, durch die Organisation identifiziert und inventarisiert werden. Ausserdem sind Verantwortlichkeiten zum Schutz dieser Werte sowie zuständige Personen für die Werte, die im Inventar beziehungsweise Verzeichnis geführt werden, festzulegen. Aus den Erläuterungen zur Norm sind die detaillierten Anforderungen nicht klar ersichtlich. Eindeutiger sind die Ausführungen, die aus dem Regulativ der Datenschutzmanagementsystem-Zertifizierung GoodPriv@cy der Schweizerischen Vereinigung für Qualitäts- und Management-Systeme (SQS) hervorgehen. Die Zertifizierung richtet sich nach der Norm ISO27001. Die geforderten Angaben sind ebenfalls mit den Anforderungen an ein Datenschutzverzeichnis der DSGVO und des E-DSG vergleichbar. Details hierzu sind dem Anhang v zu entnehmen.

3.2 Ansätze zum Verzeichnis von Verarbeitungstätigkeiten

Nach DSGVO (Art. 30) ist es möglich, das Verzeichnis in elektronischer oder nicht-elektronischer Form zu führen. Im E-DSG ist in der Beschreibung zum Artikel 11 – Verzeichnis der Bearbeitungstätigkeiten kein analoger Vermerk zu finden. Sonstige Vorgaben zur Umsetzung des VV sind in den Gesetzen nicht vorhanden.

Mit der Umsetzung des VV beschäftigen sich verschiedene Verbände und Datenschutzexperten. Die wichtigsten Publikationen stammen aus Deutschland, vom Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) (2017), von der Gesellschaft für Datenschutz und Datensicherheit (GDD) (2017), von der Datenschutzkonferenz (DSK) (2018) sowie von Bitcom (2017). Eine weitere wichtige Publikation hat ihre Herkunft in Österreich und wurde von den WKO veröffentlicht (2018b). Auch die belgische Commission for the Protection of Privacy (CPP) (Englische Bezeichnung) (2017) hat Informationen zum VV sowie eine Excel-Mustervorlage in Niederländisch und Französisch herausgegeben. Die britische Kanzlei Fieldfisher (2017) hat dazu eine inoffizielle englische Übersetzung publiziert.

Markus Schäffter, Professor für Datenschutz und Informationssicherheit an der Hochschule Ulm, hat einen Ratgeber zum Thema ‚VV für Datenschutzexperten' verfasst. Der Ratgeber beinhaltet allgemeine Erläuterungen sowie Mustervorlagen. Die publizierten Mustervorlagen dienen der Erfassung von Verarbeitungstätigkeiten aus Sicht von Unternehmen sowie aus Sicht von Auftragsverarbeitern. Die Mustervorlagen sehen grösstenteils die gesetzlichen Anforderungen vor und beinhalten Beispiele hierzu. Die Informationsdokumente enthalten Beschreibungen zu den Bestandteilen des VV, die Zusammenhänge werden jedoch nicht oder, wie in der Publikation des Bitcoms (2017) und Schäffter (2017), nur ansatzweise aufgezeigt. Eine Beurteilung der Inhalte der Publikationen der Verbände geht aus Tabelle 3 hervor. Die Beurteilung bestätigt die Lücke im Bereich der Zusammenhänge der Bestandteile des VV.

Herausgeber	Art des/der Dokuments/-e	Begriffserklärungen	Gesetzlich vorgeschriebene Bestandteile enthalten/erläutert	Zusammenhänge Bestandteile aufgezeigt
Bitcom (2017)	Allgemeine Information inkl. Mustervorlage VVU	**x**	**x**	**(x)**
BvD (2017)	Mustervorlagen VVU, VVA und TOM		**x**	
GDD (2017)	Allgemeine Information inkl. Mustervorlagen VVU und VVA	**x**	**x**	
WKO (2018b)	Begriffsbestimmungen, Mustervorlagen VVU, VVA sowie Beispiele VVU und VVA	**x**	**x**	
DSK (2018)	Allgemeine Informationen	**x**	**x**	
CPP (2017)	Allgemeine Informationen, Mustervorlage VVU	**(x)**	**(x)**	
Markus Schäffter (2017)	Allgemeine Informationen, Mustervorlage VVU	**x**	**x**	**(x)**
Legende: leer: nicht vorhanden, (x): teilweise vorhanden, x: vorhanden				

Tabelle 3: Beurteilung Publikationen Verbände

Weitere Ansätze stammen von Softwareherstellern, die mit Lösungen werben, die beim Führen des VV unterstützend wirken sollen. Dies sind zum einen deutsche Anbieter, die bisher auf das Führen des im BDSG definierten Verfahrensverzeichnisses spezialisiert waren. Ihre Softwarelösungen bestehen vereinfacht ausgedrückt aus einer Datenbank, die über eine Eingabemaske mit den gesetzlich vorgegebenen Angaben befüllt werden kann (2B Advice GmbH - Deutsch - Datenschutzsoftware, o. J.; Deichmann-Fuchs - Business Solutions, o. J.). Zum anderen sind dies Anbieter von umfassenden Datenschutzmanagementlösungen, die das VV in ihre Suite integrieren. Bekannte Anbieter sind Niymity, OneTrust, BigID, Collibra, SecuPi oder auch Global IDs (Gartner, 2017). Weitere Softwarehersteller bieten Lösungen an, die bei der Identifikation von vorhandenen Daten unterstützen (Blodon James, o. J.; Varonis, o. J.).

Die genannten Softwarelösungen helfen Unternehmen zwar beim Führen des VV und der Identifikation von Daten, jedoch nicht dabei, die geforderten Bestandteile zu verstehen. Datenmodelle, die die Zusammenhänge aufzeigen, die als Basis für die Entwicklung der Software dienen, konnten im Rahmen der Untersuchung nicht identifiziert werden. Aus einem Kurzinterview mit Christian Sonntag (2018), einem Studenten, der sich im Rahmen seiner Bachelorarbeit mit dem Themenbereich ‚Software für das DSGVO-VV' auseinandergesetzt hat, wird jedoch deutlich, dass es Anwendungen gibt, die alle gesetzlich geforderten Bestandteile berücksichtigen. Ob diese aber im korrekten Zusammenhang zueinander stehen, ist nicht geklärt. Aus Sonntags Untersuchung wird ausserdem offensichtlich, dass bei den meisten Softwareherstellern der Anwendungsfall eines VV für unternehmenseigene Verarbeitungen im Fokus steht. Daraus folgt, dass dem VV für Auftragsverarbeiter weniger Beachtung geschenkt wird.

Aus den Experteninterviews geht hervor, dass eine Anbindung des VV an bestehende Systeme wie das Customer-Relationship-Management (CRM) für die Einhaltung der gesetzlichen Vorschriften hilfreich wäre (Interview A). Einen Ansatz, der die durchgängige Dokumentation, Durchsetzung und Kontrolle von Datenschutzanforderungen gewährleisten soll, beschreiben Anke, Berning, Schmidt und Zinke (2016). Die Autoren haben ein Informationsmodell entwickelt, das die integrierte Betrachtung von Datenschutzzielen und der Anwendungssystemlandschaft aufzeigt (vgl. Anke et al., 2016, S. 72). Die Idee ist ein modulares System, das aus einer Modellierungskomponente besteht, die der Erfassung des Ist-Zustands der Unternehmensarchitektur dient sowie mit Informationen zum Datenschutz annotiert werden kann. Weiter ist im System eine Analysekomponente vorgesehen, die die Konfiguration der Systeme analysieren soll und mit den vorgegebenen Datenschutzanforderungen abgleicht. Ein dritter Bestandteil ist eine Steuerungskomponente, die mit Informationen der Analysekomponente den Soll-Zustand wieder herstellen soll, sofern Abweichungen bestehen (Anke et al., 2016, S. 76).

Das Modell zeigt ansatzweise die Verbindung zu den Bestandteilen des VV auf (Anke et al., 2016, S. 72). Bereits aus dem publizierten Ausschnitt aus dem Prototyp der Modellierungskomponente wird jedoch ersichtlich, dass nicht alle gesetzlichen Erfordernisse berücksichtigt werden. So fehlen beispielsweise Datenkategorien komplett (Anke et al., 2016, S. 79). Anke et al. (2016) scheinen einen guten Ansatz zu verfolgen, jedoch müsste das zugrundeliegende Datenmodell noch optimiert werden. Genau an diesem Punkt setzt die vorliegende Masterthesis an.

4 Modellentwicklung

4.1 Grundlagen Modellbildung und Ontologie

Ein Modell ist ein Abbild, das abstrahiert und im Hinblick auf einen bestimmten Verwendungszweck geschaffen wird (Stachowiak, 1973, S. 131f). Es wird unterschieden zwischen deskriptiver und präskriptiver Modellbildung. Die deskriptive Modellbildung orientiert sich an einem existierenden Original oder dient der Modellierung eines zukünftigen, jedoch nicht gestaltbaren Originals. Die präskriptive Modellbildung dient hingegen der Erstellung eines zu schaffenden, gestaltbaren Originals (Ludewig, 2003, S. 8). Das in der vorliegenden Masterthesis entwickelte Modell basiert sowohl auf dem Ansatz der deskriptiven als auch auf dem Ansatz der präskriptiven Modellbildung. Eine Form von Modellen sind Ontologien, formale Wissensmodelle mit expliziten Spezifikationen (Guarino, 1998, S. 4). Im Fachbereich der Informatik werden diese auch als «System von Informationen mit logischen Relationen» (Duden) definiert. Die Erstellung eines formalen Modells setzt formale Methoden voraus, deshalb wird in dieser Masterthesis, wie in Kapitel 2.2.3 erwähnt, auf die Methodologien von Uschold und King (1995, S. 2ff) sowie Noy und McGuiness (2001, S. 4ff) gesetzt. Die verwendete Methodologie orientiert sich hauptsächlich an dem Ansatz von Noy und McGuiness (2001, S. 4ff), ergänzt mit Aspekten von Uschold und King (1995, S. 2ff).

4.2 Methodologie zur Bildung der Ontologie

Abbildung 5 zeigt die Schritte der Methodologie von Noy und McGuiness (2001, S. 4ff), nach der bei der Entwicklung der Ontologie vorgegangen wurde. Es handelt sich um einen iterativen Prozess, bei dem die Ergebnisse jedes Schrittes in nachfolgende sowie vorhergehende Schritte einfliessen können. Im Kapitel 5 wird jeweils auf die Schritte verwiesen, die zu dem dokumentierten Ergebnis geführt haben.

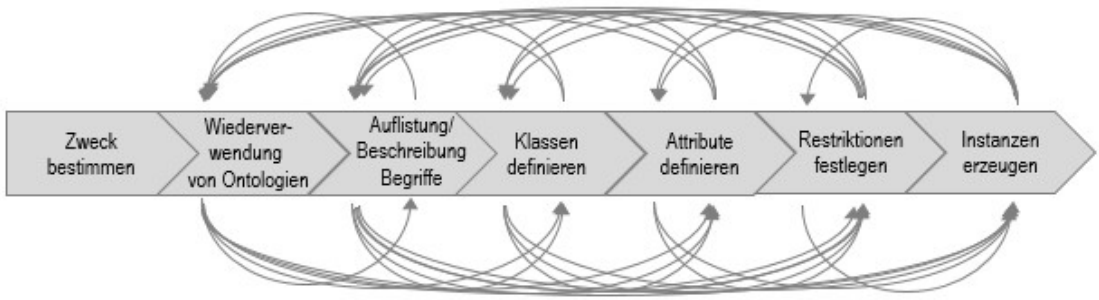


Abbildung 5: Methodologie Bildung Ontologie (in Anlehnung an Noy & McGuinness, 2001, S. 4ff)

4.3 UML-Klassendiagramm

Uschold und King (1995, S. 2ff) erwähnen in ihrer Methodologie zur Bildung von Ontologien, dass für die Erstellung einer Ontologie eine formale Sprache festgelegt werden solle. Im Hinblick auf spätere Verwendungszwecke wird die gebildete Ontologie in der aktuellen UML-Version 2.5.1 in Form eines Klassendiagramms abgebildet. Das Klassendiagramm ist ein Strukturdiagramm, das der Darstellung von Klassen, Schnittstellen und deren Beziehungen dient. Nach UML bestehen die Klassen aus einer Bezeichnung, Attributen und Operatoren. Eine Klasse beschreibt eine gemeinsame Struktur und ein gemeinsames Verhalten von Objekten. Attribute sind strukturelle Merkmale einer Klasse und spezifizieren einen Teil der Struktur von Objekten. Operatoren sind Verhaltensmerkmale, die bestimmen, wie ein Verhalten aufgerufen wird.

Die Darstellung der Klassen in der vorliegenden Ontologie ist in der nachfolgenden Abbildung 6 ersichtlich. Das ‚+' vor den Attributen steht für ‚public', was bedeutet, dass auf das Attribut uneingeschränkt zugegriffen werden kann. Im Gegensatz dazu sind Attribute, die mit ‚-' für ‚private' bezeichnet werden, nur innerhalb der Klasse sichtbar (Object Managment Group (OMG), 2017). Da die Sichtbarkeit für die Ontologie vorerst nicht von grosser Bedeutung ist, werden alle Attribute mit ‚+' für ‚public' gekennzeichnet, was alle Optionen für eine weitere Verwendung noch offen lässt. In der verwendeten vereinfachten Darstellung der Klassen wird auf Operatoren verzichtet, da diese zunächst nicht relevant sind.

Abbildung 6: Darstellung der Klassen in der Ontologie

Die UML beschreibt verschiedene Beziehungstypen, die zwischen Klassen bestehen können (Object Managment Group (OMG), 2017). Tabelle 4 zeigt die in der vorliegenden Ontologie verwendeten Beziehungstypen auf. Für die Bezeichnung der Assoziationen werden die Dreiecke ‚<' und ‚>' verwendet, die die Leserichtung angeben.

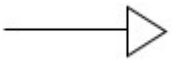
Beziehungstyp	Beschreibung
	Die ‚Assoziation' beschreibt eine Beziehung zwischen zwei Klassen.
	Die ‚Generalisierung' ist eine gerichtete Beziehung zwischen einer generellen und einer spezialisierten Klasse (zum Beispiel Baum – Eiche).
	Die ‚Komposition' bezeichnet eine Beziehung zwischen dem Ganzen und seinen Teilen, bei der die Teile nicht ohne das Ganze bestehen können (zum Beispiel Haus – Zimmer).

Tabelle 4: Erläuterung verwendete Beziehungstypen

Die Beziehungen zwischen den Klassen werden mit Multiplizitäten ergänzt. Multiplizitäten bestehen aus einer unteren und oberen Schranke. Entspricht die untere der oberen Schranke, wird nur ein Wert angegeben (Object Managment Group (OMG), 2017). In der vorliegenden Ontologie werden die in Tabelle 5 ersichtlichen Multiplizitäten verwendet.

Multiplizität	Beschreibung Das angrenzende Objekt kann…
0..n	… nicht oder bis zu einer definierten Anzahl an Malen enthalten sein.
0..*	… nicht oder unendliche viele Male enthalten sein.
1	… genau einmal enthalten sein.
1..n	… einmal bis zu einer definierten Anzahl an Malen enthalten sein.
1..*	… einmal bis unendliche viele Male enthalten sein.

Tabelle 5: Erläuterung verwendete Multipilizitäten

5 Herleitung der Ontologie für ein Datenschutzverzeichnis

In diesem Kapitel erfolgen die Erläuterungen zur Herleitung der Ontologie für ein Datenschutzverzeichnis nach den neuen gesetzlichen Vorgaben. Die Referenzen beziehen sich dabei immer auf die DSGVO, da das Schweizer Gesetz noch nicht in Kraft getreten ist und die Referenzen daher einerseits nicht exakt definiert werden können und sich anderseits möglicherweise noch etwas ändern wird. Wie bereits erläutert, werden die Anforderungen zum Verzeichnis sehr ähnlich ausfallen. Die nun folgenden Absätze sind nach dem Vorgehen gemäss der Methodologie von Noy und McGuinnes (2001, S. 4ff) gegliedert.

5.1 Zweck der Ontologie

Die Ontologie hat den Zweck, die Bestandteile und Zusammenhänge eines VV aufzuzeigen, wie es aktuell in der DSGVO (Art. 30) und bald auch in dem neuen Schweizer Datenschutzgesetz (E-DSG, Art. 10) vorgesehen ist. Die in der Ontologie repräsentierten Informationen sollen dabei helfen, Instanzen des Modells wie Anwendungen oder Wikis zu erstellen oder als Basis für die Entwicklung einer Methode dienen.

5.2 Bestehende Ontologien

Bevor mit der Bildung der neuen Ontologie begonnen wurde, wurden bestehende Ontologien identifiziert, die im gleichen Fachgebiet zu verorten sind, um deren Wiederverwendbarkeit zu prüfen. Bartolini und Muthuri (2015) haben eine Ontologie zur DSGVO erstellt, die die Inhalte der Entscheidungen aufzeigen soll, die der Verantwortliche eines VV zu treffen hat. In dieser Ontologie wird das VV nur am Rande behandelt, indem die Verarbeitungstätigkeiten in Zusammenhang mit Datenübermittlungen und den mit den Verarbeitungstätigkeiten in Zusammenhang stehenden Daten in Verbindung gebracht werden.

Eine weitere möglicherweise relevante Publikation, die identifiziert wurde, ist ein Metamodell, das datenschutzrelevante Konzepte beschreibt und in Zusammenhang zueinander bringt. Das Metamodell beinhaltet das VV nicht, zeigt jedoch eine relevante Relation zwischen Daten und Person bzw. Bürger und Bürgerin (Diamantopoulou, Angelopoulos, Pavlidis, & Mouratidis, 2017, S. 2ff).

Weitere Publikationen, die im gleichen Fachgebiet zu verorten sind, wurden nicht identifiziert. Dies gilt auch für bereits bekannte Datenschutzverzeichnisse. Da der Zweck der Ontologie von Bartolini und Muthuri (2015) sich stark von der vorliegenden Ontologie unterscheidet und sich die Bestandteile wenig überschneiden, wurden keine Bestandteile hiervon übernommen. Auch das Metamodell von Diamantopoulou et al. (2017, S. 2ff) behandelt die Thematik nur am Rande, weshalb die Ontologie zum VV komplett neu geschaffen wurde (vgl. Vorgehen von Noy & McGuinness, 2001, S. 4ff).

5.3 Relevante Begriffe

Im Verlaufe der Erstellung der Ontologie wurden die in den folgenden Absätzen erläuterten Begriffe als relevant identifiziert. Die Beschreibung der Begriffe entspricht dem Schritt ‚Auflistung/Beschreibung Begriffe' der Methodologie von Noy und McGuiness

(2001, S. 4ff). Gleichzeitig dienen die Beschreibungen der Begriffe in diesem Abschnitt dazu, ein einheitliches Verständnis zu schaffen. Die Begriffe stammen aus dem Gesetz (vgl. DSGVO Art. 30 im Anhang iv) oder wurden über die Literarturrecherche und aus den Interviews ermittelt.

Die anhand der Literaturrecherche und aus den Interviews ermittelten Begriffe wurden quantitativ anhand der Anzahl an Nennungen bewertet (vgl. Anhang vii). Zusätzlich zu der quantitativen Bewertung wurde eine qualitative Bewertung vorgenommen und aufgrund dessen entschieden, ob der jeweilige Begriff für die vorliegende Ontologie relevant ist.

Folgende Begriffe wurden bewusst nicht berücksichtigt:

Änderungshistorie

Aus dem Grundsatz der Rechenschaftspflicht nach DSGVO, Artikel 5 Abs. 2 lässt sich herleiten, dass Änderungen der Eintragungen im Verzeichnis nachvollzogen werden müssen. Die Änderungshistorie ist folglich im Zusammenhang mit dem VV durchaus relevant. Wird die Änderungshistorie manuell geführt, ist es schwierig, sie auf dem aktuellsten Stand zu halten. Wird das VV softwareunterstützt geführt, dann ist die Historisierung nicht weiter problematisch. Da die vorliegende Ontologie als Grundlage für unterschiedliche Verwendungszwecke vorgesehen ist, wird der Begriff ‚Änderungshistorie' in den weiteren Ausführungen nicht berücksichtigt.

Risikobewertung

Die Risikobewertung wird im Rahmen der technischen und organisatorischen Massnahmen (TOM) berücksichtigt und deshalb nicht als einzelner Begriff beschrieben.

Zugriffsberechtigte Personen

Auf den Begriff ‚Zugriffsberechtigte Personen' wird im Zusammenhang mit den Empfängerkategorien eingegangen.

Information der Betroffenen

Aus DSGVO, Artikel 13 geht hervor, dass die betroffene Person zum Zeitpunkt der Erhebung der Daten informiert werden muss. Der Begriff ‚Information der Betroffenen' bezieht sich demnach eher auf den Ablauf bei der Erfassung von personenbezogenen Daten

und müsste somit in den Prozessdokumentationen berücksichtigt werden. Die Information im VV zu führen, ist hingegen wenig hilfreich, weshalb der Begriff nicht weiter berücksichtigt wird.

Auf Begriffe, die gemäss der quantitativen Bewertung zweimal oder weniger oft genannt wurden, wird nicht näher eingegangen.

5.3.1 Verzeichnis von Verarbeitungstätigkeiten

Das VV (DSGVO, Art. 30, Abs. 1) ist ein Datenschutzverzeichnis, das alle Verarbeitungstätigkeiten eines Unternehmens enthält. Es kann eine bis beliebig viele Verarbeitungstätigkeiten enthalten. Im Gesetz wird davon ausgegangen, dass alle Unternehmen, abgesehen von den bereits erläuterten Ausnahmen (vgl. Kapitel 1.2.2), Verarbeitungstätigkeiten ausführen und somit ein VV führen müssen.

5.3.2 Verarbeitungstätigkeiten

Jede Verarbeitungstätigkeit (DSGVO, Art. 30, Abs. 1) hat eine Bezeichnung und eine Beschreibung der Zwecke der Verarbeitung. Die Zwecke müssen vorgängig festgelegt werden, eindeutig und legitim sein (DSGVO; Art. 5, Abs. 1b). Zudem müssen die Zwecke in der Rechtsgrundlage des betroffenen Mitgliedstaates festgelegt sein (DSGVO, Art. 6, Abs 2b). Ausnahmen gelten für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke und statistische Zwecke (DSGVO, Art. 89, Abs. 1). Wie der Begriff ‚Zweck' im Zusammenhang mit dem VV zu verstehen ist, geht aus der DSGVO nicht hervor. Das Bitcom (2017, S. 15) schreibt dazu, dass sich aus der Zweckbestimmung die Rechtsgrundlage für die Datenverwendung ableiten lassen muss. Gemäss den interviewten Experten kann diese Frage nicht eindeutig beantwortet werden (vgl. Interview A). Eine ähnliche Aussage geht aus Interview C hervor: «Der Zweck entspricht der Zielsetzung, die mit der Verarbeitung erreicht werden soll». Dieser ‚Zweck' muss so genau definiert sein, dass eine Person einschätzen kann, wozu ihre Daten verwendet werden (vgl. Interview A). So sind beispielsweise ‚Marketingzwecke' als Bestimmung eines Zwecks gemäss dem Experten aus Interview A eine zu ungenaue Zweckbestimmung. Eine eindeutigere Zweckbestimmung im Bereich Marketing wäre beispielsweise ‚Werbeanschreiben' (vgl. Interview C). Anhand dieser Aussagen könnte der Begriff ‚Zweck' im Zusammenhang mit VV wie folgt definiert werden:

‚Ein ‚Zweck' entspricht der Zielsetzung und einer Definition, die es der betroffenen Person ermöglicht, einzuschätzen, wozu ihre Daten verwendet werden'.

5.3.3 Verantwortlicher

Es ist ein Verantwortlicher für das VV beziehungsweise für die Verarbeitungstätigkeiten in einem Unternehmen zu definieren (DSGVO, Art. 30, Abs. 1). Von diesem und gegebenenfalls von einem Stellvertreter müssen die Namen und die Kontaktdaten im VV erfasst sein (DSGVO, Art. 30, Abs. 1a). Gemäss einem Kommentar zu DSGVO, Artikel 30 – Rn. 4 von Gola (2017) ist damit eine Adresse, unter der der Verantwortliche aufgesucht werden kann, gemeint. Ebenfalls unter die Kontaktdaten dürften die E-Mail-Adresse und die Telefonnummer fallen. Verantwortliche können eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle sein. Ist der Verantwortliche nicht in der EU niedergelassen, dann muss dieser einen Vertreter in der EU bestimmen (DSGVO, Art. 27 Abs. 1). Werden zwei oder mehrere Verantwortliche definiert, so haben diese gemeinsam festzulegen, wer in welcher Form welche Verpflichtungen gemäss DSGVO (Art. 26, Abs. 1) erfüllt. Wird in der Folge von ‚Verantwortlicher' gesprochen, dann ist jeweils der Verantwortliche für das VV gemeint. Ebenfalls wird in der Folge zur Vereinfachung immer der Singular verwendet.

Der Verantwortliche für das VV ist zuständig für die Einhaltung der Grundsätze für die Verarbeitung von personenbezogenen Daten und muss die Einhaltung gegenüber der Aufsichtsbehörde nachweisen können (DSGVO, Art. 5, Abs. 2). Ebenfalls muss der Verantwortliche belegen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat (DSGVO, Art. 7, Abs. 1). Zudem hat er Massnahmen zu treffen, die der betroffenen Person die gesetzlich vorgegebenen Informationen und Mitteilungen, die sich auf die Verarbeitung beziehen, in einer leicht zugänglichen Form sowie in einer klaren und einfachen Sprache übermitteln (DSGVO Art. 12, Abs. 1).

Der Verantwortliche erteilt Aufträge an Auftragsverarbeiter (DSGVO, Art. 28, Abs. 1). Dabei dürfen nur Auftragsverarbeiter berücksichtigt werden, die hinreichende Garantien dafür bieten, dass geeignete TOM bestehen, die die Verarbeitung im Einklang mit den Anforderungen der DSGVO (Art. 28, Abs. 2) sicherstellen. Zudem muss die Verarbeitung durch einen Auftraggeber auf Grundlage eines Vertrags geschehen (DSGVO, Art. 28, Abs. 3).

Der Verantwortliche ist im Weiteren zuständig für die Ernennung des Datenschutzbeauftragten. Dieser ist in jedem Fall zu benennen, wenn die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird (mit Ausnahme von Gerichten), wenn die Kerntätigkeit des Verantwortlichen in der Durchführung von Verarbeitungstätigkeiten, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmässige und systematische Überwachung von betroffenen Personen erforderlich machen, oder in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäss DSGVO, Artikel 9 besteht (vgl. Kapitel 5.3.8). Das Gleiche gilt für die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäss DSGVO, Artikel 10 (DSGVO, Art. 37, Abs. 1).

Der Verantwortliche hat ausserdem die Aufgabe, geeignete Massnahmen zu treffen, um ein angemessenes Schutzniveau zu gewährleisten. Dabei hat er sicherzustellen, dass der Datenschutzverantwortliche ordnungsgemäss und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden (Art. 38, Abs. 1) und bei der Erfüllung seiner Aufgaben unterstützt wird (Art. 38, Abs. 2).

5.3.4 Datenschutzbeauftragter

Gegebenenfalls haben Verantwortliche einen Datenschutzverantwortlichen zu nennen, der neben dem Verantwortlichen im VV geführt wird (DSGVO, Art. 30, Abs. 1a). Dasselbe gilt für den Auftragsverarbeiter (DSGOV, Art. 30, Abs. 2a).

Der Datenschutzverantwortliche muss Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzen sowie die Fähigkeit, die im Folgenden beschriebenen Aufgaben auszuführen (DSGVO, Art. 37, Abs. 5): die Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten des Unternehmens hinsichtlich ihrer Pflichten gemäss DSGVO sowie die Überwachung der Einhaltung des DSGVO einschliesslich der Zuweisung von Zuständigkeiten, der Sensibilisierung und der Schulung der an den Verarbeitungstätigkeiten beteiligten Mitarbeiter und Mitarbeiterinnen oder der diesbezüglichen Überprüfung und die Zusammenarbeit mit der Aufsichtsbehörde (DSGVO, Art. 39, Abs. 1). Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene des Verantwortlichen (DSGVO, Art. 38, Abs. 3).

5.3.5 Personenbezogene Daten

Im Zusammenhang mit dem VV sind personenbezogen Daten zentral (DSGVO, Art. 30, Abs. 1d und e). Jede Verarbeitungstätigkeit enthält per Definition personenbezogene Daten (DSGVO, Art. 4). Diese müssen auf rechtmässige Weise, nach Treu und Glauben und auf eine für die betroffene Person nachvollziehbare Art verarbeitet werden. Die Datenerfassung muss sich auf das notwendige Mass beschränken. Ebenso müssen die verwendeten Daten sachlich richtig sein. Unrichtige Daten müssen unverzüglich gelöscht oder berichtigt werden. Die Speicherung der Daten muss in einer Form erfolgen, die die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für die aktuellen Verarbeitungstätigkeiten nötig ist (DSGVO, Art. 5, Abs. 1).

5.3.6 Betroffene Person

Die personenbezogenen Daten beziehen sich auf eine betroffene Person. Diese ist deshalb für das VV ebenfalls relevant (DSGVO, Art. 30, Abs. 1c). Eine identifizierte oder identifizierbare natürliche Person wird in der DGSVO (Art. 4) als ‚betroffene Person' bezeichnet. Sofern keine besonderen Bedingungen wie eine rechtliche Verpflichtung oder die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, vorliegen, dürfen Daten nur verarbeitet werden, wenn von der betroffenen Person eine Einwilligung zu der Verarbeitung für einen oder mehrere bestimmte Zwecke gegeben wurde (DSGVO, Art. 6, Abs. 1). Die Einwilligung kann von der betroffenen Person jederzeit widerrufen werden (DSGVO, Art. 7, Abs. 3). Zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte im Zusammenhang stehenden Fragen können betroffene Personen den Datenschutzbeauftragten zu Rate ziehen (DSGVO, Art. 38, Abs. 4). Ist eine betroffene Person der Ansicht, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstösst, so hat sie das Recht auf eine Beschwerde bei der Aufsichtsbehörde (DSGVO, Art. 77, Abs. 1).

5.3.7 Personenkategorien

Gemäss DSGVO, Artikel 30, Abs. 1c sind Kategorien betroffener Personen, inklusive der Beschreibung dazu, zu definieren. Nähere Angaben zur Festlegung von Personenkategorien werden in der DSGVO nicht gemacht. Sinnvollerweise werden Personenkategorien allen Verarbeitungstätigkeiten zugewiesen, die sich auf diese beziehen. Laut Aussagen

aus Interview A ist die Definition der Personenkategorien eine Frage des Detailierungsgrads. Dazu muss die Überlegung getätigt werden, welche Funktion die Personenkategorien innehaben sollen und welche Informationen aus dem Verzeichnis ausgelesen werden können müssen (Interview A). Aus der Betrachtung des DSGVO, Artikel 8, Abs. 1 geht als eine möglicherweise sinnvolle Personenkategorie die Personenkategorie ‚Kinder unter 16 Jahren' hervor. Der Artikel besagt, dass eine Einwilligung einer erziehungsberechtigten Person vorliegen muss, wenn Daten von Kindern unter 16 Jahren verarbeitet werden. Entsprechende Verarbeitungstätigkeiten damit zu kennzeichnen, dient mit Sicherheit dazu, eine wichtige Information aus dem Verzeichnis auszulesen.

Ein klares Vorgehen für das Festlegen von Personenkategorien zeichnet sich aktuell noch nicht ab.

5.3.8 Datenkategorien

Die DSGVO schreibt vor, dass Datenkategorien, inklusive ihrer Beschreibung, zu definieren sind (DSGVO, Art. 30, Abs. 1c). Gleich wie für die Personenkategorien ergibt es für die Datenkategorien wohl Sinn, diese den Verarbeitungskategorien zuzuweisen, die diese beinhalten. Angaben zu der Kategorisierung werden in der Verordnung nicht gegeben. Einzig besondere Kategorien personenbezogener Daten wie rassische und ethnische Herkunft, politische Meinung, religiöse und weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit werden definiert. Des Weiteren fallen hierunter auch die Verarbeitung von genetischen und biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person sowie alle Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung. Die Verarbeitung der genannten Datenkategorien ist normalerweise untersagt (DSGVO, Art. 9, Abs 1).

Die GDD (2017) schreibt dazu, dass Datenkategorien so konkret wie möglich sein müssen, das heisst, dass Angaben wie beispielsweise ‚Kundendaten' nicht ausreichen. Ansonsten gehen aus der Literatur nur vage Angaben zum Thema ‚Datenkategorien' hervor. Zwei der interviewten Experten sind sich einig, dass bei der Festlegung der Kategorien die bereits im aktuellen Schweizer Datenschutzgesetz (DSG, Art. 3) vorhandene Einteilung von Personendaten in ‚schützenswerte' und ‚besonders schützenswerte' Daten beachtet werden sollte (Interview A und C). Ein Experte bemerkte ausserdem, dass er bei der Festlegung der Datenkategorien zunächst nach ‚schützenswerten' und ‚besonders schützenswerten' Daten und dann nach Zweck unterscheiden würde.

Wie bei der Festlegung der Personenkategorien zeichnet sich auch bei der Festlegung von Datenkategorien im Moment kein klares Vorgehen ab.

5.3.9 Empfängerkategorien

Im VV müssen ausserdem Kategorien von Empfängern definiert werden, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder möglicherweise offengelegt werden. Anders als bei den Daten- und Personenkategorien ist eine Beschreibung hierzu nicht explizit gefordert (DSGVO, Art. 30, Abs. 1d). Gemäss DSGVO, Artikel 4 sind ‚Empfänger' natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihnen um einen Dritten handelt oder nicht. Zu der Frage, wie Empfängerkategorien festgelegt werden sollen, macht das Gesetz keine konkretere Aussage. Als Empfängerkategorien kommen gemäss Bitcom (2017, S. 15) interne und externe Stellen in Frage, die Daten planmässig erhalten sollen, unabhängig davon, ob die Daten aktiv übertragen werden oder ob es sich um einen direkten Zugriff des Empfängers auf die Daten handelt. Darunter fallen auch am Prozess beteiligte weitere Stellen des eigenen Unternehmens (Gesellschaft für Datenschutz und Datensicherheit, 2017, S. 11), womit alle zugriffsberechtigten Personen beziehungsweise Funktionen oder Rollen gemeint sein dürften und diese somit auch unter die Empfängerkategorien fallen. Zu dem gleichen Schluss kommt auch Schäffter (2017, S. 131). Auch aus den Mustervorlagen des BvD und Schäffter (2017, S. 3; 2017, S. 131) geht hervor, dass interne und externe Empfänger kategorisiert werden müssen. Die Mustervorlage von Schäffter (2017, S. 131) sagt ausserdem aus, dass die Empfängerkategorien mit den Datenkategorien in Verbindung stehen, das heisst, dass die Zugriffsberechtigungen auf personenbezogene Daten angewendet werden sollen. Da eine Verarbeitungstätigkeit wohl nur ausgeführt werden kann, wenn der Zugriff auf alle mit dieser in Zusammenhang stehenden Daten gewährleistet ist, erscheint eine direkte Verbindung der Empfängerkategorien sinnvoller zu sein. Ist dies nicht der Fall, dann dürfte die Verarbeitungstätigkeit nicht ausreichend genau spezifiziert sein.

Auch die Auftragsverarbeiter fallen unter die Empfängerkategorien und müssen dementsprechend berücksichtigt werden (Bitcom, 2017, S. 15; Gesellschaft für Datenschutz und Datensicherheit, 2017, S. 11). Ebenso fallen Drittländer und internationale Organisationen, an die möglicherweise Datenübermittlungen erfolgen, unter die Empfängerkategorien (DSGVO, Art. 30, Abs. 1e).

Aus den Experteninterviews geht hervor, dass die Bestimmung der Empfängerkategorien in der Praxis noch unklar ist (Interview B). Das Vorgehen für die Festlegung der Empfängerkategorien scheint ebenfalls noch nicht eindeutig geklärt zu sein.

5.3.10 Datenübermittlung

Sofern Datenübermittlungen an ein Drittland, das heisst an ein Land ausserhalb der EU oder eine internationale Organisation, erfolgt sind, sind diese im VV zu dokumentieren (DSGVO, Art. 30, Abs. 1e und Abs. 2c). Als ‚internationale Organisationen' gelten nach DSGVO, Artikel 4 «völkerrechtliche Organisationen und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.» Fällt der Empfänger in eine der definierten Empfängerkategorien und liegt ein Angemessenheitsbeschluss vor, so darf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation erfolgen, ohne zusätzliche Garantien zu definieren. Ein Angemessenheitsbeschluss besteht darin, dass die EU-Kommission beschlossen hat, dass ein Land oder Gebiet oder die internationale Organisation ein angemessenes Schutzniveau bietet (Art. 45, Abs. 1). Bei einer Datenübermittlung sind die Empfängerkategorie sowie die betroffenen Datenkategorien anzugeben. Dies leitet sich daraus ab, dass die Übermittlung personenbezogene Daten betrifft und diese in eine Datenkategorie fallen. Bei Datenübermittlungen durch Auftragsverarbeiter sind wohl analog dazu die Verarbeitungskategorien anzugeben.

5.3.11 Garantien

Unter den im Folgenden beschriebenen Umständen müssen für Datenübermittlungen Garantien bestehen, die ebenfalls im VV dokumentiert werden müssen (DGSVO, Art. 30, Abs. 1e).

Besteht für eine Datenübermittlung kein Angemessenheitsbeschluss gemäss DSGVO, Artikel 45, dann müssen geeignete Garantien definiert sein, damit eine Datenübermittlung erfolgen darf (DSGVO, Art. 46, Abs. 1). Diese Garantien bestehen aus einem rechtlich bindenden Dokument zwischen Behörden und öffentlichen Stellen, verbindlichen internen Datenschutzvorschriften gemäss DSGVO, Artikel 47, Standardschutzklauseln, die von der EU-Kommission gemäss DSGVO, Artikel 93 erlassen werden, genehmigten Ver-

haltensregeln gemäss DSGVO, Artikel 40 oder einem genehmigten Zertifizierungsmechanismus gemäss DSGVO, Artikel 42. Dazu kommen rechtsverbindliche und durchsetzbare Verpflichtungen des Verantwortlichen im Drittland zur Anwendung der geeigneten Garantien (DSGVO, Art. 46, Abs. 2). Sofern die zuständige Aufsichtsbehörde einwilligt, können die Garantien auch aus Vertragsklauseln, die zwischen dem Verantwortlichen und dem Auftragsverarbeiter oder dem Empfänger der personenbezogenen Daten im Drittland oder der internationalen Organisation vereinbart wurden, bestehen. Eine weitere Möglichkeit sind Bestimmungen, die in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen aufzunehmen sind sowie durchsetzbare und wirksame Rechte für betroffene Personen einschliessen (DSGVO, Art. 46, Abs. 3).

5.3.12 Löschfristen

Löschfristen für die verschiedenen Datenkategorien sind «wenn möglich» im VV zu nennen (Art. 30, Abs. 1g). Die Formulierung «wenn möglich» ist gemäss Bitcom (2017, S. 15) nicht als optional zu verstehen, sondern so, dass die Löschregel in dem jeweils möglichen Konkretisierungsgrad angegeben werden soll. Die Löschung richtet sich in der Regel nach dem Zweck der Datenerhebung und -nutzung, das heisst, ist der Zweck erfüllt, so sind die Daten unverzüglich zu löschen (Bitcom, 2017, S. 15). Ausnahmen gelten bei den gesetzlichen Aufbewahrungspflichten, wie sie beispielsweise in der Schweiz aus dem Obligationenrecht (OR) Artikel 958 oder in Deutschland aus dem Handelsgesetzbuch (HGB) Artikel 257 hervorgehen.

5.3.13 Schutzmassnahmen

Wenn möglich, ist im VV eine allgemeine Beschreibung TOM gemäss DSGVO, Artikel 32. Abs. 1g und Abs. 2d zu führen. Dieser sieht die Sicherstellung eines angemessenen Schutzniveaus vor. Dies bedeutet eine Pseudonymisierung und Verschlüsselung personenbezogener Daten, die Fähigkeit, die Vertraulichkeit, die Integrität, die Verfügbarkeit sowie die Belastbarkeit der Systeme im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen und diese nach einem Zwischenfall schnell wiederherzustellen. Zudem ist ein Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen technischen und organisatorischen Massnahmen vorgesehen (DSGVO, Art. 32, Abs. 1). Hierunter fallen auch die Risikobewertung sowie die Datenschutz-Folgeabschätzung, die miteinander zusammenhängen (Interview C).

Die TOM können in einem allgemeinen Sicherheitskonzept geführt werden und es kann im VV darauf verwiesen werden. Zudem empfiehlt sich, Abweichungen für spezifische Verfahren in dem Verzeichnis bei dem betroffenen Verfahren gesondert aufzuführen (Bitcom, 2017, S. 16).

5.3.14 Auftragsverarbeiter

Ein Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag eines Verantwortlichen bearbeitet (DSGVO, Art. 4).

Handelt es sich bei einem Auftragsverarbeiter um eine juristische Person und somit um ein Unternehmen, dann hat dieser in Bezug auf das VV folglich die Verpflichtungen eines Unternehmens inne (DSGVO Art. 30, Abs. 1). Handelt es sich beim Auftragsverarbeiter um eine natürliche Person, so ist dieser ebenso wie ein Unternehmen verpflichtet, für Verarbeitungstätigkeiten, die er im Auftrag eines Verantwortlichen durchführt, ein VV zu führen. Für die im Auftragsverhältnis verarbeiteten Personendaten ist er den Vorgaben des Auftraggebers unterstellt. Der Auftragsverarbeiter führt im VV ebenfalls seine Kontaktdaten (Definition vgl. Kapitel 5.3.3) und anstelle von Zwecken der Verarbeitung führt er die Kategorien betroffener Personen, personenbezogener Daten (inklusive Löschfirsten) und Empfängern Kategorien von Verarbeitungen für Aufträge, die im Rahmen eines Auftrags eines Verantwortlichen durchgeführt werden (DSGVO, Art. 30, Abs. 2b). Aufgrund der unterschiedlichen Anforderungen der VV für Unternehmen und Auftragsverarbeiter liegt es für Unternehmen, die als Auftragsverarbeiter auftreten, nahe, zwei Verzeichnisse zu führen. Zum einen ist dies ein VV aus Sicht eines Unternehmens (in der Folge als VVU bezeichnet) und eines aus Sicht des Auftragsverarbeiters (in der Folge als VVA bezeichnet). Möglicherweise ist es sogar sinnvoll, pro Auftraggeber ein Verzeichnis zu führen (Interview A). Führt der Auftragsverarbeiter nur ein VVA, so ist im Sinne der Nachvollziehbarkeit der Name des auftraggebenden Verarbeiters pro Verarbeitungstätigkeit zu führen.

Ebenso wie der Verantwortliche muss auch der Auftragsverarbeiter einen Vertreter in der EU bestimmen, wenn er nicht in der EU niedergelassen ist (DSGVO, Art. 27, Abs. 1). Ausserdem benennt er unter gegebenen Umständen (vgl. Kapitel 5.3.3) einen Datenschutzbeauftragten. Ebenfalls hat er, analog zu dem Verantwortlichen, Schutzmassnahmen zu definieren (DSGVO, Artikel 32. Abs. 2d).

Will der Auftragsverarbeiter einen weiteren Auftragsverarbeiter in Anspruch nehmen, so ist die Genehmigung des auftraggebenden Verantwortlichen notwendig (DSGVO, Art. 28., Abs. 1). Zudem ist ebenfalls ein schriftlicher Vertrag zwischen dem auftraggebenden Auftraggeber und dem auftragsnehmenden Auftraggeber notwendig (DSGVO, Art. 28, Abs. 4). Im VVA sind die Kontaktdaten sämtlicher Auftragsverarbeiter in der Lieferkette zu führen (Gola, 2017, Kommentar Rn. 11 zu DSGVO Art. 30).

Wie bereits im Kapitel 5.3.9 zu den Empfängerkategorien erläutert, werden Auftragsverarbeiter als Empfängerkategorien geführt. Aus dem VV muss somit nicht ersichtlich sein, wer die konkreten Auftragsverarbeiter sind. Gemäss DSGVO, Artikel 15, Kapitel 1c müssen der betroffenen Person bei einer Anfrage die Empfänger oder die Kategorien von Empfängern der Personendaten bekannt gegeben werden, was nicht spezifiziert, ob die konkreten Auftragsverarbeiter bekannt gegeben werden müssen oder ob die Kategorien der beauftragten Auftraggeber ausreichen. Gemäss Aussagen im Interview B würden Unternehmen vermutlich versuchen, sich auf das Geschäftsgeheimnis zu berufen und die Daten nicht bekannt geben. Auch gemäss den Einschätzungen des Experten aus Interview C müssen die Auftraggeber im VV nicht namentlich genannt werden. Zum gleichen Schluss kommt auch Gola (2017, Kommentar Rn. 7 zu DSGVO Art. 30).

Auch wenn der Auftragsverarbeiter gemäss gesetzlichen Vorgaben nicht im Verzeichnis des Verantwortlichen geführt werden muss, ist es, um die Übersicht über die beauftragten Auftragsverarbeiter zu behalten, sinnvoll, diese direkt bei der betroffenen Verarbeitungstätigkeit aufzulisten. Dies erübrigt auch eine separate Auflistung der Auftragsverarbeiter. Ausserdem ergibt sich daraus, dass es sinnvoll ist, die zugehörige Empfängerkategorie zu jedem Auftragsverarbeiter zu führen.

5.3.15 Verarbeitungskategorien

Im VVA sind Kategorien von Verarbeitungen zu führen, die im Auftrag von Verantwortlichen durchgeführt werden (DSGVO, Art. 30, Abs. 2b). Die Verarbeitungskategorien entsprechen vermutlich den generell angebotenen Leistungen des Auftragsverarbeiters und können aus der Vereinbarung zur Auftragsverarbeitung entnommen werden (Bitcom, 2017, S. 16). Die Verarbeitungskategorien werden sinnvollerweise den betroffenen Verarbeitungstätigkeiten zugewiesen.

5.3.16 Ablage des VV

Das VV ist schriftlich, in Papierform oder in elektronischer Form zu führen (DSGVO, Art. 30, Abs. 3). Nähere Angaben zur Form des VV sind in der DSGVO nicht zu finden. Aus den Experteninterviews geht hervor, dass ein Verzeichnis in Papierform kaum in Frage kommt und zumindest eine Excel-Tabelle, besser noch eine Softwarelösung dafür verwendet werden sollte (Interview B).

5.3.17 Aufsichtsbehörde

Der Verantwortliche oder der Auftragsverarbeiter muss das VV der zuständigen Aufsichtsbehörde zur Verfügung stellen (DSGVO, Art. 30, Abs. 4).

In jedem Mitgliedsstaat der EU gibt es eine oder mehrere Aufsichtsbehörden, die einen Beitrag zur einheitlichen Anwendung der DSGVO (Art. 51, Abs. 1 und 2) leisten. Gibt es mehrere Aufsichtsbehörden, so bestimmt der Mitgliedstaat eine Aufsichtsbehörde, die die Behörden im Ausschuss vertritt (DSGVO, Art. 51, Abs. 3). Diese Aufsichtsbehörde ist der einzige Ansprechpartner der Verantwortlichen bei Fragen bezüglich grenzüberschreitender Verarbeitungen (Art. 56. Abs. 6). Für Unternehmen in der Schweiz bedeutet dies jedoch gemäss Aussage des Bundesrats (2018), wenn diese sowohl der DSGVO als auch dem Schweizer Datenschutzrecht unterstellt sind, dass sie sich an den Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) und die ausländische Aufsichtsbehörde wenden müssen. Die Aufsichtsbehörde oder die Aufsichtsbehörden haben die Aufgabe, die Anwendung der DSGVO zu überwachen und durchzusetzen, die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit Verarbeitungstätigkeiten zu sensibilisieren und sie darüber aufzuklären sowie die Verantwortlichen zu sensibilisieren. Ausserdem ist die Aufsichtsbehörde die Anlaufstelle für Anfragen und Beschwerden betroffener Personen (DSGVO, Art. 57). Die Aufsichtsbehörde hat das Recht, Verantwortliche auf ihre Verpflichtungen gegenüber den betroffenen Personen hinzuweisen (DSGVO, Art. 58).

Die Aufsichtsbehörde hat des Weiteren das Recht, einen Verantwortlichen oder Auftragsverarbeiter anzuweisen, ihr alle Informationen bereitzustellen, die für die Erfüllung seiner Aufgaben erforderlich sind, sowie Zugang zu allen personenbezogenen Daten und Informationen, die wiederum zur Erfüllung seiner Aufgabe notwendig sind, einzufordern. Bei einem vermeintlichen oder einem voraussichtlichen Verstoss gegen die DSGVO ist

es der Auftragsbehörde gestattet, den Verantwortlichen darauf hinzuweisen. Werden Verarbeitungstätigkeiten nicht im Einklang mit der DSGVO durchgeführt, dann kann die Aufsichtsbehörde den Verantwortlichen anweisen, die Verordnung innerhalb eines bestimmten Zeitraums einzuhalten (DSGVO, Art. 58).

Die Aufsichtsbehörde ist in jedem Mitgliedsstaat befugt, den Justizbehörden Verstösse gegen diese Verordnung zur Kenntnis zu bringen (DSGVO, Art. 58, Abs. 5). Dabei arbeitet sie auch mit anderen Aufsichtsbehörden zusammen (DSGVO, Art. 60, Abs. 1).

5.3.18 Unternehmen

Grundsätzlich sind alle Unternehmen verpflichtet, ein VV zu führen. Ausnahmen gelten für Unternehmen, die weniger als 250 Mitarbeitende beschäftigen und weitere im DSGVO beschriebene Bedingungen erfüllen (DSGVO, Art. 30, Abs. 5). Erläuterungen hierzu gehen aus Kapitel 1.2.2 hervor.

5.3.19 Rechtsgrundlage

Damit Personendaten bearbeitet werden dürfen, muss eine Rechtsgrundlage (DSGVO, Art. 6) bestehen. Diese muss gemäss DSGVO, Artikel 30 nicht im VV geführt werden. Die GDD (2017, S. 8), die DSK (2018, S. 2), das Bitcom (2017, S. 17), die WKO (2018a, S. 4), Schäffter (2017, S. 130) sowie die interviewten Experten (Interview A, B und C) sind sich jedoch einig, dass es sinnvoll ist, die Rechtsgrundlage im VV zu führen. Dies dient der Erfüllung der Rechenschaftspflichten gemäss DSGVO, Artikel 5. Ebenso führt die Dokumentation der Rechtsgrundlage für jede Verarbeitungstätigkeit dazu, dass zu jeder Verarbeitungstätigkeit überlegt wird, welche Rechtsgrundlage besteht. Dabei erscheint es sinnvoll, für möglichst viele Verarbeitungstätigkeiten eine andere Rechtsgrundlage als die Einwilligung der betroffenen Person zu finden (Interview B).

5.3.20 Dateisystem

Die DSGVO bezieht sich gemäss Artikel 2, Kapitel 1 auf alle Verarbeitungen, die in einem Dateisystem gespeichert sind. Unter ‚Dateisystem' ist jede strukturierte Sammlung personenbezogener Daten zu verstehen (DSGVO, Art. 4). Bei der Erstellung des VV bietet es sich an, alle in der Systemlandschaft des Unternehmens eingesetzten Anwendungen und Tools aufzulisten, in denen personenbezogene Daten gespeichert werden (Datenschutzbeauftragter INFO, 2016b). Die Belgische CPP (2017) sieht in ihrer Mustervorlage

für das VV das Führen der Anwendungen vor. Ebenso erwähnt eine interviewte Expertin (Interview B), dass es sinnvoll sei, die Anwendungen, in denen die personenbezogenen Daten gespeichert sind, im VV zu führen. Ausserdem ist das Führen des Dateisystems im Datenschutzverzeichnis auch aus der Norm ISO27001 bekannt, wie aus den Richtlinien für die Zertifizierung ‚GoodPriv@cy' hervorgeht. Dies leitet sich ab aus der Formulierung: «eine einfache Beschreibung der verwendeten Bearbeitungsmittel und -methoden» (Schweizerische Vereinigung für Qualitäts- und Management-Systeme (SQS), 2011, S. 6).

Es ist davon auszugehen, dass der Grossteil der Datensammlungen, sprich Dateisysteme, in einem Unternehmen in einer Anwendung gespeichert beziehungsweise über eine Anwendung aufgerufen werden können. Aus diesem Grund ist es sinnvoll, die Anwendungen für jede Verarbeitungstätigkeit zu führen, um sicherzustellen, dass alle Datensammlungen berücksichtigt wurden.

Falls eine Person Auskunft über die von ihr gespeicherten Daten im Unternehmen verlangt, dann können mit dieser Information schneller Aussagen getroffen werden (Interview C).

5.3.21 Zuständigkeit

Die GDD (2017, S. 8) und das Bitcom (2017, S. 18) empfehlen, die für die Verarbeitungstätigkeit zuständigen Personen im VV zu führen. Gleiches geht aus Interview B und C hervor.

Hat ein Unternehmen mehrere Abteilungen und Führungskräfte, so scheint es schwierig, dass ein Verantwortlicher den Überblick über alle Verarbeitungstätigkeiten behalten kann. Werden zuständige Personen pro Verarbeitungstätigkeit geführt, kann dies Abhilfe schaffen. Bei der Initiierung des VV sind Führungskräfte und insbesondere Führungskräfte, die in leitender Funktion über Personendaten bestimmen, wichtige Ansprechpartner (Interview A und B). Wenn diese Personen zu Beginn identifiziert werden, erleichtert dies die Ermittlung der für das VV relevanten Vorgänge. Später hilft diese Information auch dabei, das Verzeichnis aktuell zu halten.

5.4 Definition ‚Klassen'

Wie in der Methodologie von Noy und McGuiness (2001, S. 4ff) beschrieben, werden aus den zuvor identifizierten Begriffen Klassen ermittelt. Alle als relevant identifizierten Begriffe bilden eine Klasse (vgl. Tabelle 6). Zusätzlich wurde die Klasse ‚Verantwortlichkeit' erstellt, da sich bei der Instanziierung (Prototyp in Form einer Access-Datenbank) herausgestellt hat, dass es sinnvoll ist, die Klassen ‚Verantwortlicher' und ‚Datenschutzverantwortlicher' zusammenzufassen. Weiter wurden die Klassen ‚Papierablage' und ‚Elektronische Ablage' als ‚beschreibende' Klassen erstellt, da sich damit die Informationen aus DSGVO, Art. 30 noch besser verdeutlichen lassen.

‚Beschreibende' Klassen (vgl. Tabelle 6) sind deshalb gekennzeichnet, da diese Klassen im Zusammenhang mit der Weiterverwendung des Modells lediglich einen beschreibenden Charakter haben, aber dennoch wichtig für die Verständlichkeit des Modells sind. Klassen, die für die Weiterverwendung direkt relevant sind, werden im Folgenden als ‚Kernklassen' bezeichnet. Ausserdem könnten die Klassen durch die Weiterentwicklung des Modells eine andere Bedeutung erhalten. So würde sich beispielsweise die Bedeutung der Klasse ‚Betroffene Person' verändern, wenn das Modell in eine bestehende Unternehmensarchitektur eingebunden wird. Mit ‚Optional' sind Klassen gekennzeichnet, die nicht unmittelbar aus dem Gesetz hervorgehen (vgl. Tabelle 6).

Klasse	**Beschreibend**	**Optional**	**VVU**	**VVA**
Verzeichnis von Verarbeitungstätigkeiten	**x**			
Verarbeitungstätigkeiten			**x**	**x**
Verantwortlichkeiten			**x**	
Verantwortlicher	**x***		**x**	
Datenschutzbeauftragter	**x**		**x**	**x**
Personenbezogene Daten	**x**		**x**	**x**
Betroffene Person	**x**		**x**	**x**
Personenkategorien			**x**	
Datenkategorien			**x**	

Empfängerkategorien			**x**	
Datenübermittlungen			**x**	**x**
Garantien			**x**	**x**
Löschfristen			**x**	
Schutzmassnahmen			**x**	**x**
Auftragsverarbeiter	**x***		**x**	**x**
Verarbeitungskategorien				**x**
Ablage	**x**		**x**	**x**
Papierablage	**x**		**x**	**x**
Elektronische Ablage	**x**		**x**	**x**
Aufsichtsbehörde	**x**			
Unternehmen	**x**		**x**	
Rechtsgrundlage		**x**	**x**	
Dateisystem		**x**	**x**	**x**
Zuständigkeit		**x**	**x**	
*Im Zusammenhang mit dem VVA hat die Klasse ‚Verantwortlicher' nur einen beschreibenden Charakter. Umgekehrt hat die Klasse ‚Auftragsverarbeiter' im Zusammenhang mit dem VVU mehr als einen beschreibenden Charakter.				

Tabelle 6: Klassen der Ontologie

Aus Tabelle 6 geht zudem hervor, für welches VV die Klasse relevant ist. Damit wird verdeutlicht, dass sich die VV von Unternehmen und Auftragsverarbeitern wesentlich unterscheiden. Nur die Hälfte der Klassen, sprich Klasse 12 von 24, sind für beide VV relevant. Im Verlaufe der Entwicklung der Ontologie wurde festgestellt, dass sich das Modell aufgrund der Unterschiede des VVU und des VVA schlecht lesen lässt. Aus diesem Grund fiel der Entscheid, zwei Ontologien zu erstellen.

5.5 Assoziationen der Klassen

Nach der Definition der Klassen werden nun die Assoziationen zwischen den Klassen aufgezeigt. (vgl. Methodologie von Noy und McGuiness (2001, S. 4ff), Schritt «Klassen definieren»).

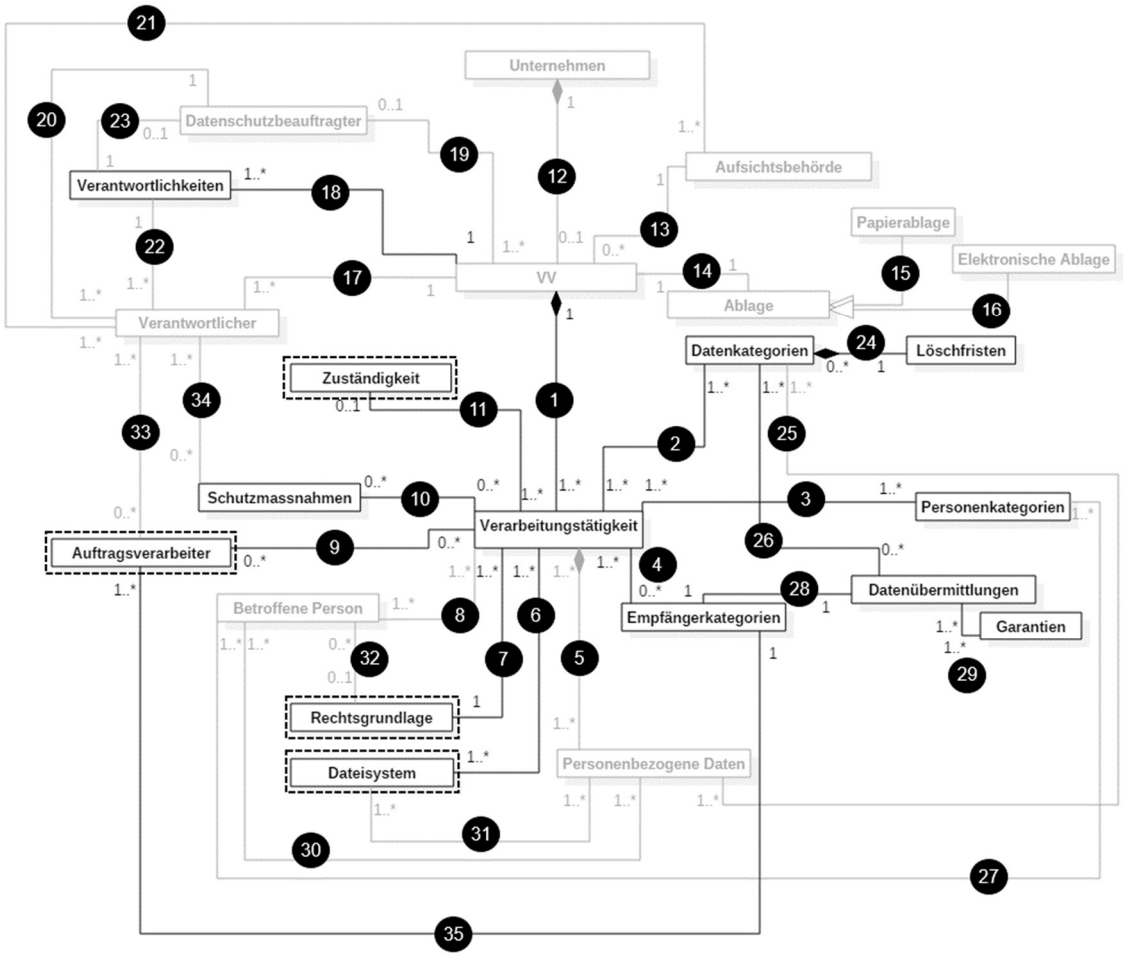


Abbildung 7: Klassenbeziehungen der ‚Ontologie des VVU'

Legende

	Beschreibende Klassen und Assoziationen
	Kernklassen und Assoziationen
	Optionale Klasse

Bei der Ermittlung der Assoziationen zwischen den Klassen wurde nach dem von Uschold und King (1995, S. 2) beschriebenen ‚Middle-Out'-Ansatz vorgegangen. Der Ansatz sieht vor, mit dem Kern zu starten und dann einerseits immer spezifischer zu werden und anderseits zu generalisieren. Die Wahl dieses Ansatzes begründet sich dadurch, dass sich die ‚Verarbeitungstätigkeit' klar als zentrales Element identifizieren lässt. Für das VVU und das VVA wurden insgesamt 44 unterschiedliche Assoziationen zwischen den Klassen ermittelt, wovon 25 Assoziationen, in den Abbildungen in Grau gehalten, der Beschreibung und damit dem besseren Verständnis der Zusammenhänge dienen. Die übrigen in Schwarz dargestellten Assoziationen sind für die Weiterverwendung des Modells von unmittelbarer Relevanz. Sowohl im Zusammenhang mit dem VVU als auch in

Zusammenhang mit dem VVA sind 15 der 44 ermittelten Assoziationen relevant, was den Entscheid zwei Ontologien zu bilden, nochmals bekräftigt. Die Assoziationen werden aus Abbildung 7 und Abbildung 8 ersichtlich. Ausserdem zeigen die Abbildungen die ermittelten Multiplizitäten zu jeder Beziehung auf.

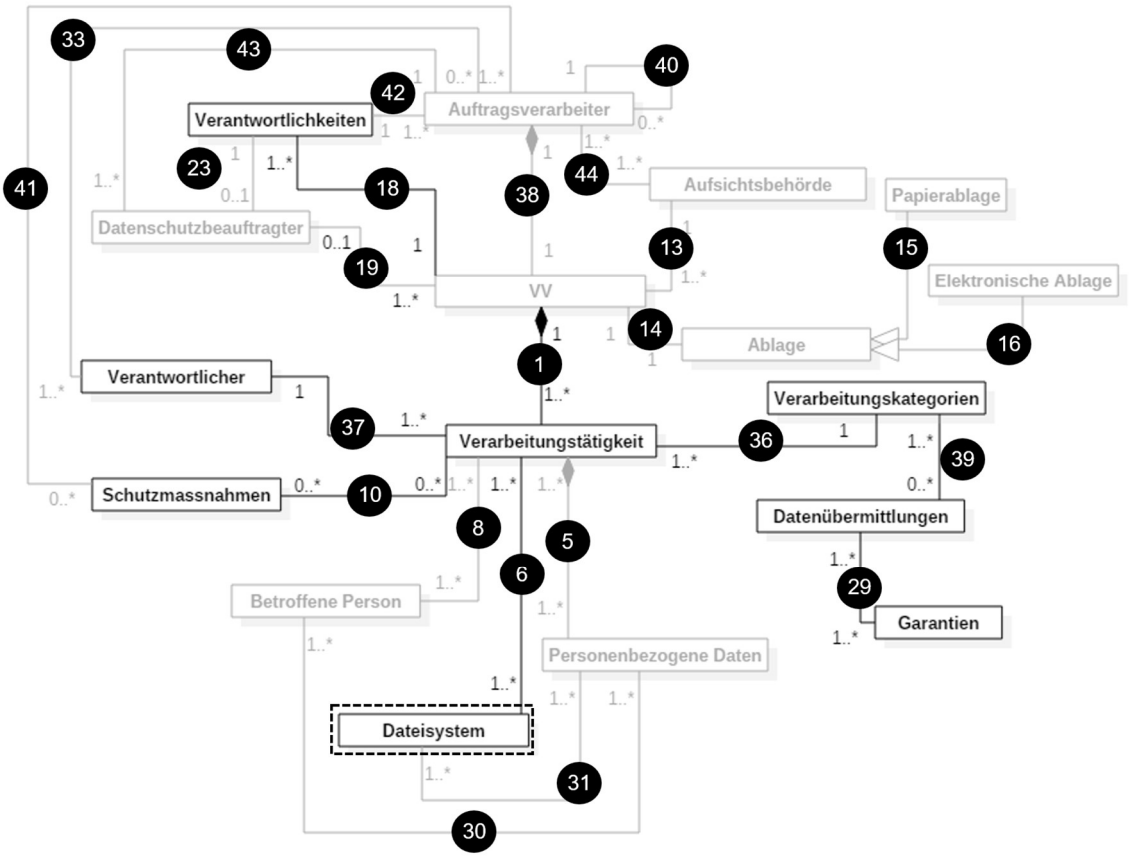


Abbildung 8: Klassenbeziehungen der ‚Ontologie des VVA'

Legende

Beschreibende Klassen und Assoziationen

Kernklassen und Assoziationen

Optionale Klasse

Wie sich die Multiplizitäten der jeweiligen Beziehung gestalten, wird in der folgenden Tabelle 7 erläutert. Die Beschreibungen ergeben sich aus den Begriffserläuterungen in Kapitel 5.3.

Nr.	Beschreibung
1	Ein VV enthält eine oder mehrere Verarbeitungstätigkeiten.

Nr.	Beschreibung
2	Eine Verarbeitungstätigkeit betrifft eine oder mehrere Datenkategorien und eine Datenkategorie kann in einer oder mehreren Verarbeitungstätigkeiten vorkommen.
3	Eine Verarbeitungstätigkeit betrifft eine oder mehrere Personenkategorien und eine Personenkategorie kann in einer oder mehreren Verarbeitungstätigkeiten vorkommen.
4	Eine Verarbeitungstätigkeit hat keine, genau eine oder mehrere Empfängerkategorien und kann in einer oder mehreren Verarbeitungstätigkeiten vorkommen. Hervorgehend aus den Erläuterungen zum Begriff ‚Empfängerkategorien' wird es in der Realität der Vermutung nach keine Verarbeitungstätigkeiten ohne eine Empfängerkategorie geben (vgl. Kapitel 7.3.9)
5	Eine Verarbeitungstätigkeit betrifft per Definition personenbezogene Daten. Es können beliebig viele personenbezogene Daten in einer oder mehreren Verarbeitungstätigkeiten enthalten sein.
6	Eine Verarbeitungstätigkeit kann in einem oder mehreren Dateisystemen abgelegt sein. In einem Dateisystem können eine oder mehrere Verarbeitungstätigkeiten bearbeitet werden.
7	Eine Verarbeitungstätigkeit erfordert eine Rechtsgrundlage. Eine Rechtsgrundlage kann auf eine oder mehrere Verarbeitungstätigkeiten angewendet werden.
8	Von einer Verarbeitungstätigkeit können eine oder mehrere Personen betroffen sein. Eine Person kann von einer oder mehreren Verarbeitungstätigkeiten betroffen sein.
9	Arbeiten keine Auftragsverarbeiter für ein Unternehmen, werden folglich auch keine Verarbeitungstätigkeiten durch Auftragsverarbeiter verarbeitet. Anderseits können mehrere Verarbeitungstätigkeiten von einem Auftragsverarbeiter verarbeitet werden und mehrere Auftragsverarbeiter Verarbeitungstätigkeiten für ein Unternehmen durchführen.
10	Sind Schutzmassnahmen generell definiert, so beziehen sich diese nicht auf eine Verarbeitungstätigkeit. Anderseits können einer Verarbeitungstätigkeit eine oder mehrere spezifische Schutzmassnahmen zugewiesen werden und eine Schutzmassnahme kann sich auf eine oder mehrere Verarbeitungstätigkeiten beziehen.
11	Für eine bis beliebig viele Verarbeitungstätigkeiten kann keine oder genau eine Zuständigkeit definiert werden. Die selbe Zuständigkeit kann für mehrere Verarbeitungstätigkeiten zutreffen.
12	Ein Unternehmen hat entweder genau ein oder kein VV.
13	Eine Aufsichtsbehörde hat die Möglichkeit, eines oder mehrere VV einzufordern. Es wird davon ausgegangen, dass sich im Zuständigkeitsbereich jeder Aufsichtsbehörde Unternehmen befinden, die ein VV führen müssen.
14	Ein VV hat genau eine Ablage.
15	Das Verzeichnis kann in Papierform abgelegt werden.

Nr.	Beschreibung
16	Das Verzeichnis kann elektronisch abgelegt werden.
17	Ein oder mehrere Verantwortliche führen ein VV.
18	Ein VV erfordert eine oder mehrere Verantwortlichkeiten.
19	Eines oder mehrere VV überwacht ein Datenschutzbeauftragter. Es ist auch möglich, dass kein Datenschutzbeauftragter für die Überwachung zuständig ist.
20	Ein oder mehrere Verantwortliche bestimmen entweder keinen oder einen Datenschutzbeauftragten.
21	Eine Aufsichtsbehörde fordert das VV bei einem oder mehreren unterschiedlichen Verantwortlichen ein.
22	Ein oder mehrere Verantwortliche haben eine Verantwortlichkeit.
23	Kein oder ein Datenschutzbeauftragter hat eine Verantwortlichkeit.
24	Keine oder mehrere Datenkategorien haben jeweils eine Löschfrist.
25	Eine oder mehrere Datenkategorien beziehen sich auf personenbezogen Daten. Personenbezogene Daten sind per Definition in Datenkategorien enthalten und können in beliebigem Ausmass vorhanden sein.
26	Eine oder mehrere Datenkategorien können in einer Datenübermittlung enthalten sein. Es ist möglich, dass keine bis beliebig viele Datenübermittlungen eine Datenkategorie betreffen.
27	Eine Personenkategorie kann sich auf eine oder mehrere betroffene Personen beziehen. Eine oder mehrere betroffenen Personen können in einer Personenkategorie enthalten sein.
28	Eine Empfängerkategorie kann eine Datenübermittlung betreffen.
29	Eine Datenübermittlung benötigt eine oder mehrere Garantien. Dieselbe Garantie kann für mehrere Datenübermittlungen verwendet werden.
30	Eine betroffene Person hat unterschiedliche personenbezogene Daten. Unterschiedliche personenbezogene Daten beziehen sich auf eine oder mehrere betroffene Personen.
31	In einem Dateisystem können unterschiedliche personenbezogene Daten enthalten sein. Unterschiedliche personenbezogene Daten sind in einem oder mehreren Dateisystemen enthalten.
32	Ist die Rechtsgrundlage die Einwilligung der betroffenen Person, so liefert eine betroffene Person eine Rechtsgrundlage. Liegt eine andere Rechtsgrundlage vor, dann wird keine Einwilligung der betroffenen Person benötigt. Rechtsgrundlagen werden entweder von keiner oder mehreren Personen benötigt.

Nr.	Beschreibung
33	Für das VVU gilt: ein Auftragsverarbeiter kann von einem oder mehreren Verantwortlichen beauftragt werden. Ein Verantwortlicher kann keinen oder mehrere Auftragsverarbeiter beauftragen. Im Falle des VVA gilt: ein Verantwortlicher kann keinen oder mehrere Auftragsverarbeiter beauftragen und ein Auftragsverarbeiter kann von mehreren unterschiedlichen Verantwortlichen beauftragt werden.
34	Es werden keine oder mehrere Schutzmassnahmen durch den Verantwortlichen festgelegt. Ein oder mehrere Verantwortliche können Schutzmassnahmen definieren.
35	Ein oder mehrere Auftragsverarbeiter gehören zu jeweils einer Empfängerkategorie.
36	Eine Verarbeitungstätigkeit kann eine oder mehrere Verarbeitungskategorien betreffen. Eine Verarbeitungskategorie kann einer Verarbeitungstätigkeit zugwiesen werden. Dies hat sich bei Instanziierung in der Access-Datenbank ergeben, da es wohl für pro VERARBEITUNGStätigkeit nur eine VERARBEITUNGSkategorie geben kann.
37	Eine oder mehrere Verarbeitungstätigkeiten werden für einen Verantwortlichen ausgeführt. Für jede Verarbeitungstätigkeit ist ein Verantwortlicher definiert. Es wird davon ausgegangen, dass nur ein Verantwortlicher eines Unternehmens als Auftraggeber auftritt.
38	Ein Auftragsverarbeiter führt ein VV.
39	Eine Datenübermittlung kann eine oder mehrere Verarbeitungskategorien enthalten. Es ist möglich, dass keine, genau eine oder mehrere Datenübermittlungen eine Verarbeitungskategorie betreffen.
40	Ein Auftragsverarbeiter kann keine oder mehrere Auftragsverarbeiter beauftragen.
41	Ein Auftragsverarbeiter legt keine oder mehrere Schutzmassnahmen fest. Schutzmassnahmen können von mehreren Auftragsverarbeitern festgelegt werden.
42	Ein oder mehrere Auftragsverarbeiter haben eine Verantwortlichkeit.
43	Ein oder mehrere Auftragsverarbeiter bestimmen entweder keinen oder einen Datenschutzbeauftragten.
44	Eine Aufsichtsbehörde fordert das VV bei einem oder mehreren unterschiedlichen Auftragsverarbeitern ein.

Tabelle 7: Beschreibung der Multiplizitäten zu den Beziehungen in den Klassendiagrammen

5.6 Definition Attribute

Nachdem die Klassen bestimmt und die Zusammenhänge zwischen den Klassen aufgezeigt wurden, werden nun die Attribute für die Klassen festgelegt (vgl. Methodologie von

Noy und McGuiness (2001, S. 4ff), Schritt ‚Attribute definieren'). Es werden alle Attribute definiert, die für die Weiterverwendung des Modells relevant sind. Für ‚beschreibende' Klassen (vgl. Kapitel 5.4) werden keine Attribute definiert. Die Attribute ergeben sich aus den Ausführungen in den Absätzen 5.3, 5.4 und 5.5. Im Folgenden werden die Attribute bezogen auf diese Ausführungen erläutert. Ausserdem wird definiert, ob es sich um ein optionales Attribut handelt, das nicht nach DSGVO, Artikel 30 vorgeschrieben ist. Zudem wird betrachtet, für welche Ontologie, das heisst, ob für die Ontologie der VVU und/oder die der VVA, dieses relevant ist.

5.6.1 Beschreibung der Attribute

Zunächst werden die Attribute der zentralen Klasse ‚Verarbeitungstätigkeit' erläutert. Diese Klasse findet sich in beiden Ontologien mit jeweils unterschiedlichen Attributen wieder. In der Klasse sind elf Attribute enthalten, wovon zehn Assoziationen für die Zuweisung von Objekten aus anderen Klassen darstellen. Fünf der Attribute sind optional. In Tabelle 8 werden die definierten Attribute verdeutlicht:

Attribut	**Beschreibung**	**Optional**	**VVU**	**VVA**
Bezeichnung	Kurze Bezeichnung, die die Verarbeitungstätigkeit erkennen lässt		**x**	**x**
Zweck	Beschreibung des Zwecks der Verarbeitungstätigkeit (Vorgabe DSGVO, Art. 30, Abs 1b)		**x**	
Dateisystem	Assoziation für die Zuweisung eines Objekts der Klasse ‚Dateisystem'	**x**	**x**	**x**
Zuständigkeit	Assoziation für die Zuweisung eines Objekts der Klasse ‚Zuständigkeit'	**x**	**x**	
Datenkategorie	Assoziation für die Zuweisung eines Objekts der Klasse ‚Datenkategorie'		**x**	
Personenkategorie	Assoziation für die Zuweisung eines Objekts der Klasse ‚Personenkategorie'		**x**	
Empfängerkategorien	Assoziation für die Zuweisung eines Objekts der Klasse ‚Empfängerkategorie'		**x**	
Auftragsverarbeiter	Assoziation für die Zuweisung eines Objekts der Klasse ‚Auftragsverarbeiter'	**x**	**x**	

Verarbeitungskategorien	Assoziation für die Zuweisung eines Objekts der Klasse ‚Verarbeitungskategorie'	**x**		**x**
Rechtsgrundlage	Assoziation für die Zuweisung eines Objekts der Klasse Rechtsgrundlage	**x**	**x**	
Schutzmassnahmen	Assoziation für die Zuweisung eines Objekts der Klasse ‚Schutzmassnahmen'	**x**	**x**	**x**
Verantwortlicher	Assoziation für die Zuweisung eines Objekts der Klasse ‚Verantwortlicher'			**x**

Tabelle 8: Attribute der Klasse ‚Verarbeitungstätigkeiten'

Die Attribute der Klasse ‚Verantwortlichkeiten' dienen dazu, die Kontaktdaten der oder des Verantwortlichen, bezogen auf das VVU, sowie der Auftragsverarbeiter oder des Auftragsverarbeiters, bezogen auf das VVA, zu erfassen. Alle acht definierten Attribute sind sowohl für das VVU als auch für das VVA relevant und sind in jedem Fall zu erfassen, das heisst nicht optional. Die definierten Attribute für diese Klasse werden in Tabelle 9 verdeutlicht.

Attribut	**Beschreibung**	**Optional**	**VVU**	**VVA**
Name	Name des/der Verantwortlichen(VVU)/des/der Auftragsverarbeiter/s (inklusive Subauftragsverarbeiter; VVA)/des Datenschutzbeauftragten		**x**	**x**
Vorname	Vorname des/der Verantwortlichen(VVU)/des/der Auftragsverarbeiter/s (inklusive Subauftragsverarbeiter; VVA)/des Datenschutzbeauftragten		**x**	**x**
Rolle	Verantwortlicher (VVU)/Auftragsverarbeiter (inklusive Subauftragsverarbeiter; VVA)/Datenschutzbeauftragter		**x**	**x**
Strasse/Hausnr.	Adressdaten des/der Verantwortlichen (VVU)/des/der Auftragsverarbeiter/s (inklusive Subauftragsverarbeiter; VVA)/des Datenschutzbeauftragten		**x**	**x**
Postleitzahl			**x**	**x**
Ort			**x**	**x**
Email	E-Mail-Adresse des/der Verantwortlichen (VVU)/des/der Auftragsverarbeiter/s (inklusive Subauftragsverarbeiter; VVA)/des Datenschutzbeauftragten		**x**	**x**

Telefonnummer	Telefonnummer des/der Verantwortlichen (VVU)/des/der Auftragsverarbeiter/s (inklusive Subauftragsverarbeiter; VVA)/des Datenschutzbeauftragten		**x**	**x**

Tabelle 9: Attribute der Klasse ‚Verantwortlichkeiten'

Die Attribute der unten aufgeführten Klasse ‚Verantwortlicher' sind nur für das VVA relevant, da es sich bei dem Verantwortlichen um den Auftraggeber handelt und nicht um einen internen Verantwortlichen beziehungsweise Auftragsverarbeiter, der in die Klasse ‚Verantwortlichkeiten' fallen würde. Die Attribute dieser Klasse dienen dazu, die Kontaktdaten des zuständigen Verantwortlichen zu erfassen. Als optionales Attribut wird die Kategorie ‚Unternehmen' definiert, was dem Auftragsverarbeiter verdeutlicht, für welches Unternehmen eine Verarbeitungstätigkeit ausgeführt wird. In der nachstehenden Tabelle 10 werden die Attribute dieser Klasse verdeutlicht.

Attribut	**Beschreibung**	**Optional**	**VVU**	**VVA**
Unternehmen	Unternehmen, das der Verantwortliche vertritt	**x**		**x**
Name	Name des Verantwortlichen			**x**
Vorname	Vorname des Verantwortlichen			**x**
Strasse/Nr.	Adressdaten des Verantwortlichen			**x**
Postleitzahl				**x**
Ort				**x**
Email	E-Mail-Adresse des Verantwortlichen			**x**
Telefonnummer	Telefonnummer des Verantwortlichen			**x**

Tabelle 10: Attribute der Klasse ‚Verantwortlicher'

Aus den Tabelle 11, Tabelle 12 und Tabelle 13 werden die Attribute der Klassen ‚Personenkategorien', ‚Datenkategorien' und ‚Empfängerkategorien' ersichtlich. Die definierten Attribute beziehen sich auf das VVU. Im VVA ist eine Erfassung der Personenkategorien nicht vorgesehen. In jeder dieser Klassen sind zwei Attribute definiert, die der Bezeichnung und Beschreibung der Kategorie dienen. In der Klasse ‚Datenkategorien' ist zudem eine Assoziation definiert, die der Zuweisung von Löschfristen dient. Das ‚Attribut' wird als optional definiert, da Löschfristen gemäss DSGVO Artikel 30, Abs. 1f nur

dann, wenn dies möglich ist, definiert werden müssen (Ausführungen dazu vgl. Kapitel 5.3.12).

Attribut	**Beschreibung**	**Optional**	**VVU**	**VVA**
Personenkategorien	Bezeichnung einer eindeutigen Personenkategorie		**x**	
Beschreibung	Erläuterungen zur Personenkategorie		**x**	

Tabelle 11: Attribute der Klasse ‚Personenkategorien'

Attribut	**Beschreibung**	**Optional**	**VVU**	**VVA**
Datenkategorien	Bezeichnung einer eindeutigen Datenkategorie		**x**	
Beschreibung	Erläuterungen zur Datenkategorie		**x**	
Löschfrist	Assoziation für die Zuweisung eines Objekts der Klasse ‚Löschfristen'	**x**	**x**	

Tabelle 12: Attribute der Klasse ‚Datenkategorien'

Attribut	**Beschreibung**	**Optional**	**VVU**	**VVA**
Empfängerkategorien	Bezeichnung einer eindeutigen Empfängerkategorie, bei internen Empfängern zum Beispiel die Funktion oder Organisationseinheit		**x**	
Beschreibung	Erläuterungen zur Empfängerkategorie	**x**	**x**	

Tabelle 13: Attribute der Klasse ‚Empfängerkategorien'

Die Attribute der Klasse ‚Datenübermittlungen' haben den Zweck, durchgeführte Datenübermittlungen zu erfassen. Die Attribute gehen alle aus der DSGVO, Artikel 30 hervor und sind daher in jedem Fall relevant. Jeweils vier der sechs definierten Attribute betreffen das VVU und das VVA. Die Attribute ‚Datenkategorien' und ‚Verarbeitungskategorien' sind Assoziationen, die der Zuweisung der in der Datenübermittlung enthaltenen Daten dienen. Das Attribut ‚Empfängerkategorie' ermöglicht es, einen Rückschluss auf den Empfänger der Datenübermittlung zu ziehen. Die definierten Attribute für diese Klassen werden in Tabelle 14 verdeutlicht.

Attribut	Beschreibung	Optional	VVU	VVA
Land	Land, in dem die Datenübermittlung erfolgt ist		x	x
Organisation	Name der Organisation oder der Behörde, an die die Übermittlung erfolgt ist		x	x
Datenkategorien	Assoziation für die Zuweisung eines Objekts der Klasse ‚Löschfristen'		x	
Empfängerkategorie	Assoziation für die Zuweisung eines Objekts der Klasse ‚Empfängerkategorie'		x	
Verarbeitungskategorien	Assoziation für die Zuweisung eines Objekts der Klasse ‚Verarbeitungskategorien'			x
Garantie	Assoziation für die Zuweisung eines Objekts der Klasse ‚Garantien'		x	x

Tabelle 14: Attribute der Klasse ‚Datenübermittlungen'

Die aus Tabelle 15 ersichtlichen Attribute wurden für die Klasse ‚Garantien' definiert. Die zwei Attribute sind für die Ontologie des VVU und des VVA relevant. Gemäss DSGVO, Artikel 30, Abs. 1e und Abs. 2c ist die Dokumentierung geeigneter Garantien vorgesehen. Für die Umsetzung wurde die Ausführung in der Verordnung so interpretiert, dass die Dokumentierung aus einer Bezeichnung und einer Beschreibung besteht. Dafür wurde jeweils ein Attribut erfasst. Wie aus der Beschreibung zur Bezeichnung in Tabelle 15 hervorgeht, wird der Angemessenheitsbeschluss ebenfalls als ‚Garantie' geführt, obwohl dieser gemäss DSGVO, Artikel 30, Abs. 1e und Abs. 2c nicht als eigentliche Garantie zählt. Den Angemessenheitsbeschluss als Garantie zu führen, dient dazu, dass es direkt erkannt werden kann, wenn keine eigentliche Garantie benötigt wird. Dies hat sich bei der Instanziierung (Prototyp in Form einer Access-Datenbank) herausgestellt.

Attribut	Beschreibung	Optional	VVU	VVA
Bezeichnung	Bezeichnung, die sich auf die in der DSGVO genannten Garantien bezieht (vgl. DSGVO Art. 45, Abs. 3 und Art. 46, Abs. 2)		x	x
Beschreibung	Beschreibung, die die Garantien verdeutlicht		x	x

Tabelle 15: Attribute der Klasse ‚Garantien'

Für die Klasse ‚Löschfristen' wurden die zwei Attribute definiert, die nur für das VVU relevant sind, da im VVA die Angabe von Löschfristen nicht vorgesehen ist. Es ist davon auszugehen, dass die Löschfristen vom auftraggebenden Verantwortlichen definiert sind und in seinem VV geführt und überwacht werden sowie dass der Auftragsverarbeiter nicht dafür verantwortlich ist. Die Attribute dieser Klasse werden in Tabelle 16 verdeutlicht.

Attribut	**Beschreibung**	**Optional**	**VVU**	**VVA**
Löschfrist	Zeitangabe oder kurze Bezeichnung		**x**	
Beschreibung	Beschreibung, die die Löschfrist begründet		**x**	

Tabelle 16: Attribute der Klasse ‚Löschfristen'

Die drei aus Tabelle 17 hervorgehenden Attribute der Klasse ‚Schutzmassnahmen' dienen der Dokumentation der Schutzmassnahmen. Da sowohl technische als auch organisatorische Schutznassnahmen definiert werden sollten, wurde das Attribut ‚Typ' definiert, das für jede Schutzmassnahme verdeutlicht, wie sie beschaffen ist. Die Schutzmassnahmen sind sowohl im VVU als auch im VVA zu führen.

Attribut	**Beschreibung**	**Optional**	**VVU**	**VVA**
Bezeichnung	Bezeichnung, die auf die getroffene Schutzmassnahme hinweist (beispielsweise bezogen auf DSGVO, Art. 32, Abs. 1)		**x**	**x**
Beschreibung	Beschreibung, wie die Schutzmassnahme umgesetzt wird, oder Verweis auf bestehende Dokumentation		**x**	**x**
Typ	Art der Schutzmassnahme (technisch oder organisatorisch)		**x**	**x**

Tabelle 17: Attribute der Klasse ‚Schutzmassnahmen'

In der Klasse ‚Auftragsverarbeiter' werden nur im VVU Attribute aufgeführt, da der Auftragsverarbeiter im VVA in der Klasse ‚Verantwortungen' geführt wird. Der Auftragsverarbeiter muss im VVU nur im Rahmen der Empfängerkategorien geführt (vgl. Kapitel

5.3.14) und nicht explizit genannt werden. Daher sind die neun Attribute als optional definiert. Damit ein Verantwortlicher weiss, welche Auftragsverarbeiter beauftragt wurden, erscheint es dennoch sinnvoll, den Auftragsverarbeiter im VV aufzuführen. Die definierten Attribute gehen aus der folgenden Tabelle 18 hervor.

Attribut	**Beschreibung**	**Optional**	**VVU**	**VVA**
Unternehmen	Name des Unternehmens des auftragsnehmenden Auftragsverarbeiters	**x**	**x**	
Name	Name des Auftragsverarbeiters bzw. Verantwortlichen im Unternehmen	**x**	**x**	
Vorname	Vorname des Auftragsverarbeiters bzw. Verantwortlichen im Unternehmen	**x**	**x**	
Strasse/Nr.	Adressdaten des Auftragsverarbeiters bzw. Verantwortlichen im Unternehmen	**x**	**x**	
Postleitzahl		**x**	**x**	
Ort		**x**	**x**	
Email	E-Mail-Adresse des Auftragsverarbeiters bzw. Verantwortlichen im Unternehmen	**x**	**x**	
Telefonnummer	Telefonnummer des Auftragsverarbeiters bzw. Verantwortlichen im Unternehmen	**x**	**x**	
Empfängerkategorie	Assoziation für die Zuweisung eines Objekts der Klasse ‚Empfängerkategorien'	**x**	**x**	

Tabelle 18: Attribute der Klasse ‚Auftragsverarbeiter'

Die aus der nachstehenden Tabelle 19 hervorgehenden zwei Attribute der Klasse ‚Verarbeitungskategorien' sind nur für das VVA relevant. Eine Beschreibung der Verarbeitungskategorien ist nicht explizit vorgesehen und daher als optional definiert, jedoch aus organisatorischen Gründen für den Auftragsverarbeiter dennoch sinnvoll.

Attribut	**Beschreibung**	**Optional**	**VVU**	**VVA**
Verarbeitungskategorien	Bezeichnung einer eindeutigen Verarbeitungskategorie			**x**
Beschreibung	Erläuterungen zur Verarbeitungskategorie mit Bezug auf die angebotenen Leistungen als Auftragsverarbeiter	**x**		**x**

Tabelle 19: Attribute der Klasse ‚Verarbeitungskategorien'

Die zwei Attribute der Klasse ‚Rechtsgrundlage' sind als optional definiert, da die Klasse ‚Rechtsgrundlage' ebenfalls optional ist, da nicht direkt aus DSGVO, Artikel 30 hervorgeht. Die Rechtsgrundlage wird nur in der Ontologie für das VVU geführt, da der Auftragsverarbeiter nicht dafür zuständig ist, weil er im Auftrag eines Verantwortlichen handelt. Die Verantwortung dafür, dass eine gültige Rechtsgrundlage vorhanden ist, liegt bei dem Verantwortlichen. Die Attribute dieser Klasse werden in Tabelle 20 verdeutlicht.

Attribut	**Beschreibung**	**Optional**	**VVU**	**VVA**
Rechtsgrundlage	Bezeichnung, die sich auf die in der DSGVO genannten Rechtsgrundlagen bezieht (vgl. DSGVO, Art. 6)	**x**	**x**	
Beschreibung	Beschreibung, die die Rechtsgrundlage verdeutlicht	**x**	**x**	

Tabelle 20: Attribute der Klasse ‚Rechtsgrundlage'

Ebenso wie bei der Klasse ‚Rechtsgrundlage' handelt es sich bei der Klasse ‚Dateisystem' um eine optionale Klasse, was bedeutet, dass auch für diese Klasse alle Attribute als optional definiert sind. Für die Klasse ‚Dateisystem' wurden die zwei aus Tabelle 21 hervorgehenden Attribute definiert, die sowohl für die Ontologie des VVU als auch für die Ontologie des VVA relevant sind.

Attribut	**Beschreibung**	**Optional**	**VVU**	**VVA**
Anwendung	Anwendung/Software, in der die Verarbeitungstätigkeit ausgeführt wird, oder physisches Verzeichnis, in dem die für die Verarbeitungstätigkeit benötigten Daten abgelegt sind	**x**	**x**	**x**
Beschreibung	Erläuterungen zu Anwendungen/Software	**x**	**x**	**x**

Tabelle 21: Attribute der Klasse ‚Dateisystem'

Abschliessend werden nun noch die Attribute der ebenfalls optionalen Klasse ‚Zuständigkeit' aufgezeigt (vgl. Tabelle 22). Die drei Attribute dieser Klasse dienen dazu, die fachlich für die Verarbeitung verantwortliche Person bzw. Rolle oder Funktion zu erfassen.

Attribut	Beschreibung	Optional	VVU	VVA
Name	Name des fachlich für die Verarbeitungs-tätigkeit Zuständigen	x	x	
Vorname	Name des fachlich für die Verarbeitungs-tätigkeit Zuständigen	x	x	
Rolle	Rolle/Funktion des Zuständigen im Unter-nehmen	x	x	

Tabelle 22: Attribute der Klasse ‚Zuständigkeit'

5.6.2 Restriktionen der Attribute

Wie gemäss der Methodologie von Noy und McGuiness (2001, S. 4ff) vorgesehen ist, werden nun die Restriktionen für die Attribute definiert. Die Restriktionen beschreiben beziehungsweise beschränken die Menge der möglichen Werte der Attribute. Mit Ausnahme der Attribute ‚Telefonnummer', und ‚Postleitzahl' deren Menge der möglichen Werte mit dem Datentyp ‚Integer' eingeschränkt werden, wird allen Attributen der Datentyp ‚String' zugewiesen. Da sich die Zuweisung der Datentypen zwischen den unterschiedlichen Attributen nur geringfügig unterscheidet, wird von einer Darstellung im Klassendiagramm abgesehen.

5.7 Instanziierung

Abschliessend sieht die Methodologie von Noy und McGuiness (2001, S. 4ff) das Erzeugen von Instanzen der zuvor definierten Klassen vor. Für die Instanziierung wurde eine Access-Datenbank erstellt (Tabellen vgl. Anhang viii), die der der Überprüfung der Ontologien dient. In der Access-Datenbank wurden für die Attribute der Klassen beispielhaft Instanzen kreiert. Die Verwendung der Access-Datenbank zum Führen eines VV in der Praxis stand nicht im Fokus, weshalb die Access-Datenbank in der aktuellen Form dafür nicht besonders geeignet ist.

6 Ontologien der Datenschutzverzeichnisse

Aus den Ausführungen in Kapitel 5 gehen eine Ontologie für ein Datenschutzverzeichnis für Unternehmen (bezeichnet als ‚Ontologie des VVU') und eine Ontologie für ein Da-

tenschutzverzeichnis für Auftragsverarbeiter (bezeichnet als ‚Ontologie des VVA') hervor. Für die ‚Ontologie des VVU' wurden 23 Klassen und 34 Assoziationen identifiziert, für die ‚Ontologie des VVA' hingegen 17 Klassen und 25 Assoziation. Das VVU ist demnach komplexer als das VVA, was bedeutet, dass das Führen des VV für Auftragsverarbeiter etwas weniger aufwändig ist als für Verantwortliche. Eine Übersicht der identifizierten Klassen und Assoziationen ist in Abbildung 9 dargestellt. Hieraus wird ebenfalls erkennbar, wie viele Klassen und Assoziationen einen beschreibenden Charakter haben und wie viele davon ‚Kernklassen' und ‚Kernassoziationen' sind.

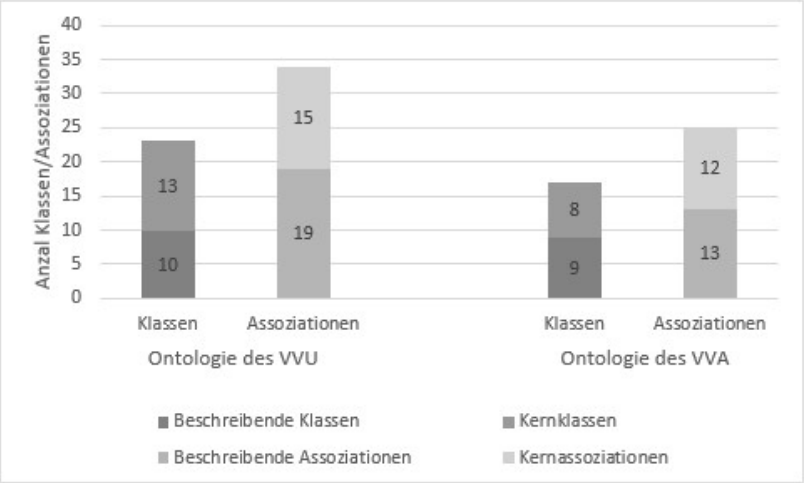


Abbildung 9: Übersicht identifizierte Klassen und Assoziationen

Abgeleitet aus den Beschreibungen zu den Assoziationen in Kapitel 5.5 wurden Bezeichnungen zu den Assoziationen hinzugefügt, zu denen jeweils die Leserichtung mit ‚<' oder ‚>' angezeigt wird. Dies dient dem besseren Verständnis der Ontologien.

Aus Abbildung 10 wird nun die komplette ‚Ontologie des VVU' ersichtlich, die eines der aus dieser Masterthesis hervorgehenden Artefakte veranschaulicht:

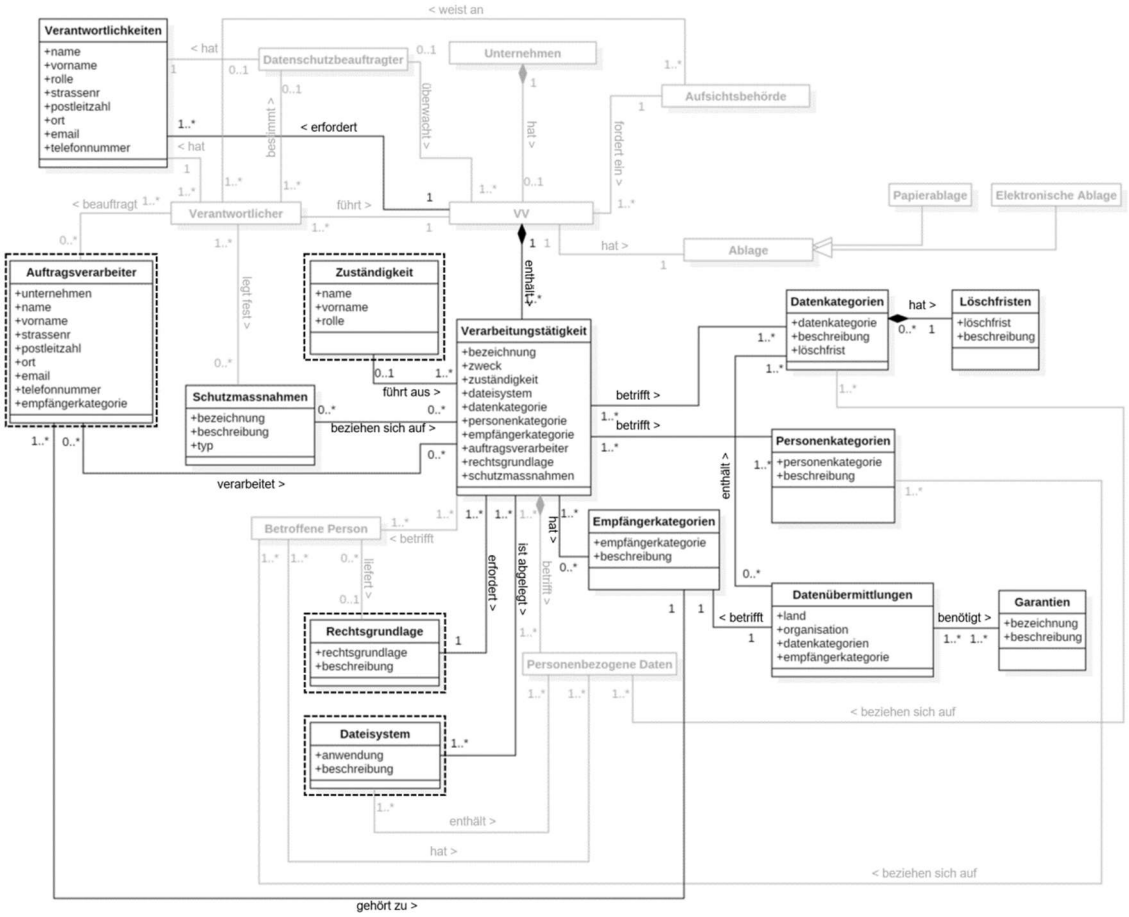


Abbildung 10: Ontologie des VVU

Legende

	Beschreibende Klassen und Assoziationen
	Kernklassen und Assoziationen
< oder >	Leserichtung der Beschriftung
	Optionale Klasse

Das zweite Artefakt, die ‚Ontologie des VVA', geht aus Abbildung 11 hervor. Aus Anhang xiii gehen Kurzbeschreibungen zu den Klassen der Ontologien hervor, die Bestandteile noch besser verdeutlichen. Dies Kurzbeschreibungen finden ausserdem Verwendung in den interaktiven Darstellungen der Ontologien, die separat erhältlich sind.

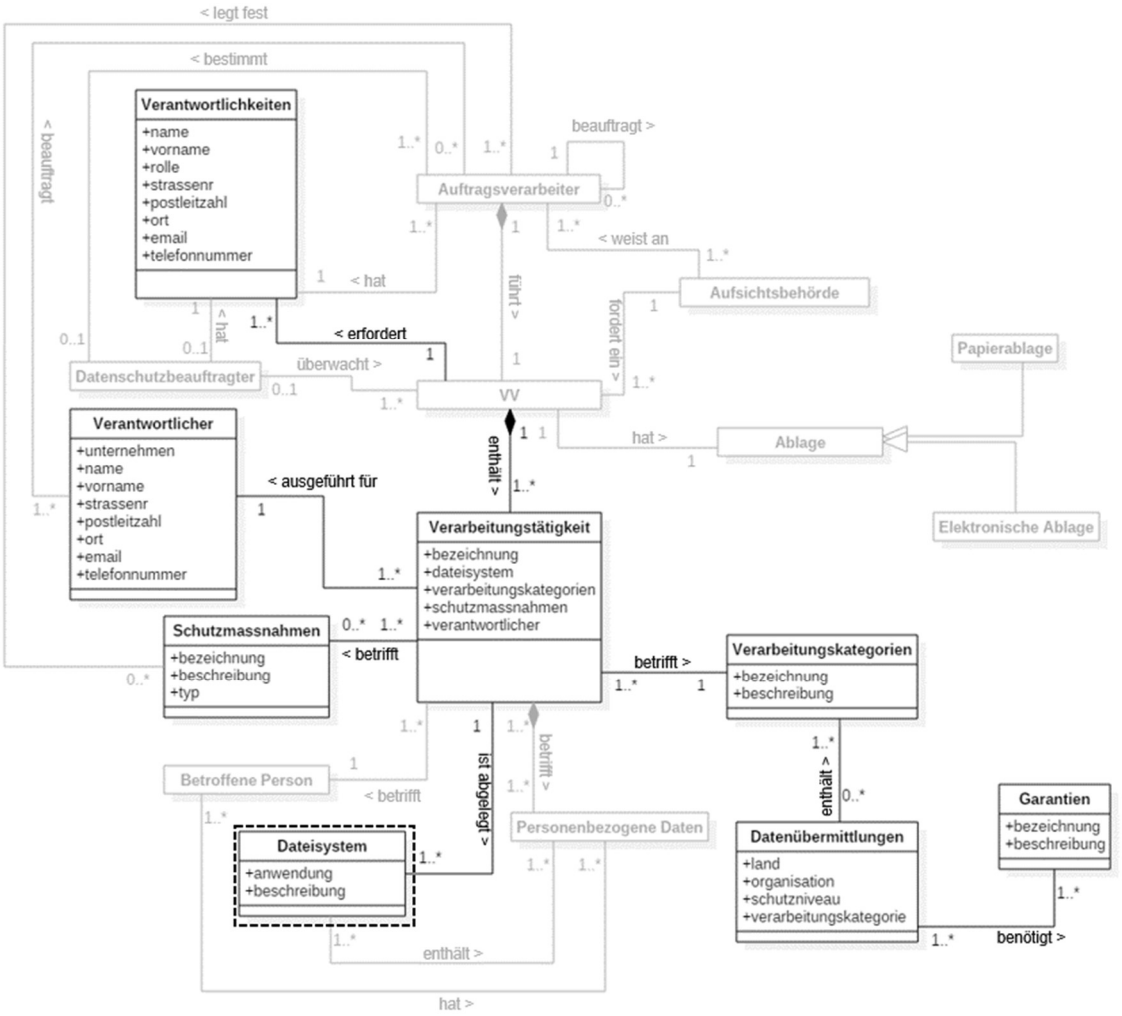


Abbildung 11: Ontologie des VVA

Legende

	Beschreibende Klassen und Assoziationen
	Kernklassen und Assoziationen
< oder >	Leserichtung der Beschriftung
	Optionale Klasse

Aus der Herleitung der Ontologien ergibt sich als zusätzliches Artefakt, eine Mustervorlage für den Bericht an die Aufsichtsbehörde (vgl. Anhang x)

7 Fazit

Abschliessend folgen nun die kritische Diskussion der Resultate, die Einschränkungen der Untersuchung sowie ein Ausblick auf die weiterführende Forschung.

7.1 Diskussion

Die Untersuchungen im Zusammenhang mit der DSGVO und mit dem E-DSG haben gezeigt, dass im Bereich der Datenschutzverzeichnisse gemäss den neuen Gesetzgebungen Klärungsbedarf besteht. Um das Bewusstsein für die neuen Anforderungen zu stärken, ist ein gemeinsames Verständnis der Entscheidungsträger im Unternehmen notwendig. Abgesehen von Deutschland, das von Seiten des BDSG bereits ein ähnliches Verzeichnis kennt, ist es in den anderen von den neuen Gesetzen betroffenen Länder eine Neuerung, dass die Verarbeitungstätigkeiten in einem solchen Detailierungsgrad erfasst werden müssen. Die neuen Gesetze sind sehr auf Informatik bezogen, was in Unternehmen die vermehrte Zusammenarbeit der für die rechtliche Seite Zuständigen mit den Zuständigen seitens der Informatik erfordert. Ein formales Modell, das die Ausführungen in den Gesetzestexten verdeutlicht, könnte dieser Anforderung gerecht werden. Im Fachbereich der Informatik sind solche Modelle weit verbreitet und die Fachleute sind folglich damit vertraut. Zu anderen Bereichen der DSGVO wurden bereits Ontologien publiziert, die die Zusammenhänge der Ausführungen in der Verordnung verdeutlichen (vgl. Kapitel 5.2). Da Verzeichnisse per Definition sehr formal sind, eignet sich die Abbildung dieses Teils der neuen Datenschutzgesetze besonders, um ihn als Ontologie zu verdeutlichen.

Durch die Verwendung einer strukturierten Methodologie, die klare Schritte für die Erstellung von Ontologien und ein iteratives Vorgehen vorsieht, sind die ‚Ontologie des VVU' sowie die ‚Ontologie des VVA' entstanden, die als Artefakte aus dieser Masterthesis hervorgehen. Die Entscheidung, zwei Ontologien zu erstellen, wurde im Verlaufe der Herleitung der Ontologien gefällt, da sich gezeigt hat, dass sich die Anforderungen an die Datenschutzverzeichnisse wesentlich unterscheiden. Das iterative Vorgehen half dabei, Informationen aus der Validierung der Ontologie durch Expertinnen und Experten sowie Erkenntnisse, die durch die Instanziierung in Form einer Access-Datenbank gewonnen wurden, in die Artefakte einfliessen zu lassen, was die Ergebnisse aufwertet.

Die validierten Artefakte zeigen die Verbindungen der Bestandteile eines Datenschutzverzeichnisses nach DSGVO, Artikel 30 beziehungsweise E-DSG, Artikel 11 formal auf

und lassen somit schneller Rückschlüsse auf die Zusammenhänge der Bestandteile zu. Durch die Betrachtung bestehender Ansätze, die Experteninterviews sowie die Instanziierung konnten ausserdem weitere Verbindungen und Bestandteile identifiziert werden, die für ein nützliches Datenschutzverzeichnis relevant sind. Die zu Beginn der Herleitung der Ontologien erläuterten Begriffe und Zusammenhänge können in der Praxis helfen, ein einheitliches Verständnis unter den Beteiligten zu schaffen.

Anhand der Erläuterung zu den als relevant identifizierten Begriffen und Zusammenhänge konnten 24 Klassen identifiziert werden, die entweder für die ‚Ontologie des VVU', die ‚Ontologie des VVA' oder für beide Ontologien von Relevanz sind. Ausserdem wurden 44 Assoziationen zwischen den Klassen ermittelt, die die Zusammenhänge verdeutlichen. Einige sind auf Herleitungen und Interpretationen der Autorin zurückzuführen. Dokumentiert beziehungsweise gekennzeichnet sind auch Klassen und Assoziationen sowie Attribute, die optional sind, das heisst nicht direkt aus dem Gesetz hervorgehen. Ebenfalls sind Klassen und Verbindungen gekennzeichnet, die für die aktuelle Verwendung des Modells ‚nur' einen beschreibenden Charakter haben.

7.2 Kritische Würdigung

Die Resultate der vorliegenden Masterthesis stammen aus den Ausführungen in der DSGVO und dem E-DSG sowie aus der Literaturanalyse und drei Experteninterviews. Bei der Literaturanalyse wurde nur ansatzweise systematisch vorgegangen. Mit einer systematischeren Vorgehensweise hätte sich die relevante Literatur gründlicher identifizieren lassen. Da sich bei der Recherche jedoch gezeigt hat, dass die Anzahl der Publikationen noch überschaubar ist, wurde von einem systematischeren Vorgehen abgesehen. Ebenso ist die geringe Anzahl der durchgeführten Interviews kritisch zu beurteilen, obwohl gemäss der Einschätzung der Interviewergebnisse wohl nur wenige zusätzliche Erkenntnisse hinzugekommen wären, wenn mehr Interviews geführt worden wären. Ausserdem wurde kein Interview mit einem Auftragsverarbeiter durchgeführt, was möglicherweise in diesem Bereich zu weiteren Erkenntnissen geführt hätte.

Die Methodologie, auf die sich die Herleitung der Ontologien stützt, wurde gewählt, da sie sich als sehr passend für die geplante Untersuchung erwiesen hat. Es ist jedoch nicht anzunehmen, dass sich die Wahl der Methodologie entscheidend auf die Ergebnisse ausgewirkt hat.

Ob anhand der gewählten Methoden alle relevanten Begriffe identifiziert wurden, ist kritisch zu beurteilen. Ausserdem konnten die identifizierten Begriffe teilweise nicht genau spezifiziert werden beziehungsweise das Vorgehen für die Ermittlung der zugehörigen Instanzen aufgrund fehlender Informationen nicht beschrieben werden.

Bei der Bestimmung der Zusammenhänge musste teilweise auf Herleitungen sowie eigene Interpretationen gesetzt werden, da sie sich anhand des aktuellen Stands der Forschung und den durchgeführten Untersuchungen nicht eindeutig feststellen liessen. Dies ist unter anderem darauf zurückzuführen, dass die Handhabung der Rechtsprechung noch unklar ist. Für die Darstellung der Artefakte wurde auf die UML-Notation sowie Ontologien gesetzt, was für ein Publikum mit Informatikwissen sehr geeignet erschien. Die Darstellung in einer anderen Form würde die Artefakte einem grösseren Publikum eröffnen.

7.3 Ausblick

Auf der Grundlage der neu entwickelten Artefakte ergeben sich neue Forschungsfelder. Das Modell kann einerseits als Basis für die Entwicklung einer Methode für die Einführung eines Datenschutzverzeichnisses dienen, anderseits können die Informationen verwendet werden, um die Thematik in einem Wiki zu veranschaulichen. Mit einer Veröffentlichung des formalen Modells könnte ausserdem die Grundlage für ein generisches Datenmodell geschaffen werden, das einem standardisierten Aufbau von Softwarelösungen dient. Das anfangs erwähnte Informationsmodell von Anke et al. (2016, S. 72) könnte durch die Erkenntnisse erweitert werden.

Begriffe und Zusammenhänge könnten mit neuen Erkenntnissen, die sich aus der Rechtsprechung und der Erfahrung mit dem VV noch ergeben müssen, besser spezifiziert werden.

Ein Vorgehen für die Festlegung von Daten- und Personenkategorien konnte nicht identifiziert werden und wurde im Rahmen dieser Masterthesis auch nicht erarbeitet. Die Untersuchungen haben jedoch gezeigt, dass ein solches Vorgehen für die Praxis sinnvoll wäre. Hieraus ergibt sich demnach ein weiteres Forschungsfeld.

7.4 Eigene Einschätzung

Mit dieser Untersuchung ist es mir gelungen, zwei neue Artefakte zu bilden, die im Zusammenhang mit der Forschung zum VV eine gewisse Relevanz haben könnten. Für die Herleitung der Artefakte habe ich mich intensiv mit den neuen Datenschutzgesetzen, das

heisst mit der DSGVO und dem E-DSG auseinandergesetzt, womit ich mein Wissen in diesem Bereich ausbauen konnte.

Eine grosse Herausforderung bei der Herleitung der Artefakte stellte die Dokumentation dar, die ich aufgrund der iterativen Vorgehensweise immer wieder anpassen musste. Alle Verbindungen zwischen den Bestandteilen zu identifizieren, zu beschreiben und zu begründen, gestaltete sich ebenfalls herausfordernd. Durch stetige quantitative Überprüfungen ist mir dies, meiner Ansicht nach, letztendlich gelungen.

8 Literaturverzeichnis

2B Advice GmbH - Deutsch - Datenschutzsoftware. (o. J.). *2B Advice PrIME*. Abgerufen von https://www.2b-advice.com/GmbH-de/Datenschutzsoftware

activeMind. (o. J.). Internationaler Vergleich der Datenschutz-Gesetze. Abgerufen 31. Oktober 2017, von https://www.activemind.legal/law/

Anke, J., Berning, W., Schmidt, J., & Zinke, C. (2016). IT-gestützte Methodik zum Management von DatenschutzanforderungenIT-based Methodology for the Management of Data Protection Requirements. *HMD Praxis der Wirtschaftsinformatik*, *54*(1), 67–83. https://doi.org/10.1365/s40702-016-0283-0

Balthasar, M. (2018, Januar). *Die neue Datenschutz-Grundverordnung (DSGVO/GDPR) und ihre Auswirkungen*. Abgerufen von https://www.infosec.ch/downloads/referate/MSI20180122/MSI_20180122_02_Balthasar_00.pdf

Bartolini, C., & Muthuri, R. (2015). Reconciling Data Protection Rights and Obligations: An Ontology of the Forthcoming EU Regulation. Gehalten auf der Workshop on Language and Semantic Technology for Legal Domain (LST4LD), Hissar, Bulgaria. Abgerufen von http://orbilu.uni.lu/bitstream/10993/21969/1/main.pdf

Berufsverband der Datenschutzbeauftragten Deutschlands. (2017, Juni 30). Mustervorlage - Verzeichnis von Verarbeitungstätigkeiten - Verantwortlicher.

Bitcom. (2017). Das Verarbeitungsverzeichnis - Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 EU-Datenschuzt-Grundverordnung. Abgerufen von https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Verarbeitungsverzeichnis-online.pdf

Blodon James. (o. J.). Data Classification Solutions & Software. Abgerufen 4. Dezember 2017, von https://www.boldonjames.com/data-classification/

Bühlmann, L. (2017, Februar 14). Totalrevision DSG: wichtigste Eckpunkte des Vernehmlassungsentwurfes für ein neues Schweizer Datenschutzgesetz. Abgerufen 19. November 2017, von https://www.mll-news.com/totalrevision-dsg-wichtigste-eckpunkte-des-vernehmlassungsentwurfes-fuer-ein-neues-schweizer-datenschutzgesetz/

Bundesministeriums der Justiz und für Verbraucherschutz. Bundesdatenschutzgesetz (BDSG) (2003). Abgerufen von https://www.gesetze-im-internet.de/bdsg_1990/BDSG.pdf

Bundesrat. (2018, März 7). Stellungnahme des Bundesrats zur Interpellation Fiala (17.4088): Umsetzungsfragen zur EU-Datenschutz-Grundverordnung. Abgerufen 19. Mai 2018, von http://datenrecht.ch/stellungnahme-des-bundesrats-zur-interpellation-fiala-17-4088-umsetzungsfragen-zur-eu-datenschutz-grundverordnung/

Bundesversammlung der Schweizerischen Eidgenossenschaft. (1992). *Bundesgesetz über den Datenschutz (DSG)*. Bern.

Christian, S. (2018, April 24). Kurzinterview zum Thema «Software für Verzeichnisse von Verarbeitungstätigkeiten».

Commission for the protection of privacy. (2017, Juli). Model voor een Register van de verwerkingsactiviteiten. Abgerufen 8. Mai 2018, von https://www.privacycommission.be/nl/model-voor-een-register-van-de-verwerkingsactiviteiten

Datenschutzbeauftragter INFO. (2016a). EU-Datenschutz-Grundverordnung: Das müssen Sie wissen. Abgerufen 31. Oktober 2017, von https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/

Datenschutzbeauftragter INFO. (2016b, November 4). Verzeichnis von Verarbeitungstätigkeiten – Infos & Tipps zur Umsetzung. Abgerufen 31. Oktober 2017, von https://www.datenschutzbeauftragter-info.de/verzeichnis-von-verarbeitungstaetigkeiten-infos-tipps-zur-umsetzung/

Datenschutzbeauftragter INFO. (o. J.). Verfahrensverzeichnis. Abgerufen 31. Oktober 2017, von https://www.datenschutzbeauftragter-info.de/fachbeitraege/verfahrensverzeichnis/

Datenschutzkonferenz (DSK). (2018, Februar). Hinweise zum Verzeichnis von Verarbeitungstätigkeiten Art. 30 DS-GVO. Abgerufen von https://www.lda.bayern.de/media/dsk_hinweise_vov.pdf

Dehmel, S., & Thiel, B. (2017, September). *EU-Datenschutzgrundverordnung – Wie gut ist die deutsche Wirtschaft vorbereitet? - Ergebnisse einer Umfrage des Bitcoms*. Gehalten auf der Privacy Conference, Berlin.

Deichmann-Fuchs - Business Solutions. (o. J.). *Verfahrensverzeichnis mit den wichtigsten Verfahrensbeschreibungen im Unternehmen*. Abgerufen von https://www.deichmann-fuchs.de/datenschutz/bdsg---verfahrensverzeichnis/bdsg-verfahrensverzeichnis-mit-den-wichtigsten-verfahrensbeschreibungen-im-unternehmen.artikel.html

Deloitte. (2017). Deloitte Umfrage: EU-Datenschutzgrundverordnung, 4.

Diamantopoulou, V., Angelopoulos, K., Pavlidis, M., & Mouratidis, H. (2017). A Metamodel for GDPR-based Privacy Level Agreements. Gehalten auf der ER Forum 2017, Cabanillas, Spanien. Abgerufen von http://ceur-ws.org/Vol-1979/paper-08.pdf

Eberle, F. (2017, März 6). Leitfaden zum Verfassen schriftlicher Arbeiten.

Europäisches Parlament und Europäischer Rat. Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, EUR-Lex - 31995L0046 - DE § (1995). Abgerufen von http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:31995L0046&from=DE

Europäisches Parlament und Europäischer Rat. (2016). *Europäische Datenschutz-Grundverordnung (DSGVO)*. Brüssel.

Fieldfisher. (2017, Juli). Belgian DPA publishes recommendation on GDPR record keeping obligation [Unternehmenswebseite]. Abgerufen 8. Mai 2018, von https://privacylawblog.fieldfisher.com/2017/belgian-dpa-publishes-recommendation-on-gdpr-record-keeping-obligation

Gartner. (2017, Juli). Hype Cycle for Risk Management, 2017. Abgerufen 11. November 2017, von https://www.gartner.com/document/3764963?ref=solrAll&refval=193684436&qid=b79ca0b9a6e0f4cf96a3c2931a274f7d

Gesellschaft für Datenschutz und Datensicherheit. (2017, April). GDD-Praxishilfe DS-GVO 5 - Verzeichnis von Verarbeitungstätigkeiten. Abgerufen von https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf

Gola, P. (2017). *DS-GVO, Kommentar - Datenschutz-Grundverordnung VO (EU) 2016/679 - Ln*. München: Beck. Abgerufen von https://www.schulthess.com/buchshop/detail/ISBN-9783406695438/Gola-Peter-Hrsg.-Eichler-Carolyn-Hrsg.-Franck-Lorenz-Hrsg.-Klug-Christoph-Hrsg.-Lepperhoff-Niels-Hrsg.-Nguyen-Alexander-Hrsg./Datenschutz-Grundverordnung-VO-EU-2016679

Guarino, N. (1998). Formal Ontology and Information Systems (S. 3–15). Gehalten auf der FOIS, Trento (IT): IOS Press, Amsterdam.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Q.*, *28*(1), 75–105.

Israel, S., & Carli, L. D. (2018, Januar 18). Schweiz riskiert bei Datenschutz neuen Konflikt mit der EU. *Tages-Anzeiger*. Abgerufen von https://www.tagesanzeiger.ch/schweiz/standard/jetzt-auch-noch-der-datenschutz/story/13706225

Kruse, J. (2015). *Qualitative Interviewforschung: ein integrativer Ansatz* (2., überarbeitete und ergänzte Auflage, Online-Ausgabe). Weinheim: Beltz Juventa. Abgerufen von http://www.content-select.com/index.php?id=bib_view&ean=9783779941620

Ludewig, J. (2003). Models in software engineering – an introduction. *Software and Systems Modeling*, *2*(1), 5–14. https://doi.org/10.1007/s10270-003-0020-3

MME. (2016). EU Datenschutz - einschneidende Konsequenzen für CH-Unternehmen - MME - Datenschutz. Abgerufen 5. November 2017, von https://www.mme.ch/de/magazin/eu_datenschutz_einschneidende_konsequenzen_fuer_ch_unternehmen/

Noy, N. F., & McGuinness, D. (2001). Ontology Development 101: A Guide to Creating Your First Ontology. *Knowledge Systems Laboratory*, *32*.

Object Managment Group (OMG). (2017, Dezember). OMG Unified Modeling Language (UML) v2.5.1. Abgerufen von https://www.omg.org/spec/UML/2.5

Ontologie. (online). Duden online. Abgerufen 17. Mai 2018, von https://www.duden.de/rechtschreibung/Ontologie

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, *24*(3), 45–77.

Polenz, S. (2018, März). *Startschuss DSGVO: Die wichtigsten Neuerungen für Unternehmen auf einen Blick*.

Raoul Egeli. (2016, November 17). Revision der Europäischen Datenschutz Grundverordnung und ihre Folgen für die Schweizer Unternehmen. Abgerufen 17. Oktober 2017, von https://www.creditreform.ch/news/presse/pressemitteilungen/news-detail/revision-der-europischen-datenschutz-grundverordnung-und-ihre-folgen-fr-die-schweizer-unternehmen.html

Schäffter, M. (2017). *Verfahrensverzeichnis 2.0* (2. Aufl.).

Schweizerische Eidgenossenschaft. (2017). *Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz. Entwurf vom 15. September 2017.* Bern.

Schweizerische Eidgenossenschaft, die Europäische Union und die Europäische Gemeinschaft. SR 0.362.31 Abkommen vom 26. Oktober 2004 zwischen der Schweize-

rischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands (mit Anhängen und Schlussakte), Pub. L. No. SR 0.362.31 (2008). Abgerufen von https://www.admin.ch/opc/de/classified-compilation/20042363/index.html

Schweizerische Normen-Vereinigung (SNV) (Hrsg.). (2017, Mai 1). Informationstechnik - Sicherheitsverfahren Informationssicherheits-Managementsysteme Anforderungen (SN EN ISO/IEC 27001:2017).

Schweizerische Vereinigung für Qualitäts- und Management-Systeme (SQS). (2011, Februar). Datenschutz-managementsystem-Zertifizierung - Good Priv@cy und VDSZ.

Seidl-Nussbaumer, K. (2017, November). *Einführung DSGVO / GDPR und E-DSG - Grundzüge der neuen Datenschutz-Gesetzgebung*. Gehalten auf der Digital Summit v0.4, Zürich.

Stachowiak, H. (1973). *Allgemeine Modelltheorie*. Wien - New York: Springer. Abgerufen von https://archive.org/details/Stachowiak1973AllgemeineModelltheorie

Uschold, M., & King, M. (1995). Towards a Methodology for Building Ontologies. Abgerufen von http://www.aiai.ed.ac.uk/project/oplan/documents/1995/95-ont-ijcai95-ont-method.pdf

Varonis. (o. J.). Data Classification Software | Varonis Systems. Abgerufen 28. November 2017, von https://www.varonis.com/products/data-classification-framework/

Verband der Internetwirtschaft (eco). (2018, April 12). DSGVO hält deutsche Wirtschaft in Atem. Abgerufen 17. Mai 2018, von https://www.eco.de/presse/eco-verband-dsgvo-haelt-deutsche-wirtschaft-in-atem/

Verzeichnis. (online). Duden online. Abgerufen 17. Mai 2018, von https://www.duden.de/rechtschreibung/Verzeichnis

Voigt, P., & Von dem Bussche, A. (2017). Practical Implementation of the Requirements Under the GDPR. In *The EU General Data Protection Regulation (GDPR)* (S. 245–249). Springer, Cham. https://doi.org/10.1007/978-3-319-57959-7_10

Widmer, U. (2016). Datenschutz: Was uns das EU-Recht angeht. *Computerworld*, (6/2016), 62–65.

Widmer, U. (2017, Juni). *Relevanz der EU-DSGVO für Schweizer Unternehmen*. Zürich. Abgerufen von http://www.isss.ch/mitgliederbereich/archiv/events/ZuercherTagung/2017/02_ISSS-ZHR-Pr%c3%a4sentation_Dr.Ursula-Widmer.pdf

Wirtschaftskammern Österreichs. (2018a, April). Beispiel Verarbeitungsverzeichnis - Auftragsverarbeiter. Abgerufen von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-bsp-verarbeitungsverzeichnis-auftragsverarbeit.pdf

Wirtschaftskammern Österreichs. (2018b, April). EU-DSGVO-MUSTER-Verarbeitungsverzeichnis-Verantwortlicher.docx.

Wirtschaftskammern Österreichs. (2018c, Mai 16). EU-Datenschutz-Grundverordnung (DSGVO). Abgerufen 18. Mai 2018, von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html

9 Anhang

i Information Systems Research Framework

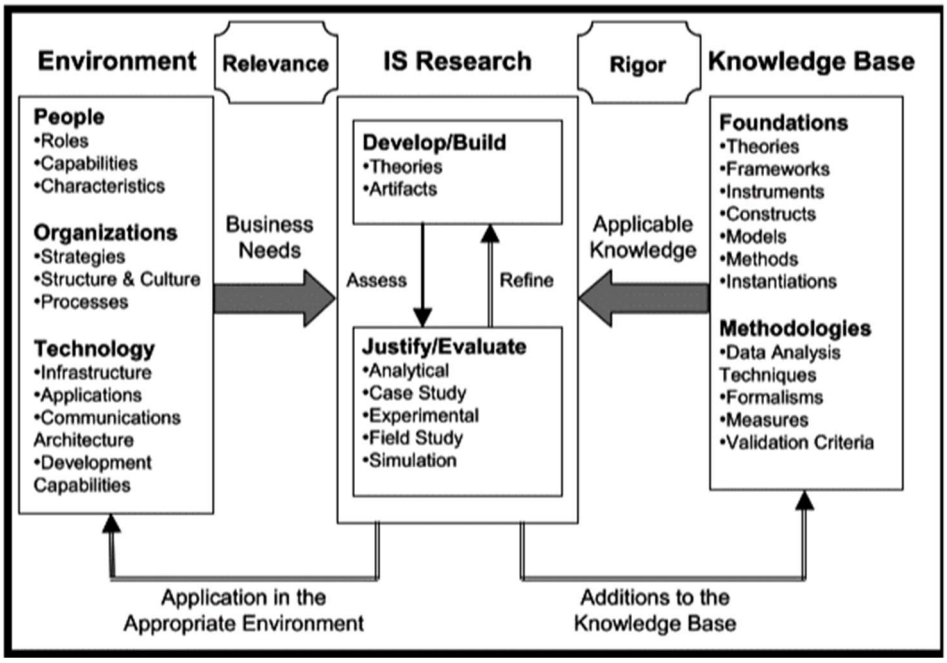


Abbildung 12: Information Systems Research Framework (Hevner et al., 2004)

ii Design Science Research Methology

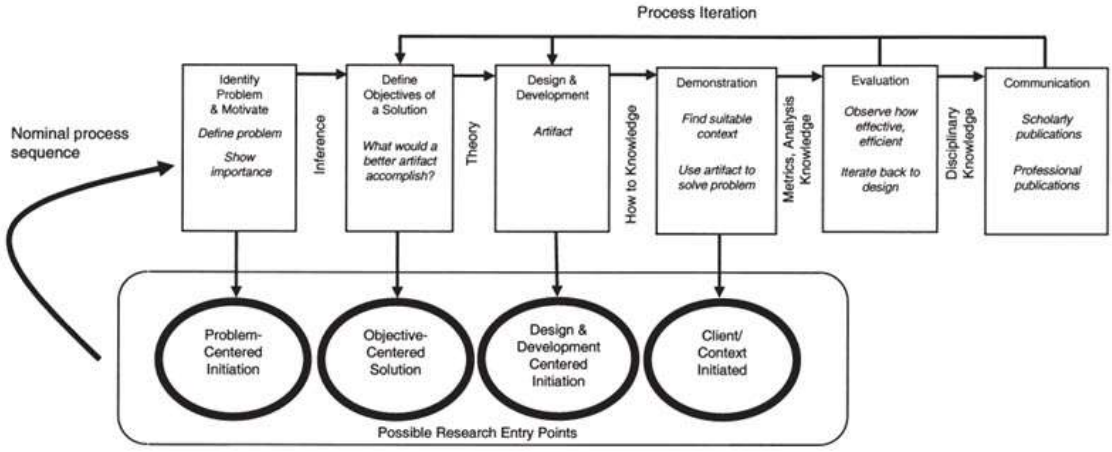


Abbildung 13: DSRM Process Model (Peffers et al., 2007)

iii Design Science Research Guidelines

Guideline	Description
Guideline 1: Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Guideline 2: Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Guideline 4: Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Abbildung 14: Design Science Research Guidelines (Hevner et al., 2004)

iv Relevante Gesetzesartikel

DSGVO Artikel 30

Artikel 30

Verzeichnis von Verarbeitungstätigkeiten

(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

b) die Zwecke der Verarbeitung; c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Kapitel 1 UnterKapitel 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien

f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Kapitel 1.

(2) Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;

b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;

c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Kapitel 1 UnterKapitel 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Kapitel 1.

(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

(4) Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

(5) Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Kapitel 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt

E-DSG Artikel 11

Art. 11 Verzeichnis der Bearbeitungstätigkeiten

Der E-DSG sieht anstelle der Dokumentationspflicht im Vorentwurf die Pflicht vor, ein Verzeichnis der Bearbeitungstätigkeiten zu führen. Die Vernehmlassung hat ergeben, dass zu wenig deutlich wurde, was die Dokumentationspflicht umfasst. Zudem wird das Verzeichnis der Bearbeitungstätigkeiten neu bei den allgemeinen Datenschutzbestimmungen eingeordnet. Dies verdeutlicht den engen Zusammenhang mit den Datenschutzgrundsätzen. Die Pflicht zur Führung eines Verzeichnisses ersetzt die Meldepflicht von Datensammlungen nach dem bisherigen Recht. Die Richtlinie (EU) 2016/680 sieht in Artikel 24 ein solches Verzeichnis vor; die Verordnung (EU) 2016/679 enthält in Artikel 30 eine analoge Vorschrift.

Die Pflicht zur Führung eines Verzeichnisses obliegt nach Kapitel 1 dem Verantwortlichen und dem Auftragsbearbeiter.

Kapitel 2 zählt die Mindestangaben auf, die das Verzeichnis enthalten muss. Dazu gehören zunächst die Identität (der Name) des Verantwortlichen (Bst. a) und der Bearbeitungszweck (Bst. b). Anzugeben ist weiter eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten (Bst. c). Mit Kategorien betroffener Personen sind typisierte Gruppen gemeint, die bestimmte gemeinsame Merkmale haben, wie z. B. «Konsumenten», «Armeeangehörige» oder «Arbeitnehmer». Die Kategorien bearbeiteter Personendaten bezeichnet die Art der

bearbeiteten Daten, z. B. besonders schützenswerte Personendaten. Aufgeführt werden müssen ebenfalls die Kategorien von Empfängern (Bst. d), denen gegebenenfalls die Personendaten bekanntgegeben werden. Auch hier sind wiederum typisierte Gruppen mit gemeinsamen Merkmalen gemeint, wie z. B. «Aufsichtsbehörden». Nach Buchstabe e muss das Verzeichnis die Aufbewahrungsdauer der Personendaten enthalten. Da sich die Aufbewahrungsdauer gemäss Artikel 5 Kapitel 4 nach dem Verwendungszweck richtet, lässt sich die Aufbewahrungsdauer mitunter nicht exakt festlegen, was durch die Wendung «wenn möglich» ausgedrückt wird. Sind genaue Angaben nicht möglich, muss das Verzeichnis zumindest die Kriterien enthalten, nach denen diese Dauer festgelegt wird. Gemäss Buchstabe f muss das Verzeichnis schliesslich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit nach Artikel 7 enthalten, soweit dies möglich ist. Durch die Beschreibung soll das Verzeichnis erlauben, Mängel in den Sicherheitsvorkehren aufzuzeigen. Die Wendung «wenn möglich» macht deutlich, dass die Beschreibung nur erfolgen soll, wenn die Vorkehrungen hinreichend konkret umschrieben werden können. Befinden sich diese Empfänger im Ausland, muss aus dem Verzeichnis auch hervorgehen, ob grundsätzlich die Voraussetzungen für Bekanntgabe ins Ausland erfüllt sind. Deswegen ist nach Buchstabe g der Staat anzugeben sowie die Garantien nach Artikel 13 Kapitel 2.

Die Aufzählung in Kapitel 2 macht deutlich, dass das Verzeichnis eine generelle Beschreibung der Bearbeitungstätigkeit ist, aus der sich Art und Umfang einer Bearbeitung ergibt. Hingegen ist das Verzeichnis kein Journal sämtlicher Datenbearbeitungen des Verantwortlichen oder des Auftragsbearbeiters, in dem protokollartig einzelne Handlungen aufgeführt werden. Das Verzeichnis ist mithin eine schriftliche Darstellung der wesentlichen Informationen zu allen Datenbearbeitungen eines Verantwortlichen oder Auftragsbearbeiters. Es lässt damit wesentliche Rückschlüsse darauf zu, ob eine Datenbearbeitung dem Grundsatz nach datenschutzkonform ausgestaltet ist oder nicht. Darüber hinaus korrelieren die Mindestangaben des Verzeichnisses in Kapitel 2 in vieler Hinsicht mit den Angaben, welche die betroffene Person aufgrund der Informationspflicht und des Auskunftsrechts erhalten muss.

Kapitel 3 enthält eine verkürzte Liste von Mindestangaben des Auftragsbearbeiters. Dieser muss insbesondere die Kategorien von Bearbeitungen aufführen, die im Auftrag jedes

Verantwortlichen durchgeführt werden. Das Verzeichnis des Auftragsbearbeiters enthält zudem die Identität der Verantwortlichen, für die er tätig ist.

Nach Kapitel 4 melden die Bundesorgane ihre Verzeichnisse dem Beauftragten. Dieser führt nach Artikel 50 ein Register der Bearbeitungstätigkeiten der Bundesorgane. Dieses wird veröffentlicht. Für Bundesorgane werden sich damit grundsätzlich keine Änderungen im Verhältnis zum bisherigen Recht ergeben. Denn sie müssen bereits jetzt ein Bearbeitungsreglement erarbeiten sowie eine Anmeldung der Datensammlung beim Beauftragten vornehmen.

Kapitel 5 gibt dem Bundesrat die Möglichkeit, für Unternehmen, die weniger als 50 Mitarbeiterinnen und Mitarbeiter beschäftigen, Ausnahmen von der Pflicht, ein Verzeichnis zu führen, vorzusehen. Dies dient insbesondere dazu, kleine und mittlere Unternehmen zu entlasten. Hierbei wird der Bundesrat jedoch nicht alleine auf die Grösse eines Unternehmens abstellen, sondern auch berücksichtigen, welche Risiken mit einer Datenbearbeitung einhergehen.

DBSG Artikel 4e

§ 4e Inhalt der Meldepflicht

Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind folgende Angaben zu machen:

1. Name oder Firma der verantwortlichen Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,

8. eine geplante Datenübermittlung in Drittstaaten,

9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

§ 4d Abs. 1 und 4 gilt für die Änderung der nach Satz 1 mitgeteilten Angaben sowie für den Zeitpunkt der Aufnahme und der Beendigung der meldepflichtigen Tätigkeit entsprechend.

v Vergleich: Verfahrensverzeichnis, Verzeichnis der Verarbeitungstätigkeiten und Verzeichnis der Bearbeitungstätigkeiten

Anforderungen	**DSGVO (Artikel 30)**	**E-DSG (Artikel 11)**	**BDSG (Artikel 4)**	**ISO27001**
Verantwortliche	**x**	**x**	**x**	**x**
Name(n) und Kontaktdaten des/der Verantwortlichen	**x**		**x**	
Name des Verantwortlichen (Identität)		**x**		
Name (n) und Kontaktdaten des/der Stellvertreter des Verantwortlichen	**x**		**x**	
Name (n) und Kontaktdaten des/der Datenschutzbeauftragten	**x**		**x**	
Zwecke der Verarbeitung/Bearbeitung	**x**	**x**	**x**	**x**
Beschreibung der Kategorien der betroffenen Personen	**x**	**x**	**x**	**x**
Beschreibung der Kategorien personenbezogener Daten	**x**	**x**	**x**	**x**

Kategorien von Empfängern, gegenüber denen personenbezogene Daten offengelegt worden sind oder offengelegt werden könnten*	**x**	**x**	**x**	**x**
*Auch Empfänger in Drittländern	**x**			
*Befindet sich ein Empfänger im Ausland, muss aus dem Verzeichnis hervorgehen ob die Voraussetzungen für die Bekanntgabe im Ausland erfüllt sind		**x**		
Übermittlungen von personenbezogenen Daten an ein Drittland inkl. Angabe des Drittlandes	**x**	**x**		
Geeignete Garantien bei Datenübermittlungen gemäss DSGVO Artikel 49 Kapitel 1 UnterKapitel 1	**x**			
Geeignete Garantien bei Datenübermittlungen gemäss DSG Artikel 13 Kapitel 2		**x**		
Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien (wenn möglich)	**x**		**x**	
Aufbewahrungsdauer der Personendaten (wenn möglich)		**x**		
Kriterien nach denen die Dauer festgelegt wird (falls Angabe genaue Aufbewahrungsdauer nicht möglich)		**x**		
Auftragsverarbeiter-/bearbeiter	**x**	**x**		
Namen und Kontaktdaten des/der Auftragsverarbeiter/s	**x**			
Namen und Kontaktdaten des Vertreters des/der Auftragsbearbeiter/	**x**			
Namen und Kontaktdaten jedes Verantwortlichen in dessen Auftrag der Auftragsverarbeiter tätig ist	**x**			
Namen (Identität) jedes Verantwortlichen in dessen Auftrag der Auftragsverarbeiter tätig ist				

Namen und Kontaktdaten jedes Vertreters eines Verantwortlichen in dessen Auftrag der Auftragsbearbeiter tätig ist	**x**			
Name (n) und Kontaktdaten des/der Datenschutzbeauftragten	**x**			
Kategorien von Verarbeitungen die im Auftrag des Verantwortlichen durchgeführt werden	**x**	**x**		
Übermittlungen von personenbezogenen Daten an ein Drittland inkl. Angabe des Drittlandes	**x**			
Geeignete Garantien bei Datenübermittlungen gemäss Artikel 49 Kapitel 1 UnterKapitel 1	**x**			
Allgemeine Beschreibung der technischen und organisatorischen Massnahmen unter Einbezug des Risikos*	**x**		**x**	
*Pseudonymisierung und Verschlüsselung personenbezogener Daten	**x**			
*Fähigkeit die Vertraulichkeit, Integrität, Verfügbarkeit und die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung dauerhaft sicherzustellen	**x**			
*Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen	**x**			
*Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung	**x**			
Verzeichnis schriftlich führen (auch in elektronischer Form möglich)	**x**			

Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung stellen	**x**			
Bundesrat hat die Möglichkeit Unternehmen die weniger als 50 Mitarbeitende beschäftigen, von der Pflicht auszunehmen. Der Entscheid hängt dabei auch davon ab, welche Risiken mit der Datenverarbeitung beim jeweiligen Unternehmen bestehen		**x**		
Unternehmen mit weniger als 250 Mitarbeitenden sind ausgenommen von der Verpflichtung ein Verzeichnis zu führen*	**x**			
*Ausnahme 1: Verarbeitung vorgenommen Verarbeitungen bringen ein Risiko für die Rechte und Freiheiten der betroffenen Personen	**x**			
*Ausnahme 2: Die Verarbeitung erfolgt regelmässig	**x**			
*Ausnahme 3: Die Verarbeitung enthält eine der folgenden Datenkategorien%	**x**			
%Daten aus denen die rassische und ethnische Herkunft hervor geht	**x**			
%Daten aus denen politische Meinungen hervor gehen	**x**			
%Daten aus denen religiöse Überzeugungen hervor gehen	**x**			
%Daten aus denen weltanschauliche Überzeugungen hervor gehen	**x**			
%Genetische oder biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person dienen	**x**			
%Gesundheitsdaten	**x**			
%Daten zum Sexualleben oder der sexuellen Orientierung einer Person	**x**			

*Ausnahme 4: Die Verarbeitung betrifft personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten	**x**			

Tabelle 23: Übersicht Verzeichnisse - DSGVO, E-DSG, BDSG (Europäisches Parlament und Europäischer Rat, 2016, Art. 30; Schweizerische Eidgenossenschaft, 2017, Art. 11; Bundesministeriums der Justiz und für Verbraucherschutz, 2003, Art. 4e)

vi Ergebnisse Datenbankrecherche

Suchbegriff/Datenbank	**WISO**	**Springer Link**	**EBSCO**	**Science Direct**	**Gartner**	**IEEE**	**ACM**
DSGVO	1'017	337	30	1	0	0	0
GDPR	549	549	946	373	229	29	10
Verzeichnis von Verarbeitungstätigkeiten	26	11	0	0	0	0	0
Verfahrensverzeichnis	85	88	0	0	0	0	0
Records of processing activities	0	15	1	8	2	0	0
Processing Operations Index	0	2	0	4	0	0	0
DSGVO AND Artikel 30	12	2	0	0	0	0	0
GDPR AND Article 30	0	14	0	9	1	0	0

Tabelle 24: Ergebnisse Datenbankrecherche vom 5. Mai 2018

vii Zusätzliche relevante Begriffe

Identifizierter Begriff	**Bezug**	**Anzahl Nennungen**	**Quellen**
Rechtsgrundlage	VVU	6	Munker (2017), Bitcom (2017), GDD (2017), DSK (2018), WKO (2018), Schäffter (2017)
Zuständigkeit (Verantwortliche MA)	VVU	4	DSK (2018), Interview A, Interview B, Interview C
Änderungshistorie	VVU/VVA	4	DSK (2018), Schäfer (2017), Interview A, Interview C
Risikobewertung	VVU	3	Munker (2017), Bitcom (2017), GDD (2017), Interview C
Zugriffsberechtigte Personen	VVU	3	Hansen-Oest (2015), Bitcom (2017), DSK (2018), Interview B
Dateisystem (Eingesetzte Software)	VVU	3	Bitcom (2017), Commission for the protection of privacy (2017), Interview B
Information der Betroffenen	VVU	3	Bitcom (2017), GDD (2017), Schäfer (2017)
Datenschutz durch Technikgestaltung	VVU	2	Bitcom (2017), Interview C
Datenquelle	VVU	2	DSK (2018), Interview B
Subunternehmer (Name)	VVA	1	BvD (2017)
Datenübertragbarkeit	VVU	1	Bitcom (2017)
Verträge mit Dienstleistern	VVU	1	GDD (2017)
Auftragsverarbeiter	VVU	1	Interview C
Schulungsmassnahmen	VVU	1	Interview C

Tabelle 25: Relevante Begriffe (nicht vorgeschrieben nach DSGVO, Art. 30)

viii Übersicht Tabellen in der Access-DB (exemplarisch für VVU)

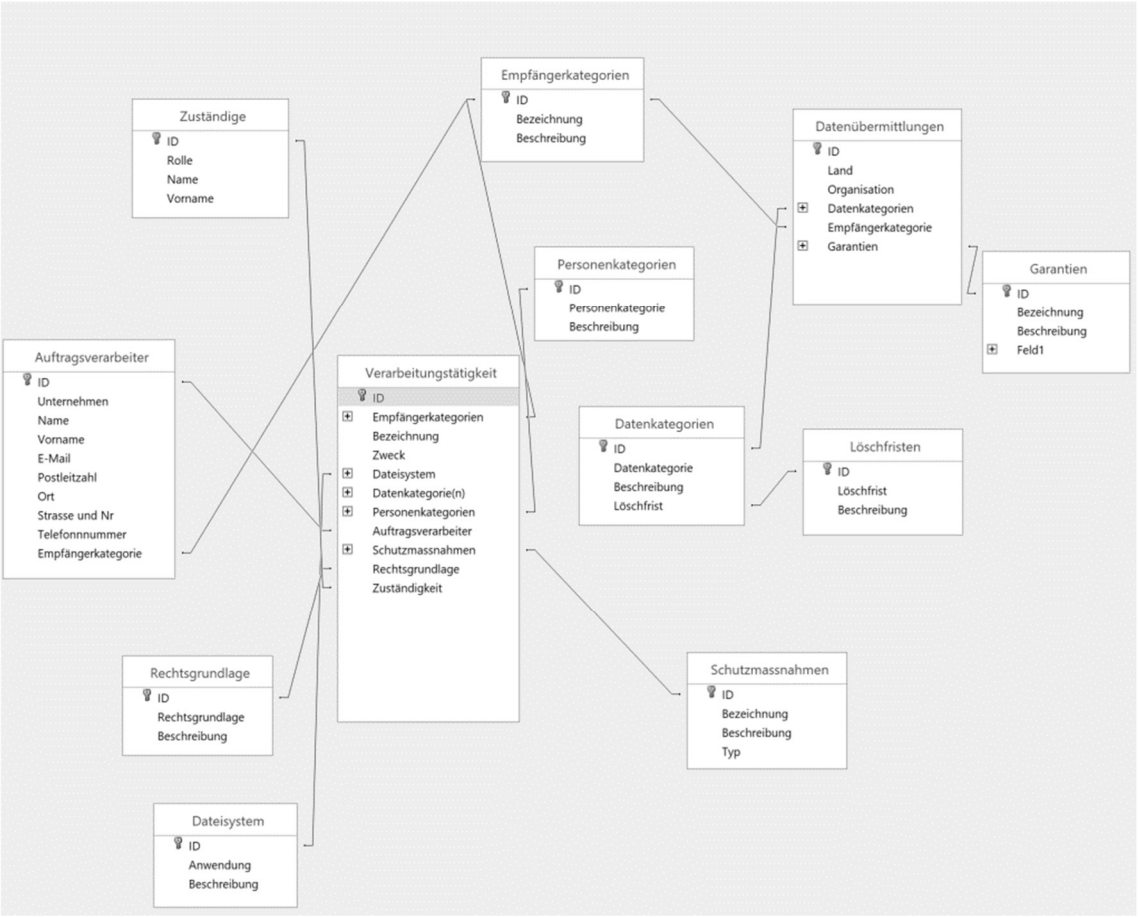


Abbildung 15: Übersicht Tabellen in der Access-DB (VVU)

ix Kurzbeschreibungen zu den Klassen der Ontologien

Klasse	**Beschreibung**
Verzeichnis von Verarbeitungstätigkeiten	Datenschutzverzeichnis, aller Verarbeitungstätigkeiten (Verarbeitungen die sich auf Personendaten beziehen) eines Unternehmens
Verarbeitungstätigkeiten	VVU: Beschreibt Verarbeitung und deren Zweck (Definition: «Ein Zweck entspricht der Zielsetzung und einer Definition, die es der betroffenen Person ermöglicht einzuschätzen, wozu ihre Daten verwendet werden») (Bsp. Bewerbermanagement, Rechnungslegung) VVA:

	Bezeichnet Verarbeitung, zeigt zugehörige Kategorien und auftraggebendes Unternehmen bzw. den Verantwortlichen des Unternehmens
Verantwortlichkeiten	VVU: Umfasst Kontaktdaten verantwortlicher Personen, d.h. den Datenschutzbeauftragten und dem/den Verantwortlichen VVA: Umfasst Kontaktdaten verantwortlicher Personen, d.h. den Datenschutzbeauftragten und dem/den Auftragsverarbeiter/Auftragsverarbeitern
Verantwortlicher	VVU: Zuständig für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten VVA: Auftraggebendes Unternehmen bzw. Verantwortlicher des auftraggebenden Unternehmens
Datenschutzbeauftragter	Zuständig für Einhaltung des Datenschutzes, benötigt Fachwissen auf den Gebieten Datenschutzrecht und Datenschutzpraxis, ist nur unter bestimmten Umständen (Bsp. Bearbeitung durch Behörde, umfangreiche Überwachung) zu benennen
Personenbezogene Daten	Alle Daten die sich auf eine natürliche Person beziehen
Betroffene Person	Identifizierte oder identifizierbare natürliche Person
Personenkategorien	Kategorien bezogen auf betroffene Personen (Bsp. Mitarbeitende, Kunden, Interessenten, Schuldner, Unter 16-jährige)
Datenkategorien	Kategorien bezogen auf personenbezogene Daten (Bsp. Adresse, Kontaktdaten, Bankverbindung)
Empfängerkategorien	Kategorien bezogen auf Empfängen, denen Daten offengelegt werden, dazu zählen interne und externe Empfänger, auch Drittländer und intern. Org.(Bsp. Marketingabteilung, Cloud Anbieter, Aktenvernichter, Institutionen der UNO)

Datenübermittlungen	Dokumentation von Datenübermittlungen an Drittländer und intern. Org.
Garantien	Nachweisung eines Angemessenheitsbeschlusses (Schutzniveau im Land des Empfängers nach EU-Kommission angemessen) oder einer anderen im Gesetz beschriebenen Garantie (Bsp. Zertifizierung, Standardschutzklausel)
Löschfristen	Genau First (Jahre) z.B. bei gesetzlichen Aufbewahrungspflichten oder Beschreibung wann die Löschung erfolgt (Bsp. nach Zweckerfüllung) – «wenn möglich» bedeutet nicht optional sondern so konkret wie möglich»
Schutzmassnahmen	Technische und Organisatorische Schutzmassnahmen (TOM), allgemein festgelegt und falls sinnvoll spezifisch für Verarbeitungstätigkeit bestimmt (Bsp. Verschlüsselung, Sicherstellung Schutzziele, Belastbarkeit der Systeme sicherstellen)
Auftragsverarbeiter	VVU: Beauftragte Auftragsverarbeiter, muss nach Gesetz nicht geführt werden, dient dazu Übersicht über beauftragte Auftragsverarbeiter zu halten VVA: Zuständig für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten die in Auftrag eines Verantwortlichen verarbeitet werden
Verarbeitungskategorien	Kategorien bezogen auf Verarbeitungstätigkeiten, die sich auf die generell angebotenen Leistungen des Auftragsverarbeiters beziehen
Ablage	Ort an dem Datenschutzverzeichnis abgelegt ist
Papierablage	Physische Ordner/Register (nicht empfohlen)
Elektronische Ablage	Softwaresystem/Tabelle für Dokumentation der Verarbeitungstätigkeiten (empfohlen)
Aufsichtsbehörde	Eine Aufsichtsbehörde pro Land die als Ansprechpartner gilt für Verantwortlicher/Auftragsverarbeiter

Unternehmen	Alle juristischen Personen, die personenbezogene Daten von sich in der EU (ab ca. 2021 auch CH) befindenden Personen bearbeiten
Rechtsgrundlage	Rechtsgrundlage muss für jede Verarbeitungstätigkeit bestehen, jedoch nicht verpflichtend im Datenschutzverzeichnis geführt werden (Bsp. Einwilligung der betroffenen Person, rechtl. Verpflichtung, lebenswichtige Interessen der betroffenen Person)
Dateisystem	Gesetze beziehen sich auf alle Verarbeitungen die strukturiert gesammelt werden, d.h. in einem Dateisystem abgelegt sind, ist nicht verpflichtend im Datenschutzverzeichnis zu führen, hilft alle Datensammlungen zu berücksichtigen
Zuständigkeit	Funktion/Person die für Verarbeitungstätigkeit zuständig ist, nicht verpflichtenden, hilft jedoch Überblick zu halten und Daten aktuell zu halten

Abbildung 16: Kurzbeschreibungen zu den Klassen der Ontolgien

x Mustervorlage Bericht für Aufsichtsbehörde (VVU)

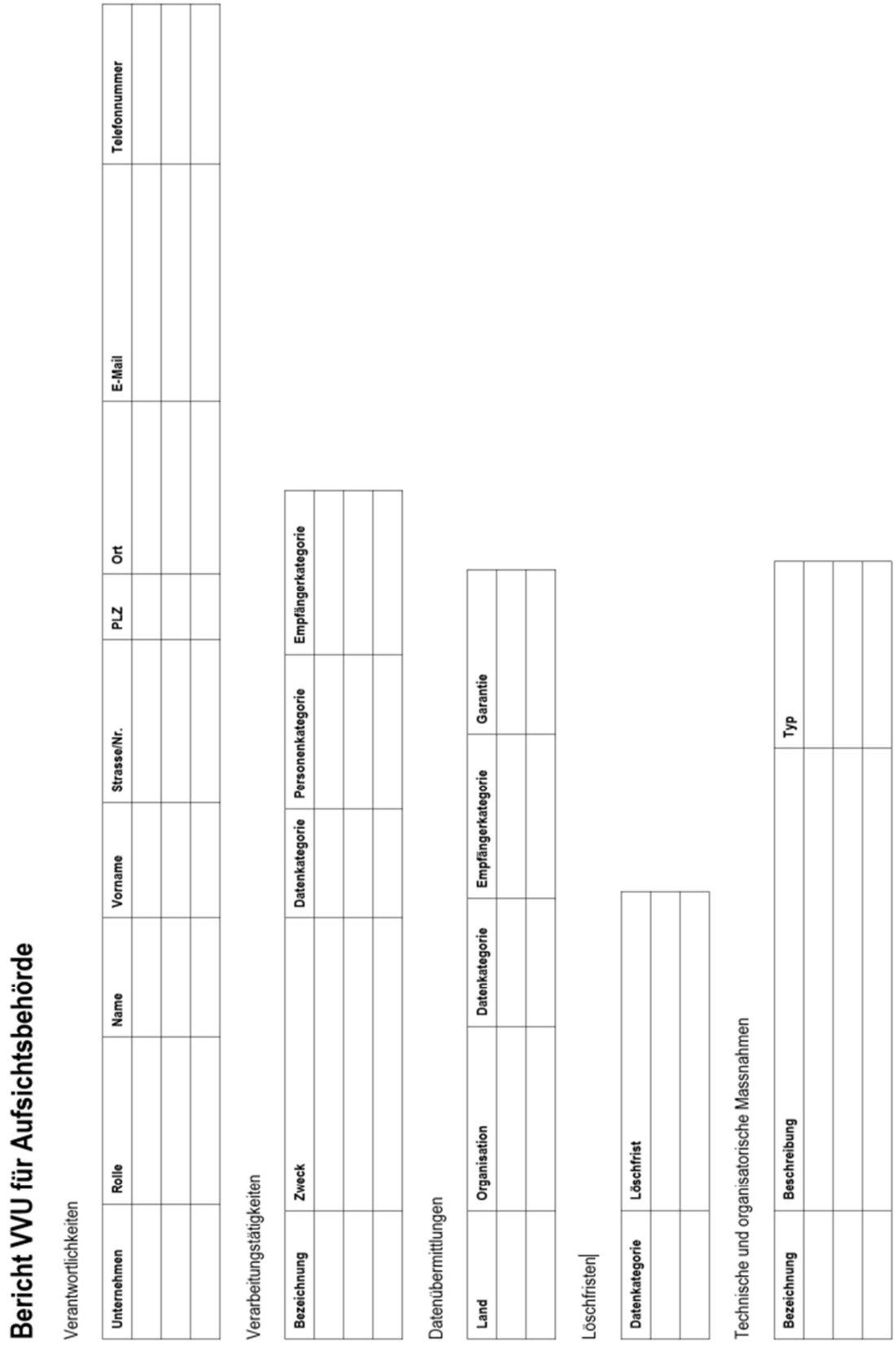


Abbildung 17: Mustervorlage Bericht VVU für Aufsichtsbehörde

xi Interviewleitfaden zu Q1

Interviewpartnerin / Interviewpartner: «Vorname», «Name»

Ort, Datum: «Ort», «Interviewdatum»

Funktion, Organisationseinheit: «Funktion», «Organisationseinheit»

Unternehmen: «Unternehmen»

Einstieg: Die interviewende Person stellt sich sowie das Projekt vor. Die interviewende Person erläutert kurz ihre Rolle für das folgende Interview und informiert den Interviewpartner/die Interviewpartnerin über den Ablauf des Interviews.

- Ablauf Gespräch 2 h
- Anonymisierung der Daten (gewünscht?)
- Art des Gesprächs: semi-strukturierte Fragen
- Einverständnis für digitale Tonaufnahme (MP3)
- Die interviewte Person wird informiert, dass die Ergebnisse des Projektes im Nachgang elektronisch zur Verfügung gestellt werden
- Einverständnis für Beginn des Interviews

Fragebereich	**Gesprächsfragen**
Warm Up: Einstieg (5 Minuten)	0 Einstiegsfragen – Wie kommt es das Sie sich mit der DSGVO beschäftigen? – Wie lange beschäftigen Sie sich bereits mit der DSGVO/DSGVO Art. 30?
Q1: Wie lassen sich bestehende Verarbeitungen/Bestände in Unternehmen mit	1 Allgemeine Fragen zur DSGVO

einem Modell beschreiben, das den gesetzlichen Vorgaben und spezifischen Anforderungen entspricht? (90 Minuten)	– Was sind aus Ihrer Sicht für ein Unternehmen die wichtigsten Aspekte bezüglich der Umsetzung der Vorgaben der DSGVO? – Wo sehen Sie die grössten Herausforderungen im Zusammenhang mit der DSGVO? 2 Begriffsdefinitionen/-eingrenzungen – Wie definieren Sie Verarbeitungstätigkeit? – Was umfasst aus Ihrer Sicht eine Verarbeitungstätigkeit? – Wie definieren Sie «Zweck» in Zusammenhang mit Verarbeitungstätigkeiten? – Welche Aufgaben hat der Verantwortliche des Verzeichnisses von Verarbeitungstätigkeiten? 3 Aufbau Verzeichnis von Verarbeitungstätigkeiten – Welche Bestandteile müssen in einem Verzeichnis von Verarbeitungstätigkeiten aus Ihrer Sicht vorhanden sein? – Welche weiteren Bestandteile wären wünschenswert? 4 Beurteilung Modell – Enthält das Ihnen vorgelegte Model l die nötigen Bestandteile? Welche weiteren Bestandteile sind nötig? – Wie beurteilen Sie das Modell hinsichtlich Nutzen für weiterführende Verwendungszwecke? Wie könnte der Nutzen erhöht werden? – *Würden sie für die jeweiligen Verarbeitungstätigkeiten weitere zuständige im VV führen? Wenn ja, welche*

	Funktion haben diese Verantwortlichen im Unternehmen? – *Wie führen Sie/würden Sie den Auftragsverarbeiter in Ihrem VV (führen)? Wie führen Sie/würden Sie Verarbeitungstätigkeiten führen, die in Ihrem Auftragsverarbeiter durchgeführt werden?* – *Wie sehen Sie die Rolle der betroffenen Person im Zusammenhang mit dem VV?* – *Wie würden Sie den Ablageort (Dateisystem) im VV führen?* 5 Weiterführende Fragen – Wie gehen Sie vor/würden Sie vorgehen bei der Umsetzung des Verzeichnisses von Verarbeitungstätigkeiten? – Welche Ressourcen ziehen Sie für die Umsetzung bei/würden Sie beiziehen (Bsp. vorhandene Dokumentationen, Personen, ...)? – Wie gehen/würden Sie bei der Definition von Personenkategorien, Datenkategorien, Empfängerkategorien vor? Auf welche Grundlagen stützen Sie sich? – In welchem Unternehmensbereich würden Sie das VV integrieren? – Stellen Sie sich vor auf Basis, dieses Modells wird eine Software oder Methode zur Einführung eines Verzeichnisses von Verarbeitungstätigkeiten entwickelt, was erachten Sie dabei als wichtig?
Cool Down: Abschluss (5 Minuten)	6 Abschlussfragen

	– Halten Sie es für möglich mit einem «guten» Verzeichnis einen wirtschaftlichen Nutzen zu erzielen? – Können Sie weitere Interviewpartner empfehlen, die sich mit der Thematik auseinandersetzen?

Abschluss

- Zusammenfassung der besprochenen Themen
- Frage nach nicht angesprochenem
- Erläuterung des Vorgehens bei der Datenanalyse
- Termin für Rückmeldung
- Dank

xii Interview Antworten (Zusammenfassung)

Interview A

Funktion	Mitarbeiter/Rechtsanwalt
Organisationseinheit	-
Unternehmen	Probst Partner AG
Ort	Winterthur
Datum	23.03.2018
Wie kommt es das Sie sich mit der DSGVO beschäftigen?	– Bin IT-Rechtsanwalt – Habe mit Digitalisierung, digitalen Geschäftmodellen zu tun – Datenschutz eines der Themen – Erste Berührungspunkte mit Datenschutzrecht im 2011
Wie lange beschäftigen Sie sich bereits mit der DSGVO/DSGVO Art. 30?	– Seit Mai 2016 – Nach Berichterstattung, dass definitiver Wortlaut festgelegt ist – Danach ruhigere Phase da sich die Unternehmen noch nicht damit befassten, vor allem im Bereich KMU, da noch Unklarheiten bestanden – In der Schweiz befasste sich vor dem Mai 2016 wohl niemand damit – Probst Partner AG macht keine Verzeichnisse selber, sondern unterstützen, ich habe in der Beratungstätigkeit schon verschiedene Ausprägungen gesehen – Themen: Über was muss ich informieren, über was muss ich Auskunft geben - diese Informationen müssen darin enthalten sein – Verzeichnis kann genutzt werden um Anfragen von betroffenen Personen zu beantworten
Was sind aus Ihrer Sicht für ein Unternehmen die wichtigsten Aspekte bezüglich der Umsetzung der Vorgaben der DSGVO?	– Dokumentation führen und up to date zu halten – Prozess implentieren, um die verschiedenen Pflichten innerhalb den vorgegebenen Zeiten zu erfüllen (Bsp. Data Breach: 72 h ab Kenntnis) --> damit Compliance ermöglichen – Nach aussen: Privacy Policies reviewen, AGBs reviewen, Auftragsverhältnisse reviewen (Verträge) – Verzeichnis von Verarbeitungstätigkeiten als einen der ersten Schritte – VV nötig um anderen Verpflichtungen gerecht zu werden (Bsp. Auskunftsrecht, Löschungsrecht)

Wo sehen Sie die grössten Herausforderungen im Zusammenhang mit der DSGVO?	– Bei CH Unternehmen - Wichtigkeit des Themas noch nicht bewusst, Meinung das es über Zustimmung oder Gerichtstandklausel (Bsp. Recht der Bermudas anwenden) geregelt werden kann --> dies bringt jedoch nichts- Anwendbar oder nicht? Immernoch nicht klar für alle Unternehmen – Thema angehen, ist unfassbar- Durchdringt alle Geschäftsprozesse- U. glauben, dass Sie keine Personendaten gespeichert haben (Jedes Unternehmen, hat Mitarbeitende, Lieferanten, Kunden)- Da es so grundlegen ist, verstehen Unternehmen noch nicht was das bedeuten kann- Delta feststellen, zwischen Ist-Zustand und Soll-Zustand – Beratungprozess: IST-Analyse, Soll-Zustand, Delta-Analyse, dann begleiten bei der Umsetzung, Management Untertützung nötig- Infos: 3- Schritt Prozess: Swiss-Data Protection Law (WebSeite) – Grösste Schwierigkeit, dass es überhaupt zum Thema wird- Ressourcen benötigt, Budget für professionelle Beratung- Relevanz wird von vielen Unternehmen erst jetzt erkannt, erst nach ersten Gerichtsentscheiden wird Lage richtig verstanden – Es wird eine ganz neue Wirtschaftsbranche mit neuen Berufen geschaffen- Feststellen, wo gibt es wirklich ‚schlimme' Sachen, die angegangen werden müssen
Wie definieren Sie Verarbeitungstätigkeit?	– «Atomisiert»: Alles, dass im weitesten Sinne etwa zu tun --> wird von einigen so gesehen – Im Zusammenhang mit dem Zweck betrachten – Bsp. HR-Daten, Zusätzliche Personendaten
Was umfasst aus Ihrer Sicht eine Verarbeitungstätigkeit?	– Keine objektive Definition – Granularität ist entscheidend – Businesssicht abbilden (Prozesse) --> Funktionen die ein Unternehmen ausführt – Evtl. einen Prozess mehreren Verarbeitungstätigkeiten zuweisen (z.B. wenn der Rechtsgrund unterschiedlich ist)
Wie definieren Sie «Zweck» in Zusammenhang mit Verarbeitungstätigkeiten?	– Zentralesterpfeiler des Datenschutzrechts ist ‚Zweckbindungung', d.h. Daten dürfen nur dafür verwendet werden, wozu sie erhoben wurden – Kann nicht absolut beantwortet werden – Überlegung muss sein, was ist der Hintergrund weshalb der Zeck bekannt sein muss – Zwecke muss so genau definiert sein, dass Person einschätzen kann wozu Daten verwendet werden und somit der Verwendung zustimmen kann oder nicht bzw. sich dieser entziehen kann – «Marketingzwecke» ist eine sehr breite Umschreibung, aus sicht Probst Partner AG sollte der Zweck detailierter definiert sein – «Adresshandel» ist auch ein Zweck

	– Auftragsverarbeiter muss Daten zum gleichen Zweck verarbeiten, sonst wird er zum Verantwortlichen, gleiches gilt für jeden Auftragsbearbeiter der wiederum von einem Auftragsbearbeiter beauftragt wurde
Welche Aufgaben hat der Verantwortliche des Verzeichnisses von Verarbeitungstätigkeiten?	– Interne Anlaufstelle – Nicht vorgesehen als juristisch Verantwortlicher gemäss Gesetz, faktisch trotzdem vermutliche verantwortlich – Wissen an einer Stelle bündeln
Welche Bestandteile müssen in einem Verzeichnis der Verarbeitungstätigkeiten aus Ihrer Sicht vorhanden sein?	– Gesetzliche Vorschriften – Im Übrigen ist man frei (Frage was brauche ich?) – sehr Abhängig wie Prozesse definiert sind (Data Breach Prozess etc.) – In Form einer DB aufsetzen: Excel, Spezialsoftware --> Damit ein Aufschlüsseln möglich ist – A4 Seite für jeden Verarbeitungsprozess (Weniger ideal) – Als Dienstleister Vorgaben des Verantwortlichen erfüllen – Flughöher nicht zu tief, abstrakte Prozesse führen – Mit Informationsystemen verbunden, um Mitarbeitende auf fehlende Bestägtigungen aufmerksam machen – Detailierterer Layer
Welche weiteren Bestandteile wären wünschenswert?	– Teil der Datenschutz/Compliance Dokumtation – Form regelmässiger Absegunung – Versionierung – Ersteller des Verarbeitungsprozesses – Wurde der GL vorgelegt am (Datum) – Historie für GL - ‚blinde' Flecken vermeiden – Vorgaben des auftraggebenden (für Dienstleister) – ‚Flughöhe' etwas höher halten und schauen, dass abstrakte Prozesse enthalten sind, d.h. nicht zu fest in die Tiefe gehen – Verbindung bsp. CRM damit bei der Bearbeitung von Daten ein Hinweis auftaucht, wenn für einen Zweck die Einwilligung fehlt --> als Arbeitstool verwenbar Detailierter Layer einfügen, der nicht explizit vom Gesetz gefordert ist, mit Kommentaren – Im Moment ist noch nicht klar wie tief die Aufsichtsbehörden bei Einforderung des Verzeichnisses gehen werden
Enthält das Ihnen vorgelegte Model die nötigen Bestandteile? Welche weiteren Bestandteile sind nötig?	– Bestandteile die von der Chronologie am Anfang stehen eher links anorden, Dateninput z.B., Lesegewohnheit des Europärs von links oben nach rechts unten – Einwilligung muss von der betroffenen Person nur gegeben werden, wenn keine Rechtsgrundlage besteht – Evtl. eher Verbindung betroffene Person - personenbezogene Daten

Wie beurteilen Sie das Model hinsichtlich Nutzen für weiterführende Verwendungszwecke? Wie könnte der Nutzen erhöht werden?	– Für Softwareentwicklung wichtig, wie viele automatische Checks können gemacht werden – Grundverständnis für Bestandteile schaffen
Optional: Würden sie für die jeweiligen Verarbeitungstätigkeiten weitere zuständige im VV führen? Wenn ja, welche Funktion haben diese Verantwortlichen im Unternehmen?	– Kann, muss aber nicht, für grosse Unternehmen sinnvoll – Bezeichnung nicht Verantwortlicher, sondern ‚Ansprechperson', sinnvoll Prozessowner – Prozessowner wissen vermutlich am besten Bescheid für was welche Daten verwendet werden
Optional: Wie führen Sie/würden Sie den Auftragsverarbeiter in Ihrem VV (führen)? Wie führen Sie/würden Sie Verarbeitungstätigkeiten führen, die in Ihrem Auftragsver-arbeiter durchgeführt werden?	– Auftragsverarbeiter führt für sich ein Verzeichnis und eines für Kunden – Sein Verzeichnis wird vermutlich zwei bzw. mehrere Verzeichnisse umfassen ein eigenes sowie jeweils eines pro Kunden, mit Spezifikas – Kunden fordert möglicherweise andere ‚Flughöhe' – Zusatzinformationen wie Versionierung evtl. von Kunden gefordert – Felder nicht editieren – Möglichkeit ein Verzeichnis oder mehrere Verzeichnisse führen
Optional: Wie sehen Sie die Rolle der betroffenen Person im Zusammenhang mit dem VV?	-
Optional: Wie würden Sie den Ablageort (Dateisystem) im VV führen?	-
Wie gehen Sie vor/würden Sie vorgehen bei der Umsetzung des Verzeichnisses von Verarbeitungstätigkeiten?	– IST-Analyse (gleicht bereits einem VV) – Comliance check – Updaten um SOLL zu erreichen
Welche Ressourcen ziehen Sie für die Umsetzung bei/würden Sie beiziehen (Bsp. vorhandene Dokumentationen, Personen, ...)?	– Leute die wissen was passiert im Unternehmen (IT, HR, Führungsebene, Markting, alle die in leitender Funktion über Personendaten bestimmen) – Für grössere Unternehmen in zwei Schritten vorgehen – erste Phase: Abstrakte Ebene Fragenbogen oder Interviews - um Grobraster festzustellen, wo werden welche Daten verarbeitet, als weitere Möglichkeiten könnte dies auch anhand einer Applikatonslandkarte ermittelt werden

	– Welche Applikationen habe ich, welche Applikationen habe ich für was – zweite Phase: Fragebogen an alle Mitarbeiter um weitere fehlende Daten zu ermitteln – Information Security Managementsystem kann ein guter Startpunkt sein --> kennt meistens nur die IT
Wie gehen/würden Sie bei der Definition von Personenkategorien, Datenkategorien, Empfängerkategorien vor? Auf welche Grundlagen stützen Sie sich?	– Frage der ‚Flughöhe' – Überlegung ‚Was ist Funktion davon?' – Wann konsultiere ich das Verzeichnis und welche Informationen müssen ausgelesen werden können – Anfrage von betroffener Person könnte lauten: Welche Daten von mir sind gespeichert? Wem werden sie bekannt gegeben? --> solche Daten sollten dem VV entnommen werden können – Antwort: Personendaten und die Daten werden weitergegeben an andere Unternehmen reicht wohl nicht – Datenkategorien Bsp: Kontaktdaten, Kommunkationsdaten (E-Mail, Telefon) – Datenkategorien müssen erlauben zu beurteilen ob sie im Zusammenhang mit der Verarbeitung stehen --> thematische Abgrenzung - objektives richtig oder falsch ist bisher noch nicht ersichtlich – ‚Besonders schützenswerte' und ‚schützenswerte' Daten als Metakategorie möglicherweise sinnvoll – Zusammenhang Datenkategorien mit Einwilligungen etc.
In welchem Unternehmensbereich würden Sie das VV integrieren?	-
Stellen Sie sich vor auf Basis, dieses Modells wird eine Software oder Methode zur Einführung eines Verzeichnisses von Verarbeitungstätigkeiten entwickelt, was erachten Sie dabei als wichtig?	– Zugänglichkeit – Form bsp. ‚FAQ' , interaktives Format, Interview, Informationen Muss vs freiwillig, Assistent der nur benötigte Bereiche einblendet, Prozess der das Ganze abbildet, Zuständige können Daten abfüllen Wichtig ist das eine Begleitung durch Datenschutzverantwortlichen bzw. Knowhowträger stattfindet – Verständnis für ‚was sind Personendaten' schaffen Schulung im Betrieb MA auf Prozess
Halten Sie es für möglich mit einem «guten» Verzeichnis einen wirtschaftlichen Nutzen zu erzielen?	Ja, definitiv. Statt nur Pflicht erfüllen kann man die Gelegenheit nutzen, sich ein Bild der Personendaten im Unternehmen zu machen und diese in Zukunft auch aktiver – und allenfalls umsatzwirksam – nutzen.]

Interview B

Funktion	Leiterin Rechtsabteilung Europa
Organisationseinheit	-
Unternehmen	Weltweit tätiges Industrieunternehmen
Ort	-
Datum	03.04.2018
Allgemeine Informationen zum Unternehmen	Verschiedene Organisationseinheiten, die Produktorganisationen (PO) und Marktorganisationen (MO), MO haben Mitarbeiter- und Kundendaten, PO nur Mitarbeiterdaten, Heterogene Systemlandschaft, Globale IT ist Systemlieferant, Datenowner sind lokal (Verkäufer und HR)
Allgemeine Bemerkungen	– Softwarelösung von OneTrust macht einen guten Eindruck auf sie – Wichtiges Feature einer Softwarelösung ist für uns ‚Prefeeding', da sehr effizient – Bisher in keiner Softwarelösung gesehen, bei OneTrust angefragt und keine brauchbare Antwort erhalten – 100% Compliance mit DSGVO ist nicht möglich, dass ist das ‚Problem' der Lösungsanbieter, sie sind ‚zu gut' – Aus meiner Sicht gilt für ein System je simpler desto besser
Wie kommt es das Sie sich mit der DSGVO beschäftigen?	– Suche nach einem generellen Verantwortlichen gescheitert – Vier Unternehmensjuristen übernehmen die Aufgabe gemeinsam
Wie lange beschäftigen Sie sich bereits mit der DSGVO/DSGVO Art. 30?	– Zuerst verging viel Zeit bis der Management Support eingeholt werden konnte – ca. 2 Jahre - Sobald die Verordnung bekannt wurde – Aktiv seit 6 Monaten - Zwei Workinggoups: Customer und Marketing Data und HR Daten
Was sind aus Ihrer Sicht für ein Unternehmen die wichtigsten Aspekte bezüglich der Umsetzung der Vorgaben der DSGVO?	– Bewusst sein schaffen – Management buy-in- Verständnis um was es eigentlich geht (z.B. was sind persönlichen Daten?) – finden einer gemeinsamen Sprache (Bsp. Begriff - Data Controller und Data Processor --> sagt dem Business nichts) – DSGVO ist «IT-lastig» --> Gemeinsame Sprache zwischen IT und Juristen finden – Verständnis für Systeme bei Juristen schaffen und im Gegenzug Verständnis für Rechtssprache bei der IT schaffen

Wo sehen Sie die grössten Herausforderungen im Zusammenhang mit der DSGVO?	– Heterogene Systemlandschaft die nicht verändert wird im Hinblick auf die DSGVO – 50 - 200 Systeme unterschiedliche Systeme in den Geschäftseinheiten, Geschäftseinheiten sind sehr unterschiedlich organisiert – Leads (IP-Adressen die gesammelt werden auf Webseiten, um mögliche Kunden zu erkennen) --> wer ist der Owner? --> diese Daten gehören auch in Verzeichnis zuerst ohne Namen und sobald verfügbar mit Namen – MO haben die Pflicht ein Verzeichnis lokal aufzusetzen (Problem Ressourcen) --> werden unterstützt mit bereits vorbereiteten Informationen – Anforderungen des Gesetzes umzusetzen im Konflikt mit Tagesgeschäft – Gemeinsame Sprache zwischen Juristen, Marketing und IT finden – Sprache der Benutzer sprechen lernen
Wie definieren Sie Verarbeitungstätigkeit?	Muss nicht immer ein Prozess sein, kann auch ein System sein - OneTrust z.B. bietet die Funktion, dass man sich für System oder Prozesse entscheidet
Was umfasst aus Ihrer Sicht eine Verarbeitungstätigkeit?	Bei uns wird vom System ausgegangen (Bsp. Payroll System) trotzdem wir der Prozess in den Vordergrund gesetzt Grund: Jedes System hat einen Verantwortlichen, aber nicht jeder Prozess
Wie definieren Sie «Zweck» in Zusammenhang mit Verarbeitungstätigkeiten?	Beschreibung welche Daten für welche Individuen und für welchen Zweck müsste zusammen beschrieben werden.- Aufnahme von Metadaten (Nebenzwecke) sekundär
Welche Aufgaben hat der Verantwortliche des Verzeichnisses von Verarbeitungstätigkeiten?	– Pro Geschäftseinheit einen Verantwortlichen --> dezentrale Kultur – Lokaler Generalmanager ist verantwortlich - kann einen Verantwortlichen benennen - Letztendlich ist aber immer Generalmanager zuständig
Welche Bestandteile müssen in einem Verzeichnis der Verarbeitungstätigkeiten aus Ihrer Sicht vorhanden sein?	– Anforderungen aus dem Gesetz – Minimale Lösung – Kontrolle externe Auftragsverarbeiter ist fast unmöglich - Data Processing Agreement ist maximal machbar -- > in Zukunft muss das gemacht werden --> geht wohl in Richtung Zertifizierung aus meiner Sicht

Welche weiteren Bestandteile wären wünschenswert?	– Name des Systems in dem die Daten gespeichert sind – Verantwortliche - d.h. Kontakt Business owner – Quelle der Daten (Bsp. von einem anderen System oder einem Kundenformular, Daten die beim Bestellprozess eingegeben, Job Kandidaten) – Wer hat Zugang zu den Systemen (Benutzer) – Privacy Impact Assessment
Enthält das Ihnen vorgelegte Model die nötigen Bestandteile? Welche weiteren Bestandteile sind nötig?	Beachten, dass nicht immer eine Einwilligung vorliegt, sondern eine andere rechtliche Grundlage bestehen kann- möglichst versuchen eine andere Legitimation zu finden anstelle einer Einwilligung- Schutzmassnahmen: Verbindung zu Verarbeitungstätigkeit - Liste mit technischen und organisatorischen Massnahmen zum ‚Ankreuzen'
Wie beurteilen Sie das Model hinsichtlich Nutzen für weiterführende Verwendungszwecke? Wie könnte der Nutzen erhöht werden?	– Verständlich aufbereitet – Zielpublikum ist entscheidend – Verständlichkeit – Unternehmen mit weniger Ressourcen in diesem Bereich (KMU, Industriebetriebe)
Optional: Würden sie für die jeweiligen Verarbeitungstätigkeiten weitere zuständige im VV führen? Wenn ja, welche Funktion haben diese Verantwortlichen im Unternehmen?	Ja, den Business owner
Optional: Wie führen Sie/würden Sie den Auftragsverarbeiter in Ihrem VV (führen)? Wie führen Sie/würden Sie Verarbeitungstätigkeiten führen, die in Ihrem Auftragsversarbeiter durchgeführt werden?	Nur am Rande, fraglich ob Details bekannt gegeben werden gegenüber den Behörden --> versuchen auf Geschäftsgeheimnis zu berufen
Optional: Wie sehen Sie die Rolle der betroffenen Person im Zusammenhang mit dem VV?	Hat wenig Zusammenhang mit dem Verzeichnis, als Bestandteil erwähnen ist richtig, jedoch keine weiteren Massnahmen notwendig

Optional: Wie würden Sie den Ablageort (Dateisystem) im VV führen?	Die Systeme im Verzeichnis von Verarbeitungstätigkeiten führen
Wie gehen Sie vor/würden Sie Vorgehen bei der Umsetzung des Verzeichnisses von Verarbeitungstätigkeiten?	– General Manager kontaktieren in den Geschäftseinheiten – General Manager bewusstgemacht, dass sie verantwortlich sind und gebeten einen Datenschutzverantwortlichen zu benennen (Datenschutzverantwortliche sind Hauptkanal für Kommunikation, auch wenn die General Manager die formelle Verantwortung tragen. – Gruppengovernance Struktur aufgebaut und definiert wo unterstützt die Gruppe und was müssen sie selber machen – Aufnahme der bekannten Daten (Exceltabelle) --> es bräuchte eine Softwarelösung, jedoch drängt im Moment die Zeit - GapAnalyse geplant wird vermutlich von den General Managern nicht durchgeführt
Welche Ressourcen ziehen Sie für die Umsetzung bei/würden Sie beiziehen (Bsp. vorhandene Dokumentationen, Personen, ...)?	General Manager, Legal-Wiki das bereits bestanden hat wurde ergänzt, Arbeitsgruppen
Wie gehen/würden Sie bei der Definition von Personenkategorien, Datenkategorien, Empfängerkategorien vor? Auf welche Grundlagen stützen Sie sich?	– Personenkategorien relativ klar – Datenkategorien (Bsp. Kontaktdaten, Lohndaten, Bankkontodaten, Marketingdaten (Leads etc. --> Risiko)) --> wie tief geht man ins Detail? In diesem Bereich gibt es sehr viele unterschiedliche Meinungen – Empfängerkategorien unklar
In welchem Unternehmensbereich würden Sie das VV integrieren?	General Management der unterschiedlichen Geschäftseinheiten und Hauptsitz

Stellen Sie sich vor auf Basis, dieses Modells wird eine Software oder Methode zur Einführung eines Verzeichnisses von Verarbeitungstätigkeiten entwickelt, was erachten Sie dabei als wichtig?	– generell schwer zu beurteilen – interne Daten und Daten die für Behörden zugänglich gemacht werden müssen trennen
Halten Sie es für möglich mit einem «guten» Verzeichnis einen wirtschaftlichen Nutzen zu erzielen?	– dadurch Zusammenhänge zwischen Systemen und Prozessen und Daten besser verstehen – Schlagwort ‚BigData' Wichtigkeit der Daten verstehen und richtig Nutzen – Verständnis im Unternehmen das Daten in Zukunft wichtiger sind als physische Produkte

Interview C

Funktion	Rechtsanwalt/Consulting
Organisationseinheit	-
Unternehmen	KPMG
Ort	Winterthur
Datum	23.04.2018
Allgemeine Informationen zum Unternehmen	-
Allgemeine Bemerkungen	-
Wie kommt es das Sie sich mit der DSGVO beschäftigen?	Beruflich/Beratung Datenschutzrecht
Wie lange beschäftigen Sie sich bereits mit der DSGVO/DSGVO Art. 30?	1 Jahr intensiv

Was sind aus Ihrer Sicht für ein Unternehmen die wichtigsten Aspekte bezüglich der Umsetzung der Vorgaben der DSGVO?	– Einhaltung gesetzliche Vorgaben des Art. 30 und gleichzeitig keine zu starke Bürokratisierung des Alltagsgeschäfts, so schlank wie möglich so umfangreich wie nötig gestalten – Artikel 30 ist Voraussetzung für Einhaltung der Vorgaben DSGVO
Wo sehen Sie die grössten Herausforderungen im Zusammenhang mit der DSGVO?	– die Masse der Neuerungen, Schwierigkeit auch alles gesehen und abgedeckt zu haben – Herausfinden wo Daten im Unternehmen sind – sich nicht verlieren – nichts übersehen – Unüberschaubar für jemanden der es nicht täglich macht – Neues Gebiet, Datenschutzrecht wurde bisher keine grosse Aufmerksamkeit geschenkt – Noch keine Rechtsprechung und Verwaltungspraxis bekannt
Wie definieren Sie Verarbeitungstätigkeit?	– entsprechend der Legaldefinitionen in Art. 4 – Speichern, lesen, löschen, bearbeiten – Begriff ist so weitgehend, das faktisch alles darunter fällt
Was umfasst aus Ihrer Sicht eine Verarbeitungstätigkeit?	– grösste Schwierigkeit, wie unterteilt man – Unterscheidung nach Zweck
Wie definieren Sie «Zweck» in Zusammenhang mit Verarbeitungstätigkeiten?	Die Zielsetzung, welche mit der Verarbeitung erreicht werden soll (Bsp. Marketingaktivität –> Werbeanschreiben, Erfassung von Bewerbungsschreiben)
Welche Aufgaben hat der Verantwortliche des Verzeichnisses von Verarbeitungstätigkeiten?	– vgl. Art. 30 Abs. 1 – Verzeichnis aktuell halten – den Pflichten gemäss Gesetz nachkommen, Richtigkeit der Daten gewährleisten – Grundsatz der Datenminimierung sicherstellen – Recht auf Auskunft, auf Löschung sicherstellen – privacy by desing und default sicherstellen – Aufsichtspflicht --> Unterlassung hat strafrechtliche Folgen (Als Verantwortlicher Versicherung beim Arbeitgeber verlangen)

Welche Bestandteile müssen in einem Verzeichnis der Verarbeitungstätigkeiten aus Ihrer Sicht vorhanden sein?	– die im Gesetz genannten – Beschreibung der Datenkategorie – Beschreibung der Kategorie betroffener Personen – Zweck der Verarbeitung – Empfänger, gegenüber denen personenbezogene Daten offengelegt werden – Datenübermittlung an Drittland und Empfänger – vorgesehene Löschfristen für die jeweilige(n) Datenkategorie(n) – allgemeine Beschreibung der technischen und organisatorischen Massnahmen em. Art. 32 Abs. 1 – verantwortliche Fachabteilung – Ansprechpartner (Kontaktdaten) – Datum der Erfassung – Änderungsdatum
Welche weiteren Bestandteile wären wünschenswert?	– Rechtsgrundlage für die Verarbeitung – Einwilligung vorhanden oder nicht (ggf. Nachweis) – Einwilligung ggf. widerrufen – Privacy by Design & Privacy by Default eingehalten (Nachweis) – Dokumentation Anfrage Auskunft, Berichtigung, Löschung – Auflistung ggf. beteiligter Auftragsdatenverarbeiter – Konformitätserklärung vom Auftragsverarbeiter – Risikobewertung (DPIA) – Schulungs- und Awarenessmassnahmen
Enthält das Ihnen vorgelegte Model die nötigen Bestandteile? Welche weiteren Bestandteile sind nötig?	– Verbindung TMO zu Verarbeitungstätigkeiten – Vertreter in der EU integrieren zwischen Verantwortlichem und Aufsichtsbehörde (Graubereich: Was darf an ausländische Behörde übermittelt werden?)
Wie beurteilen Sie das Model hinsichtlich Nutzen für weiterführende Verwendungszwecke? Wie könnte der Nutzen erhöht werden?	Klären welche Sprache sinnvoll ist, welche Sprache von den Behörden verlangt wird
Optional: Würden sie für die jeweiligen Verarbeitungstätigkeiten weitere zuständige im VV führen? Wenn ja, welche Funktion haben diese Verantwortlichen im Unternehmen?	Verantwortliche auf Funktionsstufen definieren (HR, Controlling etc.)

Optional: Wie führen Sie/würden Sie den Auftragsverarbeiter in Ihrem VV (führen)? Wie führen Sie/würden Sie Verarbeitungstätigkeiten führen, die in Ihrem Auftragsversarbeiter durchgeführt werden?	– Direkt aus Gesetz für mich nicht ersichtlich – Erste Einschätzung Auftragsverarbeiter muss nicht namentlich genannt werden – [Genauere Abklärung folgt]
Optional: Wie sehen Sie die Rolle der betroffenen Person im Zusammenhang mit dem VV?	Wenn Personen Auskunft verlangen, können Informationen schneller gefunden werden
Optional: Wie würden Sie den Ablageort (Dateisystem) im VV führen?	Ablageort von Daten ist fast immer ein Dateisystem, daher nicht so relevant
Wie gehen Sie vor/würden Sie Vorgehen bei der Umsetzung des Verzeichnisses von Verarbeitungstätigkeiten?	– Verantwortlichkeiten klar definieren und ggf. dem Umsetzungszuständigen Weisungsbefugnisse einräumen – Management Support
Welche Ressourcen ziehen Sie für die Umsetzung bei/würden Sie beiziehen (Bsp. vorhandene Dokumentationen, Personen, ...)?	– Weisung/Prozessbeschriebe – DPIA – Dokumentation Verarbeitungsprozesse – IT Abteilung – Recht und Compliance – Internes Projektmanagement
Wie gehen/würden Sie bei der Definition von Personenkategorien, Datenkategorien, Empfängerkategorien vor? Auf welche Grundlagen stützen Sie sich?	– Definition nach Gesetz und dann nach Zweck – Zuerst personenbezogene Daten, zuerst schützenswert und besonders schützenswerte Daten und dann den Zweck unterscheiden
In welchem Unternehmensbereich würden Sie das VV integrieren?	Legal & Compliance/DPO

Stellen Sie sich vor auf Basis, dieses Modells wird eine Software oder Methode zur Einführung eines Verzeichnisses von Verarbeitungstätigkeiten entwickelt, was erachten Sie dabei als wichtig?	– Vollständigkeit und Benutzerfreundlichkeit – Möglichkeit diese stets aktuell zu halten
Halten Sie es für möglich mit einem «guten» Verzeichnis einen wirtschaftlichen Nutzen zu erzielen?	Ja – Konformitätsbestätigung (Anbieter mit Bestätigung hat einen Wettbewerbsvorteil) – Marketing: Slogan: «Bei uns sind ihre Daten sicher» – Risiken von Bussgeldern und Reputationsschäden nicht ausgesetzt