Entwicklung eines Beschreibungsschemas für Workflow Privacy Patterns

Alexandra Janssen[1], Franziska Plate[1], Dominik Schneider[1], Erik Buchmann[2] und Jürgen Anke[2]

[1] Detecon International GmbH, Sternengasse 14-16, 50676 Köln
{Alexandra.Janssen, Franziska.Plate, Dominik.Schneider}@detecon.com

[2] Hochschule für Telekommunikation Leipzig, Gustav-Freytag-Straße 43-45, 04277 Leipzig
{buchmann, anke}@hft-leipzig.de

Abstract. Aufgrund der Digitalisierung von Geschäftsprozessen werden immer mehr personenbezogene Daten von computergestützten Informationssystemen erfasst, gespeichert und verarbeitet. Deshalb steigen die Anforderungen an Unternehmen bezüglich der Umsetzung von Datenschutzregelungen. Workflow Privacy Patterns (WPP) haben das Potenzial, Unternehmen bei dieser Aufgabe zu unterstützen. WPPs sind abstrakte, validierte Prozessmuster, die Prozessentwicklern, Datenschutzbeauftragten oder Auditoren bei der Modellierung, Implementierung oder Prüfung von Prozessen in Hinblick auf wiederkehrende Datenschutzprobleme helfen sollen. In diesem Beitrag wird ein Beschreibungsschema für WPPs vorgeschlagen, das als Grundlage für WPP-Modellierungen und zum Vergleich von WPPs genutzt werden kann. Weiterhin wird die Anwendbarkeit des Beschreibungsschemas anhand eines konkreten WPPs veranschaulicht, diskutiert und bewertet.

Keywords: Workflow Privacy Pattern, Beschreibungsschema, Datenschutz in Geschäftsprozessen, Prozessmodellierung, EU-DSGVO.

1 Einleitung

Für große Unternehmen wird es immer aufwändiger, die Anforderungen von Datenschutzgesetzen wie dem Bundesdatenschutzgesetz (BDSG) [1], der neuen EU-Datenschutzgrundverordnung (EU-DSGVO) [2] oder unternehmensbezogenen Compliance-Vorschriften zu erfüllen. Das liegt unter anderem daran, dass rasante Entwicklungen im Bereich der Informations- und Kommunikationstechnologien neue Möglichkeiten zur Digitalisierung von Geschäftsprozessen bieten [3].

Unternehmen, die personenbezogene Daten elektronisch erfassen, speichern und verarbeiten, müssen sicherstellen, dass die Vorgaben aus Datenschutzgesetzen und Datenschutzrichtlinien in Geschäftsprozessen eingehalten werden. Dafür entwickelte Werkzeuge wie Privacy Management-Systeme [4] helfen Unternehmen bei der Überprüfung und Realisierung des Datenschutzes bzw. der Datenschutzrichtlinien [5]. Sie setzen jedoch zumeist erst nach der Umsetzung von Datenschutz-kritischen

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Anwendungen oder Prozessen an. Die Entwicklung von Geschäftsprozessen unter Berücksichtigung des Datenschutzes ist weiterhin mit viel manueller Arbeit für Datenschutzbeauftragte, Prozessentwickler oder Auditoren verbunden.

Unser zentrales Anliegen besteht darin, dass wir den Prozessentwickler dabei unterstützen wollen, bestimmte Datenschutzkonzepte in Geschäftsprozessen einfach umzusetzen und den Analysten dazu befähigen wollen, existierende Geschäftsprozesse auf die Umsetzung dieser Datenschutzkonzepte zu prüfen. In einer Vorarbeit haben wir dazu Workflow Privacy Patterns (WPP) [6] vorgestellt. Analog zu den Design Patterns im Software Engineering sollen WPPs die Modellierung von wiederkehrenden Datenschutzproblemen in Form von standardisierten, validierbaren Prozessmustern erlauben. Ein Beispiel ist das Pattern „Anonyme Dienstnutzung“ (Abbildung 1). Hierbei kann der Aufruf eines bestimmten Services (z.B. Startseite eines Nachrichtenportals oder Hotelbuchungssystems) entweder personalisiert oder anonym angezeigt werden. Im personalisierten Fall werden personenbezogene Daten erhoben und für die Vorbereitung der Diensterbringung verwendet.

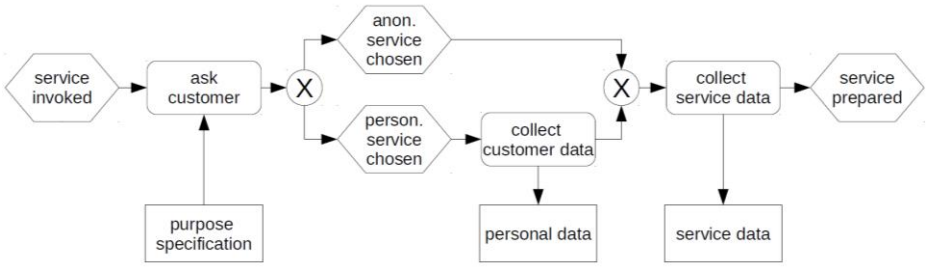

Abbildung 1: WPP für die optional anonyme Nutzung eines Service [6]

Das WPP in Abbildung 1 zeigt, dass für eine datenschutzkonforme Modellierung die Reihenfolge eine wesentliche Rolle spielt, z.B. die Bekanntgabe des Erhebungszwecks vor der Entscheidung für oder gegen eine personalisierte Dienstnutzung oder die Erfassung von personenbezogene Daten erst nach der Entscheidung für eine personalisierte Nutzung. Weitere offensichtlich wichtige Modellbestandteile sind das Vorhandensein von speziellen Datenobjekten, die gesetzliche Eigenschaften erfüllen und an ganz bestimmten Stellen im Prozess verankert sein müssen, wie z. B. eine Datenschutzerklärung. Damit ein WPP Datenschutzkonzepte aus Gesetzestexten, Datenschutz-Richtlinien oder Compliance-Vorschriften in Geschäftsprozesse umsetzen kann, darf es darum nicht nur Kontroll- oder Datenflüsse abbilden, sondern muss domänenspezifische Aspekte des Datenschutzes berücksichtigen.

In diesem Beitrag wird ein Beschreibungsschema entwickelt, das alle erforderlichen Attribute für die Abbildung von Datenschutzkonzepten auf WPPs enthält. Dies ist eine herausfordernde Aufgabe: WPPs müssen für unterschiedliche Kategorien von Datenschutzkonzepten einsetzbar sein, wie herkömmliche Workflow Pattern auch generische Eigenschaften wie Wiederverwendbarkeit oder Verständlichkeit erfüllen, und darüber hinaus domänenspezifische Eigenschaften des Datenschutzes abbilden können. Wir haben daher ausgehend vom aktuellen Stand der Forschung grundsätzliche

Eigenschaften für WPPs zusammengestellt und auf der Basis von Gesetzestexten Attribute aus der Datenschutzdomäne identifiziert. Daraus ergibt sich ein umfassendes Bild über Eigenschaften und Anforderungen von WPPs, die sich mittels Kategorisierung in ein Beschreibungsschema überführen lassen.

Der Beitrag gliedert sich in fünf Abschnitte. Im nächsten Abschnitt wird der aktuelle Stand der Forschung beschrieben. In Abschnitt 3 werden die Workflow Pattern (WP)-Kategorien als Grundlage für das Beschreibungsschema erläutert. Auf Basis der WP-Kategorien und weiterer Forschung wird in Abschnitt 4 ein Beschreibungsschema vorgeschlagen. Der Beitrag schließt mit einem Fazit und Ausblick.

2 Stand der Forschung

Nachfolgend werden verwandte Arbeiten aus vier Bereichen vorgestellt: (1) Die Umsetzung von Datenschutzkonzepten auf der Ebene der Geschäftsprozess-modellierung, (2) Vorarbeiten zu Workflow Patterns, (3) Vorarbeiten zur Spezifikation von Workflow Privacy Patterns sowie (4) allgemeine Ansätze zur Ableitung von domänenspezifischen Workflow Patterns.

2.1 Berücksichtigung von Datenschutz in Geschäftsprozessen

Datenschutzaspekte in Geschäftsprozessen werden bereits seit mehr als zehn Jahren in der Literatur diskutiert. So schlägt Lange ein Vorgehensmodell für die Gestaltung vertrauenswürdiger Informationssysteme vor, das sowohl rechtliche als auch unternehmerische Ziele berücksichtigt. Dabei wird der Zusammenhang zwischen Daten-, Regel- und Akteursmodell konzeptionell formuliert [7]. Zur Datenschutzbewertung in kleinen und mittleren Unternehmen stellen Rodeck et al. einen pattern-basierten Ansatz vor, mit dem häufige Prozessmuster als BPMN (Business Process Model and Notation)-Modell gespeichert werden. Diese werden zur Identifikation von Schwachstellen sowie deren Dokumentation in einem Tool genutzt [8].

Ein Ansatz von Karjoth widmet sich der Frage von maschinenlesbaren Datenschutzrichtlinien zur Sicherstellung von Datenschutzkonformität in Geschäftsprozessen. Dazu werden Prozessmodelle mit datenschutzrelevanten Aspekten annotiert. Zentral ist hier die Verknüpfung von Zwecken und Aufgaben („Tasks“). Durch die formale Beschreibung von Datenschutzrichtlinien können sie automatisch mit den Eigenschaften des Prozesses verglichen werden [9]. Ein weiteres Konzept für die Formulierung und Durchsetzung von Datenschutzanforderungen sind „purpose-aware policies“ [10]. Diese beschreiben formal den Zusammenhang von Zwecken, verantwortlichen Stellen, Daten sowie den zulässigen Aktionen auf diesen. Der Vorteil der formalen Beschreibung liegt in der Prüfbarkeit der Einhaltung (bei Verfügbarkeit entsprechender Daten).

2.2 Workflow Patterns

Patterns beschreiben generische Lösungen für teilweise wiederkehrende, nichttriviale Probleme [11], die in einem spezifischen Entwicklungskontext entstehen [12]. Bei Workflow Patterns bilden die betrieblichen Abläufe [13] diesen Kontext.

Allgemein werden Patterns beschrieben durch Bedingungen für die Anwendbarkeit des Patterns, konkrete Anwendungsszenarien, ggf. Probleme bei der Instanziierung des Patterns in existierenden Modellierungssprachen sowie die implementierbaren Lösungen selbst [11]. Aufgrund der verschiedenen Anwendungsbereiche werden WPs in vier Perspektiven eingeteilt. So sind nach [14] die Perspektiven Daten, Ressourcen, Kontrollfluss und Exception-Handling (Behandlung von Fehlerzuständen) definiert.

Kontrollfluss-Patterns beschreiben alle Aspekte und Abhängigkeiten von Flussobjekten. Flussobjekte bezeichnen in der BPMN-Notation Aktivitäten eines Prozesses bzw. Prozessschritte. Ein Beispiel für diese Kategorie ist ein WP, das regelt, wie eine Parallelisierung von Prozessschritten sowie deren Synchronisation modelliert werden. Daten-Patterns fokussieren sich auf die Beschreibung von Informationsaustauschen und den dazugehörigen Daten, die in Geschäftsprozessen vorkommen [15]. Daten treten in Geschäftsprozessen auf unterschiedliche Weise auf. Sie können unter anderem den Kontrollfluss verändern, von Komponenten im Prozessablauf verarbeitet werden oder einen Datenaustausch zwischen Komponenten ermöglichen [14]. Mithilfe von Ressourcen-Patterns kann die Aufgabenverteilung in Geschäftsprozessen geregelt werden [15]. Dazu werden Ressourcen-Objekte, z. B. Arbeitskräfte oder Organisationseinheiten, zu Prozess-Komponenten zugeordnet. Exception-Handling-Patterns basieren auf den drei anderen Perspektiven, während Kontrollfluss-, Daten- und Ressourcen-Patterns kaum zusammenhängen [15]. Exception-Handling-Patterns definieren, wie verschiedene Ausnahmesituationen in den einzelnen Perspektiven gehandhabt werden und welche Maßnahmen darauf erfolgen müssen. Sie geben zum Beispiel Auskunft darüber, welche Maßnahmen nach einem Ausnahmefall eingeleitet werden müssen, um diesen zu beheben [15].

2.3 Workflow Privacy Patterns

Workflow Privacy Patterns [6], wie das in Abbildung 1 dargestellte, spezifizieren eine generische, wiederverwendbare Lösung zu einem mehrfach auftretenden Problem in der Datenschutz-Domäne in Form eines Workflow Patterns.

WPPs lassen sich in drei Kategorien einteilen, die sich nach der Art und Weise der Datenschutz-Umsetzung in Geschäftsprozessen unterscheiden. „Privacy Patterns“ beschreiben Bausteine für Datenschutz-Prozesse, z.B. die Implementierung eines Auskunftsersuchens [6]. „Crosscutting Privacy Patterns“ definieren Patterns, die innerhalb der Geschäftsprozesse eines Unternehmens übergreifend Anwendung finden, beispielsweise um zu validieren, ob eine bestimmte Datennutzung vom Betroffenen autorisiert wurde. „Meta Privacy Patterns“ bilden übergeordnete Konzepte wie „Separation of Duties“ oder „Separation of Concerns“ auf Patterns ab.

WPPs finden bei Prozessmodellierern nur dann Akzeptanz, wenn sie einen klaren Vorteil gegenüber der manuellen Prozessmodellierung bieten. In [6] werden dafür drei wesentliche Anforderungen an WPPs definiert:

A1: *WPPs sollen keine Modifizierungen der Modellierungssprache erfordern.*
A2: *WPPs sollen für Prozessmodellierung als auch für Implementierung nützlich sein.*
A3: *WPPs sollen separat vom eigentlichen Geschäftsprozess entwickelt und gepflegt werden können.*

2.4 Ableitung von domänenspezifischen Patterns

Das Erstellen von WPs für konkrete Anwendungsdomänen ist schwierig, da an Patterns hohe Erwartungen gestellt werden: Sie sollen nützlich, verständlich, wiederverwendbar, in unterschiedliche Sprachen transformierbar, verifizierbar usw. sein.

Ein Bottom-Up-Ansatz [16] zur Entwicklung von Patterns besteht darin, dass aus einer Grundgesamtheit von Workflow-Instanzen jeweils wiederkehrende Muster in einem manuellen Prozess herausextrahiert werden, beginnend bei einfachen Patterns. Die Korrektheit der Patterns hängt hier von der Korrektheit der Workflow-Instanzen ab, die Zahl der identifizierten Patterns von der Erfahrung des Prozessentwicklers.

Alternativ ist auch ein Top-Down-Ansatz [13] zur Gewinnung von Patterns möglich. Dabei wird zunächst ein abstraktes Referenzmodell aufgestellt, in dem die Prozessschritte als generische Aktivitäten repräsentiert werden. In einem weiteren Schritt werden dann domänenspezifische Aspekte, Zustandsübergänge etc. zu den Aktivitäten hinzugefügt. Zuletzt werden die generischen Aktivitäten des abstrakten Referenzmodells im gewünschten Detaillierungsgrad verfeinert. Dabei lassen sich auch Design-Alternativen als unterschiedliche Workflow Patterns in die Verfeinerungen integrieren. Die gewonnenen Patterns sind korrekt, wenn das finale Referenzmodell, das diese Patterns enthält, korrekt ist.

In Bezug auf die Entwicklung von Workflow Privacy Patterns hat die unmittelbare Anwendung dieser beiden Ansätze den Nachteil, dass der wesentliche Zweck der Patterns nicht explizit berücksichtigt wird: Die korrekte Umsetzung von gesetzlichen Vorgaben in Geschäftsprozessen oder die Validierung, dass bestimmte Geschäftsprozesse gesetzeskonform umgesetzt wurden. Wir haben daher analysiert, welche domänenspezifischen Attribute in der Datenschutzgesetzgebung Anwendung finden, und aus diesen ein datenschutz-spezifisches Beschreibungsschema für Workflow Privacy Patterns entwickelt, das sich sowohl Top-Down als auch Bottom-Up zur Definition von Patterns eignet.

3 Entwicklung des Schemas zur Beschreibung von WPPs

Die Entwicklung unseres Beschreibungsschemas für WPPs folgt dem gestaltungsorientierten Forschungsparadigma [17]: (1) Beschreibung der Problemdomäne Datenschutz in Geschäftsprozessen, (2) Entwicklung und Beschreibung des Beschreibungsschemas und (3) Einsatz des Beschreibungsschemas anhand der Entwicklung eines konkreten WPPs mit anschließender Untersuchung von dessen Anwendbarkeit.

Wir beginnen mit der Identifizierung relevanter Attribute zum Zweck der Unterstützung von Entwicklern bei der Implementierung von Datenschutz in Geschäftsprozessen. Dabei ist es wichtig, diejenigen Attribute zu identifizieren, die für eine eigenständige Konzipierung eines WPPs notwendig sind, um Anforderung A3 zu erfüllen. Dazu gehört auch, dass durch die Nutzung des Beschreibungsschemas durch den Entwickler keine anderen Quellen mehr benötigt werden, um das WPP zu implementieren. Das Beschreibungsschema soll als Grundlage für eine Modellierung dienen, wobei die Auswahl der Modellierungssprache einen nachgeordneten Schritt darstellt. Insofern wird Anforderung A1 an dieser Stelle nicht weiter berücksichtigt.

Aus der Themensicht ergeben sich im Hinblick auf den Zweck und die Nutzung des Beschreibungsschemas zwei Aspekte: der Prozess-Aspekt, der sich mit den Eigenschaften eines komplexen WPs beschäftigt, und der Datenschutz-Aspekt, in den Datenschutz-relevante Zusatzinformationen fallen. Ein Überblick über sämtliche im Folgenden erläuterte Attribute ist der Tabelle 1 zu entnehmen.

Tabelle 1. Attributsammlung für WPPs nach Themensicht

Prozess-Aspekt		*Datenschutz-Aspekt*	
1	Daten	9	Paragraph
2	Ressourcen	10	WPP-Kategorie
3	Kontrollfluss	11	Nutzungsvorschrift
4	Exception-Handling	12	Auswirkungen auf andere WPPs
5	Anwendungsvoraussetzungen	13	Auswirkungen durch andere WPPs
6	Betroffene Prozesse	14	Technische Voraussetzungen
7	Einsatzstelle	15	Optionale Bestandteile
8	Interaktion mit anderen Prozessen	16	Ausnahmeregelungen
		17	Modifikationsbedarf

Für den Prozess-Aspekt lassen sich die folgenden Attribute eines WPPs aus den Vorarbeiten zu WPs identifizieren: Zum einen gibt es die vier WP-Kategorien (1-4), auf denen WPPs u.a. basieren. Weiterhin sind Situationen oder Handlungen (5) zur Durchführung von WPPs relevant, die gegeben sein müssen, damit das WPP gestartet werden kann. Ausgehend davon werden Informationen darüber benötigt, in welche Prozesse (6) das Pattern eingesetzt werden kann. Im Zusammenhang mit (5) und (6) kann dann die konkrete Einsatzstelle (7) spezifiziert werden, an der das WPP in einen Prozess integriert werden kann. Ein weiteres Attribut beschreibt die Interaktion (8) mit anderen (Sub-) Prozessen oder WPPs.

Für den Datenschutz-Aspekt wurden Paragraphen aus dem Bundesdatenschutzgesetz [1] und der EU-Datenschutzgrundverordnung [2] analysiert, um daraus Attribute zu identifizieren. So finden sich im Aspekt Datenschutz Attribute wie die dem WPP zugrundeliegenden Paragraphen (9) des Gesetzestextes. Ebenfalls ist eine Einordnung des WPPs in eine der drei bereits genannten WPP-Perspektiven (10) hilfreich. Eine weitere Information ist, wann die betreffende Regelung zwingend anzuwenden ist (11). Diese Information kann relevant sein, da bestehende Gesetze zum Datenschutz durch andere ersetzt oder ergänzt werden können (z.B. Anwendung der EU-DSGVO ab 25. Mai 2018). Unter Umständen gibt es andere Prozesse oder WPPs,

die sich auf das vorliegende WPP auswirken oder es einschränken (12). Diese Auswirkungen können ebenso umgekehrt (13) vorhanden sein. Ein weiteres WPP-Attribut betrifft die technischen Anforderungen (14), die erfüllt sein müssen, um das WPP ausführen zu können. Ein WPP kann abhängig vom Inhalt des betreffenden Paragraphen optionale Bestandteile (15) haben. Der Anwender besitzt dadurch die Entscheidungsfreiheit, ob er das WPP mit oder ohne diese optionalen Bestandteile umsetzt. Es ist wichtig, Ausnahmeregelungen mitaufzuführen, in denen das Pattern nicht oder anders angewendet wird (16). Der letzte Punkt ist der Modifikationsbedarf (17). Er dokumentiert den Fall, dass das WPP eine abstrakte Rechtsvorschrift ggf. in modifizierter Form abbilden muss, um abstrakte Rechtsbegriffe in konkrete Modellierungen zu überführen.

Anhand der Themensicht lassen sich die einzelnen Attribute zwar gut identifizieren und festhalten, jedoch wird dabei Anforderung 2 für WPPs nicht berücksichtigt. Die jeweils notwendigen Informationen für die Implementierung und die Modellierung sind als solche nicht klar erkennbar oder zuzuordnen. Deshalb empfiehlt sich für das Beschreibungsschema eine Anwendungssicht, die die Attribute Aspekten zuordnet, die für jeweils unterschiedliche Anwendungen eines WPPs sinnvoll sind.

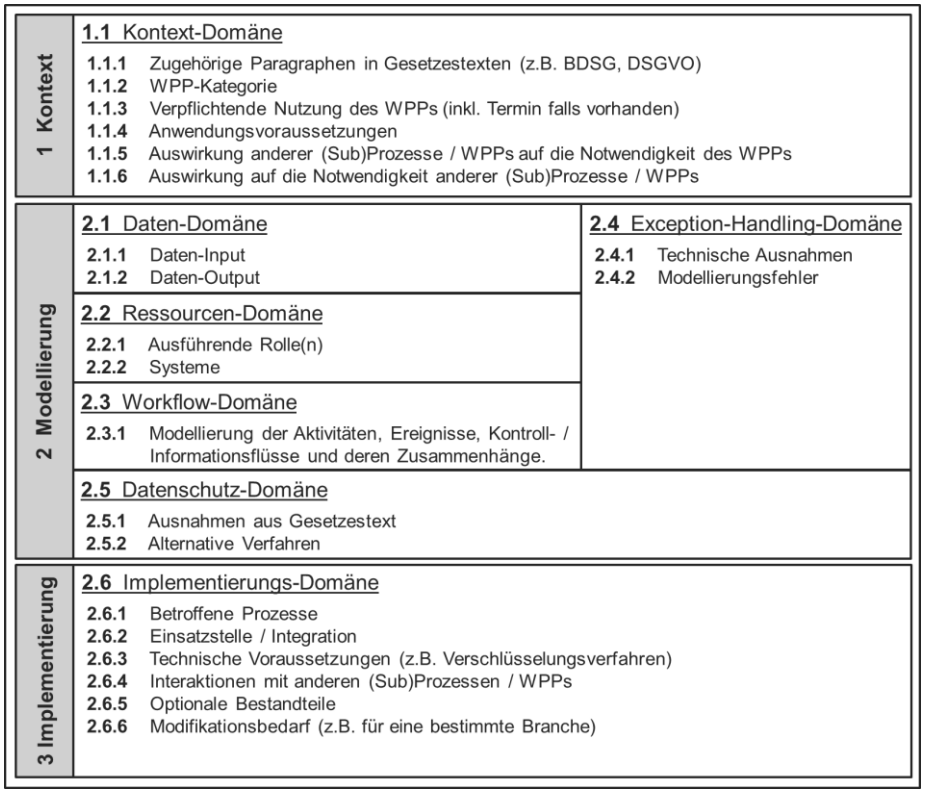

Abbildung 2. Beschreibungsschema für Workflow Privacy Patterns

Um ein WPP als solches identifizieren und darauf referenzieren zu können sind verschiedene Kontextinformationen (5, 9-13) erforderlich. Daraus ergibt sich die Kontext-Domäne, die dem Kontext-Aspekt zuzuordnen ist. Neben diesem Aspekt wird weiterhin eine Aufteilung der WPP-Attribute in zwei weitere Aspekte benötigt, die sich auf die Modellierung und die Implementierung fokussieren. Zum Aspekt „Modellierung" gehören die vier WP-Perspektiven (1-4) als eigenständige Domänen mit ihren Attributen, sowie eine spezielle Datenschutzdomäne, die sich mit den Ausnahmeregelungen (16) beschäftigt. Im Aspekt „Implementierung" befindet sich die Implementierungs-Domäne, die sämtliche Attribute (6-8, 14-15, 17) beinhaltet, um das WPP Ende-zu-Ende in einen Prozess integrieren zu können. Daraus ergibt sich ein umfassendes Schema, das in Abbildung 2 dargestellt ist. Über die aufgeführten Bereiche hinaus sind weitere Attribute aus anderen Domänen denkbar, die das Bild eines WPP vervollständigen. In diesem Beitrag wurde jedoch der Fokus auf die Anforderungen eines Entwicklers gelegt um ihm mit dem Beschreibungsschema ein nützliches Werkzeug zur Umsetzung von Datenschutz in Geschäftsprozessen zu bieten. Aus diesem Grund werden Domänen bzw. Attribute, die über diesen Zweck hinausgehen, an dieser Stelle nicht berücksichtigt.

4 Einsatz des Beschreibungsschemas

4.1 Anwendung des Beschreibungsschemas auf § 33 BDSG

Das Beschreibungsschema wurde in Tabelle 2 überführt und auf § 33 BDSG *[18]* angewendet, um die Anwendbarkeit des Schemas zu demonstrieren. § 33 BDSG beinhaltet Regelungen zur Benachrichtigung eines Betroffenen bei der Speicherung personenbezogener Daten und entspricht einem Crosscutting Privacy Pattern:

„Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen. Werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. Der Betroffene ist in den Fällen der Sätze 1 und 2 auch über die Kategorien von Empfängern zu unterrichten, soweit er nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss." [18]

Zunächst wurde die Tabelle anhand des Schemas erstellt und mit den identifizierten und abgeleiteten Informationen aus § 33 BDSG befüllt. Dafür wurde der Detaillierungsgrad des BDSG übernommen. Wie in der Tabelle 2 zu sehen ist, konnte nicht jeder Prüfaspekt des Beschreibungsschemas ausgefüllt werden. Tabelle 2 hilft dem Modellierer dabei, einen Überblick über das WPP zu erhalten und alle notwendigen Informationen zu identifizieren und zu strukturieren. Anhand der Attribute können die Informationen aus den zugrundeliegenden Paragraphen abgeleitet

werden. Hier wurde ein Paragraph ausgewählt und entlang der Domänen die dazugehörigen WPP-Eigenschaften ermittelt. Dadurch wurde ersichtlich, ob andere Paragraphen Einfluss auf das WPP haben. Diese Angaben sind für die Modellierung dieser Rechtsnorm ausreichend.

Tabelle 2. Anwendung des Schemas auf das WPP „Benachrichtigung des Betroffenen“

Domäne		*Attribut*	*Anwendung auf „Benachrichtigung des Betroffenen“*
1 Kontext	1.1	1.1.1	§ 33 BDSG
		1.1.2	Crosscutting Privacy Pattern
		1.1.3	Die Nutzung des WPPs ist verpflichtend, sobald personenbezogene Daten gespeichert werden.
		1.1.4	Speicherung personenbezogener Daten
		1.1.5	§ 29 BDSG
		1.1.6	Nicht definiert
2 Modellierung	2.1	2.1.2	Nicht definiert
		2.1.2	Benachrichtigung an den Betroffenen
	2.2	2.2.1	Die Organisationseinheit, die verantwortlich für die Speicherung der personenbezogenen Daten des Betroffenen ist: "Verantwortliche Stelle" (§ 33 BDSG).
		2.2.2	Nicht definiert
	2.3	2.3.1	Aktivitäten / Subprozesse: Erstmaligkeit der Speicherung prüfen, Ausnahmeregelungen prüfen, Zweck der Speicherung ermitteln, Betroffenen benachrichtigen. Gateways/Konnektoren: XOR bei Anti- oder Kontravalenz (positives oder negatives Prüfergebnis), OR bei Disjunktion je nach Ermittlungsergebnis: Eigene Zwecke (A), Zweck der Übermittlung (B). Ereignisse: Personenbezogene Daten werden gespeichert (Start), Betroffener ist benachrichtigt (Ende), Pflicht zur Benachrichtigung besteht nicht (Ende). Kontrollflüsse: Zwischen allen Aktivitäten bzw. Subprozessen, Ereignissen und Gateways.
	2.3	2.3.1	Anmerkungen zu "Betroffenen benachrichtigen" bei Ermittlungsergebnis A: von der Speicherung, Art der Daten, Erhebungszweck, Verarbeitung/-Nutzung, Identität der verantwortlichen Stelle, ggf. Empfängerkategorien. Anmerkungen zu "Betroffenen benachrichtigen" bei Ermittlungsergebnis B: von der erstmaligen Übermittlung, Art der Daten, ggf. Empfängerkategorien.
	2.4	2.4.1	Nicht definiert
		2.4.2	Nicht definiert
	2.5	2.5.1	§ 33 Absatz 2 Artikel 1 bis 9
		2.5.2	Der Eintritt einer der Ausnahmen § 33 Absatz 2 Artikel 1 bis 9 führt zum Ende des WPPs, also zur Abbruch-

			bedingung "Keine Benachrichtigung des Betroffenen notwendig".
3 Implementierung	3.1	3.1.1	Betroffen ist jeder Prozess, in dem personenbezogene Daten gespeichert werden.
		3.1.2	Vorhergehende Aktivität im Prozess: Speicherung personenbezogener Daten
		3.1.3	Nicht definiert
		3.1.4	Nicht definiert
		3.1.5	Nicht definiert
		3.1.6	Kenntnis des Betroffenen prüfen, Allgemeine Ausnahmefallregelungen prüfen, Zweck der Speicherung prüfen, Ausnahmefallregelungen für Übermittlungszwecke prüfen, Ausnahmefallregelung für eigene Zwecke prüfen, Betroffenen benachrichtigen

4.2 Bewertung der Anwendbarkeit des Beschreibungsschemas

In dem Beschreibungsschema existiert eine Sammlung von WPP-Attributen, die nach Kontext, Modellierung und Implementierung strukturiert sind. Wir haben festgestellt, dass hier ein Leitfaden zur Strukturierung von Gesetzestexten bzw. Paragraphen notwendig werden, um eine einheitliche Beschreibung zu gewährleisten.

Wenn Informationen im zugrundeliegenden Paragraphen fehlen oder kontextbedingt irrelevant sind, fehlen Angaben im Beschreibungsschema. Hier scheint eine Kennzeichnung der obligatorischen oder optionalen Attribute sinnvoll.

Durch die Demonstration des Beschreibungsschemas konnte noch keine Aussage über die Generalisierbarkeit des Beschreibungsschemas getroffen werden. Dazu müssen weitere Paragraphen anhand des Beschreibungsschemas strukturiert werden. Insbesondere die Überprüfung für die anderen beiden WPP-Kategorien ist relevant. Ein Beispiel dafür ist die Kategorie der Privacy Processes/Patterns. Bei diesen sind die Attribute 3.1.1 und 3.1.2 per se nicht vorhanden, sodass eine Evaluierung der Handhabung im Rahmen der Nutzung des Beschreibungsschemas notwendig wird.

5 Fazit und Ausblick

Aufgrund der steigenden Anforderungen an die Umsetzung des Datenschutzes in Geschäftsprozessen, wurden WPPs als Unterstützung für Prozessentwickler und Prozessmodellierer identifiziert. Im vorliegenden Beitrag wurde ein Beschreibungsschema erarbeitet, das zur Entwicklung und Vergleichbarkeit von WPPs eingesetzt werden kann. Für eine standardisierte Entwicklung und Modellierung von WPPs bedarf es jedoch noch weiterführender Forschung. Anhand der erkannten Herausforderungen, die sich aus dem bisherigen Entwicklungsstand des Beschreibungsschemas ergeben, lassen sich dafür folgende Themen ableiten:

- *Entwicklung eines objektiven Leitfadens:* Wie können Gesetztestexte standardisiert, strukturiert und in ein Beschreibungsschema überführt werden?
- *Ermittlung der Notwendigkeit aller Attribute:* Welche Attribute sind für welche WPP-Kategorien obligatorisch, optional oder irrelevant?
- *Validierung des Beschreibungsschemas:* Muss das Beschreibungsschema für die Anwendung auf alle Paragraphen aus allen drei WPP-Kategorien modifiziert werden und falls ja - wie?
- *Weiterentwicklung des Beschreibungsschemas:* Welche Domänen sind über die bisher berücksichtigten Domänen hinaus für WPPs relevant und um welche zusätzlichen Attribute sollte das Beschreibungsschema ergänzt werden?

Basierend auf der Entwicklung des Beschreibungsschemas für WPPs und der Diskussion dessen Anwendbarkeit anhand eines Beispiels können zudem folgende Forschungsthemen in Ausblick gestellt werden:

- *Erstellung eines Vorgehensmodells:* Wie können WPPs basierend auf Gesetzestexten und Datenschutzprinzipien nach einem einheitlichen Vorgehen entwickelt und modelliert werden?
- *Erstellung eines Modells zur Integration und Implementierung:* Wie können WPPs in Unternehmen bzw. deren Geschäftsprozesse nach einem einheitlichen Vorgehen integriert und implementiert werden?
- *Detaillierungsgrad:* Welcher Detaillierungsgrad eignet sich für WPPs?
- *Ausnahmeregelungen:* Wie können Subprozesse für die Handhabung von Ausnahmereglungen gestaltet werden und welchen Grad der Detaillierung sollten diese aufweisen?
- *Modellierungssprache:* Welche Modellierungssprache eignet sich am besten zur Modellierung von WPPs?

Damit WPPs erfolgreich in Unternehmen implementiert und genutzt werden können, kann die Bearbeitung der aufgeführten Themen hinsichtlich der Optimierung des Beschreibungsschemas und der weiteren Anwendung wichtige Beiträge liefern.

Literaturverzeichnis

1. Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003. BDSG. Bundesgesetzblatt I, 66–88 (2003)
2. Europäisches Parlament: Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG. EU-DSGVO (2016)
3. Anke, J., Berning, W., Schmidt, J., Zinke, C.: IT-gestützte Methodik zum Management von Datenschutzanforderungen. HMD 54, 67–83 (2016)
4. Mont, M.C., Pearson, S.: An Adaptive Privacy Management System for Data Repositories. In: Katsikas, S.K. (ed.) Trust, privacy, and security in digital business. Second international conference TrustBus 2005, Copenhagen, Denmark, pp. 236–245. Springer, Berlin (2005)

5. Karjoth, G., Schunter, M., Waidner, M.: Platform for Enterprise Privacy Practices. Privacy-Enabled Management of Customer Data. In: Goos, G., Hartmanis, J., van Leeuwen, J., Dingledine, R., Syverson, P. (eds.) Privacy Enhancing Technologies, 2482, pp. 69–84. Springer, Berlin, Heidelberg (2003)
6. Buchmann, E., Anke, J.: Privacy Patterns in Business Processes. In: Eibl, Maximilian, Gaedke, Martin (eds.) INFORMATIK 2017, pp. 793–798. Ges. für Informatik, Bonn
7. Lange, J.A.: Sicherheit und Datenschutz als notwendige Eigenschaften von computergestützten Informationssystemen. Ein integrierender Gestaltungsansatz für vertrauenswürdige computergestützte Informationssysteme (2005)
8. Rodeck, M., Voigt, C., Schnütgen, A., Schiering, I., Decker, R.: Toolgestützte Assessments zu Datenschutz und Datensicherheit in kleinen und mittelständischen Unternehmen. In: Plödereder, E. (ed.) INFORMATIK 2014, pp. 575–586. Ges. für Informatik, Bonn (2014)
9. Karjoth, G.: Datenschutzkonforme Geschäftsprozesse. In: Barton, T., Erdlenbruch, B., Herrmann, F., Marfurt, K., Müller, C., Seel, C. (eds.) Prozesse, Technologie, Anwendungen, Systeme und Management. Angewandte Forschung in der Wirtschaftsinformatik, pp. 20–30. mana-Buch, Heide (2015)
10. Masellis, R. de, Ghidini, C., Ranise, S.: A Declarative Framework for Specifying and Enforcing Purpose-Aware Policies. In: Foresti, S. (ed.) Security and Trust Management, pp. 55–71. Springer, Cham (2015)
11. Gamma, E., Helm, R., Johnson, R., Vlissides, J.: Design Patterns: Abstraction and Reuse of Object-Oriented Design. In: European Conference on Object-Oriented Programming. Springer (1993)
12. Buschmann, F., Meunier, R., Rohnert, H., Sommerlad, P., Stal, M.: Pattern-Oriented Software Architecture, A System of Patterns. Wiley, s.l. (2013)
13. van Dijk, A.: Contracting Workflows and Protocol Patterns. In: Goos, G., Hartmanis, J., van Leeuwen, J., ter Hofstede, A., van der Aalst, W.M.P., Weske, M. (eds.) Business Process Management, pp. 152–167. Springer, Berlin, Heidelberg (2003)
14. Russel, N., ter Hofstede, A.H.M., Edmond, D. and van der Aalst, W.M.P.: Workflow Resource Patterns
15. Gündogdu, F.: Analyse zur Verwendung der Workflow Pattern und der Business Process Modelling and Notation bei der Modellierung von Prozessen. Dissertation, http://dbis.eprints.uni-ulm.de/1101/ (2014)
16. van der Aalst, W.M.P., ter Hofstede, A.H.M., Kiepuszewski, B., Barros, A.P.: Workflow Patterns. Distributed and Parallel Databases 14, 5–51 (2003)
17. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design Science in Information Systems Research. MIS Quarterly 28, 75–105 (2004)
18. § 33 Benachrichtigung des Betroffenen. In: Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003. BGBl. I (2003)