Gunnar Auth und Tim Pidun (Hrsg.):
Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023),
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023 109

Entwicklung einer Prozessmodellierungssprache zur Unterstützung bei datenschutzrechtlicher Dokumentation

Ein studentisches Projekt

Daniel Bierschwale[1], Paul-Ferdinand Steuck[1] und Ralf Knackstedt[1]

Abstract: Aus der Datenschutz-Grundverordnung ergeben sich Anforderungen wie Dokumentationspflichten für Prozesse, welche personenbezogene Daten verarbeiten. Für Fachkräfte resultiert daraus in der Praxis oft ein umfangreicher, ressourcenintensiver Dokumentationsprozess. Als Lösungsstrategie entwickelt diese Arbeit eine neue Sprache zur Prozessmodellierung, die auf der Grundlage von Fachexpertise im Rahmen einer Real-Time Delphi-Studie und einem systematischen Literaturreview entwickelt wurde. Diese Sprache zielt darauf ab, den Prozess der Informationserhebung für die Dokumentationspflicht zu vereinfachen und zu optimieren. Die Arbeit schließt mit einer Evaluation der entwickelten Sprache und einem Ausblick auf weiterführende Forschung.

Keywords: Datenschutz, DS-GVO, Prozessmodellierung, Design Science Research

1 Einleitung

[KNW20] beschreiben die Digitalisierung in der Verwaltung als kontinuierlichen Entwicklungsprozess, durch welchen Prozesse digital abgebildet werden. Besonders durch die digitale Transformation der Verwaltung werden immer mehr personenbezogene Daten verarbeitet. Der Datenschutz tangiert dabei nicht nur technologische Lösungen und Innovationen, sondern ebenfalls die Vorstellungen und Arbeitsabläufe von Verwaltungsmitarbeitenden und Bürgern [ibid.].

Die Datenschutz-Grundverordnung (DS-GVO) stellt Fachkräfte auch aktuell noch vor komplexe und umfangreiche Herausforderungen, wie etwa die unsichere Rechtslage, die den Einsatz neuer Technologien wie KI hemmt [We22]. Die umfangreiche Dokumentationspflicht im Kontext des Datenschutzes stellt insbesondere für Fachkräfte ohne vertiefende Kenntnisse in diesem Bereich eine erhebliche Herausforderung dar.

[1] Universität Hildesheim, Informationssysteme und Unternehmensmodellierung, Universitätsplatz 1, 31141 Hildesheim, {bierschwaled, steuckp, knacks} @uni-hildesheim.de

doi:10.18420/rvi2023-009

Unternehmen wenden im Durchschnitt etwa eine Arbeitsstunde pro Verarbeitung jährlich für die Pflege und Aktualisierung der erforderlichen Informationen auf. In kleineren Unternehmen manifestiert sich der Arbeitsaufwand in einer jährlichen Zeitspanne von etwa 30 bis 40 Stunden. Dieser Aufwand divergiert jedoch abhängig von der Unternehmensgröße und -struktur. Denn im Gegensatz dazu verzeichnen mittlere bis große Unternehmen einen deutlich höheren Zeitaufwand, der zwischen 92 und 297 Stunden pro Jahr liegen kann [Ha23]. Dieses hohe Maß an benötigter Zeit und Ressourcen kann sich hinderlich auf Digitalisierungsprojekte und Innovationspotentiale auswirken [We22].

Im Kontext der Digitalisierung und der E-Government-Gesetzgebung (EGovG) gewinnt das Prozessmanagement und die Prozessmodellierung in der Verwaltung an Bedeutung, da Prozesse unter anderem zu dokumentieren sind [NP18]. Eine hiermit korrelierende Anforderung findet sich auch in der DS-GVO, denn gemäß Art. 30 Abs. 1 DS-GVO ist das Verzeichnis von Verarbeitungstätigkeiten, in welchem sämtliche Verarbeitungsprozesse personenbezogener Daten zu dokumentieren sind, ein wesentlicher Bestandteil. Darüber hinaus reguliert Art. 5 Abs. 2 DS-GVO, dass die Einhaltung der Grundsätze aus Art. 5 Abs. 1 DS-GVO nachweisbar sein muss. Im Sinne der Handhabung der umfassenden Komplexität der DS-GVO, wie in [KEF18] hervorgehoben, wird oftmals versucht die Informationsgewinnung durch den Dialog und/oder den Einsatz von Fragebögen zu erreichen. Eine Möglichkeit zur Nutzung von Synergieeffekten, um die zuvor geschilderten Aufwände für Datenschutzbeauftrage und Fachkräfte bei der Pflege des Verzeichnisses von Verarbeitungstätigkeiten und der Umsetzung der Rechenschaftspflicht zu reduzieren, stellt die Erweiterung bzw. Nutzung von Prozessmodellierungen in der öffentlichen Verwaltung um datenschutzrechtliche Informationen dar.

Dieser Beitrag ist das Produkt eines Design Science Research (DSR) Projekts, nach dem Vorgehensmodell von [Pe07], welches im Rahmen einer universitären Lehrveranstaltung von einem studentischen Team durchgeführt wurde. Im Rahmen dieser Lehrveranstaltung haben die Studierenden die Aufgabe, Prozessmodellierungssprachen zu entwickeln oder zu erweitern, um ein reales Problem zu lösen. Hierbei ist von Relevanz, dass in der wissenschaftlichen Literatur keine andere etablierte Prozessmodellierungssprache identifiziert wird, welche das vorliegende Problem in optimaler Weise lösen kann. Der Kurs beginnt mit einer Phase der Themenfindung, in der die Studierenden angehalten sind, ein relevantes und anspruchsvolles Problemfeld zu identifizieren, das sowohl praktische als auch wissenschaftliche Relevanz aufweist. Nach intensiver Diskussion und Überlegung über das Thema, wurde folgende Forschungsfrage formuliert:

Wie sollte eine Prozessmodellierungssprache gestaltet sein, um Fachabteilungen in der Verwaltung bei der Erfassung der Informationen für eine Verarbeitung im Sinne des Datenschutzes zu unterstützen?

Zur Beantwortung der Forschungsfrage und um das Problem aus verschiedenen Perspektiven zu beleuchten, werden die Phasen nach Peffers et al. durchlaufen. Zunächst wird in Kapitel 2 zum Nachweis des Problems auf die methodische Vorgehensweise und die Ergebnisse einer durchgeführten Delphi-Studie mit Personen mit Datenschutzexpertise eingegangen. Anschließend werden in Kapitel 3 mittels eines systematischen Literaturreviews und anhand der DS-GVO selbst Kriterien bzw. Anforderungen für eine Prozessmodellierungssprache, die zur Dokumentation der Informationen gemäß Art. 5 Abs. 2 und insbesondere Art. 30 Abs. 1 DS-GVO notwendig sind, formuliert. Auf Grundlage dieser Erkenntnisse wird in Kapitel 4 im Rahmen unseres DSR-Projekts eine eigene Prozessmodellierungssprache entwickelt. In Kapitel 5 erfolgt die Evaluation der Modellierungssprache unter Berücksichtigung der Vorgehensweise von [GW04] und der Durchführung der Think-Aloud-Methode. Unsere Arbeit endet mit einer Rekapitulation sowie Reflektion der Ergebnisse und einem Ausblick auf mögliche nächste Schritte, die sich sowohl aus unserer Forschungsarbeit als auch aus den in der Lehrveranstaltung erworbenen Kenntnissen ergeben.

2 Datenschutz: Eine kontinuierliche Herausforderung

Dieses Kapitel widmet sich der ersten Phase nach [Pe07], der Problemidentifikation und -motivation, für welche entsprechende Informationen über den Problemstand sowie die Relevanz einer Lösung unverzichtbar sind [ibid.]. Für den Erhalt näherer Informationen darüber, inwiefern Fragebögen und Meetings hinsichtlich datenschutzrechtlicher Dokumentationspflichten zu Mehraufwand für Fachkräfte und Personen mit Datenschutzexpertise führen, wird eine Real-Time Delphi-Studie mit dem Tool eDelphi durchgeführt[2]. Bei dessen Ablauf wurde sich an dem Vorgehensmodell von [SR09] und den Eigenheiten einer Real-Time Delphi-Studie nach [GE19] orientiert. Das Ziel der Real-Time Delphi Studie lag in der Ermittlung und Qualifikation von Ansichten einer Gruppe von Personen mit Expertise zu folgender, übergeordneter Fragestellung:

Kommt es bei der Zusammenarbeit zwischen der Datenschutzabteilung und den Fachabteilungen bei der Erfassung der Informationen für die Verarbeitung personenbezogener Daten für das Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 DS-GVO zu einer Überlastung der Datenschutzabteilung und zugleich auch zu Schwierigkeiten bei der Bereitstellung der notwendigen Informationen durch die Fachabteilungen?

Diese Fragestellung wurde im Zuge der Entwicklung des Fragebogens entsprechend der Empfehlung von [SR09] nach dem Konzept der Operationalisierung der Fragestellung nach [Hä09] in zwei Facetten untergliedert, die einzeln beleuchtet werden.

[2] Siehe eDelphi.org: https://www.edelphi.org/

Die Überlastung der Datenschutzabteilung. Diese Facette umfasst Fragen, die sich direkt mit der Belastung für eine Datenschutzabteilung durch den Mehraufwand im Rahmen der Unterstützung der Fachabteilungen bei der Erhebung der Informationen für eine Verarbeitung auseinandersetzen.

Die Bereitstellung der notwendigen Informationen durch die Fachabteilungen. Diese Facette umfasst Fragen, die sich primär auf die Qualität der bereitgestellten Informationen durch die Fachabteilung beziehen und adressieren unter anderem die Kompetenzen der Fachkräfte hinsichtlich des Themas Datenschutz.

Insgesamt haben sich an der Real-Time Delphi-Studie fünf Personen mit Expertise (n=5) beteiligt, die Ihre Qualifikation zum einen durch ihre langjährige Praxiserfahrung von mehr als 8 Jahren in einer Datenschutzabteilung eines internationalen IT-Service Providers und zum anderen durch entsprechende Zertifikate der Gesellschaft für Datenschutz und Datensicherheit zum Thema Datenschutz nachwiesen. Die Ergebnisse der Real-Time Delphi-Studie zeigen auf, dass der bestehende Prozess zur Unterstützung der Fachabteilungen bei der Erfassung der Informationen als ineffizient wahrgenommen wird. Die Personen mit Expertise sind sich nahezu einig und geben an, dass dieser Prozess erheblichen Mehraufwand für die Datenschutzabteilung verursacht. Dieser Mehraufwand führt zu Verzögerungen und Beeinträchtigungen der Arbeit. Zudem zeigen die Ergebnisse, dass Mitarbeitende der Fachabteilungen Schwierigkeiten haben, relevante Kerninformationen wie den Zweck oder die Rechtsgrundlage einer Verarbeitung zu erfassen. Unklare Verantwortlichkeiten und ein mangelndes Verständnis in den Fachabteilungen führen ebenfalls zu Problemen wie Verzögerungen bei der Klärung von Rückfragen. Die Umfrageergebnisse weisen somit auf die Bedeutung einer Lösung hin, um den Mehraufwand für die Datenschutzabteilung zu reduzieren und die Fachabteilungen effektiv bei der eigenständigen Erfassung der Kerninformationen zu unterstützen.

3 Anforderungen an eine Modellierungssprache

Die DS-GVO definiert in Art. 5 verschiedene Grundsätze, dessen Einhaltung für jeden Verantwortlichen obligatorisch sind. Einer dieser Grundsätze, die Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO, fordert die Einhaltung der anderen Grundsätze und die Fähigkeit hierfür einen Nachweis erbringen zu können. Dieser Nachweis korreliert unter anderem mit dem Art. 30 DS-GVO, nach welchem von einem Verantwortlichen und gegebenenfalls seinem Vertreter, ein Verzeichnis sämtlicher Verarbeitungen zu führen ist, die in dessen Zuständigkeit fallen. Hierbei handelt es sich jedoch um eine weitreichende Dokumentationspflicht [Br18], die sich auch auf Verarbeitungen als Auftragsverarbeiter gemäß Art. 30 Abs. 2 DS-GVO erstreckt. In Anlehnung an die zweite Phase des Vorgehensmodells nach [Pe07], haben wir den Forschungsstand hinsichtlich der Prozessmodellierung im Bereich der DS-GVO bzw. des Datenschutzes untersucht. Dies erfolgte durch ein systematisches Literaturreview gemäß der Vorgehensweise von [Br09].

Ziel des Literaturreviews war die Synthese der bestehenden Lösungen, um die Grenzen von aktuellen Modellierungssprachen aufzuzeigen und Anforderungen an eine zu entwickelnde Modellierungssprache zu definieren. Die Suche des Literaturreviews wurde anhand der PRISMA-Methode [Mo09] in Google Scholar durchgeführt[3], was zu einer Gesamtzahl von 150 Ergebnissen führte. Hierbei wurden Publikationen in dem Zeitraum von 2018-2023 berücksichtigt. Nach Prüfung der Abstracts und Titel wurden 11 Ergebnisse als relevant identifiziert, wobei als Kriterium für die Relevanz die Einführung einer neuen Modellierungssprache oder die Weiterentwicklung einer existierenden Modellierungssprache im Bereich des Datenschutzes diente. Basierend auf den aus der identifizierten Literatur abgeleiteten Anforderungen und den obligatorischen Inhalten für ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO sowie der Nachweispflicht gem. Art. 5 Abs. 2 DS-GVO wurde ein Kriterienkatalog entworfen. Dieser Katalog dient zum einen als Grundlage für einen Abgleich mit bestehenden Modellierungssprachen der Domäne und zum anderen für eine anforderungsorientierte, systematische Entwicklung der Modellierungssprache. Für den Abgleich mit bestehenden Modellierungssprachen wurden weiterhin fünf Ansätze aus der identifizierten Literatur ausgewählt. Die Kriterien werden in die Kategorien “Daten” und “Prozess” untergliedert. “Daten” umfasst hierbei alle Informationen, die nach der DS-GVO von der Fachabteilung zu dokumentieren sind. “Prozess” beinhaltet unterstützende Komponenten für die Bewertung von Sachverhalten und Entscheidungsfindungen sowie deren Dokumentation.

Kategorie	Kriterium	Kriterium-Beschreibung	[CM19]	[Ag19]	[BR19]	[WSG21]	[MA20]
Daten	Kategorisierung	Kategorien personenbezogener Daten	✓	X	X	X	✓
	Personenbezogen	Hervorhebung von Personenbezogene Daten	✓	X	X	✓	✓
	Rechtsgrundlage	Rechtsgrundlage der Verarbeitung	✓	X	X	X	✓
	Schutzbedarf	Schutzbedarf der Daten	X	X	X	✓	✓
	Speicherdauer	Aufbewahrungszeit der Daten	✓	X	X	X	✓
	Verantwortlichkeit	Verantwortliche Person	X	X	X	X	✓
	Zweckbindung	Zweck zu dem die Daten verarbeitet werden	✓	✓	X	X	✓
Prozess	Einbettung in Geschäftsprozess	Lässt sich im Geschäftsprozess modellieren	✓	✓	X	✓	✓
	Einbindung von Fachexperten	Es ist ersichtlich an welcher Stelle Fachexperten konsultiert werden	X	X	X	X	X
	Dokumentation der Prüfung innerhalb der Modellierungssprache	Durch die Modellierung von Entscheidungen und Einschätzungen sind keine extra Dokumentationen nötig	✓	✓	✓	X	~1
	Leitfragen für Prozess	Unterstützung des Anwenders durch Leitfragen	X	X	✓	X	X
	Meta-Informationen (Dokumentationsziele)	Zusammenfassung der Ergebnisse der Dokumentation	~2	X	X	~3	X
	Modellierung von Prüfschritten	Kerninformationen für einer Verarbeitung werden explizit geprüft	X	~4	✓	X	✓
Legende	✓: Kann durch Modellierungssprache dargestellt werden X: Kann durch Modellierungssprache nicht dargestellt werden ~Zahl: Keine binäre Einteilung möglich, wird im Text näher erläutert						

Abb. 1: Kriterien und Abgleich mit bestehenden Modellierungssprachen

Wie aus Abb. 1 hervorgeht, stellen [CM19] und [WSG21] BPMN-Erweiterungen dar, die die Notation um ausgewählte Aspekte der DS-GVO erweitern. Allerdings bieten sie wenig

[3] Suchstring: “GDPR” AND ((“process” OR “BPMN” OR “ERM” OR “eERM” OR “EPC” OR “eEPC” OR “S-BPM” OR “UML” OR “Flowchart” OR “Model”) AND (“Consent” OR “personal data” OR “lawfulness” OR “legal basis” OR “purpose” OR “storage limitation”))

Unterstützung im eigentlichen Prozess der Dokumentation der datenschutzrechtlichen Kerninformationen ($\sim_2$ und $\sim_3$). [Ag19] modellieren die DS-GVO in BPMN, ohne zusätzliche Notationen einzuführen, wodurch sie leicht in bestehende Geschäftsprozesse integriert werden können. Es fehlt jedoch an ausreichender Dokumentation, und es werden nur wenige Kerninformationen berücksichtigt ($\sim_4$). [BR19] konzentrieren sich ausschließlich darauf, rechtliche Normen in einzelne Workflows zu übertragen. Diese können Fachabteilungen zwar bei der Dokumentation und Bewertung unterstützen, lassen sich jedoch nicht in die konkrete Prozessmodellierungen integrieren. [Ma20] kommen den definierten Kriterien am nächsten. Durch eine umfassende Modellierung der DS-GVO lassen sich alle Kerninformationen überprüfen. Allerdings gestaltet sich die Überführung des bestehenden Geschäftsprozesses in das eigens entworfene IST-Modell als problematisch. Die Unterstützung für die Prüfschritte ist begrenzt und besteht hauptsächlich aus Anleitungen in natürlicher Sprache. Daher wird ein hohes Maß an Modellierungswissen vorausgesetzt, und zusätzliche Dokumentation ist erforderlich ($\sim_1$). Aus dem kriterienbasierten Vergleich wird ersichtlich, dass keine der betrachteten Modellierungssprachen beide Kategorien vollumfänglich abdeckt. Zur Lösung des initial beschriebenen Problems wird demnach eine Modellierungssprache entwickelt. Die zu entwickelnde Modellierungssprache soll die Fachabteilungen dabei unterstützen, die datenschutzrechtlichen Kerninformationen nach einem standardisierten Vorgehen bereits im Zuge der Prozessmodellierung der Geschäftsprozesse zu erheben und zu dokumentieren, um somit die Datenschutzabteilung zu entlasten.

4 Data Protection Process Modelling Language

Im Rahmen der Design- und Entwicklungsphase gemäß [Pe07] wurde die Data Protection Process Modelling Language (DPPML) entwickelt. Diese Sprache ermöglicht es Fachkräfte, die über begrenzte Datenschutzkenntnisse verfügen, ausgewählte Dokumentationsanforderungen eigenständig zu erfüllen, ohne zunächst den Datenschutzbeauftragten einzubeziehen. Die Grundlage der Modellierungssprache bildet BPMN 2.0. Diese Grundlage wurde durch die Einführung weiterer Elemente und Darstellungsmöglichkeiten erweitert, welche aus dem systematischen Literaturreview und der Real-Time Delphi-Studie abgeleitet wurden. DDPML besteht aus drei Bausteinen und kann in andere, bestehende Prozessmodellierungssprachen integriert werden. Ferner besteht die Möglichkeit die Bausteine modular zu verwenden, insofern gewisse Aspekte eigenständig oder anderweitig modelliert werden. Die Abbildung 2 veranschaulicht den ersten Baustein mit integrativem Charakter. Dieser besteht aus drei Symbolen, die in jeder bestehenden Modellierungssprache (hier: BPMN) ergänzt werden können, um den datenschutzrechtlichen Prüfungsbedarf einer Aktivität sowie dessen Status zu kennzeichnen.

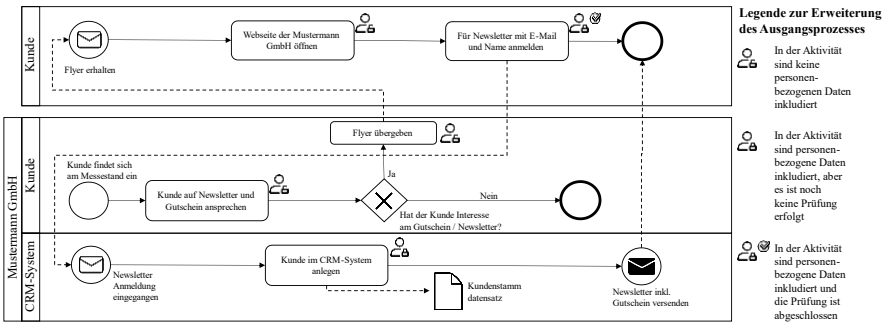

Abb. 2: Der integrative Baustein von DPPML in einem BPMN-Prozess

Der zweite Baustein der DPPML ist ein Informationskasten, in welchem datenschutzrechtliche Aspekte dokumentiert und historisiert werden können. Ferner wird hier der iterative Charakter von DPPML aufgegriffen. So besteht die Option, die relevanten Informationen in Form von eigenständigen Prüfungen für eine Aktivität zu dokumentieren. Der Informationskasten unterstützt dabei die Anforderung der Transparenz gemäß Art. 5 Abs. 1 lit. a DS-GVO und soll die Datenschutzabteilung dabei unterstützen, die Kerninformationen für die Dokumentationspflichten nach Art. 5 Abs. 2 und insbesondere Art. 30 Abs. 1 DS-GVO zu erfassen. Die Abbildung 3 verdeutlicht die aggregierten Informationen, die durch die Fachkräfte ohne Datenschutzexpertise für zwei exemplarische Aktivitäten, aus vorangegangenem Prozessbeispiel, dokumentiert wurden.

Datenschutzrechtliche Kerninformationen	
1. Iteration	**2. Iteration**
Kategorien personenbezogener Daten: Stammdaten, Kontaktdaten, Telekommunikationsdaten	**Kategorien personenbezogener Daten:** Stammdaten, Kontaktdaten, Adressdaten
Rechtmäßigkeit: Art. 6 Abs. 1 S. 1 lit. a DS-GVO	**Rechtmäßigkeit:** Art. 6 Abs. 1 S. 1 lit. a DS-GVO
Zweck: Newsletter-Anmeldung und -versand	**Zweck:** Newsletter-Anmeldung und -versand
Verantwortliche Person: Max Mustermann	**Verantwortliche Person:** Maxine Mustermann
Zeitstempel der Prüfung: 01.02.2023 13:10:34	**Zeitstempel der Prüfung:** 05.02.2023 14:15:36
Prozessschritt: Für Newsletter mit E-Mail und Name anmelden	**Prozessschritt:** Kunde im CRM-System anlegen

Abb. 3: Exemplarische Darstellung des Informationskasten aus Grundlage des Beispielprozesses

Der letzte Baustein von DPPML ist eine eigens entwickelte Modellierungssprache, welche auf grundlegende Elemente von BPMN 2.0 zurückgreift. Dieser Baustein setzt sich aus drei Prüfschritten zur Erfassung der datenschutzrechtlichen Kerninformationen einer Verarbeitung personenbezogener Daten zusammen. In Abbildung 4 werden die Dokumentationsobjekte der Prüfschritte und deren rechtlicher Ursprung dargestellt.

Prüfschritte der DPPML			
Prüfschritte	1. Prüfschritt	2. Prüfschritt	3. Prüfschritt
Dokumentationsobjekt	Personenbezogene Daten	Zweck	Rechtsgrundlage
Rechtliche Grundlage	Art. 5 und 30 DS-GVO	Art. 5 und 30 DS-GVO	Art. 5, 6 und 9 DS-GVO

Abb. 4: Dokumentationsobjekte und rechtliche Ursprung der Prüfschritte

Jeder Prüfschritt der DPPML folgt einem einheitlichen Aufbau. Das Ergebnis eines Prüfschritts stellt die Dokumentation des entsprechenden Dokumentationsobjekts (Personenbezogene Daten, Zweck, Rechtsgrundlage) im Informationskasten dar. Jeder dieser Prüfschritte weist einen iterativen Charakter auf und verfolgt den Grundgedanken der Historisierung von Entscheidungswegen, damit Entscheidungen im Nachgang nachverfolgt und nachvollzogen werden können. Zudem besteht in jedem Prüfschritt die Möglichkeit Begründungen für Entscheidungen zu hinterlegen und an gewissen Stellen bei Bedarf den Datenschutzbeauftragten zu kontaktieren. Entsprechende Elemente der entwickelten Modellierungssprache können der Abbildung 5 entnommen werden.

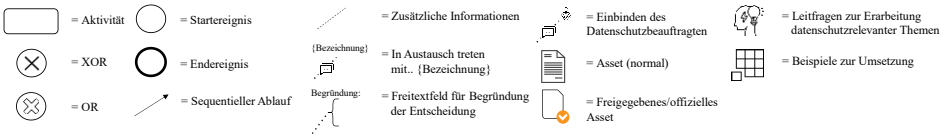

Abb. 5: Legende der DPPML-Prüfschritte

Basierend auf dem in Abbildung 2 vorgestellten Prozessbeispiel für den integrativen Baustein von DPPML in BPMN, wird in Abbildung 6 der dritte Baustein präsentiert. Hierbei wird ein Einblick in eine Teilansicht des ersten Prüfschritts gegeben, in welchem Maxine Mustermann die Aktivität "Kunde im CRM-System anlegen" durchläuft.

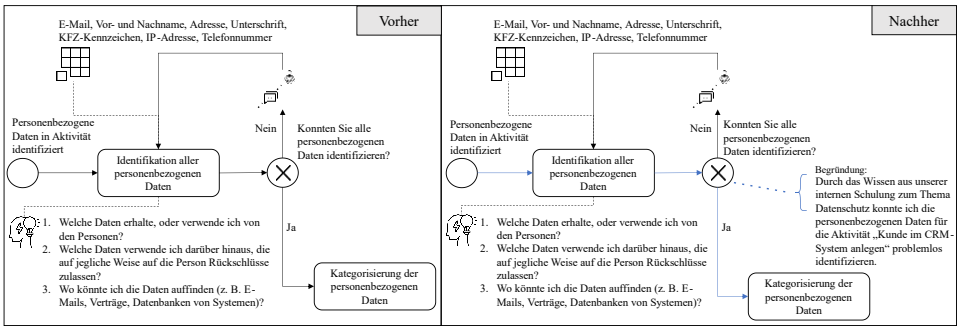

Abb. 6: Teilansicht des ersten Prüfschritts: Kategorisierung personenbezogener Daten

Wie aus Abbildung 6 hervorgeht, wird die modellierende Person, hier Maxine Mustermann, bei der Identifikation der personenbezogenen Daten unterstützt. Diese Unterstützung erfolgt durch Leitfragen und beispielhafte Angaben. Sollte Maxine

Mustermann weiterführende Unterstützung benötigen, besteht die Möglichkeit, den Datenschutzbeauftragten zu kontaktieren. Um eine spätere Nachverfolgung zu ermöglichen, werden die Entscheidungswege von Maxine Mustermann durch eine blaue Hervorhebung gekennzeichnet. Darüber hinaus besteht die Option, die getroffenen Entscheidungen durch entsprechende Begründungen zu unterstützen und zu dokumentieren. Die Ergebnisse dieses Ihrer Prüfung werden im Informationskasten dokumentiert, welcher bereits in Abbildung 3 vorgestellt wurde. Insgesamt wurde in diesem Kapitel eine Modellierungssprache vorgestellt, welche die Option offeriert, bestehende Prozessmodellierungen, um Symbole und Informationen zu ergänzen, die Aufschluss über den datenschutzrechtlichen Prüfungsbedarf einer Aktivität geben (Baustein 1 und 2). Gleichzeitig wurden exemplarisch drei Prüfschritte vorgeschlagen, die von Fachkräften ohne Datenschutzexpertise im Sinne der Unterstützung eingesetzt werden können, um die datenschutzrechtlichen Informationen zu erfassen (Baustein 3). Diese Prüfschritte sind dabei so konzipiert, dass sie von dem jeweiligen Datenschutzbeauftragen adaptiert werden können. Darüber hinaus dienen die Prüfschritte gleichzeitig als Dokumentation und können auch mehrere Iterationen von Entscheidungsprozessen abbilden, deren Ergebnisse im Informationskasten (Baustein 2) festgehalten werden.

5 Evaluation

Zur explorativen Evaluation der Verständlichkeit von DPPML wurde eine Untersuchung unter Anwendung der Think-Aloud-Methode durchgeführt. Die Teilnehmenden bestanden aus Fachkräften aus der Wirtschaft ohne spezialisierte Datenschutzexpertise (n=3), die zuvor nicht an der Delphi-Studie teilgenommen hatten. Diese Teilnehmerauswahl erfolgte in Übereinstimmung mit dem Ziel von DPPML, insb. Fachkräfte ohne tiefgehende Datenschutzkenntnisse in der beruflichen Praxis zu unterstützen. Hierbei wurde sich für die Evaluation an der Vorgehensweise von [GW04] orientiert. Hierdurch werden die Phasen der Demonstration und Evaluation nach [Pe07] umgesetzt. Im Rahmen der Durchführung der Think-Aloud-Methode wurde den Fachkräften die Bausteine von DPPML anhand eines einfachen Szenarios gezeigt. Auf eine inhaltliche Einführung der Probanden wurde verzichtet. Während der Durchführung der Think-Aloud-Methode wurden die Probanden gebeten, die einzelnen Bausteine und Prüfschritte zu betrachten und ihre Gedanken zu diesen Bestandteilen zu artikulieren. Um eine Auswertung der Transkripte in einer einfachen, visuellen Form zu ermöglichen, wird nachstehend die Bewertung der Aussagen der Probanden hinsichtlich der für die Aufgaben definierten Ziele in einer tabellarischen Form in Abbildung 7 dargestellt. Ein „X“ bedeutet dabei, dass die Person das Ziel der Aufgabenstellung nach Ansicht der Autorenschaft verstanden hat. Eine Tilde (~) wird gesetzt, sofern aus den Transkripten hervorgeht, dass die teilnehmende Person zumindest teilweise das Ziel der Aufgabenstellung verstanden hat. Wird kein Symbol gesetzt, geht aus der Antwort der teilnehmenden Person nicht die richtige Intention hervor.

Art der Frage	Ziel der Fragestellung	1. Proband	2. Proband	3. Proband
Allgemeine Fragen	Grundlegende Einordnung des Themenbereichs	~	X	X
	Verständnis der Aufteilung in initiale Modellierung und Prüfschritte		X	X
	Verbindung zwischen Prüfschritten und Prozessmodellierung (iterativ)	X	X	~
1. Prüfschritt – Kategorisierung personenbezogener Daten	Prüfen der Verständlichkeit (Zweck und Ablauf) des ersten Prüfschritts	X	X	~
2. Prüfschritt – Bestimmung des Zwecks	Prüfen der Verständlichkeit (Zweck und Ablauf) des zweiten Prüfschritts	X	X	X
3. Prüfschritt – Bestimmung der Rechtsgrundlage	Prüfen der Verständlichkeit (Zweck und Ablauf) des dritten Prüfschritts	~	X	~

Abb. 7: Ergebnisse der Think-Aloud-Methode hinsichtlich der definierten Ziele

Allgemein geht aus der Sichtung der Transkripte hervor, dass das Modell größtenteils verständlich für die Teilnehmenden war und somit die Modellinterpretation nach [GW04] als effektiv zu bewerten ist. Es wird jedoch auch deutlich, dass bei der initialen Einordnung der Modellierungssprache und den Zusammenhängen zwischen den verschiedenen Bestandteilen Verständnisprobleme auftreten. Diese manifestieren sich vor allem in der Unklarheit der Teilnehmenden bezüglich der Verbindung und Unterschiede zwischen den über- und untergeordneten Prozessebenen, wie aus Äußerungen wie „Ist das da unten der gleiche Prozess?“ oder „oben sieht es eher nach einem Beispielprozess aus und unten scheint es ein bisschen mehr ins Detail zu gehen“ hervorgeht (1. Proband). Wie bereits zuvor beschrieben, wurde im Rahmen der Durchführung der Think-Aloud-Methode auf eine inhaltliche Einführung der Teilnehmenden verzichtet. Dies könnte ein weiterer Faktor sein, welcher sich auf das initiale Verständnis auswirkt. Aus den Antworten der Teilnehmenden zu den Prüfschritten wird ersichtlich, dass die Teilnehmenden die Prüfschritte nicht vollständig durchlaufen, sondern vielmehr die Prüfschritte in Gänze betrachtet haben. Dabei wurden insbesondere die farblichen Hervorhebungen sowie die bisher unbekannten Symbole der Modellierung angesprochen. Die explorative Evaluation zeigt ein grundlegendes Verständnis der Prüfschritte und der weiteren Bausteine von DPPML. Zukünftige Evaluationen in der Verwaltung erfordern eine Einführung in die Modellierung und an den Kontext angepasste Prüfschritte durch Datenschutzbeauftragte, um das Verständnis bei Fachkräften ohne Datenschutzexpertise zu verbessern.

6 Fazit und Ausblick

Im Rahmen dieses Beitrages wurde sich mit der Frage beschäftigt, wie eine Modellierungssprache zu gestalten ist, um Fachkräfte ohne Datenschutzexpertise bei der Erfassung der Kerninformationen einer Verarbeitung im Sinne der DS-GVO zu unterstützen. Diese Frage resultierte aus einer durchgeführten Real-Time Delphi-Studie, welche aufzeigte, dass die beschriebene Aufgabe auch in der aktuellen Zeit noch eine Herausforderung in der Praxis darstellt. Im Sinne einer systematischen Erarbeitung einer Lösung für dieses Problem in Form einer Modellierungssprache, wurde zunächst auf

Grundlage eines Literaturreviews und den Anforderungen der DS-GVO ein Kriterienkatalog definiert. Diese Kriterien dienten als Werkzeug, um zu untersuchen, ob bereits bestehende Modellierungssprachen aus der Literatur eine Lösung darstellen können. Auf Grund der fehlenden Vollständigkeit dieser Lösungen in Hinblick auf den definierten Kriterienkatalog wurde auf dessen Grundlage eine eigene Modellierungssprache entwickelt und im Sinne der Verständlichkeit im Rahmen einer explorativen Evaluation der Modellinterpretation näher untersucht. Auch wenn die Anforderungen der DS-GVO im Hinblick auf das betrachtete Thema für den öffentlichen- und nicht-öffentlichen Sektor ähnlich sind, so bietet es sich zukünftig an, eine weitere Evaluation der Modellierungssprache in einer Verwaltung mit einem größeren Personenkreis durchzuführen. Jedoch ging aus dieser Evaluation hervor, dass DPPML als verständlich zu bewerten ist. Es wird dennoch deutlich, dass auf Grund der Komplexität des Datenschutzes ein Grundverständnis für die Thematik vorliegen muss, damit die Inhalte verstanden werden können. Ferner geht aus der Evaluation hervor, dass in Zukunft semantische Anpassungen vorgenommen werden können, um die Verständlichkeit der Modellierungssprache zu verbessern, indem Textbestandteile reduziert und die Zusammenhänge der einzelnen Bausteine stärker verdeutlicht werden. Weiteres Potential für eine Weiterentwicklung der DPPML ergibt sich aus dem bislang noch nicht erfüllten Kriterium der Dokumentation der Aufbewahrungsfristen personenbezogener Daten. Insgesamt wird deutlich, dass DPPML dazu beitragen kann, Laien im Bereich des Datenschutzes bei der Dokumentation von rechtlichen Anforderungen zu unterstützen. Zukünftig könnte DPPML somit im öffentlichen und nicht-öffentlichen Sektor dazu beitragen, die komplexen Dokumentationspflichten gemäß den Vorgaben der DS-GVO einfacherer zu realisieren und somit Kosten und Zeit einsparen. Die Befähigung von Datenschutz-Laien zur selbstständigen Prüfung der spezifischen Aktivitäten oder Prozesse stellt dabei eine wesentliche Herausforderung dar, bei welcher DPPML versucht, zu unterstützen. Wie aus den Limitationen dieser Ausarbeitung hervorgeht, ist die Modellierungssprache dabei in einem funktionalen Zustand, weist jedoch noch Potential für Verbesserungen durch weitere Entwicklungs- und Evaluationszyklen auf.

Literaturverzeichnis

[Ag19] Agostinelli, S. et.al.: Achieving GDPR Compliance of BPMN Process Models. In (Cappiello, C.; Ruiz, M. Hrsg.): Information Systems Engineering in Responsible Information Systems, Rom 2019. Springer, Cham, S. 10-22, 2019.

[Br09] Vom Brocke, J. et.al.: Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. In (Newell, S.; Whitley, E. A.; Pouloudi, N.; Wareham, J.; Mathiassen, L. Hrsg.): 17th European Conference on Information Systems, Verona 2009. ECIS Proceedings 2009.

[Br18] Brüggemann, S.: Art. 30 Verzeichnis von Verarbeitungstätigkeiten. In (Eßer, M., Kramer, P., von Lewinski, K., Hrsg.): Auernhammer DSGVO BDSG Kommentar, 6. Aufl., Carl Heymanns Verlag, Köln, S. 458-470, 2018.

[BR19] Buchmann, E.; Robak, M.: Deriving Workflow Privacy Patterns from Legal Documents. In: Federated Conference on Computer Science and Information Systems (FedCSIS), Leipzig, 2019. IEEE, S. 555-563, 2019.

[CM19] Capodieci, A.; Mainetti, L.: Business process awareness to support GDPR compliance. Proceedings of the 9th International Conference on Information Systems and Technologies, S. 1-6, 2019.

[Ge19] Gerhold, L.: Real-Time Delphi. In (Niederberger, M.; Renn, O. Hrsg.): Delphi-Verfahren in den Sozial- und Gesundheitswissenschaften. Springer Verlag, Wiesbaden, S. 101-124, 2009.

[GW04] Gemino, A.; Wand, Y.: A framework for empirical evaluation of conceptual modeling techniques. Requirements Engineering 9/4, S. 248-260, 2004.

[Hä09] Häder, M.: Delphi-Befragungen. Ein Arbeitsbuch, 3. Aufl., Springer Verlag, Wiesbaden, 2009.

[Ha23] Harta, L. et.al.: Burdens arising from Art. 30 and 33 of the General Data Protection Regulation. Stiftung Familienunternehmen, München, 2023.

[KEF18] Koc, H.; Eckert, K.; Flaig, D.: Datenschutzgrundverordnung (DSGVO): Bewältigung der Herausforderungen mit Unternehmensarchitekturmanagement (EAM). HMD Praxis der Wirtschaftsinformatik 55/5, S. 942-963, 2018.

[KNW20] Klenk, T.; Nullmeier, F.; Wewer, G.: Handbuch Digitalisierung in Staat und Verwaltung, Springer VS, Wiesbaden, 2020.

[Ma20] Matulevičius, R. et.al.: A Method for Managing GDPR Compliance in Business Processes. In (Herbaut, N.; La Rosa, M. Hrsg.): Advanced Information Systems Engineering, Grenoble, 2020. Springer, Cham, S. 100-112, 2020.

[Mo09] Moher, D. et.al.: Preferred reporting items for systematic reviews and meta-analyses: the PRISMA Statement. Open Medicine 3/3, S. 123-130, 2009.

[NP18] Netzwerk Prozessmanagement, Einführung in das strategische Prozessmanagement der öffentlichen Verwaltung, https://www.verwaltung-innovativ.de/SharedDocs/Publikationen/eGovernment/egov_leitfaden_prozessmanagement.pdf?__blob=publicationFile&v=2, Stand: 12.06.2023.

[Pe07] Peffers, K. et.al.: A Design Science Research Methodology for Information Systems Research. Journal of Management Informations Systems 24/3, S. 45-77, 2007.

[SR09] Schulz, M.; Renn, O.: Das Gruppendelphi. Konzept und Fragebogenkonstruktion, Springer Verlag, Wiesbaden, 2009.

[We22] Weiß, R.: Datenschutz als Herausforderung für die Digitalisierung, https://www.bitkom.org/Bitkom/Publikationen/Datenschutz-als-Herausforderung-fuer-die-Digitalisierung, Stand: 12.06.2023.

[WSG21] Windrich, M.; Speck, A.; Gruschka, N.: Representing Data Protection Aspects in Process Models by Coloring. In (Gruschka, N.; Antunes, L. F. C.; Rannenberg, K.; Drogkaris, P. Hrsg.): 9th Conf. On Privacy Technologies and Policy, Oslo 2021. Springer, Cham, S. 143-155, 2021.