Universität der Bundeswehr München

BACHELORARBEIT

Konzeption und Integration der Datenschutz-Folgenabschätzung in das Open Datenschutzcenter

Bearbeitungszeitraum: 1. April 2023 bis 30. Juni 2023

Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Professur
Datenschutz und Compliance
Universität der Bundeswehr München

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung

Für Privatpersonen, Unternehmen und den öffentlichen Dienst werden Datenschutz und seine Anforderungen im Alltag zunehmend komplexer. Vor allem in der digitalen Welt sind Datenschutz und die Gefahren von lockerem Umgang mit Daten sehr abstrakt und wenig vorhersehbar. Für Personen und Organisationen, die personenbezogene Daten verarbeiten, gilt seit Einführung der europäischen Datenschutz-Grundverordnung (DSGVO), welche im Mai 2018 in Kraft trat, ein rechtlich verbindlicher Rahmen für die Verarbeitung personenbezogener und personenbeziehbarer Daten mit teils empfindlichen Strafen bei Verstößen. Zur Einhaltung des Gesetzes hält das Standard-Datenschutzmodell (SDM) der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder Hinweise bereit, wie die gesetzlichen Anforderungen umgesetzt werden können.

Da die Datenschutz-Folgenabschätzung (DSFA) in Artikel 35 DSGVO gesetzlich verankert ist, muss diese durchgeführt werden bei Vorliegen eines hohen Risikos der Folgen der Datenverarbeitung für Rechte und Freiheiten natürlicher Personen. Dafür hält das Gesetz eine Muss-Liste bereit, in welcher die Fälle geregelt sind, in denen eine DSFA immer erforderlich ist, und beschreibt die Mindestanforderungen an die DSFA. [Hel22]

Weitere Unterstützung zur strukturierten Erarbeitung einer DSFA findet sich im SDM. Darin werden Hilfestellungen gegeben, um das Datenschutz-Risiko einer Verarbeitungstätigkeit zu bestimmen. Hier wird zur Bestimmung der Höhe des Risikos von jeder Verarbeitungstätigkeit, die Schwellwert-Analyse beschrieben, welche zur Einschätzung der Fragen dient, ob eine DSFA durchgeführt werden muss und ob in bestimmten Fällen eine vorherige Konsultation der Aufsichtsbehörden verpflichtend vorgeschrieben ist. Das SDM orientiert sich am Plan, Do, Check, Act (PDCA)-Zyklus. [Kon22]

Die Open Source Anwendung Open Datenschutzcenter (ODC) des Unternehmens H2 invent GmbH richtet sich an Unternehmen zur Erfüllung von datenschutzrechtlichen Vorgaben. Das praxisorientierte Datenschutz-Managementsystem (DSMS) enthält die wesentlichen Funktionen, die DSGVO und Bundesdatenschutzgesetz (BDSG) für ein DSMS fordern. Die Webanwendung steht als Open Source Version kostenlos zur Verfügung. [HH23]

Mit zunehmender Relevanz von Datenschutzanforderungen – nicht zuletzt durch die Durchsetzung geltenden Rechts und Umsetzung der Strafverfolgung durch die zuständigen Behörden – in Verbindung mit komplexen internen Prozessen und

Abläufen, braucht es zuverlässige technische Infrastrukturen um den reibungslosen Ablauf zu gewährleisten. Auf Grund dessen ist es notwendig zu erörtern, wie sich juristische Anforderungen auf eine Software übertragen lassen und welche technischen Möglichkeiten bestehen, um Verwaltungsprozesse zu unterstützen und zu vereinfachen. Gerade im Bereich der DSFA gibt es ein hohes Potential von Optimierungen. Da viele rechtliche Begriffe offen formuliert sind, wie z.B. der Risiko-Begriff, werden i.d.R. DSFA eher unpräzise formuliert und wenig standardisiert, es wird sich häufig an alten Dokumenten orientiert und keine individuellen Prognosen und Abschätzungen aufgestellt. Der wichtigste Ansatzpunkt für die Frage, ob eine DSFA durchgeführt werden muss, ist die Schwellwert-Analyse. Hier ist es für Laien schwierig eine qualitativ hochwertige Einschätzung durchzuführen, somit wäre hier ein konkreter Ansatzpunkt für die Optimierung von DSMS gegeben. Es gibt in Deutschland ausschließlich das ODC als Open Source Lösung eines DSMS. Es wurde keine Anwendung gefunden, die Anwendende softwareunterstützt durch die Schwellwert-Analyse führt. Hier ansetzend mit einer Standardisierung, würde ein Werkzeug geschaffen, das Datenschutzbeauftragte durch das komplexe Thema leitet und somit eine möglichst hohe Qualität und Präzision der DSFA ermöglichen. Zum Vergleich werden auch kommerzielle Produkte im Rahmen der Möglichkeiten betrachtet. Nur wenige Unternehmen, die kommerzielle Software vertreiben, bieten ausführliche Einblicke in ihre Anwendungen und den dahinter stehenden Konzepten.

Nach Abwägung der verfügbaren Anwendungen nach Relevanz für diese Ausarbeitung, werden das PIA-Tool der französischen Datenschutz-Behörde sowie die kommerzielle Anwendung 2B Advice PrIME vorgestellt, als Beispiele von bisher umgesetzten Lösungsansätzen für DSFA in DSMS.

1.1. Ziele

Der Fokus dieser Ausarbeitung liegt auf der Erarbeitung einer Konzeption für die technische Umsetzung der DSFA, anhand der Anforderungen die sich aus rechtlichen Vorgaben in Verbindung mit der Architektur des ODC ergeben. Der Schwerpunkt liegt auf der erforderlichen Schwellwert-Analyse, die dazu dient die Frage zu klären, ob eine DSFA durchgeführt werden muss.

Die DSFA im ODC besteht aktuell nur aus Freitextfeldern in denen die Datenschutzbeauftragten ihre Ergebnisse eintragen, hier erfolgt keine Auswertung oder ähnliches durch die Anwendung, es unterstützt nur zur besseren Dokumentation. Dieser Prozess soll möglichst standardisiert und automatisiert werden mit vordefinierten Formeln und Faktoren. Hier soll zur Abschätzung, ob eine DSFA nötig ist, erst eine Schwellwert-Analyse durchgeführt werden und die Risikoabschätzung um eine Risikomatrix ergänzt werden mit der Eintrittswahrscheinlichkeit und dem

Schadenspotential. Dies fließt dann in die DSFA ein, welche ebenfalls softwareunterstützt durchgeführt werden soll. Durch die Erstellung eines Konzepts soll der Baustein für die Entwicklung gelegt werden.

Der ideale Fall für Anwendende wäre eine softwaregeführte automatisierte Abfrage der relevantesten Aspekte für die DSFA mit daraus resultierenden Vorschlägen für technische und organisatorische Maßnahmen (TOM) und der Bereitstellung einer Dokumentation. Die rechtliche und technische Umsetzbarkeit wird in dieser Ausarbeitung analysiert.

Nach einer gründlichen Literatur-Recherche von rechtlichen Grundlagen und wissenschaftlichen Arbeiten, sowie der Betrachtung von vorhandenen Systemen wird ein Konzept erstellt, wie man die rechtlichen Forderungen im Einklang mit den Anforderungen des ODC in eine technische Lösung umsetzen kann. Hierbei werden die Konzepte zur DSFA und Risikoabschätzung von öffentlichen Trägern wie z.B. den Aufsichtsbehörden und Landesdatenschutzbeauftragten analysiert. Zusätzlich werden vorhandene DSMS mit DSFA betrachtet (z.B. PIA).[Sch09]

Ziele dieser Ausarbeitung:

- Herausarbeiten der rechtlichen Grundlagen und Begriffe
- Beschreibung der technischen Grundlagen desODC
- Vorstellung und Vergleich ähnlicher Arbeiten
- Erstellung eines Konzepts für die DSFA im ODC
- Ausarbeitung einer Methode für die Risiko-Analyse
- Evaluation von Konzept und Design

1.2. Aufbau der Arbeit

Die vorliegende Ausarbeitung ist wie folgt aufgebaut: In Kapitel 2 werden Grundlagen aus den Bereichen der rechtlichen Vorschriften und technischen Bedingungen erläutert und in Kapitel 3 werden verwandte Arbeiten vorgestellt sowie zu dieser Arbeit abgegrenzt. Der Fokus der Arbeit liegt auf der Entwicklung eines Konzepts, dies wird in Kapitel 4 behandelt. Abschließend werden nach einer Evaluation in Kapitel 5 die Zusammenfassung der Arbeit und der Ausblick in Kapitel 6 behandelt.

2. Grundlagen

Ziel der 2018 in Kraft getretenen Datenschutz-Grundverordnung (DSGVO) ist die Vereinheitlichung der Regelungen des Datenschutzrechts innerhalb der EU. Ergänzungen durch Gesetze einzelner EU-Mitgliedsstaaten, wie beispielsweise das deutsche Bundesdatenschutzgesetz (BDSG) werden durch sogenannte „Öffungsklauseln“ ermöglicht. Es findet Anwendung auf die Verarbeitung personenbezogener Daten innerhalb der EU. [BD17]

In diesem Kapitel werden die wesentlichen rechtlichen Grundlagen und Begriffe der Datenschutz-Folgenabschätzung (DSFA) nach DSGVO vorgestellt, sowie die technischen Voraussetzungen des Open Datenschutzcenter (ODC) beschrieben.

2.1. Rechtliche Vorschriften

Zum Verständnis der Vorschriften werden zunächst die Begriffe genannt, ein Auszug der wichtigsten Artikel der DSGVO wird ergänzt durch eine kurze Beschreibung der Inhalte.

2.1.1. Begriffserklärungen

- **Personenbezogene Daten:**
  Nach Art. 4 Abs. 1 DSGVO sind personenbezogene Daten, alle Informationen mit Bezug auf eine identifizierte oder identifizierbare natürliche Person. Identifizierbar bedeutet, dass eine natürliche Person durch Zuordnung zu einer Kennung oder zu einem oder mehreren Merkmalen direkt oder indirekt identifiziert werden kann, z.B. durch eine Online-Kennung oder soziale Identität.

- **Verarbeitung:**
  Die DSGVO definiert in Art. 4 Abs. 2 die Verarbeitung als jeden Vorgang, im Zusammenhang mit personenbezogenen Daten, egal ob mit oder ohne Hilfe automatisierter Verfahren. Dabei werden alle möglichen Verarbeitungsarten aufgeführt von Beginn bis Ende des Daten-Lebenszyklus. Hierzu gehören u.a. Erheben, Ordnen, Speichen, Verwendung, Bereitstellung, Vernichtung.
  Das Standard-Datenschutzmodell (SDM) nennt als beteiligte Komponenten an einer Verarbeitungstätigkeit die personenbezogenen Daten, beteiligte

technische Dienste und Systeme sowie technische, organisatorische und personelle Prozesse der Datenverarbeitung[Kon22].

- **technische und organisatorische Maßnahmen (TOM):**
  In Art. 24 Abs. 1 DSGVO werden TOM beschrieben als Maßnahmen zur Sicherstellung und Nachweiserbringung, dass die Verarbeitung gemäß der Verordnung erfolgt.

- **Risiko:**
  Nach ISO31000 kann der Risikobegriff beschrieben werden als ein Ereignis mit der Möglichkeit negativer Auswirkungen.[VOR23]
  Im Sinne der DSGVO stellt ein Risiko die bestehende Möglichkeit des Eintritts eines Ereignisses dar, das zu einem Schaden für Rechte und Freiheiten einer oder mehrerer Personen führt oder führen kann; dabei betrachtet man die Dimensionen der Schwere des Schadens und die Wahrscheinlichkeit[Kon22].

- **Auftragsverarbeiter:**
  Als Auftragsverarbeiter bezeichnet die DSGVO die Datenverarbeitung im Auftrag eines Dritten durch eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle.

- **Aufsichtsbehörde:**
  Die Aufsichtsbehörde ist nach Art. 51 DSGVO eine unabhängige staatliche Stelle in jedem Mitgliedstaat. Sie ist zuständig für die Überwachung und Anwendung der DSGVO zum Schutz von Grundrechten und Grundfreiheiten natürlicher Personen bei der Verarbeitung und Erleichterung des freien Datenverkehrs in der Union.

2.1.2. Datenschutz-Grundverordnung

Die relevanten rechtlichen Vorschriften der DSFA in der DSGVO sind Artikel 5: Grundsätze für die Verarbeitung personenbezogener Daten, Artikel 35: Datenschutz-Folgenabschätzung und Artikel 36: vorherige Konsultation. Auszüge dieser Artikel aus der DSGVO sind in Anhang A aufgeführt.

Artikel 5 „Grundsätze für die Verarbeitung personenbezogener Daten“ beschreibt die wesentlichen Verarbeitungsgrundsätze:

1. Rechtmäßigkeit, Fairness und Transparenz

2. Zweckbindung

3. Datenminimierung
4. Richtigkeit
5. Speicherbegrenzung
6. Integrität und Vertraulichkeit
7. Rechenschaftspflicht

Sie sind die Grundlage der Anforderungen für eine ordnungsgemäße Verarbeitung personenbezogener Daten. Die Begriffe werden im Gesetz definiert und sind relevant für Auslegung und Verständnis.

Artikel 35 „Datenschutz-Folgenabschätzung“ der DSGVO legt fest, dass eine DSFA verpflichtend durchgeführt werden muss, wenn ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen durch eine geplante Verarbeitung personenbezogener Daten zu erwarten ist. Dies trifft insbesondere bei Verwendung neuer Technologien zu. Eine DSGVO beinhaltet eine Beschreibung von Verarbeitungsvorgängen und Zwecken, eine Bewertung von Notwendigkeit und Verhältnismäßigkeit des Verarbeitungszwecks, eine Risiko-Analyse und geeignete Abhilfemaßnahmen zur Risikominderung mit Nachweisen. Die DSFA sollte insbesondere durchgeführt werden, wenn es um Verarbeitungstätigkeiten geht, bei denen umfangreiche Datenverarbeitungen, die Verarbeitung besonderer Kategorien von personenbezogenen Daten (sensible Daten), systematische Überwachung oder öffentliche Datenverarbeitung beinhaltet sind.

Nach Artikel 36 „Vorherige Konsultation“ ist die zuständige Aufsichtsbehörde zu kontaktieren, wenn aus der DSFA ein hohes Risiko der Verarbeitung zu erwarten ist. Dies trifft insbesondere dann zu, wenn durch den Verantwortlichen keine Maßnahmen zur Risikominimierung getroffen werden.

2.1.3. Datenschutz-Folgenabschätzung

Die DSFA ist ein kontinuierlicher Prozess, der den Schutz der Rechte von betroffenen Personen verbessern soll, indem die Risiken der Datenverarbeitung beherrschbar werden. Während des gesamten Lebenszyklus eines Prozesses ist die DSFA fortlaufend zu überwachen und bei Veränderung des Risikos zu wiederholen. Im Gegensatz zum Risikomanagement aus dem Bereich der Informationssicherheit liegt der Fokus nicht auf den Risiken für eine Organisation, sondern auf den Grundrechten und Freiheiten natürlicher Personen. Dennoch können durch die Identifizierung der Risiken für betroffene Personen indirekt auch Risiken für Organisatonen wie Sanktionen und Reputationsverlust vermieden werden. Identifizierte Risiken müssen durch Maßnahmen reduziert werden, verbleibende Restrisiken müssen begründet und dokumentiert werden. Es müssen Prüfgegenstand

und Verarbeitungszwecke beschrieben, Rechtsgrundlagen, Akteure und betroffene Personen identifiziert und die Verhältnismäßigkeit des Risikos für betroffene Personen bewertet werden. Zur Risikobewertung gibt es in der Informationssicherheit begrenzte Kalkulationsmöglichkeiten mit Formeln, da die Risiken oft eher abstrakt sind; insbesondere im Datenschutz ist eine Berechnung durch die Machtasymmetrie zwischen Verantwortlichen und Betroffenen nicht für beide Seiten zufriedenstellend möglich. Für natürliche Personen können aus der Verarbeitung physische, materielle oder immaterielle Schäden resultieren, beispielsweise Diskriminierung, Rufschädigung oder Identitätsbetrug. [LM17]

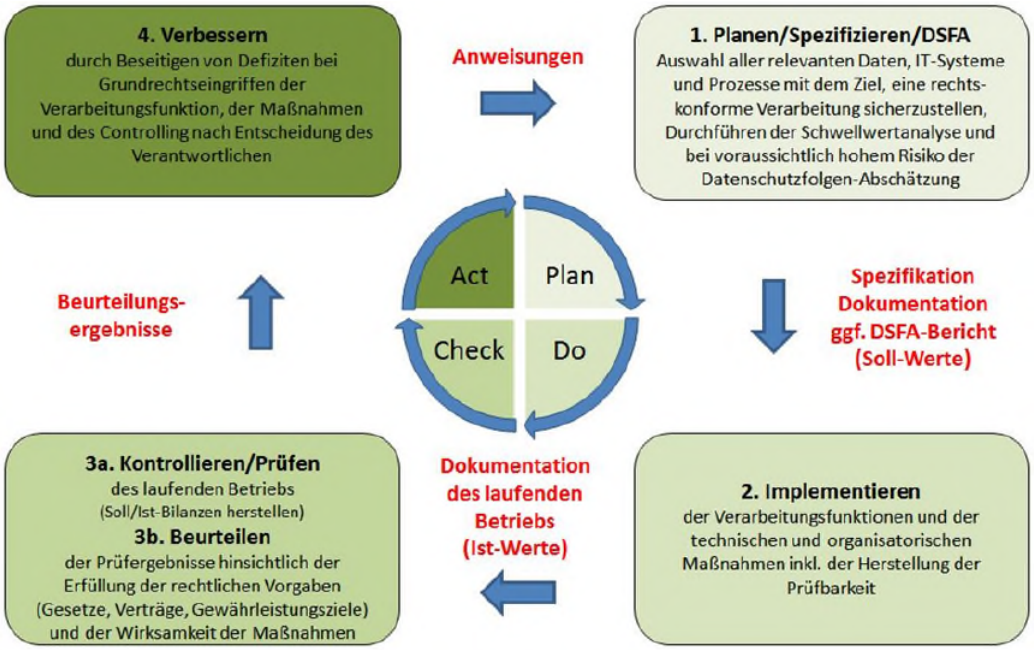

Abbildung 2.1.: PDCA Zyklus des Datenschutzmanagements [Kon22]

Abbildung 2.1 zeigt den gesamten Zyklus des Datenschutzmanagement (DSM) in Anlehnung an den bekannten Plan, Do, Check, Act (PDCA)-Zyklus mit seinen vier Phasen. Dies beschreibt einen kontinuierlichen Prozess der bei Planung, Spezifikation und DSFA beginnt. Soll-Werte werden definiert und TOM implementiert, Ist-Werte des laufenden Betriebs werden dokumentiert, kontrolliert, geprüft und beurteilt. Die Beurteilungsergebnisse fließen in Verbesserungsmaßnahmen ein, die in Anweisungen dokumentiert und wieder am Beginn des Zyklus genutzt werden. Das SDM kann so bei der Schwellwert-Analyse unterstützen. Deren Ziel ist die Feststellung, ob eine Verarbeitungstätigkeit auf Grund eines hohen Risikos eine DSFA erfordert. Dafür wird zunächst geprüft ob die jeweilige Verarbeitung in der Muss-Liste der Datenschutzaufsichtsbehörden aufgeführt ist, denn dann ist mit

einem hohen Risiko zu rechnen[Datb]. Im nächsten Schritt sollte man prüfen, ob die Verarbeitungstätigkeit in Art. 35 Abs. 3 bei den besonders riskanten Verarbeitungen aufgelistet ist, wie z.B. systematische umfassende Bewertung persönlicher Aspekte natürlicher Personen durch automatisierte Verarbeitung. Danach sollte man weitere Listen prüfen, beispielsweise die Auflistung des Europäischen Datenschutzausschusses mit voraussichtlich hohem Risiko. Zuletzt wird geprüft ob das Risiko für Betroffene durch Art, Umfang, Umstände oder Zwecke der Verarbeitung erhöht wird. [Kon22] Die Schwellwert-Analyse ist der erste und entscheidende Schritt einer DSFA und durch die offen formulierten rechtlichen Vorschriften vor allem für Laien schwierig durchzuführen. Um Rechte und Freiheiten von Personen bestmöglich zu schützen, sollte insbesondere die Frage ob eine DSFA erforderlich ist, sorgfältig geprüft werden, daher fokussiert sich diese Ausarbeitung auf diesen Aspekt der DSFA. Als bekanntes Beispiel sei die sehr umfangreiche DSFA der bekannten Corona-Warn-App genannt, deren DSFA-Bericht öffentlich zugänglich und einsehbar ist [Rob22].

2.1.4. Risiko-Analyse

Über die online zugänglichen Informationsmaterialien der deutschen Datenschutzaufsichtsbehörden ist eine Excel-basierte Tabelle für das Risikomanagement zu einer Verarbeitungstätigkeit sowie eine Orientierungshilfe zur Risikoanalyse als PDF-Datei des bayerischen Landesbeauftragten für den Datenschutz öffentlich zugänglich [Bay22]. Diese Dokumente bieten Orientierung und Handlungsanleitung für eine Risikoabschätzung. Ein wichtiger zu beachtender Aspekt ist, dass im Datenschutz-Risikomanagement die Risiken aus Sicht der betroffenen Personen betrachtet werden. Zu jeder Verarbeitungstätigkeit müssen die Art der Schwachstelle, die Risikoquelle, das Risiko-Szenario, der Risiko-Index aus der Matrix ohne TOM, die TOM sowie der zu erwartende Risikoindex bei Wirksamkeit der TOM erfasst werden. Die Risikomatrix ist in Abbildung 2.2 dargestellt, der Index errechnet sich aus dem Produkt von Eintrittswahrscheinlichkeit und Schwere des Schadens.

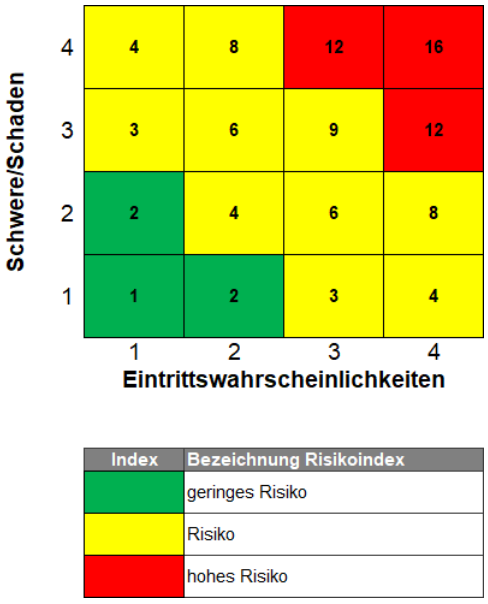

Abbildung 2.2.: Risikomatrix [Der18]

Grad	Bezeichnung des Grads	Eintrittswahrscheinlichkeit	
		Beschreibung	**Beispiel**
1	geringfügig	Schaden kann nach derzeitigem Erwartungshorizont nicht eintreten.	Befall durch Schadsoftware bei einem Stand-Alone Rechner, der an keinem Netzwerk angeschlossen ist und an dem keine weiteren Medien angeschlossen werden können.
2	überschaubar	Schaden kann zwar eintreten, aus bislang gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände scheint der Eintritt aber unwahrscheinlich zu sein.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware ausgestattet und nur mit einem BSI zertifizierten Firmennetzwerk verbunden ist.
3	substanziell	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände zwar möglich, aber nicht sehr wahrscheinlich zu sein.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware ausgestattet und direkt mit dem Internet verbunden ist.
4	groß	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände möglich und sehr wahrscheinlich zu sein.	Befall durch Schadsoftware bei einem veralteten Windows-XP Rechner ohne Antivirensoftware, der direkt mit dem Internet verbunden ist.

Tabelle 2.1.: Risiko Eintrittswahrscheinlichkeit [Der18]

Grad	Bezeichnung des Grads	Schwere der Folgen / möglicher Schaden	
		Beschreibung	**Beispiel**
1	geringfügig	Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Problemen überwinden können.	immateriell: leichte Verärgerung materiell: Zeitverlust physisch: vorübergehende Kopfschmerzen
2	überschaubar	Betroffene erleiden eventuell signifkante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.	immateriell: geringe, aber objektiv nachweisbare psychische Beschwerden materiell: deutlich spürbarer Verlust an privatem Komfort physisch: minderschwere körperliche Schäden (z. B. leichte Krankheit)
3	substanziell	Betroffene erleiden eventuell signifkante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.	immateriell: schwere psychische Beschwerden materiell: finanzielle Schwierigkeiten physisch: schwere körperliche Beschwerden
4	groß	Betroffene erleiden eventuell signifkante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.	immateriell: dauerhafte, schwere psychische Beschwerden materiell: erhebliche Schulden physisch: dauerhafte, schwere körperliche Beschwerden

Tabelle 2.2.: Risiko Schwere [Der18]

Tabelle 2.1 zeigt das Risiko der Eintrittswahrscheinlichkeit eines Schadens in den Ausprägungen geringfügig, überschaubar, substanziell und groß mit Bescheibung und Beispielen. Ähnlich aufgebaut ist Tabelle 2.2 mit dem Risiko der Schwere des Schadens. Für die Risikobeurteilung werden Eintrittswahrscheinlichkeit und Schwere des Schadens pro Verarbeitung und jeweils anhand der

Gewährleistungsziele Verfügbarkeit, Vertraulichkeit und Datenintegrität geprüft und die Risiken nach der Maximum-Methode zugeordet, d.h. pro Einzelrisiko wird der jeweils höchste Risikoindex dem SDM-Datensicherheitsziel zugeordnet.[Der18]

2.2. Technischer Rahmen

Das ODC ist eine Open Source Software, die nach eigenen Angaben die wesentlichen Funktionen, die DSGVO und BDSG für ein Datenschutz-Managementsystem (DSMS) fordern, enthält. Die Betreiber des ODC stellen eine kostenfreie und öffentlich zugängliche Demo-Version zur Verfügung, diese kann ohne Installation direkt im Browser verwendet werden. Eine schematische Darstellung ist Abbildung 2.3 zu entnehmen.

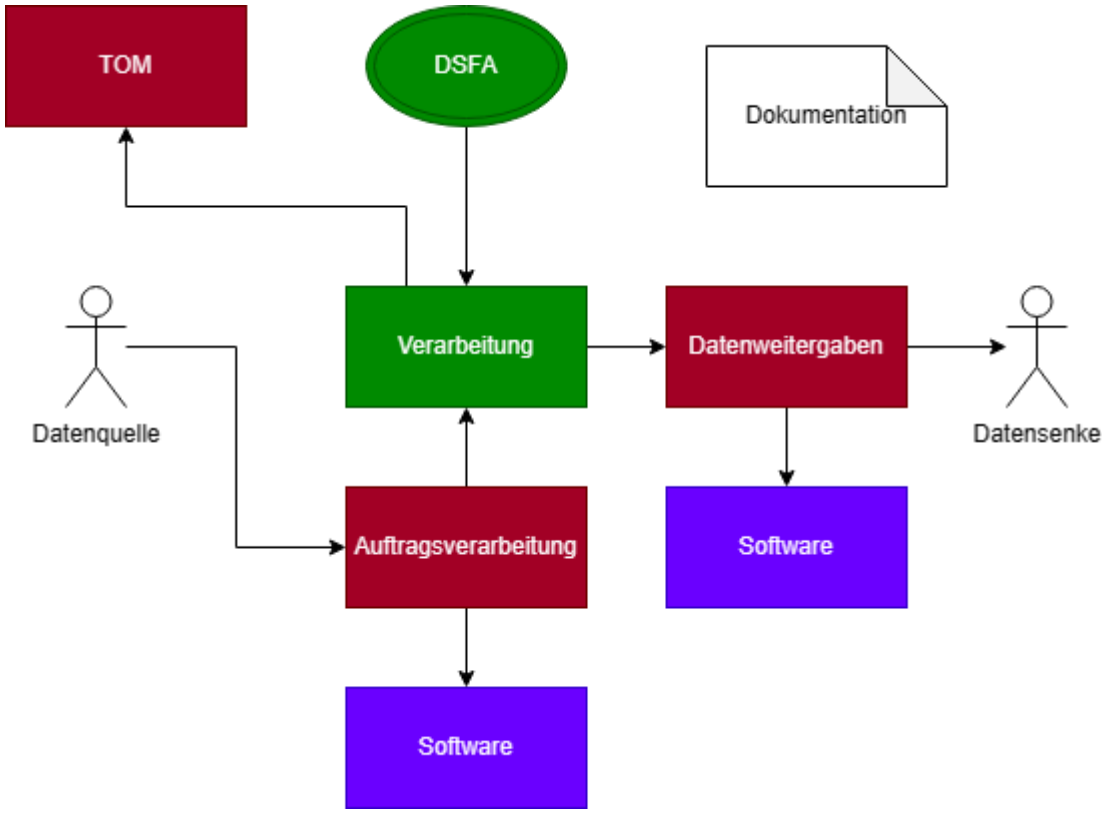

Abbildung 2.3.: Schematische Darstellung der Struktur des ODC

Als vereinfachte Beschreibung des ODC ausgehend von der Datenquelle werden Daten zugeordnet zu Datenkategorien, welche zugeordnete Eigenschaften besitzen, wie z.B. spezifische Löschkonzepte. Die Daten werden im Rahmen

einer Auftragsverarbeitung in Software abgebildet und der Datenverarbeitung zugeführt. Pro Verarbeitung können mehrere Datenweitergaben möglich sein, es können mehrere Dienstleister oder Anwendungen beteiligt sein. Die Verarbeitung steht im Zentrum, die Verarbeitungstätigkeit lässt sich umgekehrt auch ableiten von den Datenweitergaben. Für die Verarbeitung werden TOM verwaltet und die Datenweitergabe in Software, und Datensenke organisiert. Die Verarbeitungstätigkeit wird durch die DSFA ergänzt, diese besteht aktuell aus Freitextfeldern, welche durch Anwendende eigenständig ausgefüllt werden müssen. Alle wesentlichen Schritte werden im Verarbeitungsverzeichnis dokumentiert. [HH23] Das Dashboard des ODC ist in Abbildung 2.4 zu sehen. Die DSFA ist im ODC als Menüpunkt im Dashboard direkt zu finden oder über das Verarbeitungsverzeichnis. Nach aktuellem Stand besteht die DSFA im ODC aus Freitextfeldern in denen die Anwendenden ihre Ergebnisse eintragen können. Es ist möglich eine Risikobewertung einzutragen, diese ist in Abbildung 2.5 dargestellt, hierzu gibt es eine Auswahl an Fällen über ein Drop-down-Menü und Auswahl des Risikos, es ist selbst zu entscheiden, wie hoch das Risiko ist. Die Eintragungen werden vom ODC in einen Bericht übernommen, somit ist die Dokumentation gewährleistet.

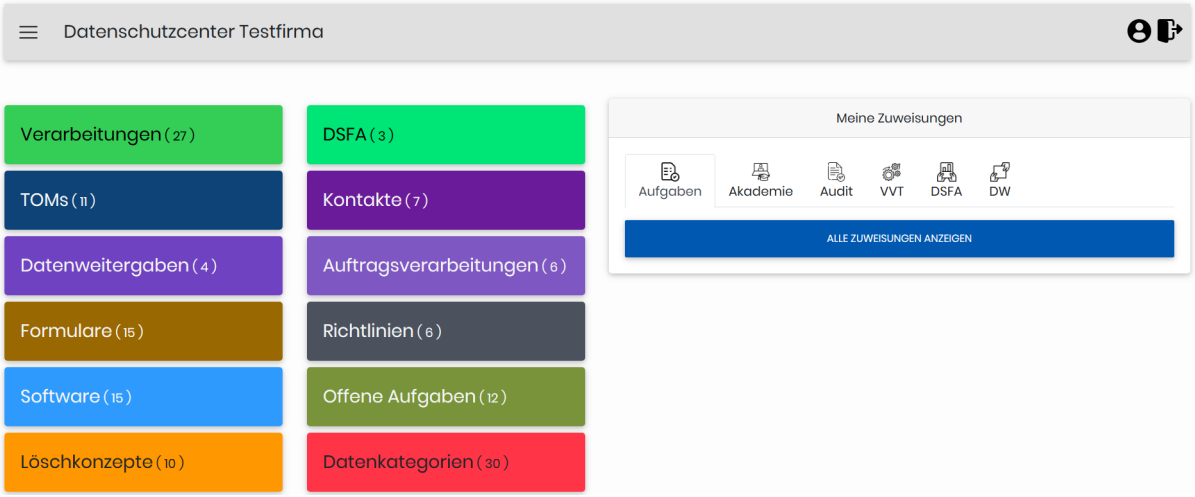

Abbildung 2.4.: Dashboard des ODC

Abbildung 2.5.: Risikoabschätzung im ODC

3. Verwandte Arbeiten

In diesem Kapitel werden verschiedene Arten verwandter Arbeiten vorgestellt. Dabei wird unterschieden zwischen wissenschaftlichen Arbeiten und Software. Abschließend werden die Erkenntnisse aus den verwandten Arbeiten zusammengefasst.

3.1. Wissenschaftliche Arbeiten

In [Fri+17] beschreiben Friedewald et al. einen Workflow für das Werkzeug Datenschutz-Folgenabschätzung (DSFA) und bieten damit Orientierung mit grundlegenden Informationen zur DSFA. Basierend auf dem Standard-Datenschutzmodell (SDM) wurde ein Workflow entwickelt, der Gesamtprozess zur Durchführung der DSFA ist in Abbildung 3.1 dargestellt. Hier wird der Prozess untergliedert in vier Phasen: Vorbereitungsphase, Durchführungsphase, Umsetzungsphase und Überprüfungsphase, sowie feingranularer in kleinere zusammenhängende Arbeitsschritte eingeteilt. Friedewald et al. stellen klar, dass es sich beim White Paper um Vorschläge für einen Prozess handelt, da es keinen allgemein akzeptierten Standard gäbe und sehen die DSFA als kontinuierlichen Prozess, der mehrmals durchlaufen wird und als eine Art „Frühwarnsystem“ um ungewollten Datenschutzrisiken vorzubeugen. In dem White Paper geht es um die Bereitstellung allgemeiner Informationen zum Prozess der DSFA. Diese Bachelorarbeit fokussiert sich darauf, ein Konzept zu entwickeln für die Umsetzung der DSFA in Software mit Schwerpunkt Schwellwert-Analyse und Risikoabschätzung.

Das Strategiepapier von Kloza et al. handelt von der Entwicklung einer Methode für die DSFA [Klo+20]. Es wird die Entwicklung eines mehrphasigen Prozesses für die DSFA beschrieben, dieser ist in Abbildung 3.2 dargestellt. Man hat zunächst eine generische Methode für die Folgenabschätzung entwickelt, die für viele Anwendungsfälle nutzbar sein soll und im zweiten Schritt an die Anforderungen von Europäische Union (EU) und Datenschutz-Grundverordnung (DSGVO) angepasst. Es wird darauf hingewiesen, dass diese Methoden nicht vollständig sind und Anleitungs- sowie Anpassungsbedarf besteht. Kloza et al. verweisen auch darauf, dass mehr Forschungsbedarf besteht für Themen wie die Bewertung der Risiken

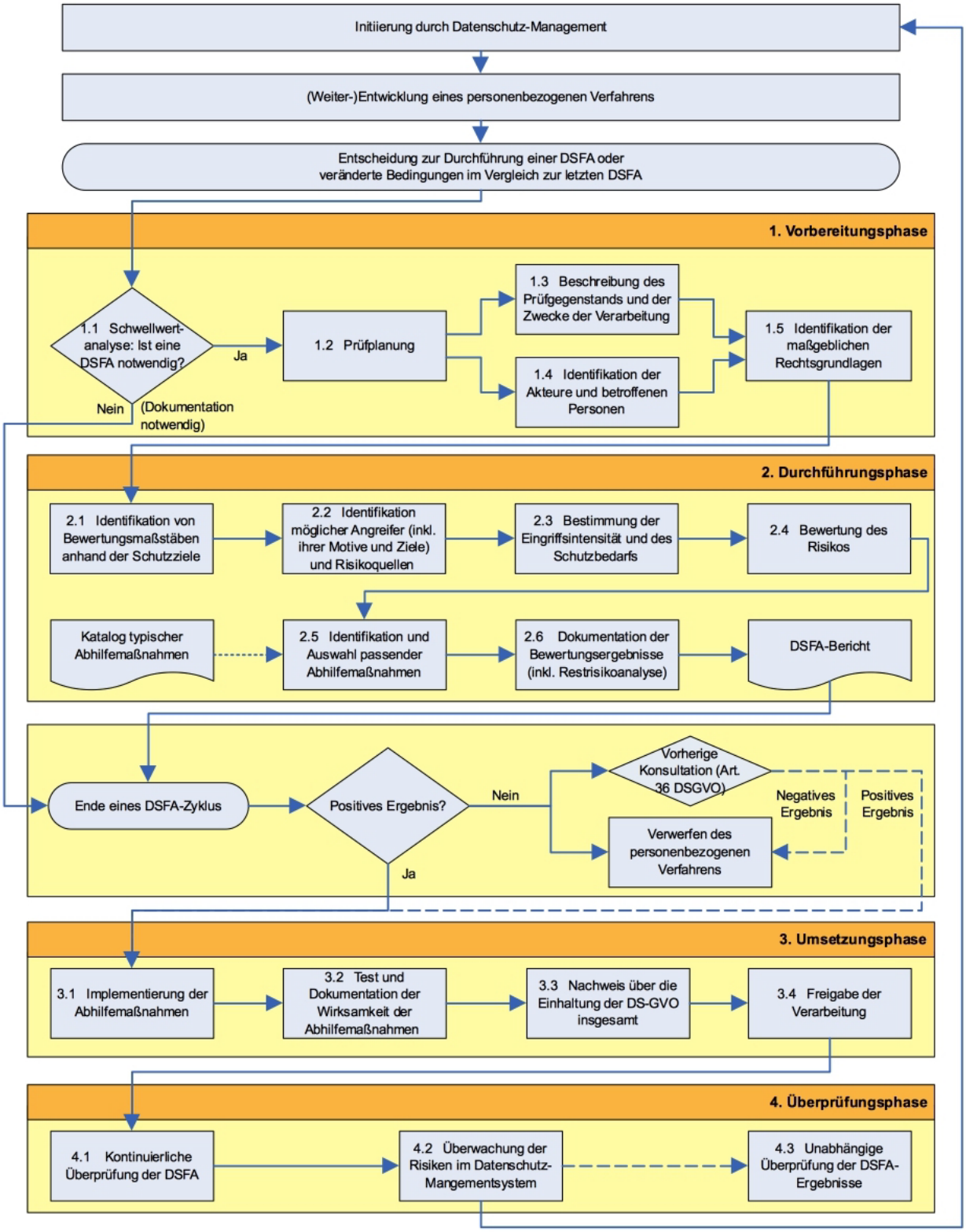

Abbildung 3.1.: Vorgehensweise für die Durchführung einer DSFA [Fri+17]

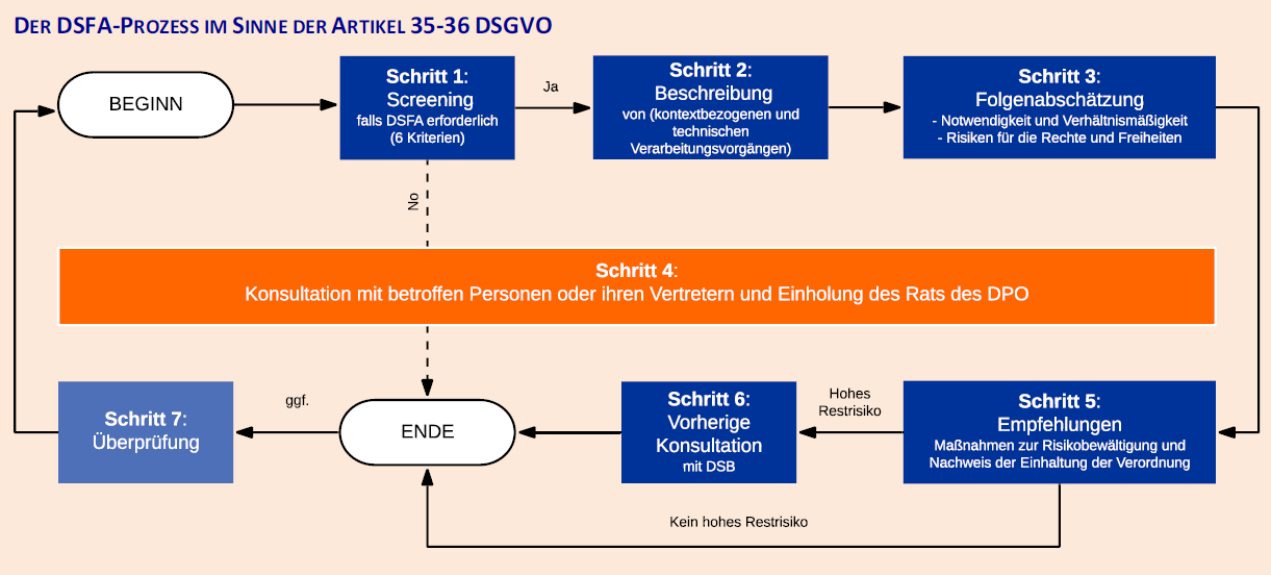

Abbildung 3.2.: DSFA-Prozess [Klo+20]

für die Rechte und Freiheiten natürlicher Personen. An dieser Stelle setzt diese Bachelorarbeit an, um die Risikobeurteilung weiter auszuarbeiten.

3.2. Software

Für die Gestaltung eines Datenschutz-Managementsystem (DSMS) gibt es verschiedene mögliche Ansätze. Stand-alone DSMS sind eigenständige Managementsysteme mit Fokus auf Datenschutzrisiken, aber ohne Nutzung von Synergien anderer Systeme. Als Erweiterung vorhandener Systeme können Synergien genutzt werden, beispielsweise Qualitätsmanagementsysteme, Compliance-Managementsysteme oder Informationssicherheitsmanagementsysteme. Aber die Zielsetzung kann problematisch sein, dies sollte geprüft werden, damit der Datenschutz gewährleistet wird. Ein weiterer Ansatz ist das integrierte DSMS, hier wird z.B. ein Informationssicherheitsmanagementsystem durch ein eigenes Anforderungswerk und Controls erweitert, somit werden Datenschutz- und Unternehmensrisiken kombiniert. [KSG19]

Basierend auf den genannten unterschiedlichen Ansätzen für DSMS wurden bei der Recherche eine Vielzahl von Systemen gefunden. Es wurde eine Auswahl getroffen an DSMS, welche nach eigenen Angaben Unterstützung bei der DSFA bieten. Die Anwendungen mit ihren relevantesten Eckdaten für diese Ausarbeitung wurden tabellarisch dargestellt, hierbei wird unterschieden zwischen den Open Source Anwendungen in Tabelle 3.1 und kommerziellen Anwendungen in Tabelle 3.2. Es sind

DSMS	Unternehmen	beworbene Funktionen	Besonderheiten	kostenfreie Demo	Bewertung
Datencockpit [Kno]	Knowledge Management Associates GmbH	unterstützt bei Dokumentation	MediaWiki basierend auf veröffentlichten Dokumenten Dritter	Zugang öffentlich	nicht relevant und aktuell nicht weiterentwickelt
PIA [CNI21]	CNIL	modulares Werkzeug zur Erfüllung von DSGVO Vorgaben	Software der französischen Datenschutzbehörde, Quellcode öffentlich auf Git	Zugang öffentlich	umfangreiche Dokumentation mit Hilfestellungen aus Knowledge Base
TSMONDO IT-Security & Compliance [Data]	Datenschutzeinfach.com (TSMONDO UG)	Datenschutz-Dokumentation	basiert auf Microsoft Office (Excel-Listen)	Zugang öffentlich, Download nicht möglich	Fokus auf Dokumenten, keine Softwaregeführte Abfrage oder Automatisierung
xmera Omnia [xme]	xmera Solutions GmbH	Managementsystem für Informationssicherheit und Datenschutz, unterstützt bei Planung, Durchführung, Überwachung und Dokumentation	geeignet für Unternehmen, Behörden und Bildungseinrichtungen. Web- und Datenbank-basierte modulare Erweiterung der Software Redmine	Demo nur als Bilder und Videos auf Webseite	Beurteilung nicht möglich

Tabelle 3.1.: Beispiele für Open Source Anwendungen

DSMS	Unternehmen	beworbene Funktionen	Besonderheiten	kostenfreie Demo	Bewertung
2B Advice PrIME [2B]	2B Advice GmbH	Integrierte Lösungen für das Risikomanagement in den Bereichen Datenschutz, Compliance und Risiken mit Dritten	cloud-basiertes DSMS mit SQL-Datenbanken	kostenfreien Zugang nach Anfrage erhalten	umfangreiche Funktionen, Vielzahl an vorgeschlagenen Fällen, kompetenter Kunden-Support, Beispiel-Mandat ist enthalten
Caralegal [Car]	caralegal GmbH	umfangreiche Funktionalitäten für die Optimierung der Datenschutzorganisation. intuitiver Workflow, vollständige Verknüpfung	unterstützt KI basiert bei der Schwellenwertanalyse und vereinfacht die Dokumentation risikobehafteter Verarbeitungstätigkeiten durch direkte Verknüpfung an das Verzeichnis von Verarbeitungstätigkeiten	angefragt, Demo nur im Rahmen einer Bestellung möglich	Beurteilung nicht möglich
Compliance-Kit [IITb]	IITR Datenschutz GmbH	Organisation von Dokumenten inkl. Vorlagen, keine Automatisierung o.ä.	zertifizierungsfähig nach ISO 27001 für große Unternehmen	angefragt, Demo nur im Rahmen einer Bestellung möglich	Fokus auf Dokumenten, keine Softwaregeführte Abfrage oder Automatisierung
Datenschutz-Kit [IITa]	IITR Datenschutz GmbH	Organisation von Dokumenten inkl. Vorlagen, keine Automatisierung o.ä.	Basisthemen zum Datenschutz für kleine Unternehmen	angefragt, Demo nur im Rahmen einer Bestellung möglich	Fokus auf Dokumenten, keine Softwaregeführte Abfrage oder Automatisierung
DPMS [DPM]	DPMS – Data Protection Management System	DSGVO konformes Datenschutzmanagement	Software-unterstützte Planung, Durchführung und Kontrolle der Datenschutz-Folgenabschätzung	kostenfreien Zugang nach Anfrage erhalten	Umfrangreiche Funktionen mit Bereitstellung von Beispielen und Vorlagen
Privacy and Data Governance Cloud [One]	OneTrust Technology Limited	Verzeichnis von Verarbeitungstätigkeiten, Bewertungsautomatisierung, taggleiche Updates zu weltweiten Datenschutzregularien, automatische Erfassung und Erfüllung von Betroffenen- und Verbraucheranfragen	globale Datenschutz- und Sicherheitsgesetze integriert	angefragt (keine Rückmeldung erhalten)	Beurteilung nicht möglich

Tabelle 3.2.: Beispiele für kommerzielle Anwendungen

nicht bei allen Softwares kostenlose Demo-Versionen verfügbar und viele Softwares bieten wenig softwaregeführte Unterstützung, sondern lediglich Dokumenten-Management an.

Nach Abwägung der Relevanz wurden zur genaueren Betrachtung die Open Source Software PIA der Commission Nationale de l'Informatique et des Libertés (französische Datenschutzbehörde) (CNIL), sowie die kommerzielle Anwendung 2B Advice PrIME der deutschen 2B Advice GmbH ausgewählt.

Die PIA ist eine Open Source Anwendung, der Quellcode ist in GitHub öffentlich verfügbar und die Software ist in vielen europäischen Sprachen verfügbar. Zusätzlich werden öffentlich zugängliche Dokumente bereitgestellt mit Methoden [CNI15], Templates [CNI18a] und Knowledge Bases [CNI18b] für die Durchführung einer DSFA. PIA ist angelehnt an den englischen Begriff „privacy impact assessment", was übersetzt für DSFA steht. Sie wurde von der CNIL entwickelt und von weiteren europäischen Datenschützern weiterentwickelt und übersetzt. Die Software kann helfen, den Prozess zu vereinfachen und die Einhaltung der Datenschutzbestimmungen gemäß der DSGVO zu erleichtern. Man hat innerhalb der Anwendung Zugriff auf die umfangreiche Knowledge Base in welcher Hinweise zu Begrifflichkeiten und Ausfüll-Beispiele hinterlegt sind. [CNI21]

Die 2BAdvice GmbH hat ihren Ursprung im Consulting; da große Unternehmen betreut werden, gibt es seit 2003 ein eigenes Datenschutzsystem. Es wurde nach Anfrage eine kostenfreie Einzelplatzlizenz zur Verfügung gestellt und in einem online-Meeting vorgestellt. Das 2B Advice PrIME läuft browserbasiert mit einem SQL-Server im Hintergrund und deckt alle Aspekte des Datenschutzes ab. In der Software ist die Dokumentation des Unternehmens abgebildet, hier können einzelne Standorte einzeln eingepflegt werden. Die Verarbeitung unterteilt sich in Kategorien bzw. Abteilungen. Bei der Risikobewertung lässt sich optional die Kritikalität einschalten, hier kann vom Anwendenden selbst ein numerischer Schwellwert hinterlegt werden, welcher anzeigt ob ein hohes Risiko vorliegt. Bei der in der Anwendung durchführbaren Schwellwertanalyse können Rechtsgrundlagen ausgewählt werden, beispielsweise die Rechtspflicht, welche als nicht kritisch eingestuft wird, da diese besagt, dass Daten auf Grund einer rechtlichen Pflicht verarbeitet werden müssen, wie beispielsweise Abführung von Lohnsteuer ans Finanzamt. Die Rechtsgrundlage der Verarbeitung nach Einwilligung kann kritisch eingestuft werden, da diese Einwilligung von Betroffenen zurückgezogen werden kann – in dem Fall muss die Löschung aller Daten erfolgen. Bei mindestens drei erfüllten Risiken für betroffene Personen muss eine DSFA durchgeführt werden. Diese wird in einem Bericht dokumentiert, welchen die Software bereitstellt. Die Anwendung stellt auch einen TOM-Fragekatalog zur Verfügung, in diesem sind mögliche technische und organisatorische Maßnahmen (TOM) hinterlegt, diese können genutzt und in der Risikomatrix beurteilt werden um welchen Anteil das jeweilige Risiko sinkt

durch die Einführung der jeweiligen Maßnahme. Die Verantwortlichen sehen die Einführung einer Automatisierung von Entscheidungsprozessen aus datenschutzrechtlicher Sicht kritisch. Diese kann unter das Verbot von ausschließlich automatisierten Entscheidungen wie Profiling nach Art. 22 DSGVO fallen, sowie selbst der Pflicht zur DSFA unterliegen nach Art. 35 wegen eines hohen Risikos bei automatisierter Verarbeitung und ggf. auch durch Nutzung neuer Technologien wie künstlicher Intelligenz. Daher hat man die DSFA nicht automatisiert, sondern soweit vorbereitet, dass die Berichterstellung möglich ist und Hilfestellungen durch Vorschläge der Anwendung gegeben werden, die Entscheidungen über Art und Höhe von Risiken sowie der Anteil von Risikominimierung durch TOM müssen von Menschen getroffen werden. [2B]

3.3. Erkenntnisse

Rechtliche Anforderungen technisch abzubilden ist auf Grund der unterschiedlichen Fachbereiche eine große Herausforderung. Da Gesetzesgrundlagen wie die DSGVO in der Regel offen und allgemein formuliert sind um möglichst viele Fälle abzudecken, ist es für Laien schwierig diese Gesetze präzise auf eigene Fälle anzuwenden. Die beschriebenen wissenschaftlichen Arbeiten beschreiben eher allgemein Methodik und Prozesse. Die Anzahl an Anwendungen scheint zunächst umfangreich zu sein, aber bei genauerer Betrachtung beziehen sich viele Anwendungen auf die Unterstützung bei Dokumentationsmanagement und nicht jedes Unternehmen stellt umfangreiche Informationen zur Verfügung, weshalb die Beurteilung über die Funktionsweise der jeweiligen Anwendung eingeschränkt ist. Vor allem das Gespräch mit der 2B Advice GmbH war sehr aufschlussreich, insb. der Hinweis die Automatisierung von Prozessen unter datenschutzrechtlichen Gesichtspunkten kritsch zu hinterfragen. Da bei der DSFA wichtige Entscheidungen getroffen werden, welche Folgen für Betroffene haben können und vor den Aufsichtsbehörden begründet werden müssen, wird diese Ausarbeitung nach aktuellem Stand von Recht und Technik, von einer Automatisierung der Entscheidungen in der DSFA absehen. Um einen Einklang zwischen Bedürfnissen von Software-Anwendenden sowie rechtlichen Vorschriften herzustellen, wird eine softwareseitige Unterstützung ohne Automatisierung angestrebt.

4. Konzept und Design

In diesem Kapitel werden die Erkenntnisse aus dem vorherigen Kapitel 3 genutzt, um basierend auf den Anforderungen die sich aus den rechtlichen Vorschriften der Datenschutz-Folgenabschätzung (DSFA) im Zusammenhang mit den technischen Gegebenheiten des Open Datenschutzcenter (ODC), ein Konzept zu beschreiben für die DSFA mit Fokus auf Schwellwert-Analyse und Risikoabschätzung. Es wird erläutert in welcher Form ein Konzept zur DSFA im ODC umsetzbar ist, sowie ein Design vorgestellt.

4.1. Anforderungen

Zur Beurteilung aller möglichen Anforderungen – sowohl juristisch, als auch technisch sowie für die Praxis – wurden gesetzliche Anforderungen aus der Datenschutz-Grundverordnung (DSGVO) abgeleitet. Regelmäßige Besprechungen mit dem Entwickler des ODC, sowie Befragung des Datenschutzbeauftragten der Universität der Bundeswehr München, wurden genutzt um technische Anforderungen aufzustellen und die Realisierbarkeit zu diskutieren.

Nach einem Gespräch mit dem Datenschutzbeauftragten der Universität der Bundeswehr München, wurde deutlich, dass der wichtigste Schritt im Prozzes der DSFA die zu Beginn stehende Schwellwertanalyse ist. Das Ergebnis dieser Analyse entscheidet darüber, ob eine DSFA durchgeführt werden muss und ob im Falle eines hohen Risikos vor der Verarbeitung die Aufsichtsbehörde konsultiert werden muss. Vor allem für Laien ist diese Analyse schwierig, da die gesetzlichen Regelungen sehr allgemein formuliert sind und es keine Definition des Risikos im Gesetz gibt, welches sich aus dem Produkt von Eintrittswahrscheinlichkeit und Schadenshöhe zusammensetzt. Hier anzusetzen mit einer für Laien verständlichen softwaregeführten Schwellwertanalyse mit anschließender Unterstützung bei der DSFA und Hilfestellung bei Identifizierung von Risiken und Maßnahmen, wäre die ideale Softwarelösung aus Sicht von Nutzenden.

Die Anforderungen an ein Konzept erschließen sich aus der Kombination aller Interessen und Hintergründe. So steht in erster Linie die Benutzbarkeit für den Anwendenden im Fokus, eine Software soll so gestaltet sein, dass sie auch

für Laien verständlich ist und sie durch die wesentlichen Schritte der DSFA führt und Verweise bietet zu Hintergründen und Erklärungen von Begriffen. Die Software selbst muss im Einklang mit den gesetzlichen Anforderungen stehen (Compliance), sie muss so konzipiert sein, dass die Nutzung selbst kein hohes Datenschutzrisiko darstellt. Im Zusammenspiel zwischen Benutzbarkeit und Compliance ergibt sich, dass eine Automatisierung der DSFA zwar eine hohe Arbeitserleichterung für Datenschutzbeauftragte bieten würde, allerdings auch ein hohes Datenschutzrisiko dem entgegensteht. Wie in Kapitel 3 beschrieben müssen die Entscheidungen im Prozess der DSFA von Menschen selbst getroffen und begründet werden. Somit kann an dieser Stelle ein strukturierter Aufbau sowie die Anzeige von Begriffserklärungen eine softwareseitige Hilfstellung bieten. Die Dokumentation ist zwar gesetzlich verankert, aber als wichtiger Bestandteil der DSFA wird sie einzeln aufgeführt und genannt, da sie als Nachweis der DSFA gegenüber den Aufsichtsbehörden dient. Sie sollte möglichst automatisch von der Software anhand der getätigten Eingaben generiert werden, sodass Anwendende die wichtigsten Informationen in die Dokumentation übernehmen können. Die Erweiterbarkeit soll bei möglichen Änderungen von rechtlichen oder technischen Bedingungen die Anpassung einer bestehenden Anwendung ermöglichen.

Folgende Anforderungen wurden identifiziert:

- Benutzbarkeit
- Compliance
- Dokumentation
- Erweiterbarkeit

Diese Anforderungen werden nachfolgend in das Konzept einfließen. Sie sind die wichtigsten Rahmenbedingungen für die Ausgestaltung des Konzepts und stellen in Kapitel 5 die Grundlage der Evaluation dar.

4.2. DSFA im ODC

Die DSFA im ODC ist im Dashboard oder über das Verarbeitungsverzeichnis zu finden. Nach aktuellem Stand besteht die DSFA im ODC aus Freitextfeldern in denen die Anwendenden ihre Ergebnisse eintragen können. Es ist möglich eine Risikobewertung einzutragen, hierzu gibt es eine Auswahl an Fällen über ein Dropdown-Menü und Auswahl des Risikos, es ist selbst zu entscheiden, wie hoch das Risiko ist. Die Eintragungen werden vom ODC in einen Bericht übernommen, somit ist die Dokumentation gewährleistet. Die Erweiterung der Funktionen um eine

standardisierte Abfrage der Schwellwert-Analyse mit Unterstützung bei Identifizierung der Risiken und Darstellung des Ergebnisses in einer Risikomatrix, sowie Vorschlag von geeigneten Maßnahmen, wird im folgenden Konzept im Abschnitt 4.3 beschrieben und ein Design-Vorschlag in Abschnitt 4.4 vorgestellt.

4.3. Konzept

Zur bestmöglichen Vereinbarung von Anforderungen mit technischer Infrastruktur fokussiert sich diese Ausarbeitung auf die Schwellwertanalyse inkl. Risikoanalyse. Dafür werden verschiedene Quellen genutzt. Es werden die öffentlich zugänglichen und europaweit ausgearbeiteten Dokumente der Commission Nationale de l'Informatique et des Libertés (französische Datenschutzbehörde) (CNIL) verwendet, welche bereits in dieser Ausarbeitung referenziert und zitiert wurden. Insbesondere die Templates [CNI18a] und Knowledge Bases [CNI18b] wurden zur Inspiration für dieses Konzept genutzt. Außerdem wurden die „Checkliste für Datenverarbeitung (DV) inkl. Datenschutzfolgenabschätzung (DSFA)“ des Bundesministerium der Verteidigung (BMVg) verwendet, da sie sowohl ausführlich als auch einfach verständlich ist und ein ergänzendes Merkblatt mit Erläuterungen ebenfalls vorliegt zur Orientierung. [BMV23b] [BMV23a]

Die Grundidee der Konzeption ist der Fokus auf die Schwellwert-Analyse, eine graphische Darstellung ist in Abbildung 4.1 abgebildet. Innerhalb des ODC knüpft die DSFA direkt an die Verarbeitung im Verarbeitungsverzeichnis an. Zur Klärung der initialen Frage, ob eine DSFA verpflichtend durchgeführt werden muss, startet der Prozess der Schwellwert-Analyse. Zu Dokumentationszwecken wird die Abfrage der Rechtsgrundlage für die Verarbeitung über ein Drop-Down-Menü abgefragt, alternativ kann diese durch bereits an anderer Stelle eingegebene Daten zu der jeweiligen Verarbeitung vorgeschlagen werden. Als nächstes werden die Listen der Aufsichtsbehörden abgefragt, wenn mindestens ein mal „ja“ auf der MUSS-Liste ausgewählt wird, besteht eine Pflicht zur DSFA. An dieser Stelle können zukünftig Negativ-Listen eingebunden werden, sollten die Aufsichtsbehörden von der Möglichkeit Gebrauch machen Fälle zu identifizieren, bei denen die Durchführung einer DSFA ausgeschlossen wird. Wird kein „ja“ auf der MUSS-Liste ausgewählt, wird eine Risiko-Anaylse durchgeführt zur Identifizierung und Bewertung der Risiken. Ist das Ergebnis kein hohes Risiko, besteht keine Pflicht zur DSFA, besteht ein hohes Risiko, so ist eine DSFA durchzuführen. Bei bestehender Pflicht zur DSFA soll die Anwendung Hinweise geben, dass technische und organisatorische Maßnahmen (TOM) durchgeführt werden müssen, hier werden softwareseitige Vorschläge angezeigt. Nach Auswahl bzw. Eingabe der TOM wird eine zweite Risikoanalyse fällig, in welcher durch die Anwendenden selbst bewertet wird wie hoch das Risiko nach Einführung der TOM eingeschätzt wird. Bleibt das

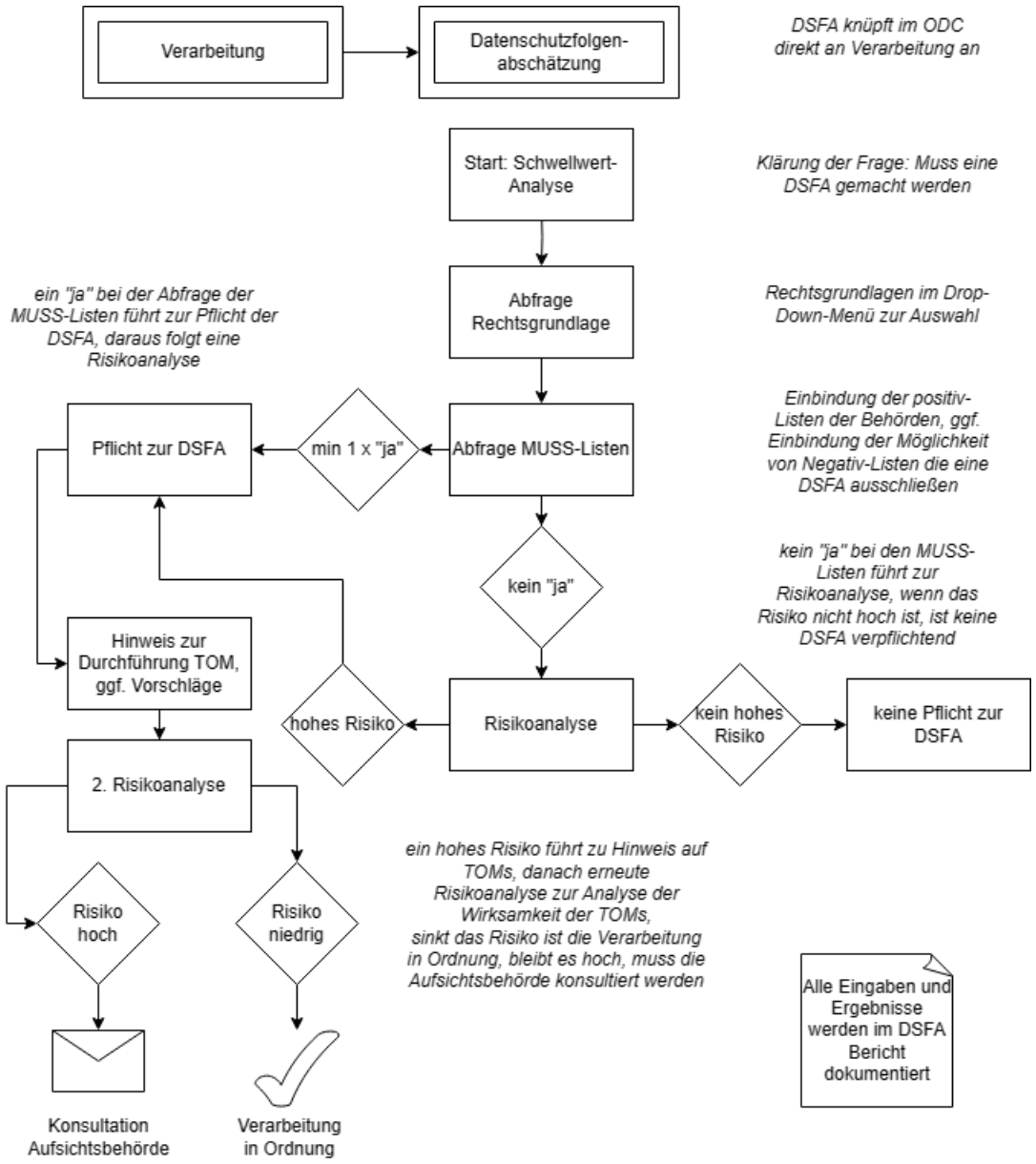

Abbildung 4.1.: Konzept der Einbindung der DSFA ins ODC

Risiko	Hauptrisikoquellen	Primäre Bedrohungen	Größte potentielle Risiken	Wesentliche Maßnahmen zur Reduzierung von Schwere und Eintrittswahrscheinlichkeit	Schwere	Eintrittswahrscheinlichkeit
Unbefugter Datenzugriff						
Unerwünschte Datenänderung						
Datenverlust						

Tabelle 4.1.: Risiko Identifikation [CNI18a]

Risiko-Beurteilung	Akzeptabel / Verbesserungswürdig?	Korrekturmaßnahmen	Restschwere	Rest-Eintrittswahrscheinlichkeit
Unbefugter Datenzugriff	[Der Verantwortliche muss feststellen, ob die vorhandenen oder geplanten Maßnahmen dieses Risiko ausreichend reduzieren, um es als akzeptabel einzustufen.]	[Wenn zutreffend, sollen hier etwaige zusätzliche Maßnahmen angegeben werden, die erforderlich wären.]		
Unerwünschte Datenänderung	[Der Verantwortliche muss feststellen, ob die vorhandenen oder geplanten Maßnahmen dieses Risiko ausreichend reduzieren, um es als akzeptabel einzustufen.]	[Wenn zutreffend, sollen hier etwaige zusätzliche Maßnahmen angegeben werden, die erforderlich wären.]		
Datenverlust	[Der Verantwortliche muss feststellen, ob die vorhandenen oder geplanten Maßnahmen dieses Risiko ausreichend reduzieren, um es als akzeptabel einzustufen.]	[Wenn zutreffend, sollen hier etwaige zusätzliche Maßnahmen angegeben werden, die erforderlich wären.]		

Tabelle 4.2.: Risiko Beurteilung [CNI18a]

Risiko hoch, muss die Aufsichtsbehörde konsultiert werden, sinkt das Risiko auf ein akzeptables Niveau, ist die Verarbeitung in Ordnung und kann durchgeführt werden. Alle Eingaben und Ergebnisse werden in einem DSFA-Bericht dokumentiert. Die Einbindung von MUSS-Listen der Aufsichtsbehörden sowie die Checkliste vom BMVg werden zur gezielten Ja/Nein-Abfrage genutzt. Als Ausfüllhilfe werden an den entsprechenden Abfrage-Stichworten weitere Informationen und Erklärungen hinterlegt, welche aus der zugehörigen Merkliste des BMVg zu entnehmen sind.

Die Risikoanalyse wird mit Abfrage von Risikoart, Eintrittswahrscheinlichkeit und Schadenshöhe und Einbindung des Ergebnisses in eine Risikomatrix gestaltet. Zur Risikobeurteilung entsprechend des Standard-Datenschutzmodell (SDM) sind die drei Phasen Risikoidentifikation, Abschätzung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden, sowie Zuordnung zu Risikoabstufungen zu durchlaufen. [Dat18] Basierend auf der Software und den Dokumenten der CNIL kann die Risikoanalyse strukturiert werden. Die Abfrage erfolgt nach Vorlage des Risk Assessment[CNI18a], die Risiko-Identifikation ist in Tabelle 4.1 und die Risiko-

Arten von Risikoquellen	Beispiele
Interne menschliche Quellen	Mitarbeitende, IT-Manager, Auszubildende, Führungskräfte
Externe menschliche Quellen	Empfänger personenbezogener Daten, autorisierte Dritte, Dienstleister, Hacker, Besucher, ehemalige Mitarbeitende, Aktivisten, Konkurrenz, Kunden, Wartungspersonal, Wartung, Angreifer, Gewerkschaften, Journalisten, Nichtregierungsorganisationen, kriminelle Organisationen, Organisationen unter der Kontrolle eines fremden Staates, terroristische Organisationen, nahegelegene industrielle Aktivitäten
Nicht-menschliche Quellen	Bösartiger Code unbekannter Herkunft (Viren, Würmer usw.), Wasser (Leitungen, Wasserwege usw.), entzündliche, korrosive oder explosive Materialien, Naturkatastrophen, Epidemien, Tiere

Tabelle 4.3.: Beispiele Riskoquellen [CNI18b]

Beurteilung ist in Tabelle 4.2 dargestellt. Hier werden Schwere und Eintrittswahrscheinlichkeit vom Anwendenden mit Zahlen bewertet, 1 steht für geringfügig, 2 für überschaubar, 3 für substanziell und 4 für ein sehr großes Risiko, ähnlich wie bereits in Kapitel 2.1.4 beschrieben. An dieser Stelle werden für den Anwendenden Hilfestellungen verlinkt sein: wie beispielhaft in Tabelle 4.3 aufgeführt werden Vorschläge von möglichen Risikoquellen genannt. Aus der numerischen Zuordnung von Risiken kann die Software Werte errechnen für eine Risiko-Matrix, in der wie in Abbildung 4.4 beispielhaft dargestellt, Risiken vor und nach Einführung von TOM visuell anzeigen lassen. Die Berechnung erfolgt durch Multiplikation der Werte von Schwere und Eintrittswahrscheinlichkeit, daraus ergeben sich Indices, die sich wie in Kapitel 2.1.4 in Abbildung 2.2 dargestellt zuordnen lassen: 1-2 geringes Risiko, 3-9 Risiko, 12-16 hohes Risiko. Bei Eingabe von TOM können Anwendende selbst eingeben um welchen prozentualen Wert ein Einzelrisiko sinkt, dann wird das Restrisiko ermittelt und ebenfalls anhand der Indices der Risikomatrix bewertet. Bleibt das Risiko hoch erscheint ein Hinweis für die Konsultation der Aufsichtsbehörden, auf Wunsch können Datenschutzbeauftragte Kontaktdaten der zuständigen Aufsichtsbehörde hinterlegen, die an dieser Stelle angezeigt werden.

4.4. Design

Als Hilfestellung für die nachfolgende Implementierung dieses ausgearbeiteten Konzepts wurden Mockups für die Schritte Schwellwertanalyse und Risikoanalyse erstellt. Dadurch werden die Vorgaben an das Design mit beispielhaften Inhalten visuell dargestellt, um die Softwareentwicklung zu unterstützen. Die Schwellwertanalyse ist für jede Verarbeitungstätigkeit einzeln zu erstellen, sie ist in Abbildung 4.2 zu sehen. Hier wurden Info-Buttons an jedem Schritt eingefügt, beim Klick auf den Kreis mit einem „i“ öffnet sich ein Fenster in dem Beispiele für die

auszuwählenden Antworten aufgeführt werden. Die Rechtsgrundlagen sind verknüpft mit der Verarbeitung, die Inhalte werden automatisch aus der vorherigen Eingabe übernommen oder können manuell eingefügt werden, eine Änderung wird ebenfalls die Eingabe in der Verarbeitung anpassen. Die Auswahl der Fälle für die Muss-Listen wurde aus der aktuellen Liste der Datenschutzkonferenz [Datb] übernommen. Hier können mehrere Auswahlen getroffen werden. Wird ausschließlich „Nicht zutreffend“ ausgewählt, geht es weiter mit der Risiko-Analyse. Wird mindestens einer der aufgeführten Fälle ausgewählt, so weist die Anwendung darauf hin, dass die DSFA auf jeden Fall verpflichtend durchgeführt werden muss und verweist auf die Durchführung von TOM mit einer beispielhaften Liste, diese kann aus der PIA Knowledge Base [CNI18b] und aus dem Merkblatt des BMVg [BMV23a] zusammengestellt werden. Anschließend geht es weiter zur Risikoanalyse.

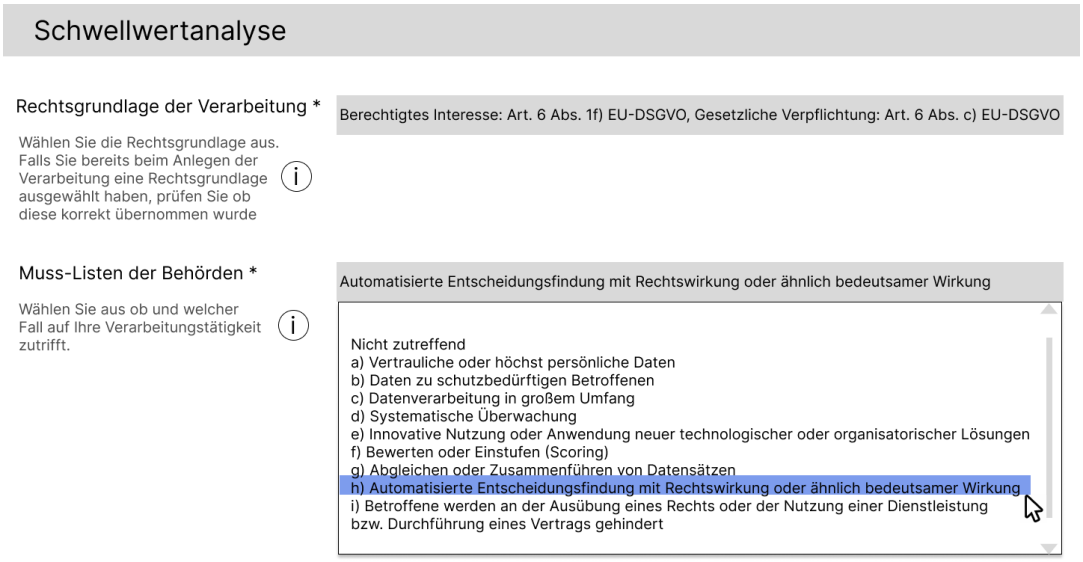

Abbildung 4.2.: Design Schwellwertanaylse

Das Design der Risikoanalyse ist in Abbildung 4.3 dargestellt. Im ersten Schritt der Risikoanalyse werden die Risiken identifiziert. Hier ist es möglich die Art des Risikos über eine Dropdown-Liste auszuwählen, auch eine Freitexteingabe ist möglich, falls keine der vorgeschlagenen Risikoarten passen sollte. Die zur Auswahl stehenden Inhalte werden wie zuvor aus den vorhandenen Dokumenten entnommen. Über ein Freitextfeld können Informationen zu Hauptrisikoquellen, primären Bedrohungen und größten potentiellen Risiken eingetragen werden. Der Grad von Risiko-Schwere und Eintrittswahrscheinlichkeit wird durch einen anklickbaren Schieberegler ausgewählt, hier sind wie in Kapitel 4.3 erläutert, ganzzahlige

numerische Parameter auswählbar mit den Zahlen 1-4. Bei der Risikobeurteilung wird das zuvor genannte Einzelrisiko automatisch übernommen, hier ist keine Auswahl möglich. Im Freitextfeld können Informationen zu TOM aus bereits vorhandenen Eingaben automatisch eingefügt werden oder manuell eingetragen. Zur Auswahl des Restrisikos nach Korrekturmaßnahmen gibt es Schieberegler, bei denen nur gleiche oder kleinere Werte ausgewählt werden als beim initialen Risiko, die Restrisiken können nicht größer sein als die Ausgangswerte. Wie bei der Schwellwertanalyse gibt es wieder zu jedem Schritt einen Info-Button mit Informationen und Beispielen als Ausfüllhilfen für Laien.
Es werden nur Einzelrisiken bewertet. Jedes Risiko kann einzeln hinzugefügt werden und wird getrennt von anderen Risiken beurteilt. Nur so ist eine genaue und individuelle Risikoanalyse möglich. Durch die automatische Übernahme des beschriebenen Einzelrisikos von der Risiko Identifikation in die Risiko Beurteilung kann die Beurteilung des Restrisikos nicht vergessen oder verwechselt werden, somit wird die Dokumentation vollständig und die Anwendenden werden darin unterstützt sich mit Maßnahmen zur Risikominimierung auseinanderzusetzen.

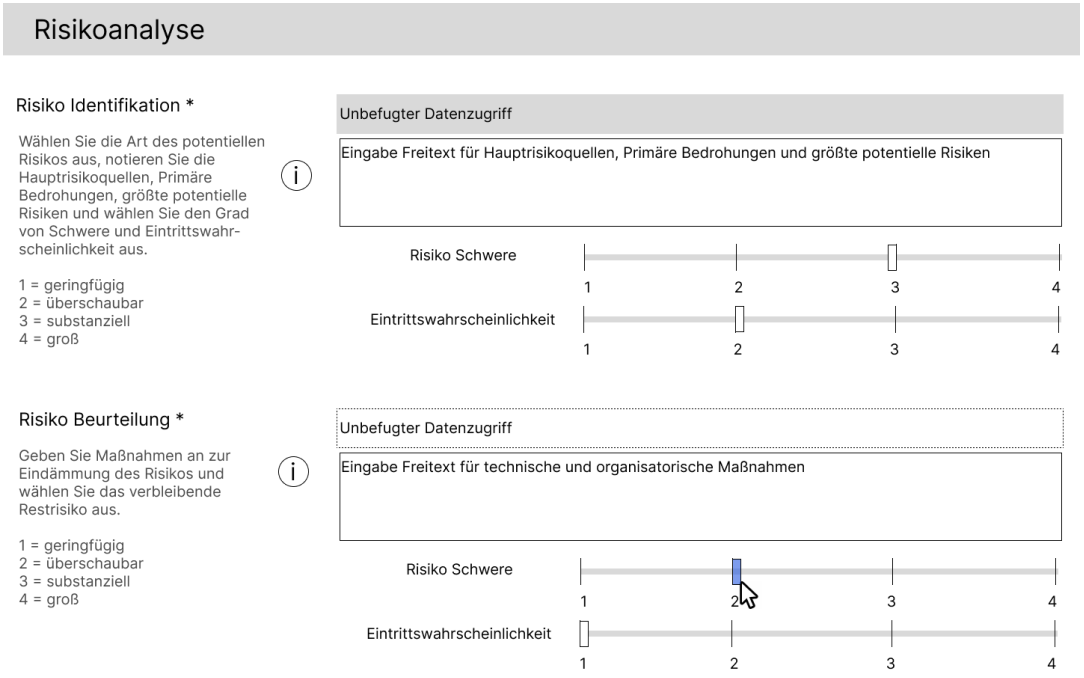

Abbildung 4.3.: Design Risikoanalyse

Das Ergebnis des gesamten Prozesses aus Risikoanalyse und der Angabe um

welchen Grad die TOM das Risiko eindämmen können, wird visuell dargestellt in einer Risiko-Matrix, in der die Schwere und Eintrittswahrscheinlichkeit mit ihrer Zuordnung von 1-4 in Relation zueinander gesetzt werden. Nach Vorbild der französischen Datenschutzbehörde [CNI18a] wurde Abbildung 4.4 für diese Ausarbeitung ins Deutsche übersetzt, hier sind die ursprünglichen Risiken in grau und die verbleibenden Restrisiken nach TOM in gelb dargestellt.

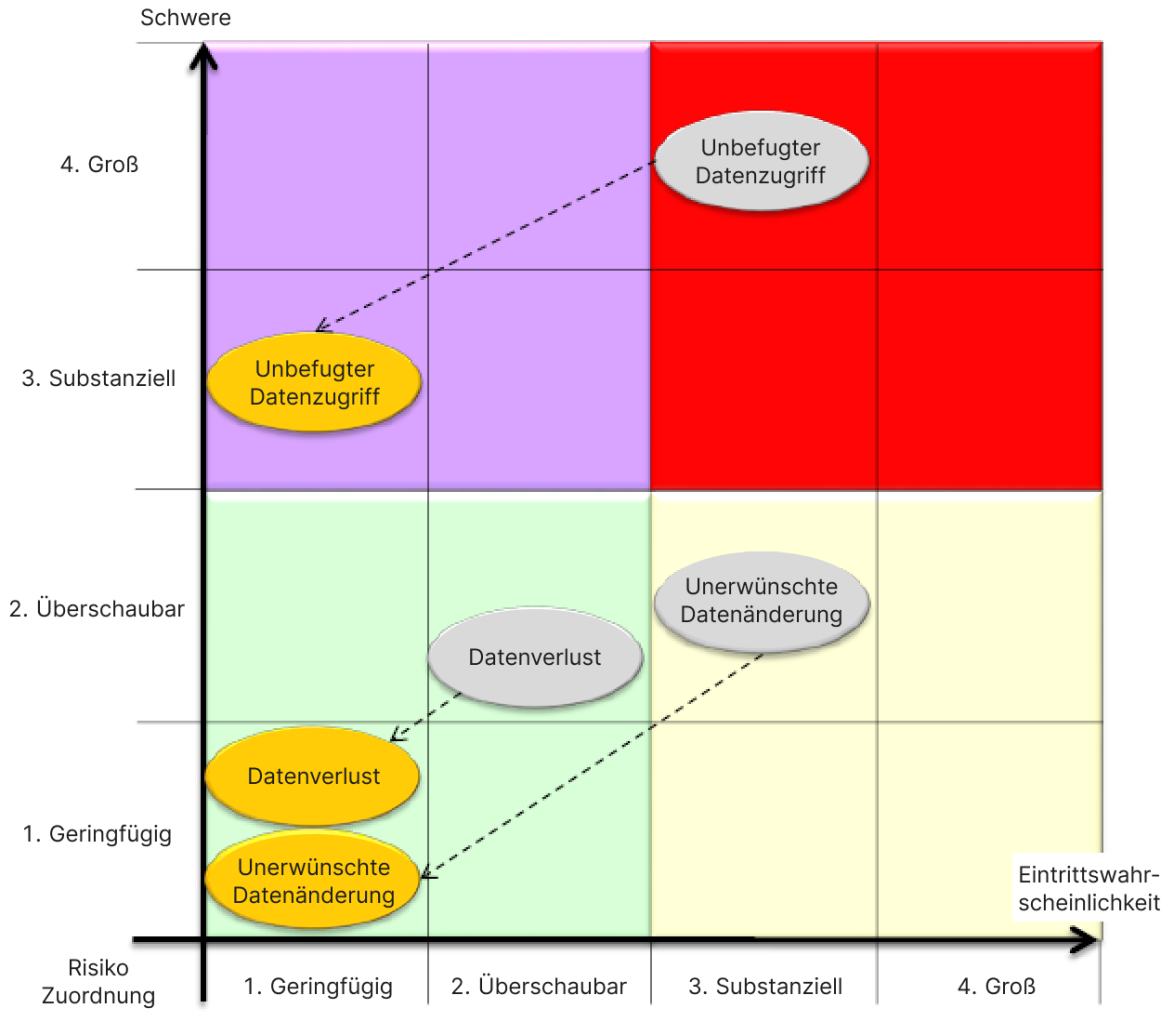

Abbildung 4.4.: Risiko Zuordnung

4.5. Diskussion

Durch den Umfang an komplexen Anforderungen von juristischer und technischer Seite wurde nur ein Teil der Bestandteile der DSFA betrachtet, der Fokus liegt hier auf Schwellwert-Analyse und der Risikobeurteilung, welche weiteres Forschungs- und Optimierungspotential bieten. Da eine umfängliche Automatisierung in einem Beurteilungs- und Entscheidungsprozess ein hohes Risiko aufweist, musste beachtet werden, dass die Entscheidungen von Menschen getroffen werden müssen, hier kann softwareseitig nur Hilfestellung gegeben werden. Die technische Implementierung sowie die Betrachtung weiterer Aspekte können im Rahmen von nachfolgenden Abschlussarbeiten untersucht werden. Folgende Themen können in weiteren Ausarbeitungen behandelt werden:

- Implementierung dieses Konzepts ins ODC
- Ergänzungen von Listen zur Schwellwertanalyse
- Alternative Berechnungen zur Risikoanalyse
- Einbindung vorgeschlagener Auswahlmöglichkeiten in der Risikoanalyse von Risikoquellen, Bedrohungen, potentielle Risiken und TOM
- Übersetzung und Einbindung der PIA Knowledge Bases
- Ergänzung weiterer Schritte der DSFA, wie Prüfplanung oder regelmäßige Überprüfung und Überwachung
- Zielgruppengerechte Anpassungen und Verknüpfungen der DSFA im ODC
- Erweiterung der Einzelrisikobewertung um unternehmensinterne interessierte Personen und Ausgliederung einzelner Teilschritte für einzelne Interessengruppen
- Juristische Ausarbeitung von Fällen zur Standardisierung
- Wissenschaftliche Prüfung von Möglichkeiten und Ansatzpunkten von Automatisierung der DSFA im ODC

Diese Liste erhebt keinen Anspruch auf Vollständigkeit, je nach Interessen und Fachgebiet können verschiedenste Aspekte relevant sein für die Betrachtung und Ausarbeitung. Es bieten sich juristische wie auch technische Blickwinkel an für das Thema der DSFA, sowie die Verknüpfung beider Fachdisziplinen.

5. Evaluation

In diesem Kapitel werden zusammenfassend die Anforderungen und deren Erfüllung innerhalb des erstellten Konzeptes für die Datenschutz-Folgenabschätzung (DSFA) mit dem Fokus auf Schwellwertanalyse, technische und organisatorische Maßnahmen (TOM) und Risikoanaylse evaluiert; sowie die Umsetzbarkeit in der Software-Entwicklung und Nutzbarkeit für Anwendende gegenüberstellend verglichen und beurteilt. Zudem wird beschrieben welchen Mehrwert es aus Sicht von Datenschutzbeauftragten als Nutzende der Software bietet. Zur Evaluation wurden erneut die Entwickler des Open Datenschutzcenter (ODC) sowie der Datenschutzbeauftragte der Universität der Bundeswehr München befragt. Hier werden die in Kapitel 4 identifizierten Anforderungen wieder aufgegriffen und beurteilt:

- Benutzbarkeit
- Compliance
- Dokumentation
- Erweiterbarkeit

Die Entwickler der ODC werden den Einbau des Workflow in ihre Anwendung prüfen. Sie haben sowohl aus technischer Sicht, als auch aus Anwendersicht das Konzept geprüft und evaluiert. Aus technischer Sicht ist der vorgeschlagene Workflow eine sehr gute und sinnvolle Erweiterung der Software. Durch die Kombination der Risikoanalyse mit den TOM lässt sich erkennen wie sie die Risiken reduzieren. Die Auswahlmöglichkeiten sind durch Dropdowns und Schieberegler für Anwendende leicht verständlich. Die Umsetzung der graphischen Darstellung wird aus technischer Sicht aufwändiger, da hier ein Canvas zur Anwendung kommen wird und dieses sich anhand der Eingaben neu generieren muss. Eine zu erstellende tabellarische Übersicht der DSFA sei ähnlich zu User Interface und User Experience der anderen Datentypen. Der Workflow für den DSFA-Ablauf sei gut in einer Statemachine (Zustandsautomat) abbildbar und somit gut implementierbar. Als Vorschlag zur Ergänzung könnte die Option einer automatischen Übermittlung von Meldungen an die zuständige Aufsichtsbehörde den gesamten Workflow digitalisieren. Aus Anwendersicht erachten die Entwickler den Schritt

der Analyse der Notwendigkeit der DSFA sinnvoll für Datenschutzbeauftragte, dadurch wird die Entscheidung unterstützt. Vor allem bei kritischen Verarbeitungen, die möglicherweise auf der Muss-Liste stehen, wäre dies ein guter Schritt mehr Datenschutz in Unternehmen einzubauen. Da alles im ODC versioniert wird, würden die Entscheidungen ob eine DSFA durchgeführt wird oder nicht, besser dokumentiert und später klar verständlich warum für eine bestimmte Verarbeitung eine oder keine DSFA erstellt wurde. Dies wäre auch über mehrere Versionen hinweg von externen und internen Auditoren nachvollziehbar und vor allem für externe Datenschutzbeauftragte wichtig, da diese in ihrer Dienstleistung noch genauer auf die Dokumentationsführung achten müssen.

Der Datenschutzbeauftragte der Universität der Bundeswehr München hat das Konzept aus Sicht von Softwarenutzenden beurteilt. Insgesamt betrachtet er die Problematik, dass das Thema DSFA in Literatur und Software nur rudimentär behandelt werden, als gut herausgearbeitet und ist der Ansicht, dass nach der Aufbereitung des Themas in dieser Ausarbeitung das Konzept in eine gut bedienbare Software eingebaut werden kann. Die zuvor identifizierten Anforderungen werden rundum gut abgedeckt. Die Benutzbarkeit ist so gut wie möglich gegeben, eingebundene Erklärungen und eine ansprechende Gestaltung der Schaltflächen mit anschließender visueller Darstellung sind zielführend für die Benutzbarkeit. Zur Compliance erachtet er diese Abschlussarbeit besser ausgearbeitet als alle vergleichbaren Arbeiten zu diesem Thema. Es ist zu beachten, dass Compliance immer aus unterschiedlichen Richtungen betrachtet werden kann, dies ist abhängig von den Anforderungen der jeweils zuständigen Aufsichtsbehörde. Wichtig ist, dass wie in dieser Ausarbeitung dargestellt, der Prozess und die Dokumentation immer von Menschen gesehen und verstanden werden muss, u.a. da oft mehrere verschiedene Rechtsgebiete zu betrachten sind. Beispielsweise können im Fall von Nutzdatenspeicherung in einer Behörde die Bereiche IT-Sicherheit, Beamtenrecht und Datenschutz gleichzeitig betroffen sein. Daher muss eine Software Querverlinkungen, Verweise und Zusammenfassungen aufzeigen, hier ist dies bereits durch das erstellte Konzept möglich durch Einbindung der Info-Buttons für Verweise. Die Darstellung des Prozesses innerhalb der Software zur Dokumentation ist bereits in der aktuellen Version des ODC möglich durch die Generierung einer PDF-Datei, nun wird dies ergänzt durch die graphische Darstellung der Analysen. Zukünftig könnte man dies erweitern durch zielgruppengerechte Anpassungen, da eine Datenschutzbehörde andere Interessen verfolgt als z.B. ein Projektleiter. So könnte als Ausblick hier die Erweiterung der Einzelrisikobewertung um unternehmensinterne interessierte Personen und Ausgliederung einzelner Teilschritte für einzelne Interessengruppen zur ergänzenden Verbesserung der technischen Bearbeitung des Verfahrens führen. Somit ist ein solidier Grundstein für eine bedienbare Anwendung mit Potential für Erweiterungen gelegt worden.

6. Zusammenfassung und Ausblick

Abschließend betrachtet konnten die in Kapitel 1.1 genannten Ziele vollständig ausgearbeitet werden. Rechtliche Grundlagen und Begriffe wurden herausgearbeitet, sowie der technische Rahmen des Open Datenschutzcenter (ODC) beschrieben. Ähnliche Arbeiten wurden vorgestellt und verglichen. Anhand der Erkenntnisse aus Grundlagen und verwandten Arbeiten wurde ein Konzept für die Datenschutz-Folgenabschätzung (DSFA) im ODC mit Fokus auf Schwellwertanalyse und Risikobeurteilung entwickelt sowie das Design vorgestellt.

Es konnte gezeigt werden, dass eine Standardisierung in begrenztem Maße möglich ist, beispielsweise bei ähnlich gelagerten Fällen. Eine komplett automatisierte Verarbeitung ist kaum denkbar, sowohl von der Durchführbarkeit schwierig, also auch rechtlich bedenklich. Die Entscheidungen im Prozess der DSFA sind immer individuell zu betrachten. Es muss immer ein Mensch hinter den wesentlichen Entscheidungen stehen, um diese der Aufsichtsbehörde gegenüber begründen zu können und selbst der Verantwortung nachzukommen, indem überlegt und verstanden wird welche Risiken vorliegen und wie diese angemessen reduziert, überprüft und kontrolliert werden können.

Durch den Umfang der Thematik und die Vielzahl an möglichen Anwendungsfällen sind weitere Forschungsansätze, die an diese Ausarbeitung anknüpfen, denkbar. Beispielsweise kann die Umsetzung und Implementierung des Konzepts in das ODC betrachtet werden, oder es können weitere Teilaspekte der DSFA analysiert werden, wie zielgruppengerechte Anpassungen in der Dokumentation. Insbesondere die Verknüpfung von juristischen und technischen Anforderungen zu einer benutzbaren Anwendung stellt eine große Herausforderung dar, welche hohes Potential aufweist für weitere wissenschaftliche Ausarbeitungen. Anwendungen müssen immer auf dem aktuellsten Stand der Gesetzesgrundlagen sein und auf Grund des jungen Alters der Datenschutz-Grundverordnung (DSGVO) und Dynamik von Rechtssprechung und technischem Fortschritt, werden sich in Zukunft weitere Risiken, Forschungslücken und Ansätze für Anwendungen ergeben.

A. Anhang 1

A.1. Auzug aus der DSGVO

Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) 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 („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) 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; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) 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 („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Art. 35 Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.

(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.

(6) Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

(7) Die Folgenabschätzung enthält zumindest Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

(8) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

(9) Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

(10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

(11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

Art. 36 Vorherige Konsultation (1) Der Verantwortliche konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung gemäß Artikel 35 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur

Eindämmung des Risikos trifft.

(2) Falls die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung gemäß Absatz 1 nicht im Einklang mit dieser Verordnung stünde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, unterbreitet sie dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu acht Wochen nach Erhalt des Ersuchens um Konsultation entsprechende schriftliche Empfehlungen und kann ihre in Artikel 58 genannten Befugnisse ausüben. Diese Frist kann unter Berücksichtigung der Komplexität der geplanten Verarbeitung um sechs Wochen verlängert werden. Die Aufsichtsbehörde unterrichtet den Verantwortlichen oder gegebenenfalls den Auftragsverarbeiter über eine solche Fristverlängerung innerhalb eines Monats nach Eingang des Antrags auf Konsultation zusammen mit den Gründen für die Verzögerung. Diese Fristen können ausgesetzt werden, bis die Aufsichtsbehörde die für die Zwecke der Konsultation angeforderten Informationen erhalten hat.

(3) Der Verantwortliche stellt der Aufsichtsbehörde bei einer Konsultation gemäß Absatz 1 folgende Informationen zur Verfügung:

a) gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen;

b) die Zwecke und die Mittel der beabsichtigten Verarbeitung;

c) die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß dieser Verordnung vorgesehenen Maßnahmen und Garantien;

d) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

e) die Datenschutz-Folgenabschätzung gemäß Artikel 35 und

f) alle sonstigen von der Aufsichtsbehörde angeforderten Informationen.

(4) Die Mitgliedstaaten konsultieren die Aufsichtsbehörde bei der Ausarbeitung eines Vorschlags für von einem nationalen Parlament zu erlassende Gesetzgebungsmaßnahmen oder von auf solchen Gesetzgebungsmaßnahmen basierenden Regelungsmaßnahmen, die die Verarbeitung betreffen.

(5) Ungeachtet des Absatzes 1 können Verantwortliche durch das Recht der Mitgliedstaaten verpflichtet werden, bei der Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe, einschließlich der Verarbeitung zu Zwecken der sozialen Sicherheit und der öffentlichen Gesundheit, die Aufsichtsbehörde zu konsultieren und deren vorherige Genehmigung einzuholen.

B. Abkürzungsverzeichnis

BDSG Bundesdatenschutzgesetz

BMVg Bundesministerium der Verteidigung

CNIL Commission Nationale de l'Informatique et des Libertés (französische Datenschutzbehörde)

DSFA Datenschutz-Folgenabschätzung

DSGVO Datenschutz-Grundverordnung

DSM Datenschutzmanagement

DSMS Datenschutz-Managementsystem

EU Europäische Union

ODC Open Datenschutzcenter

PDCA Plan, Do, Check, Act

SDM Standard-Datenschutzmodell

TOM technische und organisatorische Maßnahmen

Literaturverzeichnis

[2B] 2B Advice GmbH. *2B Advice PrIME: Datenschutz-Software*. URL: https://www.2b-advice.com/de/datenschutz-software/ (besucht am 23. 06. 2023).

[Bay22] BayLfD. *Risikoanalyse und Datenschutz-Folgenabschätzung: Systematik, Anforderungen, Beispiele*. Mai 2022. URL: https://www.datenschutz-bayern.de/dsfa/OH_Risiko.pdf (besucht am 06. 11. 2023).

[BD17] Wolf-Tassilo Böhm und Oliver Draf. *Handbuch EU-Datenschutz-Grundverordnung*. 1. Auflage. Schriftenreihe Kommunikation & Recht. Frankfurt am Main: Fachmedien Recht und Wirtschaft dfv Mediengruppe, 2017. ISBN: 9783800516230.

[BMV23a] BMVg. *BMVg Checkliste zur Datenschutzfolgenabschätzung nach Art. 35 DSGVO - 08.03.2023*. März 2023.

[BMV23b] BMVg. *BMVg Merkblatt zur Datenschutzfolgenabschätzung nach Art. 35 DSGVO - 08.03.2023*. März 2023.

[Car] Caralegal GmbH. *Caralegal*. URL: https://caralegal.eu/ (besucht am 23. 06. 2023).

[CNI15] CNIL. *Privacy Impact Assessment (PIA), Methodology (how to carry out a PIA)*. Juni 2015. URL: https://www.cnil.fr/en/privacy-impact-assessments-cnil-publishes-its-pia-manual (besucht am 10. 06. 2023).

[CNI18a] CNIL. *Privacy Impact Assessment (PIA), knowledge bases*. Feb. 2018. URL: https://www.cnil.fr/en/privacy-impact-assessments-cnil-publishes-its-pia-manual (besucht am 10. 06. 2023).

[CNI18b] CNIL. *Privacy Impact Assessment (PIA), templates*. Feb. 2018. URL: https://www.cnil.fr/en/privacy-impact-assessments-cnil-publishes-its-pia-manual (besucht am 10. 06. 2023).

[CNI21] CNIL. *PIA*. 30. Juni 2021. URL: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment (besucht am 10. 06. 2023).

[Data] Datenschutzeinfach.com. *TSMONDO IT-Security & Compliance*. URL: https://datenschutzeinfach.com/ (besucht am 23. 06. 2023).

[Datb] Datenschutzkonferenz. *Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist*. Hrsg. von Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. URL: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Liste_VerarbeitungsvorgaengeDSK.pdf?__blob=publicationFile&v=7 (besucht am 25. 06. 2023).

[Dat18] Datenschutzkonferenz. *Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen*. 26. Apr. 2018. URL: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf (besucht am 30. 05. 2023).

[Der18] Der Bayerische Landesbeauftragte für den Datenschutz. *Ausfüllbeispiel: Formulare zur Datenschutz-Folgenabschätzung - Modul 3: Tabellen für das Risikomanagement zu einer Verarbeitungstätigkeit*. 2018. URL: https://www.datenschutz-bayern.de/dsfa/3-4-1_VVT-Personalverwaltung-DSFA-Risikoanalyse-Bsp.xlsx (besucht am 19. 06. 2023).

[DPM] DPMS - Data Protection Management Software. *DPMS*. URL: https://www.datenschutz-management.software/ (besucht am 23. 06. 2023).

[Fri+17] Michael Friedewald u. a. *DATENSCHUTZ-FOLGENABSCHÄTZUNG: Ein Werkzeug für einen besseren Datenschutz: White Paper*. Hrsg. von Michael Friedewald u. a. Nov. 2017. URL: https://www.forum-privatheit.de/publikationen/white-paper-policy-paper/ (besucht am 01. 05. 2023).

[Hel22] Marcus Helfrich. *Datenschutzrecht: Datenschutz-Grundverordnung, JI-Richtlinie, Bundesdatenschutzgesetz, Informationsfreiheitsgesetz, Grundrechtecharta, Grundgesetz (Auszug), Europäische Datenschutzkonvention, Strafprozessordnung (Auszug), Strafgesetzbuch (Auszug), Telemediengesetz, Telekommunikationsgesetz (Auszug), Bundesbeamtengesetz (Auszug), Betriebsverfassungsgesetz (Auszug), Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer*. 14. Auflage, Stand: 15. März 2022. Beck-Texte im dtv. München: dtv, 2022. ISBN: 978-3-423-53136-8.

[HH23] Emanuel Holzmann und Andreas Holzmann. *Open Datenschutzcenter*. 2023. URL: https://open-datenschutzcenter.de/ (besucht am 26. 06. 2023).

[IITa] IITR Datenschutz GmbH. *Compliance-Kit*. URL: https://www.iitr.de/produkte-services/datenschutzmanagementsystem-ck2 (besucht am 23. 06. 2023).

[IITb] IITR Datenschutz GmbH. *Datenschutz-Kit*. URL: https://www.iitr.de/produkte-services/datenschutz-kit (besucht am 23. 06. 2023).

[Klo+20] Dariusz Kloza u. a. *Entwicklung einer Methode für die Datenschutz-Folgenabschätzung: Erläuterung und Auslegung der Anforderungen der DSGVO*. Brüssel, 2020. URL: http://hdl.handle.net/1854/LU-8738551 (besucht am 24. 05. 2023).

[Kno] Knowledge Management Associates GmbH. *Datencockpit*. URL: https://www.datencockpit.at/Datencockpit (besucht am 23. 06. 2023).

[Kon22] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. *Das Standard-Datenschutzmodell: Eine Methode zur Datenschutzberatung und –prüfung auf der Basis einheitlicher Gewährleistungsziele*. Hrsg. von AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. Nov. 2022. URL: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ (besucht am 12. 03. 2023).

[KSG19] Thomas Kranig, Andreas Sachs und Markus Gierschmann. *Datenschutz-Compliance nach der DS-GVO: Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden*. 2. Auflage. Köln: Bundesanzeiger Verlag, 2019. ISBN: 9783846210239.

[LM17] Niels Lepperhoff und Thomas Müthlein, Hrsg. *Leitfaden zur Datenschutz-Grundverordnung: Detailfragen und erste Schritte in der betrieblichen Praxis*. 1. Auflage. Köln: Datakontext, 2017. ISBN: 9783895777936.

[One] One Trust Technology Limited. *Privacy and Data Governance Cloud*. URL: https://www.onetrust.de/loesungen/datenschutzprogramm/ (besucht am 23. 06. 2023).

[Rob22] Robert Koch-Institut. *Bericht zur Datenschutz-Folgenabschätzung für die Corona-Warn-App der Bundesrepublik Deutschland: Öffentliche Version*. 10. Okt. 2022. URL: https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf (besucht am 01. 05. 2023).

[Sch09] Oliver Schonschek. *Tools zur Datenschutz-Folgenabschätzung nach DSGVO: Bessere Priorisierung im Datenschutz*. Hrsg. von Peter Schmitz. 2019-04-09. URL: https://www.security-insider.de/tools-zur-datenschutz-folgenabschaetzung-nach-dsgvo-a-817277/ (besucht am 16. 04. 2023).

[VOR23] VORERST AG. *Risikomanagement nach ISO 31000 - die Norm im Blickpunkt*. 2023. URL: https://www.risikomanagement-wissen.de/risikomanagement/risikomanagement-einfuehrung/iso_31000/ (besucht am 19. 06. 2023).

[xme] xmera Solutions GmbH. *xmera Omnia*. URL: https://xmera.de/ (besucht am 23. 06. 2023).

Versicherung an Eides Statt

Hiermit versichere ich, die vorliegende Arbeit selbständig und ohne fremde Hilfe verfasst, die Zitate ordnungsgemäß gekennzeichnet und keine anderen, als die im Literatur/Schriftenverzeichnis angegebenen Quellen und Hilfsmittel benutzt zu haben.
Ferner habe ich vom Merkblatt über die Verwendung von studentischen Abschlussarbeiten Kenntnis genommen und räume das einfache Nutzungsrecht an meiner Bachelorarbeit der Universität der Bundeswehr München ein/nicht ein.[1]

Neubiberg, den 27. Juni 2023 _____
Ort, Datum

[1] Nichtzutreffendes bitte streichen.

Abgabevermerk Prüfungsamt