Muster zur praxisorientierten Umsetzung und konformen Nutzung der DSGVO

Daniel Rösch[1], Thomas Schuster[1], Lukas Waidelich[1] und Sascha Alpers[2], Wasilij Beskorovajnov[2], Roland Gröll[2] und Hoa Tran[2]

Abstract: In der heutigen Wissensgesellschaft ist der Austausch von sensiblen Informationen von essenzieller Bedeutung. Sowohl unternehmensbezogene als auch persönliche Daten werden durch Nachrichten (z.B. E-Mail) oder Freigaben über Cloud-Dienste (z.B. OwnCloud) ausgetauscht. Neben individuellen Interessen unterliegt dieser Datenaustausch gesetzlichen Regularien. Seit Mai 2018 ist die Europäische Datenschutz-Grundverordnung (DSGVO) voll wirksam. Die Regularien und die möglichen Strafen führen derzeit noch in vielen Organisationen zu Unsicherheiten. Dieser Artikel zeigt Möglichkeiten auf, wie die tägliche Arbeit konform zur DSGVO gestaltet werden kann. Hierzu definieren wir Muster, welche die bestehenden Anforderungen der DSGVO in technische Lösungsansätze zur Umsetzung konformer Informationsdienste überführen. Der Artikel geht dabei beispielhaft auf einige DSGVO-Anforderungen ein. Durch die Muster wollen wir die Unsicherheiten reduzieren und die Umsetzung der DSGVO erleichtern. Die beschriebenen Muster können als Referenzkatalog für die Anbieter und Nutzer von Informationsdiensten dienen. Zur Demonstration der praktischen Umsetzung nutzen wir beispielhaft ein Anwendungssystem aus dem Forschungsprojekt Einfaches Digitales Vergessen (EDV).

Keywords: DSGVO, Datenschutz Muster, Handlungsempfehlungen, Muster zu Rechten der betroffenen Person, Muster zu Pflichten des Verantwortlichen, Cloud-Dienste.

1 Einleitung

In den vergangenen Jahren wurden viele Technologien entwickelt, die in besonderem Maß die Erzeugung und Verarbeitung großer Datenvolumina vorantreiben. Eines dieser Trendthemen im Kontext des digitalen Wandels ist Internet of Things (IoT). Durch IoT werden enorme Mengen an Daten erzeugt, die bei der Interaktion analoger und digitaler Welt beinahe kontinuierlich anfallen. Weitere technologisch orientierte Ansätze wie Big Data zielen auf die effiziente Verarbeitung dieser Datenmengen ab. Der technologische Wandel wird inzwischen auch in der Gesellschaft wahrgenommen. Besonders die Auswertung großer Datenmengen und die Analyse persönlicher Verhaltensweisen wird zunehmend kritisch betrachtet. Vor diesem Hintergrund wurde auf europäischer Ebene die neue Europäische Datenschutz-Grundverordnung (DSGVO) beschlossen, welche nach Ablauf einer Übergangsfrist seit dem 25. Mai 2018 zur Anwendung kommt. Die Harmonisierung des Datenschutzes hin zu einem Verbot mit Erlaubnisvorbehalt und die Wir-

[1] Hochschule Pforzheim, Tiefenbronner Straße 65, 75175 Pforzheim,
{daniel.roesch, thomas.schuster, lukas.waidelich}@hs-pforzheim.de
[2] FZI Forschungszentrum Informatik, Haid- und Neu-Straße 10-14, 76131 Karlsruhe, {alpers, beskorovajnov, groell, tran}@fzi.de

doi:10.18420/inf2019_50

kung der DSGVO auf Daten europäischer Bürger bei ausländischen, hier angebotenen Diensten verbessern den Schutz von natürlichen Personen gegenüber den Gefahren der Verarbeitung personenbezogener Daten [Sc18]. Mit dem Artikel wollen wir deutlich machen, dass die DSGVO vielmehr eine Vorgabe ist, die zu einer zeitgemäßen Technologieentwicklung und -nutzung beitragen kann. Dabei sollen auch die Rechte der EU-Bürger hinsichtlich ihrer digitalen Datensouveränität [BMR18] schon bei der ethisch verantwortungsvollen Entwicklung von Technologien berücksichtigt werden. Die technische Herausforderung ist die Erfüllung der DSGVO durch standardisierte Technologien. Dabei muss der Verantwortliche geeignete technische und organisatorische Maßnahmen treffen, um die Rechte der betroffenen Person zu schützen.

Im Kern soll dieses Papier das Verständnis für die Anforderungen der DSGVO im Kontext von technischen Umsetzungen verbessern. Hierfür werden Muster definiert, welche die Anforderungen beschreiben und technische Lösungsstrategien zur konformen Umsetzung liefern. Um die Wiederverwendbarkeit von technischen Lösungsansätzen zu fördern, werden auch Querverbindungen zwischen den Anforderungen aufgezeigt – hierzu werden die Muster entsprechend miteinander verknüpft. Die Muster sind nach einem definierten Schema (Problemstellung, Kontext, Lösungsansatz) aufgebaut, wie dies aus anderen Forschungsgebieten [Al95] und besonders der Softwaretechnik bekannt ist [Fo03; Ga08; HW04]. Die Muster können so als Blaupausen verstanden werden, die Lösungsstrategien für Fragen anbieten, welche in der täglichen Arbeit auftreten können. Der Entwurf der Muster folgt dem konstruktivistischen Paradigma der Designwissenschaft. Neues Wissen wird gewonnen indem Artefakte in Form von Modellen, Methoden oder Systemen beschrieben werden. Im Gegensatz zu empirischen Forschung ist das Ziel nicht unbedingt, die Gültigkeit von Forschungsergebnissen im Hinblick auf ihre Wahrheit zu bewerten, sondern den Nutzen als Werkzeug zur Lösung bestimmter Probleme darzustellen [He04].

Vor dem Hintergrund der beschriebenen Ausgangsituation, soll in diesem Artikel die folgende Fragestellung beantwortet werden: Können aus der DSGVO technische Anforderungen und passende Lösungsansätze in Form von Mustern abgeleitet werden? Aus dieser primären Fragestellung leiten sich folgende untergeordnete Forschungsfragen ab:

Q1. Lassen sich die Anforderungen aus der DSGVO in Mustern zusammenfassen?

Q2. Können auf Basis der identifizierten Muster DSGVO konforme technische Lösungen konzipiert und umgesetzt werden?

2 Grundsätze zur Muster-Entwicklung im Kontext der DSGVO

In der DSGVO werden mehrere Grundsätze für die Verarbeitung von personenbezogenen Daten beschrieben. Diese sind u.a. *Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz und Nachvollziehbarkeit*, *Zweckbindung*, *Datenminimierung*, *Richtigkeit*, *Speicherbegrenzung*, *Integrität und Vertraulichkeit und Rechenschaftspflicht* (Artikel 5).

Manche der Grundsätze lassen sich nicht vollumfänglich durch technische Maßnahmen erfüllen oder die Umsetzung weist einen sehr hohen Aufwand auf. Dazu gehören: *Rechtmäßigkeit nach Treu und Glauben, Zweckbindung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht*. Die Betrachtung dieser Grundsätze muss primär auf anderen Ebenen (bspw. Geschäftsprozesse, Geschäftsmodelle) erfolgen. Erst nach deren Betrachtung können dann technische Konsequenzen abgeleitet werden [APOR18].

In diesem Artikel sollen daher nur die Grundsätze, die mit vertretbarem Aufwand (unmittelbar) durch technische Vorkehrungen umgesetzt werden können, betrachtet werden. Somit können besonders die folgenden DSGVO-Grundsätze hier in Mustern zusammengefasst werden: *Transparenz und Nachvollziehbarkeit, Zweckbindung, Datenminimierung und Speicherbegrenzung*. Durch die Formulierung passender Muster, kann die Forschungsfrage Q1 bereits erfolgreich beantwortet werden. Zur DSGVO sind bisher keine Muster und Lösungen veröffentlicht worden. Lediglich Huth konkludiert in seinem Artikel [Hu17] wie sich die neuen Regularien der DSGVO auf bestehende Unternehmen, deren Prozesse und Systeme auswirken. Der Artikel greift bestehende Lösungen auf, erweitert diese durch Lösungsansätze und leitet daraus generalisierte Musterbeschreibungen ab.

Die Methodik zur Beschreibung der Muster weist stets eine einheitliche Struktur auf. Wir orientieren unser Vorgehen an bekannten Veröffentlichungen zu Mustern aus anderen Bereichen. Um die Muster für unsere Problemstellungen und Lösungen optimal darzustellen zu können, haben wir einige Strukturanpassungen in der Musterbeschreibung vorgenommen. Dementsprechend verstehen wir ein Muster als eine Blaupause, die für eine gegebene Problemstellung (und einen definierten Kontext) einen generalisierten Lösungsansatz (Strategie) bereitstellt. Dieses Paradigma ist in vielen Disziplinen bekannt und wurde zunächst in der Architektur und später in der Software-Entwicklung populär [Al95; Be02; BH04; Bu04; Fo03; Ga08; Wi12]. Häufig werden themenorientiert ganze Kataloge an Mustern beschrieben. Zahlreiche Publikationen beschreiben weitere Ansätze zur Entwicklung von Mustern [Ro06; Sc03; Sc04; SNL05; Wi12]. Im Bereich Security wurden bereits einige Muster identifiziert und beschrieben (siehe auch [BH04; SNL05]). Wie bereits oben erwähnt, sind im Bereich der DSGVO bislang keine Muster vorhanden. Im Forschungsbereich Datenschutz sind insgesamt wenige Musterbeschreibungen vorhanden. [Ro06] beschreibt Datenschutz-Muster in Hinblick auf Online-Transaktionen. [Ah07] definieren Datenschutzmuster und -überlegungen im Bereich der Online- und mobilen Fotoübertragung.

3 Entwicklung und Analyse von Datenschutzmustern

Insgesamt können die entwickelten Muster in drei inhaltliche Schwerpunkte untergliedert werden. Dazu gehören allgemeine Muster (I), Rechte der betroffenen Person (II) und Pflichten der Verantwortlichen (III). Jedes unserer Muster wird in einem separaten Teilkapitel innerhalb dieser Schwerpunkte vorgestellt und mit einer eindeutigen Muster-

bezeichnung identifiziert. Somit ist eine schnelle und gezielte Auffindbarkeit eines Lösungsmusters zu einem von der DSGVO auferlegten Prinzip gegeben. Dabei werden in dieser Veröffentlichung nur besonders relevante Prinzipien adressiert, weitere Prinzipien können und sollten später nach dem gleichen Schema ergänzt werden. Im ersten Abschnitt jedes Musters werden Anforderungen, welche die DSGVO fordert näher beschrieben und auf den Verordnungstext referenziert. Im Absatz *Resultierende Herausforderung* wird die daraus resultierende Problemstellung genauer beleuchtet. Es erfolgt eine klare Identifikation des Problems sowie der betroffenen Komponenten. Im dritten Teil *Technischer Lösungsansatz* werden verschiedene Wege zur Lösung der Problemstellung präsentiert. Bei der Umsetzung muss dann jeweils entschieden werden welcher Lösungsweg für den jeweiligen Kontext am besten umsetzbar ist. Abschließend wird eine Checkliste beschrieben, mit der der Anwender prüfen kann, ob alle DSGVO-Anforderungen erfüllt wurden. In jeder Kategorie werden nachfolgend nur einige, wichtige Muster ausführlich erklärt.

3.1 Allgemeine Muster (I)

Dieses Kapitel beschreibt zentrale Anforderungen aus der DSGVO, die als Muster zusammengefasst sind. Insgesamt wurden in diesem Bereich fünf Muster identifiziert: *Transparenz und Nachvollziehbarkeit (1), Zweckbindung (2), Datenminimierung (3), Richtigkeit (4) und Speicherbegrenzung (5)*. Die folgenden Abschnitte beschreiben die aus unserer Sicht wichtigsten Muster.

Transparenz und Nachvollziehbarkeit (1)

Vorgabe der DSGVO: Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Art. 5 Abs. 1a.

Resultierende Herausforderung: Die Art und Weise sowie alle relevanten Daten, die im Rahmen eines Dienstes in Bezug auf eine Person verarbeitet werden, sind auszuweisen und offenzulegen. Die Offenlegung und Ausweisung sind kontinuierliche Anforderungen an den Dienst. Die Kern-Herausforderung liegt in der Bereitstellung einer Schnittstelle, die der betroffenen Person alle, für die Transparenz und Nachvollziehbarkeit, notwendigen Informationen nach Bedarf offenlegt.

Technischer Lösungsansatz: Drei technische Teilaspekte sind zu beachten, um der Transparenz und Nachvollziehbarkeit nachzukommen.

1. *Übersicht erhebender Daten*: Schon vor der Benutzung des Dienstes muss der Anbieter eine Liste mit allen Daten, die erhoben werden sollen, vorlegen. Hierzu kann der technische Lösungsansatz der *Informationspflicht* verwendet werden.
2. *Offenlegung der gespeicherten Daten:* Hierfür empfiehlt sich die technische Maßnahme, um den Nutzern das Recht auf Auskunft zu ermöglichen.

3. *Offenlegung der Art und Weise der Verarbeitung:* Dieser Teilaspekt stellt eine besondere Herausforderung dar. Idealerweise werden alle relevanten Prozesse für die betroffene Person in transparenter Art und Weise offengelegt. Die Offenlegung von Code kann, zusätzlich zur Datenschutzerklärung, technisch versierten Personen ein tiefergehendes Verständnis der Art und Weise der Verarbeitung ermöglichen. Mindestens jedoch sollte der Anbieter vor der Erhebung der Daten die Leitfragen aus der folgenden Checkliste beantworten.

Checkliste:
- Wird der Verarbeitungsprozess von personenbezogenen Daten erläutert?
- Sind die Fragen aus der Checkliste des Musters *Informationspflicht (6)* beantwortet?
- Ist die potenzielle Datenweitergabe in der Erklärung ausführlich beschrieben?

Zweckbindung (2)

Vorgabe der DSGVO: Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Artikel 5 Abs. 1b.Davon gibt es nur wenige Ausnahmen wie bspw. Weiterverarbeitung für Archivzwecke im öffentlichen Interesse. Art. 89 Abs. 1.

Resultierende Herausforderung: Die Verarbeitungszwecke müssen aus der Datenschutzerklärung eindeutig erkennbar sein. Daten dürfen nur für die Verarbeitungsprozesse zugreifbar sein, die für einen angegebenen Zweck notwendig sind.

Technischer Lösungsansatz: Bereitstellung einer Erklärung, die die Zwecke der Verarbeitung von personenbezogenen Daten beschreibt. Je nach gewählter Art der Datenverarbeitung, können sind zwei Fälle unterschieden werden:

1. *Die Daten werden zentral abgelegt:* Hier empfiehlt sich eine logische Aufteilung von Verarbeitungsprozessen auf Verarbeitungszwecke. Die Ablage der Daten erfolgt zusammen mit dem deklarierten Zweck. Das ermöglicht es Verarbeitungsprozesse und abgelegte Daten zu organisieren, indem der Verarbeitungszweck als Zugriffsrichtlinie (Policy) für Prozesse dient.
2. *Die Daten werden direkt in den einzelnen Verarbeitungsprozessen gespeichert:* Dies ist eine einfache Variante, die Daten zweckgebunden zu speichern. In der Folge jedoch müssen viele Daten redundant gespeichert werden (eine Herausforderung bspw. Bei Auskunfts- und Löschansprüchen). Die Verarbeitungsprozesse müssen dennoch zu Verarbeitungszwecken zugeordnet sein.

Checkliste:
- Sind eindeutige und legitime Verarbeitungszwecke festgelegt?
- Beschreibt die Datenschutzerklärung alle Verarbeitungszwecke?

- Sind Verarbeitungsprozesse auf Verarbeitungszwecke abgebildet?
- Werden gespeicherte Daten explizit mit einem Attribut Zweck versehen oder ausschließlich zweckgebunden in isolierten Verarbeitungsprozessen gespeichert?

Datenminimierung (3)

Vorgabe der DSGVO: Personenbezogene Daten müssen dem Zweck angemessen und auf das für den Verarbeitungszweck notwendige Maß beschränkt sein. Artikel 5 Abs. 1c.

Resultierende Herausforderung: Verringerung der Menge der verarbeiteten Daten und Anzahl der Betroffenen. Des Weiteren ist die Mindestmenge an personenbezogenen Daten zu identifizieren, welche für die Verarbeitungszwecke notwendig sind.

Technischer Lösungsansatz: Bereits in der Entwurfsphase eines Softwaresystems muss das Datenmodell im Hinblick auf den Verarbeitungszweck überprüft und angepasst werden. Auch während des Betriebs können sich Änderungen bezüglich der Notwendigkeit bestimmter Daten und hinsichtlich mancher Zwecke ergeben. Dies erfordert eine Architektur, in der das Datenmodell dynamisch anpassbar ist.

Checkliste:
- Welche Datenstruktur ist gleichzeitig minimal und zweckdienlich, um den gewünschten Dienst zu erbringen?
- Wurden Daten (oder Attribute) die nicht (mehr) für Verarbeitungszwecke notwendig sind gelöscht?

Speicherbegrenzung (5)

Vorgabe der DSGVO: Personenbezogene Daten müssen so gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Verarbeitungszwecke erforderlich ist. Artikel 5 Abs. 1e.

Resultierende Herausforderung: Die Dauer der Speicherung von personenbezogenen Daten muss definiert sein. Mit der Zweckerfüllung sind personenbezogene Daten aus dem System zu entfernen oder die Verbindung zu den personenbezogenen Daten so aufzuheben, dass die Identifizierung der betroffenen Person nicht mehr möglich ist. Letzteres ist in vielen Fällen nur schwer zu erreichen ist, da betroffene Personen oftmals rückwirkend durch noch vorhandene Attribute identifiziert werden können [Sw02].

Technischer Lösungsansatz: Das Datenmodell muss einen Lebenszyklus für die Daten vorsehen. Als Grundlage bieten sich Zeit- und Zweckattribute an. Werden die Daten verschlüsselt ist eine unumkehrbare Löschung des Schlüssels ausreichend, um die Daten nicht-identifizierbar zu machen [BH04]. Andere Anonymisierungsmechanismen, wie

Differential Privacy [Dw08], sind auch möglich, aber in der Praxis nur schwer umzusetzen.

Checkliste:

- Sind die Daten mit einer Speicherdauer versehen, die aufgrund eines bestimmten Zwecks beschränkt ist?
- Falls Anonymisierung gewünscht: Ist der Speichermechanismus für die gespeicherte Art von Daten sinnvoll?
- Sofern die Daten verschlüsselt vorliegen: Kann der Schlüssel unumkehrbar gelöscht werden?

3.2 Rechte der betroffenen Person (II)

Neben allgemeinen Anforderungen aus der DSGVO werden in diesem Abschnitt alle Rechte der betroffenen Person aufgelistet und näher beschrieben, die sich aus der DSGVO ergeben. Dazu gehören die *Informationspflicht (6), das Recht auf Auskunft (7), das Recht auf Berichtigung (8), das Recht auf Löschung (9), das Recht auf Einschränkung der Verarbeitung (10) sowie das Recht auf Datenübertragbarkeit (11).* Analog zum vorhergegangenen Kapitel werden nun die wichtigsten dieser Muster erklärt. Wie im vorherigen Abschnitt werden die wichtigsten Muster veranschaulicht und erläutert.

Informationspflicht (6)

Vorgabe der DSGVO: Zum Zeitpunkt der Erhebung von personenbezogenen Daten müssen sämtliche Informationen über die Datenverarbeitung der betroffenen Person mitgeteilt werden. Artikel 13 Abs. 1, 2.

Resultierende Herausforderung: Gemäß den DSGVO-Vorgaben sind die Informationen verständlich, leicht zugänglich und in einer klaren Sprache in einer Erklärung schriftlich oder elektronisch an die betroffene Person zu übermitteln. Die Kenntnisnahme der Datenschutzerklärung ist eine zwingende Voraussetzung für eine Nutzung des Dienstes. Die Datenschutzerklärung muss außerdem immer (auch nach der Kenntnisnahme) leicht auffindbar sein (durch max. 2 Klicks).

Technischer Lösungsansatz: Die Datenschutzerklärung ist vor der Registrierung des Nutzers in der Anwendung als Text an die betroffene Person auszuweisen. Die anschließende Registrierung darf erst nach der Protokollierung der erfolgreichen Kenntnisnahme der Datenschutzerklärung möglich sein. Während der Nutzung muss die Datenschutzerklärung jederzeit leicht auffindbar sein.

Checkliste:

- Beinhaltet die Benachrichtigung nachfolgende Informationen? Name, Kontaktdaten des Verantwortlichen für die Datenerhebung, ggf. Kontaktdaten des Datenschutzbe-

auftragten, Zwecke der Datenverarbeitung und deren Rechtsgrundlage, Empfänger der personenbezogenen Daten, ggf. Absicht für eine Übermittlung an Drittland, Dauer der Speicherung, Recht auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerruf und Beschwerde bei einer Aufsichtsbehörde.

- Ist die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben?
- Ist Profiling vorhanden? Wenn ja, ist eine Benachrichtigung über die involvierte Logik und Tragweite erfolgt?
- Ist die Datenschutzerklärung leicht verständlich und jederzeit leicht auffindbar?

Recht auf Auskunft (7)

Vorgabe der DSGVO: Die betroffene Person hat gegenüber dem Verantwortlichen ein Recht auf Auskunft auf folgende Informationen: Verarbeitungszwecke, Kategorien der personenbezogenen Daten, Empfänger oder Kategorien von Empfängern (Drittländer, Organisationen), geplante Speicherdauer, Recht auf Berichtigung und Löschung, Beschwerderecht, Herkunft der Daten, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, automatisierte Entscheidungsfindung einschließlich Profiling Artikel 15, Abs.1 geeignete Garantien bei Datenübertragung an ein Drittland Artikel 15, Abs.2 sowie Kopie der personenbezogenen Daten. Artikel 15, Abs. 3.

Resultierende Herausforderung: Betroffene Personen können von einer Auskunftsanfrage Gebrauch machen. Der Verantwortliche muss diese Anfrage schriftlich oder elektronisch beantworten können. Außerdem muss der Verantwortliche alle vertretbaren Mittel nutzen, um die Identität einer Auskunft suchenden betroffenen Person zu überprüfen. Bei begründeten Zweifeln an der Identität kann der Verantwortliche zusätzliche Informationen anfordern. Bei mangelnder Identifizierbarkeit der betroffenen Person kann der Verantwortliche die Auskunft verweigern.

Technischer Lösungsansatz: Um diese Herausforderung technisch zu unterstützen, sind flexible Schnittstellen notwendig, die es ermöglichen bestehende Daten aus dem System abzufragen. Am besten eignen sich bekannte Standardschnittstellen, wie REST, um Daten explizit aus dem System abzufragen. Demzufolge sind Standardabfragen festzulegen, die relevante Informationen (siehe Vorgabe der DSGVO) extrahieren. Die Informationen sind dann mittels Text und ggf. Bilder an den Nutzer auszuweisen. Möchte der Nutzer lediglich bestimmte Auskunftsinformationen erlangen, sind Auswahlfunktionen bereitzustellen. Abhängig von der Auswahl werden dann nur entsprechende Informationen geliefert.

Checkliste:

- Bietet das System eine Auskunftsmöglichkeit über die betroffene Person und die mit ihr verbundenen Daten an?

- Bietet das System eine Identifizierung der Auskunft suchenden betroffenen Person?

Recht auf Löschung (9)

Vorgabe der DSGVO: Ein Nutzer kann die Löschung von personenbezogenen Daten verlangen, sofern sie ihn betreffen. Die Verantwortlichen sind verpflichtet dem nachzukommen, sobald einer der Gründe gemäß Artikel 15 Abs. 1 a-f genannten Gründe vorliegt. Auch der Widerruf einer Einwilligung zählt hierzu. Weiterhin besagt der Artikel 15 Abs. 2, dass das Verlangen nach Löschung nach Möglichkeit an weitere Verantwortliche weiterzuleiten ist. Zudem existieren Ausnahmen, unter denen der Artikel nicht gilt Artikel 15 Abs. 3.

Resultierende Herausforderung: Die DSGVO verlangt eine Funktion zur Löschung von personenbezogenen Daten. Demnach müssen betroffene jederzeit die Möglichkeit besitzen eine Löschung ihrer Daten anordnen zu können. Außerdem ist sicherzustellen, dass eine Weiterleitung der Löschung an weitere Verantwortliche möglich ist.

Technischer Lösungsansatz: Beim Recht auf Löschung ist eine Schnittstelle bereitzustellen, die eine nachträgliche Löschung von personenbezogenen Daten ermöglicht. Daten von einzelnen müssen abfragbar und separat löschbar sein. Eine nachträgliche Reproduzierbarkeit der Daten ist nach der Löschung nicht zulässig.

Checkliste:
- Ermöglicht das System die Löschung von Benutzerdaten und Accounts?
- Können die Daten nach der Löschung wiederhergestellt werden?

3.3 Pflichten des Verantwortlichen (III)

In einem dritten Teilbereich sieht die DSGVO verschiedene Pflichten vor, denen eine verantwortliche Stelle nachkommen muss. Hierzu gehören die *Mitteilungspflicht (12)* und die auf Datenschutz optimierte Voreinstellung *Privacy by Default (13)*. Wir werden in diesem Abschnitt nur das zweite Muster skizzieren.

Privacy by Default (13)

Vorgabe der DSGVO: Durch geeignete technische und organisatorische Maßnahmen soll sichergestellt werden, dass die Voreinstellungen eines Dienstes die Benutzer bei der Erhebung, Verarbeitung, Speicherung und Weitergabe von personenbezogenen Daten nicht bevormundet. Dies wird häufig als Privacy by Default bezeichnet. Artikel 25 Abs. 2.

Resultierende Herausforderung: Die Erhebung, Verarbeitung, Speicherung und Weitergabe muss technisch auf jede relevante Nutzersituation einstellbar sein. Erst dadurch sind je nach Nutzersituation variable datenschutzfreundliche Voreinstellungen möglich.

Technischer Lösungsansatz: Im Kapitel Allgemeine Muster wurde durchgehend die Empfehlung gegeben, Daten mit zusätzlichen Attributen zu versehen. Beispielsweise, beim Muster *Zweckbindung* empfehlen wir zu jedem personenbezogenen Datum ein zusätzliches Attribut Zweck zu speichern. Anhand dessen kann eine attributbasierte Zugriffskontrolle die Zweckbindung technisch garantieren. Beim Muster Speicherbegrenzung empfehlen wir ein Zeitattribut, das die Speicherdauer repräsentiert. Sind die Daten mit solchen Attributen versehen, dann ist es technisch möglich auch datenschutzfreundliche Ausprägungen über diesen Attributen zu definieren. So können Daten standardmäßig zunächst mit dem generischen Attribut Datenablage versehen werden, sodass kein Verarbeitungsprozess auf diese zugreifen kann, da diese erstmal nur zu Ablage gedacht sind. Ähnliches ist auch über das Zeitattribut möglich, das je nach Art des Datums eine Lebensdauer bestimmt, ist diese abgelaufen, kann eine weitere Bearbeitung nicht mehr erfolgen. Das Attribut sollte individuell von der betroffenen Person eingestellt werden können. Die beiden Attribute sind exemplarisch zu verstehen. Der Betreiber eines Dienstes muss die Anforderungen dieses Musters bereits während des Entwurfs des Datenmodells berücksichtigen und passende Attribute mitsamt deren Ausprägungen definieren.

Checkliste:

- Verfügt das System über geeignete Steuerungsattribute, die die Daten kennzeichnen?
- Können Nutzer Einstellungen zur Verarbeitung von personenbezogenen Daten flexibel vornehmen?
- Werden Nutzer durch bestimmte Systemeinstellungen nicht bevormundet?

3.4 Bewertung der Muster

Abgeleitet von der vorhergegangenen Analyse können Abhängigkeiten zwischen den 13 Mustern identifiziert werden (siehe Tab. 1). Das Muster *Transparenz und Nachvollziehbarkeit (1)* weist eine hohe Abhängigkeit auf. Das Muster verfügt über Beziehungen zu den Mustern *Zweckbindung (2), Datenminimierung (3), Richtigkeit (4), Informationspflicht (6), Recht auf Auskunft (7), Recht auf Datenübertragbarkeit (11) und Mitteilungspflicht (12)*. Analog dazu können weitere Abhängigkeiten festgestellt werden. Da diese Muster aus der DSGVO abgeleitet wurden, kann im Umkehrschluss eine hohe Abhängigkeit der einzelnen DSGVO-Artikel untereinander ermittelt werden. Dies bedeutet, dass auch die gemeinschaftliche Umsetzung der einzelnen technischen Maßnahmen zu empfehlen ist.

Schwerpunkt		I					II						III	
	Muster	1	2	3	4	5	6	7	8	9	10	11	12	13
I	1	-	x	x	x		x	x				x	x	
	2	x	-			x	x						x	x
	3	x		-		x								x
	4	x			-				x	x				
	5		x	x		-								x
II	6	x	x				-	x				x	x	
	7	x					x	-	x	x		x	x	
	8				x			x	-	x	x		x	
	9				x			x	x	-	x		x	
	10								x	x	-			
	11	x					x	x				-	x	
III	12	x	x				x	x	x	x		x	-	
	13		x	x		x								-
I = Allgemeine Muster, II = Rechte der betroffenen Person, III = Pflichten der Verantwortlichen														

Tab. 1: Abhängigkeiten zwischen den einzelnen Mustern

Durch die beschriebenen, technischen Lösungsansätze wird eine Teillösung zu Q2 angeboten. Zur Umsetzung der technischen Lösungsansätze, bietet die Checkliste eine problembezogene und zielorientierte Hilfestellung. Mit diesem Wissen kann die Q2 Fragestellung vollständig beantwortet werden.

4 Anwendungsbeispiel anhand des Forschungsprojekts EDV

Die Anwendbarkeit ausgewählter Muster wurde im datenschutzsensiblen Forschungsprojekt Einfaches Digitales Vergessen (EDV) evaluiert. Das EDV Projekt stellt einen Lösungsansatz bereit, der die Grundsätze der DSGVO sowie die Rechten und Pflichten der betroffenen Personen und Verantwortlichen berücksichtigt. Das EDV-System ermöglicht das Austauschen von Dokumenten mittels einer App, wobei gezielt Zugriffsrechte und Zugriffsfristen eingestellt werden können und weder Betreiber des Dienstes

noch der Empfänger der Daten (sofern er sich an das vereinbarte Protokoll hält) die Daten unberechtigt lesen, länger aufbewahren oder Weiterleiten kann. Nachfolgend wird zu den zuvor erstellten Mustern, der EDV Lösungsansatz präsentiert.

Transparenz und Nachvollziehbarkeit (1): Vor der Benutzung des EDV-Systems wird eine Datenschutzerklärung angezeigt. Erfasste personenbezogenen Daten werden aufgelistet und an den Nutzer ausgewiesen. Außerdem werden die verwendeten Technologien sowie die Art und Weise der Verarbeitung beschrieben.

Zweckbindung (2): Das EDV-System gibt Verarbeitungszwecke in der Datenschutzerklärung an. Zu den erfassten Daten werden zusätzlich Verarbeitungszwecke gespeichert. Somit kann die Zweckbindung rückwirkend nachgewiesen werden.

Datenminimierung (3): EDV speichert lediglich Daten ab, die für den Austausch der Dokumente notwendig sind. Das System erlaubt eine Bearbeitung der Attribute. Durch die Nutzung von Docker-Containern können neue Strukturen umgehend eingespielt werden.

Speicherbegrenzung (5): Personenbezogene Daten werden mit einer Bearbeitungs- und Lesefrist im System abgelegt. Mit Ablauf der Frist werden die Informationen und ausgetauschten Dokumente gelöscht und sind somit nicht mehr zugänglich.

Informationspflicht (6): Vor Benutzung der EDV Anwendung wird der Nutzer informiert, wer die Daten verarbeitet und welche Daten verarbeitet und abgespeichert werden. Außerdem wird die betroffene Person bezüglich seiner Rechte informiert.

Recht auf Auskunft (7): Der Nutzer hat die Möglichkeit eine Auskunft seiner Daten zu verlangen. Auf Anfrage erhält der Nutzer alle relevanten Informationen, die ihn betreffen. Der Nutzer kann in der Anwendung einsehen, welche Daten im System abgelegt sind.

Recht auf Löschung (9): Mittels EDV-Systems hat der Nutzer die Kontrolle über seine Dokumente. Demnach kann er bisherige Informationen berichtigen und hochgeladene Dokumente komplett auch vor dem Ende der eingestellten Frist aus dem System entfernen. Dadurch ist auch kein Zugriff der Empfänger auf die Dokumente mehr möglich.

Privacy by Default (13): Das EDV-System bietet von Grund auf benutzerfreundliche Datenschutzeinstellungen. So ist beispielsweise das Benutzerprofil zunächst als privat angelegt und öffentlich nicht sichtbar. Der Nutzer kann in den Einstellungen frei entscheiden ob das Profil auch öffentlich zugänglich sein soll.

5 Zusammenfassung und Ausblick

Die Forschungsfrage Q1 konnten wir durch die Aufstellung von 13 Mustern positiv beantworten. Es ist also möglich problemorientiert und musterbasiert Lösungsansätze zu

technischen Anforderungen, die im Rahmen der DSGVO entstehen, zu erstellen. Diese Ansätze sind auf verschiedene Systeme übertragbar, wir konnten dies exemplarisch durch die Anwendung im EDV Projekt zeigen. Durch den klaren Aufbau der Muster können diese als Leitfaden oder Nachschlagewerk genutzt werden. Die Muster ermöglichen eine anwendungsfallspezifische Entwicklung von Lösungsansätzen auf Basis der DSGVO. Dabei erlauben es die Muster Herausforderungen und technische Lösungsansätze zu erkennen (Q2). Dies wird weiterhin unterstützt, durch den strukturierten Aufbau der Muster und die Einteilung in drei Kategorien: 1) Muster, die sich allgemein aus der DSGVO ableiten lassen; 2) Muster, die den Rechten der betroffenen Person zugeordnet werden können und 3) Muster, die den Pflichten des Verantwortlichen geschuldet sind. Zur vereinfachten Umsetzung dienen die den Mustern zugeordneten Checklisten. Verantwortliche werden dadurch besser in die Lage versetzt, technische Dienste konform zur Gesetzgebung umzusetzen.

Wie bereits zu Beginn des Artikels erwähnt wird die Digitalisierung weiter voranschreiten. Daher wird der Bereich Datenschutz und Datensicherheit eine immer wichtigere Rolle in einnehmen. Wir sehen daher den Bedarf weitere Anforderungen aus der DSGVO explizit zu beschreiben und zusätzliche, musterbasierte Lösungsansätze zu entwickeln. Auch wenn die beschriebenen Checklisten und die Strukturierung bereits in diese Richtung gehen, planen wir bezugnehmend zu Q2 eine vereinfachte Anwendung der Muster zu unterstützen. Dazu planen wir die Entwicklung eines web-basierten, interaktiven Musterkatalogs. Hierzu wollen wir künftig auch einen Fragekatalog entwickeln, der es Unternehmen ermöglicht, DSGVO-basierte Anforderungen automatisch anhand ihrer Anwendungsfälle (Systeme) zu erkennen und Lösungsansätze nach Bedarf abzuleiten. Ein weiteres zukünftiges Forschungsfeld sehen wir in der Identifikation von allgemeinen Datenschutzmustern, die Lösungsstrategien unabhängig von einzelnen Gesetzesvorgaben beschreiben. Hieraus könnte künftig auch ein erweiterter Musterkatalog entstehen, der hierarchisch aufgebaut ist und indem auch nach bestimmten Gesetzen gefiltert werden kann (beispielsweise nach der DSGVO). Neben einer gesetzbasierten Erweiterung des Musterkatalogs erscheint das Themenfeld Privacy by Default besonders zur weiteren Untersuchung geeignet. Als einen der nächsten Schritte planen wir daher diesen Bereich genauer zu untersuchen, um weitere Datenschutzmuster zu identifizieren.

Diese Arbeit entstand im Forschungsprojekt EDV (Förderkennzeichen 01MT17009A), gefördert durch das BMWi in der Förderlinie SmartData.

Literaturverzeichnis

[Ah07] Ahern, S., et. al.: Over-Exposed? Privacy Patterns and Considerations in Online and Mobile Photo Sharing. ACM, New York, S. 357-367, 2007.

[Al95] Alexander, C. et. al.: Eine Muster-Sprache. Städte, Gebäude, Konstruktion. Löcker Verlag, Wien, 1995.

[APOR18] Alpers, S.; Pilipchuk, R.; Oberweis, A.; Reussner, R.: Identifying Needs for a Holistic Modelling Approach to Privacy Aspects in Enterprise Software Systems. ICISSP: S. 74-82, 2018.

[Be02] Berry, C.: 2002. J2EE Design Patterns Applied. Real World Development with Pattern Frameworks, Wrox, Birmingham, 2002.

[BH04] Blakley, B.; Heath, C.: Security Design Patterns. The Open Group, Vereinigtes Königreich, 2004.

[Bu04] Buschmann, F. et. al.: Pattern-Oriented Software Architecture. A System of Patterns, Wiley, Chichester, 2004.

[BMR18] Beyerer, J., Müller-Quade, J. & Reussner, R.: Karlsruher Thesen zur Digitalen Souveränität Europas. Datenschutz Datensicherheit 42:5: S. 277-280, 2018.

[Dw08] Dwork, C.: Differential Privacy: A Survey of Results, Springer, China, 2008.

[Fo03] Fowler, M.: Patterns of Enterprise Application Architecture. Addison-Wesley, Boston, 2003.

[Ga08] Gamma, E. et. al.: Entwurfsmuster. Elemente wiederverwendbarer objektorientierter Software, Addison-Wesley, München, 2008.

[He04] Hevner, A. et. al.: Design Science in Information Systems Research. MIS Quarterly 28:1, S. 75-105, 2004.

[HW04] Hohpe, G.; Woolf, B.: Enterprise Integration Patterns. Designing, Building, and Deploying Messaging Solutions, Addison-Wesley, Boston, 2004.

[Hu17] Huth, D.: A Pattern Catalog for GDPR Compliant Data Protection. In: Proc. 10th Int. Conf. on IFIP of Enterprise Modelling. Leuven, S. 34-40, 2017.

[Ro06] Romanosky, S. et. al.: Privacy Patterns for Online Interactions. In.: Proc. of the 2006 conference on Pattern languages of programs. ACM Press, New York, S.1-15.

[Sc03] Schumacher, M.: Security Patterns and Security Standards. With Selected Security Patterns for Anonymity and Privacy, TU Darmstadt, Darmstadt, 2003.

[Sc04] Schümmer, T.: The Public Privacy. Patterns for Filtering Personal Information in Collaborative Systems, Universität Hagen, Hagen, 2004.

[Sc18] Schild H.: BeckOK Datenschutzrecht, C.H. Beck, München, 2019.

[SNL05] Steel, C.; Nagappan, R.; Lai, R.: Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management, Prentice Hall, Saddle River, 2005.

[Sw02] Sweeney, L.: k-Annonymity: A Model for Protecting Privacy, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002.

[Wi12] Wilder, B.: Cloud Architecture Patterns. Develop Cloud-Native Applications, O'Reilly, Peking, 2012.