Der Bayerische Landesbeauftragte
für den Datenschutz

Diese Arbeitshilfe wurde vollständig ersetzt durch die Orientierungshilfe
"Risikoanalyse und Datenschutz-Folgenabschätzung - Systematik, Anforderungen, Beispiele"

Datenschutz-Folgenabschätzung

Methodik und Fallstudie

Herausgeber:

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18
Telefon: +49 89 21 26 72-0
E-Mail: poststelle@datenschutz-bayern.de
https://www.datenschutz-bayern.de

Bearbeiter:

Dr. Christoph Wambsganz
unter Mitwirkung von Oliver Brunner,
Corina Scheiter und Dr. Matthias Stief

Redaktion:

Dr. Kai Engelbrecht

Version 2.0 | Stand: 1. Oktober 2019

Dieses Arbeitspapier wird ausschließlich in elektronischer Form bereitgestellt. Es kann im Internet auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutz-Folgenabschätzung“ abgerufen werden.

Die PDF-Datei ist für den doppelseitigen Ausdruck optimiert.

Vorwort

Bereits vor der Datenschutzreform 2018 waren die bayerischen öffentlichen Stellen verpflichtet, technische und organisatorische Maßnahmen zu treffen, um Risiken bei der Verarbeitung personenbezogener Daten entgegenzuwirken (vgl. Art. 7 Bayerisches Datenschutzgesetz in der bis zum 24. Mai 2018 geltenden Fassung). Die Datenschutz-Grundverordnung führt diesen Regelungsansatz fort. Sie sieht vor, Risiken strukturiert zu ermitteln und ihnen ebenso strukturiert zu begegnen (vgl. Art. 32 Datenschutz-Grundverordnung – DSGVO). Bei Verarbeitungsvorgängen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten natürlicher Personen ist die Datenschutz-Folgenabschätzung (Art. 35 DSGVO) das dafür vorgeschriebene Instrument.

Das neue Recht fordert dabei nichts grundlegend Neues, leitet aber zu einem methodisch konsequenten Vorgehen an. Indem der Verantwortliche seine Datenschutz-Folgenabschätzung dokumentiert (vgl. Art. 35 Abs. 1 DSGVO), vergewissert er sich zum einen, dass die präventiv nötigen Maßnahmen getroffen sind. Zum anderen kann er dies so auch gegenüber der Datenschutz-Aufsichtsbehörde darlegen.

Ich habe bereits vor der Datenschutzreform 2018 eine Orientierungshilfe „Datenschutz-Folgenabschätzung“ publiziert und eine Software bereitgestellt, welche die Durchführung von Datenschutz-Folgenabschätzungen unterstützen soll. Die Veröffentlichung der „Bayerischen Blacklist“ war nun Anlass, die Orientierungshilfe zu überarbeiten und um das vorliegende Arbeitspapier „Datenschutz-Folgenabschätzung – Methodik und Fallstudie“ zu ergänzen. Das Arbeitspapier soll die Hinweise aus der Orientierungshilfe für den Praxisgebrauch ausdifferenzieren und anhand eines konkreten Fallbeispiels veranschaulichen.

Nach einer Einführung (I.) werden die einzusetzenden Methoden näher vorgestellt. Nach der Risikoanalyse als einem zentralen Baustein der Datenschutz-Folgenabschätzung (II. 1.) geht das Arbeitspapier auf die zu treffenden Schutzmaßnahmen (II. 2.) und den Bericht über die Datenschutz-Folgenabschätzung ein (II. 3.). Diesen Erläuterungen schließt sich eine Fallstudie an (III.). Zur Fallstudie gehören auch die Ausfüllbeispiele zu den für die Datenschutz-Folgenabschätzung bereitgestellten Formularen (IV. 2.).

Ich hoffe, dass das vorliegende Arbeitspapier einen weiteren Beitrag leisten kann, die mancherorts gegen die Durchführung von Datenschutz-Folgenabschätzungen noch bestehenden Vorbehalte abzubauen, und weiterhin, die bayerischen öffentlichen Stellen zu befähigen, dieses nützliche Instrument eines effizienten Risikomanagements auch in der Praxis einzusetzen – so, wie das unionsrechtlich verankerte Datenschutzrecht dies gebietet.

Verbesserungsvorschläge sind willkommen und erreichen mich unter der E-Mail Adresse orientierungshilfen@datenschutz-bayern.de.

Inhaltsverzeichnis

I. Einführung

Mit Hilfe der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO sind Verarbeitungsvorgänge, die voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen mit sich bringen, grundsätzlich vor ihrem Beginn auf ihr mögliches Schadenspotenzial zu prüfen und zu bewerten. Ziel der Datenschutz-Folgenabschätzung ist es, auf Basis der gewonnenen Erkenntnisse geeignete technische und organisatorische Maßnahmen nachhaltig umzusetzen, um die ermittelten Risiken auf ein vertretbares Maß zu reduzieren. Eine Datenschutz-Folgenabschätzung weist letztendlich nach, dass eine öffentliche Stelle als Verantwortlicher die Datenschutz-Grundverordnung hinsichtlich der jeweiligen Verarbeitung einhält. Auch wenn eine Datenschutz-Folgenabschätzung nicht erforderlich sein sollte, muss der betrachtete Verarbeitungsvorgang trotzdem die Datenschutz-Grundverordnung einhalten. Somit kann die Datenschutz-Folgenabschätzung auch als allgemeine Methode verstanden werden, mit deren Hilfe der Einklang eines Verarbeitungsvorgangs mit der Datenschutz-Grundverordnung dokumentiert werden kann.

Generelle Ausführungen zur Datenschutz-Folgenabschätzung, wie etwa die Erforderlichkeit einschließlich eines Prüfschemas, sind ausführlich in meiner Orientierungshilfe „Datenschutz-Folgenabschätzung“ dargelegt.[1]

Zu der Frage, wie ein Bericht zu einer Datenschutz-Folgenabschätzung (DSFA-Bericht), die eine öffentliche Stelle durchgeführt hat, grundsätzlich aussehen kann, sind aktuell kaum veröffentlichte Beispiele verfügbar. Daher wird mit diesem Dokument anhand der Stadt Fiktivia als eine frei erfundene öffentliche Stelle mit einem fiktiven Szenario beispielhaft gezeigt, wie ein DSFA-Bericht erstellt werden kann (siehe III.).

Die für dieses Beispiel hergeleitete und verwendete DSFA-Methode wird unter II. ausführlich dargestellt. Obwohl bei der Darstellung der Fokus auf das Wesentliche, die gesetzlichen Mindestanforderungen und auf eine möglichst hohe Verständlichkeit gelegt wird, kann eine gewisse Komplexität, die der Thematik innewohnt, nicht vermieden werden. Nach dem ersten Schritt der Sichtung bereits bestehender Methoden folgte die Erkenntnis, dass die Kombination verschiedener, schon bestehender DSFA-Ansätze zielführend erscheint.

Die DSFA-Methodik „Privacy Impact Assessment“ (→*PIA*) der französischen Datenschutz-Aufsichtsbehörde CNIL wird als methodische Grundlage verwendet (vgl. II. 3. b]) und punktuell in nicht widersprüchlichen Bereichen mit Komponenten des Standard-Datenschutzmodells (→*SDM*)[2] der Konferenz der unabhängigen Datenschutzbehörden des Bundes und

[1] Die Orientierungshilfe ist auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Datenschutz-Folgenabschätzung“ abrufbar.

[2] Das Standard-Datenschutzmodell beschreibt eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele und befindet sich in der hier verwendeten Version V.1.1 vom April 2018 noch in der Erprobungsphase; weiterführende Informationen zu diesem Modell sind zu finden unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell.

der Länder (Datenschutzkonferenz, vgl. II. 1.) sowie mit dem Risikomanagement der Datenschutzkonferenz kombiniert (vgl. II. 1. a]).[3] Der aufgezeigte Lösungsweg sollte aber auch für Befürworter einer „reinen Methodenanwendung" – ggf. mit kleinen Anpassungen – gangbar sein.

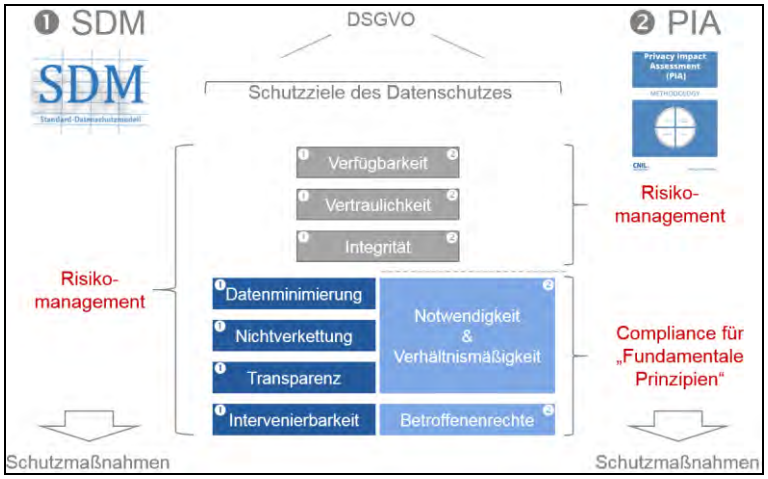

Abb. 1: Übersicht der verwendeten DSFA-Methoden

Auch wenn SDM und PIA insbesondere die Schutzziele des Datenschutzes teilweise etwas anders gruppieren und PIA die Methode des klassischen Risikomanagements für die sogenannten „Fundamentalen Prinzipien" als eine Teilmenge der Schutzziele ausdrücklich ausschließt,[4] ist die eigentliche Zielrichtung und das angestrebte Ergebnis beider Methoden identisch: **Die betrachtete Datenverarbeitung hält mit Hilfe von identifizierten und wirksam umgesetzten Datenschutz-Schutzmaßnahmen nachweislich die Datenschutz-Grundverordnung ein.**

Die im Folgenden aufgezeigte Datenschutz-Folgenabschätzung kann in fast beliebigem Maße weiter ausgebaut und detailliert werden.

Fachbegriffe und Abkürzungen werden im Glossar näher erläutert. Im Glossar befindliche Fachbegriffe sind in der Regel im Text bei ihrer ersten Nennung mit einem Pfeil und kursivem Schriftformat markiert (z. B. →*Fachbegriff*).

Aus Gründen der Lesbarkeit wird im Folgenden auf das Gendern von Personengruppen verzichtet. Die Verwendung des generischen Maskulinums schließt ausdrücklich alle Geschlechterformen mit ein.

[3] Vgl. Datenschutzkonferenz, Risiko für die Rechte und Freiheiten natürlicher Personen (Kurzpapier Nr. 18), im Internet abrufbar unter https://www.datenschutzkonferenz-online.de/kurzpapiere.html.

[4] Siehe Commission Nationale de l'Informatique et des Libertés, Privacy Impact Assessment (PIA) – Methodology, Stand Februar 2018, S. 3, im Internet abrufbar unter www.cnil.fr/en/cnil-publishes-update-its-pia-guides.

II. Herleitung der DSFA-Methode und der Rahmenbedingungen

Wie in der schon genannten „Orientierungshilfe Datenschutz-Folgenabschätzung“ erläutert, kann ein Verantwortlicher die Methode seiner Datenschutz-Folgenabschätzung frei wählen, solange sichergestellt ist, dass alle gesetzlichen Mindestanforderungen an die Datenschutz-Folgenabschätzung erfüllt werden.

1. Nachweis der Normbefolgung und Methode für die Risikoanalyse

Die Grundsätze des Art. 5 DSGVO sowie weitere, teilweise die Grundsätze konkretisierende Anforderungen der Datenschutz-Grundverordnung können in Datenschutz-Schutzziele überführt werden. Dies macht etwa das Standard-Datenschutzmodell (→*SDM*), indem es datenschutzrechtliche Anforderungen in einen Katalog von sieben →*SDM-Gewährleistungsziele* abbildet. Aus den Ausführungen im SDM geht hervor, dass der Kanon der SDM-Gewährleistungsziele vollständig alle Anforderungen der Datenschutz-Grundverordnung abdeckt. Damit ist der Erfüllungsgrad der sieben Gewährleistungsziele hinsichtlich eines konkreten Verarbeitungsvorgangs eine schon anerkannte Messmethode für den Nachweis der Einhaltung der Datenschutz-Grundverordnung.

Abb. 2: Die sieben SDM-Gewährleistungsziele

Die sieben SDM-Gewährleistungsziele besitzen in aller Kürze und auf das Wesentliche reduziert folgenden inhaltlichen Umfang:

Datenminimierung „Nur benötigte Daten verarbeiten!“

Verfügbarkeit „Daten müssen relevante Geschäftsprozesse ermöglichen!“

Vertraulichkeit „Daten nur für befugte Personen (Kenntnis und Veränderung)!“

Integrität	„Daten unversehrt, aktuell, richtig und nach Konzeption verarbeiten!“
Nichtverkettung	„Keine rechtswidrige Zweckentfremdung bei der Datenverarbeitung!“
Transparenz	„Verarbeitung ist erkennbar, nachvollziehbar und prüfbar!“
Intervenierbarkeit	„Betroffenen können die ihnen zustehenden Datenschutzrechte wirksam ausüben!“

Das SDM-Gewährleistungsziel **„Integrität“** spielt eine Sonderrolle, da es nach dem SDM folgende Teilaspekte besitzt:[5]

Datenintegrität	Anforderung, dass Korrektheit/Unversehrtheit von Informationen/Daten und die korrekte Funktionsweise von Systemen sichergestellt ist.[6]
Konzeptionseinhaltung	Anforderung, dass Prozesse und Systeme die für sie gültigen Vorgaben kontinuierlich einhalten (Gleichklang von Betrieb als Ist und der Konzeption als Soll).
Richtigkeit	Anforderung, dass zwischen der rechtlich normativen Anforderung und dem Betrieb eine hinreichende Deckung besteht.

Die →*Risikoanalyse* weist die Erfüllung der SDM-Gewährleistungsziele nach und ist somit Basis für die Beantwortung der Frage, ob der betrachtete Verarbeitungsvorgang die Anforderungen der Datenschutz-Grundverordnung einhält. Daher spielt die für die Risikoanalyse eingesetzte Methode eine besonders wichtige Rolle.

Die SDM-Gewährleistungsziele der klassischen Informationssicherheit „Verfügbarkeit“, „Vertraulichkeit“ und den Teilaspekt „Datenintegrität“ des SDM-Gewährleistungsziels „Integrität“ verweist Art. 32 Abs. 1 DSGVO mit „Eintrittswahrscheinlichkeit und Schwere des Risikos“ auf die klassische Risikomanagementmethode. Folglich wird für diese drei Ziele, die im Folgenden als „→*SDM-Datensicherheitsziele*“ bezeichnet werden, das klassische Risikomanagement als Methode für die Risikoanalyse eingesetzt (siehe II. 1. a]).

Für die vier anderen SDM-Gewährleistungsziele „Datenminimierung“, „Intervenierbarkeit“, „Transparenz“ und „Nichtverkettung“ sowie der Teilaspekte „Konzepteinhaltung“ und „Richtigkeit“ des SDM-Gewährleistungsziels „Integrität“ werden im Folgenden als „→*SDM-Schutzbedarfsziele*“ bezeichnet. Diese Ziele können als „fundamentale Rechte und Prinzi-

[5] Vgl. Datenschutzkonferenz, Das Standard Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, V.1.1 – Erprobungsfassung, 2018, S. 14, im Internet abrufbar unter https://www.datenschutzkonferenz-online.de/anwendungshinweise.html.

[6] Vgl. Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, Glossar und Begriffsdefinitionen, im Internet abrufbar unter https://ww.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html.

pien“[7] verstanden werden, die insbesondere unabhängig von der Eintrittswahrscheinlichkeit und der Schwere nicht Bestandteil von Abstufungen sein können.

Vor diesem Hintergrund kommt für die Risikoanalyse der SDM-Schutzbedarfsziele ein spezielles Zielerfüllungsmanagement zur Anwendung (siehe II. 1 b]), woraus sich folgendes Gesamtbild ergibt:[8]

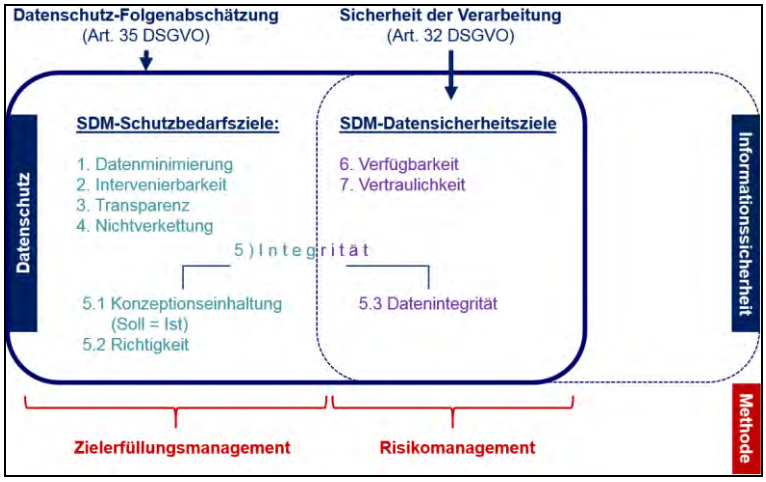

Abb. 3: Die SDM-Schutzbedarfs- und die SDM-Datensicherheitsziele mit Risikoanalysemethoden

Die Aufspaltung in unterschiedliche Risikoanalysen birgt auf der Maßnahmen-Ebene nicht die Gefahr, dass gleiche Datenschutz-Schutzmaßnahmen in beiden Risikobereichen parallel und ggf. unterschiedlich behandelt werden müssten. Denn auch nach dem SDM-Modell erfordern beide Bereiche unterschiedliche Maßnahmen zur Gefährdungseindämmung.[9]

a) Risikoanalyse der SDM-Datensicherheitsziele

Beim klassischen Risikomanagement für den Datenschutz werden die Risiken aus Sicht der betroffenen Personen betrachtet. Dieselbe Methode wird oft auch im Bereich der reinen Informationssicherheit mit dem wichtigen Unterschied eingesetzt, dass dort primär der Schwerpunkt auf die Risiken für die Einrichtung gelegt wird.

Zu jedem relevanten Einzelrisiko werden erfasst:

- die Schwachstelle,
- die Risikoquelle,
- das Risiko-Szenario,
- die Risikoindexierung (Eintrittswahrscheinlichkeit, Schwere/Schaden, Risikoindex) ohne Abhilfemaßnahmen,

7 Siehe Commission Nationale de l'Informatique et des Libertés, Privacy Impact Assessment (Fn. 4).
8 Vgl. Bitkom e. V., Risk Assessment & Datenschutz-Folgenabschätzung – Leitfaden, 2017, S. 8.
9 Vgl. Datenschutzkonferenz, Das Standard Datenschutzmodell (Fn. 5), S. 31.

– die Abhilfemaßnahmen sowie
– der ampelfarbene, mit Freitext begründete Risikoindex bei Wirksamkeit der Abhilfemaßnahmen.

Folglich kann die Risikoanalyse mittels klassischen Risikomanagements wie folgt dargestellt werden:

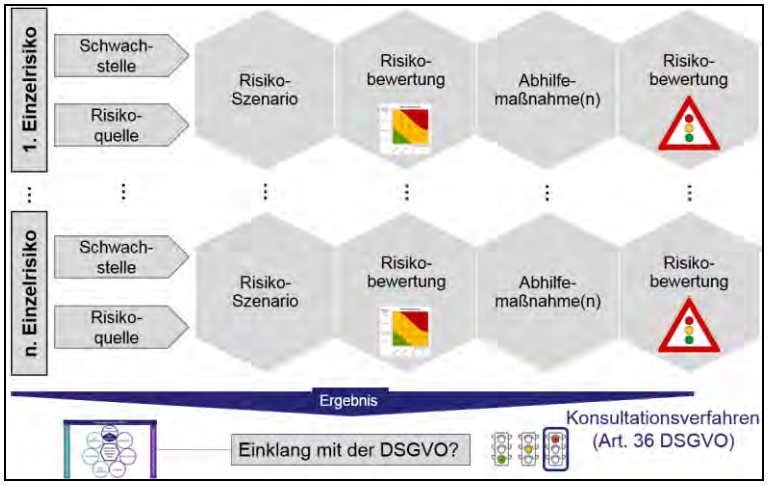

Abb. 4: Risikoanalyse der SDM-Datensicherheitsziele

Aus der Abbildung geht hervor, dass das Risiko-Szenario der eigentliche Gegenstand für die Risikobewertung ist. In jedem Szenario wird möglichst differenziert ein Ereignis beschrieben, durch das der betrachtete Verarbeitungsvorgang den normativen DSGVO-Rahmen verlassen würde und das es daher zu vermeiden gilt.

Für eine einfachere Herleitung aller relevanten Risiko-Szenarien dient die Betrachtung der Schwachstellen und der Risikoquellen. Schwachstellen sind dabei als Eigenschaften des betrachteten Verarbeitungsvorgangs definiert, die geeignet sind, bei hinzutreten einer bestimmten Risikoquelle eine Schadwirkung für die Rechte und Freiheiten natürlicher Personen zu entfalten.

Das Zusammenspiel der drei Aspekte Schwachstelle, Risikoquelle und Risiko-Szenario soll kurz an einem Beispiel des Alltags veranschaulicht werden: Falls die Reifen eines Autos nicht mehr die erforderliche Mindestprofiltiefe haben, so sind die Reifen eine Schwachstelle des Autos. Solange das Auto etwa nur auf einem Schrottplatz steht, stellen die abgefahrenen Reifen kein Risiko dar. Wird das Auto aber gefahren und tritt als Risikoquelle „Regen“ als Risikoquelle zur Schwachstelle hinzu, so stellt der Sachverhalt „Auto fährt mit abgefahrenen Reifen im Regen“ ein Risikoszenario dar, das hinsichtlich Eintrittswahrscheinlichkeit und prognostizierten Schadensausmaß bewertet werden kann.

Bei der hier festgelegten Risikobewertung werden die Eintrittswahrscheinlichkeit und die Schwere/der Schaden wie folgt abgestuft:

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.

Abb. 5: Möglicher Grad der Eintrittswahrscheinlichkeit

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

Abb. 6: Möglicher Grad der Schwere/des Schadens

Aus den festgelegten Einstufungen für die Eintrittswahrscheinlichkeit und der Schwere der Auswirkung ergibt sich im Ergebnis folgende Risikomatrix, die im Wesentlichen der Empfehlung der Datenschutzkonferenz folgt:[10]

[10] Vgl. Datenschutzkonferenz, Risiko für die Rechte und Freiheiten natürlicher Personen (Fn. 3).

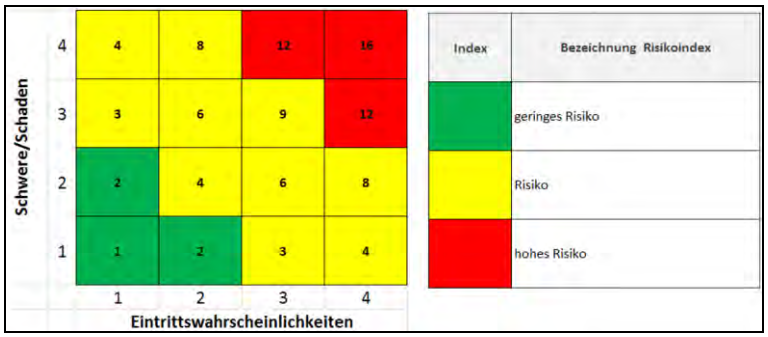

Abb. 7: Risikomatrix

Bei der anschließenden zweiten Risikobewertung (siehe Abb. 4 [Risikoanalyse der SDM-Datensicherheitsziele]) genügt die begründete Angabe des Risikoindexes bei wirksamen Abhilfemaßnahmen, weil die Wirkung der einzelnen Maßnahme auf die Eintrittswahrscheinlichkeit bzw. die Schwere i.d.R. gut erkennbar ist und hier die Beschreibung des Zusammenspiels der festgelegten Abhilfemaßnahmen und deren Wirkung auf den Risikoindex im Mittelpunkt stehen. Natürlich kann auch die zweite Risikobewertung wie die erste Risikobewertung durchgeführt werden.

Eine konkrete Anwendung der Risikoanalyse der SDM-Datensicherheitsziele ist unter Abb. 16 (Auszug aus der Anlage zum SDM-Datensicherheitsziel „Verfügbarkeit“) zu finden.

b) Risikoanalyse der SDM-Schutzbedarfsziele

Bei der Risikoanalyse der SDM-Schutzbedarfsziele steht das Risiko im Vordergrund, dass ein fundamentales DSGVO-Prinzip nicht vollständig eingehalten werden kann. Um Vermischungen mit dem Risikomanagement zu vermeiden, wird im Folgenden von der Gefährdung gesprochen, dass ein Zielerfüllungsgrad von 100% nicht erreicht werden kann. Somit ergibt sich folgendes Bild:

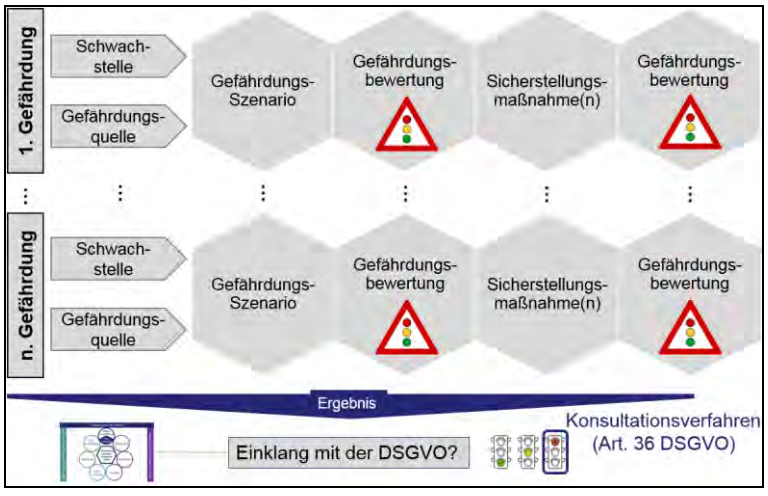

Abb. 8: Risikoanalyse der SDM-Schutzbedarfsziele

Wie in der Risikoanalyse der SDM-Datensicherheitsziele ist das einzelne Gefährdungs-Szenario der eigentliche Gegenstand für die Gefährdungsbewertung. In jedem Szenario wird möglichst differenziert ein Ereignis beschrieben, durch das der betrachtete Verarbeitungsvorgang den normativen DSGVO-Rahmen verlassen würde und das es daher zu vermeiden gilt.

Für eine einfachere Herleitung aller relevanten Gefährdungs-Szenarien dient die Betrachtung der Schwachstellen und der Gefährdungsquellen. Schwachstellen sind dabei als Eigenschaften des betrachteten Verarbeitungsvorgangs definiert, die geeignet sind, bei hinzutreten einer bestimmten Gefährdungsquelle die vollständige Zielerreichung zu verhindern.

Folgende Unterschiede zur Risikoanalyse der SDM-Datensicherheitsziele (vgl. Abb. 4: Risikoanalyse der SDM-Datensicherheitsziele) sind erkennbar:

(1) **Gefährdung:** Anstelle einzelner Risiken werden im Abstrahierungsgrad grundsätzlich frei wählbare Gefährdungen der SDM-Schutzbedarfsziele betrachtet. Naheliegend für das SDM-Gewährleistungsziel „Intervenierbarkeit“ wäre etwa ein Gefährdungsprofil, das sich aus den Gefährdungen im Hinblick auf die einzelnen DSGVO-Betroffenenrechte (Auskunft, Löschung, Berichtigung usw.) zusammensetzt.

(2) **Gefährdungsbewertung:** Die Gefährdungsbewertung, ebenfalls in Ampelfarbe kodiert, kann abgestuft folgende Ergebnisse haben:

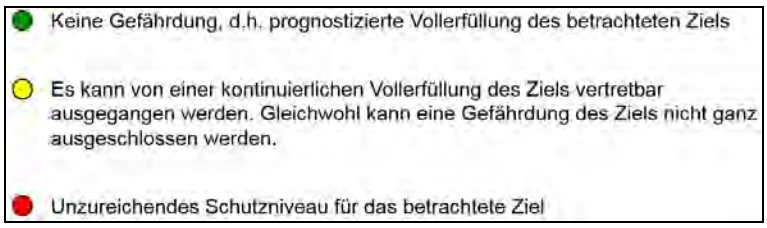

Abb. 9: Mögliche Ergebnisse der Gefährdungsbewertung

(3) **Sicherstellungsmaßnahme:** Anstelle des Begriffs „Abhilfemaßnahme“ wird hier der Begriff „Sicherstellungsmaßnahme“ verwendet. Aus der unterschiedlichen Maßnahmenbezeichnung soll nur hervorgehen, dass im Kontext des Zielerfüllungsmanagements die Maßnahmen dazu dienen, die vollständige Erfüllung des betroffenen Ziels lückenlos sicherzustellen. Da beim klassischen Risikomanagement die Maßnahmen das Einzelrisiko auf ein vertretbares Maß reduzieren bzw. ganz beseitigen, wurden die Maßnahmen dort – wie in der Datenschutz-Grundverordnung – als Abhilfemaßnahmen bezeichnet. Letztendlich dienen beide Maßnahmentypen dem gleichen Ziel, als Datenschutz-Schutzmaßnahmen das Risiko für die Rechte und Freiheiten natürlicher Personen im Compliance-Rahmen der Datenschutz-Grundverordnung zu halten.

Die Aspekte Schwachstelle, Gefährdungsquelle und Gefährdungs-Szenario besitzen die gleiche Grundbedeutung wie unter II. 1. a) dargestellt.

Eine konkrete Anwendung der Risikoanalyse der SDM-Schutzbedarfsziele ist unter Abb. 17 (Auszug aus der Anlage zum SDM-Datenschutzbedarfsziel „Nichtverkettung“) zu finden.

c) Durchführung der Gesamtbewertung

Jedes SDM-Gewährleistungsziel (siehe Abb. 3: Die SDM-Schutzbedarfs- und die SDM-Daten
sicherheitsziele mit Risikoanalysemethoden) besitzt nach Durchführung der Risikoanalysen mehrere bewertete Einzelrisiken (SDM-Datensicherheitsziele) bzw. mehrere bewertete Gefährdungen (SDM-Schutzbedarfsziele). Wie in der folgenden Abbildung dargestellt, werden die einzelnen Bewertungen in der Form auf das jeweilige SDM-Gewährleistungsziel aufsummiert, indem der höchste Risikoindex bzw. die höchste Gefährdungsstufe für das Gesamtergebnis des SDM-Ziels übernommen wird (sog. Maximum-Vorgehen):

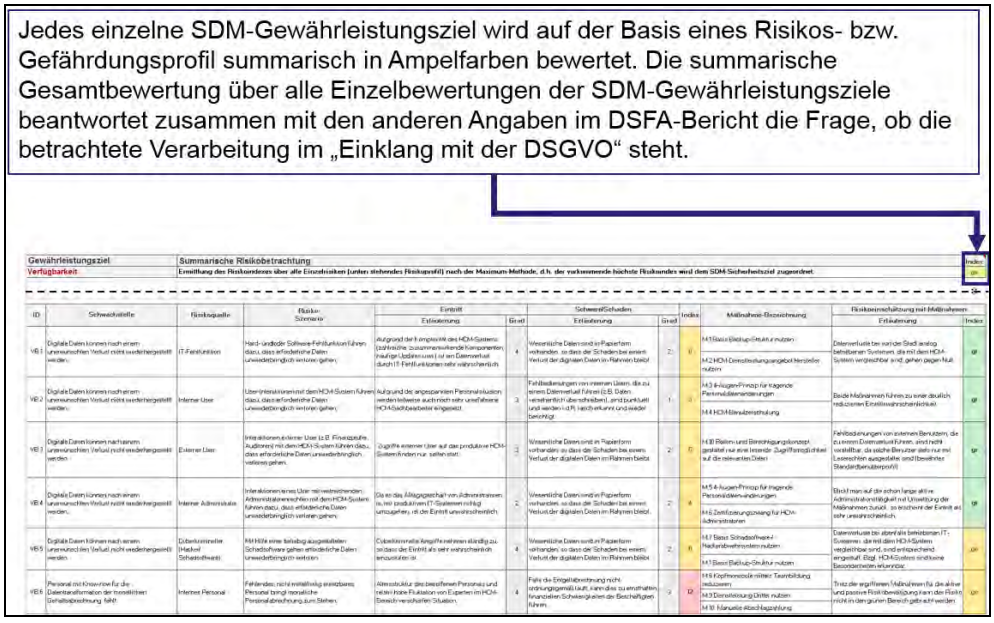

Abb. 10: Ermittlung der Bewertung eines SDM-Gewährleistungsziels

Um einen Zweifel an der gleichen Aussagekraft der Ergebnisse der beiden verwendeten Methoden (Risikomanagement für die SDM-Datensicherheitsziele und Zielerfüllungsmanagement für die SDM-Schutzziele) erst gar nicht aufkommen zu lassen, werden die Bewertungsergebnisse der einzelnen SDM-Gewährleistungsziele nicht mathematisch zu einem Gesamtbewertungswert zusammengeführt. Unverzichtbare Bestandteile der Gesamtbewertung sind folglich alle neun Zielbewertungen (siehe III. 2. d] bb] unter [6]).

2. Datenschutz-Schutzmaßnahmen

Die Datenschutz-Schutzmaßnahmen sind der eigentliche Antrieb des Datenschutzes. Denn eine großartige und überzeugende Datenschutz-Folgenabschätzung auf der Konzeptionsebene (DSFA-Bericht) ist ohne die wirksame Umsetzung der darin festgelegten Maßnahmen ein wahrer Scheinriese.

Für die Wahl geeigneter technischer und organisatorischer Maßnahmen wird von der Datenschutzkonferenz „auf das Standard-Datenschutzmodell, die Leitlinien und Orientie-

rungshilfen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und der Artikel-29-Arbeitsgruppe sowie auf die bestehenden nationalen und internationalen Standards (z. B. BSI-Grundschutz, ISO-Standards) verwiesen".[11]

Obwohl die Auswahl potenzieller Datenschutz-Schutzmaßnahmen für viele, insbesondere auch die Informationssicherheit betreffende Bereiche groß ist, bleibt die besondere Herausforderung, im konkreten Kontext sinnvoll effektive Einzelmaßnahmen zu identifizieren und einen geeigneten Abstrahierungsgrad für das Maßnahmenprofil zu finden.

3. DSFA-Bericht

a) Mindestpositionen des DSFA-Berichts

Die Mindestanforderungen an eine Datenschutz-Folgenabschätzung haben Einfluss auf die Strukturierung des DSFA-Berichts. In jedem Fall ist der nach Art. 35 Abs. 7 DSGVO gesetzlich vorgegebene Mindestinhalt einer Datenschutz-Folgenabschätzung abzubilden. Bei der Datenschutz-Folgenabschätzung besteht zusätzlich die Besonderheit, dass im Fall einer sich an die Datenschutz-Folgenabschätzung anschließenden Konsultation nach Art. 36 DSGVO die Mindestaspekte einer Datenschutz-Folgenabschätzung durch weitere Informationen ergänzt werden müssen. Zwar sollte eine Konsultation ein eher selten vorkommender Fall sein und sind diese Ergänzungen nicht Teil der eigentlichen Datenschutz-Folgenabschätzung, eine weitest mögliche Berücksichtigung dieser zusätzlichen Angaben im Rahmen der DSFA-Erstellung erscheint jedoch empfehlenswert. Dabei wird der Punkt „Sonstige angeforderte Informationen" nicht weiter berücksichtigt, da die davon ggf. betroffenen Inhalte einzelfallbezogen und vorab unbestimmt sind.

Damit ergeben sich folgende Mindestpositionen für einen DSFA-Bericht:

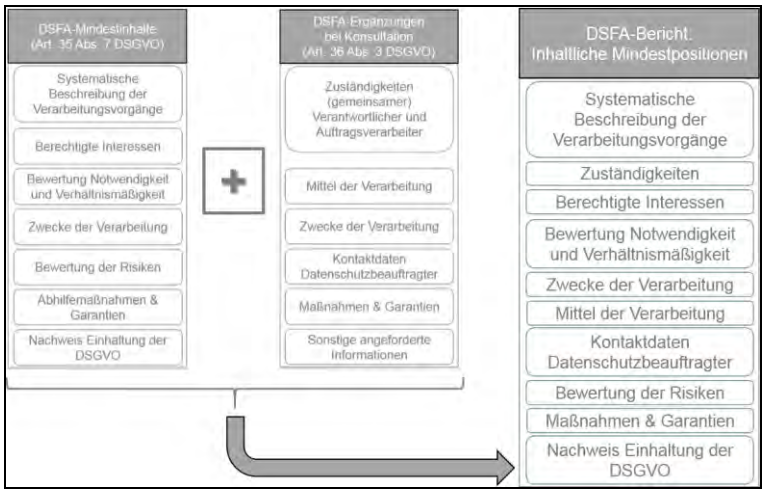

Abb. 11: Mindestpositionen eines DSFA-Berichts

[11] Siehe Datenschutzkonferenz, Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO (Kurzpapier Nr. 1), im Internet abrufbar unter https://www.datenschutzkonferenz-online.de/kurzpapiere.html.

Erwähnenswert zum DSFA-Bericht ist zum einen, dass der Bericht nicht statisch ist, sondern dynamisch bei wesentlichen Änderungen der Verarbeitung oder ihres Kontextes angepasst werden muss. Zudem erfolgen die Schritte der Risikoanalyse und die darauf basierende Maßnahmenauswahl so oft iterativ, bis das gewünschte Risiko-bzw. Gefährdungsniveau erreicht ist.

Zum anderen muss der Brückenschlag zwischen den im Bericht vollständig aufgelisteten, geplanten Datenschutz-Schutzmaßnahmen und deren Umsetzung sowie Wirksamkeitsüberprüfung zuverlässig gelingen.

Insgesamt ergibt sich danach folgendes Bild zum DSFA-Bericht und dem dazugehörigen Maßnahmemanagement:

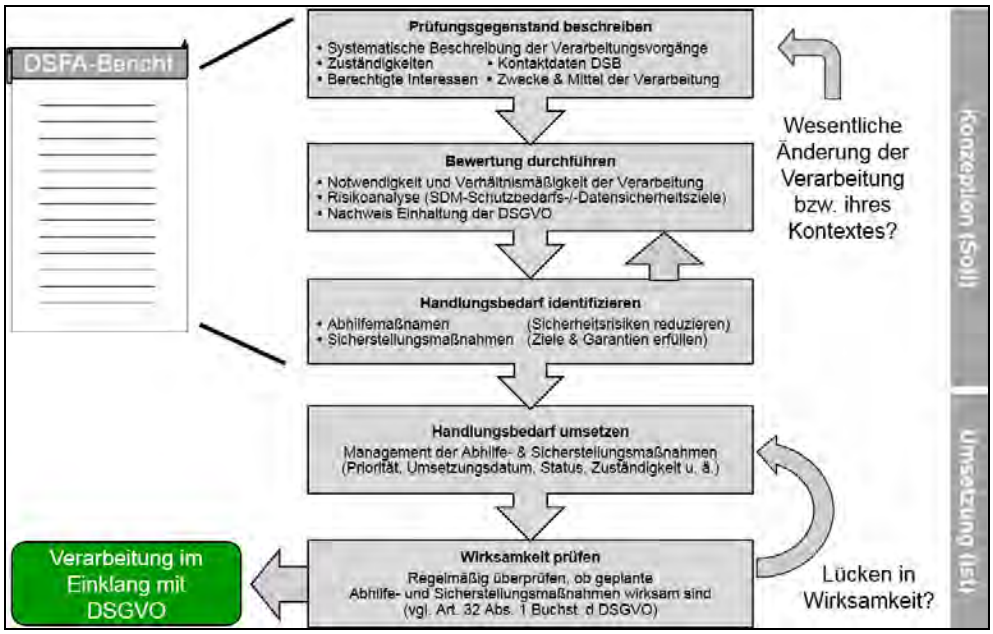

Abb. 12: DSFA-Bericht und sein Kontext

b) PIA-Tool als IT-Unterstützung für den DSFA-Bericht

Die französischen Datenschutz-Aufsichtsbehörde CNIL bietet neben einer umfangreichen Dokumentation zu ihrer DSFA-Methodik „Privacy Impact Assessment" auch das sog. →*PIA-Tool* als Software-Unterstützung an, mit dessen Hilfe u. a. ein kompletter DSFA-Bericht dokumentiert und ausgedruckt werden kann. Mit dem PIA-Tool können die einzelnen Positionen des DSFA-Berichts bei jedem Ausdruck ein- oder ausgeblendet werden.

Neben den dargestellten Eingabe-Positionen existieren weitere Informationsbereiche im PIA-Tool, die zusätzlich eingeblendet werden können. Diese Bereiche betreffen entweder die grafische Darstellung von Fachdaten (z. B. Risikokartierung) oder die sog. Aktionsplan-Funktionen, mit deren Hilfe die eingegebenen Fachdaten durch eine systemintegrierte, dokumentierte Kommunikation zwischen verschiedenen Personen/Stellen finalisiert werden können (z. B. Funktion „Kommentar zu Fachdaten abgeben", „ausdrückliche Freigabe

von Fachdaten“). Diese beiden Zusatzfunktionen kommen in dem Beispiel (III.) aber nicht zur Anwendung.

In das PIA-Tool können einzelne Dateien hochgeladen und als Anlage dem DSFA-Bericht hinzugefügt werden.

Bei Einsatz des PIA-Tools ergibt sich somit folgendes Gesamtbild für die verwendeten IT-Werkzeuge:

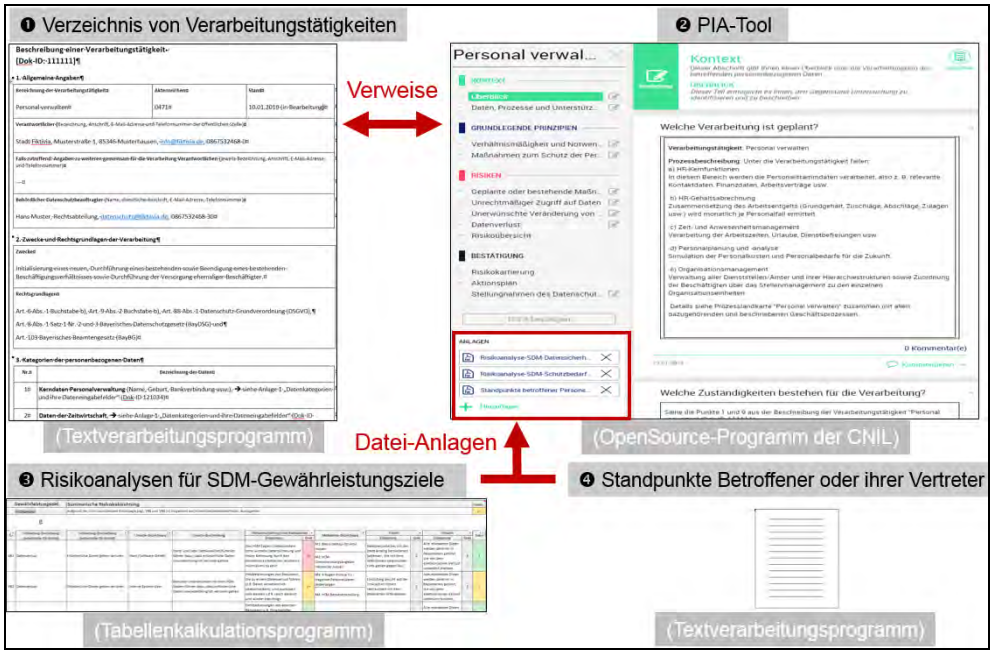

Abb. 13: IT-Bausteine beim Einsatz des PIA-Tools

Eine konkrete, beispielhafte Anwendung des PIA-Tools findet sich unter III. 2.

c) Formular als IT-Unterstützung für den DSFA-Bericht

Abgesehen von seinen gerade genannten Aktionsplan-Funktionen bildet das PIA-Tool im Wesentlichen die Funktion eines elektronischen Formulars mit kontextabhängiger Eingabeunterstützung ab. Stellen, die eine Datenschutz-Folgenabschätzung in einem ersten Schritt nicht mit Hilfe einer spezifischen IT-Anwendung - wie etwa dem PIA-Tool - starten möchten, können alternativ auch ein Formular für den DSFA-Bericht verwenden. Oft kann es hilfreich sein, eine Datenschutz-Folgenabschätzung vollständig mit einfachen, sofort zur Verfügung stehenden rudimentären IT-Werkzeugen durchzuführen. Nach der Erstellung der ersten DSFA-Berichte können die damit gemachten Erfahrungen und das dadurch vertiefte Verständnis auch dazu genutzt werden, gezielt eine passende IT-Unterstützung für das Management der DSFA-Berichte oder für das gesamte Datenschutz-Management zu suchen.

Bei Einsatz eines rudimentären Formulars ergibt sich folgendes Gesamtbild für die verwendeten IT-Werkzeuge:

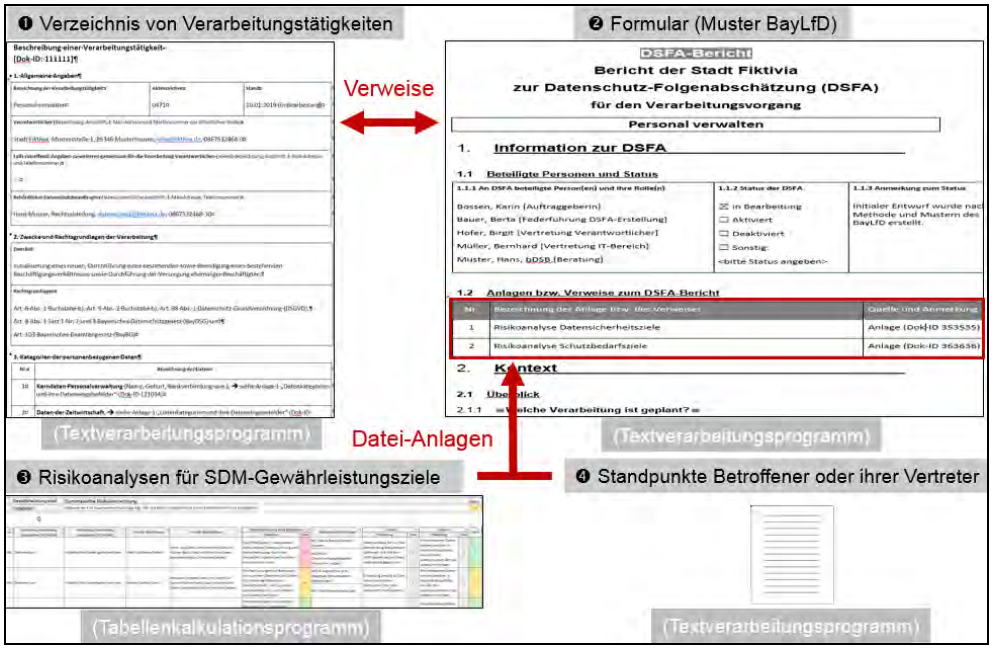

Abb. 14: IT-Bausteine bei der Verwendung eines rudimentären Formulars für den DSFA-Bericht

Für den DSFA-Bericht stehen ein Formular und ein Ausfüllbeispiel für die Verarbeitungstätigkeit „Personal verwalten“ der Stadt Fiktivia bereit (siehe IV. 2., Modul 2).

4. Zusammenspiel Datenschutz-Folgenabschätzung und Verzeichnis von Verarbeitungstätigkeiten

Eine besonders enge Verknüpfung hat die Datenschutz-Folgenabschätzung mit dem „Verzeichnis von Verarbeitungstätigkeiten“. Denn die Beschreibung einer Verarbeitungstätigkeit umfasst Informationen, die auch für die Datenschutz-Folgenabschätzung benötigt werden. Um mögliche Inkonsistenzen zu vermeiden, ist bei der nachträglichen Durchführung einer Datenschutz-Folgenabschätzung, etwa im Fall von „Bestandsverfahren“, eine gegenseitige Verweisung, wie im folgenden Schema gezeigt, gut denkbar.

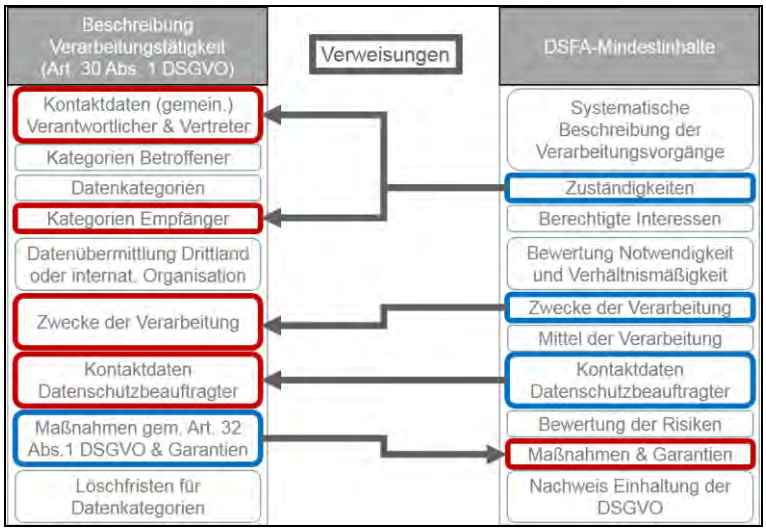

Abb. 15: Verweisungen zwischen der Beschreibung einer Verarbeitungstätigkeit und der DSFA

Grundsätzlich ist die Datenschutz-Folgenabschätzung jedoch vor dem Beginn des betrachteten Verarbeitungsvorgangs zu erstellen, also zu einem Zeitpunkt, zu dem der entsprechende Eintrag im Verzeichnis von Verarbeitungstätigkeiten noch fehlt. In diesem Fall empfiehlt es sich aus Konsistenzgründen ebenfalls, an mehreren Stellen verwendete gleiche Informationen an einer „führenden" Stelle zu pflegen, etwa, indem der (zukünftige) Eintrag in das Verzeichnis von Verarbeitungstätigkeiten bereits im Vorfeld miterstellt wird

.

III. Beispiel für einen DSFA-Bericht

1. Sachverhalt einer Stadt für das Beispiel „Personalverwaltung“

Die frei erfundene Großstadt Fiktivia hat ein Personalamt, das für den städtischen Kernprozess „Personal verwalten“ verantwortlich ist. In der Stadt und somit auch im Personalamt ist Geschäftsprozessmanagement durchgehend umgesetzt, d. h. es gibt u. a. eine Prozesslandkarte „Personal verwalten“, die alle dazugehörenden Geschäftsprozess unter sich vereint. Von dieser Prozesslandkarte umfasst sind die Geschäftsprozesse „Personal einstellen“, „Arbeitszeit und Anwesenheit managen“, „Entgelt abrechnen“, „Beschäftigungsverhältnis beenden“ und „Versorgung managen“. Nicht umfasst sind hingegen insbesondere die Prozesse „Bewerbungen managen“, „Betriebliches Gesundheitsmanagement durchführen“, „Aus- und Fortbildung managen“, „Disziplinarverfahren durchführen“ und „Beihilfe managen“.

Neben den personalwirtschaftlichen Prozessen gibt es auch Prozesse, die dem Geschäftsprozessmanagement selbst oder dem stadtweiten Datenschutzmanagement dienen.

Dem Geschäftsprozessmanagement dient etwa der Geschäftsprozess „Prozess ändern“, der die dauerhafte Übereinstimmung zwischen der konzeptionellen Prozessmodellierung (Soll) und der aktuell gelebten Prozessumsetzung (Ist) gewährleistet.

Dem Datenschutzmanagement dient insbesondere der städtische Geschäftsprozess „Ausübung eines DSGVO-Betroffenheitsrechts managen“. Bei der Stadt koordiniert und stellt eine zentrale Stelle sicher, dass Datenschutz-Anfragen betroffener Personen ggf. zur Beantwortung an die relevanten Dienststellen weitergeleitet und die qualitätsgesicherten Antworten der Dienststellen an die betroffene Person fristgerecht weitergeleitet werden.

Bei der Stadt wird der Kernprozess „Personal verwalten“ schon sehr lange und umfangreich durch das IT-System „HCM-Fiktivia“ (auf dem Markt schon sehr lange angebotenes und weit verbreitetes Standardprodukt) unterstützt, das von der Stadt selbst betrieben wird (sog. →*on-premises Systemlösung*).

Zudem betreibt die Stadt ein Maßnahmen-Managementsystem. Dieses zentrale IT-System unterstützt neben der Umsetzung der Datenschutz-Schutzmaßnahmen auch die nachhaltige und wirksame Umsetzung von Maßnahmen anderer Bereiche (z. B. Maßnahmen aus den Bereichen Betriebliches Gesundheitsmanagement, Informationssicherheit und Antikorruption).

Die Stadt Fiktivia hat als öffentliche Stelle ein Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) erstellt, das auf einer Vorlage des Bayerischen Staatsministeriums des

Innern, für Sport und Integration beruht[12] und auch die Beschreibung der Verarbeitungstätigkeit „Personal verwalten“ mit umfasst.[13]

Die datenschutzrechtliche Aufsichtsbehörde, die für die Stadt Fiktivia zuständig ist, führt in ihrer DSFA-Blacklist nach Art. 35 Abs. 4 DSGVO unter anderem die Fallgruppe „Personalverwaltung“, für die unter bestimmten Voraussetzungen eine Datenschutz-Folgenabschätzung erforderlich ist. Diese Fallgruppe ist definiert als umfangreiche Verarbeitung von Personalaktendaten, die auch vertrauliche oder höchstpersönliche Daten betrifft. Die Verarbeitungstätigkeit[14] „Personal verwalten“ der Stadt Fiktivia unterfällt dieser Fallgruppe, so dass eine Datenschutz-Folgenabschätzung erforderlich ist.

2. Städtischer DSFA-Bericht auf Basis des PIA-Tools

Die vom PIA-Tool vorgegebene Gliederungsstruktur wird von der Stadt für ihren DSFA-Bericht „Personal verwalten“ ausgefüllt und aktuell gehalten. Die einzelnen Abschnitte des Berichts und die Anlagen des DSFA-Berichts werden im Folgenden auszugsweise aufgeführt.

Hinweis zur Darstellung: Die von der Stadt Fiktivia gemachten Eingaben sind die blau schattierten Informationen. An einigen Stellen werden zusätzlich erläuternde Hinweise zu bestimmten Berichtsabschnitten gegeben.

a) Information zur DSFA

Datenschutz-Folgenabschätzung
Personal verwalten

Name des Bearbeiters
Berta Bauer, Bernhard Müller

Name des Prüfers
Peter Schulz

Name des Bestätigers
Birgit Hofer, Leitung Personalamt

[12] Vgl. Bayerischen Staatsministeriums des Innern, für Sport und Integration, Arbeitshilfen zur praktischen Umsetzung der Datenschutz-Grundverordnung, der Richtlinie (EU) 2016/680 (Richtlinie zum Datenschutz bei Polizei und Justiz) und des neuen Bayerischen Datenschutzgesetzes für bayerische öffentliche Stellen, Stand Dezember 2018, im Internet abrufbar unter http://www.stmi.bayern.de/sus/datensicherheit/datenschutz/reform_arbeitshilfen/index.php.

[13] Siehe IV. 2., Modul 1. Das bereitgestellte Ausfüllbeispiel für eine Verarbeitungstätigkeit „Personal verwalten“ der Stadt Fiktivia ist keine generelle Musterbeschreibung für eine Verarbeitungstätigkeit „Personalverwaltung“.

[14] Im Rahmen dieses Beispiels wird der Begriff „Verarbeitungstätigkeit“ synonym zu dem Begriff „Verarbeitungsvorgang“ im Sinn des Art. 35 DSGVO verstanden; vgl. hierzu bereits die Orientierungshilfe „Datenschutz-Folgenabschätzung“ (Fn. 1), S. 5.

Bearbeitungsdatum
10.01.2019 [Datum der letzten Speicherung, automatisch generiert]

b) Kontext

aa) Überblick

(1) Welche Verarbeitung ist geplant?

Verarbeitungstätigkeit: Personal verwalten
Prozessbeschreibung:
Unter die Verarbeitungstätigkeit fallen:

(a) HR-Kernfunktionen: In diesem Bereich werden die Personalstammdaten verarbeitet, also z. B. relevante Kontaktdaten, Finanzdaten, Arbeitsverträge usw.
(b) HR-Gehaltsabrechnung: Zusammensetzung des Arbeitsentgelts (Grundgehalt, Zuschläge, Abschläge, Zulagen usw.) wird monatlich je Personalfall ermittelt.
(c) Zeit- und Anwesenheitsmanagement: Verarbeitung der Arbeitszeiten, Urlaube, Dienstbefreiungen usw.
(d) Personalplanung und –analyse: Simulation der Personalkosten und Personalbedarfe für die Zukunft.
(e) Organisationsmanagement: Verwaltung aller Dienststellen/Ämter und ihrer Hierarchiestrukturen sowie Zuordnung der Beschäftigten über das Stellenmanagement zu den einzelnen Organisationseinheiten.

Details siehe Prozesslandkarte „Personal verwalten" zusammen mit allen dazugehörenden und beschriebenen Geschäftsprozessen.

(2) Welche Zuständigkeiten bestehen für die Verarbeitung?

Siehe Punkt 1 und 9 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten" (Dok-ID: 111111).

(3) Gibt es Normen oder Standards für die Verarbeitung?

Die bei der Verarbeitung umgesetzten Geschäftsprozesse halten die bestehenden normativen personalwirtschaftlichen Vorgaben ein und berücksichtigen Empfehlungen sachkundiger Dritter. Zudem wird ein weit verbreitetes IT-System mit diversen Zertifizierungen verwendet, von dessen Standards die Stadt nicht nennenswert abweicht. Da dieses HCM-System umfassend die Verarbeitungstätigkeit unterstützt, wird die Verarbeitung von den umgesetzten Standards der HCM-Fachapplikation maßgeblich mit geprägt.

bb) Daten, Prozesse und Unterstützung

(1) Welche Daten werden verarbeitetet?

Siehe Punkt 3 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten" (Dok-ID: 111111).

(2) Wie verläuft der Lebenszyklus von Daten und Prozessen?

Lebenszyklus Daten: Der Lebenszyklus der Daten richtet sich nach den Geschäftsprozessen des Kernprozesses „Personal verwalten", die die Daten erstellen, pflegen und löschen. Zum Löschen siehe Löschkonzept „Personal verwalten" (Dok-ID: 121654).

Lebenszyklus Prozesse: Das Geschäftsprozessmanagement, insbesondere die Geschäftsprozesse „Neuen Prozess etablieren“ und „Etablierten Prozess ändern“ bestimmen den Lebenszyklus der betroffenen Prozesse, siehe Prozesslandkarte „Geschäftsprozesse managen“ zusammen mit allen dazugehörigen und beschriebenen Geschäftsprozessen.

(3) Mit Hilfe welcher Betriebsmittel erfolgt die Datenverarbeitung?

Betriebsmittel sind das IT-Personalwirtschaftssystem HCM-Fiktivia, die Druckstraßen DRS-1 und DRS-2 im Druckzentrum des städtischen Hauptrechenzentrums, das städtische Intranet und der HCM-Formularserver FormServ-HCM.
Details ergeben sich aus der jeweiligen Spezifikation der genutzten Betriebsmittel.

c) Grundlegende Prinzipien

aa) Verhältnismäßigkeit und Notwendigkeit

(1) Sind die Verarbeitungszwecke eindeutig definiert und rechtmäßig?

Ja, siehe Punkt 2 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“ (Dok-ID: 111111).

(2) Aufgrund welcher Rechtsgrundlage erfolgt die Verarbeitung?

Siehe Punkt 2 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“ (Dok-ID: 111111)

(3) Sind die erhobenen Daten erforderlich, relevant und auf das für die Datenverarbeitung Notwendige beschränkt?

Ja, siehe Anlage „Datenkategorien und ihre Dateneingabefelder“ zur Beschreibung der Verarbeitungstätigkeit „Personal verwalten“ (Dok-ID 121034); in dieser Anlage wird zu jedem Eingabedatum dessen Notwendigkeit begründet. Zudem stehen keine alternativen Vorgehensweisen zur Verfügung, die in die Rechte und Freiheiten betroffener Personen weniger stark eingreifen.

(4) Sind die Daten korrekt und auf dem neuesten Stand?

Ja. Wie aus den relevanten Geschäftsprozessen hervorgeht, lösen denkbare Datenänderungen immer Ereignisse (z. B. Änderungsmitteilung) aus, die zeitnah für die erforderlichen Änderungen in den führenden Informationssystemen sorgen.

(5) Welche Speicherdauer haben die Daten?

Siehe Punkt 7 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten“ (Dok-ID: 111111).

bb) Maßnahmen zum Schutz der Persönlichkeitsrechte der betroffenen Personen

(1) Wie werden die betroffenen Personen über die Verarbeitung informiert?

Die Information betroffener Personen erfolgt zweistufig:

(a) Information im Umfang von Art. 13 f. DSGVO werden den betroffenen Personen zum jeweils gesetzlich vorgesehen Zeitpunkt erteilt. Für Bewerberinnen und Bewerber

werden Informationen auf speziellen Internetseiten der Stadt vorgehalten. Neu eingestellten Beschäftigten wird mit Einstellung ein entsprechendes Informationsdokument übergeben. Beschäftigte in bereits bestehenden Beschäftigungsverhältnissen wurden am 25.05.2018 durch Übersendung des vorgenannten Informationsdokuments informiert.

(b) Bei zusätzlichem Auskunftsbedarf sind zu den einzelnen Verarbeitungsbereichen Kontaktmöglichkeiten angegeben, über die spezifische Detailinformationen von betroffenen Personen bezogen werden können.

(2) Wenn anwendbar, wie wird die Einwilligung der betroffenen Personen eingeholt?

Es werden in vorliegendem Zusammenhang keine personenbezogenen Daten auf Grundlage einer Einwilligung verarbeitet (vgl. Punkt 2 aus der Beschreibung der Verarbeitungstätigkeit „Personal verwalten", Dok-ID: 111111).

(3) Wie können Betroffene ihr Recht auf Auskunft und Datenübertragbarkeit ausüben?

Bei der Stadt koordiniert und stellt eine zentrale Stelle sicher, dass Datenschutz-Anfragen betroffener Personen ggf. zur Beantwortung bzw. Umsetzung an die relevanten Dienststellen weitergeleitet und die qualitätsgesicherten Antworten der Dienststellen an die betroffene Person fristgerecht weitergegeben werden (Details siehe Prozesslandkarte „Ausübung eines DSGVO-Betroffenheitsrechts managen" inklusive der dazugehörenden Geschäftsprozesse (Dok-ID: 121690)).

Auskunft: Die Datenzusammenstellung zur Beantwortung eines Auskunftsersuchens einer betroffenen Person, die mit HCM-Fiktivia verarbeitet wird, wird durch einen speziellen Standard-Report technisch unterstützt.

Datenübertragbarkeit: Eine Recht auf Datenübertragbarkeit besteht vorliegend nicht: Die gesetzlichen Voraussetzungen von Art. 20 Abs. 1 DSGVO sind nicht gegeben; zudem greift der Ausschlusstatbestand des Art. 20 Abs. 3 Satz 2 DSGVO.

(4) Wie können betroffene Personen ihr Recht auf Berichtigung und Löschung (Recht auf Vergessenwerden) ausüben?

Zum Kernprozess „Ausübung eines DSGVO-Betroffenheitsrechts managen" siehe III.2.c)bb) unter (3).

Berichtigung: Rechtskonforme Berichtigungen werden u. a. durch Änderungsfunktionen von HCM-Fiktivia technisch umgesetzt.

Löschung: Rechtskonforme Löschanforderungen können in HCM-Fiktivia durch punktuelle (Löschung von „Einzeldaten" in einem Personalfall) und personalfallbezogene (Löschung gesamter Personalfall) Löschfunktionen umgesetzt werden.

(5) Wie können betroffene Personen ihre Rechte auf Einschränkung oder Widerspruch der Verarbeitung ausüben?

Zum Kernprozess „Ausübung eines DSGVO-Betroffenheitsrechts managen" siehe unter III. 2. C) bb) unter (3).

(6) Sind die Verpflichtungen der Auftragsverarbeiter klar definiert und vertraglich geregelt?

Es werden keine Auftragsverarbeiter eingesetzt.

(7) Soweit Datenübermittlungen in Länder außerhalb der Europäischen Union stattfinden, werden die Daten angemessen geschützt?

Eine Datenübermittlung in Länder außerhalb der EU findet nicht statt.

d) Risiken

aa) Geplante oder bestehende Maßnahmen (Auszug)

M.1 Basis Backup-Struktur nutzen:
Die Stadt stellt für ihre IT-Infrastruktur zahlreiche Basiskomponenten für die Datensicherung (z.B. redundantes Rechenzentrum, zentrale Backup-Server) inkl. der für die Betreuung erforderlichen Organisation zur Verfügung. Das HCM muss nachweisbar (Spezifikation und Umsetzungsnachweis) in diese Basis-Infrastruktur für die Datensicherung integriert werden.
M.2 Dienstleistungsangebot HCM-Hersteller nutzen:
Der Hersteller von HCM-Fiktivia bietet von der Stadt zu nutzende Unterstützungsleistungen beim Systembetrieb an, die über den städtischen Pflegevertrag (siehe Dok-ID 452356) abgerufen werden können. Zudem besteht zwischen der Stadt und dem Hersteller ein Dienstleistungsrahmenvertrag über 150 Personentage pro Jahr (siehe Dok-ID 985432), die im Rahmen des HCM-System flexibel eingesetzt werden können. Da dieser Vertrag am 31.12.2019 enden wird, ist ein neuer Rahmenvertrag in Höhe von 150 Personentagen pro Jahr ab 01.01.2020 auszuschreiben. Darin müssen insbesondere ausreichend Dienstleistungskapazität für die Themen „Beratung Daten HCM-System wiederherstellen", „Datenfehleingaben vermeiden und erkennen" und „Workflow (z.B. 4-Augen-Prinzip)" gesichert werden. Da keine Fernwartung existiert und der Hersteller von HCM-Fiktivia keine Möglichkeit hat, auf personenbezogene Daten der Stadt zuzugreifen, besteht keine Auftragsverarbeitung.
M.3 Löschberechtigung restriktiv vergeben:
Systembenutzer haben grundsätzlich keine Löschberechtigung, d.h. nur in begründeten und dokumentierten Ausnahmefällen kann eine Löschberechtigung zugewiesen werden.
M.4 HCM-Benutzer schulen:
Alle HCM-Benutzer, die im System personenbezogene Daten neu eingeben, ändern und/oder löschen können (Berechtigungskonzept), dürfen dies erst nach dem erfolgreichen Besuch der dafür vorgesehenen HCM-Schulung und einem regelmäßig erbrachten Kompetenznachweis.
M.5 Lesenden Zugriff für berechtigte Dritte konfigurieren:
Für berechtigte Dritte (z. B. Finanzprüfer, Auditoren) ist im Rollen- und Berechtigungskonzept eine Rolle vorhanden, die nur einen lesenden Zugriff auf die relevanten Daten gestattet. Die durchgängige Verwendung dieser Rolle in den einschlägigen Fällen ist gewährleistet..
M.6 usw.

Hinweis:
In diesem Bereich befinden sich die Liste der Bezeichnungen und die jeweilige genauen Beschreibung aller Datenschutz-Schutzmaßnahmen. Für eine eindeutige Verknüpfung in das städtische Maßnahmenmanagementsystem (siehe III. 1.) versieht die Stadt alle Maßnahmen mit einer eindeutigen Nummer („M.1", „M.2" usw.).

Da der Stadt die zentrale Übersicht aller Datenschutz-Schutzmaßnahmen wichtig ist, werden auch die ggf. bereits in der Beschreibung von Verarbeitungstätigkeiten erfassten Maßnahmen in die PIA-Tool-Liste integriert

bb) Risikoanalysen (unrechtmäßiger Zugriff auf Daten usw.)

(1) Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?

Risikobewertung siehe unten (5) und (6).

(2) Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?

Risikobewertung siehe unten (5) und (6).

(3) Was sind die Risikoquellen?

Risikobewertung siehe unten (5) und (6).

(4) Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?

Risikobewertung siehe unten (5) und (6).

(5) Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?

Risikoanalyse:
Die Risikoanalyse erfolgt in folgenden zwei unterschiedlichen Bereichen.
Risikoanalyse der SDM-Datensicherheitsziele:
Für die SDM-Gewährleistungsziele der klassischen Informationssicherheit „Verfügbarkeit", „Vertraulichkeit" und den Teilaspekt „Datenintegrität" des SDM-Gewährleistungsziels „Integrität" wurde die Risikoanalyse mittels einer klassischen Risikomanagementmethode ermittelt. Die genaue Durchführung und Ergebnisse sind aus der Anlage „Risikoanalyse-SDM-Datensicherheitsziele.pdf" ersichtlich.
Risikoanalyse der SDM-Schutzbedarfsziele:
Für die anderen SDM-Gewährleistungsziele „Datenminimierung", „Intervenierbarkeit", „Transparenz" und „Nichtverkettung" sowie der Teilaspekte „Konzepteinhaltung" und „Richtigkeit" des SDM-Gewährleistungsziels „Integrität" wurde die Risikoanalyse anhand eines Zielerfüllungsmanagements durchgeführt, dessen Inhalte und Ergebnisse sich aus der Anlage „Risikoanalyse-SDM-Schutzbedarfsziele.pdf" ergeben.

(6) Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplante Maßnahmen?

Ergebnis Zielgesamtbewertung:
Die beiden durchgeführten Risikoanalysen führten im Hinblick auf die SDM-Gewährleistungszeile zu folgendem Ergebnis:

1.	Verfügbarkeit:	🟡
2.	Vertraulichkeit:	🟡
3.	Datenintegrität:	🟡
4.	Datenminimierung:	🟡
5.1	Intervenierbarkeit:	🟡
5.2	Transparenz:	🟢
5.3	Nichtverkettung:	🟡

6. Konzeptionseinhaltung: ●
7. Richtigkeit: ●

Insgesamt ergeben somit die beiden durchgeführten Risikoanalysen für die SDM-Datensicherheitsziele und für die SDM-Schutzbedarfsziele im Ergebnis, dass die SDM-Gewährleistungsziele als erfüllt angesehen werden können. Die betrachtete Verarbeitungstätigkeit „Personal verwalten" steht nach wirksamer Umsetzung der in der Datenschutz-Folgenabschätzung festgelegten Datenschutzmaßnahmen im Einklang mit der Datenschutz-Grundverordnung.

Hinweis:
Die Stadt verankert im PIA-Tool ihre beiden unterschiedlichen Risikoanalysen im Abschnitt „Risiken -Unrechtmäßiger Zugriff auf Daten", da das PIA-Tool die Dokumentation von Risikoanalysen in Tabellenform hinsichtlich seiner inhaltlichen Gliederungsstruktur derzeit nicht vorsieht. Die anderen beiden PIA-Tool-Bereiche für die Datensicherheitsrisiken „Risiken – Unerwünschte Datenveränderung" und „Risiken – Datenverlust" werden von der Stadt nicht genutzt.

Das Gesamtergebnis für die Risikobewertung der Verarbeitungstätigkeit „Personal verwalten" mit der darauf basierenden Aussage, dass die Verarbeitungstätigkeit bei der Stadt bei wirksamer Umsetzung der festgelegten Sicherstellungs- und Abhilfemaßnahmen die DSGVO-Anforderungen einhält, ist ein wesentlicher Bestandteil des DSFA-Berichts (siehe Abb. 12: DSFA-Bericht). Grundlage hierfür sind die beiden separat durchgeführten Risikoanalysen für die SDM-Datensicherheitsziele und für die SDM-Schutzbedarfsziele. Die Zusammenführung der einzelnen Bewertungen, wie sie sich aus den beiden Risikoanalysen ergeben, zur Risikogesamtbewertung vollzieht die Stadt direkt im PIA-Tool.

e) DSFA-Anlage: Risikoanalyse für die SDM-Datensicherheitsziele (Auszug)

Eine Risikoanalyse für die SDM-Datensicherheitsziele ist auszugsweise aus Abb. 16 (Auszug aus der Anlage zum SDM-Datensicherheitsziel „Verfügbarkeit") und umfassender aus den Tabellen für das Risikomanagement zur Verarbeitungstätigkeit „Personal verwalten ersichtlich. Diese Tabellen stehen als Formularsätze – nebst Ausfüllbeispielen für die Verarbeitungstätigkeit „Personal verwalten" der Stadt Fiktivia – bereit (IV. 2., Modul 3).

Hinweis:
Die Risikoanalyse je SDM-Datensicherheitsziel besteht jeweils aus zwei Bereichen. Im unteren Bereich werden die Einzelrisiken, wie unter Abb. 4: Risikoanalyse der SDM-Datensicherheitsziele) schematisch festgelegt, aufgelistet, die jeweils mit einer eindeutigen Identifikation (z. B. „VB.1", „VB.2", usw.) markiert sind. Für die Maßnahmen wird nur die Kurzbezeichnung mit der eindeutigen Maßnahmen-Nummer erfasst, da die Maßnahmen inklusive ausführlicher Beschreibung führend im PIA-Tool gepflegt werden. Der untere Bereich kann als **„Risikoprofil"** zu einem SDM-Datensicherheitsziel verstanden werden.

Der obere Bereich hingegen besteht ausschließlich aus der dokumentierten und begründeten Einschätzung, ob nach einer summarischen Betrachtung des unten stehenden Risikoprofils hinsichtlich des betroffene SDM-Datensicherheitsziels „die Zielerfüllung gewähr-

leistet ist“ (grün), „die Zielerfüllung noch vertretbar als erreicht angesehen werden kann“ (gelb) oder aber „die Zielerfüllung nicht gewährleistet werden kann“ (rot). Der obere Bereich kann demnach als **„Ziel-Bewertung“** bezeichnet werden.

f) DSFA-Anlage: Risikoanalyse für die SDM-Schutzbedarfsziele (Auszug)

Eine auszugsweise Risikoanalyse für die SDM-Schutzbedarfsziele ist aus Abb. 17 (Auszug aus der Anlage zum SDM-Datenschutzbedarfsziel „Nichtverkettung“) ersichtlich.

Hinweis:
Wie bei der Risikoanalyse für die SDM-Datensicherheitsziele ist auch diese Anlage für jedes betrachtete Ziel in die beiden Bereiche Gefährdungsprofil und Ziel-Bewertung unterteilt.

g) DSFA-Anlage: Standpunkte betroffener Personen

Die Stadt hat der bei ihr bestehenden Personalvertretung Gelegenheit zur Stellungnahme gegeben (vgl. Art. 35 Abs. 9 DSGVO). Insbesondere vor dem Hintergrund, dass die betrachtete Verarbeitungstätigkeit schon lange ohne nennenswerte Änderungen betrieben wird, hat die Personalvertretung auf die Abgabe einer Stellungnahme verzichtet.

Gewährleistungsziel	Summarische Risikobetrachtung	Index
Verfügbarkeit	Ermittlung des Risikoindexes über alle Einzelrisiken (unten stehendes Risikoprofil) nach der Maximum-Methode, d.h. der vorkommende höchste Risikoindex wird dem SDM-Datensicherheitsziel zugeordnet.	ge

ID	Schwachstelle	Risikoquelle	Risiko-Szenario	Eintrittswahrscheinlichkeit		Schwere/Schaden		Index	Maßnahme-Bezeichnung	Risikoeinschätzung mit Maßnahmen	
				Erläuterung	Grad	Erläuterung	Grad			Erläuterung	Index
VB.1	Digitale Daten können nach einem unerwünschten Verlust nicht wiederhergestellt werden.	IT-Fehlfunktion	Hard- und/oder Software-Fehlfunktion führen dazu, dass erforderliche digitale Daten unwiederbringlich verloren gehen.	Aufgrund der Komplexität des HCM-Systems (zahlreiche, zusammenwirkende Komponenten, häufige Updates usw.) ist ein Datenverlust durch IT-Fehlfunktionen sehr wahrscheinlich.	4	Wesentliche Daten sind in Papierform vorhanden, so dass der Schaden bei einem Verlust der digitalen Daten im Rahmen bleibt .	2	8	M.1 Basis Backup-Struktur nutzen M.2 Dienstleistungsangebot HCM-Hersteller nutzen	Datenverluste bei von der Stadt betriebenen Systemen, die mit dem HCM-System vergleichbar sind, gehen gegen Null.	gr
VB.2	= VB.1 =	Interner User	User-Interaktionen mit dem HCM-System führen dazu, dass erforderliche Daten unwiederbringlich verloren gehen.	Aufgrund der angespannten Personalsituation werden teilweise auch noch sehr unerfahrene HCM-Sachbearbeiter eingesetzt.	2	Fehlbedienungen von internen Usern, die zu einem Datenverlust führen (z.B. Daten versehentlich überschreiben), sind punktuell und werden i.d.R. rasch erkannt und wieder berichtigt.	2	4	M.1 Basis Backup-Struktur nutzen M.3 Löschberechtigung restriktiv vergeben M.4 HCM-Benutzer schulen	Die Maßnahmen zusammen führen zu einer deutlich reduzierten Eintrittswahrscheinlichkeit.	gr
VB.3	= VB.1 =	Externer User	Interaktionen externer User (z.B. Finanzprüfer, Auditoren) mit dem HCM-System führen dazu, dass erforderliche Daten unwiederbringlich verloren gehen.	Zugriffe externer User auf das produktive HCM-System finden nur selten statt.	2	Wesentliche Daten sind in Papierform vorhanden, so dass der Schaden bei einem Verlust der digitalen Daten im Rahmen bleibt .	2	4	M.5 Lesenden Zugriff für berechtigte Dritte konfigurieren	Fehlbedienungen von externen Benutzern, die zu einem Datenverlust führen, sind nicht vorstellbar, da solche Benutzer stets nur mit Leserechten ausgestattet sind (bewährtes Standardbenutzerprofil).	gr
VB.4	= VB.1 =	Interner Administrator	Interaktionen eines User mit weitreichenden Administratorenrechten mit dem HCM-System führen dazu, dass erforderliche Daten unwiederbringlich verloren gehen.	Da es das Alltagsgeschäft von Administratoren ist, mit produktiven IT-Systemen richtig umzugehen, ist der Eintritt unwahrscheinlich.	2	Wesentliche Daten sind in Papierform vorhanden, so dass der Schaden bei einem Verlust der digitalen Daten im Rahmen bleibt .	2	4	M.1 Basis Backup-Struktur nutzen M.3 4-Augen-Prinzip für tragende Personaldatenänderungen umsetzen M.6 HCM-Administratoren zertifizieren	Blickt man auf die schon lange aktive Administrationstätigkeit mit Umsetzung der Maßnahmen zurück, so erscheint der Eintritt als sehr unwahrscheinlich.	gr
VB.5	= VB.1 =	Cyberkrimineller (Hacker/ Schadsoftware)	Mit Hilfe einer beliebig ausgestalteten Schadsoftware gehen erforderliche Daten unwiederbringlich verloren.	Cyberkriminelle Angriffe nehmen ständig zu, so dass der Eintritt als sehr wahrscheinlich einzustufen ist.	4	Wesentliche Daten sind in Papierform vorhanden, so dass der Schaden bei einem Verlust der digitalen Daten im Rahmen bleibt .	2	8	M.7 Basis Schadsoftware-/ Hackerabwehrsystem nutzen M.1 Basis Backup-Struktur nutzen	Datenverluste bei ebenfalls betriebenen IT-Systemen, die mit dem HCM-System vergleichbar sind, sind entsprechend eingestuft. Bzgl. HCM-System sind keine Besonderheiten erkennbar.	ge
VB.6	Monatlichen Gehaltsabrechnung kann nicht rechtzeitig durchgeführt werden	Interner User	Fehlendes, nicht mittelfristig ersetzbares Personal bringt monatliche Personalabrechnung zum Stehen.	Altersstruktur des betroffenen Personals und relativ hohe Fluktation von Experten im HCM-Umfeld verschärfen die Situation.	4	Falls die Entgeltabrechnung nicht ordnungsgemäß läuft, kann dies zu ernsthaften finanziellen Schwierigkeiten der Beschäftigten führen.	3	12	M.8 Kopfmonopole mittels Teambildung reduzieren M.9 Dienstleistung Dritter nutzen M.10 Manuelle Abschlagzahlung	Trotz der ergriffenen Maßnahmen für die aktive und passive Risikobewältigung kann das Risiko nicht in den grünen Bereich gebracht werden.	ge

Abb. 16: Auszug aus der Anlage zum SDM-Datensicherheitsziel „Verfügbarkeit“

Gewährleistungsziel	Summarische Gefährdungsbetrachtung	Index
Nichtverkettung	Ermittlung des Gefährdungsindexes über alle Einzelgefährdungen (unten stehendes Gefährdungsprofil) nach der Maximum-Methode, d.h. die vorkommende höchste Gefährdungsstufe wird dem SDM-Schutzbedarfsziel zugeordnet.	ge

ID	Schwachstelle	Gefährdungsquelle	Gefährdungszenario	Gefährdungsbewertung		Maßnahme-Bezeichnung	Gefährdungsbewertung	
				Erläuterung	Index		Erläuterung	Index
NV.1	Daten können durch den Einsatz von **integrativen IT-Systemen** zusammengeführt werden.	~ Internes Personal ~ IT-Fehlfunktion	Durch hochintegrative Systeme (z.B. EIN System für Personal- und Finanzwirtschaft) werden Daten verschiedener Fachbereiche zusammengeführt und können rechtswidrig verarbeitet werden (z.B. wegen Lücke in Berechtigungskonzept oder technischer Fehler bei Berechtigungssteuerung).	Hinsichtlich der bestehenden Komplexität integrativer IT-Systeme sind unbeabsichtigte Konfigurationslücken und technische Fehler bei der Berechtigungssteuerung als Gefährdung für die Erfüllung der Nichtverkettung einzuschätzen.	ge	M.37 Separates HCM-System verwenden M.38 Separates HCM-Datawarehouse-System verwenden	Duch die konsequente Trennung der IT-Systeme (M.80/M.81) sind Zweckentfremdungen in diesem Bereich nicht mehr denkbar.	gr
NV.2	Daten können durch **technische Datenschnittstellen** zusammengeführt werden.	~ Internes Personal ~ IT-Fehlfunktion	Technische Schnittstellen aus bzw. in das HCM-System führen aufgrund falscher Konfiguration oder eines technischen Fehlers Daten rechtswidrig zusammen.	Hinsichtlich der Schwierigkeit, Schnittstellen fehlerfrei umzusetzen, sind unbeabsichtigte Konfigurationslücken und technische Fehlfunktionen als Gefährdung für die Erfüllung der Nichtverkettung einzuschätzen.	ge	M.27 Schnittstellenkonzepte für HCM-Fiktivia managen M.39 Enterprise Architecture Management (EAM-Tool) einsetzen	Durch die beiden Maßnahmen und das Zusammenspiel mit der konsequenten Trennung der IT-Systeme (M.37/M.38) und das Berechtigungskonzept (M.29) sind Zweckentfremdungen in diesem Bereich nicht mehr denkbar.	gr
NV.3	Daten können durch **unerwünschte Dateneingabe** zusammengeführt werden.	Interner User	Interne User sehen es als sinnvoll an, weitere personenbezogen Daten im HCM-System zu erfassen und tun dies an für sie geeigneten Stellen (z.B. Freitext-Eingabefeld, ungenutzte Eingabefelder), ohne den dafür vorgesehenen Change Request-Prozess für den Änderungsbedarf anzustoßen.	In der Vergangenheit gab es bei vergleichbaren Verarbeitungen nach einiger Laufzeit einen ungewollten "Datenwildwuchs" durch manuelle zusätzliche Dateneingaben, die konzeptionell nicht vorgesehen sind.	ge	M.4 HCM-Benutzer schulen M.28 Risikoorientiert auswerten M.40 Zweckänderungsverfahren implementieren	Wie aus den langjährig gemachten Erfahrungen hervorgeht, genügen die Maßnahmen, um hier das Schutzniveau zu gewährleisten.	gr
NV.4	Daten können durch **unbefugte Datenweitergabe** zusammengeführt werden.	Internes Personal	Personal, das beim Fachthema "Personal verwalten" beteiligt ist, gibt rechtswidrig Daten für eine andere Verarbeitung weiter.	Relevante Anfragen städtischer Stellen und/oder Dritter sind oft zu beobachten, so dass das städtisches "HCM-Personal" leicht veranlasst werden kann, Daten nicht normenkonform weiterzugeben.	ro	M.4 HCM-Benutzer schulen M.29 Rollen- und Berechtigungskonzept umsetzen M.15 Dienstanweisung für die Übermittlung personenbezogener Daten umsetzen	Vertretbares Schutzniveau ist hergestellt. Vereinzelte, nicht kontrollierbare Weitergaben (z. B. mündliche Weitergabe bei Mitarbeitertreffen) können nicht ausgeschlossen werden.	ge
NV.5	Daten können durch **überschneidende Aufgabenbereiche** zusammengeführt werden.	Interne Organisations-verantwortung	Personal,das parallel in verschiedenen Fachbereichen gleichzeitig arbeitet (z.B. HCM und Finanzen), führt rechtswidrig Daten aus mehreren Bereichen zusammen.	Dem Personal, das gleichzeitig in zwei Fachbereichen arbeitet, fällt es oft sehr schwer, die Bereiche den normativen Anforderungen entsprechend abzugrenzen.	ro	M.41 Personal bereichsspezifisch einsetzen	Aufgrund der Größe der Stadt ist eine strikte Sachbearbeiter-Zuordnung ausschließlich zum Personalbereich durchzuhalten.	gr

Abb. 17: Auszug aus der Anlage zum SDM-Datenschutzbedarfsziel „Nichtverkettung“

IV. Anhang

1. Glossar

Begriff /Abkürzung	Erläuterung
BSI	Bundesamt für Sicherheit in der Informationstechnik (Internet: https://www.bsi.bund.de).
CNIL	Commission Nationale de l'Informatique et des Libertés (französische Datenschutz-Aufsichtsbehörde, Internet: https://www.cnil.fr).
Datenschutz-Schutzmaßnahmen	Alle Maßnahmen, die für die Reduzierung bzw. Beseitigung von Risiken für die Rechte und Freiheiten natürlicher Personen vorgesehen sind. Zu dieser Maßnahmengruppe gehören etwa die Abhilfe- und Sicherstellungsmaßnahmen.
Dok-ID	Jedes Dokument kann durch seine eindeutige Dokumenten-Identifikationsnummer (Dok-ID) aufgefunden und aufgerufen werden.
DSB	Datenschutzbeauftragter.
DSFA	Datenschutz-Folgenabschätzung nach Art. 35 DSGVO.
DSFA-Bericht	Ein Bericht/Report für eine Datenschutz-Folgenabschätzung.
Fachapplikation	IT-System, das die fachliche Sachbearbeitung und damit die fachlichen Geschäftsprozesse unmittelbar unterstützt.
on-premises Systemlösung	Bei on-premises-Software erwirbt oder mietet der Lizenznehmer Software und betreibt diese in eigener Verantwortung auf eigener Hardware, ggf. in einem eigenen Rechenzentrum oder auf gemieteten Servern eines fremden Rechenzentrums, in jedem Fall also auf Hardware, die nicht vom Anbieter der Software bereitgestellt wird (vgl. die Darstellung unter https://de.wikipedia.org/wiki/On_Premises).
PIA	Privacy Impact Assessment Methodik der CNIL.
PIA-Tool	Software für die Erstellung eines DSFA-Berichts, herausgegeben von der CNIL. Weitere Informationen hierzu siehe Praxishilfe „Software zur Datenschutz-Folgenabschätzung (PIA-Tool)", im Internet auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018".
Risikoanalyse	Im Hinblick auf einen bestimmten Verarbeitungsvorgang werden

	alle relevanten Szenarien erhoben, bewertet und ggf. mit Schutzmaßnahmen verknüpft, die ein Risiko bzw. eine Gefährdung bezüglich der DSGVO-Einhaltung darstellen. Mit jedem Szenario wird folglich möglichst differenziert ein Ereignis beschrieben, durch das der betrachtete Verarbeitungsvorgang den normativen DSGVO-Rahmen verlassen würde und das es daher zu vermeiden gilt.
SDM	Standard-Datenschutzmodell beschreibt eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele und befindet sich in der hier verwendeten Version V.1.1 vom April 2018 noch in der Erprobungsphase, Näheres im Internet unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell.
SDM-Datensicherheitsziele	Davon umfasst sind die beiden SDM-Gewährleistungsziele Verfügbarkeit und Vertraulichkeit sowie der Teilzielaspekt Datenintegrität des SDM-Gewährleistungsziels Integrität, siehe II. 1.
SDM-Gewährleistungsziel	Die sieben Gewährleistungsziele werden im SDM festgelegt und beschrieben, vgl. Abb. 2: Die sieben SDM-Gewährleistungsziele) sowie den Glossareintrag zu „SDM“.
SDM-Schutzbedarfsziele	Davon umfasst sind die vier SDM-Gewährleistungsziele Datenminimierung, Intervenierbarkeit, Transparenz und Nichtverkettung sowie der Teilzielaspekt Konzeptionseinhaltung und Richtigkeit des SDM-Gewährleistungsziels Integrität, siehe auch II. 1.

2. Modulverzeichnis

Auf meiner Homepage https://www.datenschutz-bayern.de stehen in der Rubrik „Datenschutz-Folgenabschätzung“ die folgenden, das PIA-Tool ergänzenden Module zur Verfügung. Angeboten werden dabei unausgefüllte Word- oder Excel-Formulare sowie als Anwendungsbeispiele ausgefüllte Formulare für eine Verarbeitungstätigkeit „Personal verwalten“ der Stadt Fiktivia, jeweils in Word- oder Excel- und PDF-Version:

Modul 1: Beschreibung der Verarbeitungstätigkeit […];

Modul 2: DSFA-Bericht in Formularform für die Verarbeitungstätigkeit […];

Modul 3: Tabellen für das Risikomanagement zur Verarbeitungstätigkeit […];

Modul 4: Tabellen für das Zielerfüllungsmanagement zur Verarbeitungstätigkeit […].