HMD
https://doi.org/10.1365/s40702-018-00449-7

SCHWERPUNKT

Datenschutzgrundverordnung (DSGVO): Bewältigung der Herausforderungen mit Unternehmensarchitekturmanagement (EAM)

Hasan Koç · Kai Eckert · Daniel Flaig

Eingegangen: 22. Juni 2018 / Angenommen: 12. August 2018

Zusammenfassung Datenschutz nimmt eine zunehmend größere Bedeutung in der modernen Datenverarbeitung ein. Seit dem 25. Mai 2018 müssen Unternehmen der EU-Datenschutz-Grundverordnung (EU-DSGVO) entsprechen. Ziel ist die Vereinheitlichung der Datenschutzgesetze aller 28 Mitgliedstaaten der EU. Unternehmen können bei Verstößen mit Bußgeldern bis zu 20 Mio. € oder vier Prozent des weltweiten Jahresumsatzes sanktioniert werden. Aktuelle Studien verdeutlichen, dass die Anzahl der Unternehmen, die den Vorgaben der EU-DSGVO entsprechen, gering ist. In diesem Zusammenhang stehen Unternehmen vor verschiedenen Herausforderungen, wie bspw. undeutliche Interpretationen der EU-DSGVO und die einhergehende Komplexität bei der Anwendung der Verordnung in der Praxis. Unternehmensarchitekturen liefern eine holistische Sicht auf wesentliche Artefakte einer Organisation. Dies geschieht durch eine Verknüpfung über verschiedene Ebenen (z. B. Business und IT). Diese Strukturen sind im Kontext der EU-DSGVO unerlässlich um festzuhalten, warum Daten verarbeitet werden und in welchen Systemen sie gespeichert sind. Vor diesem Hintergrund empfehlen wir, basierend auf den Konzepten des Unternehmensarchitekturmanagements, einen systematischen Ansatz zur Einführung eines DSGVO Projektes. Die vorgestellte Methode wird derzeit bei einem international führenden Softwarehersteller eingesetzt, unter Einhaltung des Design Science Research Paradigmas entwickelt, und evaluiert.

H. Koç (✉) · K. Eckert · D. Flaig
BOC Information Technologies Consulting GmbH, Naglerstraße 5, 10245 Berlin, Deutschland
E-Mail: hasan.koc@boc-de.com

K. Eckert
E-Mail: kai.eckert@boc-de.com

D. Flaig
E-Mail: daniel.flaig@boc-de.com

Published online: 20 August 2018

Schlüsselwörter Unternehmensarchitekturmanagement · Datenschutz · Design science research · DSGVO · EAM · Method engineering

Challenging the General Data Protection Regulation (GDPR) with Enterprise Architecture Management (EAM)

Abstract Data protection is playing an increasingly important role in modern data processing. Beginning with May 25, 2018, companies need to comply with General Data Protection Regulation (GDPR), a regulation to standardize the data protection laws across all 28 EU countries. In case of a noncompliance, the companies can be fined up to 4% of annual global turnover or €20 million. Recent studies show that the rate of the companies that put the GDPR requirements into practice is quite low. One challenge in this context is vague interpretations of GDPR and the complexity of applying the regulation in practice. Enterprise architectures deliver a holistic view of essential artefacts in an organization. This is achieved by relating information across different domains, e. g. Business and IT. In the GDPR context, such structures deem to be vital when it comes to documenting why the data is processed and in which systems it is stored. To this end, we propose a systematic approach on how to introduce a GDPR project in organizations drawing on the concepts of Enterprise Architecture Management. The approach, which is currently being used in an internationally leading software manufacturer, is developed and evaluated in line with design science research paradigm.

Keywords Enterprise architecture management · Privacy protection · Design science research · GDPR · EAM · Method engineering

1 Einführung

Datenschutz und Privatsphäre jedes Individuums spielen eine wichtige Rolle in der modernen digitalen Datenverarbeitung und gewinnen damit auch wirtschaftlich an Relevanz. In diesem Zusammenhang hat das Europäische Parlament am 27. April 2016 die Datenschutzgrundverordnung der Europäischen Union (DSGVO) verabschiedet. Die Verordnung ist am 24. Mai 2016 in Kraft getreten und ab dem 25. Mai 2018 verpflichtend anzuwenden.

Die DSGVO vereinheitlicht die Datenschutzgesetze in allen 28 EU-Ländern und hat das Ziel den EU-Bürgern das Verständnis zu erleichtern, wie ihre Daten verwendet werden. Der Kern der Verordnung betrifft die Verarbeitung personenbezogener Daten, d. h. nach Artikel 4 der DSGVO aller Informationen in Bezug auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) (DSGVO 2018a).

Die DSGVO wird Unternehmen in vielerlei Hinsicht beeinflussen. In erster Linie müssen Organisationen ein Verzeichnis über Verarbeitungstätigkeiten (VVT), die unter ihrer Verantwortung stehen, führen. Dieses Verzeichnis ist ein zentrales Konzept der DSGVO und enthält unter anderem Informationen über die Zwecke der Datenverarbeitung. Zweitens müssen Organisationen ihre internen Prozesse fortlaufend anpassen, um die Rechte des Betroffenen zu wahren. Hierzu zählen z. B. das

Auskunftsrecht der betroffenen Person, das Recht auf Löschung oder das Recht auf Berichtigung. In diesem Zusammenhang sollten notwendige Maßnahmen zum Umgang bei Datenverstößen eingeleitet werden. Drittens müssen Unternehmen im Voraus über Datenschutzaspekte nachdenken und die Privatsphäre bereits in den Entwicklungsprozess ihrer Produkte und Dienstleistungen miteinbeziehen.

Laut einer aktuellen Studie ist die Zahl der Unternehmen, die die DSGVO-Anforderungen in der Praxis umsetzen, recht gering, was zwangsläufig mit dem umfänglichen Geltungsbereich der DSGVO zusammenhängt (ZEW 2018). Mit 99 Artikeln und 173 Erwägungsgründen ist die DSGVO ein kompliziertes Dokument, welches neue Anforderungen an die Datenverantwortlichen und -verarbeitenden stellt. Viele Unternehmen wissen daher nicht, wo und wie sie mit der Umsetzung beginnen sollen. Darüber hinaus lassen die Vorschriften Raum für Interpretationen. So ist beispielsweise der Grad der Dokumentation in Bezug auf Datenkategorien nicht klar definiert.

Durch die Verknüpfung von Informationen über verschiedene Domänen hinweg liefern Unternehmensarchitekturen (Enterprise Architecture (EA)) eine ganzheitliche Sicht auf wesentliche Artefakte in einer Organisation. Unternehmensarchitekturmanagement (Enterprise Architecture Management (EAM)) ist in vielen Unternehmen eine etablierte Managementdisziplin, um eine architektonische Transparenz zu ermöglichen und schneller auf Veränderungen reagieren zu können. EAM erfordert notwendigerweise die Dokumentation von Organisationen aus verschiedenen Blickwinkeln, einschließlich verschiedener Stakeholder aus Business und IT, z. B. Prozessverantwortliche, Service-Manager und Unternehmensarchitekten. Damit kann eine Unternehmensarchitektur als Ausgangspunkt zur Bewältigung der Herausforderungen der DSGVO dienen und Unternehmensarchitekten können die Datenschutzbeauftragten in ihren Aufgaben unterstützen.

Folgende Forschungsfrage steht in diesem Beitrag im Fokus:

- Wie können die Unternehmen dabei unterstützt werden, ein DSGVO-Projekt aus EAM-Sicht zu initiieren?

Um dieses Problem zu lösen, schlagen wir eine Methode vor, die bestimmte Aktivitäten zum Initiieren eines DSGVO-Projekts mit erforderlichen Inputs, Outputs und beteiligten Rollen enthält. Die Methode basiert auf den Prinzipien der Design Science Research und wurde in einem führenden Software und Beratungshaus eingesetzt.

Der Aufbau des Papers strukturiert sich wie folgt: Abschn. 2 gibt Hintergrundinformationen zur EU-DSGVO und zum EAM und setzt die beiden Themenfeldern miteinander in Verbindung. Abschn. 3 beschreibt den Forschungsrahmen, der in diesem Paper verwendet wird. Die angewandte Methode wird in Abschn. 4 dargestellt und die Evaluationsergebnisse der Methode werden in Abschn. 5 detailliert. Abschn. 6 liefert konkrete Empfehlungen für die Praxis. Abschließend stellt Abschn. 7 die nachfolgenden Arbeitsschritte dar.

2 Grundlagen

2.1 EU-Datenschutzgrundverordung (EU-DSGVO)

Die EU-Datenschutzgrundverordnung (EU-DSGVO) ist ein „*set of new laws by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the EU*“ (EU-GDPR 2018). Es handelt sich somit um eine europäische Verordnung, mit der der Datenschutz für alle Personen innerhalb der EU vereinheitlicht werden soll und in allen Mitgliedsstaaten gültig ist. Die Gesetzgebung gilt jedoch nicht nur für europäische Organisationen, sondern umfasst gemäß Artikel 3 einen größeren Geltungsbereich. Auch Unternehmen außerhalb der EU müssen die DSGVO umsetzen, sobald diese Daten von EU-Bürgern verarbeiten.

Artikel 5 der DSGVO beschreibt die zentralen Grundprinzipien der Datenverarbeitung, wie z. B. die Rechtmäßigkeit der Verarbeitung, das Prinzip der Zweckbindung oder das Prinzip der Datenminimierung (DSGVO 2018b). Damit gewinnen die betroffenen Personen mehr Macht über ihre personenbezogenen Daten, welche in Artikel 12 bis Artikel 23 aufgeführt sind. Die betroffene Person kann beispielsweise die Löschung ihrer Daten anfordern.

Ein wichtiger Aspekt der DSGVO ist die Pflicht zur Führung eines Verzeichnisses über die Verarbeitungstätigkeiten (VVT), das eine Form der Dokumentation darstellt. Das VVT ist zum einen ein wichtiges Instrument zur Gewährleistung der betriebsinternen Transparenz bei der Verarbeitung personenbezogener Daten. Zum anderen stellt das VVT ein zentrales Dokument zur Gewährleistung der Nachweispflichten nach Artikel 5 der DSGVO dar (DSGVO 2018b). Die DSGVO gibt nicht genau vor, wie das VVT dokumentiert und gepflegt werden soll. Dennoch ist die Struktur in Artikel 30 der DSGVO dargestellt.

Die DSGVO kann den Aufbau einer Datenschutzkultur in Organisationen unterstützen. Es stellt Unternehmen jedoch keine Checklisten oder Best Practices zur Verfügung. Darüber hinaus ist die Einhaltung der DSGVO ein kontinuierlicher Prozess. Daraus ergeben sich viele Fragestellungen für die Praxis, u. a. wie man ein DSGVO-Projekt in einer Organisation beginnen kann.

2.2 Unternehmensarchitekturmanagement (Enterprise Architecture Management)

Eine Unternehmensarchitektur umfasst alle relevanten Komponenten, und deren Beziehungen untereinander, zur Beschreibung eines Unternehmens. Es ermöglicht eine holistische Sichtweise, indem es verschiedene Bereiche wie strategische Ziele, die erfüllt werden müssen, Geschäftsfähigkeiten, die erforderlich sind, um die Ziele zu erreichen, Geschäftsprozesse, Anwendungen und Technologien zur Unterstützung der Ausführung der Prozesse sowie die verantwortlichen Organisationseinheiten und Rollen miteinander verbindet.

Um die Anliegen der Stakeholder zu trennen, ist eine Unternehmensarchitektur üblicherweise in Schichten strukturiert. Obwohl es keinen Standard gibt wie die Schichten aussehen sollen, ist es möglich, zwischen der Business-Ebene und der IT-

Abb. 1 Ebenen der Unternehmensarchitektur

Ebene zu unterscheiden. Die IT-Ebene kann als Anwendungsebene und Technologieebene weiter detailliert werden. Im Rahmen dieses Beitrags werden die in Abb. 1 gezeigten Ebenen betrachtet.

Die Geschäftsobjekte sind im Wesentlichen die Daten, die von Anwendungen verarbeitet, über Schnittstellen zu Anwendungen übertragen und in einer Datenbank gespeichert werden können. Der Grund, warum Daten verarbeitet werden, ist eng mit dem Geschäftsprozessobjekt verknüpft. Um bspw. den Geschäftsprozess Audit-Management durchführen zu können, werden Auditdaten in der Datenbank „ICS DB1“ gespeichert und mit der Anwendung „Internes Kontrollsystem“ verarbeitet. Derartige Daten können zwischen verschiedenen Schnittstellen übertragen werden, die in einer Anwendungsebene dokumentiert sind. Die Informationen darüber, wie die Auditdaten verschlüsselt sind oder wie lange sie in den Systemen aufbewahrt werden, können aus den Artefakten der Technologieebene gewonnen werden. Verschiedene Rollen und Organisationen, die Zugriff auf die Auditdaten haben, können

in der Organisationsebene dargestellt werden. Daher sind wir der Überzeugung, dass Unternehmensarchitektur eine zuverlässige Grundlage für die Identifizierung der Artefakte, die im Zusammenhang mit der DSGVO relevant sind, bieten kann. Unsere Methode basiert auf dieser Überlegung und hilft, ein DSGVO-Projekt aus Sicht des Unternehmensarchitekturmanagements zu initiieren.

2.3 Stand der Forschung

Sowohl in der wissenschaftlichen Literatur als auch in der Praxis existieren nur wenige Ansätze, die sich auf die methodischen Aspekte der DSGVO konzentrieren. Diese Meinung wird auch von Feltus et al. (2017) vertreten. Die Autoren stellen fest, dass keine Lösung, kein Modell und keine Methode diese neuen Vorschriften vollständig berücksichtigen und integrieren. Sie schlagen ein Datenschutz-Metamodell vor, auf dessen Basis DSGVO-relevante Konzepte definiert und miteinander in Beziehung gesetzt werden können. Ein ähnlicher Ansatz wird von Martín und Álamo (2017) vorgeschlagen, der darauf abzielt, ein kontrolliertes Vokabular, basierend auf einem sogenannten Privacy Engineering Metamodell, zu definieren. In beiden Werken werden jedoch keine konkreten Schritte zur Umsetzung der Konzepte mitaufgeführt.

Wenn die Verarbeitung der Daten zu einem hohen Risiko bezüglich der Rechte der Person führen kann, führt der Verantwortliche eine Datenschutz-Folgenabschätzung (Data Protection Impact Assessment = DPIA) durch. Bieker et al. (2016) schlagen einen aus drei Stufen bestehenden Prozess vor, der es ermöglicht Risiken zu bewerten. Auch Alnemr et al. (2011). berichten von einer DPIA-Methodik für kleine und mittelständische Unternehmen, die personenbezogene Daten in der Cloud verarbeiten.

Wenn die personenbezogenen Daten für die Zwecke, für die sie erhoben oder anderweitig verarbeitet wurden, nicht mehr benötigt werden, hat die betroffene Person ein Recht auf Löschung. In diesem Zusammenhang diskutieren Berning et al. (2017) Datenlöschungskonzepte und definieren bestimmte Kriterien für die Aufbewahrungsfristen personenbezogener Daten.

Im Gegensatz zu wissenschaftlichen Veröffentlichungen gibt es eine beträchtliche Anzahl von Best Practices, Verfahren, Schritten usw. zur Umsetzung der DSGVO in Organisationen. Diese Ansätze werden in der Regel von Datenschutzinstitutionen entwickelt und bleiben hinsichtlich der tatsächlichen Nutzung in der Praxis sehr allgemein. Beispielsweise wird nicht dokumentiert, welche Rollen und Stakeholder in das Implementierungsprojekt einbezogen oder welche Artefakte in den einzelnen Phasen erzeugt werden sollen. Darüber hinaus werden keine Informationen über die Durchführbarkeit und Rigorosität der Methode in der Entwicklungsphase gegeben. Die vorliegende Arbeit zielt darauf ab, diese Lücke zu schließen. Dazu stellen wir in Abschn. 3 zunächst die Forschungsmethode vor, mit der die Methode entwickelt wurde.

3 Methodik

Die Methode zur Einführung der DSGVO wurde basierend auf den Prinzipien der Design Science Research (DSR) und des Frameworks zur Methodenkonzeptualisierung von Goldkuhl erstellt, die in Abschn. 3.1 bzw. 3.2 beschrieben sind.

3.1 Design Science Research (DSR)

DSR ist grundsätzlich der Prozess zur Konstruktion eines zweckmäßigen Artefakts, das ein Problem löst, indem es zum wissenschaftlichen Wissen beiträgt und davon profitiert (Baskerville 2008). Die DSR-Artefakte können Konstrukte, Modelle, Methoden und Instanziierungen darstellen. Bei dem in diesem Beitrag vorgeschlagenen DSR-Artefakt handelt es sich um eine Methode.

Es existieren verschiedene Verfahren zur Durchführung der DSR (Dresch et al. 2015), wobei diese im Wesentlichen aus zwei Phasen bestehen, dem *Gestalten* und der *Evaluation*. Die Gestaltungphase umfasst die Aktivitäten der Konstruktion eines Artefakts für einen bestimmten Zweck (vgl. Abschn. 4). Die Evaluierungsphase untersucht, wie gut dieses Artefakt in dem Kontext funktioniert, für den es entworfen wurde (vgl. Abschn. 5). Zur Entwicklung der Methode zur Einführung der DSGVO wurde das von Peffers et al. (2007) eingeführte Verfahren angewendet.

3.2 Method Engineering

Ganz allgemein beschreibt eine Methode ein systematisches Vorgehen zur Problemlösung, einschließlich der erforderlichen Hilfsmittel und Ressourcen. Die Methode zur Einführung der DSGVO wurde in Anlehnung an den Methodenkonzeptrahmen von Goldkuhl et al. (1998) entwickelt. Dieser besagt, dass eine umfassende Methodenbeschreibung die Perspektive, das Framework, die Kooperationsformen und alle Methodenkomponenten umfasst. Die Methodenkomponente ist der zentrale Begriff und bezieht sich auf das Dreigestirn „Konzepte – Prozeduren – Notation“. Konzepte

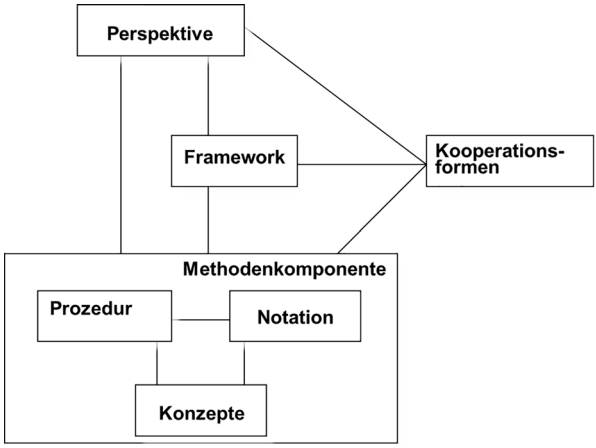

Abb. 2 Methoden Framework nach Goldkuhl et al. (1998)

beschreiben die relevanten Aspekte der Realität in der Methode. Prozeduren dokumentieren die einzelnen Schritte mit Inputs, Outputs sowie den beteiligten Rollen und Ziele der Aktivitäten. Die Notation gibt an, wie das Ergebnis des Verfahrens dokumentiert werden soll. Das Framework gibt einen Überblick über die Methode und stellt die Beziehungen zwischen den Komponenten dar.

Die Perspektive definiert die von der Methode unterstützte Modellierungs- oder Problemlösungsaufgabe. An der Anwendung einer Methode können verschiedene Akteure beteiligt sein. Kooperationsformen spezifizieren eine Reihe von Fachkompetenzen oder die Zusammenarbeit zwischen den verschiedenen Rollen. Das methodische Framework ist in Abb. 2 dargestellt.

4 Eine Methode zur Einführung eines DSGVO-Projektes

4.1 Perspektive, Framework, Kooperationsformen

Das Design-Problem, welches die Methode lösen soll, lautet: „Wie können die Unternehmen unterstützt werden, um ein DSGVO-Projekt aus der Sicht des EAM zu starten?“. Ein zentraler Aspekt der DSGVO ist die Dokumentation der Verarbeitungstätigkeiten. Im ersten Schritt besteht daher der Hauptzweck der Methode darin, ein systematisches Verfahren zu definieren, um das Verzeichnis von Verarbeitungstätigkeiten mithilfe einer holistischen Sicht, d. h. der Unternehmensarchitektur, zu erstellen. Im Teil „Prozedur“ (Abschn. 4.2) werden zusätzliche Zwecke definiert, die sich auf die Projektphasen und -aktivitäten beziehen.

Für die Anwendung der Methode gelten bestimmte Einschränkungen. Was die Methode nicht anstrebt, ist die Erreichung einer kompletten Reife in Bezug auf DSGVO-Konformität. Beispielsweise bietet die Methode aktuell keine Unterstützung für die Anpassung der organisatorischen Prozesse, d. h. wie die Verträge zur Auftragsdatenverarbeitung angepasst werden sollten oder wie die internen DSGVO-Schulungen organisiert werden sollten.

Folgende Rollen sind für die Umsetzung der Methode nötig:

- Das DSGVO-Projektteam (PT) umfasst den Datenschutzbeauftragten, einen Unternehmensarchitekten und zusätzliche unterstützende Rollen, z. B. zur Dokumen-

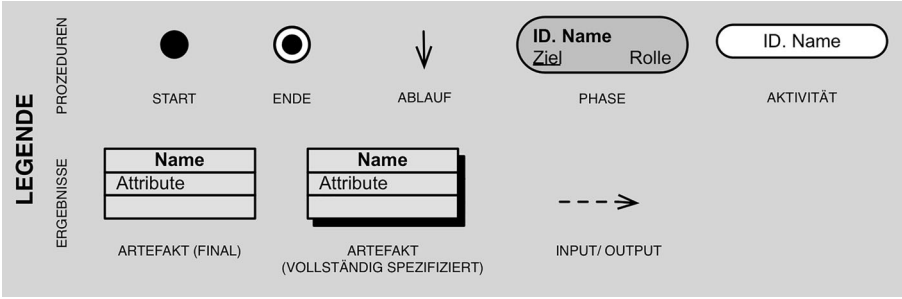

Abb. 3 Notation der Prozess-Datendiagramm-Technik

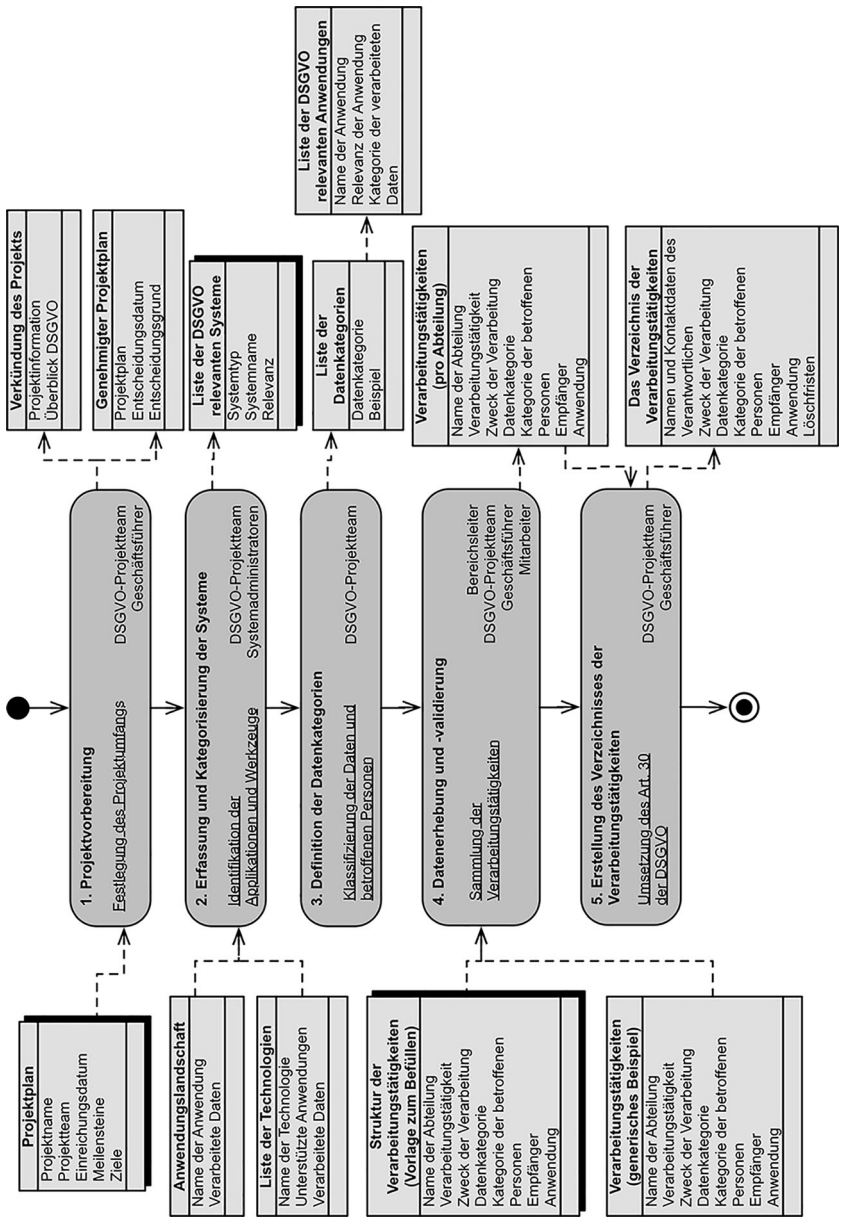

Abb. 4 Methode zur Einführung eines DSGVO-Projekt

tation der Verarbeitungstätigkeiten, Durchführung von Workshops zur Datenbewertung, Konsolidierung der Ergebnisse usw.

- Geschäftsführer genehmigen den Projektplan und das VVT. Ihre Beteiligung an dem Projekt ist von entscheidender Bedeutung, da sie im Fall von Verstößen gegen die Verordnung persönlich zur Verantwortung gezogen werden. Darüber hinaus tragen sie zur Vermarktung der Projektziele bei.

- Bereichsleiter liefern Informationen über die Verarbeitungstätigkeiten, d. h. in welcher Organisationseinheit werden welche personenbezogenen Daten zu welchen Zwecken erhoben und mit welchen Anwendungen verarbeitet.
- Die Mitarbeiter validieren die Informationen zu den Verarbeitungstätigkeiten in den jeweiligen Abteilungen, die von den Bereichsleitern dokumentiert werden. Sie können auch den Inhalt der Tätigkeiten erweitern, z. B. mit einer zusätzlichen Anwendung, Datenbank oder einer Datenkategorie, die für die Verarbeitung einer Tätigkeit relevant ist.
- Systemadministratoren sind an der Dokumentation der Anwendungen oder Konfigurationselemente, die in der Organisation verwendet werden, beteiligt. Solche Berichte können aus den Configuration Management Databases (CMDB) generiert werden, die üblicherweise von den Administratoren verwaltet werden. Um eine aktuelle Liste mit Anwendungen, Technologien und Datenbanken zu erstellen, arbeiten Systemadministratoren im Idealfall mit den Unternehmensarchitekten zusammen.

Die Methode besteht derzeit aus einer eigenständigen Methodenkomponente, nämlich das „Verzeichnis von Verarbeitungstätigkeiten“. Um einen Überblick über diese Methodenkomponente zu geben, verwenden wir die Prozess-Datendiagramm-Technik (PDD), deren Notation in Abb. 3 (de Weerd et al. 2005) dargestellt ist. Dabei ist zu beachten, dass die PDD nicht die „Notation“ ist, die zur Dokumentation der Methodenergebnisse verwendet wird, sondern eine Visualisierungstechnik, die den Überblick über die Methode darstellt. Die Methode zur Einführung eines DSGVO-Projektes ist in Abb. 4 dargestellt.

4.2 Prozedur, Konzepte und Notation

4.2.1 Phase 1: Projektvorbereitung

Ziel dieser Phase ist die Festlegung des Anwendungsbereichs des DSGVO-Projekts. Die erste Aktivität (Aktivität 1.1) sammelt die Anforderungen der Projekteigner, den Geschäftsführern. Anschließend wird ein Projektplan im DSGVO-Projektteam (Aktivität 1.2) festgelegt. Dieser enthält Informationen über das Projektteam, die beteiligten Akteure, die Meilensteine sowie die Ziele. In Aktivität 1.3 schaffen sowohl die Bereichsleiter als auch das DSGVO-Projektteam Sensibilisierung für das Thema, indem sie beispielsweise an internen Treffen der Abteilungen teilnehmen und die Mitarbeiter über das Thema informieren. Darüber hinaus wird von den Geschäftsführern eine Informations-Mail verteilt, die die Empfänger über die DSGVO und das Projekt informiert. Danach schließt das DSGVO-Projektteam den Projektplan ab und übermittelt die Ergebnisse, z. B. durch Veröffentlichung im Intranet des Unternehmens (Aktivität 1.4). Alle Aktivitäten sind in Abb. 5 dokumentiert.

Die Methodenergebnisse in dieser Phase sind der Projektplan, der von der Geschäftsführung genehmigt ist, und die Bekanntmachung des Projekts. Der Projektplan kann ein Word-Dokument sein, welches aus Informationen über das Projektteam, die durchzuführende Aktivitäten, beteiligte Stakeholder, Projekteinreichungsdatum, Meilensteine sowie Zielen besteht. Dies wird im genehmigten Projektplan

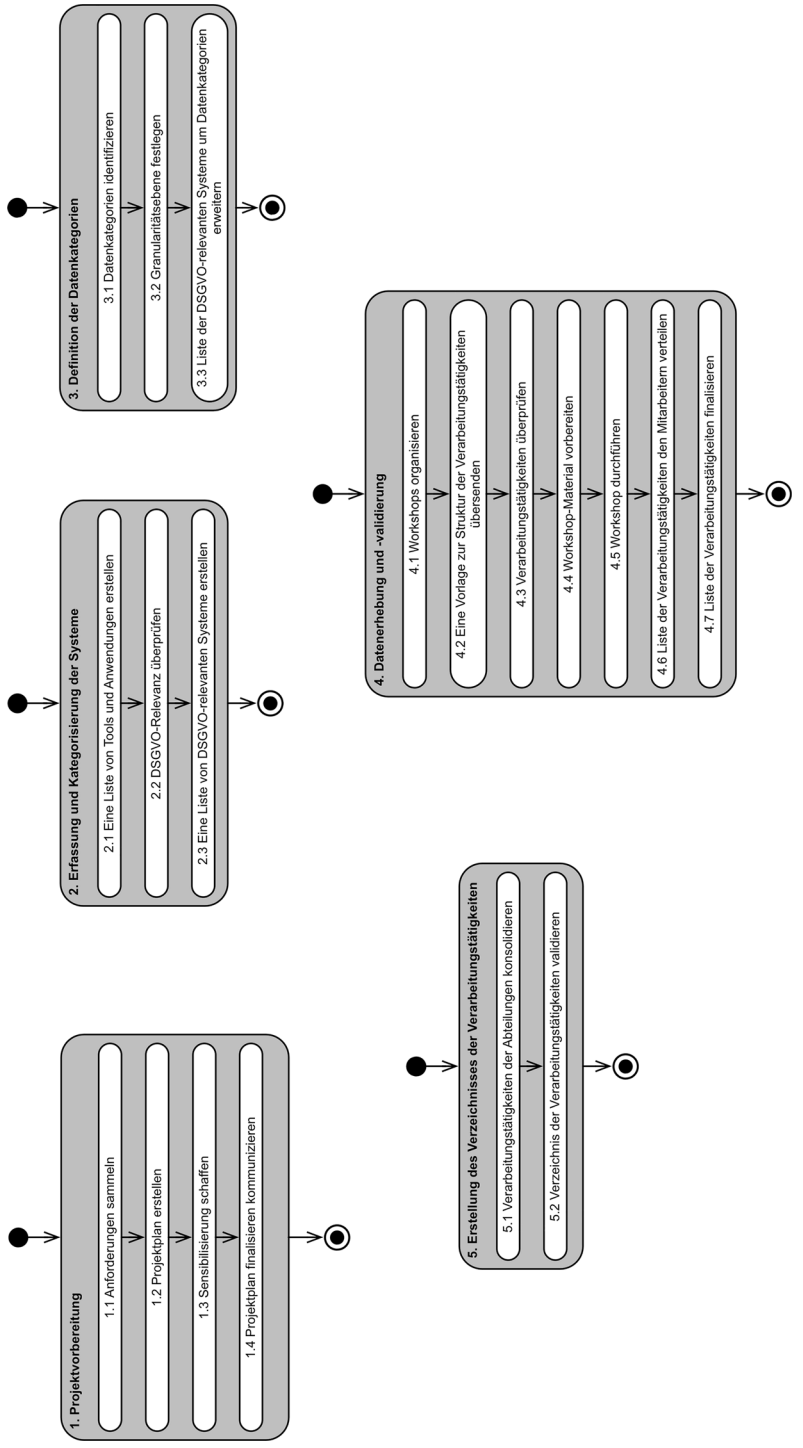

Abb. 5 Aktivitäten der Methodenkomponente

um das Entscheidungsdatum und den Entscheidungsgrund erweitert. Die Verkündung des Projektstarts kann per E-Mail oder PDF-Dokument, welches von den Geschäftsführern unterzeichnet wird, verbreitet werden.

4.2.2 Phase 2: Erfassung und Kategorisierung der Systeme

Ziel dieser Phase ist es, die für das DSGVO-Projekt relevanten Systeme zu identifizieren. Ausgangspunkt für die Datenerhebung ist die Liste aller Tools, Technologien und Anwendungen im Unternehmen, in denen personenbezogene Daten gespeichert und verarbeitet werden (Aktivität 2.1). Die Vorteile eines anwendungsorientierten Ansatzes sind zweifach. Erstens ermöglicht dieser den Datenfluss in der Organisation zu definieren und zu bestimmen, d.h. zwischen welchen Anwendungen oder Schnittstellen die Daten ausgetauscht werden. Ferner vereinfacht er die Analyse des Umsetzungsgrades der technischen und organisatorischen Maßnahmen in den späteren Phasen des Projekts. Zweitens kann die Liste der Anwendungen direkt aus den Anwendungslandschaften bzw. Applikationsarchitekturen extrahiert werden. Diese Liste kann von den Systemadministratoren angepasst werden, indem beispielsweise zusätzliche Informationen von einem CMDB-System bereitgestellt werden.

In einem weiteren Schritt muss die Liste der Systeme durch das DSGVO-Team (Aktivität 2.2) überprüft werden, um die Instanzen auszuschließen, die keine personenbezogenen Daten verarbeiten und folglich eine Liste von DSGVO-relevanten Systemen zu erstellen (Aktivität 2.3, vgl. Abb. 5). Die zwei wichtigsten Methodenergebnisse werden in Tabellenform visualisiert. Zum Beispiel kann die Liste der Systeme direkt aus einem EA-Modell-Repository oder einem CMDB-Tool exportiert werden. In der Aktivität 2.2. wird die Liste um ein zusätzliches Attribut „Relevanz“ erweitert, das dokumentiert, warum die Anwendung oder Technologie für das DSGVO-Projekt relevant ist. Beispielsweise werden die Anwendungen, die personenbezogen Daten verarbeiten, als relevant gekennzeichnet.

4.2.3 Phase 3: Definition der Datenkategorien

Ziel von Phase 3 ist die Klassifizierung der Daten und betroffenen Personen. Im ersten Schritt wird überprüft, ob die Datenkategorien unternehmensweit bekannt bzw. dokumentiert sind (Aktivität 3.1). Die Aktivität kann vom Unternehmensarchitekten ausgeführt werden, da diese Informationen auf der Ebene der Datenarchitektur zu finden sind (vgl. Abb. 3).

Die zweite Aktivität ist die Festlegung der Granularitätsebene (Aktivität 3.2). Je nach Datensatz und Projektziel können Kategorien wie „Kundendaten, Partnerdaten, Personaldaten“ oder „Adressdaten, Versicherungsdaten, Bankdaten“ etc. definiert werden. Der Vorteil des ersten Ansatzes ist eine automatische Ableitung von Datensubjekten aus den Datenkategorien. Indem man den zweiten Ansatz verfolgt, ist es einfacher festzustellen, ob sensible Daten verarbeitet werden. Des Weiteren können auf dieser Ebene Löschkonzepte bzw. Löschfristen definiert werden (DIN 66398 2018). In der letzten Aktivität soll die Liste der DSGVO-relevanten Systeme um Datenkategorien erweitert werden (Aktivität 3.3).

Das Methodenergebnis in dieser Phase ist die Liste von Datenkategorien, die auf Datenarchitekturebene dargestellt werden können. Diese ist in der Liste der DSGVO-relevanten Systeme enthalten. Beide Listen werden tabellarisch dargestellt.

4.2.4 Phase 4: Datenerhebung und -validierung

In dieser Phase sollen Informationen über die Verarbeitungstätigkeiten in der Organisation gesammelt und validiert werden. Alle identifizierten Stakeholder, mit Ausnahme der Systemadministratoren, sind in dieser Phase involviert. Verschiedene Datenerhebungsmethoden, wie Interviews, sekundäre Datenanalyse oder Beobachtungstechniken, werden dabei eingesetzt. Wir empfehlen die Erhebung der Daten mittels Workshops, die separat mit jedem Bereichsleiter organisiert werden sollten (Aktivität 4.1). Ein obligatorischer Input für solche Workshops ist eine erste Version der Verarbeitungsaktivitäten der ausgewählten Organisationseinheit, deren Leiter am Workshop teilnimmt. Dazu sendet das Projektteam eine leere Vorlage an den jeweiligen Abteilungsleiter, der von diesem ausgefüllt werden sollte. Zusätzlich empfiehlt sich ein generisches Beispiel für die Verarbeitungstätigkeiten mitzusenden, welches aufzeigt, wie der Output aussehen soll (Aktivität 4.2). Die Vorlage enthält den Namen der Abteilung, die Namen der Verarbeitungstätigkeiten, den Zweck der Verarbeitung, die Datenkategorien, die betroffenen Personen, die Empfänger und die verarbeitende Anwendungen. Um eine konsistente Dokumentation zu gewährleisten, kann den Abteilungsleitern die Liste der DSGVO-relevanten Systeme und Datenkategorien ebenfalls bereitgestellt werden. Im Gegenzug sollte das Projektteam vor dem Workshop die Verarbeitungstätigkeiten erhalten, damit der Inhalt und die Datenqualität vor dem Workshop überprüft werden kann (Aktivität 4.3). Danach bereitet das Projektteam das Workshop-Material (Foliensätze sowie Fragen zur tentativen, also probeweisen, Liste der Verarbeitungstätigkeiten) vor, das sich hauptsächlich auf zwei Hauptteile konzentriert (Aktivität 4.4). Im ersten Teil werden die Grundlagen der DSGVO und ihre Relevanz für die Organisation vermittelt. Der zweite Teil konzentriert sich auf die Überprüfung der Verarbeitungstätigkeiten, die von den Bereichsleitern dokumentiert und zum Workshop als Input geliefert werden. Es werden auch weitere Fragen gestellt (z. B. „Welche Aktivitäten erfordern die Teilnahme von zwei oder mehrere Organisationseinheiten?“) (Aktivität 4.5). Das Ergebnis des Workshops, d. h. die erweiterte/aktualisierte Liste der Verarbeitungstätigkeiten, wird den Mitarbeitern der Organisationseinheit mitgeteilt (Aktivität 4.6.). Danach kann die Liste um weitere Anwendungen ergänzt werden, die personenbezogene Daten verarbeiten, aber noch nicht erfasst wurden (vgl. Aktivität 2.1 und Aktivität 4.5). Alternativ wird die Liste, sofern sie vollständig ist, von den Mitarbeitern validiert (Aktivität 4.7).

Phase 4 erfordert somit zwei Artefakte als Input, die Vorlage zur Erfassung der Verarbeitungstätigkeiten und ein generisches Beispiel der Verarbeitungstätigkeiten. Die Vorlage sollte zuerst vom Bereichsleiter ausgefüllt, dann in den Workshops erweitert oder verkürzt werden, anschließend von den Mitarbeitern validiert und vom Projektteam finalisiert werden. Für jede Organisationseinheit entsteht entsprechend eine andere Liste von Verarbeitungstätigkeiten. Sowohl das Beispiel als auch die Verarbeitungstätigkeiten können in Tabellenform dokumentiert werden.

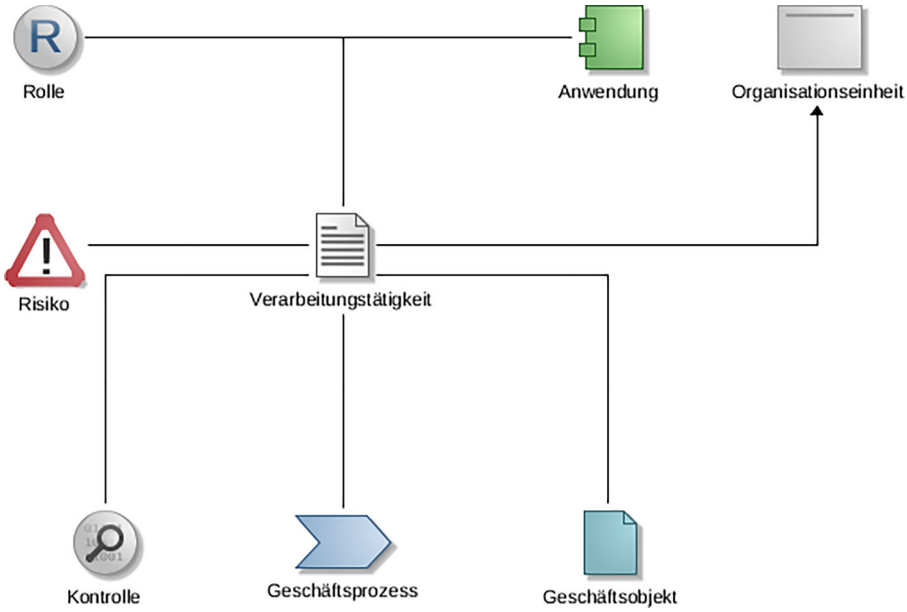

Abb. 6 Einbettung der Verarbeitungstätigkeit in ein EA-Modell

4.2.5 Phase 5: Erstellung des Verzeichnisses der Verarbeitungstätigkeiten (VVT)

In dieser letzten Phase wird das Hauptartefakt der Methode, das VVT, erstellt. Wie in Abschn. 2.1 erläutert, ist das VVT in Artikel 30 der DSGVO geregelt. Dementsprechend besteht das Verzeichnis aus Informationen über den Namen und Einzelheiten des Verantwortlichen, den Zweck der Verarbeitung, die Datenkategorie, der betroffenen Person, den Empfängern, der Anwendung und der Fristen für die Löschung. Solche Informationen können sehr gut aus den Verarbeitungstätigkeiten extrahiert werden, die von jeder Abteilung gesammelt werden (vgl. Phase 4). Diese sollten jedoch in erster Linie vom DSGVO-Projektteam (Aktivität 5.1) konsolidiert werden. Dies ist notwendig, da die Verarbeitungsaktivitäten der Abteilungen, die in den Workshops erzeugt werden, ein unterschiedliches Abstraktionsniveau besitzen können. Darüber hinaus wird es einige Querschnittsverarbeitungsaktivitäten geben. Ein Beispiel dafür ist das „Bewerbungsverfahren“. Erwartungsgemäß werden solche Verarbeitungstätigkeiten in vielen Workshops erwähnt, was eine Konsolidierungsaktivität erfordert.

Die letzte Aktivität besteht schließlich in der Validierung des Verzeichnisses der Verarbeitungsaktivitäten. Dies ist notwendig um eine hohe Datenqualität sicherzustellen und eine Genehmigung von der Managementebene zu erhalten (vgl. Abb. 5). Zu diesem Zweck ist es zielführend ein oder mehrere Workshops mit den Geschäftsführern durchzuführen. Das Methodenergebnis der abschließenden Phase ist die endgültige Liste der Verarbeitungsaktivitäten, also „das Verzeichnis der Verarbeitungstätigkeiten“, welches mithilfe eines Tabellenformulars dokumentiert werden kann.

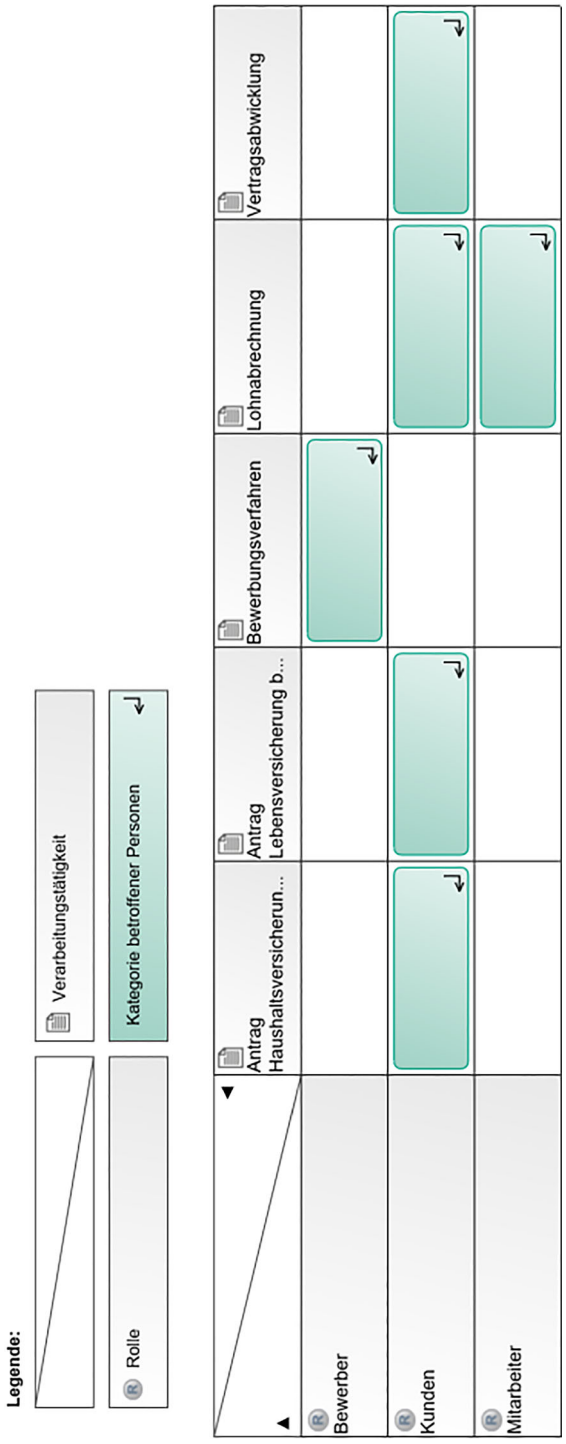

Abb. 7 Matrix-View zur Veranschaulichung von durch Verarbeitungstätigkeiten betroffener Personen

4.2.6 Verknüpfung von Verarbeitungstätigkeiten und EA Artefakten

Wie in den Phasen zur Einführung eines DSGVO-Projektes vorgestellt, werden im Zuge des Aufbaues des VVT viele Daten erhoben und dokumentiert. Bei genauerer Betrachtung lässt sich schnell eine enge Verbindung zwischen diesen erhobenen Daten und den typischen Artefakten einer EA Architektur erkennen. Diese Artefakte werden im Kontext von EAM Projekten für gewöhnlich auch erfasst und in dedizierten EA Tools verwaltet. Zur Vermeidung redundanter Datenerhebungen und vor allem Speicherungen, bietet sich an, das VVT direkt mit den EA Artefakten zu verknüpfen und in EAM Tools zu integrieren.

Abb. 6 zeigt exemplarisch die Einbettung einer Objektklasse Verarbeitungstätigkeit in ein EA Modell am Beispiel des Architekturmanagementwerkzeugs ADOIT (https://de.boc-group.com/adoit/). Die Verarbeitungstätigkeit referenziert hier typische Elemente eines EA Repository, wie bspw.

- Anwendungen: Dokumentation der Systeme, in denen die Verarbeitung erfolgt
- Rollen und Organisationseinheiten: Dokumentation von Betroffenen und Empfängern
- Geschäftsprozessen: Dokumentation des Zwecks der Verarbeitung
- Geschäftsobjekten: Kategorisierung der personenbezogenen Daten sowie
- Risiken und Kontrollen: Dokumentation von technischen und organisatorischen Maßnahmen.

Durch die Einbettung der Verarbeitungstätigkeit in das EA Modell und die Aufnahme der Elemente in ein EA Tool-Repository werden Synergien in Bezug auf den Aufbau der Dokumentation geschaffen. Gleichzeitig besteht die Möglichkeit zur Nutzung von bewährten EA Views zur Analyse und Auswertung, wie Cluster Maps, Portfolios und Matrizen (vgl. Abb. 7).

5 Evaluation

DSR ist der Prozess der Konstruktion eines zweckmäßigen Artefakts, das ein Problem löst, indem es zum wissenschaftlichen Wissen beiträgt und davon profitiert. Ein DSR Projekt besteht im Wesentlichen aus zwei Phasen, Build & Evaluate (Gestalten und Evaluieren). Die „Build"-Phase umfasst die Gestaltungsaktivitäten eines Artefakts für einen bestimmten Zweck, z. B. Entwicklung einer Methode zur Einführung eines DSGVO-Projekts. Die „Evaluate"-Phase untersucht, inwieweit das Artefakt das geäußerte Problem löst sowie die Rigorosität der Artefaktentwicklungsschritte. Als solches ist sie eine entscheidende Komponente in jedem DSR-Projekt.

5.1 Design der Evaluation

Verschiedene Artefakte, wie z. B. Modelle, Modellierungssprachen und Methoden, können in einem DSR-Projekt generiert werden. Da eine Methode keine externe Realität beschreibt, kann der „Wahrheitswert" einer Methode nicht dargestellt werden. Es ist nur möglich, seinen pragmatischen Wert, oder in der DSR-Terminologie

Tab. 1 Bewertung der Nützlichkeit

Frage	Antwort
Die Methode hat mir geholfen, das Verzeichnis der Verarbeitungstätigkeiten zu erstellen	60 % stimme voll zu 40 % stimme zu
Die Methode hat mir geholfen, Daten über die Verarbeitungstätigkeiten zu sammeln	60 % stimme voll zu 40 % stimme zu
Die Methode hat mir geholfen, die Sensibilisierung zur DSGVO innerhalb meiner Organisation zu erhöhen	60 % stimme voll zu 40 % stimme zu
Die Methode hat mir in der Einführungsphase der DSGVO geholfen	60 % stimme voll zu 40 % stimme zu
Die Methode hat mir geholfen, die offenen Punkte zur DSGVO Konformität zu identifizieren	40 % stimme voll zu 40 % stimme zu 20 % teils/teils
Insgesamt bin ich mit den Ergebnissen der Methode zufrieden	60 % stimme voll zu 40 % stimme zu
Anmerkungen zur Nützlichkeit der Methode	Freitext

seinen „Nutzen“ (Utility), zu demonstrieren. In diesem Zusammenhang entwickelt Moody das „Method Evaluation Model“ (MEM), ein Framework für die Validierung von Methoden (Moody 2003). Der Autor stellt fest, dass „das Ziel der Validierung nicht darin bestehen sollte zu demonstrieren, dass die Methode korrekt ist, sondern dass die Methode auf der Grundlage ihres pragmatischen Erfolges rational angewandt wird“. Pragmatischer Erfolg wird dabei als „Effizienz und Effektivität, mit der eine Methode ihre Ziele erreicht“, definiert. In diesem Zusammenhang ist das Ziel der Evaluation die Methode aus Sicht ihrer „Nützlichkeit“ (percieved usefulness: ob und zu welchem Grad verbessert die Nutzung des Artefakts die Arbeitsleistung) und „Benutzerfreundlichkeit“ (perceived ease of use: ob die Nutzung eines Artefakts ohne Aufwand möglich ist) zu betrachten.

Für diese Zwecke wurde eine kleine Umfrage vorbereitet und an die sechs Methodennutzer ausgegeben. Die Umfrage bestand aus zwei Teilen, „Nützlichkeit der Methode in der Projektphase 1“ sowie „Benutzerfreundlichkeit der Methode in der Projektphase 1“. Im ersten Teil der Umfrage wird die Sachdienlichkeit und das Nutzen der Methode bewertet. Der zweite Teil ist ähnlich aufgebaut, in dem die Bedienbarkeit, Erlernbarkeit und Verständlichkeit der Methode evaluiert wird[1].

5.2 Ergebnisse der Evaluation

Fünf Methodennutzer haben den Ansatz evaluiert. Die Rücklaufquote der Umfrage betrug somit 83,33 %. Alle Teilnehmer haben zugestimmt, dass die Methode bzgl. der Erstellung der Verarbeitungstätigkeiten Ihnen geholfen hat. Des Weiteren haben sie angegeben, dass die Methode zur Sensibilisierung zur DSGVO innerhalb der Organisation beigetragen hat und dem Nutzer in der Einführungsphase der DSGVO geholfen hat (60 % stimme voll zu, 40 % stimme zu). Eine ähnliche Verteilung beobachteten wir in der Frage, ob die Stakeholder mit den Ergebnissen der Methode zufrieden waren. Ein Methodenanwender hat angemerkt, dass die Methode

[1] Die Umfrage ist aufrufbar unter http://bit.ly/DSGVO_Umfrage.

Tab. 2 Bewertung der Benutzerfreundlichkeit

Frage	Antwort
Die Methode ist im Kontext meiner Organisationsstruktur anwendbar	80 % stimme voll zu 20 % stimme zu
Die Methode beschreibt die Aktivitäten zur Erhebung der personenbezogenen Daten deutlich	60 % stimme voll zu 40 % stimme zu
Die Methode beschreibt Inputs und Outputs der den Aktivitäten deutlich	60 % stimme voll zu 40 % stimme zu
Die Methode ist einfach zu verstehen	80 % stimme voll zu 20 % teils/teils
Die Methode ist einfach zu lernen	60 % stimme voll zu 40 % stimme zu
Die Methode ist einfach zu nutzen	80 % stimme zu 20 % teils/teils
Anmerkungen zur Benutzerfreundlichkeit der Methode	Freitext

einen einfachen Weg bietet zu verstehen, welche Verarbeitungstätigkeiten welche personenbezogenen Daten verarbeiten und welche Anwendungen dafür eingesetzt werden. Basierend auf diesen Werten lässt sich ableiten, dass die Methode bezüglich der Nützlichkeit gute Ergebnisse liefert.

Die Identifizierung der DSGVO Konformität wurde allerdings bei der Nützlichkeit eher kritisch betrachtet. Bei dem Punkt scheinen die Anwender uneinig zu sein. Diese lässt sich auch bei den Anmerkungen zeigen, da ein Methodenanwender angegeben hat, dass die Methode momentan lediglich einen Ausschnitt betrachtet. Das Ergebnis war zu erwarten, da die Methode komponentenbasiert gestaltet wurde und in den nächsten Aktivitäten mit weiteren Aspekten der DSGVO-Konformität erweitert wird, wie z. B. die Unterstützung zur Gewährleistung der Sicherheit der Verarbeitung. Die Ergebnisse der Umfrage über die Nützlichkeit der Methode sind in der Tab. 1 dargestellt.

Eine weitere positive Bewertung erhielt die Methode bezüglich ihrer Anwendung in der Organisation. In anderen Worten lassen sich die von der Methode benötigten Rollen (vgl. Abschn. 4.1) in der Organisation wiederfinden. bzw. die Methodenaktivitäten mittels verfügbarer Ressourcen in der Organisation umsetzen. Es wurde auch bestätigt, dass die Aktivitäten der Methode sowie Inputs und Outputs deutlich beschrieben wurden. Bis auf einen Methodennutzer gaben an, dass die Methode einfach zu verstehen wäre. Die Erlernbarkeit der Methode wurde ebenfalls positiv bewertet. Allerdings sind die Stakeholder nicht gänzlich davon überzeugt, dass die Methodennutzung einfach ist. Die Ergebnisse sind in Tab. 2 veranschaulicht.

6 Empfehlungen für die Praxis

Die in dieser Arbeit dargestellte Methode (vgl. Abb. 4 und 5) soll die Unternehmen dabei unterstützen, ein DSGVO-Projekt zu beginnen, um die seit 25. Mai 2018 geltenden Vorschriften zu erfüllen. Sie umfasst derzeit nur eine Methodenkomponente – das Verzeichnis der Verarbeitungsaktivitäten. Aktuell stellt sie somit einen ersten

Schritt in Richtung Einhaltung der DSGVO dar und führt nicht zu einer Organisationsstruktur, die die DSGVO-Anforderungen vollständig erfüllt (vgl. Abschn. 7).

Als Ausgangspunkt verwendet die Methode eine Struktur der Organisation, die in Form einer Unternehmensarchitektur (EA) erfasst wird. Dieser Ansatz hat eine Reihe von Vorteilen. Zuallererst liefert eine EA die erforderlichen Informationen, um nachzuvollziehen, warum die Daten verarbeitet werden und in welchem Zusammenhang sie mit weiteren Artefakten stehen. Dies kann über Geschäftsprozesse erfasst und dokumentiert werden, die in der Geschäftsarchitektur kategorisiert sind. Zweitens kann die Liste der Anwendungen, die personenbezogene Daten verarbeiten, aus der Anwendungsarchitektur extrahiert werden. Darüber hinaus können die technischen und organisatorischen Maßnahmen direkt mit den Gestaltungsobjekten der Anwendungsarchitektur in Verbindung gesetzt werden, was die Rückverfolgbarkeit ihrer Implementierung vereinfacht. Drittens kann man feststellen, in welchen Datenbanken welche Arten von persönlichen Daten gespeichert sind. Um die Rechte der betroffenen Personen zu gewährleisten, können die Organisationen schnell feststellen, welche Systeme relevant sind, um beispielsweise personenbezogene Daten auf Anfrage zu löschen. Zu guter Letzt enthält das Verzeichnis von Verarbeitungsaktivitäten Informationen, die typischerweise in einer Unternehmensarchitektur zu finden sind. Als Beispiel können die Kategorien von Empfängern aus den Organisationseinheiten (Geschäftsarchitektur), die Datenkategorien aus den Geschäftsobjekten (Datenarchitektur) und die betroffene Personen aus den Rollen (Organisationsarchitektur) abgeleitet werden.

Die erste Methodenkomponente wurde in einem internationalen Software- und Beratungshaus angewandt. Dazu wurde das zuvor beschriebene Verfahren befolgt, d. h. es wurde zunächst der Umfang des Projekts festgelegt, die Systeme wurden gelistet und die Daten wurden basierend auf den Eingaben aus der bestehenden Unternehmensarchitektur kategorisiert. Anschließend wurden weitere Daten über die Verarbeitungstätigkeiten erhoben und das Verzeichnis von Verarbeitungsaktivitäten erstellt. Für diese Phasen wurden die Methodenprodukte (Method Products) als Input verwendet bzw. als Output produziert. Folgende Beobachtungen wurden gemacht:

- Die erhobenen Anforderungen der Geschäftsführung in Aktivität 1.1. waren anfangs vage. Nach einigen Iterationen und Workshops wurden diese spezifiziert, sodass das Projektteam die Projektziele ausdrücken, Arbeitspakete entwerfen und Meilensteine identifizieren konnte.
- Die Geschäftsführer waren so weit wie möglich an den Aktivitäten beteiligt. Dies erhöhte das Bewusstsein über das Projekt innerhalb der Organisation. Ein konkretes Beispiel untermauerte diese Annahme, als die Geschäftsführung lediglich im ersten Teil eines Workshops anwesend sein konnte (vgl. Aktivität 4.5.). Die Konzentration und Motivation der übrigen Teilnehmer nahm in der zweiten Hälfte deutlich ab, was zu einer geringen Datenqualität führte. Diese Beobachtung wird empirisch nicht bestätigt, es kann jedoch argumentiert werden, dass die Anwesenheit der Managementebene in solchen Workshops die Qualität der Daten positiv beeinflusst.
- Aktivität 2.2 betrifft die Klassifizierung der Systeme in Abhängigkeit davon, ob sie personenbezogene Daten verarbeiten. In einigen Fällen war das Projektteam nicht

in der Lage, die direkte Relevanz zu identifizieren, da der Zugriff auf bestimmte Systeme nicht möglich war. Solche Systeme wurden separat erfasst und in den Workshops der Aktivität 4.5 evaluiert.

- Verschiedene Stakeholder sind an verschiedenen Phasen der Methode beteiligt. Zum Beispiel wird Aktivität 4.5 mit den Bereichsleitern jeder Abteilung separat durchgeführt. Aufgrund unterschiedlicher Hintergründe und Perspektiven variierte das Niveau der bereitgestellten Informationen bezüglich der Verarbeitungstätigkeiten. Folglich hat Aktivität 5.1 dem Projektteam geholfen, das richtige Maß an Abstraktion zu finden.
- Obwohl der Projektplan im Intranet der Organisation veröffentlicht und die Mitarbeiter durch Bekanntmachungen und kurze Besprechungen informiert wurden, wurde in einigen Fällen bemerkt, dass das Niveau der Zusammenarbeit mit den Mitarbeitern eher niedriger als erwartet war. Dies wurde durch bilaterale Gespräche mit den Bereichsleitern thematisiert und dabei verdeutlicht, wie sich die DSGVO auf ihre Arbeitsweise auswirken könnte. Das erhaltene Feedback zeigt, dass es ziemlich schwierig war der Thematik genügend Zeit zu widmen, um die Methodenprodukte (z. B. den Projektplan) vorzustellen und die Grundlagen der DSGVO zu verstehen. Folglich sollte aus unserer Erfahrung mehr Aufwand und Zeit zur Erhöhung der Awareness eingeplant werden, indem beispielsweise ein Informationstag über die DSGVO organisiert wird. Die Methode verwendet derzeit zwei Maßnahmen zur Sensibilisierung, (i) Information über die Mailverteiler und (ii) die Teilnahme an Team-Meetings.

7 Fazit und Ausblick

Die DSGVO zielt darauf ab Datenschutzgesetze in der EU zu standardisieren. Organisationen müssen zur Einhaltung der DSGVO ihre Prozesse anpassen und bestimmte Anforderungen erfüllen. Aktuelle Studien weisen auf die niedrige Anzahl an Organisationen hin, die die Anforderungen der DSGVO in der Praxis umgesetzt haben. Dies ist zum einen auf die Komplexität der DSGVO zurückzuführen und zum anderen, dass eine methodische Unterstützung zur praktische Anwendung nicht existiert. In diesem Kontext wurde in diesem Betrag eine Methode zur Einleitung eines DSGVO-Projekts in Organisationen vorgeschlagen.

In diesem Paper wird eine erste Version einer Methode zur Unterstützung von Projekten zur Einführung von DSGVO vorgestellt. Die Methode wird als eine Methodenkomponente dokumentiert, da weitere Bausteine zur EU-DSGVO Konformität in die Methode integriert werden sollten. In diesem Zusammenhang betrifft die zukünftige Arbeit hauptsächlich die Entwicklung von zwei weiteren Komponenten, wie z. B. die Identifikation der technischen und organisatorischen Maßnahmen und das Design von Prozessen zur Sicherung der betroffenen Rechte.

Die Methode wurde basierend auf deren Nützlichkeit und Benutzerfreundlichkeit bewertet. Die initiale Bewertungen und das Feedback zeigen, dass ein Nutzen gestiftet wurde und die Stakeholder bei der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten unterstützt wurden. Verglichen mit den Lösungen aus der Praxis deutet das Ergebnis auf einen wichtigen, wissenschaftlich fundierten Beitrag hin,

der die Schritte, die benötigten Inputs und Stakeholder detailliert beschreibt und eine tool-basierte Dokumentation ermöglicht. Da die Bewertung in einem kleinen Kreis stattgefunden hat, ist unsere Absicht die Methode in weiteren Organisationen umzusetzen und den Grad der Generalisierbarkeit unserer Erkenntnisse zu erhöhen.

Wie verhält sich die Methode gegenüber die in der Theorie vorgeschlagenen Lösungen? In Abschn. 2.3 wurden einige Ansätze dargestellt. Wir vertreten die Sicht, dass die Methode den Anwendungsbereich existierender Lösungen erweitert und mit diesen agieren kann. So ist z. B. denkbar, im ersten Schritt die Methode zur Einführung des DSGVO-Projekts umzusetzen. Basierend auf den Ergebnissen kann man in einem weiteren Schritt die DPIA-Methodik (Bieker et al. 2016) nutzen, um die Folgenabschätzung durchzuführen. Um Löschkonzepte in einer weiteren Methodenkomponente festzulegen, können ferner die Kriterien nach Berning et al. (2017) angewandt werden.

Die Anforderungen der DSGVO werden nicht allein durch die Erstellung des Verzeichnisses der Verarbeitungsaktivitäten erfüllt. Die Unternehmen müssen technische und organisatorische Maßnahmen festlegen und umsetzen, um ein gewisses Maß an Sicherheit bei der Datenverarbeitung zu gewährleisten (DSGVO 2018c). Dafür wird eine weitere Methodenkomponente entwickelt, um Organisationen bei der Umsetzung solcher Maßnahmen zu unterstützen. Ein weiterer Aspekt, der derzeit bei der Einführung der DSGVO fehlt, ist die Einführung neuer Abläufe (z. B. Einführung der Lösch- oder Berichtigungskonzepte zur Sicherung der betroffenen Rechte), sowie die gezielte Sensibilisierung der Mitarbeiter. Dies wird der Fokus der zweiten Methodenkomponente sein.

Literatur

Alnemr R, Cayirci E, Dalla Corte L, Garaga A, Leenes R et al (2011) A data protection impact assesment methodogy for cloud. https://pdfs.semanticscholar.org/5b74/2c82769c026f9c487d4d84d46f1ff86ea061.pdf. Zugegriffen: 19. Juni 2018

Baskerville R (2008) What design science is not. Eur J Inf Syst 17(5):441–443

Berning W, Meyer K, Keppeler LM (2017) Datenschutz-konformes Löschen personenbezogener Daten in betrieblichen Anwendungssystemen – Methodik und Praxisempfehlungen mit Blick auf die EU DSGVO. HMD 54(4):618–631

Bieker F, Friedewald M, Hansen M, Obersteller H, Rost M (2016) A process for data protection impact assessment under the European general data protection regulation. Privacy Technologies and Policy, S 21–37

Datenschutz-Grundverordnung (DSGVO) (2018a) Art. 4 DSGVO – Begriffsbestimmungen. Datenschutz-Grundverordnung (DSGVO). https://dsgvo-gesetz.de/art-4-dsgvo/. Zugegriffen: 28. März 2018

Datenschutz-Grundverordnung (DSGVO) (2018b) Art. 5 DSGVO – Grundsätze für die Verarbeitung personenbezogener Daten. Datenschutz-Grundverordnung (DSGVO). https://dsgvo-gesetz.de/art-5-dsgvo/. Zugegriffen: 3. Apr. 2018

Datenschutz-Grundverordnung (DSGVO) (2018c) Art. 32 DSGVO – Sicherheit der Verarbeitung. Datenschutz-Grundverordnung (DSGVO). https://gdpr-info.eu/art-32-gdpr/. Zugegriffen: 18. Apr. 2018

DIN-Norm 66398 (2018) Die Entwicklung eines Löschkonzepts. http://din-66398.de/. Zugegriffen: 19. Juni 2018

Dresch A, Lacerda DP, Antunes JAV Jr (2015) Design science research: a method for science and technology advancement. Springer, Cham https://doi.org/10.1007/978-3-319-07374-3

European Union General Data Protection Regulation (EU-GDPR) (2018) EU GDPR News & Updates—European Union General Data Protection Regulation. https://eugdpr.com/. Zugegriffen: 3. Apr. 2018

Feltus C, Grandry E, Kupper T, Colin J (2017) Model-driven approach for privacy management in business ecosystem. Proceedings of the 5th International Conference on Model-Driven Engineering and Software Development – 1, S 392–400

Goldkuhl G, Lind M, Seigerroth U (1998) Method integration: the need for a learning perspective. IEE Proc Softw 145(4):113–118

Martin Y-S, del Álamo JM (2017) A metamodel for privacy engineering methods. IWPE 2017 International Workshop on Privacy Egineering. (http:\\ceur-ws.org/Vol-1873/IWPE17_paper_24.pdf)

Moody D (2003) The method evaluation model: a theoretical model for validating information systems design methods. ECIS 2003 Proceedings. (http://aisel.aisnet.org/ecis2003/79)

Peffers K, Tuunanen T, Rothenberger MA, Chatter-jee S (2007) A design science research methodology for information systems research. J Manag Inf Syst 24(3):45–77

De Weerd V, Souer J, Versendaal J, Brinkkemper S (2005) Situational Requirements Engineering of Web Content Management Implementations. SREP2005

Zentrum für Europäische Wirtschaftsforschung (ZEW) (2018) Die Zeit drängt – Starker Nachholbedarf bei der Datenschutz-Grundverordnung. ZEW Branchenreport Informationswirtschaft. http://ftp.zew.de/pub/zew-docs/brepikt/201801BrepIKT.pdf. Zugegriffen: 17. Juni 2018