der Bundeswehr
Universität München

Masterarbeit

DSGVO: Analyse der Anforderungen sowie Umsetzung der Dokumentationspflicht

Eingereicht von:	Jan Ole Juister 1185199
Erstprüfer:	Prof. Dr. Arno Wacker
Zweitprüferin:	Dr. Corinna Schmitt
Betreuung:	Dr. Olga Kieselmann
Abgabedatum:	30. Juni 2022

Professur
Datenschutz und Compliance
Universität der Bundeswehr München

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Listings

Abkürzungsverzeichnis

BDSG Bundesdatenschutzgesetz

CRISP-DM Cross Industry Standard Process for Data Mining

CRUD create, read, update, delete

DK Datenkategorie

DSGVO Datenschutz-Grundverordnung

EA Enterprise Architecture

EAM Enterprise Architecture Management

ERP Enterprise Resource Planning

EU Europäische Union

K Kopie

KI künstliche Intelligenz

LDSG Landesdatenschutzgesetz

LK Löschkonzept

MVCS Model-View-Controller-Service

PrIME Privacy Inventory, Management & Education

TOMs technische und organisatorische Maßnahmen

VT Verarbeitungstätigkeit

VVT Verzeichnis von Verarbeitungstätigkeiten

1 Einleitung

Täglich interagieren wir mit Verarbeitern personenbezogener Daten. Social-Media Anbieter, Streamingdienste, Banken, Internetsuchmaschinen und viele mehr haben in der Regel das Einverständnis ihrer Nutzer, personenbezogene Daten zu verarbeiten. In erster Linie sind Verarbeitungen nötig, um den angebotenen Dienst bereitzustellen. Aber auch darüber hinaus werden die Daten häufig verarbeitet, um personenbezogene Werbung, Konsumvorschläge oder Angebote unterbreiten zu können. Dazu werden die erhobenen Daten teilweise auch an Drittanbieter weitergegeben, damit die Nutzer bestmöglich persönlich beraten werden können. Um die rechtmäßige und sichere Verarbeitung der personenbezogenen Daten sicherstellen und die Verarbeitungswege nachvollziehen zu können, muss es eine Regelung geben, die ausführliche Dokumentationen im Rahmen der Datenverarbeitung von dem Verarbeiter fordert.
Durch die Datenschutz-Grundverordnung (DSGVO), welche 2016 in Kraft trat und seit 2018 verpflichtend anzuwenden ist, wurde ein Gesetzestext entworfen, der verschiedenen Dokumentationen bei der Verarbeitung personenbezogener Daten durch die verarbeitenden Stellen fordert. Den Kern dieser Dokumentationen bildet das Verzeichnis von Verarbeitungstätigkeiten (VVT), in welchem der Verarbeiter alle Verarbeitungstätigkeiten von personenbezogenen Daten dokumentieren muss. Wie diese Anforderungen jedoch umgesetzt werden müssen, ist nicht vorgegeben und für Personen, die von der Verarbeitung personenbezogener Daten betroffen sind, ist die Umsetzung firmenintern bei dem Verarbeiter nicht prüfbar. Deshalb stellt sich die Frage, ob und wie Verarbeiter von personenbezogenen Daten die Anforderungen von Dokumentationspflichten umsetzen, was in den einzelnen Dokumentationen dokumentiert werden muss und wie Softwareprodukte bei der Dokumentation unterstützen können.
Diese Arbeit vermittelt dem Leser, was sich hinter den Dokumentationspflichten der DSGVO verbirgt, welche Informationen ein VVT enthalten sollte und wie die Dokumentationen den Verarbeitern, als auch den Betroffenen, beim Umgang mit personenbezogenen Daten weiterhelfen können.

1.1 Ziel der Arbeit

Im Rahmen der vorliegenden Masterarbeit mit dem Thema „DSGVO: Analyse der Anforderungen sowie Umsetzung der Dokumentationspflicht“ soll untersucht werden, welche Anforderungen die DSGVO, im Schwerpunkt Art. 30, an die Dokumentationspflicht stellt und wie diese mithilfe verschiedener Software umgesetzt

werden. Dazu werden im ersten Schritt die Anforderungen an die Dokumentationspflicht nach Art. 30 DSGVO herausgearbeitet.
Anhand der identifizierten Anforderungen aus dem Gesetzestext wird anschließend abgeleitet, wie diese Anforderungen in einer Software zur Dokumentation von Verarbeitungsprozessen umgesetzt werden können. Dadurch soll analysiert werden, ob alle Anforderungen durch eine Software erfüllt und Teile der Dokumentation automatisiert werden können. Anschließend wird geprüft, welche Programme zur Unterstützung der Dokumentationspflicht bereits vorhanden sind.
Existierende Softwareprodukte werden im weiteren Verlauf genauer analysiert. Die herausgearbeiteten Anforderungen werden mit der Umsetzung in den betrachteten Programmen verglichen. Dabei sollen Anforderungen identifiziert und festgehalten werden, die noch nicht umgesetzt wurden und in den Programmen ergänzt werden könnten. Im Anschluss werden die betrachteten Programme miteinander verglichen und Unterschiede herausgearbeitet. Abschließend sollen zu den ergänzbaren Funktionen in den betrachteten Programmen Konzepte zur Umsetzung geschrieben werden. Zudem soll eine ergänzbare Funktion in einem der Programme selbstständig hinzugefügt werden.
Im Folgenden werden die wichtigsten Ziele dieser Arbeit zusammengefasst:

- Anforderungen der DSGVO bzgl. Dokumentationspflichten herausarbeiten
- Analysieren, wie die Anforderungen in einer Software umgesetzt werden könnten
- Vorhandene Softwareprodukte finden und Umsetzung mit eigener Analyse vergleichen
- Ergänzbare Funktionen in vorhandener Software finden
- Konzepte zur Integration von ergänzbaren Funktionen entwickeln
- Entwickelte Konzepte in Software implementieren

1.2 Aufbau

Diese Arbeit besteht neben der Einleitung aus sieben weiteren Kapiteln. In Kapitel 2 werden Grundlagenbegriffe erklärt, die für das weitere Verständnis vonnöten sind. Zudem behandelt Abschnitt 2.4 die Rechenschafts- und Nachweispflichten. Hier wird herausgearbeitet, welche Artikel der DSGVO Rechenschafts- oder Nachweispflichten fordern und welche Anforderungen an eine Dokumentation daraus hervorgehen.
Kapitel 3 befasst sich anschließend mit der Frage, in welcher Form die Anforderungen der DSGVO zur Dokumentation technisch umgesetzt werden können und wie der Verantwortliche oder Auftragsverarbeiter dadurch unterstützt wird.
Nachdem die theoretischen Anforderungen herausgearbeitet wurden, wird sich in Kapitel 4 damit beschäftigt, welche anderen wissenschaftlichen Arbeiten es bereits

zum Thema DSGVO und deren Anforderungen gibt und wie sich diese von dieser Masterarbeit unterscheiden. Weiterhin werden vorhandene Softwareprodukte analysiert und hinsichtlich der Umsetzung der erarbeiteten Anforderungen untersucht, sowie in der Funktionsumsetzung verglichen.
Anschließend werden in Kapitel 5 Konzepte zur Umsetzung ergänzbarer Funktionen Software-spezifisch entwickelt, bevor in Kapitel 6 eine selbstständig implementierte Funktion ausführlich beschrieben wird. Zur Reflexion der eigenen Konzeption und Implementierung folgt in Kapitel 7 eine Evaluation, in der die Funktionsfähigkeit der Eigenentwicklung bewertet wird. Abschließend wird in Kapitel 8 die Arbeit zusammengefasst und ein Ausblick zur weiteren Entwicklung und Verwendung von Datenschutzmanagement-Software präsentiert.

2 Grundlagen

Im folgenden Kapitel werden grundlegende Begriffe erklärt, welche von Bedeutung sind, um zu verstehen, wie die Dokumentationspflichten zustande kommen. Es wird zunächst erklärt, was *personenbezogene Daten* (2.1) und *besondere personenbezogene Daten* (2.2) sind. Nachdem diese Begriffe verdeutlicht wurden, kann erklärt werden, was die *Datenschutz-Grundverordnung* (2.3) im Allgemeinen ist und warum sie für die Dokumentationspflichten wichtig ist. Anschließend wird auf die *Rechenschafts- und Nachweispflichten* (2.4) eingegangen, die in der DSGVO verankert sind. Es wird hervorgehoben, welche Absätze der DSGVO Rechenschafts- und Nachweispflichten definieren und welche Anforderungen an die Dokumentationspflicht daraus abgeleitet werden können.

2.1 Personenbezogene Daten

Unter *Personenbezogene Daten* fallen laut Artikel 4 DSGVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen“.[Amt22] Unter einer *identifizierten Person* versteht man eine natürliche Person, der personenbezogene Daten direkt zugeordnet werden können. Ist die Zuordnung personenbezogener Daten zu einer natürlichen Person nur mithilfe von weiterem Zusatzwissen möglich, spricht man von einer *identifizierbaren Person.* Als *natürliche Person* ist jede lebende Einzelperson zu verstehen.
Grundsätzlich gelten alle Daten, mit deren Hilfe ein Personenbezug hergestellt werden kann, als personenbezogen. Beispiele für solche Daten sind Name, Adresse, Telefonnummer, Kreditkartennummer, Autokennzeichen, Kontodaten oder die IP-Adresse. Auch physische Daten wie das Aussehen gehören zu den personenbezogenen Daten. Daten zu einer natürlichen Person, die für sich alleine gestellt keinen direkten Bezug zu der Person herstellen können, heißen anonymisierte Daten. Zum Beispiel das Alter oder die Körpergröße ohne weitere Zusatzinformationen. Gibt es jedoch Daten, mit deren Hilfe die anonymisierten Daten wieder einer natürlichen Person zugeordnet werden können, spricht man lediglich von pseudonymisierten Daten.[Lan22] Im Bereich der Verarbeitung personenbezogener Daten wird mit dem Verbotsprinzip gearbeitet. Das bedeutet, dass es dem Datenverarbeiter nicht gestattet ist, personenbezogene Daten zu verarbeiten, bevor die betroffene Person der Verarbeitung aktiv zugestimmt hat.

2.2 Besondere personenbezogene Daten

Neben den personenbezogenen Daten, die in Abschnitt 2.1 erläutert wurden, gibt es noch spezielle Kategorien von personenbezogenen Daten. Für diese wird ein noch sensiblerer Umgang gefordert. In Art. 9 Abs.1 DSGVO wird beschrieben, welche Kategorien personenbezogener Daten unter die besonderen personenbezogenen Daten fallen:

- Daten aus denen folgendes über eine natürliche Person hervorgeht:
  - rassische oder ethnische Herkunft
  - politische Meinung
  - religiöse oder weltanschauliche Überzeugung
  - Gewerkschaftszugehörigkeit
- genetische Daten
- biometrische Daten, die eine natürliche Person eindeutig identifizieren
- Gesundheitsdaten
- Daten zum Sexualleben und der sexuellen Orientierung

Art. 9 Abs. 4 DSGVO erlaubt es den Mitgliedsstaaten der Europäische Union (EU) zusätzliche Bedingungen einzuführen, wenn von der Verarbeitung genetische, biometrische oder Gesundheitsdaten betroffen sind. Dies ist ein Beispiel für eine Öffnungsklausel, nach der die EU-Mitgliedsstaaten Teile der DSGVO auf der Ebene nationaler Gesetzestexte weiter auslegen können. Das Bundesdatenschutzgesetz (BDSG) fasst diese Öffnungsklausel in §22 BDSG auf. Dort werden die Bedingungen für die Verarbeitung personenbezogener Daten mit Gültigkeit für die Bundesrepublik Deutschland beschrieben.[Bun22]

2.3 Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung wurde am 27. April 2016 veröffentlicht und trat mit Wirkung zum 25. Mai 2018 in Kraft. Sie regelt den Datenschutz auf europäischer Ebene und dient dazu, die Verarbeitung personenbezogener Daten zu regulieren, sowie einen freien Datenverkehr in der EU zu ermöglichen. Die DSGVO steht über den Gesetzen der Staaten, räumt ihnen aber ein, in bestimmten Bereichen durch Öffnungsklauseln individuelle Gesetzeserweiterungen zu treffen. In Deutschland wird die DSGVO durch das BDSG und die Landesdatenschutzgesetze (LDSG) ergänzt. Dadurch sollen die personenbezogenen Daten von natürlichen Personen der EU vor Missbrauch geschützt werden. Die DSGVO ist sowohl auf die automatisierte, als auch die manuelle Verarbeitung personenbezogener Daten anzuwenden. Sie muss von allen Verantwortlichen oder Auftragsverarbeitern mit

einer Niederlassung in der EU umgesetzt werden, wenn sie personenbezogene Daten verarbeiten. Auch Verantwortliche und Auftragsverarbeiter, die außerhalb der EU niedergelassen sind, müssen die DSGVO umsetzten, wenn sie personenbezogene Daten von natürlichen Personen verarbeiten, die sich in der EU befinden. Unter *Verantwortlicher* ist in diesem Kontext die Person, Behörde, Einrichtung oder andere Stelle gemeint, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Als *Auftragsverarbeiter* ist hingegen die Person, Behörde, Einrichtung oder andere Stelle zu verstehen, die im Auftrag des Verantwortlichen personenbezogene Daten verarbeitet. Diese Informationen sind in der Datenschutz-Grundverordnung in den Artikeln 1–4 zu finden.[Amt22]
Um personenbezogene Daten DSGVO-konform zu verarbeiten, muss sich die verarbeitende Stelle an die sechs vorgeschrieben Grundsätze der DSGVO halten.

Rechtmäßigkeit:
Die Verarbeitung personenbezogener Daten muss auf rechtmäßige Weise, nach bestem Wissen und Gewissen und in nachvollziehbarer Weise für die betroffene Person durchgeführt werden.

Zweckbindung:
Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitimierte Zwecke verarbeitet werden. Eine Weiterverarbeitung außerhalb der vereinbarten Zwecke ist nicht zulässig.

Datenminimierung:
Die Masse an erhobenen personenbezogenen Daten muss auf das notwendige Maß der für die Verarbeitung nach dem legitimen Zweck benötigten Daten beschränkt werden.

Richtigkeit:
Die sachliche Richtigkeit personenbezogener Daten muss für die Verarbeitung sichergestellt sein. Falsche Daten müssen gelöscht oder berichtigt werden.

Speicherbegrenzung:
Kann durch die Speicherung personenbezogener Daten eine betroffene Person identifiziert werden, ist die Speicherung nur so lange zulässig, wie sie für die Verarbeitung im Sinne des legitimen Zweckes notwendig ist.

Integrität und Vertraulichkeit:
Die Verarbeitung personenbezogener Daten muss durch technische und organisatorische Maßnahmen so abgesichert sein, dass die angemessene Sicherheit gewährleistet werden kann. Ferner müssen die Daten vor unberechtigter oder unbefugter Verarbeitung, sowie versehentlichem Verlust, versehentlicher Zerstörung oder Beschädigung geschützt werden.

Bezüglich dieser Grundsätze ist der Verantwortliche in der Pflicht, die Einhaltung gegenüber der Aufsichtsbehörde nachzuweisen. Diese Nachweispflicht wird auch Rechenschaftspflicht genannt. Diese Informationen sind in der Datenschutz-Grundverordnung im Artikel 5 zu finden.[Amt22] Um dieser Rechenschaftspflicht

nachzukommen, besteht die Möglichkeit Dokumentationen anzulegen, damit die Umsetzung gewisser Anforderungen aus der DSGVO nachgewiesen werden können. Im Abschnitt 2.4 wird auf die Anforderungen zur Dokumentation nach der DSGVO weiter eingegangen.

2.4 Rechenschafts- und Nachweispflichten

Neben der bereits angesprochenen Rechenschaftspflicht aus 2.3, welche in Art. 5 Abs. 2 DSGVO zu finden ist, gibt es noch weitere Nachweispflichten, die in der DSGVO an verschiedenen Stellen gefordert werden. Aus diesen weiteren Pflichten gehen auch Anforderungen für die Dokumentation hervor. Im Folgenden werden erst die weiteren Nachweispflichten zusammengefasst und anschließend die daraus resultierenden Anforderungen an die Dokumentation.

2.4.1 Gesetze

Alle Artikel, die in diesem Absatz aufgelistet werden, stammen aus der DSGVO.

Art. 5 Abs. 2: Allgemeine Rechenschaftsplficht
Die allgemeine Rechenschaftspflicht bezieht sich darauf, dass der Verantwortliche nachweisen muss, dass er die Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 DSGVO einhält. Welche Grundsätze das sind, wurde bereits in Kapitel 2.3 erläutert.

Art. 24 Abs. 1: Allgemeine Nachweispflicht
In Art. 24. Abs. 1 DSGVO wird allgemein aufgegriffen, dass der Verantwortliche in der Pflicht steht nachzuweisen, dass die durch ihn durchgeführte Verarbeitung personenbezogener Daten DSGVO-konform durchgeführt wird. Dazu muss er geeignete technische und organisatorische Maßnahmen (TOMs) umsetzen, die unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung angemessen sind. Außerdem müssen die Maßnahmen, hinsichtlich der Eintrittswahrscheinlichkeiten und Schwere möglicher Risiken für den Schutz der betroffenen natürlichen Personen, angepasst werden.

Art. 30 Abs. 3: Verzeichnis von Verarbeitungstätigkeiten
Das Verzeichnis von Verarbeitungstätigkeiten stellt den Mittelpunkt der Dokumentationspflicht dar. Nach Art. 30 Abs. 1 DSGVO muss jeder Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten führen, die in ihrer Zuständigkeit liegen. Art. 30 Abs. 2 DSGVO fordert auch von allen Auftragsverarbeitern ein Verzeichnis von Verarbeitungstätigkeiten, die der Auftragsverarbeiter im Auftrag des Verantwortlichen durchführt. Diese VVTs sind nach Art. 30 Abs. 3 DSGVO schriftlich zu führen. Dabei kann die Umsetzung analog oder digital erfolgen. Für Unternehmen mit weniger als

250 beschäftigten Mitarbeitern setzt Art. 30 Abs. 5 DSGVO die Pflicht zur Führung eines VVT jedoch nicht voraus. Allerdings sind diese Unternehmen nur von der Dokumentation befreit, wenn sie nicht regelmäßig personenbezogene Daten oder besondere Kategorien personenbezogener Daten verarbeiten und kein Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen bestehen.

Art. 33 Abs. 5: Datenschutzvorfall
Sollte es zu einer Verletzung des Schutzes personenbezogener Daten kommen, ist der Verantwortliche nach Art. 33. Abs. 5 DSGVO in der Pflicht, diesen Vorfall zu dokumentieren. Dazu zählen auch alle Fakten, die mit dem Vorfall in Zusammenhang stehen, die Auswirkung des Vorfalls und die Abhilfemaßnahmen, die ergriffen wurden.

Art. 35 Abs. 1: Datenschutz-Folgenabschätzung
Wenn die Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen birgt, ist der Verantwortliche nach Art. 35 Abs. 1 DSGVO in der Pflicht, eine Datenschutz-Folgenabschätzung durchzuführen und zu dokumentieren. Für ähnliche Verarbeitungsprozesse mit ähnlich hohem Risiko reicht es aus, eine einzige Abschätzung durchzuführen.

Für die folgenden Artikel und Empfehlungen gibt es keine direkte Pflicht zur Dokumentation. Jedoch bietet es sich an, schriftliche Vermerke in diesen Bereichen festzuhalten.

Art. 6 Abs.1 lit. b: Verarbeitungsvertrag
Aufgrund der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO ist es sinnvoll, dass der Verantwortliche abgeschlossene Verträge zwischen ihm und der Person, die den angebotenen Dienst bezieht, dokumentiert und sicher aufbewahrt. Dadurch kann die rechtmäßige Verarbeitung nach Art. 6 Abs. 1 lit. b DSGVO jederzeit nachgewiesen werden.

Art. 28 Abs.3: Auftragsverarbeiter-Vertrag
Damit der Verantwortliche nachweisen kann, dass die Zusammenarbeit mit einem Auftragsverarbeiter auf einem DSGVO-konformen Vertrag beruht, kann der Verantwortliche den abgeschlossenen Auftragsverarbeiter-Vertrag dokumentieren und sicher aufbewahren. Dadurch hat er die Chance, dass er im Falle eines Vorfalls bei dem Auftragsverarbeiter nachweisen kann, dass er vertraglich für eine DSGVO-konforme Verarbeitung gesorgt hat.

Art. 17 Abs.1: Recht auf Löschung und Art. 30 Abs. 1 lit. f: Löschfristen
Grundsätzlich ist der Verantwortliche dazu verpflichtet, nach Art. 17 Abs. 1 lit. a DSGVO personenbezogene Daten zu löschen, wenn sie nicht mehr für den Zweck der vorherigen Erhebung oder sonstigen Verarbeitung benötigt werden. Aber auch wenn eine betroffene Person die Einwilligung zur Verarbeitung widerruft und keine andere Rechtsgrundlage zur weiteren Verarbeitung vorliegt, müssen die personenbezogenen Daten dieser Person gemäß

Art. 17 Abs. 1 lit. b DSGVO gelöscht werden. Es gibt noch weitere Fälle, bei denen der Verantwortliche in der Pflicht zur Löschung steht, aber im Endeffekt läuft es immer auf das gleich Problem hinaus. Der Verantwortliche muss darauf achten, dass alle Datensätze, auch in Backups und Datenbanken der Auftragsverarbeiter gelöscht werden. Auch nach Art. 30 Abs. 1 lit. f DSGVO wird gefordert, dass Löschfristen für die verschiedenen Kategorien personenbezogener Daten dokumentiert werden. Um diesen Anforderungen gerecht zu werden und die vollständige Löschung sicherstellen zu können, kann ein Löschkonzept dokumentiert werden, um im Fall einer nötigen Löschung einen Ablauf zur vollständigen Löschung vorweisen zu können.

Datenschutzrichtlinie[Dr.22]
Um für die Mitarbeiter eine Richtlinie zur Umsetzung des Datenschutzes bereitzustellen, kann der Verantwortliche eine Datenschutzrichtlinie definieren, dokumentieren und für die Mitarbeiter verfügbar halten. Diese Richtlinie sollte die unternehmensinterne Umsetzung der Datenschutzgrundsätze enthalten und beschreiben, wie in einem Unternehmen Datenschutzvorfälle gehandhabt werden. Außerdem sollte definiert werden, wie das Unternehmen die Vorgänge zur Erfüllung der Betroffenenrechte umsetzt.

2.4.2 Anforderungen

Einige der bereits im Abschnitt 2.4.1 genannten Artikel werden in weiteren Absätzen detaillierter beschrieben. Im Folgenden sollen die Anforderungen aus den Artikeln zusammengefasst werden, um daraus später die Erkenntnis ziehen zu können, welche Anforderungen an eine Software zur Dokumentation in den einzelnen Bereichen aus der DSGVO gestellt werden. Alle Artikel, die in diesem Absatz aufgelistet werden, stammen aus der DSGVO. Die Anforderungen an ein Löschkonzept wurden aus der „Leitlinie zur Entwicklung eines Löschkonzeptes mit Ableitung von Löschfristen für personenbezogene Daten“ des Deutschen Institut für Normen abgeleitet.

Art. 30 Abs. 1: VVT – Verantwortlicher

a) Name und Kontaktdaten:
   - des/der Verantwortlichen
   - des Vertreters des Verantwortlichen
   - des Datenschutzbeauftragten
b) Zweck der Verarbeitung
c) Kategorien betroffener Personen und Kategorien personenbezogener Daten

d) Kategorien von Empfängern personenbezogener Daten, inkl. Empfänger in Drittländern oder internationalen Organisationen

e) Übermittlung in ein Drittland oder eine internationale Organisation:

- Nennung des Drittlandes oder der internationalen Organisation
- Bei Datenübermittlungen nach Art. 49. Abs. 1 Unterabsatz 2 Dokumentation geeigneter Garantien

f) Löschfristen der verschiedenen Datenkategorien

g) Beschreibung TOMs nach Art. 32 Abs. 1 DSGVO

Art. 30 Abs. 2: VVT – Auftragsverarbeiter

a) Namen und Kontaktdaten:

- des Autragsverarbeiters/der Auftragsverarbeiter
- jedes Verantwortlichen, in dessen Auftrag gehandelt wird
- des Vertreters des Verantwortlichen oder Auftraggebers
- des Datenschutzbeauftragten

b) Kategorien von Verarbeitungen

c) Übermittlung in ein Drittland oder eine internationale Organisation:

- Nennung des Drittlandes oder der internationalen Organisation
- Bei Datenübermittlungen nach Art. 49. Abs. 1 Unterabsatz 2 DSGVO: Dokumentation geeigneter Garantien

d) Beschreibung TOMs nach Art. 32 Abs. 1 DSGVO

Art. 33 Abs. 3: Datenschutzvorfall

a) Angaben zu:

- Art der Verletzung des Schutzes personenbezogener Daten
- Kategorie und Anzahl betroffener Personen
- Kategorie und Anzahl betroffener personenbezogener Datensätze

b) Name und Kontaktdaten des Datenschutzbeauftragten oder anderer verantwortlicher Stelle

c) Beschreibung der wahrscheinlichen Folgen des Datenschutzvorfalls

d) Beschreibung zu:

- ergriffene oder vorgeschlagene Maßnahmen zur Behebung durch den Verantwortlichen

- Maßnahmen zur Eindämmung möglicher negativer Folgen

Art. 35 Abs. 7: Datenschutz-Folgenabschätzung

a) systematische Beschreibung von:
   - geplanten Verarbeitungsvorgängen
   - Zweck der Verarbeitung
   - verfolgte Interessen

b) Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge bezüglich des Zweckes

c) Bewertung der Risiken hinsichtlich der Rechte und Freiheiten betroffener Personen bezüglich Art. 35 Abs. 1 DSGVO

d) geplante Abhilfemaßnahmen, inkl. Garantien, Sicherheitsvorkehrungen und Verfahren, um den Schutz der personenbezogenen Daten sicherzustellen und die DSGVO-konforme Verarbeitung nachweisen zu können

Löschkonzept [Ham22]

- erhobene Datenarten
- Löschfristen
- Systeme in denen die personenbezogenen Daten abgelegt werden
- Datenweitergabe – Auftragsverarbeiter
- Löschbeauftragter

3 Analyse der technischen Umsetzung

In diesem Kapitel wird die Frage beantwortet, ob die Anforderungen an die Dokumentation durch die Rechenschafts- und Nachweispflichten der DSGVO aus Abschnitt 2.4.2 technisch umgesetzt werden können. Dabei wird unter anderem betrachtet, ob eine manuelle oder automatische Dokumentation möglich ist, in welcher Form die einzelnen Dokumentationen miteinander verbunden sind und wie die technische Umsetzung den Verantwortlichen oder Auftragsverarbeiter unterstützt.
Im Folgenden wird zusammengefasst, was eine technische Umsetzung enthalten sollte, um den Ansprüchen der DSGVO bezüglich der Rechenschafts- und Nachweispflichten mit Dokumentationen gerecht zu werden und was darüber hinaus den Verantwortlichen oder Auftragsverarbeiter bei seinen Nachweispflichten unterstützt.

- Verzeichnis von Verarbeitungstätigkeiten
- Dokumentation von Datenschutzvorfällen
- Datenschutz-Folgenabschätzungen
- Löschkonzept
- Verarbeitungsverträge
- Auftragsverarbeiter-Verträge
- unternehmerische Datenschutzrichtlinie

Den größten Umfang stellt das VVT dar. Neben dem Namen und den Kontaktdaten des oder der Verantwortlichen, des Vertreters des oder der Verantwortlichen und des Datenschutzbeauftragten muss der Zweck der Verarbeitung dokumentiert werden. An dieser Stelle besteht die erste Verknüpfung zu weiteren Dokumentationen. Eine Art des Zweckes der Verarbeitung ist ein Vertrag mit der oder den betroffenen Personen (Art 6 Abs. 1 lit. a und b DSGVO). Demnach können die Verarbeitungsverträge an dieser Stelle integriert werden, um einer Verarbeitungstätigkeit den möglicherweise zugrunde liegenden Verarbeitungsvertrag hinterlegen zu können.
Eine weitere Forderung des VVT ist die Dokumentation der Kategorien betroffener Personen und personenbezogenen Daten. Wenn dabei festgestellt wird, dass eine umfangreiche Verarbeitung besonderer personenbezogener Daten stattfindet, muss eine Datenschutz-Folgenabschätzung durchgeführt und dokumentiert werden (Art. 35 Abs. 3 lit. b DSGVO). Die nötige Datenschutz-Folgenabschätzung kann

an dieser Stelle in das Verzeichnis von Verarbeitungstätigkeiten integriert werden. Als Nächstes fordert das VVT von dem Verantwortlichen, dass die Kategorien von Empfängern personenbezogener Daten dokumentiert werden. Dies schließt auch die Auftragsverarbeiter mit ein. Wenn der Verantwortliche Verarbeitungen an Auftragsverarbeiter abgibt, muss er nachweisen, dass er für die DSGVO-konforme Verarbeitung bei dem Auftragsverarbeiter gesorgt hat. Diesen Nachweis kann er am besten erbringen, indem er die Bedingungen zur Verarbeitung in einem Auftragsverarbeiter-Vertrag dokumentiert und diesen Vertrag mit dem Auftragsverarbeiter abschließt. Um im Falle eines Datenschutzvorfalls auf Seiten des Auftragsverarbeiters diesen Nachweis parat zu haben, kann der Vertrag der Dokumentation zur Datenweitergabe als Grundlage hinzugefügt werden.
Die Anforderung zur Dokumentation von Löschfristen für die verschiedenen Kategorien personenbezogener Daten in einem VVT lässt sich durch ein Löschkonzept umsetzen. In diesem können Löschkategorien mit den betroffenen Datenarten, passenden Löschfristen und Ablageorten der Daten dokumentiert werden. Zudem kann ein Löschbeauftragter bestimmt werden, der für die Löschung zuständig ist. Dieses Löschkonzept kann dem Verantwortlichen zum Zeitpunkt der nötigen Löschung helfen zu erkennen, welche Daten gelöscht werden müssen, wo sie abgelegt sind und wer dafür zuständig ist. Diese Löschung kann nicht nur durch die Löschfrist erforderlich werden, sondern auch durch das Recht auf Löschung gemäß Art. 17 Abs. 1 DSGVO. Ein Löschkonzept kann demnach das Risiko minimieren, dass Löschungen ganz oder teilweise vergessen werden. Auch dieses Löschkonzept lässt sich in das VVT integrieren und bietet eine Unterstützung für den Verantwortlichen. Abschließend fordert das VVT noch die Beschreibung eingesetzter TOMs. In diesem Bereich bieten die weiteren Dokumentationen keine Unterstützung.
Im Falle eines Datenschutzvorfalls hilft das Gesamtkonzept der beschriebenen Dokumentationen dem Verantwortlichen zu erkennen, welche Kategorien personenbezogener Daten und Kategorien betroffener Personen in den Vorfall involviert sind. Das ist wichtig, da der Verantwortliche entscheiden muss, ob er die betroffenen Personen nach Art. 34 DSGVO über den Vorfall informieren muss. Bei der Entscheidung helfen die dokumentierten TOMs in den betroffenen Verarbeitungsvorgängen, da bei ausreichend sicheren TOMs eine Benachrichtigung nicht nötig ist, zum Beispiel, wenn die betroffenen personenbezogenen Daten durch Verschlüsselung zugriffs-beschränkt sind. Auch die Behandlung eines Datenschutzvorfalls muss durch den Verantwortlichen dokumentiert werden.
Neben den nötigen Dokumentationen sollte auch noch eine unternehmerische Datenschutzrichtlinie erstellt werden. Dadurch kann der Verantwortliche nachweisen, dass sein Personal datenschutzkonform eingewiesen wurde und das Unternehmen datenschutzkonform eingestellt ist.
Um den Überblick über die Einzeldokumentationen nicht zu verlieren und eine Verknüpfung dieser zu erleichtern, erscheint es praktikabel, dass eine technische Umsetzung nicht nur einzelne Dokumentationen unterstützt, sondern in einem Datenschutz-Management-Tool umgesetzt wird. Dadurch kann dem Verantwortlichen eine Plattform geboten werden, die es ihm erlaubt, die einzelnen Dokumentationen gesammelt abzulegen und innerhalb der Software zu verknüpfen. So kann er

zum Beispiel einen TOM-Katalog hinterlegen, indem alle technischen und organisatorischen Maßnahmen hinterlegt sind, die in dem Unternehmen angeboten werden und kann bei der Erstellung einer neuen Verarbeitungstätigkeit auf die eingesetzten TOMs verweisen. Ähnlich kann die Verknüpfung von Auftragsverarbeitern funktionieren. Der Verantwortliche kann einen Katalog mit allen Auftragsverarbeitern erstellen und darin auch die Auftragsverarbeiter-Verträge hinterlegen. Bei der Erstellung einer neuen Verarbeitungstätigkeit kann er dann die betroffenen Auftragsverarbeiter aus diesem Katalog mit der Verarbeitungstätigkeit verknüpfen.
Durch eine Software, die all diese Anwendungsfälle abdeckt, hat der Verantwortliche eine zentrale Anlaufstelle für Arbeiten, die den Datenschutz und die Verarbeitung personenbezogener Daten betreffen. Dieses Tool könnte zum Beispiel durch den Datenschutzbeauftragten alleine verwaltet werden. Ebenso ist es denkbar, dass der Datenschutzbeauftragte durch weitere verantwortliche Personen einzelner Abteilungen in der Pflege der Dokumentationen unterstützt wird.
Da sowohl neue Verarbeitungstätigkeiten, als auch Datenschutz-Folgenabschätzungen, Verarbeitungsverträge, Auftragsverarbeitungsverträge, Datenschutzvorfälle und Löschfristen sich nicht automatisch eintragen lassen, wird eine Software zum Datenschutzmanagement immer eine Person benötigen, die sie pflegt. Die Erinnerung an Löschungen von Datensätzen und das Erstellen einer aussagekräftigen Übersicht aus den Datenbanken der Software für die Aufsichtsbehörde lassen sich sicherlich automatisieren. Auch eine vollständige Automatisierung der Löschung ist möglich, wie ein Praxisbericht von Christian Knuchel und Nico Ebert zeigt.[KE22] Diese Arbeit wird in Abschnitt 4.1 näher behandelt. Jedoch sind diese Automationen nur unterstützend. Die grundlegenden Dokumentationen müssen manuell getätigt werden, da es zu viele unregelmäßige Variablen gibt. Eine neue Verarbeitungstätigkeit muss zum Beispiel manuell erstellt werden, damit die Software mit Daten gefüllt wird. Ebenso verhält es sich mit dem TOM-Katalog, Auftragsverarbeiter-Katalog, Löschkonzept, den Kategorien personenbezogener Daten und betroffener Personen sowie Verträgen. Dazu kommt noch, dass jedes Unternehmen ein anderes Profil von Datensätzen benötigt. Das Grundgerüst benötigen alle Unternehmen, die zur Dokumentation verpflichtet sind. Doch welche Kategorien personenbezogener Daten und betroffener Personen behandelt werden, kann sich individuell unterscheiden. Das trifft unter anderem auch auf die Auftragsverarbeiter und die aufgesetzten Verträge, sowie die im Unternehmen umgesetzten TOMs und die unternehmerische Datenschutzrichtlinie zu. Es gibt viele Wege, um das Ziel des geforderten Datenschutzes zu erreichen.

4 Verwandte Arbeiten

Nachdem in Kapitel 3 herausgearbeitet wurde, in welcher Form eine technische Umsetzung praktikabel erscheint, wird sich in diesem Kapitel damit beschäftigt, welche wissenschaftlichen Arbeiten sich ebenfalls schon mit diesem Themengebiet beschäftigt haben und was dabei herausgefunden wurde. Anschließend wird herausgearbeitet, welche Softwareprodukte es bereits gibt und wie die Entwickler die verschiedenen Anforderungen in diesen umgesetzt haben.

4.1 Wissenschaftliche Arbeiten

Wie in Abschnitt 2.4.2 herausgearbeitet wurde, formuliert die DSGVO verschiedene Anforderungen zur Dokumentation. Seit der Einführung der DSGVO im Jahr 2016 haben sich verschiedene Verantwortliche selbst um praktische Umsetzungsmöglichkeiten bemüht. Zudem sind wissenschaftliche Arbeiten entstanden, die sich mit verschiedenen Themen rund um die DSGVO-konforme Dokumentation und Datenerfassung befassen. Im Folgenden werden Arbeiten betrachtet, welche sich auch mit dem Thema DSGVO und deren Anforderungen auseinandergesetzt haben.

Datenschutzgrundverordnung (DSGVO): Bewältigung der Herausforderungen mit Unternehmensarchitekturmanagement (EAM)

Gümüs at al. befassen sich in ihrer Arbeit „Datenschutzgrundverordnung (DSGVO): Bewältigung der Herausforderungen mit Unternehmensarchitekturmanagement (EAM)“ [KEF18] mit der Forschungsfrage, wie Unternehmen dabei unterstützt werden können, ein DSGVO-Projekt aus Enterprise Architecture Management (EAM)-Sicht zu initiieren. Unter Enterprise Architecture (EA) versteht man die Verknüpfung von Informationen über verschiedene Domänen hinweg, sodass eine ganzheitliche Sicht auf die wesentlichen Artefakte eines Unternehmens möglich wird. Durch das Management kann eine architektonische Transparenz geschaffen werden, die es ermöglicht, schnell auf Veränderungen reagieren zu können. Die dafür notwendigen Dokumentationen von Organisationen aus verschiedenen Blickwinkeln inklusive verschiedener Stakeholder, wie zum Beispiel Prozessverantwortliche oder Service-Manager, können als Ausgangspunkt zur konformen Dokumentation der DSGVO-Anforderungen dienen.

Das Konzept zur Einführung eines DSGVO-Projektes sieht eine Prozedur von fünf Phasen vor. In der ersten Phase werden die Projektvorbereitungen getroffen. Dazu werden die Anforderungen erarbeitet, ein Projektplan erstellt und die betroffenen Abteilungen für den Datenschutz und die Anforderungen nach der DSGVO sensibilisiert. Abschluss dieser Phase ist die Fertigstellung des Projektplans und die Veröffentlichung im Intranet des Unternehmens.
In der zweiten Phase werden die für das DSGVO-Projekt relevanten Systeme erfasst und kategorisiert. Dazu müssen zunächst alle Tools, Technologien und Anwendungen des Unternehmens, die personenbezogene Daten verarbeiten, identifiziert werden. Diese werden hinsichtlich ihrer Relevanz für das DSGVO-Projekt geprüft und bewertet, sodass eine bewertete Liste aller betroffenen Systeme entsteht. In der dritten Phase werden alle Daten und betroffenen Personen klassifiziert, sodass der Liste von relevanten Systemen Daten- und Personenkategorien hinzugefügt werden können.
Die vierte Phase dient dazu, dass in Workshops alle Verarbeitungstätigkeiten des Unternehmens erfasst und validiert werden können. Dazu müssen alle identifizierten Stakeholder in diese Phase integriert werden. Nach Abschluss dieser Phase kann in der finalen Phase das VVT erstellt werden.
Die Autoren stellen fest, dass zwischen den erhobenen und dokumentierten Daten für das VVT und den typischen Artefakten einer Enterprise Architecture eine enge Verbindung besteht. Daten, die zur VVT-Dokumentation erhoben werden, müssen auch im Kontext von EAM-Projekten erhoben werden. Deshalb kommen die Autoren zu dem Schluss, dass man das VVT mit den EA Artefakten verknüpfen kann, um redundante Datenerhebungen und Dokumentationen zu vermeiden.
In der Arbeit von Gümüs, Köhler, Schulz und Rasche wurde in erster Linie ein Konzept zur Erarbeitung VVT-relevanter Daten vorgestellt und in den Zusammenhang mit EAM gebracht. Die fünf Phasen Prozedur zur Erhebung VVT-relevanter Daten bildet die Vorbereitung ab, um im weiteren Verlauf die nötigen Dokumentationen ausfüllen zu können. Auch die Feststellung, dass bei einem EAM-Projekt viele gleiche Daten erhoben werden müssen, ist eine wichtige Erkenntnis. Dadurch kann den Nutzern von Datenschutzmanagement-Software, wie die, die in dieser Masterarbeit betrachtet wird, ein Weg aufgezeigt werden, aus welchen Quellen sie Informationen zur Befüllung der Dokumentationen entnehmen können. Diese Masterarbeit befasst sich im Gegensatz zu der hier betrachteten Arbeit mit den Anforderungen der DSGVO und deren Umsetzung in Datenschutzmanagement-Tools. In diesen Tools können die erarbeiteten Daten dokumentiert werden. Dabei achtet diese Masterarbeit auf die vollständige Implementierung aller Anforderungen der DSGVO.

Konzept eines Modells zur ganzheitlichen Datenschutzbetrachtung unter Anwendung von Data Mining

Koc at al. befassen sich in ihrer Arbeit „Konzept eines Modells zur ganzheitlichen Datenschutzbetrachtung unter Anwendung von Data Mining“ [GKSR21] mit der

Frage, wie Data Mining zur Einhaltung des Datenschutzes in Unternehmen entwickelt werden kann. Dabei wird der Schwerpunkt auf die Pflege des VVT gerichtet, da das VVT das Kernelement der DSGVO-Dokumentationen bildet. In der Arbeit wird geprüft, welche technologischen Anforderungen nötig sind, um mithilfe von Data Mining die Vollständigkeit und Aktualität des VVT sicherstellen zu können. Zudem wird sich damit beschäftigt, wie Data Mining effizient umgesetzt, die Komplexität der Arbeitsvorgänge verringert und die Flexibilität der Geschäftsprozesse erhöht werden kann.
Die Autoren entwickeln ein Konzept zur Datenerhebung mittels Data Mining nach dem Cross Industry Standard Process for Data Mining (CRISP-DM)-Model. Dieses Model besteht aus sechs Phasen und hat keinen festen Endpunkt. Die Phasen können ja nach Problemstellung mehrfach durchlaufen und ausdifferenziert werden. In der ersten Phase soll ein Umsetzungsplan aufgestellt werden, der die zeitlichen, personellen und sachlichen Ressourcen berücksichtigt. Um diesen Plan aufstellen zu können, müssen Zielkriterien festgestellt werden, aus denen anschließend Anforderungen an die Datenanalyse abgeleitet werden.
Die zweite Phase dient der Selektierung relevanter Datenbestände, deren Verarbeitung zur Zielerfüllung notwendig ist. Nach dem Anlegen einer Datensammlung mit Beschreibung der typischen Eigenschaften der Daten endet diese Phase mit einer Bewertung der Datenqualität und -quantität. Um das Data-Mining-System mit der richtigen Datenmenge füllen zu können, wird in der dritten Phase die Datenvorbereitung durchgeführt. Dabei werden irrelevante und relevante Daten klar voneinander getrennt und dahingehend bereinigt, dass das Data-Mining-System die Datenauswahl mit vordefinierten und anwendungsspezifischen Algorithmen erfolgreich verarbeiten kann.
In der vierten Phase wird mittels Modellbildung die Präzision und Qualität des Entwicklungsergebnisses geprüft und bewertet. Das Entwicklungsergebnis wird anschließend in Phase fünf durch den Vergleich der Zielsetzung mit dem erarbeiteten Data-Mining-Verfahren evaluiert. Wenn die Qualität des Modells zur Erfüllung der Zielkriterien nicht vollständig erreicht werden konnte, muss CRISP-DM wiederholt werden. In Phase sechs wird abschließend die Implementierung des Data-Mining im Unternehmen geplant und umgesetzt.
Die Autoren stellen fest, dass die ersten drei Phasen auch durchlaufen werden müssen, wenn das VVT manuell gepflegt wird. Deshalb ist es auch möglich, dass Unternehmen ihre bereits gepflegten Daten des VVT in KI-Algorithmen und Regeln überführen, um fortan ein Data-Mining-System die Arbeit durchführen zu lassen. Auch wenn kein Data-Mining-System eingeführt werden soll, helfen die Phasen des CRISP-DM-Modells Verarbeitungsprozesse hinsichtlich Erfassung, Dokumentation und Aktualisierung aufzubereiten. Weiter kommen die Autoren zu der Erkenntnis, dass Data-Mining zwar bei der vollständigen Erfassung personenbezogener Daten, dem Ableiten von Verarbeitungstätigkeiten, der Dokumentation und der Aktualisierung unterstützend genutzt werden kann. Nachgelagerte Prozesse, wie zum Beispiel die Zentralisierung von Verarbeitungstätigkeiten im VVT, die Überführung neuer datenschutzrechtlicher Vorgaben in konkrete Anforderungen an das Data-Mining-System oder die konstante Überwachung der Qualität der

Analyseergebnisse müssen jedoch weiterhin manuell durchgeführt werden.
Im Kern schafft die Arbeit von Koc, Eckert und Flaig ein Konzept zur Erhebung der Daten, die für die Dokumentation eines VVT relevant sind. An dieser Stelle werden die Daten mittels Data-Mining erhoben und geordnet in ein VVT übertragen. Dadurch unterscheidet sich diese Arbeit dahingehend von dieser Masterarbeit, dass ein Konzept zur Erhebung der Daten erstellt wird, während diese Masterarbeit Umsetzungen von Datenschutzmanagement-Tools betrachtet, in die diese erhobenen Daten übertragen werden können.

Löschkonzepte nach der DSGVO – ERP-Systeme

Der Autor Sven Hunzinger befasst sich in seiner Arbeit „Löschkonzepte nach der DSGVO am Beispiel von ERP-Systemen“ [Hun22] mit der Erstellung von Löschkonzepten nach der DSGVO. Dafür prüft er zunächst, ob es für Verantwortliche eine gesetzliche Pflicht zur Erstellung eines Löschkonzeptes nach der DSGVO gibt. Anschließend zeigt er auf, welche Fragen bezüglich Lösch- und Aufbewahrungspflichten geklärt werden müssen, bevor Verantwortliche ein Löschkonzept erstellen. Anhand von Enterprise Resource Planning (ERP)-Systemen behandelt er abschließend die praktische Erstellung von Löschkonzepten.
Wie auch in dieser Arbeit angemerkt, stellt Hunzinger fest, dass es keine explizite Regelung zur Erstellung eines Löschkonzeptes in der DSGVO gibt. Selbst das Wort „Löschkonzept“ ist in dem Gesetzestext nicht zu finden. Jedoch leitet sich aus anderen Pflichten zur Dokumentation ab, dass ein Löschkonzept den Verantwortlichen dabei unterstützen kann, die Rechenschaftspflicht, Informationspflicht, das VVT und weitere indirekte Verpflichtungen zu erfüllen. Weiter führt er auf, welche Lösch- und Aufbewahrungspflichten es gibt und dass es kompliziert ist, all diese Pflichten zu analysieren und in einem Löschkonzept zu berücksichtigen.
Bei der praktischen Erstellung von Löschkonzepten verweist Hunzinger auch auf die DIN 66398 „Leitlinie zur Entwicklung eines Löschkonzeptes mit Ableitung von Löschfristen für personenbezogene Daten“ [Ham22]. Auch er leitet aus dieser Norm die nötigen Informationen ab, die ein Löschkonzept enthalten sollte. Hunzinger betont, dass das Erstellen eines Löschkonzeptes für ein ERP-System schwer und kompliziert ist, da man jedes einzelne Datenfeld betrachten und mit einer Löschfrist versehen muss. Die daraus entstehende tabellarische Auflistung von Löschfristen für die einzelnen Datenfelder muss eng mit den Fachabteilungen und Verantwortlichen abgestimmt werden. Dies entspricht laut Hunzinger einer „Mammutaufgabe“, die jedoch durchgeführt werden muss, um den Anforderungen der DSGVO bezüglich gesetzestreuer Löschung gerecht zu werden.
Sven Hunzinger hat sich in seiner Arbeit auf das Erstellen eines Löschkonzeptes fokussiert. Speziell für ERP-Systeme hat er sich mit der praktischen Entwicklung eines Löschkonzeptes auseinandergesetzt. Diese Masterarbeit betrachtet einen ganzheitlichen Ansatz zur Erfüllung der Dokumentationspflichten, welche von der DSGVO gefordert werden und entwickelt die praktische Umsetzung in einer Datenschutzmanagement-Software weiter. Die Erkenntnisse von Hunzin-

ger sind informativ und werden in dieser Arbeit als Ausgangspunkt für weitere Forschung genutzt. Insbesondere die Informationen bezüglich der Inhalte eines Löschkonzeptes aus Abschnitt III seiner Arbeit unterstützen die herausgearbeiteten Inhalte eines Löschkonzeptes aus Abschnitt 2.4.2.

DSGVO-konformes Löschen

Die Autoren Christian Knuchel und Nico Ebert befassen sich in ihrer Arbeit „DSGVO-konformes Löschen“ [KE22] mit der konzeptionellen und technischen Umsetzung der Löschung von personenbezogenen Daten nach Artikel 17 DSGVO bei dem Unternehmen AXA Schweiz AG. Grundlage der Arbeit ist, dass die AXA Schweiz AG im Rahmen des unternehmensinternen DSGVO-Programms die DSGVO-Anforderungen gesetzeskonform umsetzen muss. Es wird hervorgehoben, dass die Löschung von personenbezogenen Daten dadurch erschwert wird, dass viele Anwendungen miteinander verbunden sind und Daten untereinander austauschen. Das führt dazu, dass Datensätze an mehreren Stellen gelöscht werden müssen und auch nur dann gelöscht werden dürfen, wenn keine Anwendung mehr Informationen dieser Datensätze benötigt. Die AXA Schweiz AG hatte vor der Einführung der DSGVO firmeninterne Aufbewahrungspflichten, nach denen Daten möglichst lange und sicher aufbewahrt wurden. Durch die DSGVO wird es nötig, einen Mechanismus zum endgültigen Löschen von personenbezogenen Daten zu schaffen.
Das Unternehmen verfolgte daraufhin den Lösungsansatz, personenbezogene Daten kontinuierlich zu löschen. Der Löschvorgang sollte dabei durch das Entfallen einer Rechtsgrundlage für die Verarbeitung der Daten eingeleitet werden. Der Löschvorgang soll eine Löschkette auslösen, die alle Speicherorte der Daten, Datentypen und die logische Reihenfolge, in der die Daten gelöscht werden sollen, enthält. Dadurch soll eine vollständige Löschung sichergestellt und einer Inkonsistenz zwischen den Anwendungen vorgebeugt werden. Die AXA Schweiz AG definierte im Rahmen des DSGVO-Programms 40 verschiedene Löschketten. Um die Löschung zu automatisieren wurde ein zentrales Metadaten-Managementsystem erarbeitet, welche nach dem „Hub-and-Spoke“-Ansatz arbeitet. Das bedeutet, dass das Managementsystem als zentrales Element die verschiedenen, dezentralen Anwendungen im Rahmen der automatischen Löschung verwaltet. Dadurch wird sichergestellt, dass Daten erst gelöscht werden, wenn keine rechtlichen Gründe, wie offene Rechnungen, dagegen sprechen. Der Löschvorgang wird in 5 Schritten durchgeführt.
Zu Beginn muss der Löschvorgang durch das Erlöschen der Rechtsgrundlage ausgelöst werden. Dann werden alle Daten in den Hauptsystemen selektiert, die für eine Löschung infrage kommen. Anschließend wird geprüft, ob seitens des Unternehmens Vorbehalte gegen die Löschung vorliegen. Wenn der Löschung nichts im Wege steht, werden anschließend die selektierten Daten gelöscht und der Löschvorgang wird protokolliert. Da es sich bei der automatischen Löschung um ein kompliziertes Vorgehen handelt, wurde die Umsetzung erst an einigen wenigen Systemen getestet, bevor anschließend weitere Löschketten schrittweise integriert wurde.

Im Rahmen dieser Auseinandersetzung mit der DSGVO-konformen Löschung von personenbezogenen Daten, haben die Autoren festgestellt, dass die hohe Komplexität und Abhängigkeit zwischen den Anwendungen ein hohes Risiko für die automatische Löschung darstellt. Durch das iterative Vorgehen konnte das Verfahren jedoch erfolgreich in die Geschäftsstruktur integriert werden und stellt einen neuen zentralen Baustein im Management des Lebenszyklus von personenbezogenen Daten dar. Dieser Lösungsansatz soll nach erfolgreicher Integration auch in anderen großen Unternehmen zum Einsatz kommen.
Während sich diese Masterarbeit mit allen Anforderungen der DSGVO und deren Umsetzung in einer Datenschutzmanagement-Software auseinandersetzt, hat die Arbeit von Knuchel ihren Fokus auf das automatische Löschen von personenbezogenen Daten in einem großen Unternehmen gesetzt. Die Erkenntnis, dass es möglich ist, die geforderte Löschung von personenbezogenen Daten DSGVO-konform zu automatisieren ist potentiell verwertbar. Jedoch stellt die Arbeit auch heraus, dass dazu ein erheblicher Aufwand nötig ist und die Automatisierung nur spezifisch für das Unternehmen funktioniert, mit dem sich hier beschäftigt wurde. Für andere große Unternehmen kann zwar das entwickelte Konzept angewendet werden, aber die technische Umsetzung wird nur individuell erfolgen können. Für große Unternehmen, wie die AXA Schweiz AG, ist es sinnvoll, ein solch aufwendiges Verfahren für die Definition von Löschketten anzuwenden, da viele personenbezogenen Daten verarbeiten und verwaltet werden müssen. Ein Datenschutzmanagement-Tool, welches kleinere und mittlere Unternehmen bei der Datenschutz-konformen Handhabung von personenbezogenen Daten unterstützt, hat nicht das Ziel den Menschen durch Automatisierung zu ersetzen, sondern sie bei der Arbeit zu unterstützen. Diese Erkenntnis ist bei der weiteren Betrachtung von Datenschutzmanagement-Tools zu beachten und kann zu einem späteren Zeitpunkt auch eine Rolle bei der Weiterentwicklung eines solchen Tools spielen.

4.2 Vorhandene Software

Im Rahmen einer Recherche konnte eine Vielzahl von kostenpflichtigen Datenschutzmanagement-Softwareprodukten gefunden werden. Im Folgenden eine namentliche Auswahl von Produkten (alphanumerisch sortiert):

- 2B Advice PrIME [adv22]
- Guardileo [fua22]
- otris privacy [otr22]
- preeco [pre22]
- Proliance360 [pro22]

Im Bereich der kostenlosen Datenschutzmanagement-Softwareprodukte wurde hingegen nur ein Produkt gefunden. Die Software *Open Datenschutzcenter* [ope22] ist

eine kostenlose und Open-Source-Software und stammt von dem Unternehmen H2 invent GmbH.[h2i22] Der Quellcode kann bei Github eingesehen und heruntergeladen werden.[odc22]
Nachdem das Angebot im Bereich der kostenpflichtigen Softwareprodukte umfangreicher ist und 2B Advice auf Anfrage eine kostenlose Einzelplatzlizenz zum Testen bereitgestellt hat, wird im Folgenden die Software *2B Advice PrIME* (Privacy Inventory, Management & Education) als Vertreter der kostenpflichtigen Anwendungen betrachtet. Dem gegenüber wird die kostenlose und Open-Source-Software *Open Datenschutzmanager* analysiert.
2B Advice PrIME ist eine Datenschutzmanagement-Software der 2B Advice GmbH. Sie wird von großen Unternehmen, wie dem ADAC, Lufthansa oder Microsoft, genutzt. Die Software ist cloud-basiert und benötigt demnach keine Synchronisation zwischen den benutzen Geräten. Da per Web auf die Software zugegriffen wird, ist sie mit einer Vielzahl an Betriebssystemen kompatibel.
Die kostenlose Open-Source-Software *Open Datenschutzcenter* richtet sich an Unternehmen, die den hohen Anforderungen der DSGVO gerecht werden möchten, aber nicht die Ressourcen besitzen, um eine teure Datenschutzmanagement-Software zu finanzieren. Zudem benötigt die Einrichtung der Software Fachwissen über die Administration eines Linux-Servers. Dieser wird benötigt, um anschließend per Webbrowser auf die Software zugreifen zu können. Bei *2B Advice PrIME* reicht es eine Installationsdatei auszuführen und die Installation läuft automatisch ab. Allerdings kann *2B Advice PrIME* nur auf Windows Betriebssystemen installiert werden.

Umsetzung in 2B Advice PrIME

Der Funktionsumfang von *2B Advice PrIME* ist wesentlich umfangreicher, als die Anforderungen zur Dokumentation in der DSGVO. Es gibt zum Beispiel ein Kommunikationszentrum, über welches die Benutzer untereinander und mit Mandanten per Mail kommunizieren können. Zudem gibt es ein Ticket-System für den Support und Dienste zur Erstellung von Online-Trainings und Prüfungen zu DSGVO-relevanten Themen. Es gibt vorausgefüllte Datenbanken mit Inhalten zu relevanten Gesetzestexten, ein Praxishandbuch zum Umgang mit der DSGVO und einen Hilfe-Bereich zur Handhabung aller Systemfunktionen. Im Rahmen dieser Arbeit wird der Fokus jedoch auf der Umsetzung der herausgearbeiteten Anforderungen aus Kapitel 2.4 liegen. Im Folgenden werden deshalb die einzelnen Anforderungen aufgegriffen und mit der Umsetzung in dieser Software verglichen.

Auftragsverarbeiter-Verträge

Im Rahmen des Verzeichnisses für Verarbeitungstätigkeiten lässt sich durch den Verwalter der Datenschutzmanagement-Software bei der Erstellung einer Verarbeitung die Verantwortlichkeiten festlegen. Unter dem Punkt „Verantwortliche Stelle“ (Abb. 4.1) kann neben der verantwortlichen Stelle, die immer beauftragende Stelle ist, auch spezieller eine verantwortliche Person, Fachabteilung und viele weitere

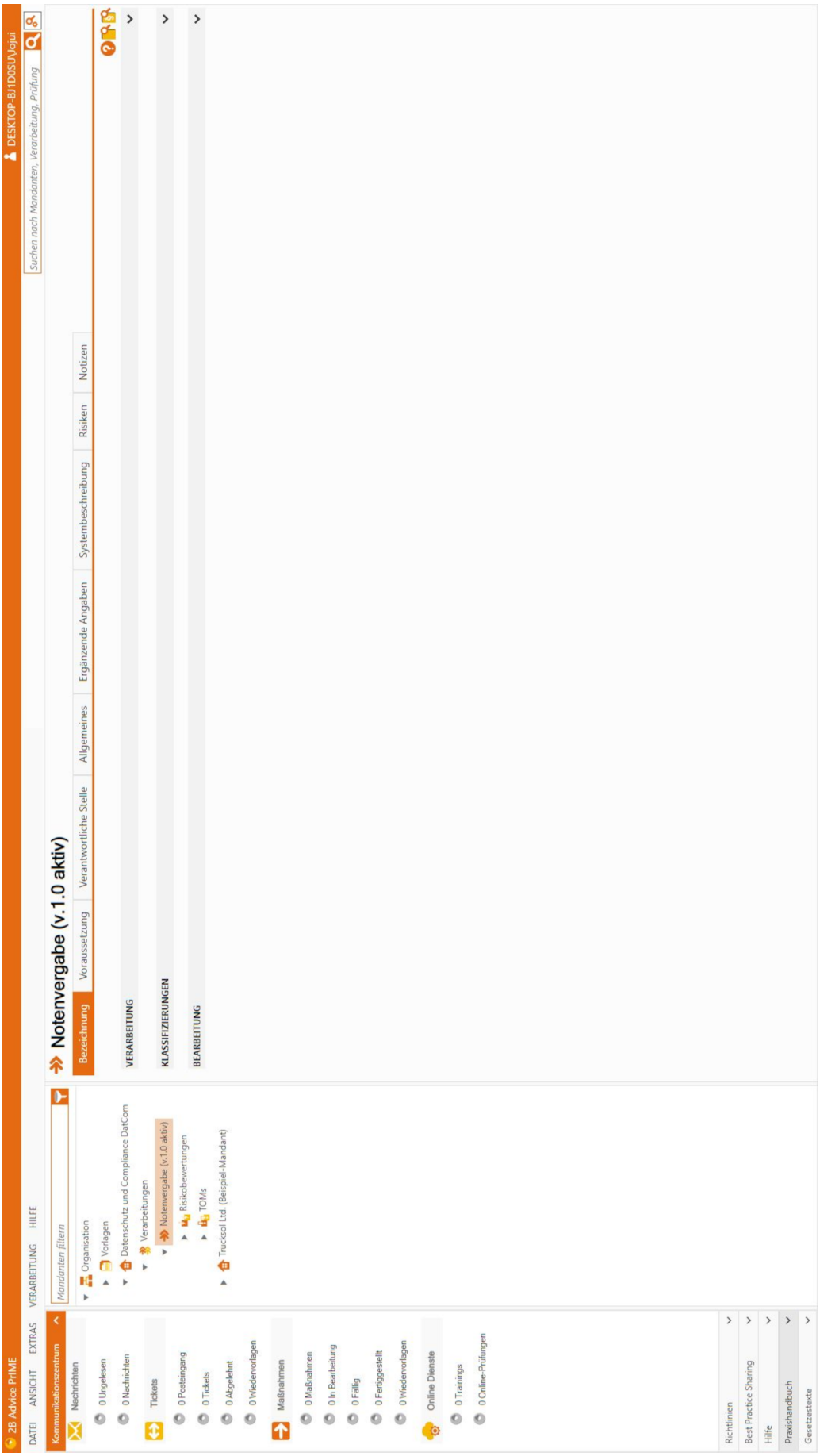

Abbildung 4.1: *2B Advice PrIME* – Übersicht

Kontaktdetails ergänzend festgelegt werden. Unter der Rubrik „Voraussetzungen“ (Abb. 4.1) können zudem im Bereich Richtlinien Dokumente hinterlegt werden, welche die DSGVO-konforme Verarbeitung nachweisen können. Hier kann auch der Auftragsverarbeiter-Vertrag als Richtlinie hinterlegt werden.

Datenschutz-Folgenabschätzung

Auch eine Datenschutz-Folgenabschätzung kann während des Anlegens einer Verarbeitung dokumentiert oder später nachgereicht werden. Unter dem Punkt „Risiken“ (Abb. 4.1) kann die Risikobewertung ergänzt werden. Dabei kann eine einfache Bewertung des Gesamtrisikos oder eine Bewertung anhand eines Risikokatalogs durchgeführt werden.

Dokumentation von Datenschutzvorfällen

Im Rahmen des Ticket-Systems werden auch Datenschutzvorfälle behandelt. Wenn es zu einem Datenschutzvorfall kommt, kann dieser im Bereich „Tickets“ (Abb. 4.1) als priorisiertes Ticket dokumentiert werden. Anschließend können Folgemaßnahmen durchgeführt und dokumentiert, sowie externe Dokumente in das Ticket mit eingepflegt werden.

Löschkonzepte

Die Löschkonzepte sind bei *2B Advice PrIME* auch in das VVT verteilt integriert. Unter dem Punkt „Allgemeines“ (Abb. 4.1) werden die von der Verarbeitung betroffenen Datenkategorien ausgewählt. Diese sind mit den enthaltenen Datenarten und Löschfristen versehen. Weiter können die erlaubten Empfänger zur Datenweitergabe bestimmt und Datenflüsse zwischen Verarbeitungen grafisch dargestellt werden. Unter dem Punkt „Systembeschreibung“ (Abb. 4.1) können die Speicherarten und die Speicherorte dokumentiert werden. Zudem kann ein Verantwortlicher für die Systembeschreibung definiert werden. Ein direkter Löschbeauftragter wird dabei nicht bestimmt, allerdings könnte diese Aufgabe durch den Systemverantwortlichen übernommen werden.

Unternemerische Datenschutzrichtlinie

Wie bereits bei der Hinterlegung der Auftragsverarbeiter-Verträge beschrieben, können unternehmerische Datenschutzrichtlinien unter dem Punkt „Voraussetzung“ (Abb. 4.1) im Bereich Richtlinien hinterlegt werden. Dazu kann entweder eine ausführliche Beschreibung als Richtlinie dokumentiert werden oder das Unternehmen setzt eine Richtlinie auf, die als Dokument hinzugefügt werden kann.

Verarbeitungsverträge

Unter dem Punkt „Voraussetzung“ (Abb. 4.1) können neben der Rechtsgrundlage und den Richtlinien auch Willenserklärungen hinterlegt werden. Als Willenserklärung zählt auch der abgeschlossene Vertrag zwischen dem Verantwortlichen

und dem Betroffenen. Demnach können hier die abgeschlossenen Verträge abgelegt werden, um die Rechtmäßigkeit der Verarbeitung zu unterstützen.

Verzeichnis von Verarbeitungstätigkeiten

Um den Anforderungen des VVT gerecht zu werden sind die benötigten Angaben unter verschiedenen Punkten dokumentiert. Unter „Verantwortliche Stelle“ (Abb. 4.1) können die Namen und Kontaktdaten des Verantwortlichen, des Vertreters und des Datenschutzbeauftragten hinterlegt werden. Der Punkt „Allgemeines“ (Abb. 4.1) umfasst die Informationen bezüglich Zweck der Verarbeitung, Kategorien betroffener Personen und personenbezogener Daten inklusive Löschfristen, Kategorien von Empfängern personenbezogener Daten und mögliche Übermittlung ins Ausland. Ebenso wird bei einer Übermittlung ins Ausland das Drittland benannt und das benötigte Datenschutzniveau sichergestellt. Unter dem Punkt „Risiken“ (Abb. 4.1) werden neben den Risikobewertungen auch die TOMs dokumentiert. Damit sind alle wesentlichen Punkte des VVT erfüllt.

Die Software *2B Advice PrIME* erfüllt nach dieser Analyse alle herausgearbeiteten Anforderungen, welche die DSGVO an die Dokumentation durch Verantwortliche stellt. Die Entwicklerteams haben mit ihrer Fachkompetenz alle nötigen Dokumentationen berücksichtigt und den Verantwortlichen darüber hinaus mit weiteren Features unterstützt. Das bedeutet, dass Verantwortliche gegen Bezahlung eine lückenlose Datenschutzmanagement-Software kaufen können, die sie vollumfänglich bei der Dokumentation unterstützt. Im weiteren Verlauf wird aber auch noch eine alternative Software betrachtet, welche mit ihrem offenen Quellcode mehr Transparenz bietet und durch das kostenlose Angebot auch kleinen Unternehmen ohne finanzielle Aufwendung zur Verfügung steht.

Umsetzung in Open Datenschutzcenter

Das *Open Datenschutzcenter* bietet ebenfalls einen größeren Funktionsumfang zur Dokumentation hilfreicher Informationen für den Datenschutz, als es von der DSGVO gefordert ist. Auch diese Software bietet unter anderem eine Funktion zum Anlegen von Online-Training und Kursen, eine Dokumentation von Softwareprodukten, die im Rahmen der Verarbeitungen genutzt werden und einen Bereich für offene Aufgaben, in denen speziellen Verantwortlichen Aufgaben erteilt werden können. Nutzt man die Open-Source-Software als kostenloses Datenschutzmanagement-Tool, so müssen alle Datenbanktabellen durch den Benutzer selbst befüllt werden. Dazu zählen Datenkategorien, Personenkategorien, TOMs und Richtlinien. Alternativ kann der Nutzer über den Entwickler des Produktes vordefinierte Datensätze kaufen, sodass die klassischen Informationen, wie zum Beispiel häufig benötigte Personen- und Datenkategorien, bereits in dem Tool enthalten sind. Diese können anschließend durch den Nutzer in dem Tool individuell angepasst werden. Auch bei diesem Produkt wird der Fokus auf den Anforderungen

aus Kapitel 2.4 liegen. Im Folgenden werden deshalb die einzelnen Anforderungen aufgegriffen und mit der Umsetzung im *Open Datenschutzcenter* verglichen.

Auftragsverarbeiter-Verträge

Im Dashboard des *Open Datenschutzcenters* findet der Nutzer die meisten Bearbeitungspunkte für das Erfüllen der DSGVO-Anforderungen wieder. Auch der Punkt „Auftragsverarbeitungen“ (Abb. 4.2) wird hier aufgeführt. Klickt der Nutzer auf diesen Button, so gelangt er in eine Übersicht aller bereits angelegten Auftragsverarbeitungen. Über den Button „Auftragsverarbeitung anlegen“ kann der Nutzer anschließend eine neue Auftragsverarbeitung anlegen. Neben wichtigen Informationen, wie Vertragsgegenstand, Kontakt und Grundlage der Verarbeitung, lässt sich auch ein Dokument zur Datenweitergabe hochladen. An dieser Stelle bietet es sich an, den Auftragsverarbeiter-Vertrag abzulegen, um ihn speziell auf diese Verarbeitung bezogen immer griffbereit zu haben.

Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzungen sind unter dem Punkt „DSFA“ (Abb. 4.2) im Dashboard zu finden. Klickt man auf diesen Button, so gelangt man zu einer Übersicht der angelegten Verarbeitungen. Wenn es für eine Verarbeitung eine Datenschutz-Folgenabschätzung gibt, so wird diese Verarbeitung hervorgehoben. Nachdem man die Verarbeitung ausgewählt hat, kann man sich die Datenschutz-Folgenabschätzung über den Button „DSFA anzeigen“ anzeigen lassen. Die Datenschutz-Folgenabschätzung besteht dabei aus einer schriftlichen Dokumentation in Freitextfeldern, die durch das Tool mit Überschriften und Anforderungen definiert sind.

Dokumentation von Datenschutzvorfällen

Die Abteilung für Datenschutzvorfälle ist nicht im Dashboard zu finden. Um Datenschutzvorfälle aufzurufen, muss der Nutzer die Sidebar über den Button „Navigation“ (Abb. 4.2) auswählen und dort den Button „Vorfälle“ betätigen. Damit gelangt der Nutzer in eine Übersicht aller dokumentierten Datenschutzvorfälle. Um hier einen neuen Datenschutzvorfall anzulegen, muss der Button „Neuen Vorfall anlegen“ ausgewählt werden. Anschließend können in einem Formular wichtige Informationen zu diesem Datenschutzvorfall dokumentiert werden. Eine Option, externe Dokumente hinzuzufügen, gibt es hier nicht. Jedoch lassen sich über den Button „Formulare“ (Abb. 4.2) im Dashboard jederzeit Dokumente hochladen, auf die im Datenschutzvorfall-Formular verwiesen werden kann. Diese Methode des Verweisens lässt sich auf alle anderen Themengebiete übertragen, in denen ein direktes Hochladen von externen Dokumenten nicht möglich ist.

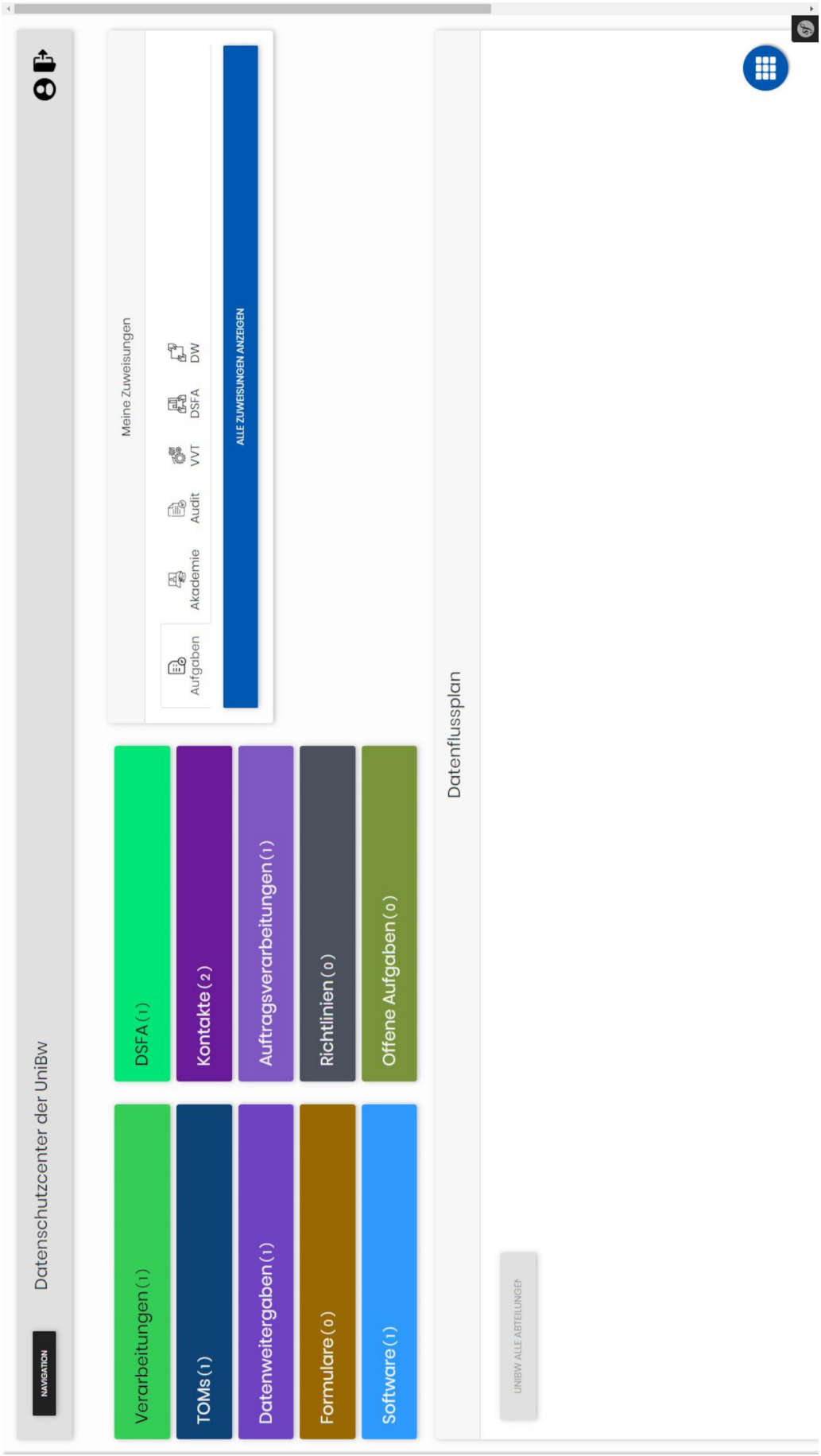

Abbildung 4.2: *Open Datenschutzcenter* – Dashboard Übersicht

Löschkonzept

Ein Löschkonzept als eigenständiger Punkt ist im *Open Datenschutzcenter* zurzeit nicht enthalten. Bei der Erstellung einer Verarbeitung werden zwar die Speicherorte und Löschfristen dokumentiert, jedoch beziehen sich diese Informationen auf die gesamte Verarbeitung und nicht auf die einzelnen Datenkategorien, die von der Verarbeitung betroffen sind. Dadurch ist es schwierig, nachzuvollziehen, welche Daten zum Zeitpunkt der Löschfrist tatsächlich gelöscht werden müssen. Ebenso kann es sein, dass im Rahmen einer anderen Verarbeitung, die Daten auch an anderen Speicherorten abgelegt werden. Deshalb ist es nötig, dass zum Löschen von Daten alle Verarbeitungen auf das Enthalten der besagten Daten geprüft werden müssen, um anhand dessen die Speicherorte herausfinden zu können. An dieser Stelle besteht Potenzial, die Software gewinnbringend zu erweitern.

Unternehmerische Datenschutzrichtlinien

Unter dem Punkt „Richtlinien“ (Abb. 4.2) im Dashboard findet man eine Übersicht aller angelegten Richtlinien. An diesem Ort bietet es sich auch an, die unternehmerische Datenschutzrichtlinie abzulegen. Über den Button „neue Richtlinie anlegen“ gelangt man zu einem Formular, in welchem nötige Punkte für eine Richtlinie oder Arbeitsweise dokumentiert werden können. Wie bei den anderen Formularen auch, wird der Nutzer durch Überschriften und Anweisungen im korrekten Ausfüllen unterstützt. Bei diesem Formular ist es zudem möglich ein externes Dokument hochzuladen, sodass die unternehmerische Datenschutzrichtlinie in Form eines PDF-Dokuments hier abgelegt werden kann.

Verarbeitungsverträge

Verträge, auf deren Basis eine Verarbeitung erfolgt, können auch unter dem Punkt „Formulare“ (Abb. 4.2) im Dashboard hochgeladen werden. Auf diese Verträge kann anschließend in den Dokumentationen der Verarbeitungen unter dem Titel „Zweck der Verarbeitung“ verwiesen werden. Dadurch kann die Rechtmäßigkeit der Verarbeitung unterstützt werden.

Verzeichnis von Verarbeitungstätigkeiten

Um die Dokumentation des umfangreichen VVT, welches von der DSGVO gefordert wird, übersichtlich umzusetzen, gibt es auch für diese Funktion einen Punkt im Dashboard. Über den Button „Verarbeitungen“ (Abb. 4.2) gelangt der Nutzer in eine Übersicht aller angelegten Verarbeitungen. Um in diesem Verzeichnis von Verarbeitungstätigkeiten eine neue Verarbeitung anzulegen, muss der Nutzer über den Button „neue Verarbeitung anlegen“ eine neue Verarbeitung eröffnen. Auch hierfür präsentiert sich ein Formular, in dem der Nutzer mithilfe von kurzen Anleitungen durch die Dokumentationsfelder hindurchgeführt wird. Neben einigen Freitextfeldern gibt es in diesem Formular auch viele Dropdown Menüs, in denen man Informationen auswählen kann, die vorher in anderen Datenbanktabellen eingepflegt wurden. So gibt es zum Beispiel Dropdown Menüs für *verantwortliche*

Person, Zweck und Grundlage, betroffene Personen- und Datenkategorien, verwendete Software und *verwendete TOMs*. Das Verzeichnis von Verarbeitungstätigkeiten baut demnach auf den Dokumentationen in allen anderen Teilbereichen auf und bietet eine ordentliche Übersicht über die Verarbeitungen mit einem Mausklick.

Aus dieser Analyse stellt sich heraus, dass die kostenlose Open-Source-Software in vielen Punkten mit den kostenpflichtigen Alternativen mithalten kann. Bezüglich des Löschkonzeptes konnte aber auch festgestellt werden, dass es noch keine Funktion gibt, die diese Dokumentation im vollen Umfang abdeckt. Es lässt sich folglich erkennen, dass diese Software eine nutzbare Alternative zu den kostenpflichtigen Programmen darstellt, aber auch noch Potenzial für Weiterentwicklungen bietet. Für diese Masterarbeit ist das ergänzbare Löschkonzept ein Ansatz zur gewinnbringenden Weiterentwicklung von Open-Source-Datenschutzmanagement-Software. Dadurch kann die Nutzergemeinschaft kostenloser und quelloffener Software und Unternehmen, die auf diese Software zurückgreifen, noch besser bei der Erfüllung von Dokumentationspflichten unterstützt werden.

Vergleich der Umsetzung in verschiedener Software

Aus der Benutzung beider Softwareprodukte gehen zwei unterschiedliche Anwendungsumgebungen hervor. *2B Advice PrIME* arbeitet im Kern mit einem Multilevel Dropdown Menü. Dort können mehrere Mandanten und ihre Datenverarbeitungen verwaltet werden. Unter Mandanten sind in diesem Zusammenhang Unternehmen zu verstehen, welche über diese Software ihr Datenschutzmanagement bearbeiten. Dazu kommt das präsente Kommunikationszentrum, welches dem Nutzer dazu dient, mit weiteren Nutzern oder den Mandanten zu kommunizieren. Daraus ergibt sich, dass diese Software im Schwerpunkt für externe Unternehmen, welche die Datenschutzmanagement-Dienstleistung anbieten, oder externe Datenschutzbeauftragte konzipiert ist. Der Nutzer dieses Tools kann mehrere Mandanten gleichzeitig verwalten und das Datenschutzmanagement bearbeiten. Gleichzeitig kann über das Kommunikationszentrum Unterstützung geleistet werden.
Das *Open Datenschutzcenter* hingegen besteht im Kern aus dem Dashboard, über welches der Nutzer alle wichtigen Bereiche des Datenschutzmanagements verwalten kann. Allerdings ist dieses Produkt darauf ausgerichtet, dass lediglich ein Mandant verwaltet wird. Der Einsatz dieser Software lässt sich demnach in dem Szenario vorstellen, dass diese Software der Datenschutzabteilung des zu verwaltenden Unternehmens mit mehreren Nutzerzugängen zur Verfügung steht, um das Datenschutzmanagement des eigenen Unternehmens zu verwalten. Über den Punkt „Offene Aufgaben“ können die Nutzer der Software sich untereinander Aufgaben verteilen und kommunizieren. Auch die Kommunikation mit dem Kunden ist über den Punkt „Kundenanfragen“ in der Seitenleiste möglich. Jedoch ist diese nicht so präsent wie bei *2B Advice PrIME* und in der Benutzung nicht so relevant.
2B Advice PrIME setzt auf einen ganzheitlichen Ansatz, der im Folgenden detaillierter erklärt wird. Bei der Erstellung einer Verarbeitung ist diese mit Untermenüs

versehen, in denen der Verarbeitung Informationen hinzugefügt werden können. Dabei hat man Zugriff auf verschiedenen Datenbanktabellen, wie zum Beispiel die *Rechtsgrundlagen, Verarbeitungszwecke, betroffene Personen und Datenkategorien, Empfänger* und *TOMs*. Alle diese Datenbanktabellen können während der Erstellung oder Bearbeitung einer Verarbeitung editiert werden. So ist es möglich eine Datenkategorie zu ergänzen, falls diese noch nicht in der Datenbanktabelle enthalten ist oder eine Löschfrist zu ändern, falls sich interne Abläufe oder die Gesetzeslage geändert haben. Dadurch wird der Prozess der Verarbeitungserstellung oder -bearbeitung nicht gänzlich unterbrochen, sondern die Bearbeitung der Datenbanktabellen wird in den Prozess integriert.
Bei dem *Open Datenschutzcenter* ist die Verwaltung komplizierter. Da die Datenbanktabellen zu Beginn der Nutzung des Tools noch leer sind, muss der Nutzer sich Gedanken machen, mit welchen Datensätzen er diese füllen möchte. Alternativ kann eine befüllte Datenbank über den Entwickler kostenpflichtig bezogen werden. Nachdem die Datenbank mit Datensätzen gefüllt ist, können Verarbeitungen erstellt werden. Innerhalb einer Verarbeitungserstellung oder -bearbeitung können jedoch keine Änderungen an den Datenbanktabellen vorgenommen werden. Fällt während der Erstellung auf, dass eine betroffene Personengruppe nicht in der Datenbanktabelle enthalten ist, muss die Verarbeitungserstellung entweder abgebrochen werden oder eine falsche Personengruppe angegeben werden, um die unvollständige Verarbeitungsdokumentation zwischenzuspeichern. Dies ist nötig, da einige Formularfelder nicht leer sein dürfen, wenn die Dokumentation abgespeichert wird. Nach Abbruch oder Zwischenspeicherung muss der Nutzer dann zu der betroffenen Datenbanktabelle navigieren, um im Untermenü den fehlenden Datensatz zu ergänzen. Dies ist zum Beispiel der Fall bei *zugeordneter Abteilung, betroffene Personen und Datenkategrorien, zugehörige Datenweitergaben, verwendete Software* und *eingesetzte TOMs*.

4.3 Erkenntnis durch verwandte Arbeiten

Es gibt verschiedene wissenschaftliche Arbeiten, die sich mit dem Problem befassen wie die Daten, die in den geforderten Dokumentationen der DSGVO eingetragen werden müssen, überhaupt erhoben werden können. Dazu wurden zwei Arbeiten betrachtet, die mit unterschiedlichen Konzepten dieses Problem behandeln.
Zudem sind bei der Recherche zwei Arbeiten aufgefallen, die sich mit der Erstellung von Löschkonzepten beschäftigen. Während eine Arbeit sich damit auseinandergesetzt hat, wie Löschkonzepte in ein komplexes ERP-System integriert werden können, hat sich die andere Arbeit mit dem Problem beschäftigt, wie das Löschen, welches durch die Löschkonzepte initiiert wird, automatisiert werden kann. In beiden Arbeiten stellte sich heraus, dass die Erstellung von Löschkonzepten eine komplexe und aufwendige Arbeit ist. Häufig muss mit vielen Datensätzen, die an unterschiedlichen Speicherorten liegen, gearbeitet werden. Hinzu kommt, dass der Zweck zur Erlaubnis zum Speichern der Daten an verschiedenen Speicherorten zu

verschiedenen Zeiten nicht mehr gegeben sein kann. Diese Dynamik in Löschkonzepten abzubilden, ist schwer.
Bei der Betrachtung bereits existierender Datenschutzmanagement-Tools wurde festgestellt, dass es viele kostenpflichtige Tools gibt, während im Bereich der kostenlosen Angebote nur wenige Alternativen vorhanden sind. Bei der Auseinandersetzung mit *2B Advice PrIME* als Vertreter der kostenpflichtigen Datenschutzmanagement-Lösungen wurde festgestellt, dass alle Anforderungen zur Dokumentation durch die DSGVO umgesetzt wurden und es keinen Bedarf an weiteren Funktionsimplementierungen gibt. Das *Open Datenschutzcenter* als kostenlose Open-Source Alternative bietet hingegen nicht alle Funktionen im vollen Umfang an. Im Bereich der Löschkonzept-Dokumentation werden lediglich Löschfristen in den einzelnen Verarbeitungstätigkeiten eingetragen. Es existiert kein Löschkonzept, sodass an zentraler Stelle Informationen zur Löschung verwaltet werden können.
An dieser Stelle bietet es sich an, dass in dieser Masterarbeit im weiteren Verlauf ein Konzept zur Implementierung der Funktion „Löschkonzepte erstellen“ erarbeitet und anschließend das *Open Datenschutzcenter* um diese Funktion erweitert wird. Dadurch wird die erkannte Abweichung des Funktionsumfangs von den Anforderung der DSGVO behoben.

5 Konzept und Design

In diesem Kapitel wird die zu ergänzende Funktion, die in Abschnitt 4.3 herausgearbeitet wurde, durch konzeptionelle Lösungsvorschläge beschrieben. Dadurch wird es möglich, eine praktische Implementierung der Funktion konzeptionell zu unterstützen. Wie sich in der Betrachtung von *2B Advice PrIME* herausgestellt hat, sind in diesem Datenschutzmanagement-Tool alle Anforderungen zur Dokumentation nach DSGVO vollständig implementiert. Es gibt in diesem Bereich keine Funktionen zu ergänzen. Beim *Open Datenschutzcenter* wurde jedoch erkannt, dass aktuell noch keine umfassende Lösung für die Dokumentation von Löschkonzepten vorhanden ist. Beim *Open Datenschutzcenter* handelt es sich um eine kostenlose Open-Source-Software, die durch die Nutzergemeinschaft von Entwicklern, Interessenten und Nutzern regelmäßig weiterentwickelt wird. Um in diesem Bereich die Weiterentwicklung zu fördern, leistet diese Arbeit im Folgenden einen Beitrag zur Verbesserung dieser Software, indem die Implementierung der Funktion zum Dokumentieren von Löschkonzepten konzeptionell erarbeitet wird.

5.1 Löschkonzept im Open Datenschutzcenter

Um das Ziel der gewinnbringenden Erweiterung der Open-Source-Software durch das Implementieren der Funktion zum Dokumentieren von Löschkonzepten zu erreichen, muss zunächst eine Anforderungsanalyse durchgeführt werden. Wie in Abschnitt 4.2 bereits deutlich wurde, wird das Thema *Löschen* aktuell nur mit Löschfristen behandelt, die in jeder Verarbeitung individuell eingetragen werden müssen. Zudem entsteht der Eindruck, dass sich in dieser Form die Löschfristen auf die Verarbeitungstätigkeiten beziehen und nicht auf die Datenkategorien, die in diesen Verarbeitungstätigkeiten verarbeitet werden. Da außerdem mehrere Datenkategorien in einer Verarbeitungstätigkeit verarbeitet werden können, die möglicherweise unterschiedliche Löschfristen haben, ist es in dieser Form schwer den verschiedenen Datenkategorien die richtigen Löschfristen zuzuordnen. Selbiges Problem besteht bei der Dokumentation von Speicherorten. Durch Löschkonzepte sollen unter anderem diese Probleme gelöst werden.
Die neue Dokumentationsfunktion soll es ermöglichen, dass durch Löschkonzepte die Datenkategorien übersichtlich zu ihren passenden Löschfristen und Speicherorten hinzugefügt werden können, sodass der Nutzer über kurze Wege eine Übersicht über die bestehenden Löschkonzepte erhält. Zudem sollen die Löschkonzepte so standardisiert werden, dass mehrere Datenkategorien dem gleichen Löschkonzept zugeordnet und die Löschkonzepte auch in mehreren Verarbeitungstätigkeiten

angewendet werden können. Durch diese Standardisierung soll die Benutzerfreundlichkeit gesteigert werden, da der Nutzer nicht für jede Datenkategorie oder Verarbeitungstätigkeit ein neues Löschkonzept anlegen muss. Um die Bedienbarkeit der neuen Funktion intuitiv zu gestalten, sollte sich das Design der neuen Arbeitsoberfläche in das bestehende Design integrieren. Um Berichte exportieren zu können, in denen alle zuvor angelegten und angepassten Löschkonzepte aufgezeigt werden können muss dafür gesorgt werden, dass die Datensätze revisionssicher angelegt werden. Noch wichtiger ist die Revisionssicherheit für die Dokumentation von Verarbeitungstätigkeiten. Hier soll eine Lösung entwickelt werden, welche es dem Nutzer zwar ermöglicht Löschkonzepte und Datenkategorien anzupassen, jedoch ohne die Informationen, die in einer Verarbeitungstätigkeit hinterlegt sind, zu verändern. Beim Exportieren des VVT mit Historie sollen alle Verarbeitungstätigkeiten in zeitlicher Reihenfolge mit den richtigen Informationen ausgegeben werden. Der Historien-Bericht ist aktuell auch schon ohne die Einbindung von Löschkonzepten und den neuen Datenkategorien exportierbar.
Im Folgenden wird das Ziel dieses Konzeptes aufgegriffen, bevor die Anforderungen zur Zielerfüllung gesammelt aufgestellt werden.

Konzeptziel

Die Datenschutzmanagement-Software *Open Datenschutzcenter* bietet aktuell keine Möglichkeit zur zentralen Verwaltung von Löschkonzepten. Mit Hilfe dieses Konzeptes soll eine gewinnbringende Implementierung der Funktion zum Dokumentieren von Löschkonzepten in das *Open Datenschutzcenter* ermöglicht werden.

Anforderungen

A1: Benutzbarkeit der Software fördern

A2: Intuitive Bedienung der neuen Funktion gewährleisten

A3: Zentrale Verwaltung der Löschkonzepte ermöglichen

A4: Datenkategorien um Datenarten ergänzen

A5: Möglichkeit zur Standardisierung schaffen

A6: Kurze Wege ermöglichen

A7: Kompatibilität mit alten Software-Versionen sicherstellen

A8: Revisionssicherheit für die Berichterstellung

5.2 Design

Bei der Betrachtung des *Open Datenschutzcenter* ist eine Strukturlinie zu erkennen. Alle Hauptfunktionen sind auf dem Dashboard in farblicher Abgrenzung zu finden. Durch das Klicken auf die verschiedenen Buttons gelangt der Nutzer zu den jeweiligen thematischen Übersichten. Beispielsweise gelangt er durch das Klicken auf den Button „Verarbeitungen“ in die Übersicht aller angelegten Verarbeitungstätigkeiten. Von hier aus lassen sich bereits angelegte Verarbeitungen durch ein erneutes Anklicken bearbeiten. Durch das Klicken auf den Button „neue Verarbeitung anlegen“ kann eine neue Verarbeitung dokumentiert werden. Des Weiteren gibt es die Möglichkeit über den Button „Navigation“ die Sidebar zu öffnen. Über diese kann der Nutzer zurück zum Dashboard gelangen oder direkt in ein anderes Themengebiet navigieren. Auch sind in der Übersicht die Funktion zur CSV-Exportierung der Übersicht und eine Suchfunktion zu finden, mit der nach allen Wörtern gesucht werden kann, die in der Übersicht angezeigt werden. Ein Beispiel dieser Übersicht ist in Abb. 5.1 zu sehen. Durch das Klicken auf den Button „neue Verarbeitung anlegen“ gelangt der Nutzer zu einem Formular, das in zwei Spalten getrennt ist. In der linken Spalte sind die Bezeichnung und Beschreibung des auszufüllenden Formularfeldes zu finden und auf der rechten Seite die dazu passenden Formularfelder (Abb. 5.2). Dabei ist bei den Feldern zwischen verschiedenen Freitextfeldern, Dropdown-Feldern und Checkbox-Feldern zu unterscheiden. Klickt der Nutzer in der Übersicht auf eine bereits existierende Verarbeitung, gelangt er in das jeweilige Formular. Dieses ist in diesem Fall mit den Informationen befüllt, welche zu der Verarbeitung passen und kann nun bearbeitet werden. Auch das Löschen der gesamten Verarbeitung ist in dieser Ansicht möglich.
Die Implementierung einer Funktion zum Erstellen von Löschkonzepten sollte in der Darstellung auch mindestens diese Ansichten bieten. Demnach ist es nötig, dass das Dashboard einen weiteren Button „Löschkonzepte“ erhält, über den der Nutzer in die Übersicht aller erstellten Löschkonzepte gelangt und auch neue Löschkonzepte erstellen kann. Ebenso sollte es einen gleichnamigen Button in der Sidebar geben, damit man über die Navigation auch aus anderen Bereichen heraus direkt zur Löschkonzept-Übersicht gelangen kann. In der Übersicht sollten dem Nutzer alle wichtigen Informationen angezeigt werden, ohne die Ansicht zu überladen. Dadurch kann gewährleistet werden, dass die Anforderungen A1, A2, A3 und A6 umgesetzt werden.

Das Löschkonzept sollte diese Formularfelder enthalten:

- Datenkategorien
- Datenarten
- Standard-Löschfrist
- gesetzliche Löschfrist
- Speicherorte

Abbildung 5.1: *Open Datenschutzcenter* – Übersicht VVT

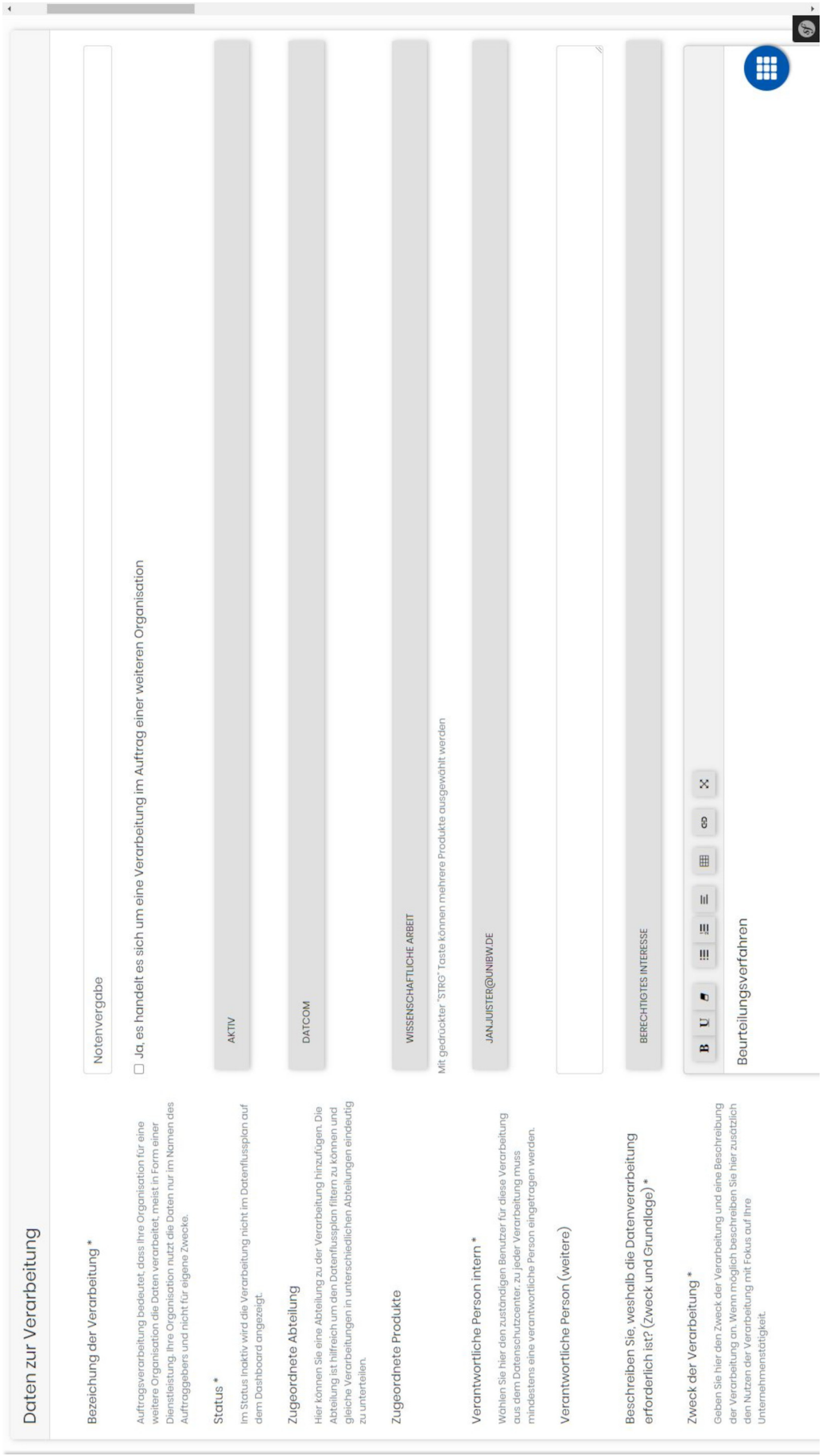

Abbildung 5.2: *Open Datenschutzcenter* – Ausschnitt Formular

- Löschbeauftragter
- Beschreibung

Unter *Datenkategorien* sollte ein Dropdown-Feld zu finden sein, über welches die Datenkategorien zu finden sind, die vorher in der Tabelle für Datenkategorien hinzugefügt wurden. Hier sollten beliebig viele Datenkategorien ausgewählt werden können, um alle Datenkategorien, auf die dieses Löschkonzept zutrifft, hinzufügen zu können. Wichtig dabei ist, dass eine Datenkategorie nur einem Löschkonzept zugeordnet werden kann, damit keine Überschneidungen entstehen und es immer eindeutig bleibt, welchem Löschkonzept die Datenkategorie angehört. Dadurch ist es auch möglich, bei der Erstellung einer Verarbeitung, die verarbeiteten Datenkategorien direkt mit der Standard-Löschfrist zu hinterlegen. Mit dieser Konfiguration können die Anforderungen A1, A5 und A6 gefördert werden.
Unter dem Punkt *Datenarten* sollen alle Datenarten angezeigt werden, die im Rahmen des Unternehmens den betroffenen Datenkategorien zuzuordnen sind. Da die Dokumentation von Datenarten in Verknüpfung zu den passenden Datenkategorien aktuell nicht möglich ist, muss auch hier der Funktionsumfang erweitert werden. Dies kann durch einen weiteren Button „Datenkategorien“ auf dem Dashboard erfolgen, wodurch der Nutzer zu einer Übersicht bereits existierender Datenkategorien gelangt. Dort können weitere Datenkategorien und die dazugehörigen Datenarten angelegt werden, damit diese später bei der Dokumentation von Löschkonzepten integriert werden können. Auch diese Umkonfiguartion dient dazu, dass die Anforderungen A1, A2, A4 und A6 erfüllt werden.
Die *Standard Löschfrist* beschreibt die Löschfrist, auf die sich unternehmensintern geeinigt wurde. Diese kann früher sein, als das Gesetz vorsieht, falls es eine gesetzliche maximale Speicherdauer gibt. Jedoch darf die Standard-Löschfrist nie länger sein, als die gesetzliche Löschfrist. Auch kann es sein, dass eine Mindest-Speicherdauer gesetzlich vorgeschrieben ist. Dann darf die Standard-Löschfrist diese nicht unterschreiten. Gibt es keine gesetzliche Löschfrist, sollte durch das Unternehmen trotzdem eine Löschfrist definiert werden. Der Punkt *gesetzliche Löschfrist* kann in dem Fall unausgefüllt bleiben. Wenn die Löschfrist nicht direkt in Jahren angegeben werden kann, kann auch auf Definitionen wie „2 Jahre nach Kündigung“ zurückgegriffen werden. Die festgeschriebene Standard-Löschfrist wird anschließend hinter der Datenkategorie mit angezeigt.
Speicherorte werden zwar schon bei der Erstellung einer Verarbeitung hinterlegt, jedoch beziehen sich diese Speicherorte nur auf die Speicherung innerhalb dieser Verarbeitung. Wird eine Datenkategorie innerhalb mehrerer Verarbeitungen aufgegriffen, kann es sein, dass sie an verschiedenen Orten gespeichert werden. Um nicht alle Dokumentationen von Verarbeitungen nach den Speicherorten durchsuchen zu müssen, sollen an dieser Stelle im Löschkonzept unter dem Punkt *Speicherorte* alle Speicherorte zentral dokumentiert werden. Kommen im Rahmen von neuen Verarbeitungstätigkeiten neue Speicherorte hinzu, kann das Löschkonzept jederzeit angepasst werden. Dadurch kann gewährleistet werden, dass die Anforderungen A3 und A6 eingehalten werden.
Unter dem Punkt *Löschbeauftragter* soll eine verantwortliche Person namentlich

genannt oder eine verantwortliche Abteilung bestimmt werden. Dadurch soll sichergestellt werden, dass sich regelmäßig definiertes Personal um die Einhaltung des Löschkonzeptes bemüht. Bei Fragen oder Änderungen zu den betroffenen Datenkategorien oder zum Löschkonzept selbst sollte diese Person oder Abteilung die erste Anlaufstelle sein. Abschließend sollte dem Nutzer unter dem Punkt *Beschreibung* die Möglichkeit gegeben werden, relevante Informationen im Freitext zu ergänzen. Dies könnten Löschabläufe, Prüfintervalle, Ausnahmen oder Ähnliches sein. Auch diese Möglichkeit fördert die Anforderung A1.
In Abschnitt 2.4.2 wurde im Rahmen der Anforderungsanalyse auch der Punkt *Datenweitergabe – Auftragsverarbeiter* genannt. Sollten Daten im Rahmen der Datenweitergabe auch von Auftragsverarbeitern gespeichert werden, können diese Auftragsverarbeiter auch als Speicherort mit aufgenommen werden. An welchen Orten genau der Auftragsverarbeiter die betroffenen Daten speichert, ist für diese Dokumentation nicht wichtig. Dafür muss der Auftragsverarbeiter selber eine Dokumentation führen. Wenn Daten gelöscht werden sollen, ist es wichtig, dass die beteiligten Auftragsverarbeiter darüber informiert werden können, dass auch sie die Daten löschen müssen. Da diese Verknüpfung durch das Dokumentieren des Auftragsverarbeiters als Speicherort vorhanden ist, kann diese Maßnahme durchgeführt werden. Mit Hilfe von kurzen Beschreibungen, die unter den Benennungen der Formularfelder zu finden sind, soll eine Ausfüllhilfe für die Dokumentationen geboten werden. Dadurch können die Anforderungen A1 und A2 noch stärker gefördert werden.
Um die Anforderungen A1 und A6 zu fördern, soll außerdem eine Verknüpfung zwischen den Datenkategorien und den Löschkonzepten entstehen. Diese kann eingerichtet werden, indem in der Übersicht der Datenkategorien angezeigt wird, ob die Datenkategorien einem Löschkonzept zugeordnet sind. Wenn das der Fall ist, soll die Möglichkeit angeboten werden, durch Klicken auf „anzeigen“ direkt zu dem zugeordneten Löschkonzept der Datenkategorie zu gelangen. Dort werden weitere Informationen angezeigt, die das Löschen der ausgewählten Datenkategorie betreffen.
Damit es bei der Migration der Weiterentwicklung bei Bestandskunden nicht zu Komplikationen kommt muss darauf geachtet werden, dass keine Daten verloren gehen oder bestehende Funktionen der aktuellen Softwareversion nicht mehr durchgeführt werden können. Das ist vor allem bei der Integration der neuen Löschfristen zu beachten. Damit die alten Löschfristen nicht verloren gehen, dürfen diese zum aktuellen Zeitpunkt nicht einfach aus den Datenbanken und den Formularen entfernt werden. Das alte Formularfeld zum Eintragen von Löschfristen bei der Dokumentation von Verarbeitungen muss bestehen bleiben, damit die Nutzer diese Fristen nach eigenem Ermessen in die neuen Löschkonzepte übertragen können. Eine automatische Übertragung ist nicht möglich, da sich die alten Löschfristen nicht direkt auf die verarbeiteten Datenkategorien beziehen, sondern an die Verarbeitung gebunden sind. Damit die Nutzer fortan trotzdem die neue Funktion zum Dokumentieren von Löschkonzepten nutzen und an dieser Stelle neue Löschfristen eintragen, muss das alte Dokumentationsfeld schreibgeschützt werden. Dadurch wird sichergestellt, dass die Nutzer ihre alten Löschfristen einsehen, aber keine

neuen Eintragungen an dieser Stelle vornehmen können. In einer weiteren Aktualisierung der Software kann dann die Funktion zur Dokumentation von Löschfristen in den Verarbeitungen vollständig entfernt und komplett auf die Nutzung der neuen Löschkonzepte übergegangen werden. Dadurch ist sichergestellt, dass die Anforderung A7 eingehalten wird.
Damit die Revisionssicherheit gewährleistet werden kann, müssen alle jemals bestandenen Relationen zwischen Verarbeitungstätigkeiten, Datenkategorien und Löschkonzepten erhalten bleiben. Ein Datensatz darf nie vollständig gelöscht werden. Um zum Beispiel ein Löschkonzept trotzdem für den Nutzer zu entfernen, kann mit einem Flag gearbeitet werden, welches Löschkonzepte als aktiv oder inaktiv kennzeichnet. Um Datensätze nicht zu verändern und damit die Revisionssicherheit beizubehalten, müssen Datensätze bei einer Veränderung dupliziert werden. Durch die Markierung als aktiv/inaktiv, das Duplizieren und die Relationen soll sichergestellt werden, dass bei der Berichterstellung nur Informationen dargestellt werden, welche der Nutzer zu den ausgewählten Zeitpunkten auch wirklich dokumentiert hat. Damit kann die Anforderung A8 umgesetzt werden.
Auf der GitHub-Seite von H2-invent [odc22] ist unter dem Punkt „Issues“ auch ein Forenbeitrag zum Thema „Aufbewahrungsfristen und Löschkonzepte ermöglichen“ zu finden. In diesem Beitrag schlägt ein Autor mit dem Nicknamen Ymela eine ähnliche Umsetzung vor. Jedoch möchte er die Löschfristen in einem eigenen Menüpunkt mit den dazugehörigen Datenkategorien verknüpfen und die Löschkonzepte mit den weiteren Informationen separat behandeln. Diese Lösung schlägt er mit der Begründung vor, dass Löschkonzepte sich bei verschiedenen Löschfristen gleichen können. Er geht davon aus, dass das Herausziehen der Löschfristen aus den Löschkonzepten ein sparsameres Vorgehen für die Datenbank ist.
Nach der Betrachtung mehrerer Datenmanagement-Tools kommt man in dieser Arbeit jedoch zu dem Schluss, dass die Anzahl an Löschfristen das separate Behandeln nicht rechtfertigt. Im Rahmen dieser Masterarbeit fand keine ausführliche Auseinandersetzung mit Gesetzestexten bezüglich konkreter Aufbewahrungsfristen statt, da es sich hierbei um ein komplexes juristisches Thema handelt und es viele Gesetzestexte für verschiedene Datenkategorien gibt. Allerdings konnten bei der Recherche häufig die Löschfristen 2 Jahre, 6 Jahre und 10 Jahre ermittelt werden. Da es den Anschein macht, dass Löschfristen vereinfacht in diese Abschnitte eingeteilt werden können, sofern es gesetzliche Vorgaben gibt, ist eine separate Behandlung nicht sinnvoll. Sollte es für Datenkategorien keine gesetzlichen Vorgaben geben, verringert die gemeinsame Behandlung von Datenkategorien unter demselben Löschkonzept mit derselben Löschfrist den Aufwand des Nutzers und erleichtert ihm die Arbeit. Deshalb wurde sich dafür entschieden, die Löschfristen ebenfalls in die Löschkonzepte zu integrieren.

6 Implementierung

In diesem Kapitel wird beschrieben, wie das Design, welches in 5.2 beschrieben wurde, in dem *Open Datenschutzcenter* umgesetzt werden kann. Dazu wird anfangs darauf eingegangen, wie die Software grundsätzlich aufgebaut ist und wie man die Funktion in das bestehende Programm integrieren kann. Anschließend werden die wichtigsten Relationen zwischen den Dokumentationen dargestellt und erläutert, bevor die relevanten Codesegmente, welche ergänzt wurden, hervorgehoben und erklärt werden. Abschließend wird in kurzen Beschreibungen auf die Anforderungen aus 5.1 Bezug genommen und erklärt, wie diese umgesetzt wurden.

6.1 Architektur des Open Datenschutzcenters

Das *Open Datenschutzcenter* wurde mithilfe des Symfony-Framworks in PHP programmiert. Dabei bildet die Model-View-Controller-Architektur die grundlegende Basis der Entwicklungsarbeit. Durch diese Architektur werden die Daten (Model), Ansicht (View) und Logik (Controller) voneinander getrennt. Das hat den Vorteil, dass spätere Änderungen leicht in die einzelnen Komponenten integriert und Komponenten wiederverwendet werden können. Im Falle der betrachteten Software wurden zudem Services eingeführt, welche die Kommunikation mit der externen SQL-Datenbank übernehmen. Das bedeutet, dass jede Funktion, wie zum Beispiel die Dokumentation von Kontakten, über ein eigenes Model, eine eigene View, einen eigenen Controller und einen eigenen Service verfügen.
Die Module des Models repräsentieren jeweils eine Einheit in der verwendeten Datenstruktur. Module der View definieren die grafische Benutzeroberfläche und die Controller-Module sind für die Kommunikation zwischen Model und View zuständig. Die Service-Module übernehmen den Datenaustausch mit der externen Datenbank.
Erklärt am Beispiel der Dokumentation von Kontakten bedeutet dies, dass es die Kontakte-Entity und -Repository-Klassen gibt, welche dem Model angehören. Für die View gibt es die Kontakte-Type und -Template-Klassen und für den Controller die Kontakte-Controller-Klasse. Die Kontakte-Service-Klasse gehört funktionell zum Controller, wird aber ausgelagert behandelt um eine bessere Wiederverwendbarkeit und Lesbarkeit zu erreichen. Innerhalb der View-Klassen kann auf andere Klassen verwiesen werden, damit der Nutzer durch Interaktionen auf andere Views weitergeleitet werden kann. Ebenso können Model-Klassen miteinander verknüpft

werden, damit Model-übergreifend Daten abgefragt werden können. Auch ein Service kann auf weitere Services zugreifen, um Informationen zu erhalten. In Abb. 6.1 sind die Zusammenhänge zwischen den einzelnen Modulen dargestellt.

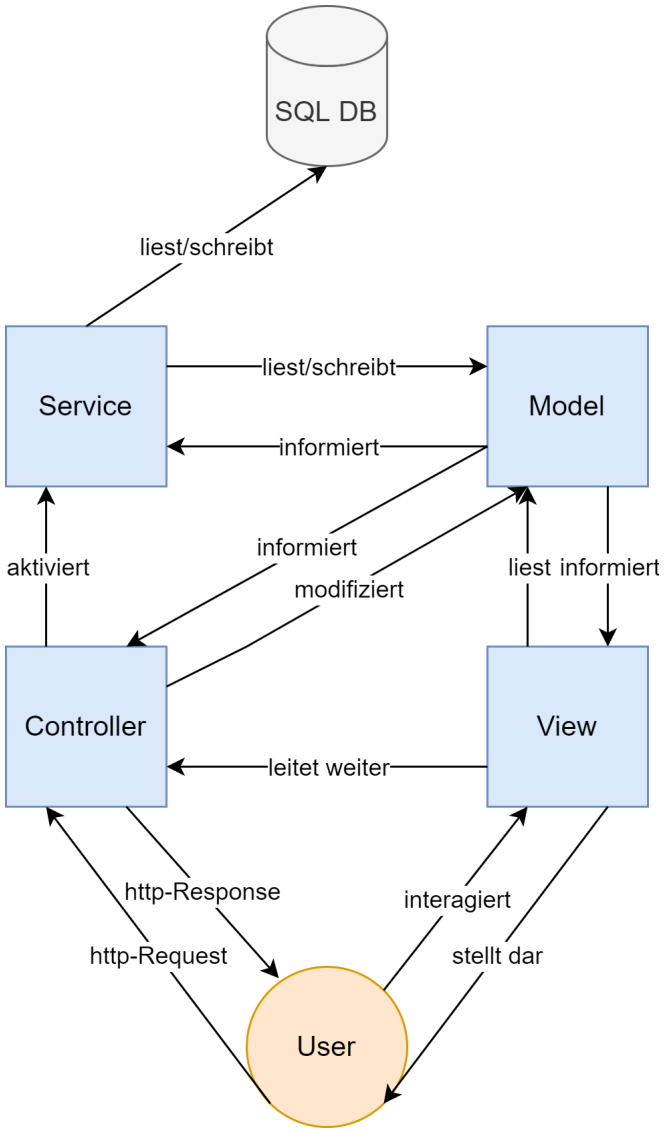

Abbildung 6.1: MVCS-Architektur

Für die Implementierung der Funktion „Löschkonzepte dokumentieren“ bedeutet dies, dass ein neues Model-View-Controller-Service (MVCS)-Pattern erstellt werden muss. Das Model muss die Variablen zur Datenerfassung enthalten, die in 5.2 beschrieben wurden. Die View sollte die Informationen im gleichen Design präsentieren, wie auch in anderen Teilen des Programms. Für die Umsetzung der Komponenten-Logik und Weiterleitung von Eingabeparametern wird auch ein neuer Controller benötigt. Um den Datenaustausch zwischen der Anwendung und der SQL-Datenbank zu realisieren, wird zudem ein neuer Service benötigt.

6.2 Implementierung von Löschkonzepten

Wie in Absatz 6.1 beschrieben, ist es nötig, ein neues MVCS-Pattern in die bestehende Architektur zu integrieren. Neben dem MVCS-Pattern für die Löschkonzepte sind zudem noch weitere Klassenimplementierungen vonnöten. Jenseits der beschriebenen Umsetzungen muss noch einiges mehr implementiert werden, was benötigt wird, damit alle Funktionen und Darstellungen fehlerfrei funktionieren. In diesem Abschnitt werden jedoch nur die wichtigsten Praxisanteile beschrieben. Im Folgenden werden in der Tabelle 6.1 die wichtigsten Klassen aufgezeigt, die neu erstellt werden müssen.

	Löschkonzept	Datenkategorien
Model	Loeschkonzept.php	
View	LoeschkonzeptType.php	VVTDatenkategorieType.php
	_form.html.twig	_form.html.twig
	index.html.twig	index.html.twig
Controller	LoeschkonzeptController.php	VVTDatenkategorieController.php
Service	LoeschkonzeptService.php	VVTDatenkategorieService.php

Tabelle 6.1: Neu erstellte Klassen

Außerdem muss die Datei *__berichtLoeschkonzept.html.twig* erstellt werden, damit die Berichte über alle bestehenden Löschkonzepte mit oder ohne Historie als PDF-Datei exportiert werden können. Daneben gibt es weitere bestehende Klassen, die modifiziert werden müssen. Diese werden in Tabelle 6.2 aufgezählt.

	Datenkategorien	VVT
Model	VVTDatenkategorie.php	
View		VVTType.php

Tabelle 6.2: Modifizierte Klassen

Auch die Datei *__vvtBericht.html.twig* muss modifiziert werden, damit bei der Berichterstellung von Verarbeitungstätigkeiten anschließend auch die neuen Löschkonzepte enthalten sind.

6.2.1 Datenkategorien erstellen und verwalten

Im Rahmen der Erstellung von Löschkonzepten sollen auch Datenkategorien überarbeitet werden. Die Datenkategorien verfügten über kein eigenes MVCS-Pattern. Lediglich das Model zu den Datenkategorien hat existiert und wurde überall da, wo sie gebraucht wurden, mit verknüpft. Nun sollen die Datenkategorien für sich alleine stehen können, das heißt, die Funktion „Datenkategorien dokumentieren“ kann ohne weitere Verknüpfungen zu anderen Pattern durchgeführt werden. Dazu musste nun ein eigenes MVCS-Pattern um das Model Modul herum aufgebaut werden.

Eine wichtige Eigenschaft der Dokumentationen des *Open Datenschutzcenters* ist die Revisionssicherheit. Das bedeutet, dass angelegte Datenkategorien nicht mehr verändert werden können, damit bei einer späteren Berichterstellung die Datenkategorien, die zu den Zeitpunkten in der Vergangenheit aktuell waren, auch noch in ihrer vergangenen Form angezeigt werden. Dennoch muss es möglich sein, dass Datenkategorien angepasst werden können. Im Rahmen der Neugestaltung wurden den Datenkategorien auch Datenarten als Dokumentationsfeld hinzugefügt, sodass der Nutzer unter dem Überbegriff der Datenkategorie detaillierter definieren kann, welche Datenarten dieser Datenkategorie zugeordnet werden. Gerade dieser Detailgrad kann sich mit der Zeit ändern, wenn neue Datenarten erhoben werden oder bis dato erhobene Datenarten in Zukunft nicht mehr erhoben werden.
Um die Revisionssicherheit und Anpassbarkeit der Datenkategorien zusammenführen zu können, werden die Datensätze bei der Bearbeitung grundsätzlich dupliziert. Der alte Datensatz wird mit einem activ-Flag auf *false* gesetzt, während der duplizierte Datensatz den Status *true* erhält. Dadurch kann der alte Datensatz erhalten und unverändert bleiben, wird durch den neuen Status nicht mehr angezeigt und nur bei der Berichterstellung berücksichtigt. Die neusten Änderungen werden in dem Duplikat vorgenommen und dieses wird fortan für weitere Dokumentationen und Verknüpfungen genutzt. Damit diese Datenkategorie allerdings noch über eine Relation verfügt, von wem sie abstammt, wird mittels einer *OneToOne*-Verknüpfung ein previous-Zeiger gesetzt, der auf die duplizierte Datenkategorie verweist. Wenn der Nutzer eine Datenkategorie löscht, wird auch dieser Datensatz nicht aus der Datenbank entfernt, sondern das activ-Flag wird auf *false* gesetzt. Somit ist auch die neuste Version dieser Datenkategorie inaktiv und kann nicht mehr durch den Nutzer abgerufen werden. Damit endet der Versionsverlauf dieser Datenkategorie. Möchte der Nutzer zu einem späteren Zeitpunkt dieselbe Datenkategorie wieder einführen, muss er eine neue Datenkategorie anlegen. Diese hat keine Verknüpfung zur alten, gelöschten Datenkategorie und ein neuer Versionsverlauf beginnt.
In Abb. 6.2 sind diese Relationen dargestellt. Die roten Datenkategorie (DK) sind activ=*false* und die grüne ist activ=*true*. Der Nutzer kann zu diesem gegenwärtigen Zeitpunkt nur noch mit der DK1.2 interagieren, DK1.0 und DK1.1 existieren jedoch noch und können bei der Berichterstellung herangezogen werden.

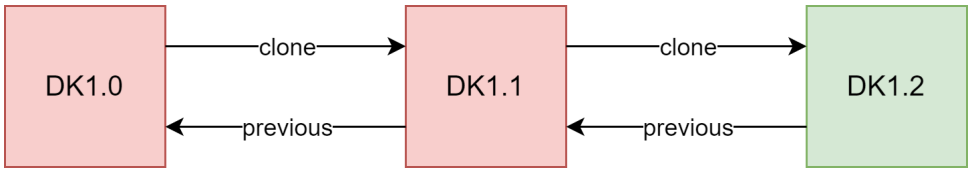

Abbildung 6.2: Datenkategorie duplizieren

VVTDatenkategorie.php und VVTDatenkategorieRepository.php
Entity- und Repository-Klasse

Einige Variablen wurden in der Entity Klasse hinzugefügt, um Relationen zu den Löschkonzepten und Verarbeitungstätigkeiten zu ermöglichen. Zum Beispiel wurde die *ManyToMany*-Relation zu den Löschkonzepten hinzugefügt, um den Datenkategorien Löschkonzepte zuordnen zu können. Wichtig ist auch, dass die *OneToOne*-Verknüpfung zwischen den Datenkategorien hinzugefügt wurde, um nach dem Duplizieren noch nachvollziehen zu können, von welcher Datenkategorie die neu duplizierte Version abstammt. Außerdem wurde der Entity-Klasse die Variable Datenarten hinzugefügt, damit ab jetzt die Datenkategorien detaillierter mit Unterarten beschrieben werden können. Auch die Erstellung einer Repository-Klasse war notwendig, damit aus Services anderer MVCS-Pattern auf die Datenkategorien zugegriffen werden kann.

VVTDatenkategorieController -Service, -Type und Templates
Controller- , Service- und View-Klassen

Um mit den Datenkategorien unabhängig interagieren zu können, musste auch eine neue Controller-Klasse erstellt werden. Diese beinhaltet die Logik für das Anzeigen des Indexes und für die Erstellung, das Bearbeiten und das Löschen von Datenkategorien. Der wichtigste Teil in Bezug auf die Datenkategorien befindet sich jedoch in der Service-Klasse. Wie in Abb. 6.5 bereits abstrahiert beschrieben, werden die Datenkategorien und ihre zugehörigen Löschkonzepte bei der Verknüpfung mit einer Verarbeitungstätigkeit kopiert. Dafür wird die *createChild*-Funktion benötigt, die in Listing 6.1 zu sehen ist.

```
1  function createChild(VVTDatenkategorie $vVTDatenkategorie)
2  {
3   $childVVTDatenkategorie = new VVTDatenkategorie();
4   $childVVTDatenkategorie->setCloneOf($vVTDatenkategorie);
5   $childVVTDatenkategorie->setCreatedAt(new \
       DateTimeImmutable())
6   ->setPrevious(null)
7   ->setName($vVTDatenkategorie->getName())
8   ->setDatenarten($vVTDatenkategorie->getDatenarten())
9   ->setTeam($vVTDatenkategorie->getTeam())
10  ->setUser($vVTDatenkategorie->getUser())
11  ->setActiv(false);
12
13  $loeschkonzept = $vVTDatenkategorie->getLastLoeschkonzept
       ();
14  if ($loeschkonzept) {
15   $childLoeschkonzept =new Loeschkonzept();
16   $childLoeschkonzept->setUser($loeschkonzept->getUser())
17   ->setTeam($loeschkonzept->getTeam())
18   ->setPrevious(null)
19   ->setCloneOf($loeschkonzept)
20   ->setUser($loeschkonzept->getUser())
21   ->setActiv(false)
22   ->setBeschreibung($loeschkonzept->getBeschreibung())
```

```
23      ->setCreateAt(new \DateTimeImmutable())
24      ->setLoeschbeauftragter($loeschkonzept->
            getLoeschbeauftragter())
25      ->setLoeschfrist($loeschkonzept->getLoeschfrist())
26      ->setSpeicherorte($loeschkonzept->getSpeicherorte())
27      ->setStandartlf($loeschkonzept->getStandartlf());
28
29      $childVVTDatenkategorie->addLoeschkonzept(
            $childLoeschkonzept);
30    }
31    return $childVVTDatenkategorie;
32  }
```

Listing 6.1: VVTDatenkategorieService.php – createChild-Funktion

Die *createChild*-Funktion erstellt zunächst eine neue Datenkategorie und verknüpft diese per *setCloneOf* mit der Datenkategorie, welche kopiert werden soll.(Z. 3-4) Anschließend werden die meisten Parameter der zu kopierenden Datenkategorie übernommen. Mit *setPrevious(null)* wird jedoch die Kopie vom restlichen Versionsverlauf der kopierten Datenkategorie gelöst.(Z. 6) Die Kopie steht für sich alleine und verweist lediglich per *getCloneOf* auf ihren Ursprung, nicht aber auf den Versionsverlauf. Auch wird die Kopie von Beginn an auf inaktiv gesetzt, damit der Nutzer diese Kopie nur bei der Berichterstellung zu Gesicht bekommt. Dies geschieht mit *setActiv(false).*(Z. 11)
Im zweiten Teil der Funktion wird nun das aktuelle Löschkonzept zu dieser Datenkategorie gesucht.(Z. 13) Wenn es ein aktuelles Löschkonzept gibt, wird auch dieses kopiert. Die meisten Parameter werden übernommen, einige müssen angepasst werden, wie zum Beispiel der activ-Status, und abschließend wird das kopierte Löschkonzept der kopierten Datenkategorie zugeordnet.(Z. 14-27) Damit ermöglicht diese Funktion die Kopie von Datenkategorien mit ihren Löschkonzepten, um diese einer Verarbeitungstätigkeit zuordnen zu können und dabei die Revisionssicherheit zu gewährleisten, indem die Kopien nicht mehr bearbeitet werden können.
Eine zweite wichtige Funktion ist die *findLatestKategorie-Funktion.* Diese ermöglicht es, dass man über die previous-Verknüpfung die neuste Version einer Datenkategorie finden kann. Das ist wichtig, wenn eine Verarbeitungstätigkeit bearbeitet wird und man automatisch die neusten Versionen der Datenkategorien anzeigen lassen möchte, die bei der Erstellung der Verarbeitungstätigkeit kopiert wurden.

6.2.2 Löschkonzepte erstellen und verwalten

Nachdem die Datenkategorien ihr eigenes MVCS-Pattern erhalten haben, ist es notwendig, das MVCS-Pattern für die Lösch-konzepte zu implementieren. Die Löschkonzepte sollen keine eigenen Namen haben, sondern sich über die Datenkategorien definieren, die ihnen zugeordnet sind. Das Model enthält mehrere Variablen, von denen einige aktiv durch den Nutzer manipuliert werden können. Zur Erstellung eines Löschkonzeptes wird dem Nutzer in der View ein Formular

dargestellt, indem er per Dropdown-Menü auswählen kann, welchen Datenkategorien er das neue Löschkonzept zuordnen möchte. Anschließend muss der Nutzer eine Standard-Löschfrist, möglicherweise eine gesetzliche Löschfrist, Speicherorte, Löschbeauftragte und weitere Beschreibungen zum Löschkonzept dokumentieren. Auch bei Löschkonzepten ist die Revisionssicherheit von großer Bedeutung, da diese in Form eines PDF-Berichtes exportiert werden können. Um die Revisionssicherheit herzustellen, werden auch die Löschkonzepte beim Editieren dupliziert, sodass das alte Löschkonzept unverändert bleibt. An dieser Stelle wird auf Abb. 6.3 verwiesen, in der die Relationen zwischen Datenkategorien und Löschkonzepten dargestellt sind.
Auch die Löschkonzepte enthalten ein activ-Flag, mit dem alte Löschkonzepte inaktiv geschaltet werden können und neue aktiv bleiben. Da inaktive Datenkategorien und Löschkonzepte weiterhin im Hintergrund existieren und für die Berichterstellung auch vergangene Relationen bekannt bleiben müssen, besteht zwischen Löschkonzepten und Datenkategorien eine *ManyToMany*-Relation. Eine Datenkategorie kann zum gegenwärtigen Zeitpunkt nur einem Löschkonzept aktiv angehören. Die gleiche Datenkategorie kann in der Vergangenheit aber auch einem anderen oder gar keinem Löschkonzept angehört haben. In der Übersicht der aktiven Datenkategorien werden auch ihre zugewiesenen Löschkonzepte angezeigt. Über eine Funktion, welche die neuste Relation heraussucht, wird sichergestellt, dass hier auch immer das neuste verknüpfte Löschkonzept angezeigt wird. Wenn eine Datenkategorie bearbeitet wird, wird auch hier die neueste Version automatisch in dem zugeordneten Löschkonzept übernommen. Um die Revisionssicherheit nicht zu gefährden, werden bei der Berichterstellung aber auch diejenigen inaktiven Datenkategorien mit ausgegeben, die jemals mit diesem Löschkonzept verknüpft waren. Die inaktiven Datenkategorien werden dementsprechend markiert. Bei der Aktualisierung des Löschkonzeptes und einer damit einhergehenden neuen Version durch das Duplizieren, werden die inaktiven Datenkategorien aus der Relation entfernt, da diese niemals mit der neuen Version des Löschkonzeptes verknüpft waren.
Abb. 6.3 zeigt folgenden Ablauf: DK1.0 wurde erstellt. Anschließend wurde DK1.0 das Löschkonzept (LK) 1.0 zugewiesen. DK1.0 wurde dupliziert und DK1.1 hat das LK1.0 übernommen. DK1.0 wurde dabei inaktiv gesetzt. Daraufhin wurde LK1.0 dupliziert und ebenfalls inaktiv. Das neue LK1.1 hat die zugeordnete DK1.1 übernommen. Abschließend wurde DK1.1 bearbeitet, sodass DK1.2 entstanden ist. DK1.1 wurde dadurch auch inaktiv und die aktive DK1.2 hat das aktive LK1.1 übernommen. In der Datenkategorien-Übersicht wird jetzt nur die DK1.2 angezeigt mit der LK1.1 als zugeordnetem Löschkonzept. In der Übersicht der Löschkonzepte wird nur das LK1.1 angezeigt mit DK1.2 als zugeordnete Datenkategorie. Bei der Erstellung des Löschkonzeptberichtes wird LK1.1 hingegen mit DK1.1 als inaktiv und DK1.2. als aktiv zugeordnete Datenkategorie angezeigt. Die Revisionssicherheit strebt aber mehr an, als das aktuelle Löschkonzept mit allen jemals zugeordneten Datenkategorien anzuzeigen. Um einen Historien-Bericht erstellen zu können, müssen auch die Löschkonzepte mit einer *OneToOne*-Relation so verknüpft sein, dass eine Version des Löschkonzeptes immer auf die vorherige Version

verweist, solange eine frühere Version vorhanden ist. Dadurch wird es möglich, neben der aktuellen Version des Löschkonzeptes mit allen jemals verknüpften Datenkategorien, auch alle früheren Versionen in historisch korrekter Reihenfolge mit allen jemals ihnen zugeordneten Datenkategorien anzuzeigen. Auch die Datenarten werden in den Berichten mit angezeigt. Da diese aber im gleichen Datensatz, wie die zugehörige Datenkategorie enthalten sind, werden diese ebenso als aktiv oder inaktiv bei den richtigen Löschkonzepten mit angezeigt.

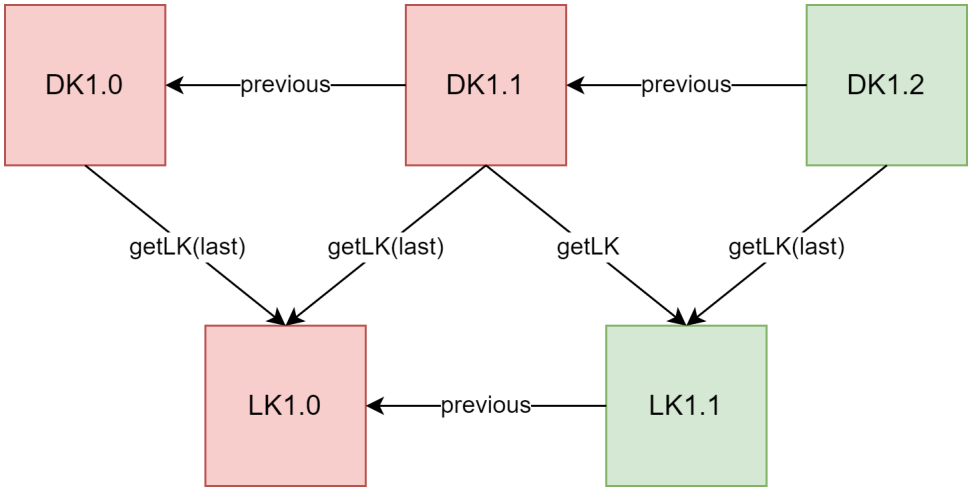

Abbildung 6.3: Datenkategorie-Löschkonzept-Relation

Loeschkonzept.php und LoeschkonzeptRepository.php
Entity- und Repository-Klasse

In der Entity Klasse werden die Variablen definiert, mit denen man im Rahmen der Löschkonzept-Dokumentation arbeiten möchte. Dazu wird die Basis-Entity-Klasse mit dem Konsolen-Befehl `php bin/console make:entity` erstellt. Die Erstellung der Klasse ist ein Prozess, in dem auch die benötigten Eigenschaften abgefragt werden. Zu einer Variable gehören die mit ihr in Verbindung stehenden Funktionen. Per Default erstellt die Maker-Funktion automatisch die get- und set-Funktion, um die erstellte Variable abrufen oder neu definieren zu können. Im weiteren Verlauf können weitere benötigte Funktionen manuell hinzugefügt werden. Neben der Erstellung der Entity-Klasse wird mit diesem Befehl auch die Repository-Klasse erstellt. Diese Klasse sorgt dafür, dass man aus anderen Klassen auf die Entität zugreifen kann. In Abb. 6.4 ist die Löschkonzpet-Entity-Klasse mit ihren wichtigsten Variablen und Funktionen dargestellt. Die Verknüpfung mit den Datenkategorien, die in ihrer eigenen Entity verwaltet werden, ist in dieser Klasse am wichtigsten. Dem Nutzer soll es möglich sein, dass er bei der Erstellung von Löschkonzepten Datenkategorien, welche in der Datenkategorien-SQL-Tabelle verwaltet werden, auswählen kann. Dafür ist die *ManyToMany*-Verknüpfung nötig. Diese Verknüpfung ermöglicht es, dass Datenkategorien Löschkonzepten zugeordnet werden

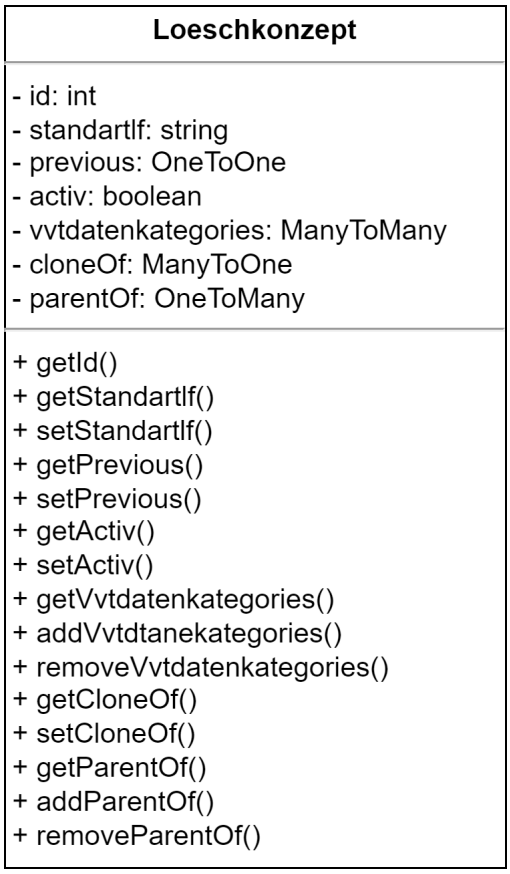

Abbildung 6.4: Löschkonzept Klassendiagramm

können. In der Löschkonzept-Entity-Klasse in Listing 6.2 wurden folgende Funktionen ergänzt, damit das Abfragen (Z. 4-7), Hinzufügen (Z. 8-15) und Entfernen (Z. 17-26) von Datenkategorien bei Löschkonzepten möglich wird:

```
1  /**
2  * @return Collection<int, VVTDatenkategorie>
3  */
4  public function getVvtdatenkategories(): Collection
5  {
6   return $this->vvtdatenkategories;
7  }
8  public function addVvtdatenkategory(VVTDatenkategorie
       $vvtdatenkategory): self
9  {
10  if (!$this->vvtdatenkategories->contains($vvtdatenkategory
       )) {
11   $this->vvtdatenkategories[] = $vvtdatenkategory;
12   $vvtdatenkategory->setLoeschkonzept($this);
13  }
14  return $this;
15 }
16
```

```
17  public function removeVvtdatenkategory(VVTDatenkategorie
        $vvtdatenkategory): self
18  {
19   if ($this->vvtdatenkategories->removeElement(
        $vvtdatenkategory)) {
20    if ($vvtdatenkategory->getLoeschkonzept() === $this) {
21     $vvtdatenkategory->setLoeschkonzept(null);
22    }
23   }
24   return $this;
25  }
```

Listing 6.2: Loeschkonzept.php – Datenkategorie-Funktionen

LoeschkonzeptController -Service, -Type und Templates

Controller- , Service- und View-Klassen

Nachdem man mit `php bin/console make:entity` die Entity- und Repository-Klassen erstellt hat, hilft der Konsolen-Befehl `php bin/console make:crud` dabei, dass zu der ausgewählten Entity der passende Controller und die passenden Klassen der View generiert werden. CRUD ist die Abkürzung für create, read, update, delete und steht damit für die Funktionalitäten, die durch den Controller bereitgestellt werden. Auch hier werden standardisierte Klassen generiert, die anschließend manuell an die Anforderungen angepasst werden müssen. Die Controller-Klasse ist dafür zuständig, dass das Model und die View miteinander kommunizieren können. Hier wird die Logik der Funktion implementiert. Dazu gehört, was geschehen muss, wenn eine Übersicht angezeigt werden soll oder wenn, in diesem Fall, Dokumentationen erstellt, bearbeitet oder gelöscht werden sollen. Im Löschkonzept-Controller ist die Funktion zum Bearbeiten von Löschkonzepten die komplexeste. Der gesamte Vorgang des Bearbeitens wurde in Abb. 6.3 bereits abstrahiert beschrieben. Im Folgenden wird der Codeabschnitt dazu dargestellt und erklärt.

```
1   /**
2   * @Route("/{id}/edit", name="app_loeschkonzept_edit",
        methods={"GET", "POST"})
3   */
4   public function edit([...]): Response
5   {
6    $team = $this->getUser()->getTeam();
7    if ($securityService->teamCheck($team) === false) {
8     return $this->redirectToRoute('app_loeschkonzept_index');
9    }
10   $vvtDatenkategories = $VvtDatenkategorieRepository->
        findByTeam($team);
11   foreach ($vvtDatenkategories as $vvtDatenkategorie) {
12    if ($vvtDatenkategorie->getLoeschkonzept()->last() !=
        $loeschkonzept) {
13     $loeschkonzept->removeVvtdatenkategory(
         $vvtDatenkategorie);
14    }
```

```
15    }
16    $newloeschkonzept = $loeschkonzeptService->
          cloneLoeschkonzept($loeschkonzept);
17    foreach ($loeschkonzept->getVvtdatenkategories() as
          $datenkategorie){
18     $newloeschkonzept->addVvtdatenkategory($datenkategorie);
19    }
20    $form = $loeschkonzeptService->createForm(
          $newloeschkonzept, $team);
21    $form->handleRequest($request);
22    if ($form->isSubmitted() && $form->isValid()) {
23     $loeschkonzeptRepository->add($newloeschkonzept);
24     $newloeschkonzept->setActiv(true);
25     $loeschkonzept->setActiv(false);
26     $entityManager->persist($loeschkonzept);
27     $entityManager->persist($newloeschkonzept);
28     $entityManager->flush();
29     return $this->redirectToRoute('app_loeschkonzept_index',
           [], Response::HTTP_SEE_OTHER);
30    }
31    return $this->renderForm('loeschkonzept/edit.html.twig', [
32    'loeschkonzept' => $newloeschkonzept,
33    'form' => $form,
34    ]);
35   }
```

Listing 6.3: LoeschkonzeptController.php – Edit-Funktion

Die Edit-Funktion in Listing 6.3 sorgt dafür, dass der Nutzer nicht das bereits bestehende Löschkonzept bearbeitet, sondern die Änderungen in einem Duplikat vorgenommen werden. Bei der Bearbeitung eines Löschkonzeptes wird das vorhandene Löschkonzept mit der Funktion *cloneLoeschkonzept* aus dem Loeschkonzept-Servie dupliziert. Das duplizierte Löschkonzept wird in Zeile 25 auf inaktiv gesetzt und fortan nicht mehr angezeigt, bis ein Bericht über alle erstellten Löschkonzepte mit Historie ausgegeben werden soll. In dem duplizierten Löschkonzept werden die Änderungen eingetragen. Anschließend wird das geänderte Löschkonzept als neues Löschkonzept gespeichert und in Zeile 26 auf aktiv gesetzt, damit der Nutzer fortan mit dieser Version des Löschkonzeptes interagieren kann. Es besteht aber weiterhin eine Verknüpfung zu dem inaktiven Löschkonzept als sein Vorgänger, damit die Verknüpfung bei der Historie auch richtig ausgegeben wird. Dieser Prozess des Duplizierens wurde in Zeile 16-21 durchgeführt. Dieses Duplizieren sorgt mit der Zeit dafür, dass die Datenbank sehr viele Datensätze enthält, mit denen der Nutzer nicht mehr interagiert. Jedoch werden diese Datensätze zum Erstellen der Historie benötigt. Da diese Funktion auch in den anderen Dokumentationen, wie zum Beispiel der VVT-Dokumentation vorhanden ist, muss das Duplizieren auch hier durchgeführt werden, um später eine durchgehende Dokumentationsstruktur vorweisen zu können.

6.2.3 Verarbeitungstätigkeiten erstellen und verwalten

Da die Datenkategorien nun mit den Löschkonzepten verknüpft sind, müssen die Datenkategorien noch korrekt mit den Verarbeitungstätigkeiten verbunden werden. Da die Verarbeitungstätigkeiten keine direkte Verknüpfung zu den Löschkonzepten haben, sondern über die Datenkategorien auf die dazugehörigen Löschkonzepte zugreifen, ist es auch hier kompliziert, die Revisionssicherheit zu gewährleisten. Der Zugriff auf die Löschkonzepte über die Datenkategorien wurde in dieser Form implementiert, damit im Verarbeitungsverzeichnis die richtigen Löschkonzepte zu den richtigen Datenkategorien angezeigt werden können. Da das VVT die Kerndokumentation der DSGVO darstellt, ist die Revisionssicherheit hier am wichtigsten, um eine nicht manipulierbare Historie erstellen zu können. Aus diesem Grund wurde entschieden, dass bei der Erstellung einer Verarbeitungstätigkeit keine Verknüpfungen zu den bestehenden Datenkategorien vorgenommen, sondern dass die ausgewählten Datenkategorien unverändert kopiert und der Verarbeitungstätigkeit zugeordnet werden. Diese kopierten Datenkategorien existieren in der gleichen Datentabelle, wie alle anderen Datenkategorien. Allerdings existieren sie nur im Hintergrund, sie sind für den Nutzer nicht aufrufbar. Diese parallele Existenz in der gleichen Datentabelle wird durch ein clone-Flag ermöglicht, wodurch man die darstellbaren Datenkategorien von den kopierten Datenkategorien abgrenzen kann. Durch das Kopieren der ausgewählten Datenkategorien in ihrer gegenwärtigen Version wird ermöglicht, dass an der Verarbeitungstätigkeit keine Änderungen durchgeführt werden können, ohne aktiv die Verarbeitungstätigkeit zu bearbeiten und dadurch eine neue duplizierte und anschließend angepasste Version dieser Verarbeitungstätigkeit zu erstellen. Im Rahmen der Anpassung einer Verarbeitungstätigkeit werden automatisch die neusten Versionen der bis dato ausgewählten Datenkategorien kopiert und der neuen Verarbeitungstätigkeit zugeordnet. Auch die aktuellsten Versionen der Löschkonzepte zu den Datenkategorien werden kopiert und mit den kopierten Datenkategorien verknüpft. Die kopierten Löschkonzepte existieren, wie bei den Datenkategorien auch, in der gleichen Datentabellen, wie alle anderen Löschkonzepte. Durch das clone-Flag kann auch hier eine separate Betrachtung stattfinden. Dadurch wird gewährleistet, dass, selbst wenn der Nutzer keine Änderungen an den zugewiesenen Datenkategorien durchführt, nach einer Bearbeitung nur die neusten Versionen der zugeordneten Datenkategorien, mit den aktuellen Versionen der zugeordneten Löschkonzepte, der neuen Version der Verarbeitungstätigkeit zugeordnet werden. Sollte der Nutzer bei der Bearbeitung einer Verarbeitungstätigkeit ein Datenkategorie entfernen, wird von der entfernten Kategorie keine Kopie mehr angelegt und die Datenkategorie hat keine weitere Verknüpfung zu der neuen Version der Verarbeitungstätigkeit. Durch das Kopieren der Datenkategorien mit ihren Löschkonzepten und die weitere passive Existenz dieser Kopien kann garantiert werden, dass keine Änderungen an der Zuordnung und der Beschreibung der Datenkategorien sowie Löschkonzepten vorgenommen werden können.
Um bei der Erstellung und Bearbeitung einer Verarbeitungstätigkeit die benötigten Datenkategorien auswählen zu können, wurde die Dropdown-Darstellung der

bereits existierenden Formulardarstellung übernommen. Lediglich die Anzeige der Datenkategorien innerhalb des Dropdown-Menüs wurde angepasst. Die Datenkategorien werden nun nicht mehr alleine mit ihrem Namen angezeigt, sondern auch mit ihrer Standard-Löschfrist, sofern die Datenkategorien einem Löschkonzept zugeordnet sind. Dadurch braucht der Nutzer sich bei der Dokumentation von Verarbeitungstätigkeit nicht mehr um Löschkonzepte und Löschfristen kümmern, da er vorher bei der Auseinandersetzung mit den Löschkonzepten, die Löschfristen und Zuordnungen zu den Datenkategorien bereits dokumentiert hat.
In Abb. 6.5 sind die Relationen zwischen Verarbeitungstätigkeiten, Datenkategorien und ihren Löschkonzepten dargestellt. Im Folgenden wird erläutert, welcher Prozess stattgefunden hat, damit es zu diesen Verknüpfungen gekommen ist. Zu Beginn wurde die DK 1.0 erstellt. Diese ist in der Abbildung nicht zu erkennen. DK1.0 wurde bearbeitet, sodass DK1.1 entstanden ist. Parallel wurde das LK1.0 erstellt. Auch dieses ist hier nicht abgebildet. LK1.0 wurde ebenfalls bearbeitet, sodass LK1.1 die neuste Version des Löschkonzeptes ist. Nun wurde DK1.1 dem LK1.1 zugeordnet. Anschließend wurde die Verarbeitungstätigkeit (VT) 1.0 erstellt. Dieser Verarbeitungstätigkeit wurde die Datenkategorie DK1.1 zugeordnet. Da nun aber keine Verknüpfung zwischen der Datenkategorie DK1.1, die dem Nutzer zur Bearbeitung zur Verfügung steht, und der Verarbeitungstätigkeit VT1.0 erstellt wird, wurde DK1.1 und das zugehörige Löschkonzept LK1.1 kopiert. Diese Kopien (K) DK1.1K1 und LK1.1-K1 werden mit der VT1.0 verknüpft. Bei einer Berichterstellung zum gegenwärtigen Zeitpunkt würde lediglich das VT1.0 mit der DK1.1-K1 als Datenkategorie und LK1.1-K1 als zugehöriges Löschkonzept ausgegeben werden.
Als Nächstes wird die Datenkategorie DK1.1 angepasst. Es entsteht die neue Version DK1.2. DK1.1 wird inaktiv gesetzt und DK1.2 wird zur neuen aktiven Datenkategorie. An dem zugeordneten Löschkonzept ändert sich nichts, sodass die DK1.2 weiterhin mit dem LK1.1 verknüpft bleibt. Im weiteren Verlauf wird die VT1.0 angepasst. Dadurch wird die VT1.0 dupliziert und inaktiv gesetzt. Es entsteht die VT1.1. VT1.1 prüft nun über die Herkunft der kopierten DK1.1-K1, ob es eine neuere Version dieser Datenkategorie gibt. Da DK1.1 DK1.2 als neuere Version vorweisen kann, wird die DK1.2 kopiert und mit der VT1.1 verknüpft. Auch das LK1.1, als neustes Löschkonzept der DK1.2, wird kopiert und mit der DK1.2-K1 verknüpft. So ist die Verknüpfung entstanden, dass der VT1.1 die DK1.2-K1 zugeordnet wurde und der DK1.2-K1 das LK1.1-K2. Bei der Berichterstellung der aktuellen Verarbeitungstätigkeiten wird nun die VT1.1 mit der DK1.2-K1 als Datenkategorie und LK1.1 als zugehöriges Löschkonzept ausgegeben. Wird ein Bericht mit Historie erstellt, steht auch die VT1.1 an oberster Stelle. Es wird jedoch auf VT1.0 verwiesen. VT1.0 wird anschließend mit DK1.1-K1 und LK1.1-K1 angezeigt. Durch diese separate Behandlung wird sichergestellt, dass egal, was bei den Datenkategorien und Löschkonzepten angepasst oder gelöscht wird, die Verarbeitungstätigkeiten in ihren Versionen unveränderbar bleiben und die Revisionssicherheit bzgl. Datenkategorien und Löschkonzepten sichergestellt ist. Einer Verarbeitungstätigkeit können auch mehreren Datenkategorien mit unterschiedli-

chen Löschkonzepten zugeordnet werden. Für alle zugeordneten Datenkategorien wird der Prozess des Kopierens und neu Verknüpfens wiederholt.

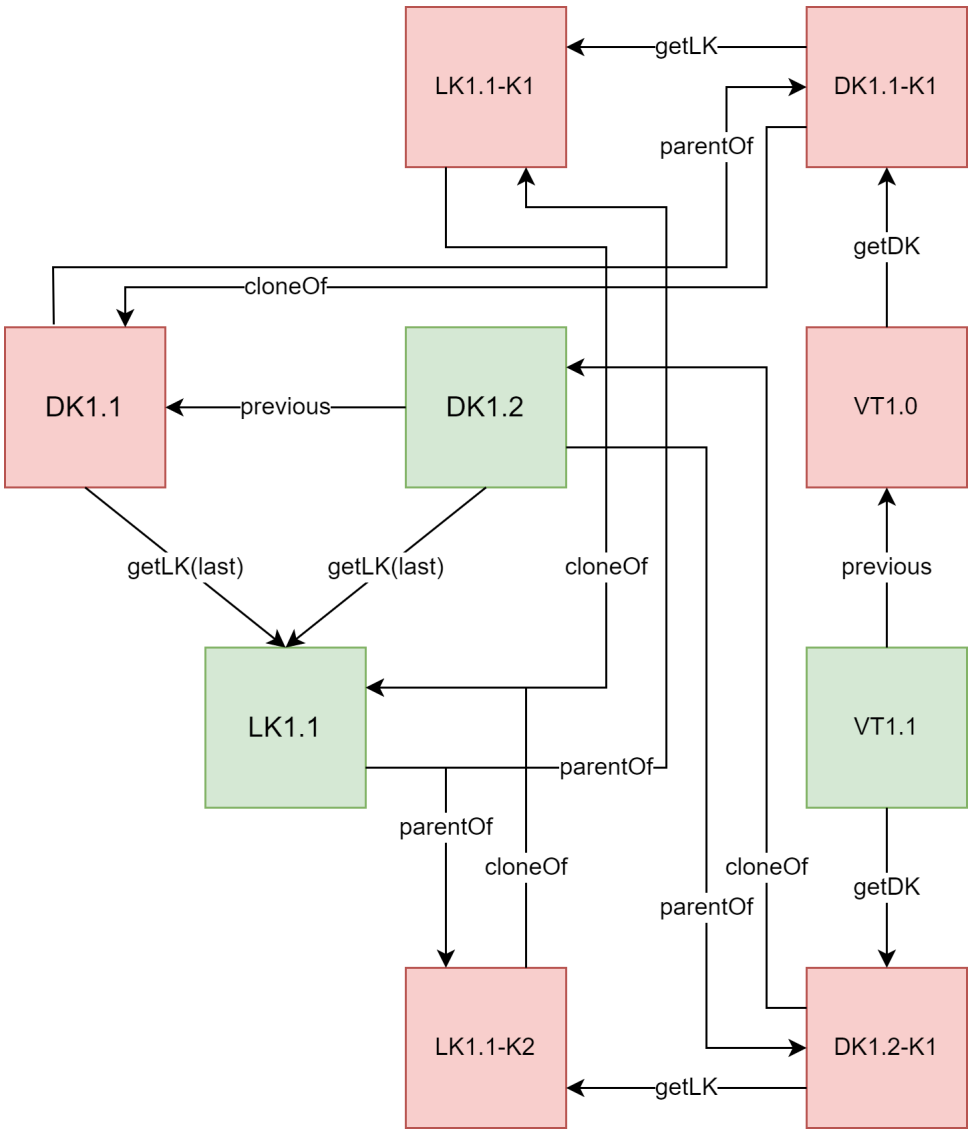

Abbildung 6.5: VT-Datenkategorie-Löschkonzept-Relation

6.2.4 Anforderungen und ihre Umsetzung

In diesem Abschnitt wird in kurzen Beschreibungen darauf eingegangen, wie die Anforderungen aus 5.1 praktisch umgesetzt wurden.

Benutzbarkeit der Software fördern (A1)
Um die Benutzbarkeit der Software zu fördern wurde aufseiten des Designs die Designstruktur der bereits bestehenden Software beibehalten. Die Funktionen „Datenkategorien dokumentieren“ und „Löschkonzepte dokumentieren“ haben vier

verschiedenen Anzeigekomponenten. Die Übersicht, das Formular zum Erstellen neuer Datenkategorien oder Löschkonzepte, das Formular zum Bearbeiten der bestehenden Dokumentationen und eine Ansichtsseite, in der alle Informationen zu einer Dokumentation angezeigt werden. Innerhalb der Formulare wurden kurze Hilfstexte angegeben, die dem Nutzer erläutern, welche Informationen in die Formularfelder eingetragen werden sollen. Es bestehen Verlinkungen zwischen den Datenkategorien und den Löschkonzepten und bei der Auswahl von Datenkategorien bei Verarbeitungstätigkeiten, werden die Löschfristen automatisch mit angezeigt.

Intuitive Bedienung der neuen Funktion gewährleisten (A2) und zentrale Verwaltung der Löschkonzepte ermöglichen (A3)
Das intuitive Bedienen der neuen Funktionen wird ebenfalls durch die Übernahme des Designs und der Erläuterungstexte in den Formularen gewährleistet. Um die zentrale Verwaltung der Löschkonzepte zu ermöglichen, wurde ein neuer Button auf dem Dashboard eingeführt, der zur Funktion „Löschkonzepte dokumentieren“ weiterleitet. In dieser Funktion werden in der Übersicht alle Löschkonzepte zentral angezeigt, sodass der Nutzer einen schnellen Überblick über seine existierenden Löschkonzepte erhalten kann. Wenn er innerhalb dieser Funktion neue Löschkonzepte anlegt oder existierende Konzepte bearbeitet, werden die Neuerungen zu den Datenkategorien und in den Verarbeitungstätigkeiten automatisch übernommen.

Datenkategorien um Datenarten ergänzen (A4)
Damit die Datenkategorien um ihre Datenarten ergänzt werden können und man besser mit den Datenkategorien arbeiten kann, wurde ein weiterer Button auf dem Dashboard platziert, mit dem man in die Funktion „Datenkategorien dokumentieren“ gelangt. Auch hier gibt es eine Übersicht über alle bereits existierenden Datenkategorien mit ihren zugeordneten Löschkonzepten. Im neuen Formular können nun die Datenarten zu den Datenkategorien ergänzt werden.

Möglichkeit zur Standardisierung schaffen (A5)
Die Standardisierung wurde damit geschaffen, dass mehrere Datenkategorien einem Löschkonzept zugeordnet werden können, damit nicht für jede Datenkategorie ein Löschkonzept angelegt werden muss. Außerdem können die Datenkategorien mit ihren zugeordneten Löschkonzepten mehreren Verarbeitungstätigkeiten zugeordnet werden. Beide Auswahlangebote wurden über ein Dropdown-Menü realisiert, in dem der Nutzer sieht, welche Datenkategorien bereits ausgewählt sind, welche Datenkategorien aktuell zu andern Löschkonzepten gehören und welche er noch zu den Dokumentationen hinzufügen kann.

Kurze Wege ermöglichen (A6)
Um kurze Wege zu ermöglichen wurden die beiden Funktionen direkt auf dem Dashboard platziert. Außerdem gibt es Verlinkungen zwischen den Datenkategorien und ihren Löschkonzepten, sodass man für weitere Informationen zu den Löschkonzepten, aus der Datenkategorie-Übersicht direkt zu dem Löschkonzept navigieren kann, welches betrachtet werden soll. Bei der Berichterstellung sind die Löschkon-

zepte und Datenkategorien so verlinkt, dass man aus dem PDF-Dokument die angezeigten Datenkategorien und Löschkonzepte abrufen kann.

Kompatibilität mit alten Software-Versionen sicherstellen (A7)
Um die Kompatibilität mit alten Software-Versionen sicherzustellen wurden einige Migrationen für die SQL-Datenbank erstellt. Dabei wurde beachtet, dass bereits bestehende Datensätze bei den Nutzern durch ein Update nicht zerstört, sondern nur ergänzt werden. Um kleine notwendige Änderungen in den bestehenden Datensätzen der Nutzer durchführen zu können, wurde zudem ein Migrations-Command geschrieben. Alte Löschfristen, die in den einzelnen Verarbeitungstätigkeiten dokumentiert wurden, können jetzt nicht mehr verändert werden. Jedoch werden sie dem Nutzer noch übergangsweise angezeigt, damit er die alten Löschfristen möglicherweise mit in die neuen Löschkonzepte einarbeiten kann. Damit wird erreicht, dass die Nutzer ihre bestehenden Datensätze weiter nutzen können, aber nun die neuen Funktionen in ihre Dokumentationen mit einbeziehen müssen.

Revisionssicherheit für die Berichterstellung (A8)
Die Revisionssicherheit für die Berichterstellung wird dadurch sichergestellt, dass sowohl die Datensätze der Datenkategorien, als auch die der Löschkonzepte bei der Bearbeitung dupliziert werden, sodass einmal erstellte Datensätze nicht verändert werden können. Durch ein boolean-Flag werden bearbeitete Datensätze inaktiv geschaltet, damit diese nicht mehr angezeigt werden. Die duplizierten Datensätze, die auch die Änderungen enthalten, werden aktiv geschaltet und stehen dem Nutzer weiter zur Verfügung. Bei der Dokumentation von Verarbeitungstätigkeiten und der Verknüpfung mit Datenkategorien und ihren Löschkonzepten werden sowohl die Datenkategorien, als auch die zugehörigen Löschkonzepte exklusiv für die dokumentierte Verarbeitungstätigkeit kopiert. Auch diese Kopien sind für den Nutzer nicht einsehbar. Bei der Berichterstellung wird dadurch sichergestellt, dass Verarbeitungstätigkeiten nur mit den zum Zeitpunkt der Erstellung der Verarbeitungstätigkeit zugeordneten Datenkategorien und ihren Löschfristen angezeigt werden. Weder Änderungen an den Datenkategorien, noch an den Löschkonzepten können diese Dokumentation beeinflussen. Bei der Bearbeitung der Verarbeitungstätigkeit werden neue Kopien der neusten Versionen der Datenkategorien und ihrer Löschkonzepte erstellt. Dadurch entsteht auch eine neue Version der Verarbeitungstätigkeit, die im Historien-Bericht zwar mit der älteren Version verknüpft ist, ansonsten aber alleinstehend existiert.

7 Evaluation

In diesem Kapitel werden die Anforderungen aus Abschnitt 5.1 aufgegriffen. Mithilfe einer Befragung wird evaluiert, ob die Umsetzung der Funktion „Löschkonzepte dokumentieren“ diese Anforderungen aus Sicht der Befragten erfüllt. Das *Open Datenschutzcenter* ist dafür ausgelegt, dass es von Datenschutzbeauftragten für die Dokumentation der von der DSGVO geforderten Dokumentationen genutzt wird. Deshalb ist die Befragung von Datenschutzbeauftragten bezüglich der aufgestellten Anforderungen eine geeignete Möglichkeit fachmännisches Feedback zu erhalten und so die Implementierung evaluieren zu können. Da im Rahmen dieser Masterarbeit keine Feldstudie durchgeführt werden konnte, wurde exklusiv der Datenschutzbeauftragte der Universität der Bundeswehr München zu der Software befragt. Des Weiteren wurde die Befragung zu der Funktionsimplementierung nach dem gleichen Schema mit den Entwicklern des *Open Datenschutzcenters* durchgeführt. Vor der Befragung wurde den Befragten die neue Funktionalität vorgeführt und erklärt. Anschließend konnten sie die Software selbstständig testen. Danach wurden sie dazu befragt, wie sie die Umsetzung der Anforderungen A1-8 im Hinblick auf die Implementierung der Funktion „Löschkonzepte dokumentieren“ bewerten.
Im Folgenden werden die Anforderungen an die Implementierung der Funktion „Löschkonzepte dokumentieren“ aus Abschnitt 5.1 wiederholt.

Anforderungen

A1: Benutzbarkeit der Software fördern

A2: Intuitive Bedienung der neuen Funktion gewährleisten

A3: Zentrale Verwaltung der Löschkonzepte ermöglichen

A4: Datenkategorien um Datenarten ergänzen

A5: Möglichkeit zur Standardisierung schaffen

A6: Kurze Wege ermöglichen

A7: Kompatibilität mit alten Software-Versionen sicherstellen

A8: Revisionssicherheit für die Berichterstellung

7.1 Prüfung durch Datenschutzbeauftragten

Bei der Befragung des Datenschutzbeauftragten stellte sich heraus, dass er die Open-Source-Software bereits kennt und auch schon selbst mit ihr gearbeitet hat. Laut dem Datenschutzbeauftragten sind Löschvorgänge im Rahmen der DSGVO extrem komplexe Vorgänge in der Praxis. Deshalb ist es wichtig, dass man sich vor der Einführung von praktischen Löschvorgängen Gedanken darüber macht, wie man diese Löschvorgänge in das Datenmanagement integrieren kann. Die Dokumentation von Löschkonzepten ist laut seiner Aussage dafür zwingend notwendig, um Verarbeitungsprozesse zu erfassen und qualitätsorientiert bewerten zu können. Man muss sich mit allen Datenkategorien, die verarbeitet werden, auseinandersetzen, alle Speicherorte zusammentragen, Löschfristen und Verantwortliche festlegen und detaillierte Beschreibungen zu den einzelnen Löschkonzepten anlegen. Damit wird eine theoretische Basis für die Praxis geschaffen. Die Verschriftlichung der theoretischen Löschkonzepte dient folglich als Handwerkzeug zur erfolgreichen Einführung von praktischen Löschvorgängen und ist laut dem Datenschutzbeauftragten heutzutage nahezu unverzichtbar.
Auf die Frage, ob die Implementierung der Funktion „Löschkonzepte dokumentieren“ die Anforderung A1 erfüllt, antwortet der Datenschutzbeauftragte, dass das Beibehalten des Designs, die Struktur des Formulars und die kurzen Erklärungstexte zu den Formularfeldern die Benutzbarkeit fördern. Jedoch betont er auch, dass man überlegen könnte, weitere benutzerdefinierte Formularfelder anzubieten, damit die Nutzer die Dokumentation individueller gestalten können. Zudem fällt ihm auf, dass die meisten Formularfelder in Freitextform auszufüllen sind. Er gibt zu bedenken, dass diese Form der Dokumentation fehleranfällig ist. Einige Dokumentationsfelder in ihrer Eingabe zu beschränken, könnte die Benutzbarkeit im Sinne der Standardisierung weiter fördern.
Bezüglich der Anforderung A2 stellt der Datenschutzbeauftragte fest, dass die Beschriftungen geeignet gewählt wurden. Zudem unterstützen die Erklärungstexte das Verständnis. Die Verlinkung von Datenkategorien mit entsprechenden Löschkonzepten und anschließend mit Verarbeitungstätigkeiten ist mithilfe der Drop-Down-Menüs leicht verständlich umgesetzt. Eine intuitive Bedienung ist seiner Meinung nach gewährleistet.
Dadurch, dass die Dokumentation als eigenständige Funktion auf dem Dashboard dargestellt wird und man durch das Klicken auf den Button „Löschkonzepte“ in eine Übersicht aller vorhandener Löschkonzepte gelangt, findet der Datenschutzbeauftragte, dass die Zentralisierung gelungen ist. Da ein Nutzer aus der Übersicht heraus alle vorhandenen Löschkonzepte verwalten und neue Löschkonzepte anlegen kann, wird zudem die zentrale Verwaltung ermöglicht (A3).
Da die Dokumentation von Datenkategorien auch zu einer eigenständigen Funktion weiterentwickelt wurde, in der nun auch die detaillierteren Datenarten mit dokumentiert werden können, ist die Anforderung A4 aus Sicht des Datenschutzbeauftragten erfüllt.
Hinsichtlich der Standardisierung (A5) fällt dem Datenschutzbeauftragten auf, dass man einem Löschkonzept per Drop-Down-Menü mehrere Datenkategorien

zuordnen kann. Bei der Dokumentation von Verarbeitungstätigkeiten können anschließend alle vorhandenen Datenkategorien mit ihrem entsprechenden Löschkonzepten der Verarbeitung ebenfalls per Drop-Down-Menü zugeordnet werden. Dadurch wird die Möglichkeit einer Standardisierung geschaffen, die dem Nutzer viel Arbeit erspart, da er nicht für jede Verarbeitungstätigkeit eigene Datenkategorien und für jede Datenkategorie ein Löschkonzept erstellen muss.
Der Nutzer muss sich zu Beginn der Dokumentation von Löschkonzepten einmal initial intensiv mit den benötigten Löschkonzepten auseinandersetzen. Der anschließende Wartungsaufwand ist nur minimal, zum Beispiel wenn eine weitere Datenkategorie einem Löschkonzept hinzugefügt werden oder eine Datenkategorie das Löschkonzept wechseln soll. Jedoch fällt dem Datenschutzbeauftragten auf, dass die Dokumentation von Speicherorten in den Löschkonzepten noch nicht standardisiert sind. Er findet es umständlich, dass an dieser Stelle alle Speicherorte in Freitextform eingetragen werden müssen. Hier erkennt er Potenzial zur Verbesserung einer Standardisierung.
Durch die Verlinkung von Datenkategorien mit ihren Löschkonzepten, die Übersicht aller Löschkonzepte mit den wichtigsten Informationen und das Einfügen von Verlinkungen zu den Löschkonzepten als auch Datenkategorien in der Navigationsbar werden dem Nutzer kurze Wege zwischen verschiedenen Ansichten ermöglicht (A6).
Da die Weiterentwicklung zum Zeitpunkt der Befragung noch nicht abschließend in den laufenden Betrieb migriert wurde, konnte der Datenschutzbeauftragte die Erfüllung von Anforderung A7 nicht bewerten.
Nachdem der Datenschutzbeauftragte einige Datenkategorien, Löschkonzepte und Verarbeitungstätigkeiten zu Testzwecken erstellt, verknüpft und bearbeitet sowie anschließend die Berichte von Löschkonzepten und Verarbeitungstätigkeiten generiert hat, konnte er feststellen, dass die Revisionssicherheit für die Berichterstellung gewährleistet ist.
Zusammengefasst ist die Meinung des Datenschutzbeauftragten, dass er alle Anforderungen, mit Ausnahme von A7, als erfüllt ansieht und die Erweiterung selber nutzen würde, da sie absolut sinnvoll und durchdacht ist, auch wenn es noch Verbesserungsmöglichkeiten gibt. Alternativ zu dieser Erweiterung wäre die aktuelle Lösung, dass lediglich die Löschfristen in jeder einzelnen Verarbeitungstätigkeit eingetragen werden müssen und keine Möglichkeit zur zentralen Verwaltung besteht. Dadurch ist die Fehleranfälligkeit viel höher und die Verwaltung komplizierter und unflexibel. Grundsätzlich ist es allerdings durchaus möglich, dass verschiedene Datenkategorien unterschiedliche Löschfristen haben. Im Rahmen der Datenminimierung und gegebenenfalls vorhandenen gesetzlich festgelegten Löschfristen ist es oft nicht notwendig, komplette Datensätze einer Verarbeitungstätigkeit aufzubewahren, sondern nur einzelne Datenkategorien davon. Aus der Sicht des Datenschutzbeauftragten stellt damit die Erweiterung des *Open Datenschutzcenters* um die Möglichkeit zur Erfassung von Löschkonzepten eine wesentliche Verbesserung dar.

7.2 Prüfung durch Entwickler

Da es sich bei dem *Open Datenschutzcenter* um eine Open-Source-Software handelt, welche man über GitHub beziehen kann [odc22], konnten die Änderungen am Quellcode per pull-request an die Entwickler der Software weitergeleitet werden. Anschließend wurde per E-Mail Kontakt zu den Entwicklern aufgenommen, um Feedback zu der Implementierung zu erhalten. In einer Besprechung wurden die Entwickler ebenso wie der Datenschutzbeauftragte dazu befragt, ob die aufgestellten Anforderungen aus Abschnitt 5.1 aus ihrer Sicht durch die Funktionsimplementierung erfüllt wurden.
Bezüglich der Benutzbarkeit der Software fiel die Meinung der Entwickler ähnlich der des Datenschutzbeauftragten aus. Hinsichtlich der oft genutzten Freitextfelder sind sie jedoch der Meinung, dass dem Nutzer dadurch viel Freiheit in der Gestaltung seiner Dokumentationen gegeben wird. Sie finden es wichtig, dass der Nutzer viele Möglichkeiten hat, die Felder individuell auszufüllen und die Dokumentation dadurch seinen Bedürfnissen anpassen kann. Insgesamt sehen sie die Anforderung A1 als erfüllt an.
Da sich das Design und die Struktur der neuen Funktion an bereits bestehende Funktionen anlehnt, sind die Entwickler der Meinung, dass die Nutzer die neue Funktionalität schnell erlernen und intuitiv bedienen können. Deshalb sehen sie auch die Anforderung A2 als erfüllt an.
Dadurch, dass der Nutzer aus der Übersicht aller Löschkonzepte diese weiter verwalten kann und sich auch diese Struktur damit an bereits bestehenden Strukturen orientiert, sind die Entwickler der Meinung, dass eine zentrale Verwaltung der Löschkonzepte gegeben ist. (A3)
Den Entwicklern ist auch aufgefallen, dass auf dem Dashboard ein weiterer Button „Datenkategorien“ hinzugefügt wurde. Die Weiterentwicklung der Funktion „Datenkategorien dokumentieren“ fanden sie interessant und stellten fest, dass die Ausweitung der Datenkategorien um die Datenarten eine geeignete Erweiterung darstellt. Somit ist auch festzustellen, dass die Anforderung A4 erfüllt wurde.
Hinsichtlich der Standardisierung (A5) haben die Entwickler die Umsetzung in Form der Drop-Down-Menüs getestet und stellten fest, dass eine Standardisierung im Hinblick auf die Verknüpfungen von Datenkategorien mit Löschkonzepten, sowie Datenkategorien mit Verarbeitungstätigkeiten geschaffen wurde. Zudem ist den Entwicklern aufgefallen, dass die Löschkonzepte über die Datenkategorien auch mit den Verarbeitungstätigkeiten verknüpft werden, sodass bei den Verarbeitungstätigkeiten die Datenkategorien mit ihren zugeordneten Löschkonzepten angezeigt werden. Auch diese Funktionalität zählen die Entwickler zur Standardisierung.
Im Hinblick auf kurze Wege zwischen den einzelnen Funktionalitäten der Software stellten die Entwickler fest, dass die neue Funktion „Löschkonzepte dokumentieren“ sowie die überarbeitete Funktion „Datenkategorien dokumentieren“ zweckmäßig in die Navigationsstruktur integriert wurden, sodass dem Nutzer kurze Wege zwischen den Funktionalitäten ermöglicht werden (A6).
Nachdem die Entwickler den Quellcode überprüft hatten, fanden einige Bespre-

chungen statt, um Migrationsprobleme mit Softwareversionen im laufenden Betrieb zu lösen. Dadurch konnten die Entwickler die Frage, ob die erweiterte Softwareversion mit alten Versionen kompatibel ist (A7), abschließend als erfüllt anerkennen.
Auf die Frage, ob die Revisionssicherheit für die Berichterstellung sichergestellt wurde, betonten die Entwickler, dass die Revisionssicherheit für sie, insbesondere für die Dokumentation von Verarbeitungstätigkeiten, welches die Kerndokumentation der DSGVO ist, eine wichtige Rolle spielt. Nur dadurch kann gewährleistet werden, dass eine Berichterstellung mit Historie der Versionen einer Verarbeitungstätigkeit möglich ist, ohne dass an einer Version Änderungen durchgeführt werden können, nachdem sie einmal erstellt wurde. In Kombination mit den Löschkonzepten und Datenkategorien, die Teil einer Verarbeitungstätigkeit sind und unabhängig von dieser bearbeitet werden können, stellt diese Revisionssicherheit ein komplexes Problem dar. Es muss auch dafür gesorgt werden, dass die Datenkategorien und Löschkonzepte Revisionssicherheit bieten. Nach Prüfung der Umsetzung durch die Entwickler stellten sie fest, dass auch diese Anforderung (A8) erfüllt wurde.
Zusammengefasst fand die Implementierung der neuen Funktion „Löschkonzepte dokumentieren“ positiven Anklang bei den Entwicklern und nach einigen Besprechungen, in denen die Revisionssicherheit und die Möglichkeit zum Migrieren sichergestellt wurden, wurde der erweiterte Quellcode von den Entwicklern zur Übernahme akzeptiert. Die neue Version der Software wird zunächst als Beta in einer öffentlichen Demo zur Verfügung stehen, damit Nutzer die neue Funktionalität testen können. Durch das Testen mithilfe der Nutzergemeinschaft soll sichergestellt werden, dass keine Fehler bei der Benutzung auftreten. Des Weiteren bietet die Demo den Nutzern die Möglichkeit, Feedback zur neuen Funktionalität und deren Integration in die Dokumentation von Verarbeitungstätigkeiten zu geben. Dadurch können Anpassungen durchgeführt werden, wenn noch Fehler auftreten, die beim Entwickeln nicht ausgelöst werden konnten oder Verbesserungsvorschläge als Feedback eingehen.

7.3 Ergebnis der Befragung

Aus den Befragungen des Datenschutzbeauftragten und den Entwicklern geht hervor, dass alle Anforderungen aus 5.1 hinsichtlich der neu eingeführten Funktion „Löschkonzepte dokumentieren“ erfüllt wurden. Beide Parteien finden insbesondere die zentrale Verwaltung und die Standardisierung gelungen implementiert. Darüber hinaus war den Entwicklern die Möglichkeit zur Migration in die aktuell genutzte Softwareversion und die Revisionssicherheit wichtig. Auch diese beiden Anforderungen wurden geeignet umgesetzt. Dennoch gibt es Verbesserungsvorschläge. Die Anzahl an Freitextfeldern sollte laut dem Datenschutzbeauftragten nach Möglichkeit reduziert werden, um die Fehleranfälligkeit zu minimieren. Um die Dokumentation von Löschkonzepten flexibler zu gestalten, könnten zudem weitere benutzerdefinierte Formularfelder für eine detailliertere Dokumenta-

tion ergänzt werden. Abschließend sollte geprüft werden, ob es eine Möglichkeit gibt, die Speicherorte in der Dokumentation von Löschkonzepten nicht in Freitextform zu dokumentieren, sondern automatisch hinzuzufügen, damit der Nutzer nicht jeden Speicherort separat eintragen muss.

8 Zusammenfassung und Ausblick

In diesem Kapitel werden die Ergebnisse und Erkenntnisse, die aus dieser Arbeit hervorgehen, zusammengefasst. Abschließend wird ein Fazit gezogen und ein Ausblick gegeben, wie sich Software-Produkte für den Bereich „DSGVO-Dokumentationen“, insbesondere das *Open Datenschutzcenter*, weiterentwickeln können.

8.1 Zusammenfassung

Zu Beginn der Arbeit wurden in Kapitel 2 Grundlagen zum Verständnis im Themengebiet der DSGVO erklärt. Dabei wurden unter anderem die Grundsätze zur DSGVO-konformen Verarbeitung personenbezogener Daten betrachtet. Auch wurde herausgestellt, welche Rechenschafts- und Nachweispflichten die DSGVO fordert und welche Anforderungen an diese Dokumentationen gestellt werden. In Kapitel 3 wurde anschließend analysiert, wie die einzelnen Dokumentationen technisch umgesetzt werden können.
Nachdem die technische Umsetzung analysiert wurde, wurde sich in Kapitel 4 mit wissenschaftlichen Arbeiten auseinandergesetzt, die sich auch mit den Anforderungen der DSGVO auseinandergesetzt haben. Unter anderem wurden hier Methoden vorgestellt, mit denen der Nutzer kontrolliert eine Übersicht darüber erarbeiten kann, welche Datenkategorien er an welchen Orten verarbeitet. Erst dadurch wird es dem Nutzer möglich im Anschluss die geforderten Dokumentationen der DSGVO zu erstellen. In zwei weiteren Arbeiten wurde betrachtet, wie Löschkonzepte erstellt und umgesetzt werden können.
Daraufhin wurden in Abschnitt 4.2 vorhandene Datenschutzmanagement-Software-Produkte vorgestellt. Eine kostenpflichtige Software und eine kostenlose Open-Source Alternative wurden anschließend im Hinblick auf die Anforderungen der DSGVO zum Dokumentieren vertieft betrachtet. Bei der kostenpflichtigen Software stellte sich heraus, dass diese sehr umfangreich ist und in der Ausprägung eher für große Unternehmen ausgelegt ist, welche für mehrere Mandanten die Dienstleistung des Datenschutzbeauftragten anbieten. Die kostenlose Open-Source-Software *Open Datenschutzcenter* stellte sich hingegen als Anwendung heraus, die im Wesentlichen für einzelne Datenschutzbeauftragte ausgelegt ist, die einen oder wenige Mandanten unterstützen. Der Funktionsumfang der Software ist nicht so groß, wie bei den kostenpflichtigen Alternativen, jedoch beinhaltet sie alle Funktionen zur Dokumentation, welche die DSGVO direkt verlangt. Eine eigenständige Funktion zum Dokumentieren von Löschkonzepten existiere zum Zeitpunkt der Betrachtung allerdings nicht.

In Kapitel 5 wurde deshalb ein Konzept erstellt, mit dem es möglich werden sollte, Löschkonzepte im *Open Datenschutzcenter* zu dokumentieren. Anhand des Konzeptes wurde ein Design erarbeitet, welches in der späteren Implementierung als Grundlage dienen sollte. Auf Basis des Konzeptes und Designs wurde die Funktion „Löschkonzepte dokumentieren " anschließend in das *Open Datenschutzcenter* implementiert.
In Kapitel 6 wurden erklärt, auf welche Architektur das *Open Datenschutzcenter* aufbaut und welche Klassen dementsprechend implementiert oder modifiziert werden müssen. Anschließend wurden die wichtigsten Klassen, ihre Zusammenhänge und die relevanten Codesegmente aufgegriffen und mit ihren Funktionen erklärt. Nachdem die Funktion erfolgreich implementiert wurde, konnte die Codeerweiterung an die Entwickler des *Open Datenschutzcenters* zur Migration in die genutzte Software übergeben werden. Indem die Software dem Datenschutzbeauftragten der Universität der Bundeswehr München und den Entwicklern des *Open Datenschutzcenters* präsentiert wurden, konnte Feedback zur Umsetzung eingeholt werden.
Anhand des Feedbacks konnte in Kapitel 7 die Implementierung der Funktion „Löschkonzepte dokumentieren“ und deren Integration in den bereits bestehen Dokumentationsprozess evaluiert werden. Der Datenschutzbeauftragte hob die Standardisierung und Zentralisierung der Dokumentation positiv hervor. Wäre die Anwendung in dieser Form schon frei verfügbar, würde er sie nutzen. Dennoch nannte er auch Punkte zur Verbesserung. Zum Beispiel, dass dem Formular noch weitere benutzerdefinierte Formularfelder hinzugefügt werden könnten.
Auch die Entwickler bewerteten, dass alle Anforderungen an die Erweiterung erfüllt wurden. Insbesondere die integrierte Revisionssicherheit bei der Dokumentation von Löschkonzepten und das Beibehalten der Revisionssicherheit bei der Dokumentation von Verarbeitungstätigkeiten war ihnen sehr wichtig. Auch diese Anforderung konnte sichergestellt werden. Des Weiteren fanden die Entwickler, dass die Integration in die bereits bestehende Software, die Standardisierung sowie die Zentralisierung geeignet umgesetzt wurden.

8.2 Fazit

Durch die Erarbeitung der Anforderungen, welche die DSGVO an Dokumentationen durch den Datenschutzbeauftragten stellt, die Analyse der technischen Umsetzung und das Betrachten von verwandten wissenschaftlichen Arbeiten, sowie bereits vorhandenen Softwarelösungen zum Digitalisieren dieser Dokumentationen, wurde eine Grundlage geschaffen, um anschließend ein Konzept zu erstellen. Da bei der Betrachtung der vorhandenen Softwarelösungen eine Möglichkeit zur Funktionserweiterung bei der Open-Source-Software *Open Datenschutzcenter* gefunden wurde, befasste sich das Konzept mit der Integration der Funktion „Löschkonzepte dokumentieren“ in die bestehende Software und die nötigen Anpassungen bei bereits vorhandenen Funktionen. Mithilfe des Konzeptes und des darauf basierenden Designs konnte die Funktion anschließend erfolgreich in das *Open Datenschutzcenter* implementiert werden. Dabei wurden alle Anforderungen aus 5.1 erfüllt.

Mit dieser Konzepterarbeitung und Implementierung in die Open-Source-Software leistet diese Masterarbeit einen Beitrag, der so in keiner anderen wissenschaftlichen Arbeit gefunden werden konnte. Zudem unterstützt sie den Open-Source-Gedanken, dass durch gemeinsame Entwicklung frei verfügbare Programme mit einsehbarem Quellcode der Öffentlichkeit bereitgestellt werden können. Durch die Funktionserweiterung erhält das *Open Datenschutzcenter* ein qualitatives Upgrade.

8.3 Ausblick

Eine Evaluation durch die Nutzer der Software konnte zum aktuellen Zeitpunkt noch nicht durchgeführt werden. Um Feedback zu der Funktionserweiterung zu erhalten, muss der erweiterte Quellcode erst final von den Entwicklern der Software übernommen und integriert werden. Zudem müssen die Nutzer anschließend ihre Software aktualisieren und Migrationen durchführen, bevor sie die neue Softwareversion nutzen können. Da dieser Prozess in der Zuständigkeit der Entwickler und Nutzer liegt, kann im Rahmen dieser Masterarbeit nur wenig Einfluss auf die benötigte Zeit genommen werden. Dennoch wurde mit den Entwicklern vereinbart, dass die neue Version der Software erstmals als Beta in einer Demo präsentiert wird, die offiziell von den Entwicklern angeboten wird. Möglicherweise kann anhand dieser Demo schon frühzeitig Feedback von einzelnen Nutzern gesammelt werden, sodass die Software noch weiter bearbeitet werden kann, falls Fehler auftreten, die bis dato nicht ausgelöst werden konnten oder Vorschläge für Verbesserungen eingehen.
Neben der finalen Einführung des neuen Quellcodes gibt es einige weitere Punkte, die in der Zukunft noch betrachtet werden können. Sowohl bei der Bearbeitung der Software, als auch bei der Betrachtung durch den Datenschutzbeauftragten ist aufgefallen, dass sowohl bei der Dokumentation von Verarbeitungstätigkeiten, als auch von Löschkonzepten, Speicherorte in Freitextform angegeben werden müssen. Die Speicherorte der Verarbeitungstätigkeiten beziehen sich darauf, wo die Datenkategorien, die in dieser Verarbeitung verarbeiten werden, gespeichert werden. Die Speicherorte der Löschkonzepte hingegen beziehen sich darauf, wo die Datenkategorien, welche diesem Löschkonzept angehören, gespeichert sind. Somit konnten die Speicherorte nicht aus den Verarbeitungstätigkeiten übernommen werden, sondern müssen nochmal manuell zentral in den Löschkonzepten dokumentiert werden.
Ein Ansatz, um dieses Problem in der Zukunft zu lösen, ist, dass die Funktion „Speicherorte dokumentieren“ ebenso eigenständig implementiert wird, wie im Rahmen dieser Masterarbeit die Funktion „Datenkategorien dokumentieren“. Anschließend wäre es möglich, den Datenkategorien Speicherorte zuzuordnen, an welchen die Datenkategorien grundsätzlich gespeichert werden. Diese zugeordneten Speicherorte könnten dann automatisch in die Löschkonzepte und Verarbeitungstätigkeiten übernommen werden. Trotzdem sollte dem Nutzer die Möglichkeit gegeben werden, Datenkategorien, welche der Verarbeitung angehören, weitere Speicherorte hinzuzufügen. Diese neu hinzugefügten Speicherorte müssten

dann automatisch mit den Datenkategorien verknüpft werden und auch in den Löschkonzepten hinzugefügt werden, da die betroffenen Datenkategorien fortan auch an einem weiteren neuen Ort gespeichert werden. Bei dieser Umsetzung wird jedoch erneut die Revisionssicherheit eine große Herausforderung sein. Denn bestehende Verarbeitungstätigkeiten und Löschkonzepte dürfen nicht in ihrer bestehenden Version verändert werden. Demnach müssten bei der Aktualisierung der Speicherorte auch die zusammenhängenden Datenkategorien, Löschkonzepte und Verarbeitungstätigkeiten neu versioniert werden. Das wiederum würde einen extremen Anstieg an Datensätzen und damit gestiegenen Bedarf an Speicherplatz bedeuten.
Ein weiterer Punkt, nachdem das *Open Datenschutzcenter* weiterentwickelt werden kann ist, dass viele Formularfelder in Form von Freitexten auszufüllen sind. Dadurch können Regelungen umgangen werden, wie zum Beispiel, dass eine Standard-Löschfrist die gesetzliche Löschfrist nicht über- oder unterschreiten darf, je nachdem welche Grenzen gesetzlich vorgeschrieben sind. Ebenso ist die Fehleranfälligkeit für sachlich oder grammatikalisch falsche Dokumentationen hoch, da der Nutzer nicht in seinen Dokumentationsmöglichkeiten eingeschränkt ist. Einige Freitextfelder in Auswahlfelder oder Freitext mit Überprüfung umzuwandeln, würde dem *Open Datenschutzcenter* noch mehr Qualität bieten.
Abschließend bleibt festzustellen, dass die Funktionsimplementierung im Rahmen dieser Masterarbeit positiv von den Entwicklern des *Open Datenschutzcenters* angenommen wurde. Die finale Integration in den laufenden Betrieb und die Reaktion der Nutzer bleibt jedoch noch abzuwarten. Auch nach dieser Masterarbeit gibt es weitere Ansätze, an denen gearbeitet werden kann, um die Open-Source-Software für die Nutzergemeinschaft zu verbessern. Insgesamt ist diese kostenlose Software jedoch eine Alternative im Vergleich zu den kostenpflichtigen Softwareprodukten. Der Datenschutz in Europa und speziell in Deutschland ist in den letzten Jahren immer wichtiger geworden und für Unternehmen ist es zur Pflicht geworden, die Anforderungen der DSGVO umzusetzen. Dabei kann ein Datenschutzmanagement-Tool hilfreich unterstützen, indem der Nutzer alle nötigen Dokumentationen zentralisiert aufbewahren kann. Anhand dieser Arbeit ist hervorzuheben, dass Datenschutzmanagement-Tools nicht teuer sein müssen. Wenn genügend Interessierte sich zusammenschließen und Softwareprodukte, wie beispielsweise das *Open Datenschutzcenter* weiterentwickeln, können viele Nutzer davon profitieren.

Literaturverzeichnis

[adv22] *2B Advice PrIME – Datenschutz-Software.* https://www.2b-advice.com/de/datenschutz-software, März 2022

[Amt22] Amt für Veröffentlichungen der Europäischen Union: *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).* https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE#d1e1815-1-1, Februar 2022

[Bun22] Bundesministerium der Justiz: *Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU.* https://www.bgbl.de/xaver/bgbl/, Februar 2022

[Dr.22] Dr. Datenschutz: *Dokumentationspflichten unter der DSGVO.* https://www.dr-datenschutz.de/dokumentationspflichten-unter-der-dsgvo/, Februar 2022

[fua22] *Datenschutzmanagement Software – Guardileo.* https://www.intersoft-consulting.de/guardileo/, März 2022

[GKSR21] Gümüs, Can ; Köhler, Wolfgang ; Schultz, Christian ; Rasche, Christoph: *Konzept eines Modells zur ganzheitlichen Datenschutzbetrachtung unter Anwendung von Data Mining.* https://dl.gi.de/bitstream/handle/20.500.12116/37753/K1-5.pdf?sequence=1&isAllowed=y, 2021

[h2i22] *H2 invent – Open Source and Cyber Security Enthusiast.* https://h2-invent.com/, März 2022

[Ham22] Hammer, Volker: *Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten.* https://www.secorvo.de/publikationen/din-leitlinie-loeschkonzept-hammer-schuler-2012.pdf, Februar 2022

[Hun22] Hunzinger, Sven: *Löschkonzepte nach der DSGVO am Beispiel von ERPSystemen*. https://www.degruyter.com/document/doi/10.9785/cr-2018-340608/html, April 2022

[KE22] Knuchel, Christian ; Ebert, Nico: *DSGVO-konformes Löschen*. https://link.springer.com/content/pdf/10.1007/s11623-020-1235-y.pdf, April 2022

[KEF18] Koç, H. ; Eckert, K. ; Flaig, D.: *Datenschutzgrundverordnung (DSGVO): Bewältigung der Herausforderungen mit Unternehmensarchitekturmanagement (EAM)*. https://link.springer.com/content/pdf/10.1365/s40702-018-00449-7.pdf, 2018

[Lan22] Lang, Carsten: *DSGVO – So definieren sich personenbezogene Daten*. https://www.lpsp.de/blog/was-sind-personenbezogene-daten, Februar 2022

[odc22] *Github – Opem Datenschutzcenter*. https://github.com/H2-invent/open-datenschutzcenter, März 2022

[ope22] *Open Datenschutzcenter – Open Source und Enterprise Datenschutzmanagement-System*. https://open-datenschutzcenter.de/, März 2022

[otr22] *otris privacy – Datenschutzmanagement*. https://www.otris.de/produkte/datenschutzmanagement-datenschutzsoftware, März 2022

[pre22] *preeco – Datenschutzmanagement-Software*. https://www.preeco.de/, März 2022

[pro22] *Proliance360 – Software für effizientes Datenschutzmanagement*. https://www.datenschutzexperte.de/lp/datenschutzmanagement-software, März 2022

Versicherung an Eides statt

Hiermit versichere ich, die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, die Zitate ordnungsgemäß gekennzeichnet und keine anderen als die im Literatur-/Schriftenverzeichnis angegebenen Quellen und Hilfsmittel benutzt zu haben.

Ferner habe ich vom Merkblatt über die Verwendung von studentischen Abschlussarbeiten Kenntnis genommen und räume das einfache Nutzungsrecht an meiner Masterarbeit der Universität der Bundeswehr München ein.

München, den 9. Juli 2022

Jan Ole Juister