

DIN EN ISO/IEC 29101

ICS 35.030

**Informationstechnik –
Sicherheitstechniken –
Architekturrahmenwerk für Datenschutz (ISO/IEC 29101:2018);
Deutsche Fassung EN ISO/IEC 29101:2021**

Information technology –
Security techniques –
Privacy architecture framework (ISO/IEC 29101:2018);
German version EN ISO/IEC 29101:2021

Technologies de l'information –
Techniques de sécurité –
Architecture de référence de la protection de la vie privée (ISO/IEC 29101:2018);
Version allemande EN ISO/IEC 29101:2021

Gesamtumfang 60 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC 29101:2018 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als EN ISO/IEC 29101:2021 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitskreis NA 043-01-27-05 AK „Identitätsmanagement und Datenschutz-Technologien“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 29100 siehe DIN EN ISO/IEC 29100

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 29100, *Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Datenschutz*

Deutsche Fassung

Informationstechnik —
Sicherheitstechniken —
Architekturrahmenwerk für Datenschutz (ISO/IEC 29101:2018)

Information technology —
Security techniques —
Privacy architecture framework (ISO/IEC 29101:2018)

Technologies de l'information —
Techniques de sécurité —
Architecture de référence de la protection de la vie
privée (ISO/IEC 29101:2018)

Diese Europäische Norm wurde vom CEN am 27. September 2021 angenommen.

Die CEN- und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN- und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Symbole und Abkürzungen	7
5 Überblick über das Architekturrahmenwerk für Datenschutz	7
5.1 Elemente des Rahmenwerks	7
5.2 Zusammenhang mit Managementsystemen	9
6 Akteure und pbD	9
6.1 Übersicht	9
6.2 Phasen des Lebenszyklus der Verarbeitung von pbD	11
6.2.1 Erhebung	11
6.2.2 Übertragung	12
6.2.3 Verwendung	12
6.2.4 Speicherung	13
6.2.5 Entsorgung	13
7 Bedenken	14
7.1 Übersicht	14
7.2 Die Datenschutzprinzipien aus ISO/IEC 29100	14
7.3 Datenschutzerfordernisse	15
8 Architekturansichten	15
8.1 Allgemeines	15
8.2 Komponentenansicht	16
8.2.1 Allgemeines	16
8.2.2 Schicht für die Datenschutzeinstellungen	16
8.2.3 Schicht für Identitäts- und Zugangsverwaltung	21
8.2.4 Schicht der personenbezogenen Daten	23
8.3 Akteursansicht	31
8.3.1 Allgemeines	31
8.3.2 IKT-System der betroffenen Person	31
8.3.3 IKT-System der verantwortlichen Stelle	32
8.3.4 IKT-System des Auftragsdatenverarbeiters	33
8.4 Interaktionsansicht	34
8.4.1 Allgemeines	34
8.4.2 Schicht für die Datenschutzeinstellungen	35
8.4.3 Schicht für Identitäts- und Zugangsverwaltung	35
8.4.4 Schicht der personenbezogenen Daten	36
Anhang A (informativ) Beispiele für die pbD-bezogenen Bedenken eines IKT-Systems	37
A.1 Allgemeines	37
A.2 Einholung und Kommunikation der Einwilligung	37
A.3 Übermittlung des Zwecks für die Erhebung der personenbezogenen Daten	38

A.4	Sichere Verarbeitung personenbezogener Daten	38
A.5	Klassifizierung und Steuerungsmaßnahmen für personenbezogene Daten.....	39
A.6	Verbuchung und Audit von pbD-Vorgängen.....	39
A.7	Archivierung und Entsorgung personenbezogener Daten.....	40
A.8	Zusammenhang mit Datenschutzprinzipien	42
Anhang B (informativ) Ein System zur Aggregation personenbezogener Daten mit sicheren		
	Berechnungen.....	43
B.1	Allgemeines	43
B.2	Zweck, Akteure und Bereitstellung	43
B.3	Architektur für die Anwendung zur Eingabe personenbezogener Daten	44
B.4	Architektur für die Anwendung der Studiensteuerung	46
B.5	Architektur für die Anwendung zur sicheren Analyse von personenbezogenen Daten	48
B.6	Zusammenfassung	50
Anhang C (informativ) Ein datenschutzfreundliches, pseudonymes System für das Identitäts-		
	und Zugangskontrollmanagement.....	51
C.1	Allgemeines	51
C.2	Zweck, Akteure und Bereitstellung	51
C.3	Architektur des IKT-Systems des Herausgebers der Anmeldedaten an der Universität.....	53
C.4	Architektur des IKT-Systems des Studenten.....	54
C.5	Architektur der Kursbewertungssoftware	56
C.6	Zusammenfassung	57

Europäisches Vorwort

Der Text von ISO/IEC 29101:2018 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 29101:2021 durch das Technische Komitee CEN-CENELEC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis April 2022, und etwaige entgegenstehende nationale Normen müssen bis April 2022 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN-CENELEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN und CENELEC abrufbar.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 29101:2018 wurde von CEN-CENELEC als EN ISO/IEC 29101:2021 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames Technisches Komitee, ISO/IEC JTC 1 (JTC, en: Joint Technical Committee), eingerichtet.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe: www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *Information security, cybersecurity and privacy protection*, erarbeitet.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO/IEC 29101:2013), die technisch überarbeitet wurde. Die wesentliche Änderung im Vergleich zur Vorgängerausgabe besteht darin, dass der alte Anhang D entfernt wurde.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

Einleitung

Dieses Dokument beschreibt ein hochrangiges Architekturrahmenwerk und zugehörige Maßnahmen für den Datenschutz in Systemen der Informations- und Kommunikationstechnologie (IKT), die personenbezogene Daten (pbD) speichern und verarbeiten.

Das in diesem Dokument beschriebene Architekturrahmenwerk für Datenschutz

- bietet einen konsistenten, hochrangigen Ansatz für die Umsetzung von Steuerungsmaßnahmen für den Datenschutz zur Verarbeitung personenbezogener Daten in IKT-Systemen,
- bietet Orientierungshilfe für die Planung, Gestaltung und den Aufbau von IKT-Systemarchitekturen, die den Datenschutz von betroffenen Personen sicherstellen, indem sie die Verarbeitung, den Zugriff und die Übertragung von personenbezogenen Daten steuern, und
- zeigt, wie die Technologien zum Datenschutz (PET) als Steuerungsmaßnahmen für den Datenschutz verwendet werden können.

Dieses Dokument baut auf dem Rahmenwerk für Datenschutz der ISO/IEC 29100 auf, um eine Organisation dabei zu unterstützen, ihre Datenschutzanforderungen zu definieren, soweit sie sich auf von einem beliebigen IKT-System verarbeitete pbD beziehen. In einigen Ländern werden die Anforderungen an den Schutz der Privatsphäre als gleichbedeutend mit den Anforderungen an den Datenschutz/der Privatsphäre verstanden und unterliegen der Gesetzgebung zum Datenschutz/der Privatsphäre.

1 Anwendungsbereich

Dieses Dokument legt ein Architekturrahmenwerk für Datenschutz fest, das

- Sicherheitsbedenken für IKT-Systeme festlegt, die personenbezogene Daten verarbeiten,
- Komponenten für die Umsetzung solcher Systeme auflistet und
- Architekturansichten bietet, die diese Komponenten kontextualisieren.

Dieses Dokument ist anzuwenden für Einheiten, die sich mit der Festlegung, Beschaffung, dem Aufbau, der Gestaltung, der Prüfung, Aufrechterhaltung, Verwaltung und dem Betrieb von IKT-Systemen befassen, die pbD verarbeiten.

Es konzentriert sich hauptsächlich auf IKT-Systeme, die für die Interaktion mit betroffenen Personen gestaltet sind.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

ISO/IEC/IEEE 42010, *Systems and software engineering — Architecture description*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 29100 und ISO/IEC/IEEE 42010.

4 Symbole und Abkürzungen

Die folgenden Abkürzungen gelten für dieses Dokument.

IKT Informations- und Kommunikationstechnologie (en: information and communication technology, ICT)

PET Technologie zum Datenschutz (en: privacy enhancing technology)

pbD personenbezogene Daten (en: personally identifiable information, PII)

5 Überblick über das Architekturrahmenwerk für Datenschutz

5.1 Elemente des Rahmenwerks

Das in diesem Dokument vorgestellte Architekturrahmenwerk für Datenschutz dient als technische Referenz für Entwickler von IKT-Systemen, die personenbezogene Daten verarbeiten. Dieses Dokument stellt keine Anforderungen an Datenschutzrichtlinien; es geht davon aus, dass eine Datenschutzrichtlinie vorhanden ist, Datenschutzanforderungen festgelegt wurden und dass geeignete Schutzmaßnahmen innerhalb des IKT-Systems umgesetzt sind.

Dieses Architekturrahmenwerk konzentriert sich auf den Schutz personenbezogener Daten. Da dies zum Teil ein Sicherheitsziel ist, sollten IKT-Systeme, die personenbezogene Daten verarbeiten, auch den Leitlinien der Informationssicherheitstechnik folgen. Dieses Architekturrahmenwerk listet einige Komponenten der Informationssicherheit auf, die für den Schutz der in IKT-Systemen verarbeiteten pbD entscheidend sind. Das vorgestellte Architekturrahmenwerk basiert auf dem in ISO/IEC/IEEE 42010 verwendeten Modell.

Die Stakeholder im Zusammenhang mit diesen Bedenken sind die in ISO/IEC 29100 definierten Datenschutz-Akteuren. Sie werden in Abschnitt 6 näher erläutert.

Die Bedenken für das Architekturrahmenwerk sind in Abschnitt 7 beschrieben und beinhalten die Datenschutzprinzipien aus ISO/IEC 29100 und die für ein IKT-System spezifischen Datenschutzanforderungen.

Das Architekturrahmenwerk wird wie folgt dargestellt:

- a) die Schichten des technischen Architekturrahmenwerks in 8.2 zeigen die Architektur aus Sicht der Komponenten. Jede Schicht gruppiert Komponenten mit einem gemeinsamen Ziel oder einer ähnlichen Funktion;
- b) das Bereitstellungsmodell in 8.3 zeigt das Architekturrahmenwerk aus der Sicht eines eigenständigen IKT-Systems. Jede Ansicht zeigt eine Gruppierung der Komponenten anhand ihrer Bereitstellung in den IKT-Systemen der Stakeholder; und
- c) die Ansichten in 8.4 zeigen das Architekturrahmenwerk aus der Sicht der Interaktion. Die Ansichten veranschaulichen, wie die Komponenten zwischen den IKT-Systemen verschiedener Stakeholder interagieren.

Das Architekturrahmenwerk stellt auch Übereinstimmungsregeln zwischen den Bedenken und Sichtweisen durch die Verwendung von Zuordnungstabellen dar.

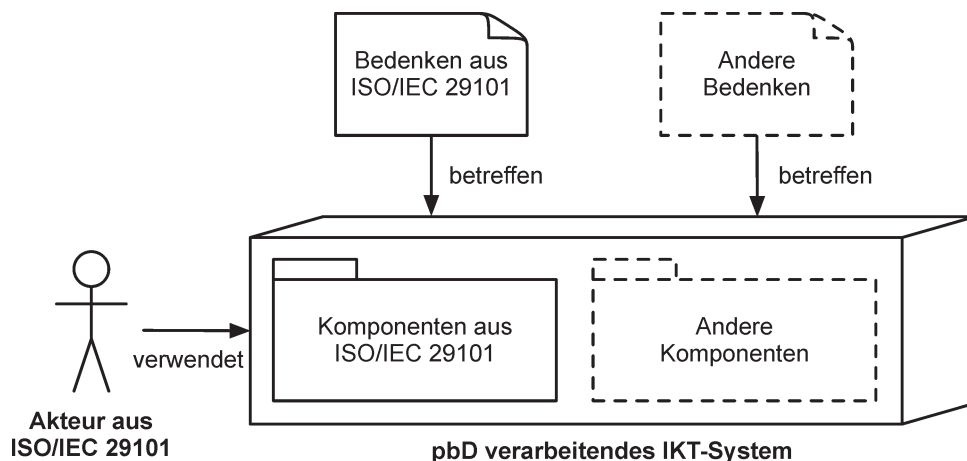


Bild 1 — Elemente des Architekturrahmenwerks für Datenschutz im Kontext

Bild 1 veranschaulicht den Zusammenhang zwischen den Elementen des Architekturrahmenwerks für Datenschutz. Das zentrale Element des Architekturrahmenwerks ist das zu erstellende IKT-System. Ein Akteur aus ISO/IEC 29101 verwendet das IKT-System. Die Gestaltung der IKT-Systeme wird sowohl von den in diesem Dokument angesprochenen Bedenken als auch von anderen Bedenken beeinflusst. Beispiele für andere Bedenken sind nichtfunktionale Anforderungen, die die Leistung, die Zugänglichkeit und die Gestaltung des IKT-Systems betreffen und sich nicht auf die funktionale Verarbeitung personenbezogener Daten auswirken. Diese anderen Bedenken liegen außerhalb des Anwendungsbereiches dieses Dokuments.

Das IKT-System kann sowohl Komponenten aus dem Architekturrahmenwerk für Datenschutz dieses Dokuments als auch andere Komponenten enthalten. Diese Komponenten verarbeiten keine personenbezogenen Daten, sondern übernehmen stattdessen andere Funktionen im IKT-System, wie z. B. Vorkehrungen zur Barrierefreiheit oder das Rendern spezieller Benutzungsschnittstellen. Solche Komponenten liegen außerhalb des Anwendungsbereiches dieses Dokuments.

5.2 Zusammenhang mit Managementsystemen

Die Verwendung eines Managementsystems ermöglicht es den verantwortlichen Stellen und den Auftragsdatenverarbeitern, ihre Datenschutzanforderungen mithilfe eines strukturierten Ansatzes effektiver zu erfüllen. Dieser strukturierte Ansatz bietet den verantwortlichen Stellen und den Auftragsdatenverarbeitern auch die Möglichkeit, die Ergebnisse zu messen und die Effektivität des Managementsystems kontinuierlich zu verbessern.

Ein effektives Managementsystem ist so transparent wie möglich, hat aber dennoch Auswirkungen auf Menschen, Prozesse und Technologie. Es sollte Teil des internen Maßnahmenprogramms und der Risikominderungsstrategie einer Organisation sein und seine Umsetzung dient zur Erfüllung von Datenschutzbestimmungen.

6 Akteure und pbD

6.1 Übersicht

Die Akteure des Architekturrahmenwerks nach ISO/IEC sind die an der Verarbeitung personenbezogener Daten beteiligten Datenschutz-Akteure, die in ISO/IEC 29100 beschrieben sind. Diese Akteure sind

- a) die betroffene Person,
- b) die verantwortliche Stelle und
- c) der Auftragsdatenverarbeiter.

ANMERKUNG Der „Dritte“, der als eine der vier Kategorien von Akteuren in ISO/IEC 29100 definiert ist, liegt außerhalb des Anwendungsbereichs des in diesem Dokument festgelegten Architekturrahmenwerks.

Aus Sicht der Bereitstellung ist das Architekturrahmenwerk in drei Teile untergliedert. Jeder Teil gilt für das bereitgestellte IKT-System aus der Sicht eines jeden dieser Akteure.

Bild 2 zeigt die IKT-Systeme der Akteure und die pbD-Flüsse zwischen diesen IKT-Systemen. Es veranschaulicht die logische Aufteilung der Funktionalität für das in diesem Dokument beschriebene Architekturrahmenwerk. Es ist nicht als Darstellung der physischen Struktur, der Organisation oder der Eigentumsverhältnisse der IKT-Systemhardware gedacht.

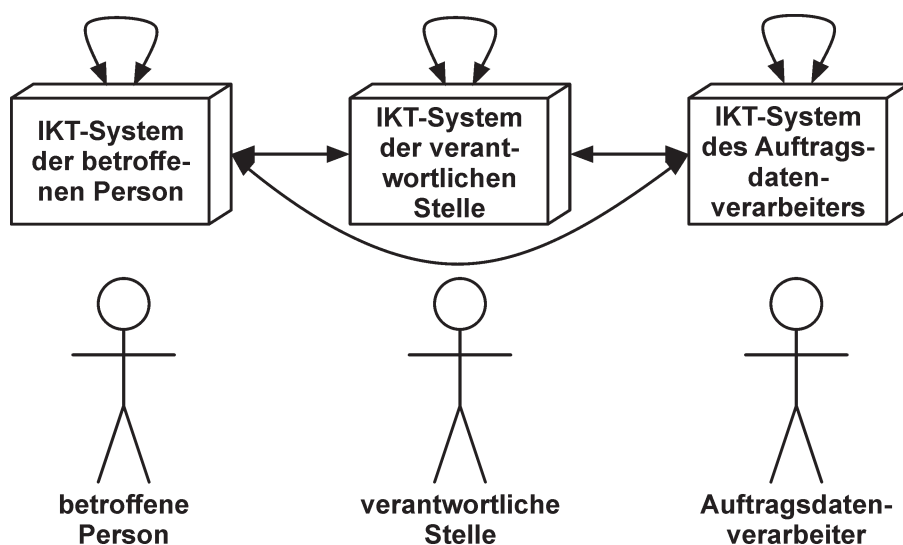


Bild 2 — Akteure und ihre IKT-Systeme nach diesem Dokument

Ein Akteur kann für den Aufbau der IKT-Systeme, die er verwendet, verantwortlich sein oder auch nicht. Beispielsweise kann die betroffene Person ein System verwenden, das von der verantwortlichen Stelle erstellt wurde und für das diese verantwortlich ist, oder das IKT-System der betroffenen Person kann ein Teil des IKT-Systems der verantwortlichen Stelle sein. Außerdem kann die Funktionalität des IKT-Systems der betroffenen Person auf verschiedene IKT-Hardwaresysteme aufgeteilt werden, die der betroffenen Person und der verantwortlichen Stelle gehören. In ähnlicher Weise kann die verantwortliche Stelle das IKT-System des Auftragsdatenverarbeiters bereitstellen. Geschäftsprozesse, in denen IKT-Systeme eingesetzt werden, verwenden eine Vielzahl von Kommunikations- und Vertrauensmodellen. Das Architekturrahmenwerk in diesem Dokument baut auf einer Abstraktion dieser Modelle auf.

Wenn die betroffene Person ein privat genutztes IKT-System verwendet, können die anderen Datenschutz-Akteure Anforderungen an dieses IKT-System stellen. Zum Beispiel kann das IKT-System der betroffenen Person ein Mindestmaß an Sicherheitsanforderungen erfüllen müssen, um eine Verbindung zu den anderen IKT-Systemen herstellen zu dürfen. Weitere Beispiele sind die Verwendung spezieller Sicherheitskomponenten wie Hardware-Authentifizierungstoken, bestimmte Betriebssystemversionen oder spezielle Webbrowser-Versionen.

In IKT-Systemen mit direkter Kommunikation (Kommunikationsverfahren, Kommunikationsmodell oder Kommunikationstechnologie, bei dem bzw. bei der die Kommunikation zwischen/unter den Einheiten erfolgt, die ohne zentrale Server miteinander verbunden sind) kann beispielsweise jede Anwendung die Rollen aller drei aufgeführten Akteure übernehmen. Informationen werden von jedem Partner sowohl gesendet als auch empfangen, so dass jeder Partner eine verantwortliche Stelle oder Auftragsdatenverarbeiter für pbD sein kann, die von einer anderen Partei in der Rolle einer betroffenen Person übertragen werden.

In Anwendungen für soziale Netzwerke können personenbezogene Daten von jedem verarbeitet werden, der Zugriff auf die Profile anderer Personen hat. Webbasierte Anwendungen für soziale Netzwerke ermöglichen allen autorisierten und möglicherweise anonymen Benutzern des Dienstes die Verarbeitung personenbezogener Daten, die von den mit dem sozialen Netzwerk verbundenen Betroffenen bereitgestellt werden.

6.2 Phasen des Lebenszyklus der Verarbeitung von pbD

6.2.1 Erhebung

Viele Organisationen erheben Informationen von betroffenen Personen. Diese Informationen können personenbezogene Daten enthalten.

Bei der Erhebung personenbezogener Daten sollten Organisationen immer die Datenschutzpräferenzen und die gesetzlichen Rechte der betroffenen Person sowie die Datenschutzanforderungen nach geltendem Recht berücksichtigen. Faktoren wie die Art der personenbezogenen Daten, die erteilte Einwilligung oder die angegebenen Datenschutzpräferenzen müssen in allen Phasen der Verarbeitung berücksichtigt werden. Personenbezogene Daten sollten nur erhoben werden, wenn sie für die angegebenen Zwecke benötigt werden.

Die Dokumentation sollte mit den pbD im Zusammenhang stehen. Beispiele hierfür sind u. a.

- a) Software-Tags, die den Zweck/die Zwecke angeben, für den/die die pbD verwendet werden können,
- b) Aufzeichnungen, die den Zweck/die Zwecke beschreiben, für den/die personenbezogene Daten verwendet werden können, und
- c) Aufzeichnungen über die erteilte Einwilligung und besondere Sensibilitäten, die beachtet werden sollten (z. B. sollten bestimmte Kategorien von personenbezogenen Daten verschlüsselt oder nach einem bestimmten Zeitraum gelöscht werden).

Steuerungsmaßnahmen für den Datenschutz sollten überall dort umgesetzt werden, wo Daten als pbD gekennzeichnet sind oder wo pbD mit zusätzlichen Informationen über die betroffene Person markiert sind. Es ist auch wichtig, Tags aufzubewahren, die für die Verarbeitung von pbD während der Nutzungs-, Übertragungs-, Speicherungs- und Entsorgungsphasen relevant sind. Wenn gespeicherte pbD wahrscheinlich geändert wurden, sollten sie vor der Verwendung auf Genauigkeit und Aktualität überprüft werden.

Darüber hinaus sollten Erhebungsprozesse personenbezogener Daten so gestaltet sein, dass nur die pbD erhoben werden, die für die jeweilige Transaktion erforderlich sind. Organisationen sollten Schritte unternehmen, um die versehentliche/unbeabsichtigte Erhebung personenbezogener Daten durch Dateneingabesysteme zu minimieren (z. B. Web-Anwendungsformulare, die die Eintragung beliebiger Informationen ermöglichen). Die Eintragung beliebiger pbD sollte durch die Verwendung einer kontextspezifischen Anzeige von Eingabefeldern minimiert werden, indem Bereiche im Webformular, in denen diese Informationen eingegeben werden können, reduziert oder entfernt werden (z. B. Löschen unnötiger Kontrollkästchen und Freitextfelder). Darüber hinaus sollte die Verwendung von Feldern mit vordefinierten Einträgen (z. B. Listboxen und Dropdown-Listen), die Nicht-pbD-Optionen enthalten, in Betracht gezogen werden. Wenn Freiform-Textfelder erforderlich sind, sollte die Benutzerschnittstelle (UI, en: user interface) Folgendes bieten:

- a) Warnhinweise, um die betroffene Person zu alarmieren, keine anderen pbD einzugeben als die, nach denen sie ausdrücklich gefragt wird und in die sie eingewilligt hat oder die durch geltendes Recht vorgeschrieben sind;
- b) klare Angabe der Felder, in denen pbD einzugeben sind und welche pbD eingegeben werden sollten (z. B. Name, Anschrift, Gesundheitsinformationen); und
- c) klarer Hinweis auf die Felder, in die keine pbD eingegeben werden sollten.

6.2.2 Übertragung

Das Übertragen, Verbreiten oder Freigeben von pbD an andere bedeutet, dass die pbD nicht mehr unter der alleinigen Kontrolle der betroffenen Person stehen. Übertragung ist üblicherweise der Begriff für die Weitergabe personenbezogener Daten von der verantwortlichen Stelle oder dem Auftragsdatenverarbeiter an andere verantwortliche Stellen und Auftragsdatenverarbeiter. Wenn personenbezogene Daten von der verantwortlichen Stelle an einen anderen Akteur übertragen werden, wird die Übertragung manchmal auch als Offenlegung bezeichnet.

Die Rechenschaftspflicht und Verantwortung für die übertragenen pbD sollte mit jeder an der Verarbeitung der pbD beteiligten Partei vereinbart und von ihr gewahrt werden. Diese Vereinbarung sollte schriftlich erfolgen, sofern dies nach geltendem Recht erforderlich ist. Darüber hinaus müssen solche Vereinbarungen mit den Datenschutzgesetzen in der Quell- und Zieldomäne der Übertragungen konform sein. Wenn es relevant und angemessen oder dies gesetzlich vorgeschrieben ist, sollte die betroffene Person darüber informiert werden, dass eine Übertragung stattfindet, und über den Inhalt und Zweck der Übertragung informiert werden. Wenn es zu einem Streitfall zwischen der betroffenen Person und der verantwortlichen Stelle oder dem Auftragsdatenverarbeiter kommt, sollten Aufzeichnungen über relevante Übertragungstransaktionen der personenbezogenen Daten zur Verfügung stehen, um bei der Beilegung eines solchen Streits Hilfestellung zu leisten.

Die Übertragung sensibler pbD sollte vermieden werden, es sei denn, sie

- ist notwendig, um eine Dienstleistung zu erbringen, die die betroffene Person angefordert hat,
- erfüllt eine geschäftliche Anforderung für das Angebot des angeforderten Dienstes oder
- ist gesetzlich vorgeschrieben.

Einige Rechtssysteme haben Gesetze erlassen, die ausdrücklich formale vertragliche Vereinbarungen verlangen, die alle Datenschutzerfordernisse zwischen den beteiligten Parteien enthalten, wenn personenbezogene Daten außerhalb eines Rechtssystems mit einem vorgeschriebenen Maß an Datenschutz übertragen werden. Bei grenzüberschreitenden Übertragungen sollte den Schutzmaßnahmen für die zu übertragenden pbD besondere Aufmerksamkeit geschenkt werden.

Während der Übertragung personenbezogener Daten sollten angemessene Schutzmechanismen vorhanden sein. Im Falle einer digitalen Übertragung sollten personenbezogene Daten über einen sicheren Kanal oder in verschlüsselter Form übertragen werden, wenn die Übertragung über einen unsicheren Kanal erfolgt. Wenn personenbezogene Daten auf physischen Datenträgern übertragen werden, sollten sie verschlüsselt werden. Bei einer Verschlüsselung sollte der Kodierungsschlüssel nicht zusammen mit den verschlüsselten personenbezogenen Daten gespeichert oder übertragen werden.

6.2.3 Verwendung

Die Verwendung personenbezogener Daten bedeutet jede Form der Verarbeitung von pbD, die nicht „Erheben“, „Übertragen“, „Speichern“, „Archivieren“ oder „Entsorgen“ beinhaltet. Die in ISO/IEC 29100 (Rahmenwerk für Datenschutz) beschriebenen Datenschutzprinzipien sowie einige Datenschutzgesetze können die Verarbeitung personenbezogener Daten einschränken, wenn diese Verarbeitung mit den ursprünglich festgelegten Zwecken unvereinbar ist. Daher sollten personenbezogene Daten nur für die erklärten Zwecke verarbeitet werden, für die sie erhoben wurden.

Wenn die personenbezogenen Daten für einen anderen Zweck zu verarbeiten sind, der nicht durch geltendes Recht abgedeckt ist, sollte die Einwilligung der betroffenen Person oder ihres Bevollmächtigten eingeholt werden. Der betroffenen Person sollte ein Mittel zur Verfügung gestellt werden, um die verantwortliche Stelle oder den Auftragsdatenverarbeiter zu kontaktieren, falls es Fragen zu Aktivitäten gibt, über die die betroffene Person im Unklaren ist.

Wenn eine solche Verarbeitung als notwendig erachtet wird, sollte die Einwilligung der betroffenen Person eingeholt werden, es sei denn, das Gesetz erlaubt etwas anderes. Betroffene Personen sollten klar über die spezifische Verwendung der personenbezogenen Daten informiert werden.

Zusätzlich sollten Schutzmechanismen, die für die Verwendung personenbezogener Daten geeignet sind, angewendet werden, wenn dies durch eine umfassende Risikoanalyse als notwendig erachtet wird. Dies beinhaltet die Verwendung von Anonymisierungs- oder Pseudonymisierungsverfahren vor der Verarbeitung und die Verwendung von sicheren Berechnungsverfahren während der Verarbeitung.

6.2.4 Speicherung

Wenn es notwendig ist, personenbezogene Daten zu speichern, sollte die Einwilligung der betroffenen Person eingeholt werden, wobei alle konkreten Maßnahmen, die gesetzlich vorgeschrieben sein können, zu berücksichtigen sind. In solchen Fällen sollten die personenbezogenen Daten nur so lange gespeichert werden, wie es zur Erreichung des konkreten Geschäftszwecks erforderlich ist.

Personenbezogene Daten sollten mit geeigneten Maßnahmen und Mechanismen gespeichert werden, um unbefugten Zugriff, Änderung, Vernichtung, Entfernung oder andere unbefugte Verwendung zu verhindern. Zu diesen Maßnahmen gehören u. a. Verschlüsselung, Secret Sharing, Pseudonymisierung und Anonymisierung.

Archivierte personenbezogene Daten bedürfen besonderer Aufmerksamkeit. Die Datenschutzprinzipien besagen, dass personenbezogene Daten nur so lange aufbewahrt werden sollten, wie es zur Erfüllung der angegebenen Zwecke erforderlich ist, und dann sicher vernichtet oder anonymisiert werden sollten. Wenn die verantwortliche Stelle oder der Auftragsdatenverarbeiter jedoch nach geltendem Recht verpflichtet ist, pbD nach Ablauf der anderen Zwecke aufzubewahren, sollten die pbD gesperrt werden (d. h. archiviert und mit einem Zugriffskontrollmechanismus geschützt werden, um eine weitere Verwendung zu verhindern). Die Hauptüberlegungen bei der Archivierung von personenbezogenen Daten sollten darin bestehen, sicherzustellen, dass die entsprechenden Datenschutzmechanismen vorhanden sind, einschließlich Lösungen für das Zugriffsmanagement, die den Zugriff auf archivierte personenbezogene Daten nur für autorisierte Benutzer ermöglichen.

Die verantwortliche Stelle sollte Maßnahmen in Speichersystemen umsetzen, um personenbezogene Daten zu entsorgen, wenn sie ablaufen oder wenn der Zweck für die Speicherung oder Verarbeitung der personenbezogenen Daten nicht mehr gültig ist.

6.2.5 Entsorgung

In der letzten Phase des Lebenszyklus der Auftragsdatenverarbeitung werden personenbezogene Daten gelöscht, anonymisiert, vernichtet, zurückgegeben oder auf eine andere Weise entsorgt. Bestimmte personenbezogene Daten innerhalb von Datensätzen können vor unbefugter Verwendung gesperrt werden, indem sie zur Entsorgung markiert werden. Es sollte beachtet werden, dass das Löschen von personenbezogenen Daten nicht zwangsläufig bedeutet, dass die Daten letztendlich entsorgt werden, da in IKT-Systemen gelöschte Daten oft wiederhergestellt werden können. Obwohl es eine offensichtliche Aufgabe im Umgang mit personenbezogenen Daten zu sein scheint, entsprechen die Verfahren zur Entsorgung von personenbezogenen Daten manchmal nicht den Datenschutzanforderungen. Von der betroffenen Person vorgegebene Spezifikationen (z. B. Verwendungszweck) oder durch die Gesetzgebung festgelegte Anforderungen (z. B. Ablaufdatum für bestimmte pbD) sollten berücksichtigt werden, bevor personenbezogene Daten entsorgt werden.

7 Bedenken

7.1 Übersicht

Bedenken nach der Definition in ISO/IEC/IEEE 42010 sind ein Interesse an einem System, das für einen oder mehrere seiner Stakeholder relevant ist. Das Architekturrahmenwerk für Datenschutz in diesem Dokument konzentriert sich auf die Bedenken der Datenschutz-Akteure in Bezug auf die Verarbeitung personenbezogener Daten. Die Bedenken in diesem Dokument umfassen die Datenschutzprinzipien der ISO/IEC 29100 und alle Datenschutzanforderungen, die von diesen Prinzipien abgeleitet sind und diesen entsprechen.

Die Datenschutzanforderungen sollten durch einen Datenschutz-Risikomanagementprozess ermittelt werden, der dem in ISO/IEC 29100:2011, 4.5 beschriebenen Prozess entspricht. Jede Person oder Organisation, die ein IKT-System entwickelt, das personenbezogene Daten verarbeitet, sollte diesen Prozess befolgen. Alle identifizierten Datenschutzanforderungen sollten den geltenden Datenschutzgesetzen entsprechen.

7.2 Die Datenschutzprinzipien aus ISO/IEC 29100

Die verantwortliche Stelle ist für den Schutz personenbezogener Daten und den fairen und rechtmäßigen Umgang mit ihnen zu jeder Zeit und in der gesamten Organisation verantwortlich, ebenso wie für die Verarbeitung personenbezogener Daten, die an Auftragsdatenverarbeiter ausgelagert wurden.

Die verantwortliche Stelle ist letztendlich für die Umsetzung von Steuerungsmaßnahmen für den Datenschutz in einem IKT-System verantwortlich. Steuerungsmaßnahmen für den Datenschutz sollen sicherstellen, dass die für eine bestimmte betroffene Person, Transaktion oder ein bestimmtes Szenario festgelegten Datenschutzanforderungen berücksichtigt und konsequent erfüllt werden. Der Nachweis der Umsetzung sollte durch eine ordnungsgemäße Dokumentation der vorhandenen Steuerungsmaßnahmen für den Datenschutz und die Bereitstellung von Audit-Dokumenten erbracht werden, die verifizieren, dass die Maßnahmen bestehen, dass sie korrekt umgesetzt wurden und dass sie ordnungsgemäß funktionieren. Letztendlich sollte die verantwortliche Stelle die Datenschutzprinzipien, die in ISO/IEC 29100 beschrieben sind, akzeptieren und einhalten.

- a) Einwilligung und Wahlfreiheit;
- b) Zulässigkeit des Zwecks und Zweckbestimmung;
- c) Beschränkung der Erhebung;
- d) Datensparsamkeit;
- e) Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung;
- f) Genauigkeit und Qualität;
- g) Offenheit, Transparenz und Benachrichtigung;
- h) persönliche Teilnahme und Zugang;
- i) Verantwortlichkeit;
- j) Informationssicherheit; und
- k) Einhaltung der Datenschutzpflichten.

7.3 Datenschutzanforderungen

IKT-Systeme sollten Steuerungsmaßnahmen für den Datenschutz als Hauptbestandteil in jeder Phase des Lebenszyklus der Verarbeitung von pbD einführen. Die Datenschutzanforderungen ermöglichen es dem Entwickler des IKT-Systems, die Verbindung zwischen den Datenschutzprinzipien und den in Abschnitt 8 festgelegten Architekturkomponenten zu operationalisieren.

Um effektive Steuerungsmaßnahmen für den Datenschutz in einem IKT-System zu implementieren, sollten Verarbeitungsabläufe für pbD erstellt werden, die die Verarbeitung von pbD beschreiben. Verarbeitungsablaufdiagramme für personenbezogene Daten sind eine grafische Darstellung des „Flusses“ von personenbezogenen Daten durch das IKT-System und zwischen den verschiedenen Akteuren. Wenn z. B. ein Akteur personenbezogene Daten an andere Akteure (z. B. Auftragsdatenverarbeiter) überträgt, sollte das Verarbeitungsablaufdiagramm für personenbezogene Daten diese Übertragungen enthalten.

Ein Verarbeitungsablaufdiagramm für personenbezogene Daten kann auch als Ablauftabelle für pbD dargestellt werden. Dieses Diagramm oder diese Tabelle verfolgt die Erhebung, Übertragung, Verwendung, Speicherung oder Entsorgung von personenbezogenen Daten und enthält Informationen wie z. B. die Art der personenbezogenen Daten, wer die personenbezogenen Daten erhoben hat, den Zweck der Verarbeitung, an wen die personenbezogenen Daten übertragen werden, den Erhalt der Einwilligung der betroffenen Person, die Aufbewahrungsfrist und den Ort, an dem sie gespeichert werden, sowie die daraus resultierende Datenschutzrisikostufe. Die Verarbeitungsablaufinformationen für pbD sind ein Input für den Datenschutz-Risikomanagementprozess, der die Datenschutzanforderungen erzeugt.

Nachdem die Anforderungsanalyse eines IKT-Systems abgeschlossen ist, sollten die Entwickler die Datenschutzanforderungen des IKT-Systems mit der Liste der Bedenken in diesem Dokument abgleichen. Die Datenschutzanforderungen sollten dann für die Auswahl der Architekturkomponenten verwendet werden, die besagte Anforderungen erfüllen.

Anhang A enthält eine Beispielliste von Bedenken und veranschaulicht, wie Bedenken mit den Datenschutzprinzipien aus ISO/IEC 29100 und den Architekturkomponenten dieses Dokuments verknüpft werden können.

8 Architekturansichten

8.1 Allgemeines

Die Architekturansichten in diesem Abschnitt sind in drei Ansichten gegliedert. Zunächst werden in der Komponentenansicht die IKT-Systemkomponenten detailliert beschrieben und anhand ihrer Funktionalität in Schichten aufgeteilt. Jede Schicht gruppiert Komponenten, die zur ordnungsgemäßen Verarbeitung von personenbezogenen Daten beitragen. Für jede Komponente werden begrenzte Umsetzungsleitlinien bereitgestellt. Gegebenenfalls werden akteursbezogene Leitlinien angegeben. Diese Ansicht ist hilfreich für das Verständnis der Bausteine im Architekturrahmenwerk für Datenschutz.

In der Komponentenansicht finden sich Tabellen mit Beispielen für typische Beziehungen zwischen den Datenschutzprinzipien aus ISO/IEC 29100 und den Komponenten der Architektur. Solche Zuordnungstabellen sind hilfreich, um zu verstehen, wie ein IKT-System die Datenschutzprinzipien aus ISO/IEC 29100 einhält. Ähnliche Tabellen können als Beispiele verwendet und während der Systemgestaltung aktualisiert werden, um zu beschreiben, wie ein bestimmtes IKT-System die Datenschutzprinzipien aus ISO/IEC 29100 einhält.

Die Akteursansicht betrachtet die in der Komponentenansicht beschriebenen Komponenten aus der Perspektive des IKT-Systems eines einzelnen Akteurs. Diese Ansicht ist hilfreich bei der Gestaltung der Architektur eines bestimmten IKT-Systems. Die Interaktionsansicht betrachtet die Komponenten aus der Perspektive der Bereitstellung. Diese Ansicht ist hilfreich für das Verständnis, wie die Komponenten in den IKT-Systemen der verschiedenen Akteure miteinander interagieren.

8.2 Komponentenansicht

8.2.1 Allgemeines

Die Komponentenansicht ist dazu gedacht, IKT-Systemkomponenten zu beschreiben, die an der Verarbeitung personenbezogener Daten beteiligt sind.

Die Auswahl der Komponenten sollte sich an den entsprechenden Datenschutzanforderungen orientieren. Der Entwickler des IKT-Systems für einen bestimmten Akteur (siehe Bild 2) sollte die Komponentenansicht verwenden, um die Komponenten zu bestimmen, die in die Architektur des von ihm zu entwickelnden Systems aufgenommen werden müssen. Diese Architektur sollte auf den Datenschutzanforderungen basieren, die unter Verwendung der in Abschnitt 7 angegebenen Leitlinien festgelegt wurden. Es ist zu beachten, dass nicht alle in diesem Dokument beschriebenen Komponenten notwendigerweise in einem bestimmten IKT-System angemessen sind.

Die Komponentenansicht wird in drei Schichten dargestellt. Jede Schicht ist eine logische Gruppe von Komponenten, die zu einem bestimmten Ziel bei der Verarbeitung von personenbezogenen Daten beitragen. Die Komponenten in der Schicht für die Datenschutzeinstellungen regeln die Verwaltung von Metadaten über die Verarbeitung personenbezogener Daten, u. a. den Austausch von Informationen über den Zweck der Verarbeitung, die Einwilligung und die Präferenzen der betroffenen Person. Die Komponenten in der Schicht für die Identitäts- und Zugangsverwaltung sind dafür verantwortlich, dass bei der Verarbeitung personenbezogener Daten die richtigen Identitätsinformationen verwendet werden und der Zugriff auf die personenbezogenen Daten entsprechend den Datenschutzanforderungen gesteuert wird. Schließlich führen die Komponenten in der Schicht der personenbezogenen Daten verschiedene Aufgaben zur Verarbeitung der personenbezogenen Daten aus.

Das Architekturrahmenwerk ist unter der Annahme gestaltet, dass alle Komponenten mit mehreren anderen Komponenten interagieren. Um die Allgemeinheit und die Lesbarkeit zu erhalten, wurden jedoch die möglichen Interaktionen zwischen den Komponenten in der Darstellung weggelassen.

Einige der Komponenten im Architekturrahmenwerk sind Technologien zum Datenschutz (PET). Diese Auswahl an PET ist nicht vollständig. Es gibt weitere PET, die in diesem Dokument nicht beschrieben werden. Der Entwickler des IKT-Systems ist dafür verantwortlich, geeignete PET auszuwählen und sie an dieses Architekturrahmenwerk anzupassen.

Anhang B führt ein Beispiel für eine IKT-Systemarchitektur an, die PET für die sichere Verarbeitung personenbezogener Daten anwendet. Anhang C nennt ein Beispiel für die Verwendung von attributbezogenen Anmeldedaten zum Aufbau eines IKT-Systems, das pseudonymes Identitäts- und Zugriffskontrollmanagement bietet.

Die folgenden Unterabschnitte beschreiben die Schichten, die darin enthaltenen Komponenten und die Akteure, die mit den Komponenten interagieren. Es erfolgt eine allgemeine Beschreibung der einzelnen Komponenten mit anschließenden akteurspezifischen Leitlinien. Für manche Komponenten werden keine auf die IKT-Systeme eines bestimmten Akteurs zugeschnittenen Leitlinien angegeben, da das Verhalten der Komponente in den IKT-Systemen aller Akteure ähnlich ist.

8.2.2 Schicht für die Datenschutzeinstellungen

8.2.2.1 Allgemeines

Die Schicht für Datenschutzeinstellungen umfasst Komponenten, die die Datenschutzrichtlinien des Systems an die relevanten Akteure kommunizieren und die Datenschutzanforderungen für das System umsetzen. Diese Komponenten ermöglichen es dem IKT-System, die Datenschutzrichtlinien des Systems zu kommunizieren und die entsprechenden Maßnahmen zum Datenschutz umzusetzen.