Thema:

Auswirkungen der Europäischen Datenschutzgrundverordnung auf das IT-Projektmanagement am Fallbeispiel eines IT-Dienstleisters

Bachelorarbeit

Arbeitsgruppe Managementinformationssysteme

Themensteller: Prof. Dr. Hans-Knud Arndt

Vorgelegt von: David Morva

Abgabetermin: 20. Juli 2020

Kurzfassung

Die Europäische Datenschutzgrundverordnung (DSGVO) beeinflusst seit ihrer Einführung im Mai 2018 die Unternehmenslandschaft in Europa nachhaltig. Während auf der Ebene der Gesamt-Unternehmen bereits einige wissenschaftliche Vorschläge zur Umsetzung der DSGVO existieren, gibt es noch wenig Forschung in Bezug auf die Auswirkungen der DSGVO auf das IT-Projektmanagement, insbesondere im Softwareentwicklungskontext. Die vorliegende Arbeit untersucht deshalb, welche Anforderungen aus der DSGVO sich für die Softwareentwicklung ergeben. Diese Anforderungen werden dann in einem IT-Artefakt gemäß der konstruktionsorientierten Forschung in der Wirtschaftsinformatik gebündelt. Der daraus resultierende Anforderungskatalog wird im Rahmen einer Fallstudie in einem existierendes Softwareentwicklungsprojekt validiert, um seine praktische Nutzbarkeit zu untersuchen und DSGVO-konforme Software herzustellen.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Bachelorarbeit selbstständig und ohne unerlaubte Hilfe angefertigt, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch nicht veröffentlicht.

Magdeburg, den 14. Juli 2020 David Morva

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Hintergrund

Die Europäische Datenschutzgrundverordnung (im weiteren Verlauf DSGVO genannt) ist seit Mai 2018 in Kraft und stellt die datenschutzrechtlichen Vorkehrungen von Unternehmen auf die Probe. Mit ihrer Einführung hat die Europäische Union insbesondere das Ungleichgewicht datenschutzrechtlicher Bestimmungen zwischen den EU-Mitgliedsstaaten ins Visier genommen.[1] Bei Nichteinhaltung der neuen Rechtslage drohen Unternehmen Bußgelder von bis zu vier Prozent ihres weltweit erzielten Jahresumsatzes und beteiligten natürlichen Personen Sanktionen von bis zu 20 Millionen Euro.[2] Das sorgt einerseits für Unsicherheit in deutschen Unternehmen, andererseits für Herausforderungen. Mit der Deutsche Wohnen SE gab es bereits ein Unternehmen in Deutschland, dass für Schlagzeilen sorgte, weil es mit einem Bußgeld von 14,5 Millionen Euro belegt wurde. Als Grund dafür gab die Berliner Datenschutzbehörde an, dass das Archivsystem der Deutsche Wohnen SE gegen die Grundsätze der Datenschutzverarbeitung (Artikel 5 DSGVO) und Datenschutz durch Technikgestaltung (Artikel 25 DSGVO), bekannt unter *privacy-by-design*, verstoßen würde.[3] Dies rückt den Terminus *privacy-by-design* im Umgang mit Software in den Fokus der Forschung.

In der DSGVO selbst wird unter Erwägungsgrundsatz 78 beschrieben, was sich hinter dem Begriff im juristischen Sinne verbirgt. „[…] sollen die Hersteller der Produkte, Dienstleistungen und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienstleistungen und Anwendungen zu berücksichtigen […]“.[4] Die DSGVO sieht also bewusst schon in der Entstehung von Software die Notwendigkeit, Datenschutz zu implementieren. Die TOP 3 Herausforderungen bei der Umsetzung der DSGVO sind nach Umfragen in Unternehmen jedoch eine vorherrschende Rechtsunsicherheit, ein schwer abzuschätzender Umsetzungsaufwand und mangelnde praktische Umsetzungshilfen.[5] Unternehmen wünschen sich demnach Hilfe, damit sie die Anforderungen der DSGVO im Unternehmen implementieren können.

Bereits bestehende Forschung hat betreffende Aspekte schon angefangen zu untersuchen. So gibt es mittlerweile vielfach Literatur, die die einzelnen Artikel der DSGVO näher erklären und in den Kontext eines gesamten Unternehmens einordnen, um Rechtssicherheit zu schaffen. Vereinzelt wurden im

[1] Vgl. ErwGr. 9 DSGVO
[2] Vgl. Art. 83 Abs. 5 DSGVO
[3] Vgl. Dachwitz, Ingo: Deutsche Wohnen kassiert erste Millionenstrafe [Update], in: netzpolitik.org, 2019, [online] https://netzpolitik.org/2019/datenschutzgrundverordnung-deutsche-wohnen-erste-millionenstrafe/ [06.07.2020]
[4] Vgl. ErwGr. 78 DSGVO
[5] Vgl. Dehmel, Susanne / Thiel, Barbara: Vier Monate DS-GVO – wie weit ist die die deutsche Wirtschaft?, in: Bitkom Research, 2018, S. 4

Bereich der Softwareentwicklung schon Anforderungen aus der DSGVO abgeleitet, die notwendig sind, um den Grundsatz des *privacy-by-design* in der Softwareentwicklung implementieren zu können.

1.2 Problemstellung und Zielsetzung

Diese Forschungsarbeit nähert sich den Herausforderungen bei der Umsetzung der DSGVO über den Aspekt der praktischen Hilfe. Wie von befragten Unternehmen angegeben, werden diese Vielfach vermisst. Explizit soll eine praktische Hilfe für den Bereich der Softwareentwicklung gegeben werden, damit diese schon bei der Erstellung von Software die Anforderungen der DSGVO implementieren können. Die zentrale Forschungsfrage lautet demnach: „Wie lassen sich die Anforderungen der DSGVO in der Softwareentwicklung implementieren?“

Die Fragestellung gliedert sich in zwei Teilbereiche auf. Um Anforderungen implementieren zu können, müssen sie vorher erhoben werden. Die Anforderungen müssen dabei ein möglichst breites Spektrum an Softwareentwicklern betreffen, um für die Praxis relevant zu sein. Das Verfahren zur Anforderungserhebung wird durch diese Einschränkung der Problemstellung eingeschränkt. Die Anforderungserhebung selbst ist der erste Teil der Forschungsarbeit. Der zweite Teil der Forschungsfrage befasst sich mit der Implementierung der vorher erhobenen Anforderungen. Dies kann im Kontext der Wirtschaftsinformatik durch die Schaffung eines IT-Artefakts geschehen. Das IT-Artefakt muss Anforderungen derart genau wiedergeben, dass damit reale Probleme der Softwareentwicklung bedient werden können. Auf der anderen Seite muss es so allgemein formuliert sein, dass die Anforderungen sich in die jeweilige projektspezifische Umgebung übertragen lassen können.

Ziel ist es deshalb einen Anforderungskatalog als IT-Artefakt zu schaffen, der genau diese Aspekte erfüllt und sich im Rahmen einer durchgeführten Fallstudie als wirksam erweist, um die Softwareentwicklung bei der Herstellung DSGVO-konformer Software zu unterstützen.

1.3 Aufbau der Arbeit

Für die Erschaffung des Katalogs ist zunächst die Auseinandersetzung mit thematischen Grundlagen erforderlich. Dafür findet in Kapitel 2 eine Betrachtung der für die Arbeit relevanten Passagen der DSGVO statt. Erläuterungen helfen dabei, sich dem Gesetzestext auch ohne juristisches Vorwissen nähern zu können. Kapitel 3 befasst sich dann mit dem IT-Projektmanagement und seinen Vorgehensweisen. Eine kurze Auseinandersetzung ist in diesem Zusammenhang notwendig, da in der Fallstudie ein spezifisches Projekt betrachtet wird, das unterschiedliche Methoden bei der Erstellung von Software nutzt. Das IT-Artefakt soll diesen Methoden nicht entgegenstehen und sie im besten Fall unterstützen. Kapitel 4 zeigt den methodischen Ansatz der Forschungsarbeit auf. Da am Ende ein IT-Artefakt erschaffen wird, werden zunächst Hintergründe des konstruktionsorientierten Forschungsansatzes

erklärt und daran das eigene Vorgehen ausgerichtet. In Kapitel 5 findet dann eine Literaturanalyse statt, um Anforderungen aus der DSGVO zu identifizieren, die eine Auswirkung auf die Softwareentwicklung haben. Die exzerpierten Anforderungen werden in Kapitel 6 in einem Anforderungskatalog gesammelt. Auf einen solchen ist die Wahl als IT-Artefakt gefallen. Eine Struktur und Gliederung werden in diesem Zusammenhang festgelegt. Um das theoretische Konstrukt Anforderungskatalog für seine Praxistauglichkeit bewerten zu können, wird der entstandene Katalog in Kapitel 7 in eine Fallstudie eingebettet. Im Zuge dieser wurden Interviews mit Experten durchgeführt, die Teil eines Softwareprojektes bei einem IT-Dienstleister sind und den Anforderungskatalog durch ihre Erfahrung validieren. Kapitel 8 fasst schlussendlich die Erkenntnisse der Forschungsarbeit zusammen und gibt einen Ausblick auf die weitere Forschung.

2 Datenschutzgrundverordnung

Im nachfolgenden Kapitel soll die Europäische Datenschutzgrundverordnung, kurz DSGVO, näher beleuchtet werden. Im ersten Schritt werden die Hinter- und Entstehungsgründe genannt, um das Ziel der Einführung einer gemeinsamen Verordnung innerhalb der EU zu verstehen. Daraufhin folgt die Auseinandersetzung mit wichtigen Begriffen der DSGVO, die zum weiteren Verständnis der Theorie notwendig sind. Sodann werden die wichtigsten Änderungen, im Vergleich zu vorherigem Recht, herausgegriffen und erläutert.

Die wissenschaftliche Arbeit fokussiert sich auf die unternehmerische Sicht im Umgang mit der DSGVO, insbesondere im Kontext des Projektmanagements. Es ist daher nicht der Anspruch eine juristisch vollständige Auseinandersetzung zu betreiben, sondern für die weitere Bearbeitung der Forschungsfrage notwendige Grundlagen zu schaffen. Inhalte können daher verkürzt dargestellt sein oder fehlen, wenn sie für den weiteren Verlauf undienlich sind.

2.1 Hintergründe

Die Ansätze der Europäischen Gemeinschaft zur Verallgemeinerung und Standardisierung des Umganges mit personenbezogenen Daten gehen bis in das Jahr 1995 zurück. Mit der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 war das Ziel verbunden, den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr zu gewährleisten. [6] Auch wenn damit eine gesamtheitliche Lösung suggeriert wird, sieht die Richtlinie eine einzelstaatliche Umsetzung vor.[7] Die Gefahr: Geltendes Recht in einem Land ist rechtswidrig in einem anderen Land. Exemplarisch für organisatorische Schwierigkeiten bei der Umsetzung stehen die Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland aus zeitlichen oder inhaltlichen Gründen bei der Integration in das Bundesdatenschutzgesetz (BDSG).[8]

Mit der Verabschiedung der Datenschutzgrundverordnung (DSGVO) im Jahr 2016 und dem Inkrafttreten am 25. Mai 2018 sollen nun eine tatsächliche Vereinheitlichung gewährleistet und Wettbewerbsnachteile beseitigt sein.[9] Die Europäische Union bietet ihren Mitgliedsstaaten damit grundsätzlich

[6] Vgl. Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995)
[7] Vgl. Richtlinie 95/46/EG, Kapitel 1 und 2
[8] Vgl. Datenschutz.org: EU-Datenschutzrichtlinie (Richtlinie 95/46/EG) – Alte Rechtsgrundlage (24.05.2018), [online] https://www.datenschutz.org/eu-datenschutzrichtlinie [09.03.2020]
[9] Vgl. Jaspers, Andreas: Die EU-Datenschutz-Grundverordnung, in: Datenschutz und Datensicherheit, Band 36, Berlin: Deutschland, 2012, S. 571 - 575

keine Regelungsmöglichkeiten mehr, wohl aber Öffnungsklauseln für ergänzende nationale Regelungen.[10] Hinzukommend wird der räumliche Anwendungsbereich der DSGVO explizit geklärt.

In Deutschland findet die DSGVO im neuen Bundesdatenschutzgesetz vom 30. Juni 2017 Anwendung und enthält sowohl gemeinsame Bestimmungen als auch vorher genannte Verfeinerungen.[11]

Die DSGVO selbst besteht aus elf Kapiteln mit insgesamt 99 Artikeln. In diesen werden sowohl allgemeine Bestimmungen und Grundsätze als auch ein expliziter Umgang mit personenbezogenen Daten bestimmt. Dazu kommen 173 Erwägungsgründe, die erklären, warum die Artikel der DSGVO erlassen wurden.

2.2 Begriffe

Zentraler Gegenstand und Ziel der DSGVO ist der Schutz *personenbezogener Daten* von *Betroffenen*, das heißt Personen, deren Daten verarbeitet werden. In diesem Zusammenhang gilt es zu klären, was im Anwendungskontext *personenbezogen* bedeutet und was *Daten* sind. Nach Laudon et al. sind Rohdaten, die nicht strukturiert oder menschlich verständlich oder verwendbar sind, Daten.[12] Damit Daten für den Menschen verständlich sind, ist ein Kontext oder logisches Konzept nötig. Dieser Kontext wird durch den Personenbezug geliefert. Im juristischen Sinne handelt es sich demnach bei personenbezogenen Daten um „Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.“[13] Personenbezogene Daten liegen also schon dann vor, wenn einer natürlichen Person physische, soziale oder andere Charakteristika direkt oder indirekt zugeordnet werden können.[14] Beispiele hierfür sind Namen, Online-Kennungen oder Mail-Adressen. Berücksichtigt wird durch die DSGVO außerdem die Einfachheit der Identifizierung einer Person. Erwägungsgrundsatz 26 DSGVO sieht dazu eine Einzelfallbetrachtung vor. Alle objektiven Faktoren werden in eine Beurteilung einbezogen, die klären soll, ob die Identifizierung einer Person wahrscheinlich ist. Nach Voigt und von dem Bussche umfassen diese objektiven Faktoren insbesondere den zeitlichen und monetären Aufwand, die zum Verarbeitungszeitpunkt verfügbare Technologie und den Zweck der Verarbeitung.[15] Für ein Unternehmen ist es daher unumgänglich, personenbezogene Daten möglichst schwer zugänglich zu machen.

[10] Vgl. Voigt, Paul / von dem Bussche, Axel: EU-Datenschutz-Grundverordnung (DSGVO), Berlin: Springer, 2018, S. 3
[11] Vgl. Bundesdatenschutzgesetz
[12] Laudon, Kenneth / Laudon, Jane / Schoder, Detlef: Wirtschaftsinformatik – eine Einführung, 3. Aufl., Hallbergmoos: Pearson Deutschland GmbH, 2016, S. 15
[13] Paal, Boris / Pauly, Daniel / Ernst, Stefan: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl., München: C.H.Beck, 2018, Art. 4 Rn. 1
[14] Voigt / von dem Bussche, 2018, S. 13
[15] Voigt / von dem Bussche, 2018, S. 15

Bei allen weiteren Ausführungen ist es wichtig zu definieren, wer für die Umsetzung der DSGVO überhaupt zuständig ist. Die DSGVO verwendet in diesem Zusammenhang den Begriff des *Verantwortlichen*. Dieser kann eine natürliche oder juristische Person, Behörde oder Einrichtung sein, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.[16] In der Praxis bedeutet das, dass beispielsweise die Geschäftsführung eines Unternehmens die Verantwortung für die Verarbeitung personenbezogener Daten im Unternehmen inne hat. In der Definition des Verantwortlichen stechen vor allem zwei Dinge heraus: Erstens die Möglichkeit einer gemeinsamen Verantwortung und zweitens die Zwecke und Mittel der Verarbeitung. Der erste Punkt ist im Kontext von Wertschöpfungsketten zu sehen. Bei Verflechtungen von Lieferanten werden durchaus die gleichen personenbezogenen Daten in unterschiedlichen Unternehmen verarbeitet. In diesem Fall ist eine gemeinsame Verantwortung durch die DSGVO vorgesehen.[17] Der zweite Punkt, Zweck und Mittel, ist bei jeglicher Verarbeitung personenbezogener Daten immer wieder zu reflektieren und zu begründen. Eine detaillierte Betrachtung findet in Kapitel 2.3 statt. Konkrete Maßnahmen im Zusammenhang mit der DSGVO kann der Verantwortliche einer geeigneten Person überlassen. Als solche bietet sich der *Datenschutzbeauftragte* im Unternehmen an. In Deutschland ist nach dem Bundesdatenschutzgesetz die Benennung eines Datenschutzbeauftragten Pflicht, sobald mehr als zehn Personen regelmäßig automatisiert personenbezogene Daten verarbeiten.[18] Dies kann praktisch schon im Zusammenhang mit Personalverwaltung im Unternehmen vorliegen.

Neben dem Verantwortlichen weist die DSGVO einer weiteren Gruppe besondere Pflichten zu: den *Auftragsverarbeitern*. Diese unterscheiden sich von den Verantwortlichen darin, dass sie personenbezogene Daten im Auftrag von Verantwortlichen verarbeiten. Die Verarbeitung geschieht nur für Zwecke des Verantwortlichen. Auftragsverarbeiter sind daher eigenständig und unabhängig vom Verantwortlichen.[19] Beispiele in dieser Rolle sind Cloud Computing-Anbieter und externe Rechenzentren.[20]

Der letzte zu klärende Begriff ist der des *räumlichen Anwendungsbereiches*. Die DSGVO steckt damit den örtlichen Rahmen ihrer Verordnung, respektive wer davon betroffen ist und wer nicht. Grundsätzlich sind alle Verarbeitungen personenbezogener Daten innerhalb der EU der DSGVO unterworfen. Erstmalig sieht das Recht hier jedoch auch einen Einbezug von Niederlassungen vor, die sich innerhalb der EU befinden, deren Verarbeitungstätigkeiten aber außerhalb der EU stattfinden.[21] Mediale Aufmerksamkeit erreichte zum Beispiel die Datenschutz-Klage französischer Aktivisten gegen Google auf Basis der DSGVO. Darin wurde Google vorgeworfen ihre Nutzer nicht ausreichend über Verarbeitungen

[16] Vgl. Art. 4 Nr. 7 DSGVO
[17] Vgl. Art. 26 DSGVO
[18] Vgl. §38 Abs. 1 Satz 1 BDSG
[19] Vgl. Art. 4 Nr. 8 DSGVO
[20] Vgl. Voigt / von dem Bussche, 2018, S. 24
[21] Vgl. Art. 3 Nr. 1 DSGVO

aufgeklärt zu haben und insbesondere Zweck und Aufbewahrungsfristen nicht offen zu kommunizieren.[22]

2.3 Grundsätze der Datenverarbeitung

Die DSGVO stellt den Schutz personenbezogener Daten auf ein Fundament von Grundsätzen, die für jeden Datenverarbeitungsvorgang Anwendung finden. Mittels dieser Grundsätze, für deren Umsetzung der Verantwortliche zuständig ist, soll eine transparente und einheitliche Verarbeitung von personenbezogenen Daten gewährleistet sein. Viele weitere Rechte und Pflichten innerhalb der DSGVO sind direkte Umsetzungen der Verarbeitungsgrundsätze. In Tabelle 1 sind die Grundsätze aufgeführt, die auf Verlangen nachzuweisen sind und bei Nicht-Befolgen empfindliche Geldstrafen nach sich ziehen können.[23]

Tabelle 1: Grundsätze der Datenverarbeitung[24]	
Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	Personenbezogene Daten müssen auf rechtmäßige Art und Weise, nach Treue und Glauben und in einer für die Person nachvollziehbaren Weise verarbeitet werden. Alle personenbezogenen Daten sind daher leicht zugänglich, klar verständlich und in einfacher Sprache. Der Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung. Betroffene Personen haben ein Recht auf Auskunft.
Zweckbindung	Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.
Datenminimierung	Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Technische und organisatorische Maßnahmen sollen die Einhaltung dieses Verarbeitungsgrundsatzes sicherstellen.[25]

[22] Vgl. Rebiger, Simon / Dachwitz Ingo: Die DSGVO zeigt erste Zähne: 50-Millionen-Strafe gegen Google verhängt, in: Datenschutz – 27 Ergänzungen, 2019, [online] https://netzpolitik.org/2019/die-dsgvo-zeigt-erste-zaehne-50-millionen-strafe-gegen-google-verhaengt [09.04.2020]
[23] Vgl. Art. 83 Abs. 5 DSGVO
[24] Mühlbauer, Holger: EU-Datenschutzgrundverordnung (DSGVO) Praxiswissen für die Umsetzung im Unternehmen - Schnellübersichten, 2. Auflage, Berlin: Beuth, 2018, S. 8-9
[25] Vgl. Voigt / von dem Bussche, 2018. S. 117

Richtigkeit	Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neusten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit unrichtige Daten unverzüglich gelöscht oder berichtigt werden.
Speicherbegrenzung	Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.
Integrität und Vertraulichkeit	Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

In Artikel 6 DSGVO ist eine Verfeinerung des Grundsatzes der Rechtmäßigkeit zu finden. Die genannten Bedingungen spielen insbesondere bei der Bewertung der Rechtmäßigkeit im Projektumfeld eine Rolle und sollen daher explizit noch einmal beschrieben werden. Demnach ist eine Verarbeitung rechtmäßig, wenn:

a) Die betroffene Person eine Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat, oder
b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen, oder
c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt.[26]

2.4 Betroffenenrechte

Als eine Möglichkeit der Einflussnahme auf die personenbezogene Datenverarbeitung wurden Rechte festgesetzt, mit deren Hilfe Betroffene sich über erhobene Daten informieren, Vorgänge beschränken oder gar sämtliche eigene Daten löschen lassen können. Insofern ist hier eine direkte Umsetzung der Grundsätze Transparenz und Zweckbindung zu sehen. Dies stellt insbesondere die Verantwortlichen in

[26] Vgl. Art. 6 Abs. 1 a - c DSGVO

die Pflicht, geeignete organisatorische Rahmen zu schaffen, um die Anforderungen an die Rechte erfüllen zu können.[27] Der erste Teil der Betroffenenrechte besteht aus Informations- und Auskunftsrechten, während der zweite Teil aus *Eingriffsrechten* besteht. Abbildung 1 zeigt die wichtigsten Betroffenenrechte, die anschließend kurz erläutert und mit Beispielen unterlegt werden sollen.

Abbildung 1: Betroffenenrechte[28]

Informations- und Auskunftsrechte sind für alle weiteren Maßnahmen wichtig. Wenn betroffene Personen darüber informiert sind, ob und wie weit Daten von ihnen erhoben oder verarbeitet werden, können sie von ihren Eingriffsrechten Gebrauch machen. Verantwortliche sind daher verpflichtet, grundsätzliche Angaben wie Verantwortlichkeiten, Zweck und Dauer der Speicherung von Daten, sowie Rechte des Betroffenen schon bei der Erhebung in geeigneter Weise mitzuteilen.[29] Ein Praxisbeispiel sind Datenschutzrichtlinien in Unternehmen, die Betroffenen zugänglich gemacht werden, sobald sie ihre Daten im Zuge eines Bewerbungsprozesses angeben. Durch das Auskunftsrecht hat ein Betroffener allerdings auch nach der Erhebung jederzeit die Möglichkeit durch einen Verantwortlichen darüber Auskunft zu erhalten, welche personenbezogenen Daten zu welchem Zweck verarbeitet werden.[30]

Auf Basis der gewonnenen Informationen ergeben sich vor allem drei Eingriffsrechte: das Recht auf Berichtigung, das Recht auf Löschung und das Recht auf Einschränkung der Verarbeitung. In allen Fällen muss der Betroffene sich aktiv an den Verantwortlichen wenden. In der Folge hat dieser die Umsetzung des Verlangens unverzüglich umzusetzen. Durch das Recht auf Berichtigung ist der Verantwortliche verpflichtet, falsche personenbezogene Daten unverzüglich zu korrigieren. Bei dem Recht

[27] Vgl. Art. 12 DSGVO
[28] Verdat24 Team: Betroffenenrechte Teil 1 – Das Recht auf Berichtigung, in: verdat24, 2020, [online] https://www.verdat24.de/betroffenenrechte-teil-1-das-recht-auf-berichtigung/ [12.07.2020]
[29] Vgl. Art. 13 DSGVO
[30] Vgl. Art. 15 DSGVO

auf Löschung spricht man auch von einem *Vergessenwerden*, weil alle personenbezogenen Daten eines Betroffenen gelöscht werden. Um beim vorherigen Beispiel zu bleiben, könnte hier eine Löschung aller personenbezogenen Daten stattfinden, die im Zuge des Bewerbungsprozesses verarbeitet wurden, sobald der Prozess abgeschlossen ist. Die Einschränkung der Verarbeitung spielt insbesondere dann eine Rolle, wenn die Verarbeitung eingeschränkt werden soll, die bisherigen erhobenen Daten jedoch für die Geltendmachung von Rechtsansprüchen benötigt werden.[31] Abseits dieser drei Rechte besteht ein generelles Widerspruchsrecht, mit dem ein Betroffener jederzeit die Einwilligung zur Verarbeitung personenbezogener Daten zurücknehmen kann.[32]

Mit dem Recht auf Datenübertragbarkeit ist ein letztes Betroffenenrecht zugesprochen. Durch dieses Recht soll ein „Umzug" von einem Verantwortlichen zu einem anderen möglich sein. Denkbar ist eine Anwendung bei Versetzung von Betroffenen eines Unternehmensteils zu einem anderen.

2.5 Rechenschaftspflicht und Zusammenarbeit mit den Behörden

Explizit in der DSGVO ist eine Rechenschaftspflicht für den Verantwortlichen festgehalten. In Artikel 5 Absatz 2 DSGVO steht dazu: „[…] und muss dessen Einhaltung nachweisen können."[33] Das bedeutet für Verantwortliche, dass sie stets in der Lage sein müssen die Einhaltung der Grundsätze der Datenverarbeitung belegen zu können.[34] Auch hierbei helfen geeignete organisatorische Maßnahmen im Sinne der DSGVO. Auf zwei obligatorische Methoden soll hier näher eingegangen werden:

1. Verzeichnisse über Verarbeitungstätigkeiten: Eine verpflichtende Form des Nachweises sind die Verzeichnisse über Verarbeitungstätigkeiten. Artikel 30 DSGVO enthält hierzu den Verpflichtungstext für Verantwortliche und Auftragsverarbeiter, sowie die notwendigen Angaben. Wie üblich in der DSGVO sind hier vor allem der Zweck und die Dauer der Verarbeitung und erstmals eine Folgenabschätzung zu nennen.[35] Die Datenschutz-Folgenabschätzung kommt insbesondere dann zum Tragen, wenn neue Verarbeitungen (ggf. unter dem Einsatz neuer Technologien) durchgeführt werden sollen. Hierzu werden „die spezifische Eintrittswahrscheinlichkeit und die Schwere dieses hohen Risikos unter Berücksichtigung der Art des Umfangs, der Umstände und der Zwecke der Verarbeitung und der Ursachen des Risikos" bewertet. Gleichsam sollen geeignete Gegenmaßnahmen festgehalten werden.[36]
2. Datenschutz-Managementsystem: Ein Datenschutz-Managementsystem (kurz: DSMS) soll den Grundsatz der Transparenz erfüllen, indem es den datenschutzrechtlichen Blick auf das Risiko

[31] Vgl. Art. 18 DSGVO
[32] Vgl. Art. 21 DSGVO
[33] Vgl. Art 5 Abs. 2 DSGVO
[34] Vgl. Voigt / von dem Bussche, 2018, S. 40
[35] Vgl. Art. 30 DSGVO
[36] Vgl. ErwGr. 90 DSGVO

Dritter lenkt. Es ist Teil des gesamten Managementsystems einer Organisation und deckt den gesamten Datenschutzprozess von der Entwicklung bis hin zur Verbesserung der Verfahren in dieser ab.[37] Als solches ist es insbesondere für die Nachweispflicht gut geeignet, um weitergehende technische und organisatorische Maßnahmen in einem Unternehmen nachzuweisen.

Die Vorlage der Nachweise und aller weiteren Maßnahmen geschieht grundsätzlich auf Anfrage der Aufsichtsbehörde.[38] Eine freiwillige proaktive Zusammenarbeit mit den Aufsichtsbehörden ist möglich.

Verpflichtend ist eine Meldung an die Aufsichtsbehörde immer dann, wenn eine Datenschutzverletzung festgestellt wurde. In diesen Fällen beträgt die Frist 72 Stunden oder eine Ausnahme muss begründet werden.

[37] Vgl. Rost, Martin: Datenschutzmanagementsystem, in: Datenschutz und Datensicherheit, Ausgabe 5/2013, Berlin: Deutschland, 2013, S.295 - 300
[38] Vgl. Art. 31 DSGVO

3 Projektmanagement

Das zu erschaffene IT-Artefakt hat den Anspruch, ein Softwareentwicklungsprojekt zu unterstützen. Dahingehend gilt es zu klären, was ein Projekt ist und welche Akteure, Verfahren und Methoden es beinhalten kann. Das nachfolgende Kapitel führt daher grundlegendes Wissen auf. Im weiteren Verlauf der Arbeit werden vereinzelte Begriffe immer wieder aufgegriffen. Während der Evaluation des Anforderungskatalogs in Kapitel 7 wird dann die Nutzbarkeit innerhalb eines charakteristischen Softwareprojektes bewertet.

3.1 Definition Projekt und Projektmanagement

Laut DIN 69901 ist ein Projekt ein „Vorhaben, das im Wesentlichen durch Einmaligkeit der Bedingungen in ihrer Gesamtheit gekennzeichnet ist, z.B. Zielvorgabe, zeitliche, finanzielle, personelle und andere Begrenzungen, Abgrenzung gegenüber anderen Vorhaben, projektspezifische Organisation“.[39] Eine andere literarische Meinung definiert ein Projekt als „neuartig, zeitlich begrenzt, komplex und die Beteiligung mehrerer Stellen ist erforderlich.“[40]

Wie sich erkennen lässt, gibt es keine einheitliche Definition eines Projektes. Nichtsdestotrotz lassen sich Gemeinsamkeiten extrahieren, mit denen anschließend Aufgaben hinsichtlich ihrer Projektmerkmale verglichen werden können. Einschlägig ist der Faktor Zeit. Nach den Definitionen gibt es einen fest definierten Anfang und ein fest definiertes Ende, welche zusammen die zeitliche Begrenzung bilden. Hervorzuheben ist außerdem der besondere organisatorische Rahmen, mit denen ein Projektteam versucht, die gesetzte Zielstellung gemäß ihren vorhandenen Ressourcen zu erreichen. Um dies bestmöglich zu erreichen, gibt es das Projektmanagement.

Nach Laudon et al. werden im Projektmanagement Wissen, Fähigkeiten, Tools und Techniken angewandt, um bestimmte Ziele in einem festgelegten Budget- und Zeitrahmen zu erreichen.[41] Kuster et al. ergänzen das Projektmanagement im IT-Kontext (hier: Softwareentwicklung) um Maßnahmen, die der Um- und Neugestaltung von Systemen oder Prozessen bzw. Problemlösungen dienen. Zusätzlich ist laut den Autoren das Verfahren selbst, die erforderlichen Mittel und Einsatz und Koordination wichtiger als die Lösung.[42]

[39] Vgl. Deutsches Institut für Normung e.V. (Hrsg.): DIN 69901 Begriffe der Projektwirtschaft, Berlin: Beuth, 1987
[40] Vgl. Kraus, Georg/ Westermann, Reinhold: Projektmanagement mit System, 6. Aufl., Berlin: Springer, 2019, S. 2
[41] Vgl. Laudon et al., 2016, S. 935
[42] Vgl. Kuster et al., 2019, S.12

In diesem Zusammenhang fällt oftmals der Terminus des „magischen Dreieck im Projektmanagement“, sichtbar in Abbildung 1.

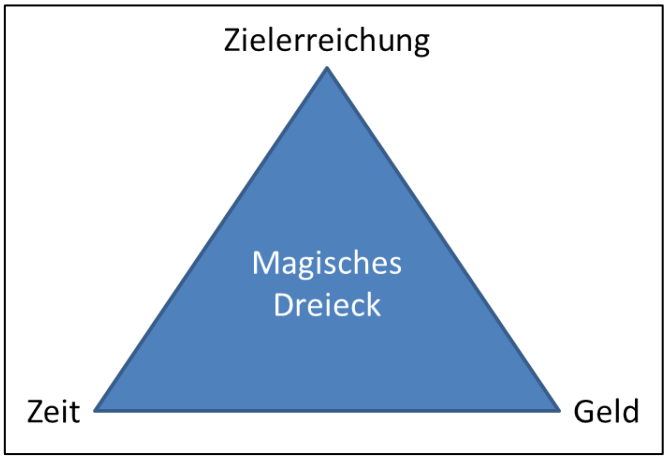

Abbildung 2: Magisches Dreieck im Projektmanagement[43]

Das Dreieck spiegelt die Wechselbeziehungen der wesentlichen Einflussfaktoren auf ein Projekt und damit Stellgrößen für das Projektmanagement wider. Dabei obliegt die Möglichkeit des Einflusses auf einen der Faktoren nicht allein beim Projektmanagement, sondern vielmehr bei den unterschiedlichen Anspruchsgruppen, die auf ein Projekt einwirken. Es ist nach der Logik des Dreiecks nicht möglich einen Einflussfaktor allein zu variieren, ohne damit die anderen Einflussfaktoren direkt mit zu beeinflussen. Folgendes Beispiel soll die Ausführungen unterstützen und aufzeigen, inwiefern das Dreieck bei der weiteren Arbeit berücksichtigt werden muss:

Die DSGVO stellt neue Anforderungen an die Softwareentwicklung. Wie in Kapitel 2 festgestellt, müssen sogenannte Betroffenenrechte implementiert werden. Unter Berücksichtigung von Zeit, Geld und Zielerreichung muss eine IT-Architektur so geschaffen oder verändert werden, dass die Ausübung der Rechte für einen Betroffenen möglich ist.

Das Projektmanagement selbst orientiert sich an unterschiedlichen Vorgehen, die je nach Charakteristika des Projektes ausgewählt werden. Die Auswahl des Vorgehens beeinflusst die verwendeten Methoden innerhalb des Projekts. Es existieren zwei unterschiedliche Vorgehen in der IT, auf die Kapitel 3.3 und 3.4 näher eingehen.

[43] Bättig, Peter: Projektmanagement Erfolgsfaktoren für erfolgreiche Projekte, in: Fachbibliothek, 2012, [online] https://www.fachbibliothek.ch/projektmanagement-erfolgsfaktoren-erfolgreiche-projekte/ [10.07.2020]

3.3 Traditionelles Projektmanagement

Traditionelles Projektmanagement zeichnet sich durch einen anfänglich erstellten Plan aus, von dem, trotz äußerer Einflüsse, möglichst minimal abgewichen werden soll.[44] Dieses *Anfang-zu-Ende-Denken* durchzieht sich bis auf die Ebene der Arbeitspakete und deren Abfolge[45], was ein sehr prozessual gesteuertes Vorgehen impliziert. Arbeitspakete sind in mehrere Phasen aufgeteilt. Eine Phase ist ein in sich abgeschlossener Arbeitsabschnitt, der mit einem Meilenstein endet. Meilensteine sollen dann als überprüfbares Zwischenergebnis dienen, das inhaltlich und zeitlich definiert ist und eine Gesamtbeurteilung des Projekts erlaubt.[46] Stellvertretend für ein traditionelles Vorgehen in der Softwareentwicklung findet eine genauere Betrachtung des Wasserfallmodells statt, das 1970 von Winston Royce entwickelt wurde.

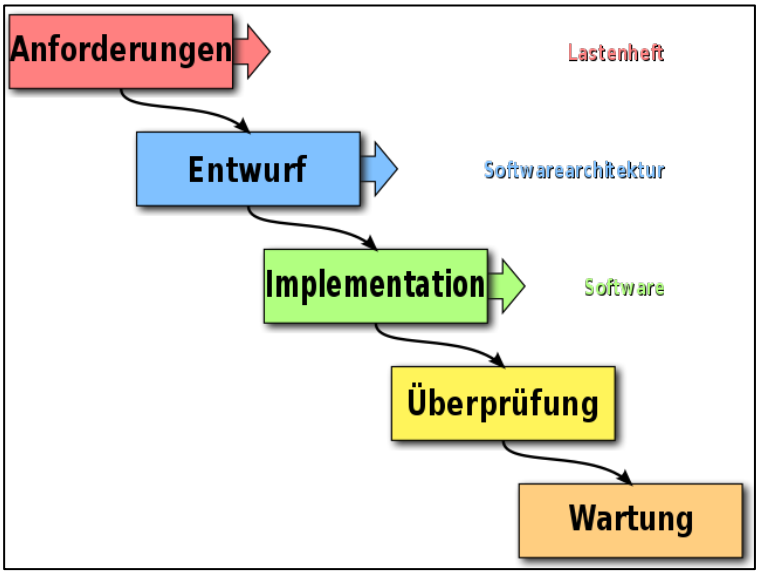

Abbildung 3: Stufen des Wasserfallmodells[47] (Hoadley, Paul / Smith, Paul / Traian, Shmuel Csaba, 2013, https://commons.wikimedia.org/w/index.php?curid=29119277)

In Abbildung 3 sind die unterschiedlichen Phasen des Wasserfallmodells dargestellt. Die Phasen werden sequenziell, das heißt von oben nach unten durchlaufen, was dem Modell, in Anlehnung an einen stetig fließenden Wasserfall, seinen Namen gibt. Eine neue Phase wird immer dann bearbeitet, wenn die vorherige abgeschlossen ist. Eine parallele Bearbeitung mehrerer Phasen ist nicht möglich. Ein Rückgriff auf eine vorherige Phase kann beim Auftreten eines Fehlers möglich bzw. erforderlich sein,

[44] Vgl. Angermeier, Dr. Georg: Traditionelles Projektmanagement, in: Projektmanagementmagazin, 2014, [online] https://www.projektmagazin.de/glossarterm/traditionelles-projektmanagement [20.03.2020]
[45] Vgl. Eckkrammer, Tobias / Eckkrammer, Florian / Gollner, Helmut: Agiles IT-Projektmanagement im Überblick, in: Ernst Tiemeyer (Hrsg.), Handbuch IT-Projektmanagement, 2. Aufl., München, Deutschland: Hanser, 2014, S. 81
[46] Kraus / Westermann, 2019, S. 35
[47] Hoadley, Paul / Smith, Paul / Traian, Shmuel Csaba: Waterfall model, in: Wikimedia Commons, 2013, [online] https://commons.wikimedia.org/w/index.php?curid=29119277 [10.07.2020]

wodurch von diesem Punkt an eine erneute sequenzielle Abfolge ausgelöst wird.[48] Tabelle 3 fasst die wichtigsten Inhalte der jeweiligen Phasen zusammen.

Tabelle 2: Phasen des Wasserfallmodells (Petersen et al., 2009, S. 400f)	
Anforderungen	Identifizieren der Anspruchsgruppen, Kundenbedürfnisse werden in Anforderungen überführt, Anforderungen sollen in der Entwurfs- und Implementationsphase als Input dienen, Überprüfen des Lösungskonzeptes, Output des Anforderungsmanagements ist ein Lastenheft
Entwurf	Modellieren und Entwerfen der Softwarearchitektur, Output des Entwurfs ist ein Modell der Software
Implementation	Umsetzen der Anforderungen in Software, Testen der umgesetzten Einheit, Dokumentieren von Abweichungen (qualitativ, zeitlich), Output der Implementation ist die Software
Überprüfung	Testen der Systemintegration bezüglich Qualität und Funktionalität, Messen der ganzheitlichen Performance, Output der Überprüfung ist Verifikation des Systems (z.B. durch Checkliste) und die Übergabe an den Kunden
Wartung	Lösen von auftretenden Problemen beim Kunden, Output der Wartung sind Updates zur Fehlerbehebung

Das traditionelle Projektmanagement bietet den Vorteil einer ganzheitlichen Ressourcenplanung, sei es in Form von Kosten, Zeit oder Projektmitgliedern. Die Überwachung und Steuerung lassen sich zu jedem Zeitpunkt nachvollziehen. Für den Kunden können schon nach der Anforderungserhebung ein Kostenansatz und für das Projekt damit eine Umsatzplanung stattfinden.[49] Der feste Rahmen lässt

[48] Vgl. Litke, Hans-Dieter: IT-Projekte richtig strukturieren und systematisch planen in: Ernst Tiemeyer (Hrsg.), Handbuch IT-Projektmanagement, 2. Aufl., München, Deutschland: Hanser, 2014, S. 194
[49] Vgl. Angermeier, 2014

allerdings wenig Möglichkeiten für Veränderungen zu. Müssen vorhergehende Phasen in Folge von Fehlern nochmal durchlaufen werden, steigt der Kosteneinsatz zur Beseitigung. Dies wirkt umso mehr, je weiter das Projekt fortgeschritten ist.[50]Modernere Varianten des traditionellen Projektmanagements integrieren aus diesen Gründen ein Prototyping, damit das Gesamtsystem früher evaluiert werden kann als mit Abschluss der Testphase.[51]

3.4 Agiles Projektmanagement

Im Jahr 2001 verfassten mehrere Softwareentwickler und IT-Projektmanager das *Agile Manifesto* als neuen Ansatz für das Projektmanagement.

Vier Grundprinzipien innerhalb des Manifests sollen den Unterschied zum traditionellen Projektmanagement ausdrücken: Individuen und Interaktionen mehr als Prozesse und Werkzeuge, Funktionierende Software mehr als umfassende Dokumentation, Zusammenarbeit mit dem Kunden mehr als Vertragsverhandlung und Reagieren auf Veränderung mehr als das Befolgen eines Plans.[52]

Daraus ergibt sich ein wertgetriebener Ansatz von Softwareentwicklung. Software wird sequentiell und inkrementell entwickelt, das heißt ein Produkt wird in mehreren Schleifen immer weiter ausgebaut. Anforderungen werden nicht ausschließlich am Projektanfang erhoben, sondern können auch in späteren Projektphasen hinzugefügt, verändert oder verfeinert werden. Durch einen regelmäßigen Austausch mit allen Anspruchsgruppen können Abweichungen einfach festgestellt und angepasst werden.[53]

Stellvertretend für agile Projektmanagementvorgehen soll auf Scrum näher eingegangen werden, da Elemente daraus auch für das Unternehmen der Fallstudie eine Rolle spielen. Der Ablauf von Scrum ist in Abbildung 4 dargestellt.

[50] Vgl. Eckkrammer et al., 2014, S. 82f
[51] Vgl. Litke, 2014, S. 194
[52] Vgl. Beck, Kent / Beedle, Mike / van Bennekum, Arie / Cockburn, Alistair / Cunningham, Ward / Fowler, Martin / Grenning, James / Highsmith, Jim / Hunt, Andrew / Jeffries, Ron / Kern, Jon / Marick, Brian / Martin, Robert C. / Mellor, Steve / Schwaber, Ken / Sutherland, Jeff / Thomas, Dave: Manifest für agile Softwareentwicklung, [online] https://agilemanifesto.org/iso/de/manifesto.html [06.07.2020]
[53] Vgl. Kusay-Merkle, Ursula: Agiles Projektmanagement im Berufsalltag, Berlin: Springer, 2018, S. 21

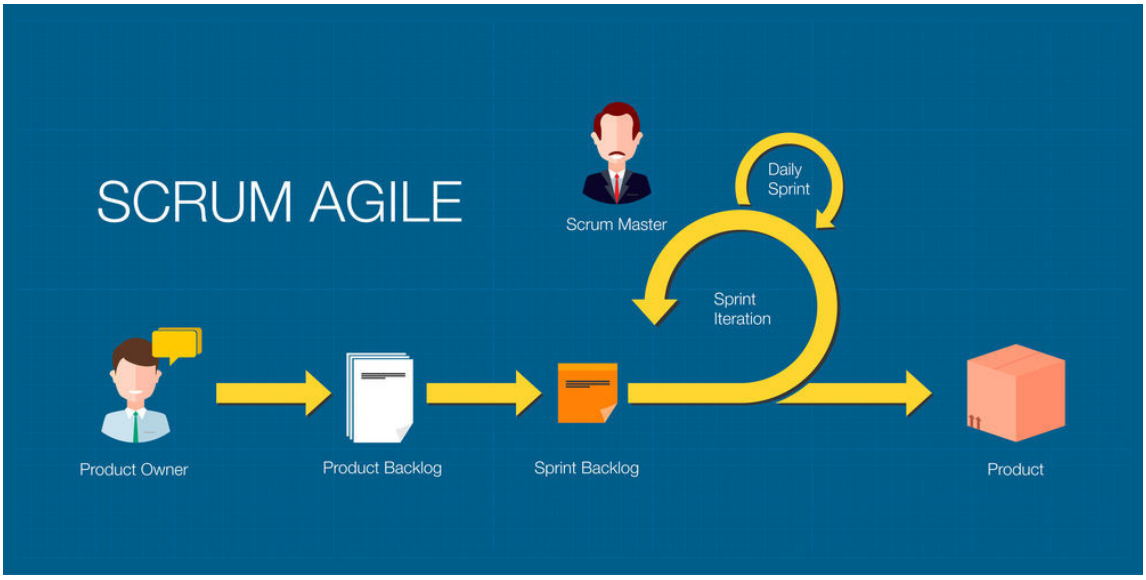

Abbildung 4: Ablauf Scrum[54]

Der Scrum-Prozess wird eingeleitet durch den Product Owner. Analog zu einem Produktmanager betreut er das zu entwickelnde Produkt über den kompletten Lebenszyklus.[55] Damit ist der Product Owner auch für die komplette Erhebung und kontinuierliche Verbesserung des Anforderungsmanagements zuständig. Daraus resultierend obliegt die Verantwortung über den Product Backlog bei ihm. Gleichzeitig schlägt der Product Owner die Brücke zum Projektteam. Der Product Owner priorisiert und spezifiziert die erhobenen Anforderungen und legt zusammen mit dem Entwicklerteam fest, in welchen Sprints welche Anforderungen implementiert werden. Darüber hinaus liegt die Gesamtverantwortung über das Projekt bei ihm, womit er verantwortlich für die Einhaltung von Kosten- und Zeitzielen ist.[56]

Wie bereits erwähnt werden die Anforderungen an das Produkt bzw. Projekt im Product Backlog festgehalten. Der Product Backlog wird auch als *lebendiges Dokument* bezeichnet[57], weil hier eine direkte Umsetzung des agilen Denkens stattfindet: Anforderungen innerhalb des Product Backlogs sind variabel und können hinzugefügt oder entfernt werden. Im Rahmen des Sprint Planning findet eine Planung der Arbeitspakete für die kommende Projektphase statt, die auch Sprint genannt wird. Das Entwicklerteam legt darin gemeinsam mit dem Product Owner die geplanten Anforderungen und die geplante Arbeitszeit an der jeweiligen Anforderung fest. Als Ergebnis steht am Ende des Sprint Planning der Sprint Backlog. Im Gegensatz zum Product Backlog sind die Anforderungen im Sprint Backlog auch mit einer *Definition-of-Done* versehen, also einer festgelegten Definition der Zielerreichung.[58] Der sich nun

[54] Luber, Stefan / Augsten, Stephan: Was ist Scrum?, in: Dev-Insider, 2017, [online] https://www.dev-insider.de/was-ist-scrum-a-575361/ [10.07.2020]
[55] Vgl. Maximini, Dominik: The Scrum Culture, Wendlingen: Springer, 2015, S. 290
[56] Vgl. Eckkrammer et al., 2014, S. 92
[57] Vgl. Eckkrammer et al., 2014, S. 91
[58] Vgl. Maximini, 2015, S. 299

anschließende Sprint hat eine gesetzte Dauer. Diese kann variieren, üblich sind allerdings Abstände von zwei bis drei Wochen.[59] Ein Vorgehen nach Scrum setzt mehrere solcher Sprint-Zyklen voraus.

Die Überwachung und Einhaltung des Vorgehens und der darin enthaltenen Artefakte, Werkzeuge und Rollen, stellt der Scrum Master sicher. Während der Product Owner das Produkt in den Vordergrund stellt, stellt der Scrum Master das Scrum-Vorgehen als solches in den Vordergrund. Er hat zwar keine disziplinarischen Befugnisse, fungiert aber als Moderator innerhalb des Teams und nach außen.

Innerhalb eines Sprints findet ein täglicher Abgleich der Wissensstände, Erfahrungen und Probleme statt. Das dazugehörige Ereignis wird Daily Sprint genannt. Vertreten sind dabei grundsätzlich der Product Owner, das Entwicklerteam und der Scrum Master. Darüber hinaus kann jede Anspruchsgruppe des Projektes an dem Treffen teilnehmen. Nach jedem Sprint ist nach Möglichkeit ein funktionierendes (Teil-)Produkt implementiert, sodass dem Kunden die Fortschritte vorgeführt werden können. Eine Rückschau, auch genannt Sprint Retrospective, schließt den vorangegangenen Sprint ab und reflektiert gemachte Erfahrungen mit dem Ziel der kontinuierlichen Verbesserung des Prozessablaufes.[60]

Ein Vorteil der Verwendung von Scrum im Projekt ist die gewonnene Flexibilität. Auf Änderungen, sei es im Anforderungsmanagement oder in den Projektvereinbarungen, kann auch in späteren Projektphasen einfacher als im traditionellen Projektmanagement reagiert werden. Ein zweiter Punkt ist, dass die interne und externe Kommunikation durch regelmäßige Diskussionsrunden gefördert wird. Im Sinne der kontinuierlichen Verbesserung ermöglicht der Einsatz der *Retrospective* eine schnellere Umsetzung von Prozessverbesserungen, die dann schon im nächsten *Sprint* umgesetzt werden können. Nachteilig wirkt sich der fehlende Gesamtüberblick aus. Bei Initialisierung des Projektes können genaue Kosten- oder Zeitabschätzungen nicht getroffen werden. Durch mehrere unterschiedliche Rollen, aber fehlende Hierarchien, können Zuständigkeiten potentiell unklar oder schwer durchgesetzt werden. Außerdem setzt der hohe Kommunikationsaufwand ein intaktes Teamgefüge voraus, welches durch Gruppenprozesse sensibel gestört werden kann.

3.5 User Stories in der agilen Softwareentwicklung

Im vorangegangenen Unterkapitel wurde das agile Projektmanagement beleuchtet. Von besonderer Bedeutung für diese Arbeit ist, wie mit Anforderungen umgegangen wird. Dazu wurde bereits geklärt, dass Anforderungen im Product Backlog gesammelt werden, bis sie in einem Sprint implementiert werden. Es fehlt die Auseinandersetzung mit der Formulierung von Anforderungen, die für den Anforderungskatalog festgelegt werden muss.

[59] Vgl. Maximini, 2015, S. 301
[60] Vgl. Maximini, 2015, S. 303

Im agilen Projektmanagement werden in der Regel User Stories verwendet. User Stories sind Anforderungen an ein Softwaresystem, die aus Sicht des Benutzers beschrieben werden und einen eindeutigen Nutzen liefern sollen.[61] Sie sind absichtlich unvollständig formuliert, damit eine genaue Implementierung einer Anforderung in einer späten Phase der Softwareentwicklung in das Gesamtsystem passt.[62] Dahingehend unterstützen User Stories die Kommunikation und das Verständnis zwischen allen Beteiligten.[63] Außerdem funktionieren sie zusammen mit iterativem Entwicklungsvorgehen sehr gut, aufgrund der Möglichkeit des Abstraktionsgrades der User Stories.[64]

Der Aufbau einer User Story besteht aus einem Subjekt, verbunden mit [möchte ich/kann ich], einem aktiven Prädikat und einem Objekt, das vom Subjekt ausgeführt wird.[65] Dazu kann das Ende eine Klarstellung des Satzes, eine andere Funktionalität oder Abhängigkeit oder einen qualitativen Nutzen ausdrücken.[66] Ein Beispiel für eine User Story ist: „Als Nutzer möchte ich die Löschung meiner personenbezogenen Daten anfragen können." User Stories können auf Story-Karten festgehalten werden, die üblicherweise aus DIN A5 großen Karteikarten bestehen. [67] Wichtiger als das Medium, auf das die User Stories geschrieben werden, sind die Akzeptanzkriterien, die einerseits definieren, wann eine Lösung eine Anforderung komplett bedient und andererseits darlegen, ob wirklich ein Mehrwert entstanden ist.[68] Die Akzeptanzkriterien werden vom Product Owner zusammen mit den Entwicklern festgelegt. Sie sind nicht festgeschrieben und bis zur Implementierung variabel.[69]

[61] Vgl. Wirdemann, Ralf: Scrum mit User Stories, 3. Aufl., München: Hanser Verlag, 2017, S. 49
[62] Vgl. Wirdemann, 2017, S. 49
[63] Vgl. Cohn, Mike: User Stories Applied for Agile Software Development, USA, Boston: Pearson Education Inc., 2004, S. 154
[64] Vgl. Cohn, 2004, S. 154
[65] Vgl. Lucassen, Garm / Dalpiaz, Fabiano / van der Werf, Jan Martijn E. M. / Brinkkemper, Sjaak: Improving agile requirements: the Quality User Story framework and tool, Requirements Eng 21, Springer, 2016, S. 385
[66] Vgl. Lucassen et al., 2016, S. 385
[67] Vgl. Wirdemann, 2017, S. 51
[68] Vgl. Wirdemann, 2017, S. 52
[69] Vgl. Wirdemann, 2017, S. 53

4 Forschungsmethodik zur Konstruktion eines Anforderungskatalogs für DSGVO-Anforderungen in der Softwareentwicklung

Das vorliegende Kapitel klärt, durch welche Verfahrensweisen die Beantwortung der Forschungsfrage ermöglicht werden kann. Der Kontext aus DSGVO-Anforderungen und Softwareentwicklung wird mittels konstruktionsorientiertem Forschungsansatz bearbeitet. Als Ergebnis des Kapitels entsteht ein Vorgehensmodell, welches die weiteren Schritte der Arbeit absteckt und als roter Faden dient.

Die eingangs aufgestellte Forschungsfrage „Wie lassen sich die Anforderungen der DSGVO in der Softwareentwicklung implementieren?“ beinhaltet bereits ein konstruierendes Element. Eine *Implementierung* ist im Kontext der Informationstechnik die Phase der Softwareentwicklung, in der die Module der Entwurfsphase als Programm realisiert werden.[70] Ziel der Wirtschaftsinformatik ist in diesem Zusammenhang Theorien oder Methoden zu entwickeln, die die „Entwicklung, organisatorische Implementierung und das Management betrieblicher Informationssysteme fördern“.[71] Um diesem Anspruch gerecht zu werden, soll mithilfe der konstruktionsorientierenden Forschung ein geeignetes IT-Artefakt geschaffen werden.

Als Voraussetzung für die Verwendung dieser Forschungsart gilt nach Hevner et al. zuallererst die Identifizierung eines organisatorischen Problems, das mittels IT-Artefakten gelöst werden soll.[72] Auch nach March und Smith muss die Forschung in diesem Zusammenhang geeignete Techniken und Lösungen finden, um real existierende Probleme zu lösen.[73] Winter unterscheidet drei Kategorien von IT-Artefakten als Lösung der Probleme: Konstrukte, Modelle und Methoden.[74] Um nun eine konstruktionsorientierte Forschung zu betreiben, haben Pfeffers et al. ein Prozessmodell geschaffen, das die Ansätze von sieben Autoren im Bereich des *Design Science Research* in einem Modell vereint. Dadurch soll ein hoher Konsens sichergestellt werden.[75] Abbildung 5 zeigt das erschaffene Prozessmodell und seine sechs Aktivitäten.

[70] Vgl. Siepermann, Markus: Implementierung, in: Gabler Wirtschaftslexikon, 2018, [online] https://wirtschaftslexikon.gabler.de/definition/implementierung-31993/version-255541 [10.06.2020]
[71] Vgl. Frank, Ulrich: Konstruktionsorientierter Forschungsansatz, in: Enzyklopädie der Wirtschaftsinformatik, 2016, [online] https://www.enzyklopaedie-der-wirtschaftsinformatik.de/wi-enzyklopaedie/lexikon/uebergreifendes/Forschung-in-WI/Konstruktionsorientierter-Forschungsansatz/index.html [10.06.2020]
[72] Hevner, Alan / March, Salvatore / Park, Jinsoo: Design Science in Information Systems Research, in: MIS Quarterly, Vol. 28 No.1, 2004, S. 77
[73] March, Salvatore / Smith, Gerald: Design and natural science research on information technology, in: Decision Support Systems 15, Elsevier, 1995, S. 251
[74] Winter, Robert: Design science research in Europe, in: European Journal of Information Systems 17, 2018, S. 471
[75] Pfeffers, Ken / Tuunanen, Tuure / Rothenberger, Marcus / Chatterjee, Samir: A Design Science Research Methodology for Information Systems Research, in: Journal of Management Information Systems, Vol. 24 No. 3, 2007-8, S. 52

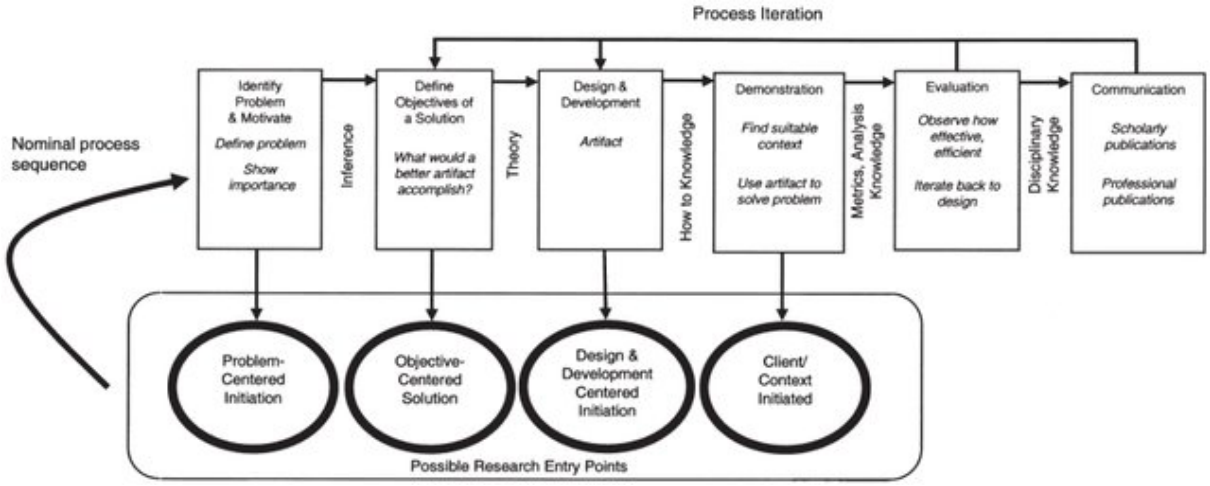

Abbildung 5: Design Science Research Methodology Prozessmodell[76]

Tabelle 3 beschreibt die einzelnen Aktivitäten des Prozessmodels. Danach wird die vorliegende Forschungsaufgabe nach den jeweiligen Aktivitäten analysiert und ihnen zugeordnet. Gleichzeitig ist mit Abschluss der Analyse auch die Eignung der konstruktionsorientierten Forschung gezeigt, wenn die einzelnen Aktivitäten in einem validen Vorgehensmodell für die weitere Forschungsarbeit münden.

Tabelle 3: Sechs Aktivitäten der Design Science Research Methodology[77]	
Aktivität 1: Problemidentifikation und Motivation	Definieren des spezifischen Forschungsproblems und begründen des Wertes einer Lösung
Aktivität 2: Definieren der Objekte einer Lösung	Erschließen von Objekten einer Lösung aus Anwendung der Problemdefinition und Wissen darüber, was möglich und machbar ist Quantitativ: Mittels Vergleichen, wann eine angestrebte Lösung besser als bisherige ist Qualitativ: Beschreibung darüber, wie ein neues Artefakt die Problemlösung unterstützen soll
Aktivität 3: Design und Entwicklung	Erschaffen des Artefakts, zum Beispiel Konstrukte, Modelle, Methoden oder Instanziierungen

[76] Pfeffers, 2007-8, S. 54
[77] Pfeffers, 2007-8, S. 52 – 57

Aktivität 4: Demonstration	Demonstrieren des Nutzens des Artefakts zum Lösen einer oder mehrerer Instanzen des Problems Zum Beispiel durch Experimente, Fallstudien, Simulationen oder Beweise
Aktivität 5: Evaluierung	Beobachten und Messen, wie erfolgreich das Artefakt die Problemlösung unterstützt Zum Beispiel durch relevante Metriken oder Analysetechniken
Aktivität 6: Kommunikation	Die Kommunikation des Problems und seiner Wichtigkeit, das Artefakt, Nützlichkeit und Neuheit, Präzision des Designs und Effektivität für andere Forscher oder relevanten Personenkreis

Darüber hinaus bezieht Winter den Einstiegspunkt der Forschung in sein Modell ein. Für die weitere Bearbeitung wird der Einstiegspunkt *Problem-Centered Initiation* festgelegt, das heißt ausgehend von einem realen Problem eine Lösung erforscht. Die Analyse des vorliegenden Forschungsproblems und seiner möglichen Lösung ergibt nachfolgende Einteilung.

1. *Problemidentifikation und Motivation*: Mit der Einführung der DSGVO im Jahr 2018 hat der Gesetzgeber neue Rahmenbedingungen u.a. für Software festgelegt. Werden diese nicht eingehalten, ist ein hoher wirtschaftlicher Schaden möglich.[78] In vielen Unternehmen ist eine Umsetzung noch nicht vollständig abgeschlossen.[79] Um der Nachweispflicht gerecht zu werden, sollen Anforderungen der DSGVO bereits in die Softwareentwicklung implementiert werden. Teure Strafen, wie auch Softwarenachbesserungen, sollen im Stadium der Entwicklung vermieden werden.
2. *Definieren der Objekte einer Lösung*: Aufgrund vorhandener Literatur im Zusammenhang mit der Erhebung von Anforderungen aus der DSGVO, die einen Einfluss auf die Softwareentwicklung haben, werden diese durch eine Literaturanalyse extrahiert. Die sich daraus ergebenen Anforderungen werden dann in einem Anforderungskatalog gesammelt.

[78] Vgl. Art. 83 Abs. 5 DSGVO
[79] Vgl. Dehmel, Susanne / Thiel, Barbara: Vier Monate DS-GVO – wie weit ist die deutsche Wirtschaft?, Berlin: Bitkom Research, 2018, S. 2

3. *Design und Entwicklung*: Das geschaffene Artefakt ist ein Anforderungskatalog, der allgemeingültig für die Softwareentwicklung sein soll. Der Katalog soll außerdem organisch sein, das heißt wie eine Sammlung von „Best Practices“ stets aktuell gehalten und zukünftige Erfahrungen geteilt werden.
4. *Demonstration*: In einer Fallstudie wird der entstandene Katalog einem bestehenden Projektteam zugänglich gemacht. In diesem Kontext wird analysiert, ob der Katalog akzeptiert ist und in den Ablauf integriert werden kann.
5. *Evaluation*: Die Evaluation des Katalogs wird mittels Experteninterviews stattfinden. Dabei sollen je ein Anforderungsmanager, Softwareentwickler und -tester den Katalog nach vorher festzulegenden, objektiven Gütekriterien bewerten.
6. *Kommunikation*: Der Katalog wird als fertiges Artefakt einem Unternehmen zur Verfügung gestellt. Für den Kreis der Forschung werden dann sowohl der Katalog als auch die Forschungsarbeit veröffentlicht.

Nachdem Aktivität 1 im Rahmen der methodischen Betrachtung bereits abgegrenzt wurde, startet der weitere konstruktionsorientierte Forschungsprozess mit Aktivität 2. Aktivität 6 ist darüber hinaus nicht mehr inhaltlicher Bestandteil zur Beantwortung der Forschungsfrage und wird deswegen nicht weiter aufgeführt. Daraus ergibt sich folgendes methodisches Vorgehensmodell für den weiteren Verlauf der Arbeit:

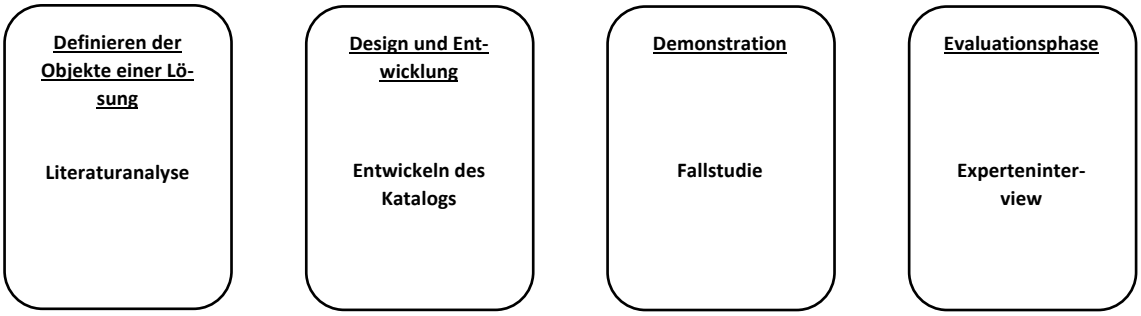

Abbildung 6: Vorgehensmodell der Forschungsarbeit

5 Analyse der DSGVO-Anforderungen im Kontext der Softwareentwicklung

Nachdem im vorherigen Kapitel der Weg zu einer adäquaten Lösung aufgezeigt wurde, widmet sich dieses Kapitel dem Erheben von Anforderungen aus der DSGVO, die im Zusammenhang mit der Softwareentwicklung stehen. Da sich bereits Autoren den Anforderungen der DSGVO gewidmet haben, beleuchtet eine Literaturanalyse unterschiedliche Herangehensweisen und extrahiert die Erkenntnisse für die eigene Forschungsarbeit. Durch die Analyse werden die erhobenen, relevanten Anforderungen in das IT-Artefakt „Anforderungskatalog“ übernommen.

5.1 Literaturanalyse

Eine Aufgabe der Literaturanalyse ist nach Fettke[80], in Anlehnung an Cooper[81], das Beschreiben, Zusammenfassen, Bewerten, Klären oder Integrieren von Ergebnissen ausgewählter Primäruntersuchungen. Unterschieden wird dabei zwischen qualitativer und quantitativer Analyse. Mittels der Kategorien von Fettke zur Charakterisierung von Literaturanalysen, wird die weitere Literaturanalyse in Tabelle 4 eingeordnet.

Tabelle 4: Kategorien zur Charakterisierung von Reviews[82]	
1. Typ	Natürlichsprachliche Analyse durch verbale Erläuterungen und Argumentationen
2. Fokus	Untersuchen bisheriger Forschungsergebnisse im Bereich Anforderungen der DSGVO an Softwareentwicklung
3. Ziel	Mittels einer Fragestellung die vorliegenden Ergebnisse bzw. theoretischen Ansätze integrieren und zusammenführen
4. Perspektive	Neutrale Position des Autors bei der Analyse
5. Literatur	Die Auswahl der zu untersuchenden Literatur erfolgt nicht expliziert und beschränkt sich auf repräsentative Schlüsselarbeiten der Thematik
6. Struktur	Thematische Strukturierung, d.h. inhaltlich ähnliche Arbeiten werden vergleichend behandelt

[80] Vgl. Fettke, Peter: State-of-the-Art des State-of-the-Art - Eine Untersuchung der Forschungsmethode „Review“ innerhalb der Wirtschaftsinformatik, in: Wirtschaftsinformatik 48, 2006b, S. 257 - 266
[81] Vgl. Cooper, Harris M.: Synthesizing Research – A Guide for Literature Reviews, 3. Auflage, Thousand Oaks, USA: Sage Publications Inc, 1998
[82] Fettke, 2006b, S. 259

7. Zielgruppe	Praktiker im Bereich der Softwareentwicklung, Öffentlichkeit
8. Zukünftige Forschung	Nicht expliziert dargestellt

Damit sind die Rahmenbedingungen der Literaturanalyse abgesteckt. Das weitere Vorgehen richtet sich nach den fünf Phasen der Literaturanalyse.[83] Die Phasen begründen sich auch aus Coopers vorhergehender Arbeit.[84] Es findet demnach eine Unterteilung in *Problemformulierung*, *Literatursuche*, *Literaturauswertung*, *Analyse und Interpretation* und *Präsentation* statt.

Die *Problemformulierung* soll die zentrale Frage, die mit einer Literaturanalyse beantwortet werden soll, ausformulieren, abgrenzen und präzisieren.[85] Die zentrale Frage dieser Literaturanalyse ist gleichsam die Forschungsfrage. Ausgewählte Literatur soll demnach Anforderungen der DSGVO an die Softwareentwicklung identifizieren und Vorschläge zu deren Umsetzung geben. Während es dabei Anforderungen gibt, die eine komplette Neustrukturierung des Softwareentwicklungsprozesses voraussetzen, werden hier lediglich die Anforderungen für den Anforderungskatalog benutzt, die eine Anpassung beziehungsweise Optimierung der bisherigen Softwareentwicklung als Ziel haben. Dies begründet sich nicht zuletzt aus dem finanziellen Aspekt der Benutzung des IT-Artefakts Anforderungskatalog.

In der Phase der *Literatursuche* wird nun anhand der eben aufgestellten Kriterien Literatur gesucht, die die zentrale Frage beantworten kann. Als Ansatz wird hier die Verwendung von Schlüsselbegriffen verwendet, mit deren Hilfe Schlüsselliteratur gefunden werden soll. Naheliegend ist dabei die Verwendung der wichtigsten Schlüsselbegriffe aus der Forschungsfrage: Anforderungen, DSGVO und Softwareentwicklung. Allerdings ist die Verwendung der deutschen Begriffe nicht zielführend. Die Verwendung der englischen Übersetzungen der Begriffe (also: Requirements, GDPR und Software development) führt zu einer weitaus größeren Treffermenge.

Es schließt sich die Phase der *Literaturauswertung* an. Vor dem Hintergrund der sehr speziellen Fragestellung und den gemachten Einschränkungen, gilt es für die Analyse eher wenige, sehr aussagekräftige und konkrete Literatur zu finden. Als entsprechend gelten daher insbesondere die Werke von Hjerppe

[83] Vgl. Fettke, 2006b, S. 260
[84] Vgl. Cooper, Harris / Hedges, Larry: Research Synthesis As a Scientific Enterprise, in: The Handbook of Research Synthesis, New York, USA: Russell Sage Foundation, 1993
[85] Vgl. Fettke, 2006b, S. 260

et al.[86], Ringmann et al.[87], Huth und Matthes[88] und zu Teilen Ayala-Rivera und Pasquale[89]. Die wissenschaftliche Relevanz der Werke lässt sich anhand der Bewertungen der Konferenzen, für die die Werke gemacht wurden, durch gängige Konferenz-Rankings zeigen. Die Konferenzen werden innerhalb dieser Rankings als relevant bewertet.

Die Phase der *Analyse und Interpretation* untersucht nun die ausgewählte Literatur vor dem Hintergrund der aufgeworfenen Problemformulierung. Dies findet, zusammen mit der *Präsentation*, in einem eigenen Unterkapitel statt.

5.2 Exzerpieren der Anforderungen

In der ausgewählten Literatur gibt es unterschiedliche Herangehensweisen zum Erheben der Anforderungen. Ein Ansatz kommt von Hjerppe et al., die Anforderungen im Kontext von mittelständischen Softwareentwicklern in Finnland erheben. Anhand von Einschränkungen, die in diesem Kontext existent sind, werden Implementierungsvorschläge für die abgeleiteten Anforderungen aus der DSGVO getroffen. Die verwendeten Einschränkungen lauten:

> E1: Heterogenität der Kunden = Unterschiedliche Anforderungen bei Neu- oder Bestandskunden
>
> E2: Technologische Abhängigkeit = Ähnlich wie Einschränkung 1 können Bestandskunden existierende IT-Infrastruktur haben, die Lösungen einschränkt
>
> E3: Größe der Projekte = Bedeutet, dass der Projektgröße Rechnung getragen werden soll. Das heißt umfassende Architekturen sind für kleine Projekte gegebenenfalls ungeeignet
>
> E4: Externe Investitionen = Eine zu hohe Angepasstheit an einen Kunden schränkt eine Wiederverwendung des erschaffenen Frameworks ein, was wiederum Investitionen erhöht
>
> E5: Varietät der Server = Für unterschiedliche Zwecke (persönliche Daten, Testen) unterschiedliche Server
>
> E6: Erneuern alter Systeme = Die Lösungen der Autoren setzen ein gewisses Level an Systemfunktionalität voraus, das alte Systeme vielleicht nicht mehr haben

[86] Hjerppe, Kalle / Ruohonen, Jukka / Lepännen, Ville: The General Data Protection Regulation: Requirements, Architectures, and Constraints, in: 2019 IEEE 27th International Requirements Engineering Conference (RE), 2019

[87] Ringmann, Sandra Domenique / Langweg, Hanno / Waldvogel, Marcel: Requirements for Legally Compliant Software Based on the GDPR, in: On the Move to Meaningful Internet Systems – OTM 2018 Conferences, Springer, 2018, S. 258 - 276

[88] Huth, Dominik / Matthes, Florian: "Appropriate Technical and Organizational Measures": Identifying Privacy Engineering Approaches to Meet GDPR Requirements, in: 25th Americas Conference on Information Systems, Cancun, 2019

[89] Ayala-Rivera, Vanessa / Pasquale, Liliana: "The Grace Period Has Ended": An Approach to Operationalize GDPR Requirements, in: 2018 IEEE 26th International Requirements Engineering Conference (RE), 2018

E7: Wiederverwendbarkeit = Wiederverwendbarkeit von einzelnen (Software-)Modulen, auch um personenbezogene Daten nur auf benötigte Module zu verteilen

E8: Wartung und Support = Neben Bugfixes und patchen auch Rollenverteilung für spätere Zugriffe im Rahmen der Wartung und des Supports

E9: Verteilung personenbezogener Daten = Im Grundsatz soll gelten, dass eine geringe Verteilung von personenbezogenen Daten am besten ist (Nachverfolgbarkeit, Datenminimierung)

Die Einschränkungen sind inhaltlich sowohl an die Softwareentwicklung als auch an externe Business-Faktoren angelehnt.[90] Abbildung 7 stellt die erhobenen Anforderungen und deren zugrunde liegenden Artikel der DSGVO dar. Einbezogen werden durch die Autoren nur jene Anforderungen, die einen Einfluss auf Softwarearchitektur haben.[91] Tabelle 5 liefert anschließend die Erklärung der Autoren zu den neun Anforderungskategorien und deren Beziehung zu den getroffenen Einschränkungen.

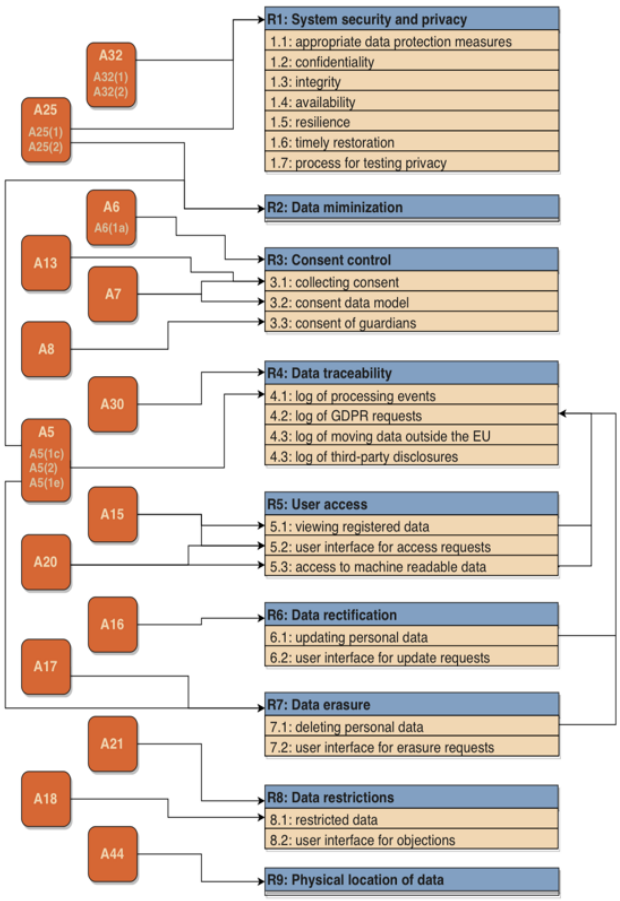

Abbildung 7: Anforderungen der DSGVO[92]

[90] Vgl. Hjerppe et al., 2019, S. 3
[91] Vgl. Hjerppe et al., 2019, S. 9
[92] Hjerppe et al., 2019, S. 5

Tabelle 5: Erklärung zu Anforderungserhebung nach Kategorien[93]	
R1: Systemsicherheit und Privatsphäre	Betrifft den Datenschutz und die Informationssicherheit im Allgemeinen, d.h. vor allem technische und organisatorische Maßnahmen. Wird beeinflusst durch Einschränkungen E1, E2, E4, E7, E8 und E9.
R2: Datenminimierung	Betrifft insbesondere den Grundsatz der Datenminimierung nach Art. 5 Abs. 1 c DSGVO. Wird beeinflusst durch Einschränkungen E5 und E9.
R3: Einwilligungskontrolle	Betrifft die Rechtmäßigkeit der Verarbeitung und setzt damit Einwilligung nach Art. 6 und 7 DSGVO voraus. Einschränkungen resultieren aus E1, E4 und E7.
R4: Verarbeitungsverzeichnis	Betrifft mit Art. 30 DSGVO vor allem die Führung von Verarbeitungsverzeichnissen zum Erfüllen der Rechenschaftspflicht gegenüber Aufsichtsbehörden. Ziel ist eine Nachverfolgbarkeit von Verarbeitungswegen im Zusammenhang mit allgemeinen Verarbeitungstätigkeiten, Anfragen von Betroffenenrechten, Datenverkehr außerhalb der EU und zu Drittparteien. Einschränkungen sind E5, E6, E7, E8 und E9.
R5: Nutzerzugang	Setzt sich aus den Betroffenenrechten und deren Ausübung im Allgemeinen und der Auskunftspflicht und Datenportabilität zusammen (Art. 15 und 20 DSGVO). Dafür sollen die Daten des Nutzers einsehbar, ein Interface zur Verfügung gestellt und der Zugang zu einer Kopie der Dateien bereitgestellt werden. Einschränkungen sind E5 und E9.

[93] In Anlehnung an Hjerppe et al., 2019, S. 5 – 7

R6: Datenberichtigung	Begründet sich aus und dient dem Recht auf Berichtigung nach Art. 16 DSGVO und umfasst die Änderung der eigenen Daten sowie ein Interface für die Anfrage.
R7: Datenlöschung	Begründet sich aus und dient dem Recht auf das *Vergessenwerden* nach Art. 17 DSGVO und umfasst das Löschen der Daten sowie die Anfrage.
R8: Einschränkung der Datenverarbeitung	Begründet sich aus und dient dem Recht auf die Einschränkung der Datenverarbeitung und das Widerspruchsrecht nach den Art. 18 und 21 DSGVO und umfasst die eigentliche Einschränkung sowie die Anfrage.
R9: Ort der Speicherung	Umfasst den physischen Speicherort von Daten innerhalb der Architektur und begründet sich aus Art. 44 DSGVO. Einschränkungen entstehen aus E2, E5 und E8.

Einige Anforderungen werden explizit in User Stories überführt. Dies soll nach Hjerppe et al. dem Beweis dienen, dass die erhobenen Anforderungen der DSGVO auch als User Stories formulierbar sind und daher in der agilen Softwareentwicklung verwendet werden können.[94]

Ringmann et al. erheben in ihrem Beitrag wiederverwendbare technische Anforderungen für Softwareprodukte, die personenbezogene Daten verarbeiten.[95] Als Methode nutzen sie *KORA* (Konkretisierung rechtlicher Anforderungen), eine Herangehensweise, um rechtliche Anforderungen durch mehrere Phasen in technische Anforderungen für Informationssysteme zu überführen. [96] Auch Ringmann et al. sammeln ihre Anforderungen unter neun thematischen Oberbegriffen. Da für die Literaturanalyse nur die technischen Anforderungen notwendig sind, wird auf diese kurz eingegangen.

Vertraulichkeit umfasst den ersten Bereich und meint laut Ringmann et al. als Anforderungen insbesondere eine sichere Authentifizierung und Autorisierung als Grundlage für den Zugang zu personenbezogenen Daten, Zugangskontrolle und Verschlüsselung von personenbezogenen Daten. *Integrität* ist

[94] Hjerppe et al., 2019, S. 5
[95] Ringmann et al., 2018, S. 258
[96] Ringmann et al., 2018, S. 261

der zweite Bereich, in den die Limitierung von Nutzer- und Bearbeitungsrechten sowie die Sicherstellung der Datenintegrität durch Kontrollmechanismen fallen. *Verfügbarkeit* ist Bereich drei und teilt sich in die Verfügbarkeit der personenbezogenen Daten eines Betroffenen nach dem Artikel der Datenportabilität sowie der Verfügbarkeit des Gesamtsystems auf. Den Grundsatz der Zweckbindung bezieht Bereich vier mit der *Unverkettbarkeit* ein. Hier weisen die Autoren auf die Anforderung einer Dokumentationspflicht hin, wenn nicht Gründe wie etwa Profiling eine besondere Behandlung des Bereiches notwendig macht. Bereich fünf enthält den Grundsatz der *Datenminimierung* und soll daher als Funktion innerhalb der Software entweder Daten löschen, falls diese nicht mehr notwendig sind oder zumindest regelmäßig Daten identifizieren, deren Zweck erloschen sein könnte. *Transparenz* bildet Bereich sechs und stellt laut den Autoren einen der wichtigsten Ziele der DSGVO dar. In diesen Bereich fällt laut den Autoren der Grundsatz der Transparenz nach der DSGVO und damit insbesondere das Nachgehen der Nachweispflicht sowohl für Nutzer (in Form einer Datenschutzerklärung) als auch die Behörden. Die sogenannte *Intervenierbarkeit* umfasst Bereich sieben. Hinter dem Begriff verbirgt sich die Ausübung von Betroffenenrechten, was nach Ringmann et al. eine Intervention in die Datenverarbeitungsprozesse von Verantwortlichen bzw. Datenverarbeitern darstellt. Technische Anforderungen ergeben sich aus dem gesamten Prozess der Ausübung eines einzelnen Betroffenenrechts von der Anfrage bis hin zur tatsächlichen Umsetzung. Bereich acht besteht aus Anforderungen, die aus dem *Datentransfer des Verantwortlichen* resultieren. Insbesondere die Dokumentation von Datenverarbeitungen ins EU-Ausland oder zu Drittparteien, sind erforderlich, falls zutreffend. Der letzte Bereich nach Ringmann et al. ist der der *Rechtskonformität/Rechenschaftspflicht/Fairness*. Er umfasst damit vor allem die Rechenschaftspflicht in Form einer Datenschutzerklärung, dem Zweck der Datenerhebung und der technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten. Anforderungen umfassen also die konkrete Umsetzung dieser Punkte.

Als dritte Quelle für die Anforderungserhebung wird die Literaturanalyse von Huth und Matthes zu Anforderungen an technische und organisatorische Maßnahmen untersucht.[97] Der Schwerpunkt der Autoren liegt zwar bei der Bewertung unterschiedlicher Ansätze im Zusammenhang mit der Implementierung von sogenannten Privacy Pattern, aber ein Teil der Arbeit beschäftigt sich mit Anforderungen der DSGVO, die sie an ein angemessenes (Daten-)Schutzniveau im Sinne des Artikels 32 DSGVO stellt.[98] Unterschieden wird von Huth und Matthes zwischen drei Kategorien von Anforderungen: Allgemeine, die als Oberbegriff noch eine Konkretisierung benötigen, Privatsphäre-Einstellungen (vom Englischen privacy properties), die gängige Privatsphäre-Mechanismen umsetzen sollen und Anforderungen im Zusammenhang mit Betroffenenrechten. Die letzte Kategorie wird von den Autoren in ihrer Arbeit,

[97] Vgl. Huth / Matthes, 2019, S. 1
[98] Vgl. Huth / Matthes, 2019, S. 3

aufgrund der späteren Einbeziehung in Umsetzungsmethoden, nicht näher betrachtet. Aus den verbliebenen zwei Kategorien werden zwölf Anforderungen abgeleitet. *Pseudonymität*, also die fehlende Möglichkeit einer Zuordnung von personenbezogenen Daten zu einer bestimmten Person. *Unverkettbarkeit,* als Unmöglichkeit eines Angreifers zu erkennen, ob zwei Items miteinander verbunden sind oder nicht. *Zugangskontrolle/Autorisierung* soll als Zugangseinschränkung zu Informationen dienen. *Integrität* bezeichnet den Schutz der Daten vor versehentlichem Verlust, Beschädigung oder Zerstörung. *Vertraulichkeit* als Anforderung an den Schutz von personenbezogenen Daten vor unerlaubter Verarbeitung und Informationen, die nur für einen bestimmten Personenkreis zugänglich sind. *Verfügbarkeit/Zugang* beschreibt die Anforderung, dass Daten zugänglich und nutzbar für autorisierte Personen sein soll. *Datenminimierung* stellt die Anforderung an minimale Datenmengen zur Erfüllung eines bestimmten Zwecks. Die transparente Verarbeitung von personenbezogenen Daten heißt *Information/Transparenz.* Die Anforderung, dass Daten nicht länger als benötigt gespeichert werden soll, nennen die Autoren *Speicherbeschränkung*. *Zweckbindung* hebt den Grundsatz der Erhebung/Verarbeitung nur für explizite, spezifizierte und legitimierte Zwecke hervor. Die *Nachweispflicht* stellt die Anforderung an den Nachweis DSGVO-konformer Datenverarbeitung dar. Die letzte Anforderung ist die *Verschlüsselung* und damit die Unverständlichkeit von Daten für unautorisierte Personen. Abbildung 8 stellt eine Übersicht über die Anforderungen von Huth und Matthes dar.

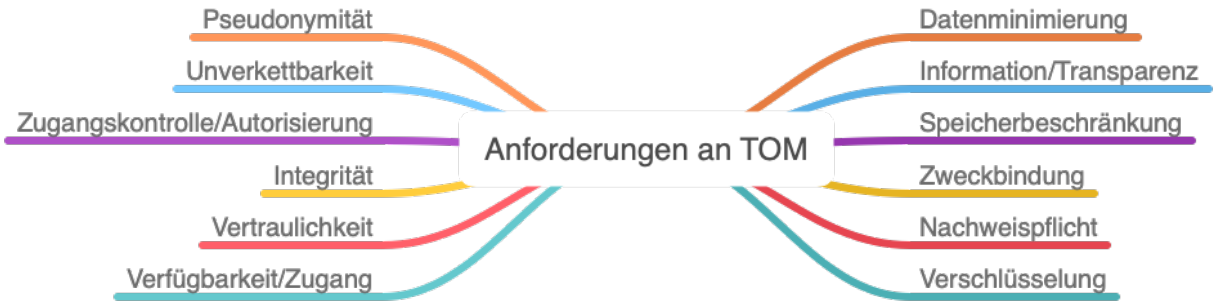

Abbildung 8: Anforderungen an technische und organisatorische Maßnahmen[99]

Die letzte betrachtete Literaturquelle ist die von Ayala-Rivera und Pasquale. In ihrer Arbeit wollen die Autoren Organisationen helfen, rechtliche Verpflichtungen der DSGVO zu verstehen und geeignete Maßnahmen zu treffen, um diese Verpflichtungen zu erfüllen.[100] Dazu verwenden sie den sogenannten *GuideMe*-Ansatz, der aus dem Bereich der Business-Analyse stammt. Als einschlägiges Werk, das den Autoren die Methoden für ihren Ansatz liefert, dient das Handbuch *Business Analysis Body of Knowledge* (BABOK).[101] BABOK beschreibt sich selbst als Sammlung von *Best Practices* im Bereich der

[99] In Anlehnung an Huth / Matthes, 2019, S. 4
[100] Vgl. Ayala-Rivera / Pasquale, 2018, S. 1
[101] International Institute of Business Analysis: A Guide to the Business Analysis Body of Knowledge (BABOK Guide), Version 2.0, 2005

Business-Analyse.[102] Die erhobenen Anforderungen von Ayala-Rivera und Pasquale unterteilen sich deshalb auch in zwei Kategorien: Business-Anforderungen und Lösungs-Anforderungen. Business-Anforderungen bilden die Ziele oder den Nutzen von Anforderungen aus Unternehmenssicht ab. Als Antwort auf den festgestellten Bedarf gibt es Lösungs-Anforderungen, die die Business-Anforderungen erfüllen sollen und eine Lösung dahingehend charakterisieren. Lösungs-Anforderungen unterteilen sich nochmals in funktionale und nicht-funktionale Anforderungen.[103]

In der ersten Phase der Literaturanalyse sind nun lediglich die Business-Anforderungen interessant, da diese die Anforderungen der DSGVO an eine Softwarearchitektur spezifizieren. Ayala-Rivera und Pasquale richten ihre Business-Anforderungen an den Grundsätzen für die Verarbeitung personenbezogener Daten aus.[104] Hinzu kommt die Forderung der DSGVO nach geeigneten technischen und organisatorischen Maßnahmen für Datenschutz durch *privacy-by-design* und *privacy-by-default*, die die Autoren als Anlass für Unternehmen zur Auseinandersetzung mit Datenschutzregeln sehen. Die Business-Anforderungen sind aus der Sicht einer Organisation geschrieben, die die Autoren repräsentativ gewählt haben.[105] Die inhaltliche Übereinstimmung zu den bisherigen Anforderungen und den Grundsätzen der Verarbeitung personenbezogener Daten ist so hoch, dass hier lediglich eine Anforderung repräsentativ betrachtet wird.

Requirement ID:	BREQ-4
Requirement Statement:	The organization must identify the specific ***purpose*** for which ***personal data*** will be processed apriori collection. The organization must only ***process*** the ***personal data*** for the specific ***purpose*** identified. The organization can carry out further processing of the obtained ***personal data*** for a secondary ***purpose*** only when this is compatible with the original ***purpose***.
Author:	Alice Brown
Revision Number:	1.0
Release Date:	14-Feb-18
Keywords:	Purpose limitation, Principle
Legal Compliance:	GDPR Art. 5.1b, Recital 39, 50

Abbildung 9: Repräsentative Business-Anforderung zu Zweckbindung[106]

Das Requirement Statement, also die Anforderungsbeschreibung, enthält Informationen zu der jeweiligen Anforderung. Für die hier dargestellte Anforderung ist demnach der Zweck der Erhebung und

[102] Vgl. International Institute of Business Analysis, 2005, S. 1
[103] Vgl. International Institute of Business Analysis, 2005, S. 5f
[104] Art. 5 DSGVO
[105] Vgl. Ayala-Rivera / Pasquale, 2018, S. 2
[106] Ayala-Rivera, Vanessa / Pasquale, Liliana: Supplementary material for paper entitled "The Grace Period Has Ended": An Approach to Operationalize GDPR Requirements, 2018, [online] https://drive.google.com/file/d/1hXmr-6OqO9G1ZfKnfnyIX0L5-7tJ30G5/view [10.07.2020]

Verarbeitung personenbezogener Daten hervorgehoben. Diesem Schema der Anforderungserhebung folgen die anderen acht Business-Anforderungen.

5.3 Ergebnis der Anforderungsanalyse

In der betrachteten Literatur werden unterschiedliche Methoden benutzt, um Anforderungen aus der DSGVO zu erheben. Wenngleich sich die Autoren dadurch in einzelnen Anforderungen unterscheiden, gibt es sehr viele Gemeinsamkeiten. Auffällig ist zum einen, dass alle Autoren die Grundsätze der Verarbeitung personenbezogener Daten, sehr eng angelehnt an die DSGVO, als Anforderungen auffassen. Während Hjerppe at al. diese in einen Themenblock *Systemsicherheit und Privatsphäre* zusammenfassen[107], liegt bei den anderen drei Quellen der Schwerpunkt der Arbeit auf den Grundsätzen der Dtaenverarbeitung und der dazugehörigen Implementierungsmöglichkeiten. Sehr eng damit verbunden ist die Gestaltung technischer und organisatorischer Maßnahmen. Diese sollen helfen die Grundsätze der Datenverarbeitung zu unterstützen.[108] Insofern kann man den Terminus *technische Anforderungen* von Ringmann et al.[109] verstehen, weil die Anforderungen in diesem Zusammenhang immer technische Auswirkungen, das heißt auf die Softwarearchitektur, haben.

Den zweiten Themenblock bildet die Rechenschaftspflicht. Zwar ist die Rechenschaftspflicht ein Teil der Grundsätze für die Verarbeitung personenbezogener Daten, aber dem Grundsatz schließen sich eine Reihe von weiteren Anforderungen an. Diese lassen sich besonders bei Hjerppe et al. nachvollziehen. Die Autoren haben zwei Kategorien namens *Einwilligungskontrolle* und *Verarbeitungsverzeichnis* eingeführt. Beide Punkte entsprechen so direkt dem Gesetzestext. In dem Gesetzestext wird explizit auf das Bestehen der Einwilligung und Verarbeitungsverzeichnisse aus Gründen des Nachweises verwiesen.[110] Trotzdem stellen die Anforderungen im Vergleich zu reinen technischen Anforderungen, bei denen teilweise die Softwarearchitektur grundlegend geändert werden muss[111], einen nicht so erheblichen Implementierungsaufwand dar. Das liegt daran, dass lediglich ein schriftliches Format für die Verzeichnisse vorgegeben ist.[112]

Der dritte Themenblock betrifft die Betroffenenrechte. Hier gehen die betrachteten Werke auseinander. Einzig Hjerppe et al. und Ringmann et al. haben in ihrer Arbeit auf die Betroffenenrechte verwiesen. Huth und Matthes haben die Betroffenenrechte explizit, aufgrund des fehlenden Wissens mit dem

[107] Vgl. Hjerppe at al., 2019, S. 5
[108] Vgl. Art. 25 Abs. 1 DSGVO
[109] Vgl. Ringmann et al, 2018, S. 261
[110] Vgl. ErwGr. 42 und 82
[111] Vgl. dazu die aufgestellten Einschränkungen von Hjerppe et al.
[112] Vgl. Art. 30 Abs. 3 DSGVO

Umgang, ausgelassen.[113] Wie aber bei Hjerppe et al. zu sehen ist[114], stellen die Anforderungen im Zusammenhang mit den Betroffenenrechte auch direkte Anforderungen an die Softwareentwicklung. Einerseits müssen die Betroffenenrechte aktiv von betroffenen Personen angefragt beziehungsweise ausgeübt werden. Die Art und Weise, in der dies geschehen muss, ist von der DSGVO nicht festgelegt. Andererseits müssen die Auswirkungen eines Betroffenenrechts umgesetzt werden können. Das heißt die Anforderungen haben auch immer eine direkte technische Komponente, zum Beispiel wenn aufgrund der Einschränkung der Verarbeitung Daten eingefroren werden müssen.

[113] Vgl. Huth / Matthes, 2019, S. 3
[114] Vgl. Hjerppe et al., 2019, S. 5

6 Erschaffen des IT-Artefaktes Anforderungskatalog aus den erhobenen Anforderungen

Die exzerpierten Anforderungskategorien und Einzelanforderungen liegen dank der Literaturanalyse vor. Damit zukünftig Softwareentwickler DSGVO-konforme Software erstellen können, müssen die Anforderungen in ein Format überführt werden, dass diesen Personenkreis unterstützt. Dafür wird in diesem Kapitel das IT-Artefakt Anforderungskatalog erschaffen.

6.1 Aufbau des Anforderungskatalogs

Im Kapitel 3.5 wurde beschrieben, warum User Stories ein geeignetes Format sind, um Anforderungen zu formulieren. Aus den genannten Gründen finden User Stories auch im Anforderungskatalog Anwendung. Bewusst soll in diesem Anforderungskatalog lediglich eine Sammlung von Anforderungen zu finden sein. Das Artefakt stellt keinen Anspruch auf eine Eins-zu-Eins-Umsetzung, schon aufgrund der fehlenden Dimension der Lösungsspezifizierung. Das bedeutet, dass eine Verwendung des Katalogs immer nur Problemfelder aufzeigt, während die eigentlichen Spezialisten, also Anforderungsmanager, Softwareentwickler und -tester, eine individuelle Lösung unter Berücksichtigung aller Umstände vorantreiben.

Der Aufbau des Anforderungskatalogs orientiert sich stark an den Erkenntnissen der Literaturanalyse. Der dreiteilige Aufbau aus technischen Anforderungen, Rechenschaftspflicht und Betroffenenrechten wird im Kern beibehalten. Trotzdem werden die letzten beiden Punkte stärker differenziert. Dies liegt vor allem an der praxisnahen Verwendung des Katalogs. Wird davon ausgegangen, dass Projektmitglieder in der Softwareentwicklung nicht alle Experten für die Datenschutzgrundverordnung sind, müssen einzelne Sachverhalte ausgiebiger erklärt werden. Dies ist ein Zweck der Unterteilung der Rechenschaftspflicht in die Unterpunkte *Einwilligung* und *Verarbeitungsverzeichnisse*. Dazu stützt sich die Praktikabilität dieser Unterteilung auf die Arbeit von Hjerppe et al. und ihrem Aufbau. Bei ihnen wurde die Herangehensweise gewählt, weil ein eigenes *Einwilligungsmanagementsystem* und *Loggingverzeichnis* der Verarbeitungstätigkeiten implementiert wurden.[115] Eine getrennte Architektur kann so auch nachvollziehbar für andere Unternehmen gewährleistet werden.

Einen ähnlichen Ansatz verfolgt die Einführung der Nutzerverwaltung und Trennung von den Betroffenenrechten. In der Nutzerverwaltung inbegriffen sind die Betroffenenrechte des Auskunftsrechts und der Datenportabilität. Ermöglicht wird dadurch ein gesicherter beziehungsweise verschlüsselter Bereich der Nutzerverwaltung, der nur verifizierten Personen den Zugang zu ihren eigenen personenbezogenen Daten erlaubt. Eine selbstständige Ausübung der beiden genannten Betroffenenrechte wird

[115] Vgl. Hjerppe et al., 2019, S. 10

so ermöglicht, ohne dass ein Prozess bei dem Verantwortlichen angestoßen werden muss. Darüber hinaus ist das Anfragen aller weiteren Betroffenenrechte vereinfacht, weil durch ein User Interface für Betroffenenrechte der Aufwand für deren Ausübung möglichst minimal gehalten werden kann. Der Bescheid über ein angefragtes Betroffenenrecht kann direkt in der Nutzerverwaltung sichtbar gemacht werden. Auf der anderen Seite kann dann eine berechtigte, autorisierte Person durch ein eigenes Interface die Betroffenenrechte bearbeiten und bekommt nur den Zugang auf die Nutzerverwaltung, der zur Entscheidung über ein Betroffenenrecht notwendig ist. Abbildung 10 zeigt sehr vereinfacht die Interpretation einer Nutzerverwaltung als mögliche Implementierung. Auch hier haben Hjerppe et al. den grundsätzlichen Denkanstoß durch ihre vorhergehende Arbeit gegeben.

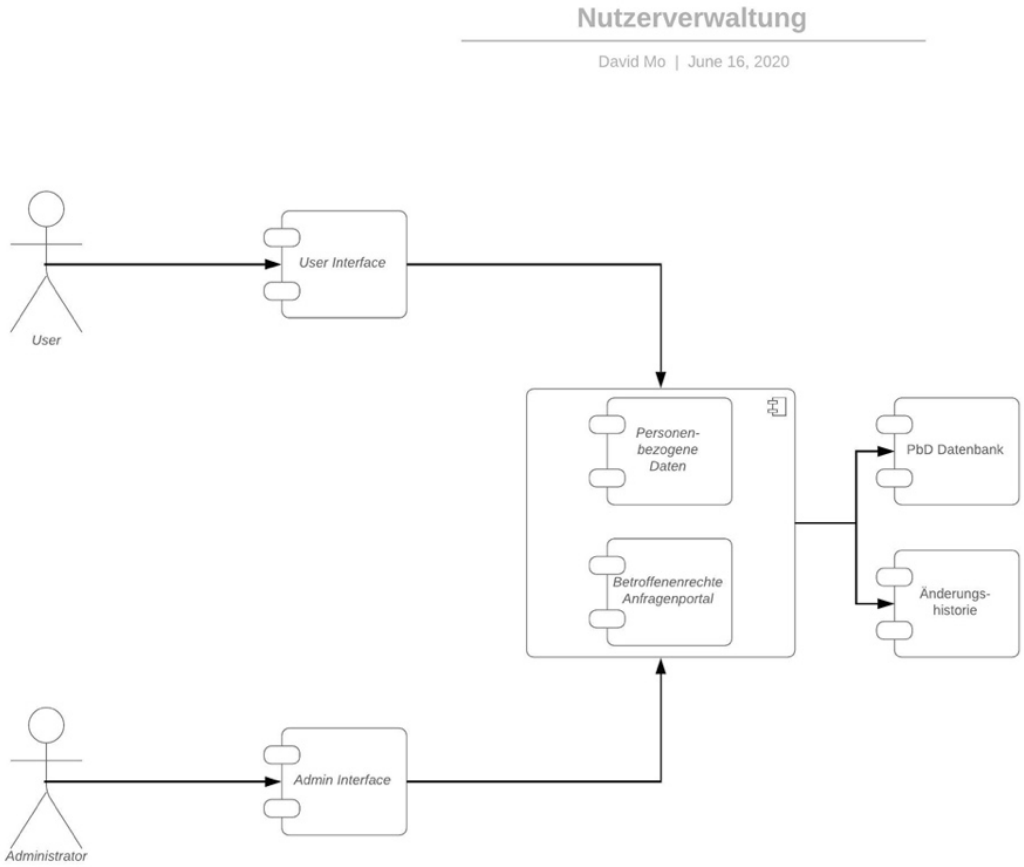

Abbildung 10: Mögliche Implementierung einer Nutzerverwaltung

Die resultierende Unterteilung des Katalogs stellt Tabelle 6 dar.

Tabelle 6: Anforderungskategorien nach ID	
ID 1.X	Technische Anforderungen an die Datenverarbeitung
ID 2.X	Einwilligung
ID 3.X	Verzeichnis über Verarbeitungstätigkeiten
ID 4.X	Nutzerverwaltung
ID 5.X	Betroffenenrechte

6.2 Verwendung des Anforderungskatalogs

Beispielhaft für die 20 Anforderungen des Katalogs soll die Betrachtung einer Anforderung sein. Diese ist in Abbildung 11 aufgeführt. Der gesamte Katalog ist im Anhang zu finden.

ID:	1.1
Name:	Vertraulichkeit
User Story:	*Als User möchte ich, dass meine personenbezogenen Daten nicht unerlaubt verarbeitet werden, damit sie geschützt sind.*
Ziel:	Vertraulichkeit
Beschreibung:	Personenbezogene Daten müssen in einer Weise verarbeitet werde, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen. (Art. 5 Abs. 1 f) Verantwortliche treffen unter Berücksichtigung der Technik, Kosten, des Umfangs, der Umstände, Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere von mit der Verarbeitung verbundenen Risiken geeignete technische und organisatorische Maßnahmen […] . (Art. 25 Abs. 1 DSGVO) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind. (Art. 32 Abs. 2 DSGVO)
Lösungskonzept:	Sichere **Authentisierungs- und Autorisierungsmechanismen** für alle Instanzen, die personenbezogene Daten speichern oder verarbeiten **Identitätsmanagement** insbesondere für den Zugang zur Nutzerverwaltung **Rollen- und Zugriffsberechtigungen**, damit nur notwendiger Personenkreis Zugriff auf notwendige Daten hat **Verschlüsselungsmethoden** von Daten

Abbildung 11: Anforderung Vertraulichkeit aus dem Anforderungskatalog

Das Muster einer Anforderung bedient sich keinem klar vorgegebenen System. Als feststehendes Element galt in der Phase der Entstehung lediglich die Verwendung von User Stories aus den angegebenen Gründen. Naheliegend ist das Anfertigen von Story-Karten, wenn User Stories verwendet werden.[116] Eine derartige Verwendung ist jedoch nicht zielführend. Der Grund dafür ist die Annahme, dass jedes Projektmitglied, egal welchen Kenntnisstand es über die DSGVO aufweist, in der Lage sein soll, den Katalog zu verwenden. Während also Story-Karten den Nutzen einer Anforderung direkt aufzeigen, indem sie User Stories verwenden, weitere Erklärungen aber auf die Konversation untereinander vertagen, sind Hintergrundinformationen zu den User Stories nicht aufgeführt. Damit die Hinzuziehung externer Berater oder die Aneignung zusätzlichen Wissens minimiert wird, enthält eine Anforderung eine Beschreibung mit den jeweils wichtigsten Passagen der DSGVO. Ziel ist es, die Basis für ein gemeinsames Verständnis einer User Story zu legen. Zusätzlich unterstützt die Erklärung einer Anforderung bei der Festlegung von Akzeptanzkriterien. Vielfach gibt die DSGVO Dimensionen einer Lösung an, zum Beispiel in der expliziten Aufführung bestimmter Informationen.[117] Um Akzeptanzkriterien zumindest aus rechtlicher Sicht zu definieren, hilft die Beschreibung der Anforderung mit den Kernpunkten der DSGVO. Das Projektteam kann sich somit mehr auf die technischen Komponenten der Akzeptanzkriterien fokussieren. Umgekehrt können in der Phase des Softwaretests eben jene aufgeführten rechtlichen Kriterien geprüft werden. Hingegen wäre eine bereits jetzt getroffene Festlegung von Akzeptanzkriterien in rechtlicher Sicht nicht umsetzbar, da an vielerlei Stellen in der DSGVO die Implementierung von technischen und organisatorischen Maßnahmen an die *Berücksichtigung der Umstände* gekoppelt ist.[118] Diese Berücksichtigung ist situativ abhängig von dem Softwareentwickler und noch viel mehr von dem jeweiligen Kunden der Software. Eine intern zu verwendende Software, die später von drei Mitarbeitern verwendet wird, weist in der Regel nicht den gleichen datenschutzrechtlichen Aufwand auf, wie eine Software, die für eine millionenfache Nutzerzahl entwickelt wurde.

Die Aufführung eines Lösungskonzeptes ist zwar für einen reinen Anforderungskatalog nicht gefordert, aber dennoch nützlich. Während der Literaturanalyse fehlte beim Identifizieren mancher Anforderungen das Verständnis darüber, wie die Anforderung zu verstehen ist. Geholfen hat, zum Beispiel bei Ringmann et al. das umgekehrte Vorgehen: dem Schließen von der Lösung auf die Anforderung. Insofern enthält das Lösungskonzept eine Sammlung von Lösungsideen aus der Phase der Literaturanalyse, wie auch Beobachtungen beziehungsweise Untersuchungen während der Fallstudie und eigene Lösungsansätze. Projektmitglieder profitieren jedoch, gerade wenn sie bis dahin mit der DSGVO weniger Berührungspunkte hatten, von Ideen, wie eine Lösung ausgestaltet werden kann. Hier kommt auch der Punkt der Sammlung von *Best Practices* zum Tragen. Das Lösungskonzept erhebt aktuell keinen

[116] Vgl. Wirdemann, 2017, S. 51
[117] Art. 6 DSGVO gibt eine Reihe von Informationen an, die einer Einwilligung vorausgehen müssen.
[118] Vgl. Art 25 Abs. 1 DSGVO

Anspruch auf Vollständigkeit oder Korrektheit. Gleichsam können innerhalb eines Unternehmens erprobte Lösungskonzepte gesammelt werden, damit sie als Bausteine immer wieder verwendet werden können. Dies spart Zeit, Geld und sichert ein gleiches Level von Qualität über Projektgrenzen hinaus.

Eine typische Verwendung eignet sich demnach insbesondere bei Erstellung des Product Backlogs durch den Product Owner, beim Sprint Planning zum Festlegen, welche Anforderungen nach welchen Kriterien im nächsten Sprint umgesetzt werden sollen und zum Testen der einzelnen Anforderung nach deren Implementierung. *Best Practices* können zu jedem Zeitpunkt dem Anforderungskatalog hinzugefügt werden. Auch im klassischen Projektmanagement kann der Anforderungskatalog projektbegleitend eingesetzt werden. Hier bietet sich die Verwendung entlang des gesamten Projektlebenszyklus an. Im Sinne der gesamtheitlichen Planung eines Projektes im traditionellen Projektmanagement sind alle Anforderungen im Zusammenhang mit der DSGVO schon in der Phase der Anforderungserhebung sichtbar und unterstützen diese. Eine Abschätzung des gesamten Projektes aus Sicht der Implementierung von DSGVO-Anforderungen wird schon zu einem sehr frühen Zeitpunkt ermöglicht.

7 Anwendung des Anforderungskatalogs bei einem IT-Dienstleister

Gemäß des konstruktionsorientierten Forschungsansatzes soll der Nutzen eines geschaffenen IT-Artefaktes gezeigt werden. Dazu eignet sich zum Beispiel eine Fallstudie[119], um das IT-Artefakt in einem realitätsnahen Kontext anzuwenden und zu evaluieren. In diesem Kapitel werden daher zuerst die Methoden der Fallstudie und qualitativen Inhaltsanalyse erklärt. Anschließend werden notwendige Informationen zu dem betrachteten Unternehmen geliefert, damit die Fallstudie eingeordnet werden kann. Sodann wird die Fallstudie durchgeführt und mittels qualitativer Inhaltsanalyse die getätigten Interviews ausgewertet.

7.1 Methodik der durchgeführten Fallstudie

Yins Case Study (zu deutsch: Fallstudie) ist eine Methode, die vor allem im Bereich der Sozialwissenschaft gängig ist. Sie eignet sich insbesondere als empirische Untersuchung, wenn es sich um eine Forschungsfrage mit *wie?* oder *warum?* handelt und wenn ein aktuelles, realexistierendes Phänomen untersucht werden soll und die Grenzen zwischen Phänomen und seinem Umfeld nicht klar abgrenzbar sind.[120] Die Forschungsfrage enthält eben jene Frage nach dem „*Wie* lassen sich die Anforderungen der DSGVO in der Softwareentwicklung implementieren?“ und die Aktualität im Umgang mit der DSGVO ist nach ihrer Einführung ebenfalls gegeben. Schlögel und Tomczak identifizieren aus bestehenden Arbeiten drei Untersuchungssituationen, in denen die Fallstudie einen maßgeblichen Erkenntnisbeitrag liefert. Die Situation, die dieser Forschung zugrunde liegt, ist dabei die der starken Beeinflussung des Erkenntnisobjektes durch menschliches Verhalten, insbesondere im Umgang spezifischer Phänomene des Managements bestimmter Unternehmensherausforderungen.[121] Diese Situation begründet sich aus dem Umgang mit dem Anforderungskatalog im Kontext der Softwareentwicklung. Eines der Ziele von User Stories ist die Anregung der Kommunikation zwischen allen Projektbeteiligten.[122] Die User Stories implizieren keine einheitliche Lösung, sondern zeigen die Dimension einer Lösung auf, die durch Erfahrung und Wissen der Projektmitglieder und der technischen Komponente in eine situationsspezifische Lösung umgewandelt werden soll. Der Prozess ist also, wie dargelegt, von der Komponente Mensch und der verfügbaren Technik abhängig.

Für die weitere Bearbeitung der Fallstudie werden die fünf Phasen aus Abbildung 12 durchlaufen.

[119] Vgl. Dazu die “Sechs Aktivitäten der Design Science Research Methodology“ aus Kapitel 4
[120] Vgl. Yin, Robert K.: Case Study Research Design and Methods, 3. Aufl., Thousand Oaks, USA: SAGE Publications, 2003, S. 13
[121] Vgl. Schlögel, Marcus / Tomczak, Torsten: Fallstudie, in: Baumgarth, Carsten / Eisend, Martin / Evanschitzky, Heiner (Hrsg.), Empirische Mastertechniken – Eine anwendungsorientierte Einführung für die Marketing- und Managementforschung, Wiesbaden: Gabler, 2009, S. 83
[122] Vgl. Cohn, Mike, 2004, S. 154

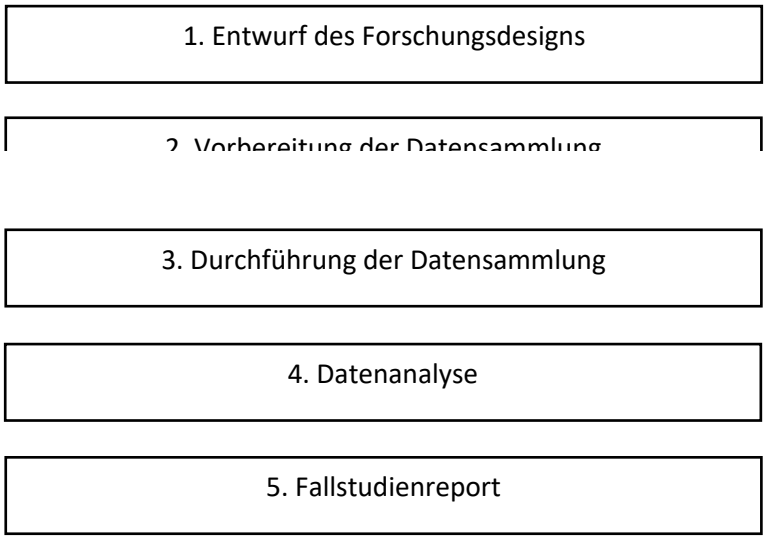

Abbildung 12: Forschungsprozess einer Fallstudie[123]

1. **Entwurf des Forschungsdesigns:** Das verwendete Forschungsdesign wird das der Einzelfallstudie sein. Nach Yin eignet sich das Design besonders, wenn ein repräsentativer oder typischer Fall untersucht werden soll.[124] Zusätzlich wird eine Entscheidung bezüglich der Analyseebene getroffen. Weil innerhalb dieser Fallstudie ein Kontext betrachtet wird, der genau eine Forschungsfrage beantworten soll, ist die holistische, also ganzheitliche Analyseebene, die getroffene Wahl.[125] Diese beiden Annahmen wurden getroffen, weil der Anforderungskatalog möglichst repräsentativ für die Branche der Softwareentwicklung sein soll und auf Einzelfragestellungen innerhalb der Fallstudie verzichtet wird. Das Ergebnis soll eine repräsentative Bewertung des Anforderungskatalogs innerhalb eines Projektteams darstellen.
2. **Vorbereitung der Datensammlung:** Unterschiedliche Einflussfaktoren haben eine Auswirkung auf die Qualität der Fallstudie. Nennenswerte Punkte sind in diesem Zusammenhang das Hintergrundwissen des Durchführenden, die Fähigkeit gut zuzuhören und flexibel auf neue Situationen einzugehen sowie das gewählte Vorgehen.[126] Durch die getätigte Literaturanalyse wird das Hintergrundwissen des Durchführenden sichergestellt. Das Vorgehen entspricht einem Leitfaden, der für das anschließende Interview verwendet wird.
3. **Durchführung der Datensammlung:** Ein Experteninterview dient als Datenerhebungsverfahren innerhalb der Fallstudie. Nach Yin sind Vorteile eines Interviews, dass ein direkter Bezug zu dem Thema der Fallstudie möglich ist und es aufschlussreich ist, da es kausale Schlüsse zulässt.[127] Dem entgegen können ungenaue Fragen oder subjektive Antworten die Untersuchung

[123] Schlögel, Tomczak, 2009, S. 86
[124] Vgl. Yin, 2003, S. 41
[125] Vgl. Yin, 2003, S. 43
[126] Vgl. Yin, 2003, S. 59
[127] Vgl. Yin, 2003, S. 86

verzerren, ebenso wie eine schlechte Wiedergabe oder der Umstand, dass Befragte genau das antworten könnten, was der Interviewer hören will.[128] Da menschliches Verhalten im Umgang mit dem Anforderungskatalog in der Fallstudie beobachtet werden soll, macht es Sinn, Menschen zum zentralen Untersuchungsobjekt zu machen. Experteninterviews greifen auf Experten mit „spezifischem Rollenwissen zurück, die solches zugeschrieben bekommen und eine darauf basierende besondere Kompetenz für sich selbst in Anspruch nehmen".[129] Die Einteilung der drei Befragten in die Kategorie *Experte* erfolgt aufgrund der täglichen Tätigkeit in ihrem jeweiligen Gebiet und der Berufserfahrung, die sie mitbringen. Ein neutraler und breiter Blick, wie von einem Experteninterview im Gegensatz zum reinen Leitfadeninterview[130] gefordert, wird aufgrund der Auswahl der befragten Personen durch den Durchführenden vorausgesetzt.

4. **Datenanalyse:** Da es sich um einen qualitativen Inhalt handelt, der durch ein Interview gewonnen wird, wird zur Analyse die qualitative Inhaltsanalyse verwendet. Sie orientiert sich an der Paraphrasierung von Kommunikationsinhalten zwischen dem Durchführenden und den Interviewten. In Anlehnung an Mayring[131] wird dabei ein strukturiertes Vorgehen gewählt, das heißt vorab Kategorien entwickelt, denen dann mittels fester Kodierung Inhalte des Interviews zugeordnet werden können. Das Ergebnis ist eine mehrstufige Intensitätsanalyse, mittels derer die Meinung zu unterschiedlichen Kategorien validiert werden kann.
5. **Fallstudienreport:** Die Darstellung der Ergebnisse erfolgt im eigenen Kapitel Ergebnisse (Kapitel 8). In diesem soll abschließend gezeigt werden, ob der zusammengestellte Anforderungskatalog die Softwareentwicklung bei der Entwicklung DSGVO-konformer Software unterstützt.

7.2 Das Unternehmen der Fallstudie

Bei dem betrachteten Unternehmen handelt es sich um einen IT-Dienstleister aus dem Raum Niedersachsen. Als Teil einer Unternehmensgruppe, die deutschlandweit und in einigen Ländern der EU Standorte unterhält, ist ihr Kundenstamm eng verbunden mit der Wahl des Standortes. Wenngleich die Unternehmensgruppe in den Bereichen Öffentlicher Sektor, Versicherungen, Banken oder Health-Science unterwegs ist, werden in dem betrachteten Unternehmensteil, aufgrund der Nähe zu einem namenhaften Automobilhersteller in Niedersachsen, überwiegend IT-Dienstleistungen für die Automobilbranche angeboten. Das angebotene Spektrum an Produkten und Dienstleistungen umfasst

[128] Vgl. Yin, 2003, S. 86
[129] Vgl. Przyborski, Aglaja / Wohlrab-Sahr, Monika: Qualitative Sozialforschung, München: Oldenbourg, 2008, S. 133
[130] Vgl. Baur, Nina / Blasius, Jörg: Methoden der empirischen Sozialforschung, in: Baur, Nina / Blasius, Jörg (Hrsg.), Handbuch Methoden der empirischen Sozialforschung, Wiesbaden: Springer, 2014, S. 53
[131] Mayring, Philipp: Qualitative Inhaltsanalyse, in: Boehm, A. / Mengel, A. / Muhr, T (Hrsg.), Texte verstehen: Konzepte, Methoden, Werkzeuge, Konstanz: UVK Univ.-Verl. Konstanz, 1994, S. 159 - 175

Standard- und Individualsoftware, SAP-Lösungen, Mobil- und Webapplikationen, Datenbankentwicklungen, aber auch strategische Gesamtkonzepte der IT-Landschaft im Unternehmen und Schulungsangebote.

Der relevante Ausschnitt, auf den sich die Fallstudie bezieht, beschäftigt sich mit einem Projekt innerhalb des Unternehmens. Das Projekt begleitet den Produktlebenszyklus eines Webtools, das innerhalb der Automobilbranche eingesetzt wird. Intern wird das Projekt als Bestandsprojekt tituliert, weil es ständig durch Feedback des Kunden erweitert wird und somit das Tagesgeschäft um die Bereiche Anforderungsmanagement, Softwareentwicklung, Test und Wartung und Support ausgerichtet ist. Insofern bedient es nicht die klassischen zeitlichen Grenzen eines Projektes und schränkt deshalb die Validierung des Anforderungskatalogs entlang eines Projektlebenszyklus ein. Infolge der Verbreitung des Virus Covid-19 und seiner wirtschaftlichen Folgen wurde das Budget für das Projekt gekürzt und mehrere Projektmitglieder von dem Projekt abgezogen. Vorhandene Ideen des Managements die DSGVO stärker in das Projekt zu integrieren, wurden auf Eis gelegt. Zurzeit wird demnach nur noch der Bereich Wartung und Support bedient.

7.3 Ablauf der Experteninterviews

Ein Experteninterview gehört zur Kategorie der Leitfadeninterviews, also zu semi-strukturierten Erhebungsformen verbaler Daten.[132] Voraussetzung für ein solches Interview ist der Erstellung eines Leitfadens. Dieser erfüllt die Funktion eines roten Fadens und damit der thematischen Rahmung und Fokussierung, Auflistung aller relevanter Themenkomplexe des Interviews, Vergleichbarkeit der Daten und Strukturierung des Kommunikationsprozesses.[133] Für die Erstellung des Leitfadens ist in erster Linie das Aufstellen der leitenden Forschungsfrage und darauf abgeleiteten Hypothesen wichtig.[134] Sie dienen zur Festlegung Fragen innerhalb des Interviews. Die leitende Forschungsfrage ist weiterhin die Forschungsfrage dieser Arbeit:

„Wie lassen sich die Anforderungen der DSGVO in der Softwareentwicklung implementieren?“

Daraus resultieren folgende zwei Hypothesen:

1) Es existiert in der Unternehmenspraxis kein Leitfaden zur DSGVO-konformen Erstellung von Software auf Projektebene.
2) Das erstellte IT-Artefakt Anforderungskatalog unterstützt Softwareentwicklungsteams bei der Erstellung DSGVO-konformer Software.

[132] Vgl. Misoch, Sabina: Qualitative Interviews, 2. Aufl., Berlin: De Gruyter Oldenbourg, 2019, S. 65
[133] Vgl. Misoch, 2019, S. 67
[134] Vgl. Mieg, Harald A. / Näf, Matthias: Experteninterviews, 2. Aufl., Institut für Mensch-Umwelt-Systeme (HES), Schweiz, Zürich: ETH Zürich, 2005, S. 12

Mit der ersten Hypothese lässt sich bestätigen, ob der Anforderungskatalog die Voraussetzung an ein neues, einzigartiges IT-Artefakt in einem erheblichen Problemfeld, im Sinne des konstruktionsorientierten Forschungsansatzes, erfüllt. Die zweite Hypothese soll sodann validieren, ob der Anforderungskatalog ein adäquates Mittel zur Beseitigung des Problemfelds ist.

Die Wahl der Experten wurde schon kurz umrissen. Es wird jeweils ein Anforderungsmanager, ein Entwickler und ein Softwaretester aus dem Unternehmen der Fallstudie befragt. Die Gesprächspartner sind repräsentativ für beteiligte Personen an einem Softwareentwicklungsprojekt. Mit ihrer Erfahrung und ihrem Wissen können sie beurteilen, ob gängige Lösungen für Hypothese 1 existieren und auch einschätzen, ob der erstellte Anforderungskatalog ihnen, und damit im besten Fall auch weiteren Softwareentwicklern, im Sinne der Hypothese 2 bei der Erstellung von Software helfen kann. Aus Gründen des Datenschutzes und dem Schutz von Betriebsgeheimnissen werden alle identifizierbaren Daten, insbesondere der Name der Interviewpartner, der Name des Unternehmens, der Name des Kunden und der Name des Projektes, generalisiert.

Die Struktur des Leitfadens orientiert sich am Aufbau von Misoch.[135] In der *Informationsphase* wird der Befragte über die durchgeführte Studie aufgeklärt. In der *Aufwärmphase* soll durch eine Eingangsfrage nach Art der Tätigkeit und Dauer der Zugehörigkeit zum Unternehmen der Einstieg in das Gespräch erleichtert werden. Die *Hauptphase* soll dann die Fragen zur Beurteilung der Hypothesen enthalten. Tabelle 7 zeigt die Fragen, die in diesem Zusammenhang gestellt werden.

Tabelle 7: Fragen während des Experteninterviews	
Frage 1:	Wie viel Vorwissen über die DSGVO ist vorhanden? Durch welches Medium?
Frage 2:	Wie wird die DSGVO in der Software aktuell implementiert?
Frage 3:	Wie kann die Implementierung verbessert werden?
Frage 4:	Kann der Anforderungskatalog die Softwareentwicklung unterstützen? Wenn ja, wie?
Frage 5:	Welche Verbesserungsvorschläge gibt es für den Anforderungskatalog?

Diese Fragen werden während des Interviews in der gegebenen Reihenfolge gestellt. Die semi-strukturierte Herangehensweise ermöglicht darüber hinaus eine thematische Vertiefung der jeweiligen Fragen durch weiteres Nachfragen oder aber die Flexibilität, andere zusätzliche Fragen zu stellen, insofern

[135] Vgl. Misoch, 2019, S. 68

sie als zielführend erachtet werden. Die *Abschlussphase* dient der Reflektion des Interviews und ermöglicht weitere, ungebundene Aussagen zu treffen, falls vom Befragten gewünscht.

Die Fragen folgen dem gewählten Kategoriensystem für die qualitative Inhaltsanalyse. Das bedeutet, dass die Fragen und deren Antworten eine Kategorie betreffen, die anschließend qualitativ ausgewertet wird. Frage 1 ist der Kategorie *Vorwissen DSGVO* zuzuordnen. Die Frage 2 der Kategorie *IST-Zustand Softwareentwicklung*. Frage 3 beschäftigt sich mit dem *SOLL-Zustand Softwareentwicklung* und bildet diese Kategorie ab. Die drei Fragen und Kategorien bilden inhaltlich die Grundlage zur Validierung der aufgestellten Hypothese 1. Die Fragen 4 und 5 spannen die Kategorie *Evaluation Anforderungskatalog* auf und bilden die Grundlage zur Validierung der Hypothese 2.

7.4 Ergebnisse der Interviews

Zuerst hat jeder einzelne Interviewpartner im Rahmen der Aufwärmphase sein Tätigkeitsfeld aufgezeigt, damit anschließend gezielte Nachfragen in Verbindung mit der DSGVO möglich waren. Eine Übersicht enthält Tabelle 8.

Tabelle 8: Eigene Vorstellung durch die Interviewpartner	
Person A:	Anforderungsmanager/Projektleiter des besprochenen Projekts, seit knapp drei Jahren im Unternehmen, Erfahrung auch als Consultant
Person B:	Java-Softwareentwickler, Erfahrung auch als Consultant im Bereich IT-Architektur
Person C:	Testmanager im besprochenen Projekt, seit sechs Jahren im Unternehmen tätig

Ein fundiertes Vorwissen über die DSGVO ist nicht vorhanden. Zwar wurde im Unternehmen eine Schulung durchgeführt, diese umfasste allerdings nur wenige Stunden.

„Wenn ich Schulung sage, dann meine ich sowas wie eine zwei, drei Stunden Remoteschulung“[136]

Der überwiegende Teil des Wissenszugangs erfolgte privat durch externe Berichterstattung. Dies wird unter anderem auch damit begründet, dass in der täglichen Arbeit die Überschneidungspunkte noch wenig sind. Ein wirklicher Anlass zur tiefergehenden Auseinandersetzung mit der DSGVO wurde bisher noch nicht gesehen.

„Also eigentlich sind bisher noch keine Überschneidungspunkte, wo es für mich darum ging, da tiefer in die Materie einzusteigen“[137]

[136] Anhang Interview Person A, S. 87, Zeitmarke [0:03:58]
[137] Anhang Interview Person B, S. 93, Zeitmarke [0:03:02]

Dies nimmt auch schon den überwiegenden Teil von Frage 2 vorweg. Wenngleich das derzeitige Projekt, respektive das Webtool, nicht mit technischen oder organisatorischen Maßnahmen versehen ist, die es DSGVO-konform machen sollen, ist dies für die Zukunft angedacht.

„Wir haben durchaus vor dieses Ding DSGVO-konform zu machen“[138]

Dafür gibt es in Teilen schon eine Analyse, die intern durchgeführt wurde. Aus Sicht von Person B ist das Resultat der Analyse, dass die DSGVO nicht angewandt werden kann, da ein Personenbezug für die Nutzung des Webtools benötigt wird. Person C hat diesen Personenbezug unter anderem in der Testumgebung, die vom Kunden mit Daten gespeist wird.

„Allerdings wurde da quasi mehr oder weniger beschlossen, dass aufgrund der fachlichen Notwendigkeit […], es quasi nicht möglich sei, genauer die DSGVO bei uns umzusetzen“[139]

„In der Umgebung des Automobilherstellers haben die Daten mehr oder weniger einen Personenbezug, weil es anders auch gar nicht zu testen ist“[140]

Nicht nur auf das Projekt selbst bezogen, sondern im Allgemeinen, wird die Erstellung DSGVO-konformer Software als Zusatzfeature gesehen. Einerseits als Qualitätsmerkmal des IT-Dienstleisters selbst, um Projekte zu akquirieren, andererseits soll der zusätzliche Aufwand auch vergütet werden.

„Aber auf der anderen Seite machen wir natürlich auch ein bisschen Druck, damit wir Projekte akquirieren und da dann halt noch einen Zusatzumsatz generieren“[141]

Insofern sind eine wirtschaftliche Relevanz und ein Praxisproblem erkennbar. Bezogen auf die eingangs aufgestellte Hypothese 1 hat sich gezeigt, dass diese vollumfänglich zutrifft. Innerhalb des betrachteten Projekts äußert sich dies durch fehlendes Vorwissen im Umgang mit der DSGVO, wie auch einer fehlenden Integration der DSGVO in der Softwareentwicklung. Dadurch existiert auf IST-Ebene kein Leitfaden zur Herstellung DSGVO-konformer Software.

Alle drei Interviewpartner haben sich eher positiv über den Anforderungskatalog geäußert. Hervorgehoben wird der strukturierende Charakter des Anforderungskatalogs. Als strukturierend wird dabei von Person A empfunden, dass er in der Phase der Anforderungserhebung alle DSGVO-relevanten Punkte aus dem Katalog ableiten und in eine Planung für ein Produkt integrieren kann. Dazu dient der Katalog im Gespräch mit potenziellen Kunden als Gesprächsgrundlage und Vorzeigeobjekt.

[138] Anhang Interview Person A, S. 88, Zeitmarke [0:06:02]
[139] Anhang Interview Person B, S. 93, Zeitmarke [0:03:58]
[140] Anhang Interview Person C, S. 99, Zeitmarke [0:05:50]
[141] Anhang Interview Person A, S. 88, Zeitmarke [0:06:02]

„Wenn ich jetzt aber beispielsweise diesen Katalog hätte, dann könnte ich mir diese Zettelchen direkt nehmen und an diese Story-Map hängen“[142]

„Gleichzeitig kann das aber natürlich auch eine Gesprächsgrundlage sein, wenn man in ein Gespräch mit dem Kunden geht […]“[143]

Person B empfindet den informativen Charakter des Anforderungskatalogs als vorteilhaft. Zum einen als vorgegebene Struktur zum Entlanghangeln, zum anderen zum Überprüfen, ob jegliche relevante Punkte beachtet wurden. Dazu hilft ihm als Softwareentwickler das Lösungskonzept, in dem es Denkanstöße zur Realisierung gibt.

„Naja also der Katalog bildet ja schon mal so eine gewisse Struktur ab, die man so ein bisschen abarbeiten kann“[144]

„Da hat man mit deinem Lösungskonzept auch immer schon echt gute Hinweise gegeben, wie man das eventuell umsetzen könnte“[145]

User Stories würden nach Einschätzung von Person B helfen, dass trotz fehlendem Vorwissen die Anforderung gut verstanden wird. Dabei hilft auch die zusätzliche Beschreibung aus dem Gesetzestext.

„Also der kleine Text der User Stories ist echt schon sehr gut und verständlich beschrieben“[146]

„Zusätzlich hilft dazu ja immer noch die Beschreibung aus dem Gesetzestext sozusagen“[147]

Person A hatte schon erwähnt, dass er eine Verwendung insbesondere am Anfang eines Projekts sieht. Person C hebt dies explizit hervor.

„Also ich glaube, dass es tendenziell eher am Anfang nützlich ist oder wenn das Thema eben aufkommt“[148]

„Für mich ist das ein kompletter Zyklus“[149]

Eine selektive Verwendung erachtet Person C dementsprechend als nicht sinnvoll. Person C lobt den Realismus der Anforderungen, unterstreicht aber aus dem Blickwinkel des Softwaretests, dass die generischen User Stories schwierig zu testen seien.

[142] Anhang Interview Person A, S. 89, Zeitmarke [0:09:33]
[143] Anhang Interview Person A, S. 89, Zeitmarke [0:09:33]
[144] Anhang Interview Person B, S. 94, Zeitmarke [0:07:41]
[145] Anhang Interview Person B, S. 94, Zeitmarke [0:07:41]
[146] Anhang Interview Person B, S. 94, Zeitmarke [0:08:48]
[147] Anhang Interview Person B, S. 94, Zeitmarke [0:08:48]
[148] Anhang Interview Person A, S. 90, Zeitmarke [0:13:08]
[149] Anhang Interview Person C, S. 100, Zeitmarke [0:08:05]

„Sowas ist schwer nachzuvollziehen oder zu testen. Da sind viele Variablen drin“[150]

Damit lässt sich aus dem Gespräch mit Person C besonders hervorheben, dass eine Einzelfallbetrachtung notwendig ist, wenn es um die Beurteilung des Katalogs geht. Der Katalog entfaltet für ihn erst seine Wirkung, wenn er in einen projektspezifischen Kontext gebracht wurde.

„Das ist halt immer sehr abhängig von der Applikation“[151]

Grundsätzliche Verbesserungsvorschläge gibt es wenig. Person A meint, dass Best Practices integriert werden könnten. Ansonsten sind die Interviewpartner zufrieden mit dem Anforderungskatalog und würden sich nur mehr Praxiserfahrung wünschen.

„Ja, genau [der Katalog sollte in der Praxis erprobt werden]. Es wird sich auch ziemlich schnell zeigen, wo es Probleme geben könnte. Da kriegt man recht schnell Feedback“[152]

Möchte man die Meinung der Befragten zum Katalog quantifizieren, damit eine Validierung der Hypothese möglich ist, kann man die Meinungen auf einer Skala abbilden. Diese enthält die Werte *negativ*, *mittel* und *positiv*, wobei damit kritisch das Gesagte zum Katalog einbezogen werden soll. Rein positive Antworten sorgen für die Einordnung in die Rubrik *positiv*. Keine rein positiven oder negativen Antworten sorgen für eine Einordnung in die Rubrik *mittel*, während rein negative Antworten zu einer Einordnung in *negativ* führen. Nimmt man diese Kodierung und wendet sie hier an, ergibt sich für die einzelnen Personen folgendes Stimmungsbild, anhand von Tabelle 9.

[150] Anhang Interview Person C, S. 100, Zeitmarke [0:10:56]
[151] Anhang Interview Person C, S. 101, Zeitmarke [0:14:32]
[152] Anhang Interview Person B, S. 96, Zeitmarke [0:13:16]

Tabelle 9: Quantifizierung der Antworten		
Person	**Aussagen**	**Einordnung**
A	„Also ja, auf jeden Fall [kann der Katalog die Softwareentwicklung unterstützen]“ „Spontan aus dem Bauch heraus würde ich sagen nein [zu dem Nutzen einer Verwendung im täglichen Berufsalltag]“	mittel
B	„Von daher finde ich deinen Katalog schon ziemlich gut“ „Meiner Meinung nach ja [der Katalog wäre hilfreich bei der Erstellung DSGVO-konformer Software]“	positiv
C	„Grundsätzlich ja [der Anforderungskatalog kann den Projektlebenszyklus unterstützen]“ „Sowas ist schwer nachzuvollziehen oder zu testen“	mittel

Dies bestätigt, dass der Anforderungskatalog die Softwareentwicklung unterstützen kann. Obwohl auch Einschränkungen und Probleme des Anforderungskatalogs für den Arbeitsalltag ausgemacht werden, empfinden die einzelnen Interviewpartner unterstützende Elemente und sind eher positiv eingestellt. Die Hypothese 2 kann demnach verifiziert werden.

8 Schluss

8.1 Zusammenfassung und Fazit

Die noch junge Einführung der Europäischen Datenschutzgrundverordnung sorgt weiterhin für ein Spannungsfeld zwischen rechtlichen Anforderungen an den Datenschutz und bereitgestellter Software durch IT-Unternehmen. Vielfach existieren in Unternehmen schon Ansätze oder sogar Komplettlösungen, um die DSGVO im Unternehmen einzuhalten. Auf der operativen Ebene der Softwareentwicklung in Projekten sind diese allerdings vielfach noch nicht eingearbeitet.

Diese Forschungsarbeit hat ein Werkzeug erschaffen, mit dem die vorhandene Lücke geschlossen werden könnte. Dazu teilt sich die Arbeit in zwei Schwerpunkte auf. Der erste Schwerpunkt ist die Identifizierung der Anforderungen, die die DSGVO an die Softwareentwicklung stellt. Aufgrund bereits vorhandener Literatur in diesem Themengebiet, wurden Anforderungen aus der Literatur exzerpiert und für die eigene Arbeit strukturiert. In diesem Zusammenhang gibt es drei Arten von Anforderungskategorien. Die erste Kategorie umfasst alle Anforderungen, die vorwiegend die Grundsätze der Verarbeitung personenbezogener Daten beinhalten. Diese sind überwiegend technischer Natur und haben eine Auswirkung auf die Ausgestaltung der Softwarearchitektur. Die zweite Kategorie umfasst die Rechenschaftspflicht der DSGVO und dient dem Nachweis von Verarbeitungswegen und Einwilligungen zur Verarbeitung von Daten. Die dritte Kategorie umfasst die Betroffenenrechte, die die DSGVO Personen zuspricht, von denen personenbezogene Daten verarbeitet werden. Auswirkungen der Betroffenenrechte haben auch immer eine technische Komponente und spielen eine wichtige Rolle bei der Anforderungserhebung.

Es wurde dann mit den Erkenntnissen der Anforderungserhebung ein Anforderungskatalog erschaffen. Darin wurden die gebildeten Kategorien aus der Literaturanalyse übernommen und alle betreffenden Anforderungen beigefügt. Um die Anforderungen zu formulieren, fiel die Wahl auf User Stories. User Stories sind eine Variante der Formulierung von Anforderungen, die die Kommunikation innerhalb eines Projekts unterstützt und sich gut an den jeweiligen Projektkontext anpassen lässt. Im Rahmen der Fallstudie wurde die Wahl von User Stories durch die Interviewpartner bestätigt und für die Praxis als nützlich bewertet. Den Aufbau des Anforderungskatalogs runden eine Beschreibung durch die wichtigsten, betreffenden Passagen der DSGVO und ein beispielhaftes Lösungskonzept ab. Auch diese Struktur wurde im Nachhinein innerhalb der Fallstudie als unterstützendes Element zur Integration in ein Projekt und Anwendung im Rahmen der Softwareentwicklung empfunden.

Im letzten Schritt der Forschungsarbeit wurde der durch theoretisches Wissen gewonnene Anforderungskatalog auf seine Praxistauglichkeit überprüft. Dazu wurden Interviewpartner eines IT-Dienstleisters ausgewählt, die repräsentativ unterschiedliche Rollen innerhalb eines

Softwareentwicklungsteams einnehmen: Anforderungsmanager, Softwareentwickler und -tester. Im Rahmen der Fallstudie sollten zwei wichtige Hypothesen für die Verwendung einer konstruktionsorientierten Forschungsmethodik, die für die Erstellung des Anforderungskatalogs Grundlage war, geklärt werden. Es musste ein für die Praxis relevantes Problemfeld identifiziert werden und validiert werden, ob der Anforderungskatalog die Lösung dieses Problems unterstützt.

Die erste Hypothese konnte vollumfänglich bestätigt werden: Ein Leitfaden für die Erstellung DSGVO-konformer Software existiert in dem betrachteten Unternehmen noch nicht. In der Praxis ist die DSGVO nur rudimentär in der Softwareentwicklung angekommen. Der betrachtete IT-Dienstleister hat zwar schon Analysen zur Erstellung DSGVO-konformer Software angetrieben, über diese Phase hinaus sind allerdings noch keine Maßnahmen vollzogen worden. Zum einen wurde durch die Interviewpartner herausgestellt, dass Bestandsprojekte sich schwierig anpassen lassen, wenn sie schon im Gange sind. Tiefgreifende Veränderungen, wie sie die Anforderungen der DSGVO auf die Softwareentwicklung teilweise voraussetzen, bedingen die ganze IT-Infrastruktur einer Software. Zum anderen fehlt Vorwissen im Umgang mit der DSGVO und ein dahingehender Aufwand zur Erstellung DSGVO-konformer Software wird eher als Zusatzfeature gesehen, das vom Kunden auch gewollt sein muss.

Die zweite Hypothese, dass der Anforderungskatalog die Softwareentwicklung unterstützen kann, konnte nicht gänzlich bestätigt werden. Die Meinung der Interviewpartner war überwiegend positiv. Hervorgehoben wurde die ordnende Struktur des Katalogs, insbesondere im Rahmen der Anforderungserhebung eines Projekts und als Checkliste im Rahmen der Entwicklung, der Nutzen einer durchgehenden Verwendung während des gesamten Projektlebenszyklus wurde aber zumindest angezweifelt. Hier konnte auch durch die Begleitumstände der Praxis, das untersuchte Projekt wurde im Rahmen der Covid-19 Pandemie sehr weit beschränkt, nur auf den Erfahrungsschatz der Interviewpartner zurückgegriffen werden, ohne dass eine tatsächliche Anwendung des Katalogs stattgefunden hätte.

Die Forschungsfrage wurde mithilfe des Anforderungskatalogs trotzdem beantwortet. Der Anforderungskatalog hat sich als ein Mittel erwiesen, um die DSGVO in der Softwareentwicklung zu implementieren. Dieser Fakt wurde auch durch die Interviewpartner bestätigt.

8.2 Ausblick

Im Rahmen der Forschungsarbeit wurde nur innerhalb eines IT-Dienstleisters die Verwendung des Anforderungskataloges validiert. Um seine Eignung für eine größere Bandbreite zu überprüfen und eine kontinuierliche Verbesserung einzuarbeiten, sollte der Katalog auch weiteren IT-Dienstleistern und Softwareentwicklern zur Verfügung gestellt werden. Mithilfe dieser breit angelegten Forschung kann untersucht werden, ob vom theoretisch angelegten Anforderungskatalog auch andere Unternehmen in der Praxis profitieren können.

Dazu werden sicherlich auch Erfahrungsberichte nötig sein, die bei der Verwendung des Katalogs während eines gesamten Projektlebenszyklus gemacht werden, das heißt: Von der Phase der Initiierung des Projektes bis hin zum Abschluss. Damit könnte sich klären lassen, ob der Katalog die Softwareentwicklung auch im weiteren Verlauf eines Projekts unterstützen kann. Zusätzlich hat der Anforderungskatalog den Anspruch durch *Best Practices* zu wachsen und eine noch bessere Verwendung zu ermöglichen. In diesem Zuge muss genau das beobachtet werden und validiert werden, ob der Katalog bei einer zyklischen Verwendung innerhalb eines Unternehmens gar als Standardwerk bei der Implementierung von Lösungskonzepten mit DSGVO-bezug dienen kann.

Literaturverzeichnis

Angermeier, Dr. Georg: Traditionelles Projektmanagement, in: Projektmanagementmagazin, 2014, [online] https://www.projektmagazin.de/glossarterm/traditionelles-projektmanagement [20.03.2020]

Ayala-Rivera, Vanessa / Pasquale, Liliana: "The Grace Period Has Ended": An Approach to Operationalize GDPR Requirements, in: 2018 IEEE 26th International Requirements Engineering Conference (RE), 2018

Ayala-Rivera, Vanessa / Pasquale, Liliana: Supplementary material for paper entitled "The Grace Period Has Ended": An Approach to Operationalize GDPR Requirements, 2018, [online] https://drive.google.com/file/d/1hXmr-6OqO9G1ZfKnfnyIX0L5-7tJ30G5/view [10.07.2020]

Bättig, Peter: Projektmanagement Erfolgsfaktoren für erfolgreiche Projekte, in: Fachbibliothek, 2012, [online] https://www.fachbibliothek.ch/projektmanagement-erfolgsfaktoren-erfolgreiche-projekte/ [10.07.2020]

Baur, Nina / Blasius, Jörg: Methoden der empirischen Sozialforschung, in: Baur, Nina / Blasius, Jörg (Hrsg.), Handbuch Methoden der empirischen Sozialforschung, Wiesbaden: Springer, 2014

Beck, Kent / Beedle, Mike / van Bennekum, Arie / Cockburn, Alistair / Cunningham, Ward / Fowler, Martin / Grenning, James / Highsmith, Jim / Hunt, Andrew / Jeffries, Ron / Kern, Jon / Marick, Brian / Martin, Robert C. / Mellor, Steve / Schwaber, Ken / Sutherland, Jeff / Thomas, Dave: Manifest für agile Softwareentwicklung, [online] https://agilemanifesto.org/iso/de/manifesto.html [06.07.2020]

Cohn, Mike: User Stories Applied for Agile Software Development, USA, Boston: Pearson Education Inc., 2004

Cooper, Harris M.: Synthesizing Research – A Guide for Literature Reviews, 3. Auflage, USA, Thousand Oaks: Sage Publications Inc, 1998

Cooper, Harris / Hedges, Larry: Research Synthesis As a Scientific Enterprise, in: The Handbook of Research Synthesis, USA, New York: Russell Sage Foundation, 1993

Dachwitz, Ingo: Deutsche Wohnen kassiert erste Millionenstrafe [Update], in: netzpolitik.org, 2019, [online] https://netzpolitik.org/2019/datenschutzgrundverordnung-deutsche-wohnen-erste-millionenstrafe/ [06.07.2020]

Datenschutz.org: EU-Datenschutzrichtlinie (Richtlinie 95/46/EG) – Alte Rechtsgrundlage (24.05.2018), [online] https://www.datenschutz.org/eu-datenschutzrichtlinie [09.03.2020]

Dehmel, Susanne / Thiel, Barbara: Vier Monate DS-GVO – wie weit ist die die deutsche Wirtschaft?, in: Bitkom Research, 2018

Deutsches Institut für Normung e.V. (Hrsg.): DIN 69901 Begriffe der Projektwirtschaft, Berlin: Beuth, 1987

Eckkrammer, Tobias / Eckkrammer, Florian / Gollner, Helmut: Agiles IT-Projektmanagement im Überblick, in: Ernst Tiemeyer (Hrsg.), Handbuch IT-Projektmanagement, 2. Aufl., München, Deutschland: Hanser, 2014

Fettke, Peter: State-of-the-Art des State-of-the-Art - Eine Untersuchung der Forschungsmethode „Review" innerhalb der Wirtschaftsinformatik, in: Wirtschaftsinformatik 48, 2006b

Frank, Ulrich: Konstruktionsorientierter Forschungsansatz, in: Enzyklopädie der Wirtschaftsinformatik, 2016, [online] https://www.enzyklopaedie-der-wirtschaftsinformatik.de/wi-enzyklopaedie/lexikon/uebergreifendes/Forschung-in-WI/Konstruktionsorientierter-Forschungsansatz/index.html [10.06.2020]

Hevner, Alan / March, Salvatore / Park, Jinsoo: Design Science in Information Systems Research, in: MIS Quarterly, Vol. 28 No.1, 2004

Hjerppe, Kalle / Ruohonen, Jukka / Lepännen, Ville: The General Data Protection Regulation: Requirements, Architectures, and Constraints, in: 2019 IEEE 27th International Requirements Engineering Conference (RE), 2019

Hoadley, Paul / Smith, Paul / Traian, Shmuel Csaba: Waterfall model, in: Wikimedia Commons, 2013, [online] https://commons.wikimedia.org/w/index.php?curid=29119277 [10.07.2020]

Huth, Dominik / Matthes, Florian: "Appropriate Technical and Organizational Measures": Identifying Privacy Engineering Approaches to Meet GDPR Requirements, in: 25th Americas Conference on Information Systems, Cancun, 2019

International Institute of Business Analysis: A Guide to the Business Analysis Body of Knowledge (BABOK Guide), Version 2.0, 2005

Jaspers, Andreas: Die EU-Datenschutz-Grundverordnung, in: Datenschutz und Datensicherheit, Band 36, Berlin: Deutschland, 2012

Kraus, Georg/ Westermann, Reinhold: Projektmanagement mit System, 6. Aufl., Berlin: Springer, 2019

Kusay-Merkle, Ursula: Agiles Projektmanagement im Berufsalltag, Berlin: Springer, 2018

Laudon, Kenneth / Laudon, Jane / Schoder, Detlef: Wirtschaftsinformatik – eine Einführung, 3. Aufl., Hallbergmoos: Pearson Deutschland GmbH, 2016

Litke, Hans-Dieter: IT-Projekte richtig strukturieren und systematisch planen in: Ernst Tiemeyer (Hrsg.), Handbuch IT-Projektmanagement, 2. Aufl., München, Deutschland: Hanser, 2014

Luber, Stefan / Augsten, Stephan: Was ist Scrum?, in: Dev-Insider, 2017, [online] https://www.dev-insider.de/was-ist-scrum-a-575361/ [10.07.2020]

Lucassen, Garm / Dalpiaz, Fabiano / van der Werf, Jan Martijn E. M. / Brinkkemper, Sjaak: Improving agile requirements: the Quality User Story framework and tool, Requirements Eng 21, Springer, 2016

March, Salvatore / Smith, Gerald: Design and natural science research on information technology, in: Decision Support Systems 15, Elsevier, 1995

Maximini, Dominik: The Scrum Culture, Wendlingen: Springer, 2015, S. 290
Mühlbauer, Holger: EU-Datenschutzgrundverordnung (DSGVO) Praxiswissen für die Umsetzung im Unternehmen - Schnellübersichten, 2. Auflage, Berlin: Beuth, 2018

Mayring, Philipp: Qualitative Inhaltsanalyse, in: Boehm, A. / Mengel, A. / Muhr, T (Hrsg.), Texte verstehen: Konzepte, Methoden, Werkzeuge, Konstanz: UVK Univ.-Verl. Konstanz, 1994

Mieg, Harald A. / Näf, Matthias: Experteninterviews, 2. Aufl., Institut für Mensch-Umwelt-Systeme (HES), Schweiz, Zürich: ETH Zürich, 2005

Misoch, Sabina: Qualitative Interviews, 2. Aufl., Berlin: De Gruyter Oldenbourg

Paal, Boris / Pauly, Daniel / Ernst, Stefan: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl., München: C.H.Beck, 2018

Pfeffers, Ken / Tuunanen, Tuure / Rothenberger, Marcus / Chatterjee, Samir: A Design Science Research Methodology for Information Systems Research, in: Journal of Management Information Systems, Vol. 24 No. 3, 2007-8

Przyborski, Aglaja / Wohlrab-Sahr, Monika: Qualitative Sozialforschung, München: Oldenbourg, 2008

Rebiger, Simon / Dachwitz Ingo: Die DSGVO zeigt erste Zähne: 50-Millionen-Strafe gegen Google verhängt, in: Datenschutz – 27 Ergänzungen, 2019, [online] https://netzpolitik.org/2019/die-dsgvo-zeigt-erste-zaehne-50-millionen-strafe-gegen-google-verhaengt [09.04.2020]

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995)

Ringmann, Sandra Domenique / Langweg, Hanno / Waldvogel, Marcel: Requirements for Legally Compliant Software Based on the GDPR, in: On the Move to Meaningful Internet Systems – OTM 2018 Conferences, Springer, 2018

Rost, Martin: Datenschutzmanagementsystem, in: Datenschutz und Datensicherheit, Ausgabe 5/2013, Berlin: Deutschland, 2013

Schlögel, Marcus / Tomczak, Torsten: Fallstudie, in: Baumgarth, Carsten / Eisend, Martin / Evanschitzky, Heiner (Hrsg.), Empirische Mastertechniken – Eine anwendungsorientierte Einführung für die Marketing- und Managementforschung, Wiesbaden: Gabler, 2009

Siepermann, Markus: Implementierung, in: Gabler Wirtschaftslexikon, 2018, [online] https://wirtschaftslexikon.gabler.de/definition/implementierung-31993/version-255541 [10.06.2020]

Verdat24 Team: Betroffenenrechte Teil 1 – Das Recht auf Berichtigung, in: verdat24, 2020, [online] https://www.verdat24.de/betroffenenrechte-teil-1-das-recht-auf-berichtigung/ [12.07.2020]

Voigt, Paul / von dem Bussche, Axel: EU-Datenschutz-Grundverordnung (DSGVO), Berlin: Springer, 2018

Winter, Robert: Design science research in Europe, in: European Journal of Information Systems 17, 2018

Wirdemann, Ralf: Scrum mit User Stories, 3. Aufl., München: Hanser Verlag, 2017

Yin, Robert K.: Case Study Research Design and Methods, 3. Aufl., Thousand Oaks, USA: SAGE Publications, 2003

Anhang

I. DSGVO-Katalog

Welche Anforderungen ergeben sich an Software?

Anforderungskategorien nach ID	
ID 1.X	Grundsätze der Verarbeitung personenbezogener Daten
ID 2.X	Einwilligung
ID 3.X	Verzeichnis über Verarbeitungstätigkeiten
ID 4.X	Nutzerverwaltung
ID 5.X	Betroffenenrechte

ID:	1.1
Name:	Vertraulichkeit
User Story:	*Als User möchte ich, dass meine personenbezogenen Daten nicht unerlaubt verarbeitet werden, damit sie geschützt sind.*
Ziel:	Vertraulichkeit
Beschreibung:	Personenbezogene Daten müssen in einer Weise verarbeitet werde, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen. (Art. 5 Abs. 1 f) Verantwortliche treffen unter Berücksichtigung der Technik, Kosten, des Umfangs, der Umstände, Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere von mit der Verarbeitung verbundenen Risiken geeignete technische und organisatorische Maßnahmen […] . (Art. 25 Abs. 1 DSGVO) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten , die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind. (Art. 32 Abs. 2 DSGVO)
Lösungskonzept:	Sichere **Authentisierungs- und Autorisierungsmechanismen** für alle Instanzen, die personenbezogene Daten speichern oder verarbeiten **Identitätsmanagement** insbesondere für den Zugang zur Nutzerverwaltung **Rollen- und Zugriffsberechtigungen**, damit nur notwendiger Personenkreis Zugriff auf notwendige Daten hat **Verschlüsselungsmethoden** von Daten

ID:	1.2
Name:	Integrität
User Story:	*Als User möchte ich, dass meine personenbezogenen Daten vor Verlust, Beschädigung oder Zerstörung sicher sind.*
Ziel:	Integrität und Vertraulichkeit
Beschreibung:	Personenbezogene Daten müssen in einer Weise verarbeitet werde, die eine angemessene Sicherheit der personenbezogene Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen. (Art. 5 Abs. 1 f) Verantwortliche treffen unter Berücksichtigung der Technik, Kosten, des Umfangs, der Umstände, Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere von mit der Verarbeitung verbundenen Risiken geeignete technische und organisatorische Maßnahmen […] . (Art. 25 Abs. 1 DSGVO) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind. (Art. 32 Abs. 2 DSGVO)
Lösungskonzept:	Nutzen geeigneter **IT-Infrastruktur** **Monitoring** von Datenströmen **Testen der Belastbarkeit** der IT-Architektur

ID:	1.3
Name:	Verfügbarkeit
User Story:	*Als User möchte ich geeignete technische und organisatorische Maßnahmen, damit das System nach einem Zwischenfall schnell verfügbar ist.*
Ziel:	Integrität und Vertraulichkeit
Beschreibung:	Verantwortliche treffen unter Berücksichtigung der Technik, Kosten, des Umfangs, der Umstände, Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere von mit der Verarbeitung verbundenen Risiken geeignete technische und organisatorische Maßnahmen. Diese Maßnahmen schließen die Fähigkeit ein, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. (Art. 32 Abs. 1 c DSGVO)
Lösungskonzept:	**IT-Service-Management**, dass im Falle von Incidents eine schnelle Behebung ermöglicht Nutzen geeigneter **IT-Infrastruktur**

ID:	1.4
Name:	Unverkettbarkeit
User Story:	*Als User möchte ich, dass ein Angreifer keine Verbindung zwischen meinen personenbezogenen Daten herstellen kann.*
Ziel:	Integrität und Vertraulichkeit
Beschreibung:	Verantwortliche treffen unter Berücksichtigung der Technik, Kosten, des Umfangs, der Umstände, Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere von mit der Verarbeitung verbundenen Risiken geeignete technische und organisatorische Maßnahmen. Diese Maßnahmen schließen die Fähigkeit ein, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. (Art. 32 Abs. 1 c DSGVO)
Lösungskonzept:	**Bestenfalls Anonymisieren** von Daten, die nur einmalig benötigt werden oder bei denen eine spätere Zuordnung nicht mehr nötig ist. (Testdaten) Anonymisierte Daten fallen nicht mehr unter die DSGVO! **Pseudonymisieren** von Daten, die eine spätere Zuordnung benötigen durch geeignete Verschlüsselung.

ID:	1.5
Name:	Datenminimierung
User Story:	*Als User möchte ich, dass nur meine für den Zweck notwendigen personenbezogene Daten erhoben werden.*
Ziel:	Minimierung der Anzahl personenbezogener Daten, Senken der Schwere eines Incidents, Integrität und Vertraulichkeit
Beschreibung:	Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. (Art. 5 Abs. 1c DSGVO) Verantwortliche treffen unter Berücksichtigung der Technik, Kosten, des Umfangs, der Umstände, Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere von mit der Verarbeitung verbundenen Risiken geeignete technische und organisatorische Maßnahmen […] . (Art. 25 Abs. 1 DSGVO) […] durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. (Art. 25 Abs. 2 DSGVO)
Lösungskonzept:	Personenbezogene Daten nur erheben / in dem Umfang erheben, in dem sie **nötig** sind **Anonymisieren** von Daten, die nur einmalig benötigt werden oder bei denen eine spätere Zuordnung nicht mehr nötig ist. (Testdaten) Anonymisierte Daten fallen nicht mehr unter die DSGVO! **Pseudonymisieren** von Daten, die eine spätere Zuordnung benötigen durch geeignete Verschlüsselung.

ID:	1.6
Name:	Transparenz
User Story:	*Als User möchte ich nachvollziehen können, auf welche Art und Weise meine personenbezogenen Daten verarbeitet werden.*
Ziel:	Transparenz
Beschreibung:	Personenbezogene Daten müssen […] in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. (Art. 5 Abs. 1a DSGVO)
Lösungskonzept:	Je höher die **Komplexität eines Systems**, desto eher Kenntlichmachung **ob, von wem und zu welchem Zweck** personenbezogene Daten verarbeitet werden. **Datenschutzerklärung** leicht zugänglich machen

ID:	1.7
Name:	Speicherbeschränkung
User Story:	*Als User möchte ich, dass meine personenbezogenen Daten nur so lange gespeichert werden, wie sie für den erfassten Zweck benötigt werden.*
Ziel:	Speicherbeschränkung, Minimierung der Anzahl personenbezogener Daten, Senken der Schwere eines Incidents
Beschreibung:	Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, […], ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden. (Art. 5 Abs. 1e DSGVO)
Lösungskonzept:	**Regelmäßige / Automatisierte Prüfung alter Datenbestände** auf Notwendigkeit **Anonymisieren** von Daten, die nur einmalig benötigt werden oder bei denen eine spätere Zuordnung nicht mehr nötig ist. (Testdaten) Anonymisierte Daten fallen nicht mehr unter die DSGVO! **Pseudonymisieren** von Daten, die eine spätere Zuordnung benötigen durch geeignete Verschlüsselung.

ID:	1.8
Name:	Zweckbindung
User Story:	*Als User möchte ich, dass meine personenbezogenen Daten nur für legitime festgelegte und eindeutige Zwecke verarbeitet werden.*
Ziel:	Speicherbeschränkung, Minimierung der Anzahl personenbezogener Daten, Senken der Schwere eines Incidents,
Beschreibung:	Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken. (Art. 5 Abs. 1b DSGVO)
Lösungskonzept:	**Überprüfen des Zwecks** der Verarbeitung personenbezogener Daten in Verbindung mit Softwareanforderungen schon in der **Phase der Anforderungserhebung**

ID:	2.1
Name:	Einwilligungserklärung – Abgabe
User Story:	*Als User möchte ich eine Einwilligung zur Verarbeitung meiner personenbezogenen Daten geben, damit ich frei zustimmen kann.*
Ziel:	Rechtmäßigkeit der Verarbeitung
Beschreibung:	Die Verarbeitung ist rechtmäßig, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke freiwillig, also zwanglos, gegeben hat. (Art. 6 Abs. 1a und Art. 7 Abs. 4 DSGVO) Beruht die Verarbeitung auf einer Einwilligung, muss sie der Verantwortliche nachweisen können. (Art. 7 Abs. 1 DSGVO) Im Zuge der Einwilligungseinholung teilt der Verantwortliche Name und Kontaktdaten des Verantwortlichen (ggf. Vertreter), ggf. Kontaktdaten des Datenschutzbeauftragten, die Zwecke sowie Rechtsgrundlage der Verarbeitung, ggf. die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und ggf. die Absicht des Verantwortlichen personenbezogene Daten an ein Drittland oder internationale Organisation zu übermitteln. (Art. 13 Abs. 1 DSGVO) Zusätzlich stellt der Verantwortliche Informationen über die Dauer der Speicherung, die Rechte der betroffenen Person, ein mögliches Widerrufen der Einwilligung, das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde, gesetzliche oder vertragliche Notwendigkeit der Bereitstellung pbD, ggf. Profiling zur Verfügung. (Art. 13 DSGVO)
Lösungskonzept:	Einwilligung in **Nutzerverwaltung** speichern (Historie der Einwilligung mit Datum) Bestätigen der Einwilligungserklärung bei **Login** auf Plattform mittels Checkbox (ggf. bei jeder Anmeldung)

ID:	2.2
Name:	Einwilligungserklärung - Widerruf
User Story:	*Als User möchte ich die Einwilligung zur Verarbeitung meiner Daten widerrufen können, damit meine Daten nicht länger verarbeitet werden.*
Ziel:	Rechtmäßigkeit der Verarbeitung
Beschreibung:	Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der Einwilligung [der bis hierhin verarbeiteten personenbezogenen Daten] nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein. (Art. 7 Abs. 3 DSGVO)
Lösungskonzept:	Auswirkung auf **Nutzerverwaltung** (Historie über Veränderungen) **Einfachheit Einwilligung = Einfachheit Widerruf** Ggf. Auswirkungen auf Zugänge treffen (sind **Einschränkungen** im Zugang betroffen?)

ID:	3.1
Name:	Verzeichnis über Verarbeitungstätigkeiten - Verantwortlicher
User Story:	*Als Aufsichtsbehörde möchte ich Verarbeitungsverzeichnisse kontrollieren, damit ein hoher Schutzstandard gehalten wird.*
Ziel:	Transparenz, Rechenschaftspflicht
Beschreibung:	Jeder Verantwortliche und ggf. sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgende Angaben: - Namen und Kontaktdaten des Verantwortlichen (ggf. mit Datenschutzbeauftragten); - Zwecke der Verarbeitung; - Beschreibung der Kategorien betroffener Personen und Kategorien personenbezogener Daten; - Kategorien von Empfängern; - Gegebenenfalls Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation; - Wenn möglich, die vorhergesehene Frist zur Löschung der Datenkategorien; - Wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen. (Art. 30 Abs. 1 DSGVO) Das Verzeichnis ist schriftlich/elektronisch zu führen. (Art. 30 Abs. 3 DSGVO) Der Verantwortliche stellt der Aufsichtsbehörde da Verzeichnis auf Anfrage zur Verfügung. (Art. 30 Abs. 4 DSGVO)
Lösungskonzept:	Einführung eines **Verarbeitungsverzeichnisses** Insbesondere in der **Entwicklung und im Test** notwendiger Detailgrad an technischen und organisatorischen Maßnahmen für geeignetes Schutzniveau.

ID:	3.2
Name:	Verzeichnis über Daten außerhalb der EU
User Story:	*Als Aufsichtsbehörde möchte ich Datenströme nachvollziehen, die außerhalb der EU gehen, weil sie ein besonderes Schutzniveau haben.*
Ziel:	Transparenz, Rechenschaftspflicht
Beschreibung:	Jeder Verantwortliche und ggf. sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgende Angaben: - Namen und Kontaktdaten des Verantwortlichen (ggf. mit Datenschutzbeauftragten); - Zwecke der Verarbeitung; - Beschreibung der Kategorien betroffener Personen und Kategorien personenbezogener Daten; - Kategorien von Empfängern; - Gegebenenfalls Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation; - Wenn möglich, die vorhergesehene Frist zur Löschung der Datenkategorien; - Wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen. (Art. 30 Abs. 1 DSGVO) Das Verzeichnis ist schriftlich/elektronisch zu führen. (Art. 30 Abs. 3 DSGVO) Der Verantwortliche stellt der Aufsichtsbehörde da Verzeichnis auf Anfrage zur Verfügung. (Art. 30 Abs. 4 DSGVO)
Lösungskonzept:	**Dokumentieren** sämtlicher Datenströme, die außerhalb der EU führen (**Verarbeitungsverzeichnis**) Es gelten **länderspezifische Anforderungen** gemäß Art. 45 DSGVO, die es einzeln zu berücksichtigen gilt!

ID:	3.3
Name:	Verzeichnis über Drittparteien
User Story:	*Als Aufsichtsbehörde möchte ich Datenströme nachvollziehen, die zu Drittparteien gehen, weil sie ein besonderes Schutzniveau haben.*
Ziel:	Transparenz, Ausübung Betroffenenrechte, Rechenschaftspflicht
Beschreibung:	Jeder Verantwortliche und ggf. sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgende Angaben: - Namen und Kontaktdaten des Verantwortlichen (ggf. mit Datenschutzbeauftragten); - Zwecke der Verarbeitung; - Beschreibung der Kategorien betroffener Personen und Kategorien personenbezogener Daten; - Kategorien von Empfängern; - Gegebenenfalls Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation; - Wenn möglich, die vorhergesehene Frist zur Löschung der Datenkategorien; - Wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen. (Art. 30 Abs. 1 DSGVO) Das Verzeichnis ist schriftlich/elektronisch zu führen. (Art. 30 Abs. 3 DSGVO) Der Verantwortliche stellt der Aufsichtsbehörde da Verzeichnis auf Anfrage zur Verfügung. (Art. 30 Abs. 4 DSGVO)
Lösungskonzept:	**Dokumentieren** sämtlicher Datenströme, die zu Drittparteien führen (**Verarbeitungsverzeichnis**) Gegebenenfalls **Plug-in**, das die Ausübung betreffender Betroffenenrechte an Drittparteien weitergibt (z.B.: Löschung personenbezogener Daten bis in Drittparteiensoftware)

ID:	3.4
Name:	Verzeichnis über Ausübung Betroffenenrechte
User Story:	*Als Aufsichtsbehörde möchte ich eine Historie über die Betroffenenrechte nachvollziehen, damit diese kontrolliert werden können.*
Ziel:	Rechtmäßigkeit, Transparenz
Beschreibung:	Im Sinne der Nachweispflicht und juristischer Vollständigkeit werden alle Anfragen, Bearbeitungen und Ergebnisse der Anfragen von Betroffenen-rechten dokumentiert.
Lösungskonzept:	**Zentrale Dokumentation** der Ausübung von Betroffenenrechten durch Nutzer **Verschlüsselung** und **Speicherfristen** beachten!

ID:	4.1
Name:	Anzeigen der Nutzerdaten
User Story:	*Als User kann ich nachvollziehen, ob und welche* personenbezogenen Daten *von mir verarbeitet werden, damit meine Betroffenenrechte ausüben kann.*
Ziel:	Ausübung des Auskunftsrechts gemäß Art. 15 DSGVO
Beschreibung:	Die betroffene Person hat das Recht vom Verantwortlichen eine Bestätigung darüber zu erhalten, ob und welche personenbezogenen Daten verarbeitet werden und auf Informationen zu: - Verarbeitungszwecken; - Kategorien der personenbezogenen Daten; - Empfänger oder Kategorien von Empfängern; - Ggf. Dauer der Speicherung; - Das Bestehen des Rechts auf Berichtigung oder Löschung; - Das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde; - Wenn die Daten nicht bei der betroffenen Person erhoben wurden, Herkunft der Daten; - Ggf. Übermittlung an Drittland oder Drittpartei (Art. 15 Abs. 1 DSGVO) Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Kommt die Anfrage elektronisch ein, soll nach Möglichkeit auch eine elektronische Antwort stattfinden. (Art. 15 Abs. 3 DSGVO)
Lösungskonzept:	**Zentrale Nutzerverwaltung** mit zwei Sichten – Nutzersicht und Administratorensicht

ID:	4.2
Name:	User Interface für Betroffenenrechte
User Story:	*Als User kann ich über ein User Interface meine Betroffenenrechte ausüben, verwalten, den Bearbeitungsstand erfahren und ein Ergebnis erhalten.*
Ziel:	Ausübung der Betroffenenrechte gemäß Art. 16 – 21 DSGVO
Beschreibung:	Aus Nutzersicht: Vereinfachung der Möglichkeit der Ausübung von Betroffenenrechten durch ein User Interface. Informationen über Bearbeitungsstände und Ergebnisse sowie vorherige Anfragen. Verwalten aktiver Anfragen. Aus Unternehmenssicht: Zentrale Verwaltung von Nutzeranfragen im Zusammenhang mit Betroffenenrechten.
Lösungskonzept:	**Zentrale Nutzerverwaltung** mit geeignetem **User Interface** zur Anfrage, Dokumentation und Verwaltung von Betroffenenrechten

ID:	4.3
Name:	Zugang zu maschinenlesbarem Format
User Story:	*Als User möchte ich Zugriff auf ein maschinenlesbares Format meiner Daten erhalten, um sie an einen anderen Verantwortlichen übermitteln zu können.*
Ziel:	Ausübung der Datenportabilität gemäß Art. 20 DSGVO
Beschreibung:	Die betroffene Person hat das Recht, […] ihre personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und […] diese Daten einem anderen Verantwortlichen […] zu übermitteln, sofern die Verarbeitung auf einer Einwilligung oder Vertragserfüllung beruht. (Art. 20 Abs. 1 DSGVO) Soweit technisch möglich, sollen die Daten direkt von einem Verantwortlichen zum anderen übertragen werden. (Art. 20 Abs. 2 DSGVO)
Lösungskonzept:	Zugriff auf eigenen Datensatz innerhalb der **zentralen Nutzerverwaltung**

ID:	5.1
Name:	Anfrage auf Berichtigung
User Story:	*Als User möchte ich die Korrektur/Ergänzung meiner personenbezogenen Daten veranlassen können, damit keine falschen Daten verarbeitet werden.*
Ziel:	Recht auf Berichtigung gemäß Art. 16 DSGVO
Beschreibung:	Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen. (Art. 16 DSGVO)
Lösungskonzept:	Über **Zentrale Nutzerverwaltung** mit geeignetem **User Interface** zur Ausübung des Rechts auf Berichtigung Auf **Administratorenseite**: Prüfen und Annahme/Ablehnung der Änderung **Back-Up** alter Datensätze Ggf. Weiterleitung der Daten zu Drittparteien durch **Schnittstelle** **Änderungshistorie** in Verzeichnis über Betroffenenrechte

ID:	5.2
Name:	Anfrage auf Löschung
User Story:	*Als User möchte ich die Löschung meiner personenbezogenen Daten veranlassen können, damit sie aus dem Einflussbereich Dritter entzogen werden.*
Ziel:	Recht auf Vergessenwerden gemäß Art. 17 DSGVO
Beschreibung:	Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, dem der Verantwortliche unverzüglich nachkommen muss, sofern einer der folgenden Gründe zutrifft: - Die Zwecke für die Erhebung/Verarbeitung nicht mehr notwendig; - Widerruf der Einwilligung; - Widerspruch gegen die Verarbeitung; - Unrechtmäßige Verarbeitung der personenbezogenen Daten; - Löschung ist zur Erfüllung einer rechtstaatlichen Verpflichtung notwendig. (Art. 17 Abs. 1 DSGVO) Der Verantwortliche ist verpflichtet, veröffentlichte/weitergegebene Daten ebenfalls löschen zu lassen. (Stichwort Drittparteien) (Art. 17 Abs. 2 DSGVO) Der Löschung entgegen sprechen: Freie Meinungsäußerung, öffentliches Interesse/Erfüllung eines Vertrags, Archivzwecke, Ausübung/Geltendmachung von Rechtsansprüchen. (Art. 17 Abs. 3 DSGVO)
Lösungskonzept:	Über **Zentrale Nutzerverwaltung** mit geeignetem **User Interface** zur Ausübung des Rechts auf Berichtigung Auf **Administratorenseite**: Prüfen und Annahme/Ablehnung der Änderung Wenn Löschen aufgrund von öffentlichem Interesse/Verträgen nicht möglich: **Pseudonymisieren**! Geeignetes **Löschkonzept** entwickeln, um automatisiert Fristen oder Datenzwecke einzuhalten

ID:	5.3
Name:	Anfrage auf Einschränkung der Verarbeitung
User Story:	*Als User möchte ich die Verarbeitung meiner personenbezogenen Daten einschränken können, um Rechtsansprüche geltend zu machen.*
Ziel:	Recht auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO
Beschreibung:	Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, sofern: - Die Richtigkeit der personenbezogenen Daten bestritten wird und der Verantwortliche eine angemessene Zeit zum Prüfen haben soll; - Die Verarbeitung unrechtmäßig ist, aber die Daten nicht gelöscht, sondern eingeschränkt werden sollen; - Der Verantwortliche die Daten nicht länger benötigt, aber der Nutzer zur Geltendmachung/Ausübung von Rechten; - Die betroffene Person Widerspruch gegen die Verarbeitung gegen die Verarbeitung eingelegt hat, solange noch nicht feststeht, wessen Interessen überwiegen. (Art. 18 Abs. 1 DSGVO) Wurde die Verarbeitung eingeschränkt, dürfen die personenbezogenen Daten nur mit Einwilligung des Betroffenen oder im Zusammenhang mit Rechtsausübung/öffentlichen Interesses verarbeitet werden. (Art. 18 Abs. 2 DSGVO) Wird die Einschränkung aufgehoben, muss der Betroffene vorher informiert werden. (Art. 18 Abs. 3 DSGVO)
Lösungskonzept:	Über **Zentrale Nutzerverwaltung** mit geeignetem **User Interface** zur Ausübung des Rechts auf Berichtigung Auf **Administratorenseite**: Prüfen und Annahme/Ablehnung der Änderung **Sperren der Nutzerverwaltung** während des Prüfungsvorgangs für beide Sichten Weiterleitung zu Drittparteien durch **Schnittstelle** **Änderungshistorie** in Verzeichnis über Betroffenenrechte

II. Interview Person A

I: [0:00:00] Also, ich würde dein Einverständnis einmal einholen, dass ich das gemachte Interview einmal für meine Bachelorarbeit verwenden darf und im Zweifelsfall noch für ein wissenschaftliches Paper. Allerdings alles anonymisiert, d.h. dein Name steht dann da nicht drin, sondern nur ein Kürzel.

B: [0:00:17] Ja, ist in Ordnung.

I: [0:00:17] Sehr schön. Am Anfang wäre es ganz schön, wenn du dich einmal vorstellen könntest. Vielleicht irgendwie, was du bisher schon gemacht hast, was du jetzt im Unternehmen machst. Einfach zum Reinkommen.

B: [0:00:31] Ja ich bin Person A. Ich bin gerade ein Hybrid aus Projektleitung und Anforderungsmanager. Ich bin seit knapp drei Jahren im Unternehmen und habe so vereinzelt Beratungsprojekte gemacht *bei einem Automobilhersteller* (anonymisiert) und bin jetzt seit mehr als einem Jahr im Entwicklungsprojekt als Anforderungsmanager/Projektleiter tätig. Da ist ein bisschen fachliche Führung dabei. Das ist es auf oberer Ebene.

I: [0:01:08] Wie läuft so das Projektmanagement bei euch. Also nach welchem Vorgehensmodell oder gibt es vielleicht keine klare Struktur?

B: [0:01:16] Ich habe jetzt kein Vorgehensmodell erkannt. Also meinst du wie ein Angebotsprozess abläuft?

I: [0:01:22] Nach dem Motto traditionelles Projektmanagement oder Methoden davon oder eher agiles oder eine hybride Variante.

B: [0:01:29] Ah, ok. Also wir sind jetzt, ich würde sagen, relativ agil unterwegs. Jetzt aber nicht puristisch agil, wie man das kennt nach irgendwelchen SCRUM-Frameworks oder so. Wir haben aber trotzdem Zyklen, die aus Zweimonats-Releases bestehen, also alle zwei Monate wird ein Release gemacht. Zyklisch werden innerhalb eines Releases Umfänge definiert, die gemacht werden sollen. D.h. beim Kunden wird abgefragt: "Hey, was hättest du gerne als nächstes entwickelt?" und die Anforderungen werden dann einmal aufgenommen und durchspezifiziert und in so einem Backlog niedergeschrieben. Das Backlog wird dann durchpriorisiert, damit halt immer die wichtigsten Sachen im nächsten Releasezyklus dann enthalten sind. Wenn die Umfänge feststehen, dann werden die Aufwände geschätzt und dann wird geguckt was schaffen wir tatsächlich innerhalb dieser zwei Monate umzusetzen und dann wird das umgesetzt. Also mit Testen und so weiter. Es kann dann sein, dass vielleicht während eines laufenden Sprints nochmal irgendwelche Rückfragen sind, nochmal kleine Anpassungen gemacht werden sollen. Aber die Idee ist eigentlich, dass sich der Entwicklungsumfang nicht mehr ändert. Während der Entwicklungszeit werden parallel die Umfänge des nächsten Releases dann

wieder geklärt. So ist das dann halt ein überlappender, zyklischer Kreislauf aus Anforderungsmanagement und Entwicklung.

I: [0:03:12] Also gibt es quasi keine richtige Trennung für dich im Sinne der Anforderungserhebung, sondern das läuft halt so nebenbei und immer wieder zu Spitzenzeiten in Intervallen mehr, wenn ein neuer Sprint ansteht?

B: [0:03:23] Ja genau. Eigentlich ist das durchgängig. Nur halt verschoben zur Entwicklung.

I: [0:03:31] Das könnte dann nochmal interessant werden, wenn ich nachher genauer auf den Katalog selbst eingehe. Ich mache nochmal einen Schritt weiter vor. Du weißt ja, dass es um die DSGVO in meiner Bachelorarbeit geht. Da ist jetzt erstmal interessant zu gucken, wieviel Vorwissen eigentlich überhaupt bei euch oder allgemein bei dem IT-Dienstleister auf Ebene der reinen Projekte an Vorwissen DSGVO vorhanden ist. Und wenn ja, durch welches Medium sowas kommuniziert wurde.

B: [0:03:58] Also es gibt so eine Datenschutzschulung bei uns und im Rahmen der DSGVO wurde die, glaube ich, auch ein bisschen angepasst und es gab auch noch eine spezifische Schulung, wo nochmal genau auf sowas wie Betroffenenrechte oder sowas eingegangen wird. Wenn ich Schulung sage, dann meine ich sowas wie ein zwei, drei Stunden Remoteding (gemeint: Schulung). Das hatte dann so einen Vorlesungscharakter. Das wurde dann vorgestellt, die wichtigsten Kernpunkte der DSGVO. Dann konnte man nochmal Fragen stellen und musste dann, glaube ich, sogar nochmal so einen kleinen Mini-Test schreiben. Also so ein bisschen Multiple-Choice, zehn Fragen, so von wegen "hast du wirklich daran teilgenommen?".

I: [0:04:57] Da schließt sich quasi gleich die zweite Frage so ein bisschen an. Du hast damit zwar nicht ganz so extrem zu tun direkt, aber weißt du oder kannst du einschätzen, wie die DSGVO aktuell in der Software implementiert wird? Schafft ihr es oder habt ihr schon als Ziel DSGVO-konforme Software zu erstellen?

B: [0:05:22] Ähm.

I: [0:05:24] Oder ist das vielleicht noch ein fehlender Punkt?

B: [0:05:29] Ich würde sagen wir haben das gerade noch nicht drin. Puh, jetzt kommen wir gerade so in die Richtung Unternehmensstrategie, also wo wir hinwollen.

I: [0:05:41] Ja, du hast recht. Aber ich will das gar nicht auf der Makroebene sehen, weil ich da weiß, dass zumindest ein Datenschutzmanagementsystem existiert, was ja sehr viele Sachen aufgreift.

Sondern mich interessieren jetzt mehr die Sachen auf der Ebene des Mikrokosmos des Projektes des reinen.

B: [0:06:02] Ok. Wir haben vor, durchaus, dieses Ding DSGVO-konform zu machen. Wir haben da ja schon mal so einen Analyseauftrag gehabt, wo wir das System mal analysieren sollten. So nach (dem Motto): "Hey, wie DSGVO-konform ist das und was muss da vielleicht gemacht werden?" Das haben wir ja schon mal gemacht. Wir haben auch schon vorgeschlagen, dass wir genau diese Änderungen umsetzen. Bisher haben wir aber noch nicht den Auftrag dafür bekommen. Wir sind ein Dienstleister, wir machen kein Produktgeschäft. Deswegen haben wir nicht den Drang das aus eigener Tasche DSGVO-konform zu bezahlen. Das ist in dem Moment hauptsächlich das Problem unseres Auftraggebers. Die müssen sich dann am Ende einigen, ob sie das Geld dafür ausgeben wollen. Deswegen können wir nur, natürlich aus unserem wirtschaftlichen Interesse, also einmal aus Beratungsinteresse und einmal aus wirtschaftlichem Interesse, immer nur pushen "Hey Leute, das müsste mal gemacht werden". Beratungstechnisch eben "Hey Leute, das ist gesetzesrelevant". Wir sind da jetzt vielleicht noch nicht ganz so top dabei. Wir kennen natürlich die Arbeitsverträge bei dem *Automobilhersteller* (anonymisiert) nicht, was da vielleicht schon gemacht wird. Aber es ist auf jeden Fall relevant. Aber auf der anderen Seite machen wir natürlich auch ein bisschen Druck, damit wir Projekte akquirieren und da dann halt noch einen Zusatzumsatz generieren.

I: [0:07:31] Also ist das für euch quasi eine Zusatzanforderung oder ein Zusatzanforderungspaket, was monetär vergütet werden kann oder sollte in Zukunft.

B: [0:07:42] Ja, es ist immer mit extra Aufwand verbunden und der muss eben berechnet werden. Deswegen kann man nicht sagen, dass die ganzen DSGVO-Anpassungen immer für lau mitlaufen. Die Anpassungen im Sinne der DSGVO sind normale Anforderungen, die im Rahmen eines Projekts mit aufgenommen werden. Genau wie eine Anforderung beispielsweise sein kann: "Hey, ich als Kunde hätte gerne eine Möglichkeit mit PayPal zu bezahlen." Das ist eine Anforderung und gleichzeitig muss es aber auch andere Anforderungen geben, die da heißen: "Als Nutzer müssen DSGVO-Bestimmungen gewahrt werden." Ganz grob. Und genau so müssen die mit in die Entwicklung eingeplant werden. Dann würden wieder ganz normal die Aufwände dafür geschätzt werden, um das umzusetzen.

I: [0:08:36] Gut. Angedacht ist also ein wirtschaftlicher Nutzen daraus.

B: [0:08:42] Ja, das ist es ja am Ende immer.

I: [0:08:45] Geht nur darum, dass man das Problemfeld aufzeigt und sagt "das hat wirtschaftliche Relevanz" oder "eine praxisnahe Relevanz" letztendlich. Gut. Ich habe dir ja im Vorfeld schon den Katalog geschickt. Du konntest reingucken und wir haben über eine vorherige Fassung sogar schon mal gesprochen, die User Stories habe ich ja nochmal ein bisschen angepasst. Der grundsätzliche Aufbau

ist aber gleichgeblieben. Jetzt ist meine Frage: Aus deiner Sicht als Product Owner oder Anforderungsmanager, der schon viel gesehen hat, meinst du dieser Anforderungskatalog kann die Softwareentwicklung unterstützen auf Projektebene und wenn ja, wie?

B: [0:09:21] Also ja, auf jeden Fall. Du hast ja schon erwähnt, dass es nicht bis ins letzte Detail durchplanen kannst.

I: [0:09:32] Genau.

B: [0:09:33] Was auch total verständlich ist, weil es auch immer wieder projektabhängig ist. Es gibt so eine Methodik, die nennt sich Story Mapping. Das ist eigentlich etwas, was man im ersten Schritt macht, wenn man ein neues Projekt aufzieht. Dass man mal versucht die Umfänge des Produkts zu definieren. Wenn man mal bei diesem Online-Shop-Beispiel bleibt, dann fängt man an zu sagen: "Alles klar, wir hätten gerne eine Einkaufsmöglichkeit. Wir hätten gerne eine Shop-Seite. Wir hätten gerne ein Benutzerprofil." Und diese ganzen Blöcke werden einfach aneinandergereiht. Das muss man sich vorstellen wie eine riesengroße Wand und das wird dann immer detaillierter und da werden eine Menge Zettelchen drangehangen. Das gemeine beim Brainstormen ist ja immer, dass nicht unbedingt alle Ideen da sind. Wenn ich jetzt aber beispielsweise diesen Katalog hätte, dann könnte ich mir diese Zettelchen direkt nehmen und an diese Story-Map dranhängen. Wo ich dann sagen kann "Alles klar, das Betroffenenrecht, das brauchen wir. Das brauchen wir. Das brauchen wir." Dann kann ich quasi unter so einer ganzen Spalte DSGVO kann ich genau diese Dinge hinhängen und könnte dann mit hoher Sicherheit sagen, dass damit schon, im besten Fall, alles abgedeckt ist, worüber wir uns Gedanken machen müssen. In welchem Detailgrad das dann natürlich noch ausformuliert werden muss und ob dann davon vielleicht wieder irgendetwas weg kann aus Gründen, vielleicht weil die Unternehmensinfrastruktur schon manche DSGVO-Sachen schon abdeckt, das kann dann individuell entschieden werden. Aber das wäre dann für mich der erste Anknüpfungspunkt, den ich da sehen würde. Gleichzeitig kann das aber natürlich auch eine Gesprächsgrundlage sein, wenn man in ein Gespräch mit dem Kunden geht, der darüber redet, wie er sich das Produkt vorstellen könnte und wir dann noch sagen "Hey, hast du schon an die DSGVO gedacht?" "Was muss denn da alles gemacht werden?" "Ja warte mal, ich habe da etwas."

I: [0:11:18] **(**Thematisch irrelevant.)

B: [0:11:21] **(**Thematisch irrelevant.)

I: [0:11:57] Auf der Ebene des täglichen Geschäftes, wenn wir uns vom anfänglichen Anknüpfungspunkt loslösen, siehst du da noch eine Möglichkeit den Katalog einzubinden? Sodass du nicht nur einmalig den Nutzen davon hast, sondern auch im Daily Business?

B: [0:12:17] Da muss ich jetzt überlegen. Spontan aus dem Bauch heraus würde ich nein sagen. Kommt drauf an. So wie du den Katalog beschrieben hast, was ich bisher gesehen habe, da waren ja nochmal ein paar Referenzen auf irgendetwas. Oder vielleicht warum es relevant ist. Das wäre dann vielleicht was, wo ich dann im Alltagsgeschäft nochmal reingucken könnte als Referenzliste. Wo muss ich nochmal nachgucken, wenn ich mich für irgendetwas interessiere. Das ist jetzt aber nichts, was ich an fünf Tagen die Woche mache. Das ist dann eher etwas, was ich vielleicht mal punktuell mache.

I: [0:12:56] Also meinetwegen, wenn wieder neue Sprints oder Meilensteine festgelegt werden oder neue Meilensteine.

B: [0:13:00] Ja, genau. Kommt drauf an.

I: [0:13:05] Also eine generelle Aussage, glaube ich schon, ist da nicht möglich.

B: [0:13:08] Also ich glaube, dass es tendenziell eher am Anfang nützlich ist, oder wenn das Thema eben aufkommt. Also am Anfang des Aufkommens des Themas und weniger, wenn das alles schon ins Rollen gekommen ist.

I: [0:13:22] Letzte Frage. Was würdest du, wenn du ihn so vor Augen hast, am Anforderungskatalog noch verbessern.

B: [0:13:30] Uff.

I: [0:13:32] Ja, das ist die gemeinste Frage am Schluss. Das muss jetzt nicht mal so sein, dass du den komplett vor Augen hast und nur daran Verbesserungen hast, sondern, wenn du jetzt aus deiner Sicht als Anforderungsmanager dieses Artefakt verwenden möchtest, was würde da deiner Meinung nach noch Nutzen bringen, damit du es, einmal aus deiner Sicht und einmal aus der Sicht des ganzen Projekts, nutzenbringend einbringen kannst.

B: [0:13:56] Ja. Ich habe mir den Katalog nebenbei nochmal kurz aufgemacht.

I: [0:14:17] Das kann was an der Struktur sein, das kann was am Inhalt sein. Völlig frei raus, was dir einfällt. Kann auch ein ganz anderes Format sein, wenn du sagst ein Anforderungskatalog ist blöd, aber eine DSGVO-Sammlung in Form von xyz ist besser. Ganz allgemeine Verbesserungsvorschläge.

B: [0:14:33] Es ist gar nicht so leicht ad hoc zu sagen, was noch besser wäre.

I: [0:15:05] Der Sinn dieser Frage ist nur, dass die Literaturanalyse dazu geführt hat, dass es dadurch eher ein forschungsnaher Praxiskatalog ist und den Anspruch hat praxisnah zu werden durch meine Modifikationen. Jetzt geht es halt darum, was man für die tatsächliche Praxis noch machen könnte.

B: [0:15:19] Das ist ein bisschen kritische Würdigung, ne? Da ist jetzt nur die Frage, was man da für einen Anspruch hat. Wir haben anfangs gesagt, dass man nicht bis ins letzte Detail gehen kann mit den Sachen. Ich kann mir nur vorstellen, dass man eventuell bei den Lösungskonzepten einen Lösungsbaukasten, Bausteine, beschreiben könnte. In dem Sinne, welche Möglichkeiten es vielleicht gibt Daten zu anonymisieren. Da gibt es dann vielleicht Anonymisierungstabellen oder sowas. Oder Pseudonymisierungstabellen. You get the idea.

I: [0:16:03] Ja, also Verfeinerung der Verbesserungsvorschläge. Was ich da auch heraushöre jetzt...

B: [0:16:10] Best Practices.

I: [0:16:13] Ich wollte gerade sagen, dass der Anspruch war, dass der Katalog im Sinne einer "Best Practices"-Sammlung wachsen kann, damit immer mehr zugeschnitten ist auf das jeweilige Unternehmen oder die Projekte selbst und du dann immer mehr Nutzen generierst im Rahmen dieses Anforderungskatalogs.

B: [0:16:25] Ja.

III. Interview Person B

I: [0:00:00] So, ich würde das Interview, was wir beide führen, einmal gerne für meine Bachelorarbeit verwenden und für ein wissenschaftliches Paper, was wir danach vielleicht verwenden. Wenn das für dich in Ordnung ist, dann stimme bitte einmal zu.

B: [0:00:11] Ja, kannst du gerne verwenden.

I: [0:00:14] Sehr schön. Es wäre ganz gut, wenn du dich einmal vorstellst. Vielleicht was du vorab gemacht hast, was du jetzt zurzeit machst, wie so deine tägliche Arbeit aussieht. Das man einmal so ein bisschen Background hat.

B: (Irrelevant)

I: (Irrelevant)

B: [0:00:34] Ich habe Informatik studiert mit Bachelorabschluss und bin dann danach bei dem *Unternehmen* (anonymisiert) eingestiegen. Bin dort als Java-Entwickler im Projekt tätig. Aktuell durch die Corona-Phase allerdings nur noch als Support, bzw. zum Bugfixen. Neuere Dinge entwickeln wir derzeit nicht. Genau, das waren so bisher meine Aufgaben bei uns.

I: [0:01:08] Wie sieht sonst so dein täglicher Tag in Nicht-Corona-Zeiten aus? Was übernimmst du so für Aufgaben ansonsten?

B: [0:01:17] Schon direkter Kontakt mit dem Kunden. Absprache von neuen Themen, was ist möglich, was gibt es schon, was könnte noch kommen. Direkter Kontakt auch in Sachen Fehlerbehebung. Also wir kriegen schon E-Mails direkt vom Kunden, wen gesagt wird "hier haben wir ein Problem, guckt euch das mal an". Ansonsten ganz normale Entwicklungstätigkeiten. Von Datenbank, also SQL-Abfragen, zu ganz normal Java-Code. Aber auch ein bisschen infrastrukturiellere Themen bei uns, wenn es darum geht unsere Deployment-Chain am Laufen zu halten. Dann muss halt auch immer einer Kontakt halten zu unseren DevOps und schauen, dass das auch weiterhin funktioniert, sodass wir theoretisch zu jeder Zeit ausliefern könnten. Genau.

I: [0:02:25] Ja, sehr schön. Dann bist du schon mal insofern ein Experte, als das wenn es um das große Thema DSGVO-Architektur geht, du da definitiv zumindest den Gesamtüberblick in der Projektarchitektur hast. Ich würde nochmal einen Schritt zurückgehen, losgelöst jetzt mal von dem Projekt per se, sondern würde einfach mal gerne von dir wissen, wie so dein Vorwissen über die DSGVO ist. Du musst jetzt nicht wiedergeben, was die DSGVO macht, sondern ich will jetzt einfach nur deine Bewertung, was an Vorwissen über die DSGVO vorhanden ist. Vielleicht auch durch welches Medium.

B: [0:03:02] Ich glaube mein Vorwissen ist gar nicht so groß diesbezüglich. Ja, klar. Als das Thema frisch auf den Tisch gekommen ist durch die Medien, also durch Internet, durch das Fernsehen, hat man sich da schon ein bisschen schlau gemacht. Aber jetzt wirklich so in die Tiefe reingelesen habe ich mich diesbezüglich noch nicht, weil es, ja, wenn man es auch gerade auf die Arbeit bezieht, mich bisher weniger berührt hat. Also eigentlich sind es bisher noch keine Überschneidungen gewesen, wo es für mich darum ging, da tiefer in die Materie einzusteigen. Aber sonst im Privaten, außer das man jetzt überall der DSGVO zustimmen muss, wenn man irgendwas Neues unterschreibt, hatte ich da jetzt auch großartig bewusst..., unbewusst macht man das ja überall. Kommt man da ja überall mit in Kontakt, aber so bewusst jetzt eher weniger.

I: [0:04:08] Dem schließt sich so ein bisschen meine zweite Frage an, auch wenn die jetzt natürlich dadurch schon ein Stück weit vorweggenommen ist. Also durch meine Fallstudie, durch mein Praktikum, habe ich ja zumindest so auf der Makroebene im *Unternehmen* (anonymisiert) ja einen Blick dafür, wie da die DSGVO umgesetzt ist in Form von einem Datenschutzmanagementsystem. Interessant ist jetzt allerdings im Zusammenhang mit der Abschlussarbeit oder der Fallstudie, wie das so auf Mikroebene ist. Das heißt so linke, rechte Grenze dein *Projekt* (anonymisiert) oder halt allgemein in den Projektteams, wenn du es von einem anderen Projekt weißt. Also wie wird da die DSGVO in der Software implementiert oder wie ist sie in der Projektebene überhaupt vertreten?

B: [0:04:47] Wir hatten da mal ein Thema zu, auch von Seiten des *Automobilherstellers* (anonymisiert), weil die auch abklären wollten, wie weit die DSGVO bei uns umgesetzt ist, bzw. was dort noch umgesetzt werden könnte. In dem Rahmen sind wir damit so ein bisschen in Kontakt gekommen. Allerdings wurde da quasi mehr oder weniger beschlossen, dass aufgrund der fachlichen Notwendigkeit der personenbezogenen Daten, also Name, Nachname, E-Mailadressen und so was, es quasi nicht möglich sei, genauer die DSGVO bei uns umzusetzen. Von daher haben wir wirklich bei uns im Projekt gar keine Berührungspunkte, was die Entwicklung angeht und haben da mehr oder weniger freie Hand. Ohne, dass wir da Rücksicht drauf nehmen.

I: [0:05:49] Ja, verstehe ich. In dem Katalog selber sind ja Sachen drin, oder allgemein von der DSGVO auch Anforderungen, die sich nicht allein auf, meinetwegen nur Nachnamen und irgendwelche personenbezogene Daten beziehen, sondern vielleicht auch so infrastrukturell. Das heißt, wie können zum Beispiel Betroffenenrechte in welchem Rahmen ausgeübt werden und so. Gibt es da irgendwelche Berührungspunkte? Also, dass ihr das irgendwie eingesteht oder nachvollziehen könntet, wenn jetzt ein Betroffenenrecht angefragt wird.

B: [0:06:22] Bei uns im Tool gibt es dafür keine Möglichkeit. Also es gibt kein eigenes UI, wo die Nutzer sehen können, was über sie so gesammelt wird oder auch keine Möglichkeit direkt eine Abfrage der Daten, die wir von den Anwendern haben, auszuspucken. Also dafür gibt es keine Möglichkeit.

I: [0:06:50] Meine dritte Frage wäre gewesen, wie man die Implementierung verbessern kann. Gut, sagen wir mal, man könnte prüfen, wo überhaupt Anknüpfungspunkte sind. Meinetwegen bei sowas wie Betroffenenrechten, ja? Dass man die vielleicht automatisiert, dann abrufen könnte oder whatever. Also man müsste überhaupt etwas machen, so nach dem Motto?

B: [0:07:11] Genau. Da aktuell überhaupt nichts gemacht wird, müsste man überhaupt etwas machen, um dann zu gucken, was man da für Potenzial hat.

I: [0:07:21] Ok. Meine nächste Frage wäre, vielleicht auch jetzt nicht nur auf dein Projekt (anonymisiert) bezogen, sondern jetzt aus deiner Erfahrung heraus. Meinetwegen auch bei neuen Projekten, die irgendwie mal gegebenenfalls eingeführt werden könnten. Meinst du der Anforderungskatalog kann die Softwareentwicklung unterstützen und wenn ja, wie?

B: [0:07:41] Naja also der Katalog bildet ja schon mal so eine gewisse Struktur ab, die man so ein bisschen abarbeiten kann. Du hast das ja bei dir ganz gut gegliedert, auch mit den einzelnen Punkten. Erstmal grundsätzlich, wenn man so einen Katalog hat und den durchgelesen hat, hat man ja schon mal im Hinterkopf vielleicht eine andere Sicht als vorher. Das hilft. Und eben, dass man so einen Katalog hat, an dem man sich etwas entlang hangeln kann, um dann eventuell zu gucken "alles klar, haben wir den Punkt beachtet? Ja, nein? Wie könnten wir das eventuell umsetzen?". Da hat man mit deinem Lösungskonzept auch immer schon echt gute Hinweise gegeben, wie man das eventuell umsetzen könnte. Von daher finde ich so einen Katalog schon ziemlich gut.

I: [0:08:34] Hast du das Gefühl, dass du jetzt auch mit deinem eher wenigen vorhandenen Vorwissen die einzelnen Punkte, vielleicht nicht im Detail alle, aber ein Gefühl dafür kriegst, wie Datenschutzrichtlinien im Zusammenhang mit der DSGVO sich auf die Softwareentwicklung auswirken können?

B: [0:08:48] Ja, auf jeden Fall. Zum einen durch die User Stories. Also der kleine Text der User Stories ist echt schon sehr gut und verständlich beschrieben. Zusätzlich hilft dazu ja immer noch die Beschreibung aus dem Gesetzestext sozusagen. Also das fand ich sehr gut. Und auch richtig gut verständlich, das konnte man alles recht gut nachvollziehen.

I: [0:09:14] Also fassen wir zusammen: Würde sich definitiv als hilfreich erweisen, wenn man DSGVO-konforme Software entwickeln möchte.

B: [0:09:22] Meiner Meinung nach ja.

I: [0:09:23] Sehr schön. Dann last but not least. Ich weiß, die Frage war bei den anderen auch sehr unbeliebt, aber so im Sinne eines Ausblicks oder Verbesserungspotenzial: Was hättest du mal losgelöst von dem Anforderungskatalog, den ich da so habe, allgemein für Verbesserungsvorschläge, um DSGVO-konforme Software zu erstellen oder meinetwegen auch eine Weiterentwicklung von

meinem? Irgendwelche Punkte, die du vielleicht aus dem Alltag siehst, die man noch als Art von "Best Practices" integrieren kann?

B: [0:10:15] Ja schwierig. Schwierig allein deshalb, weil wir selber kaum damit Kontakt haben. Von daher müsste der Kunde schon mal selber gewillt sein, sowas haben zu wollen. Wenn das schon nicht gegeben ist, dann bringt dir das leider alles nichts.

I: [0:10:50] Das hat Person A auf den Punkt gebracht, indem er gesagt hat, das ist ein Zusatzfeature was der Kunde im Endeffekt anfragen muss.

B: [0:10:57] Hm, ja. Schwierig.

I: [0:11:14] Wenn du jetzt nichts hast als Verbesserung, dann ist das ja auch nicht schlimm.

B: [0:11:20] Zumindest jetzt nicht so auf die Schnelle.

I: [0:11:23] Na ja, man müsste damit auch erst arbeiten, glaube ich. Siehst du vielleicht das Potenzial, dass man während der Entwicklung an so einem Katalog als organisches Element "Best Practices" implementieren kann? Nach dem Motto: "Daraus habe ich was gelernt und mein Lösungskonzept verbessert". Also, wenn man dann so möchte, Verbesserungsvorschlag, dass das Dokument wächst.

B: [0:11:53] Ja, so ein Dokument sollte schon mitwachsen, ja. Das sehe ich auch. Mitwachsen und auch aktualisiert werden. Das ist ja jetzt nicht in Stein gemeißelt. Der Katalog ist ja jetzt auch mehr aus der Theorie erstmal entstanden.

I: [0:12:16] Richtig. Deswegen führen wir ja auch die Interviews, um dann festzustellen, wie die Theorie überhaupt vereinbar ist mit der Praxis.

B: [0:12:21] Genau. Je nachdem, wie es sich dann in der Praxis ergibt, muss eventuell der Katalog dann angepasst werden. Wenn man merkt "ok, das klappt überhaupt nicht, aber hier und da müsste man noch ein paar Stellschrauben drehen", dann sollte es natürlich auch wieder im Katalog festgehalten werden. Um für die Zukunft auch auf dem aktuellen Stand zu bleiben. Der Katalog ist ja nicht nur für ein Mal gedacht.

I: [0:12:55] Also halten wir mal fest: Als Verbesserungsvorschlag vielleicht, dass der in der Praxis erprobt werden sollte, um ihn dann weiterentwickeln zu können oder seine Tauglichkeit zu beweisen. Also dann einen Zyklus einen Sprint mit dem Katalog machen.

B: [0:13:16] Ja, genau. Es wird sich auch ziemlich schnell zeigen, wo es Probleme geben könnte. Da kriegt man recht schnell Feedback. Zumindest in kleinen Teilen.

IV. Interview Person C

I: [0:00:00] Ich hätte gerne dein Einverständnis dafür, dass ich unser Interview im Rahmen meiner Bachelorarbeit und gegebenenfalls danach in Form eines wissenschaftlichen Papers verwenden darf.

B: [0:00:13] Ja, ich bin einverstanden.

I: [0:00:14] Sehr schön. Es wäre ganz nett, wenn du dich einmal kurz vorstellen könntest. Was du vorab gemacht hast, was du jetzt machst im *Unternehmen* (anonymisiert) und ein bisschen deinen täglichen Ablauf definieren kannst.

B: [0:00:26] Ich bin Person B. Ich bin jetzt mittlerweile seit fast sechs Jahren im *Unternehmen* (anonymisiert). Seit vier Jahren bin ich im Bereich Test unterwegs und habe seit fast vier Jahren im *Projekt X* (anonymisiert) das komplette Gebiet Test abgearbeitet. Anfänglich Automatisierung, am Ende dann auch viel in Richtung Testmanagement. Parallel kam dann noch parallel ein anderes Projekt dazu, das mittlerweile ein bisschen auf Eis liegt und momentan bin ich einem anderen Projekt unterwegs, wo ich aber wieder hauptsächlich im Bereich Testautomatisierung und entwicklungsbegleitenden Tests agiere.

I: [0:01:11] Also quasi alles was in dem großen Bereich Test zusammengefasst werden kann.

B: [0:01:15] Genau. Aber mit Schwerpunkt der Testautomatisierung.

I: [0:01:20] Wie läuft das ab? Wie setzt du Anforderungen im Test um bzw. wie testest du die?

B: Anforderungen gibt es anhand von User Stories zu bestimmten Features und die enthalten Akzeptanzkriterien, an denen wir uns entlang hangeln. Anhand dieser Akzeptanzkriterien werden dann auch Testfälle erstellt. Bei Kernfunktionalitäten, die ich mit den entsprechenden Stakeholdern bespreche, setze ich das Augenmerk dann darauf das zu automatisieren und das als Regressionstest zu jedem Build durchlaufen zu lassen. So der Plan.

I: [0:02:03] So, dass du quasi ein vergleichbares, qualitatives Kriterium am Ende hast, um zu entscheiden, ob die Anforderung passt oder nicht?

B: Es ist ja immer so, dass wenn du an einer Stelle schraubst, es immer sein kann, dass es dir an einem ganz anderen Ende, an das man gar nicht gedacht hat, vor die Füße fällt. Deswegen sind die Regressionstests sehr nützlich und relativ einfach bzw. kostengünstig. Es fällt relativ schnell auf, wenn es automatisiert ist und man muss dann nicht ewig manuell durchklicken.

I: [0:02:35] Ich würde nochmal einen Schritt zurückgehen oder einen Schritt losgelöst von der eigentlichen Projektarbeit, die ihr macht, machen. Du weißt, dass sich meine Bachelorarbeit mit dem Thema DSGVO beschäftigt. Da ist es erstmal interessant zu wissen, wieviel Vorwissen bei den Projektmitgliedern oder bei dir im Einzelnen vorhanden ist und wenn ja, durch welches Medium?

B: [0:03:00] Was soll ich dir genau erzählen? Ich weiß, dass das es vor zwei Jahren oder so eingeführt wurde. Dass Benutzerdaten auf Wunsch gelöscht werden müssen und so weiter. Dass ich jetzt zum Beispiel, wenn ich nicht will, dass mein Name in einem Programm nicht mehr auftaucht oder so, ich das anfordern kann. Dass ich aber auch Auskunft bekomme, wo mein Name überhaupt überall auftaucht. Ja, das ist es im Prinzip.

I: [0:03:33] Wie hast du den Wissenszugang gehabt? Gibt es im Unternehmen eine Variante oder hast du es dir privat angeeignet?

B: [0:03:41] Das war privat. Das war ja eine Zeitlang die ganze Zeit in den Nachrichten, wo auf jedem Newsportal ganz viel stand darüber. Aber so nach und nach kamen da die Informationen rein und letzten Endes wurde es ja bei uns umgesetzt und dahingehend hatten wir dann auch mal eine Schulung, meine ich, an die ich mich aber ehrlich gesagt nicht mehr großartig erinnere. Aber größtenteils privat.

I: [0:04:08] Dem schließt sich die folgende Frage an: Im Rahmen meines Praktikums bzw. Fallstudie habe ich ja ein bisschen den Datenschutzkosmos des *Unternehmens* (anonymisiert) durchforstet und in der Makroebene, also dem Unternehmen als Gesamtgebilde, gibt es ja ein Datenschutzmanagementsystem, wo sehr viele DSGVO-Anforderungen umgesetzt sind. Mich interessiert jetzt nur der Mikrokosmos Projekt, also linke und rechte Grenze dein Projekt. Da ist die Frage, wie die DSGVO aktuell implementiert wird, wenn sie denn implementiert wird.

B: [0:04:46] Hm. Kann ich dir ehrlich gesagt nicht sagen, weil wir mal die Aufgabe hatten festzustellen, an welchen Stellen diese Daten auftauchen und so, aber umgesetzt ist es noch nicht. Das wurde nicht beauftragt. Das heißt es wurde nur in dem Sinne implementiert, dass es wahrscheinlich Absprachen mit dem Kunden gab.

I: [0:05:12] Also gibt es als Anweisung oder als Prozess innerhalb der Softwareentwicklung noch keine DSGVO-Eingliederung?

B: [0:05:22] Genau. Das einzige, was da in Sachen Test ist, ist das wir da mit Testfällen arbeiten. Aber ansonsten ist das relativ offen.

I: [0:05:33] Wenn du gerade die Testfälle ansprichst. Da gibt es ja auch oft das Problem, dass die Daten echte Daten sind oder generische Daten. Weißt du, ob die einen Personenbezug haben oder frei erfunden sind?

B: [0:05:50] In der Umgebung des *Automobilherstellers* (anonymisiert) haben die Daten mehr oder weniger einen Personenbezug, weil es anders auch gar nicht zu testen ist. Da arbeiten wir mit Datenbankabbildern und da sind aus einer produktiven Datenbank Daten, wenn wir auf QS testen. Da fehlt der Zwischenschritt, dass die ganzen Benutzerdaten pseudonymisiert werden. Es sind halt auch eigentlich immer nur so zwei, die das melden und auf die es da ankommt.

I: [0:06:18] Na ja, gut. Aber so gesehen findet die DSGVO da noch keine Anwendung?

B: [0:06:22] Nee.

I: [0:06:24] Ok. Gut, also wenn ich dir dann die nächste Frage stellen würde, wie die Implementierung verbessert werden kann, dann wahrscheinlich durch überhaupt erst eine Implementierung?

B: [0:06:31] Exakt. Alleine schon als Zwischenschritt für Tests, dass man da den Datenbank-Dump nimmt und da ein Skript drüber laufen lässt, was da die ganzen Namen ändert.

I: Das sind dann so ad hoc alle Verbesserungsvorschläge, die dir in deinem Tätigkeitsbereich einfallen würden?

B: [0:06:50] Genau, im Prinzip wäre das schon der Hauptpunkt. Dass die ganzen Namen da in irgendeiner Form verschwinden. Namen und Fahrzeugprojekte sind ja auch in gewisser Weise zurückführbar. Aber das ist dann halt in der Praxis nicht umsetzbar. Erstmal selbst wenn es anonymisiert ist, kann man das trotzdem noch anhand der anhängenden Elemente herausfinden, was das denn für eins sein könnte. Über kurz oder lang kommt man dann notfalls auch auf einen User zurück, wenn man sich da ein bisschen auskennt. Das ist sehr schwer zu anonymisieren.

I: [0:07:30] Glaube ich. Die DSGVO gibt da auch nichts Klares vor. Sie sagt nur: "Je schwerer, desto besser.". Dass es nicht komplett geht, ist klar. Aber es geht immer um die Berücksichtigung des Stands der Technik, was kann man da machen, um es dem Angreifer möglichst kompliziert zu machen. Gut. Dann haben wir den IST-Zustand. Jetzt ist die Frage, wenn du den Anforderungskatalog mal überflogen hast, meinst du der Anforderungskatalog kann die Softwareentwicklung, oder den ganzen Projektlebenszyklus unterstützen? Und wenn ja, wie? Aus deiner Sicht als Tester.

B: [0:08:05] Grundsätzlich ja. Dann müssten eben alle an einem Strang ziehen. Da geht's immer los. Geld muss passen in gewisser Weise. Es muss wirklich Zeit dafür investiert werden, dass es jeder

auch lebt. Das ist nichts, was man mal so überstülpen kann. Für mich ist das ein kompletter Zyklus. So ist es jetzt relativ einfach gesagt, aber so ist aus meiner Sicht die Lösung. Jeder muss das verinnerlichen und in seiner täglichen Arbeit mit anwenden, um da auch eine gewisse Sensibilität zu entwickeln, was denn jetzt userbezogen ist und so. Ich glaube viele haben das gar nicht auf dem Schirm.

I: [0:08:53] Vielleicht nochmal spezifischer auf den Katalog selbst gesehen. Dass man das als Gesamtprozess integrieren müsste, vielleicht auch nochmal in Form einer Schulung, damit man nochmal vertiefter darauf eingeht, damit mehr Hintergrundwissen vorhanden ist, ok. Aber jetzt auf den Anforderungskatalog selbst, oder den Aufbau meinetwegen. Dass man sagt: man hangelt sich lang an User Stories und sagt "die Funktionalität muss eine Software aufweisen, damit sie DSGVO-konform ist". Mit den zusätzlichen Erklärungen, wo das zu finden ist bzw. welche Sachen da vorhanden sein müssen aus der DSGVO selbst und einem Lösungskonzept, dass sicherlich nicht vollständig ist, aber erste Hinweise gibt, wie man sowas implementieren kann, Wo würdest du das vielleicht ansetzen, wenn du es ansetzen würdest in dem Projekt selbst?

B: [0:09:41] Im Prinzip müsste man die ganzen User Stories einarbeiten in die Applikation. Es ist aber auch, was ich da so lese, ist das alles sehr realistisch. Also man kann es machen. Da sind dann halt so Sachen wie: "Ich möchte, dass meine Daten nur so lange gespeichert werden, wie sie für den erfassten Zweck benötigt werden". Das ist definitiv möglich, aber der erfasste Zweck kann sich ja über Jahrzehnte teilweise erstrecken. Trotzdem, klar. Umsetzbar.

I: [0:10:36] Meinst du, du kannst die dann im Sinne des Tests auch testen, also die User Stories? Also vielleicht nicht genau so, wie sie sind, weil den Anspruch haben sie ja nicht, weil sie ja projektspezifisch im Endeffekt sich noch entwickeln. Aber jetzt so vom reinen Katalog her, wenn du den Katalog vorgesetzt bekommst und meinetwegen eine Anforderung zum Testen bekommen würdest oder Akzeptanzkriterien. Könntest du dir vorstellen, dass du damit Testen kannst und dich damit als Tester wohlfühlen würdest sozusagen?

B: [0:10:56] Wie gesagt. Bei so Sachen die einen zeitlichen Rahmen beinhalten eher nicht. Auch ein erfasster Zweck, der kann ja zum Beispiel weitreichend sein. Das muss ja nicht unbedingt irgendeine Arbeit sein, mit der ich unmittelbar zu tun hatte, sondern irgendwas im Konglomerat der Software. Sowas ist schwer nachzuvollziehen oder zu testen. Da sind viele Variablen drin.

I: [0:11:28] Es kann keine eins oder null sein in Anführungsstrichen, sondern es ist halt auch irgendwas dazwischen möglich. Verstehe ich. Also im Test ist es dann tatsächlich sehr fallspezifisch davon abhängig, wie es dann implementiert wird, ja?

B: [0:11:42] Genau. So ganz einfache Sachen, wie Einwilligungserklärungen und sowas, klar das lässt sich gut nachvollziehen. Aber auch Verzeichnisse über die Daten außerhalb der EU ist schwierig, weil

ich da zum Beispiel auch keinen Überblick habe, wo zum Beispiel die Ganzen Server des Automobilherstellers (anonymisiert) hin replizieren.

I: [0:12:04] Ich denke, mutmaßlich ist es ja so, dass solche Sachen, die so weitreichend sind und keine direkten technischen Anforderungen abbilden, weil so ein Verzeichnis erstmal eine Modellierungs- oder Architekturfrage ist, klären sich meistens schon am Anfang des Projektes. Ich glaube da geht es sowieso darum eine vernünftige IT-Infrastruktur zu entwickeln und das wird dann, mit meiner Laienmeinung, nicht mehr viel mit Test hinten raus zu tun haben.

B: [0:12:34] Genau. Es kommt halt darauf an, wie Architekten vertrauen, dass das dann so reinpasst.

I: [0:12:40] Weil ich gerade schon mit Person A gesprochen habe und das sozusagen auch bei meiner Überlegung im Vordergrund stand bei der Phase der Anforderungserhebung. Für dich sind die Akzeptanzkriterien das wichtigste, hast du gesagt. Würdest du sagen, dass man mit dem Katalog gute Akzeptanzkriterien oder das nötig Hintergrundwissen hätte, um Akzeptanzkriterien für gewisse Anforderungen herzustellen, damit du sie anschließend testen kannst?

B: [0:13:09] Sowohl, als auch. Bei den meisten ja, aber da muss ich wieder auf diese schwammigeren Formulierungen zurückkommen. Im Sinne von: Nur Arbeit, die mit meinem Projekt zu tun hat. Oder nur, was habe ich noch gelesen, ich hatte ein gutes Beispiel, ach hier, genau: "Als User möchte ich, dass meine personenbezogenen Daten nur auf legitime, festgelegte und eindeutige Zwecke verarbeitet werden." Das ist ja auch Ansichtssache. Was ist legitim?

I: [0:13:49] Ja, da ist die DSGVO nicht ganz eindeutig.

B: [0:13:52] Deswegen ist sowas schwer nachzuvollziehen. Wenn man vorher dem gegenüberstellt, was denn die Zwecke sind, dann kann man das natürlich abgleichen. Ob die eingehalten werden. Also da muss man dann noch ein bisschen mehr dazuschreiben, aber nachtestbar wäre es dann auch in dem Fall, wenn die Eingangskriterien vorhanden sind.

I: [0:14:12] Ja. Eigentlich nur noch eine einzige Frage. Vielleicht fällt dir da was ein. Welche Verbesserungsvorschläge hättest du an den Anforderungskatalog oder würde dir sonst ein System einfallen, was das noch besser machen könnte? Um DSGVO-konforme Software zu erstellen im Endeffekt.

B: [0:14:32] Ja. Spontan nichts. Das ist halt immer sehr abhängig von der Applikation. Wenn wir uns jetzt nur auf mein Projekt (anonymisiert) beziehen zum Beispiel, kann man da dann noch ein bisschen ausführen, was da für mich legitime Kriterien sind, da irgendwie Werte für mich hinter setzen.

I: [0:14:58] Also, dass du es in einen projektspezifischen Kontext setzt.

B: [0:15:02] Genau.

I: [0:15:05] Ansonsten vielleicht was vom Aufbau oder der Struktur her?

B: [0:15:08] Finde ich gut. Ich habe da sonst keine Schmerzen mit.