

DIN EN ISO/IEC 29101



ICS 35.030

Einsprüche bis 2021-07-21

Entwurf

**Informationstechnik –
Sicherheitstechniken –
Rahmenwerk für Datenschutz (ISO/IEC 29101:2018);
Deutsche und Englische Fassung prEN ISO/IEC 29101:2021**

Information technology –
Security techniques –
Privacy architecture framework (ISO/IEC 29101:2018);
German and English version prEN 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 et anglaise prEN ISO/IEC 29101:2021

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2021-05-21 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 106 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) erarbeitet und als prEN 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).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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*

Titel de: Informationstechnik — Sicherheitstechniken — Rahmenwerk für
Datenschutz (ISO/IEC 29101:2018)

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

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

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	10
6.2.1 Erhebung	10
6.2.2 Übertragung	11
6.2.3 Verwendung	12
6.2.4 Speicherung	12
6.2.5 Entsorgung	13
7 Bedenken	13
7.1 Übersicht	13
7.2 Die Datenschutzprinzipien aus ISO/IEC 29100	13
7.3 Datenschutzanforderungen	14
8 Architekturansichten	15
8.1 Allgemeines	15
8.2 Komponentenansicht	15
8.2.1 Allgemeines	15
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	30
8.3.1 Allgemeines	30
8.3.2 IKT-System der betroffenen Person	31
8.3.3 IKT-System der verantwortlichen Stelle	31
8.3.4 IKT-System des Auftragsdatenverarbeiters	32
8.4 Interaktionsansicht	33
8.4.1 Allgemeines	33
8.4.2 Schicht für die Datenschutzeinstellungen	34
8.4.3 Schicht für Identitäts- und Zugangsverwaltung	34
8.4.4 Schicht der personenbezogenen Daten	34
Anhang A (informativ) Beispiele für die pbD-bezogenen Bedenken eines IKT-Systems	36
A.1 Allgemeines	36
A.2 Einholung und Kommunikation der Einwilligung	36
A.3 Übermittlung des Zwecks für die Erhebung der personenbezogenen Daten	37

A.4	Sichere Verarbeitung personenbezogener Daten	37
A.5	Klassifizierung und Steuerungsmaßnahmen für personenbezogene Daten.....	38
A.6	Verbuchung und Audit von pbD-Vorgängen.....	38
A.7	Archivierung und Entsorgung personenbezogener Daten.....	39
A.8	Zusammenhang mit Datenschutzprinzipien	41
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 prEN ISO/IEC 29101:2021 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 29101:2018 wurde von CEN als prEN 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, *Security techniques*, 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 Datenschutzanforderungen als gleichbedeutend mit den Anforderungen an den Schutz personenbezogener Daten/der Privatsphäre verstanden und unterliegen der Gesetzgebung zum Schutz personenbezogener Daten/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 gilt für Einheiten, die sich mit der Festlegung, Beschaffung, dem Aufbau, der Gestaltung, der Prüfung, Aufrechterhaltung, Verwaltung und dem Betrieb von pbD verarbeitenden IKT-Systemen befassen.

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 werden.

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 Betroffenen, Verantwortlichen und anderen Interessengruppen des Datenschutzes. 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:

- 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;
- 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
- 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.

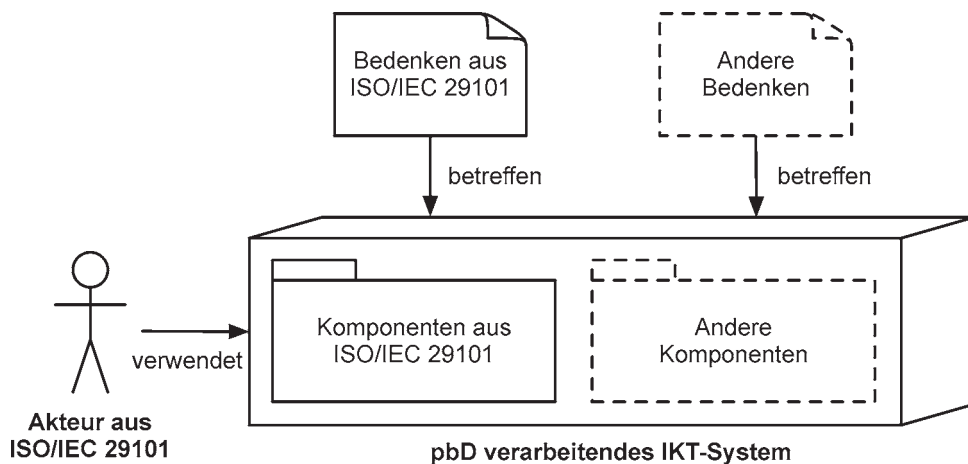


Bild 1 — Elemente des Architekturrahmenwerks für Datenschutz im Kontext

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 Bauteile, der Organisation oder der Eigentumsverhältnisse der IKT-Systemhardware gedacht.

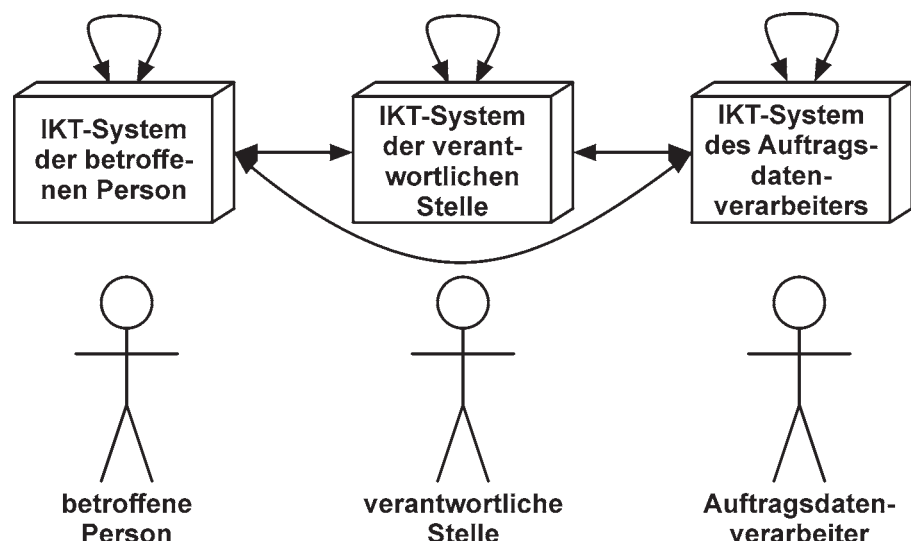


Bild 2 — Akteure und ihre IKT-Systeme nach diesem Dokument

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 Benutzungsschnittstelle (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 eingegeben werden sollen 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 Datenschutzanforderungen 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 verarbeitet werden sollen, 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 Datenschutzerfordernngen

IKT-Systeme sollten Steuerungsmaßnahmen für den Datenschutz als Hauptbestandteil in jeder Phase des Lebenszyklus der Verarbeitung von pbD einführen. Die Datenschutzerfordernngen 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 Datenschutzerfordernngen erzeugt.

Nachdem die Anforderungsanalyse eines IKT-Systems abgeschlossen ist, sollten die Entwickler die Datenschutzerfordernngen des IKT-Systems mit der Liste der Bedenken in diesem Dokument abgleichen. Die Datenschutzerfordernngen 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.

Darüber hinaus sollten die Komponenten in dieser Schicht der verantwortlichen Stelle und dem Auftragsdatenverarbeiter alle Datenschutzpräferenzen und Einwilligungsinformationen übermitteln, die von der betroffenen Person erhoben wurden.

8.2.2.2 Kommunikation von Richtlinie und Zweck

- Allgemeines: Diese Komponente ist für die Weitergabe von Informationen, einschließlich Aktualisierungen, über die Datenschutzrichtlinie der verantwortlichen Stelle und den Zweck der Erhebung von personenbezogenen Daten an die IKT-Systeme der Datenschutz-Akteure verantwortlich.

Die übermittelten Informationen sollten mindestens Folgendes enthalten:

- a) die Identitäten der verantwortlichen Stellen und aller zugehörigen Auftragsdatenverarbeiter;
- b) Richtlinien bezüglich der Übertragung von pbD an Auftragsdatenverarbeiter;
- c) die Verwendung von Technologien zum Datenschutz (z. B. Anonymisierung) mit ihren jeweiligen Zielen;
- d) die Zwecke, für die die pbD erhoben werden;
- e) Identifizierung der zu erhebenden pbD; und
- f) die gesetzlichen Rechte der betroffenen Person, auf ihre personenbezogenen Daten zuzugreifen, um den Umfang der gespeicherten pbD zu bestimmen und um etwaige Ungenauigkeiten zu überprüfen und zu korrigieren, sowie die Verfahren, um dies zu tun.

- Betroffene Person: Die Kommunikationskomponente für Richtlinie und Zweck des IKT-Systems der betroffenen Person sollte
 - a) Informationen zu Richtlinien und Zweck aus der entsprechenden Komponente im IKT-System der verantwortlichen Stelle erhalten,
 - b) die erhaltenen Informationen bearbeiten und der betroffenen Person deren Bedeutung anzeigen oder sie ihr auf andere Weise in klar verständlicher Weise vermitteln,
 - c) der betroffenen Person die Möglichkeit bieten, die empfangenen Informationen lokal zu speichern, und
 - d) der verantwortlichen Stelle bestätigen, dass die Informationen über die Richtlinie und den Zweck bei der betroffenen Person eingegangen sind.
- Verantwortliche Stelle: Die Kommunikationskomponente für Richtlinie und Zweck eines IKT-Systems unter der Kontrolle der verantwortlichen Stelle sollte
 - a) Informationen über Richtlinien und Zwecke speichern, die den betroffenen Personen übermittelt wurden,
 - b) die Handlungen der Übermittlung von Informationen über Richtlinien und Zwecke an Betroffene so protokollieren, dass festgestellt werden kann, welche Informationen aktuell waren und zu welchem Zeitpunkt sie an Betroffene übermittelt wurden, zusammen mit einer Bestätigung des Empfangs dieser Informationen,
 - c) die aktuellen Informationen über Richtlinien und Zwecke an die entsprechende Komponente des IKT-Systems der betroffenen Person in einer solchen Weise übermitteln, dass sie von diesem System direkt verwendet werden kann, um die betroffene Person vollständig und verständlich zu informieren, oder dass sie von dieser Komponente durch eine vordefinierte Zuordnung in eine solche Form gebracht werden kann,
 - d) eine Verweisung auf die angezeigten Informationen zu Richtlinien und Zwecken an die Komponenten übermitteln, die die Speicherung von Einwilligungsinformationen und die Speicherung von personenbezogenen Daten selbst vornehmen, und
 - e) Aktualisierungen über Änderungen von Informationen zu Richtlinien und Zwecken an die entsprechenden Komponenten der IKT-Systeme übermitteln, die denjenigen Betroffenen gehören, die in den Erhalt solcher Informationen eingewilligt haben.
- Auftragsdatenverarbeiter: Das IKT-System des Auftragsdatenverarbeiters sollte üblicherweise digitale Kopien der Datenschutzrichtlinie und des Verarbeitungszwecks vom IKT-System der verantwortlichen Stelle erhalten. Das IKT-System des Auftragsdatenverarbeiters sollte die von der verantwortlichen Stelle erhaltene Datenschutzrichtlinie und die Dokumentation des Verarbeitungszwecks in einer klar verständlichen Form für jeden darstellen, der Zugang zu personenbezogenen Daten hat, die unter diese Richtlinie fallen.

Die verantwortliche Stelle kann die Verarbeitung von personenbezogenen Daten durch verschiedene Auftragsdatenverarbeiter veranlassen. Die Kommunikationskomponente für den Zweck im IKT-System der verantwortlichen Stelle sollte den Zweck, der mit den bereitgestellten personenbezogenen Daten verbunden ist, an alle relevanten Auftragsdatenverarbeiter übermitteln. Jeder Auftragsdatenverarbeiter sollte über den/die Zweck(e) der Verarbeitung personenbezogener Daten informiert werden.

8.2.2.3 Kategorisierung personenbezogener Daten

- Allgemeines: Ein IKT-System, das personenbezogene Daten verarbeitet, muss die Kategorien von personenbezogenen Daten, die es verarbeitet, kennen, damit es zwischen verschiedenen Arten von Daten (z. B. sensible personenbezogene Daten, personenbezogene Daten und nicht personenbezogene Daten) unterscheiden kann. Dies ist für Dienste erforderlich, die personenbezogene Daten je nach Kategorie unterschiedlich verarbeiten. Zusätzlich sollte das IKT-System pbD-Werte kennen, die direkte Zuordnungsmerkmale wie Namen und Sozialversicherungsnummern enthalten. Diese Komponente sollte die Funktionen umsetzen, die eine solche Kategorisierung im IKT-System ermöglichen.

Beim Umgang mit nicht personenbezogenen Daten sollte das Risiko der Kombination von nicht personenbezogenen Daten, um eine Identität oder ein Profil eines eindeutigen Benutzers oder zumindest einer ausreichend kleinen Teilmenge von Benutzern abzuleiten, verstanden und bewertet werden.

Alle personenbezogenen Daten sollten korrekt kategorisiert werden, damit sie vom IKT-System entsprechend ihrer ausgeprägten Sensibilität verarbeitet und gespeichert werden können. Wenn personenbezogene Daten unwissentlich erhoben wurden, z. B. durch unaufgeforderte Eingaben, darf dies nicht möglich sein, und es sollten daher Maßnahmen ergriffen werden, um die Möglichkeit der unaufgeforderten Erhebung von personenbezogenen Daten zu minimieren.

Während das IKT-System pbD-Werte erkennen sollte, die direkte Zuordnungsmerkmale wie Namen und Sozialversicherungsnummern enthalten, ist dies bei unaufgefordert erhobenen personenbezogenen Daten unter Umständen nicht möglich.

- Betroffene Person: Das IKT-System der betroffenen Person sollte in der Lage sein, die mit den personenbezogenen Daten verbundene Kategorisierungskennzeichnung zu bestimmen, und sollte die personenbezogenen Daten entsprechend ihrer Kategorie verarbeiten. Die Kategorisierung kann auch verwendet werden, um die personenbezogenen Daten zu identifizieren, die mit Hilfe von Technologien zum Datenschutz geschützt werden sollten (z. B. sensible pbD). Die Komponente zur Kategorisierung von personenbezogenen Daten bietet auch eine weitere Kategorisierung der personenbezogenen Daten in Unterkategorien, sofern Unterkategorien eine Anforderung einer bestimmten Anwendungsdomäne sind.
- Verantwortliche Stelle: Das IKT-System der verantwortlichen Stelle sollte eine umfassende Kategorisierung der in den IKT-Systemen verwendeten personenbezogenen Daten enthalten, die die kategorisierten personenbezogenen Daten verarbeiten. Diese Informationen sollten an Auftragsdatenverarbeiter übermittelt werden. Außerdem kann diese Kategorisierung von den Komponenten für Audit-Protokollierung, pbD-Pseudonymisierung, pbD-Offenlegung und pbD-Archivierung sowie –Aufbewahrung verwendet werden, damit sie bestimmen können, welche Teile der Daten pbD enthalten.
- Auftragsdatenverarbeiter: Das IKT-System des Auftragsdatenverarbeiters sollte in der Lage sein, die Kategorisierung der personenbezogenen Daten in Verbindung mit den empfangenen personenbezogenen Daten zu verarbeiten. Die Informationen sollten bei der Auditierung von personenbezogenen Daten und der sicheren Verarbeitung von personenbezogenen Daten verwendet werden.

8.2.2.4 Einwilligungsmangement

- Allgemeines: Die Einwilligung der betroffenen Person ist eine wichtige Voraussetzung für die Verarbeitung personenbezogener Daten, sofern eine solche Verarbeitung nicht anderweitig gesetzlich zulässig ist.

Diese Komponente übernimmt u. a. die folgenden Aufgaben des Einwilligungsmanagements:

- a) Einholung der Einverständniserklärung der betroffenen Person;
- b) Speicherung von Einwilligungsinformationen in den IKT-Systemen eines Datenschutz-Akteurs;
- c) Herstellung des Zusammenhangs der gespeicherten Einwilligungsdaten mit der Version der Informationen zur Richtlinie und zum Zweck, für die die Einwilligung erteilt wurde;
- d) Überprüfung der Einwilligung vor der Verarbeitung personenbezogener Daten; und
- e) Pflege des Status der Einwilligungsdaten.

Anwendbares Recht kann dazu führen, dass die fehlende oder eingeschränkte von der betroffenen Person ausgedrückte Einwilligung außer Kraft gesetzt wird.

- Betroffene Person: Die verantwortliche Stelle sollte die Einverständniserklärung der betroffenen Person mit Hilfe der Komponente des Einwilligungsmanagements im IKT-System der betroffenen Person einholen. Unter bestimmten Umständen kann die betroffene Person ihre Einwilligung ändern oder zurückziehen, und diese Information sollte an das IKT-System der verantwortlichen Stelle weitergeleitet werden.
- Verantwortliche Stelle: Im IKT-System der verantwortlichen Stelle sollte diese Komponente aktuelle Informationen über den Status der Einwilligung bereithalten. Das IKT-System der verantwortlichen Stelle sollte in der Lage sein, die Einwilligungsdaten abzurufen, zu speichern, zu verwalten und zu pflegen.

Das IKT-System der verantwortlichen Stelle sollte Einwilligungsdaten an andere Parteien im System übermitteln, die sie benötigen. Zusätzlich sollte diese Komponente Aktualisierungen des Einwilligungsstatus der betroffenen Person akzeptieren (z. B. Änderung oder Widerruf der Einwilligung). Das IKT-System der verantwortlichen Stelle sollte diese Informationen bei Bedarf darstellen und weitergeben.

- Auftragsdatenverarbeiter: Das IKT-System des Auftragsdatenverarbeiters sollte die bestehende Einwilligung von allen Betroffenen verifizieren, die mit den ihm zur Verfügung gestellten pbD verbunden sind. Diese Informationen sollten aus dem IKT-System der verantwortlichen Stelle stammen. Vor jeder Verarbeitung sollte das IKT-System des Auftragsdatenverarbeiters sicherstellen, dass es über aktuelle Einwilligungsdaten zu den jeweiligen Betroffenen verfügt. Das IKT-System des Auftragsdatenverarbeiters sollte bereit sein, Änderungen des Einwilligungsstatus zu akzeptieren, wenn solche Änderungen von der verantwortlichen Stelle mitgeteilt werden.

8.2.2.5 Management der Datenschutzpräferenzen

- Allgemeines: In einigen Situationen ist es möglich, dass die betroffene Person ihre Präferenzen hinsichtlich der Verarbeitung ihrer pbD durch eine verantwortliche Stelle oder einen Auftragsdatenverarbeiter ausdrücken kann. In diesen Fällen sollten die jeweiligen IKT-Systeme der Akteure in der Lage sein, diese Präferenzen aufzuzeichnen und sie gegebenenfalls der verantwortlichen Stelle und dem Auftragsdatenverarbeiter mitzuteilen. Die verantwortliche Stelle und der Auftragsdatenverarbeiter sollten in der Lage sein, diese Präferenzen zu verstehen, und sollten diese Präferenzen bei der Verarbeitung personenbezogener Daten so weit wie möglich berücksichtigen.

- Betroffene Person: Wenn die Verarbeitung personenbezogener Daten auf Einstellungen für Datenschutzpräferenzen basiert, sollte der betroffenen Person eine Schnittstelle zur Verfügung gestellt werden, über die sie die für ihren Zweck am besten geeigneten Einstellungen auswählen kann. Dazu können zum Beispiel Einstellungen gehören, die bestimmen, wie das IKT-System personenbezogene Daten verwendet, überträgt oder offenlegt.
- Verantwortliche Stelle: Wenn die betroffene Person irgendwelche Datenschutzpräferenzen angegeben hat, sollte das IKT-System der verantwortlichen Stelle diese Entscheidungen der verantwortlichen Stelle mitteilen.

Das IKT-System der verantwortlichen Stelle sollte die relevanten Datenschutzpräferenzen erfassen, die die betroffene Person aus den verfügbaren Auswahlmöglichkeiten, soweit vorhanden, angegeben hat. Die verantwortliche Stelle sollte diese Informationen auch an alle Parteien weitergeben, die die mit diesen Einstellungen verbundenen pbD verarbeiten.

- Auftragsdatenverarbeiter: Wenn es für die zugewiesenen Aufgaben des Auftragsdatenverarbeiters relevant ist, sollte das IKT-System des Auftragsdatenverarbeiters alle Einschränkungen der Verarbeitung personenbezogener Daten durch die gewählten Datenschutzpräferenzen der betroffenen Person kennen und entsprechend handeln. Diese Informationen und ihre möglichen Aktualisierungen sollten von der verantwortlichen Stelle oder direkt von der betroffenen Person über ihre jeweiligen IKT-Systeme bezogen werden.

8.2.2.6 Beziehung zwischen Datenschutzprinzipien und Komponenten in der Schicht für die Datenschutzeinstellungen

Tabelle 1 zeigt eine beispielhafte Zuordnung von den Datenschutzprinzipien der ISO/IEC 29100 zu den Komponenten der Schicht für die Datenschutzeinstellungen. Ein „X“ in der Tabelle zeigt eine Beziehung zwischen einer Komponente der Schicht und einem Prinzip an. Diese Beziehung ist jedoch nur als Beispiel dargestellt.

Tabelle 1 — Beispiel für die Beziehung zwischen den Datenschutzprinzipien und den Komponenten in der Schicht für Datenschutzeinstellungen

Komponenten	Prinzipien									
	Einwilligung und Wahlfreiheit	Zulässigkeit des Zwecks und Zweckbestimmung	Beschränkung der Erhebung	Datensparsamkeit	Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung	Genauigkeit und Qualität	Offenheit, Transparenz und Benachrichtigung	Persönliche Teilnahme und Zugang	Verantwortlichkeit	Maßnahmen zur Informationssicherheit
Kommunikation von Richtlinie und Zweck	X	X	X	X			X		X	
Kategorisierung personenbezogener Daten			X	X	X					
Einwilligungsmanagement	X	X	X					X		
Management der Datenschutzpräferenzen	X	X	X		X		X			

8.2.3 Schicht für Identitäts- und Zugangsverwaltung

8.2.3.1 Allgemeines

Komponenten in der Schicht der Identitäts- und Zugangsverwaltung helfen, die Akteure dieses Dokuments und ihre IKT-Systeme zu identifizieren und die zugehörigen Identitätsinformationen zu verwalten. Zusätzlich steuern die Komponenten in dieser Schicht, wie die Akteure dieses Dokuments auf personenbezogene Daten zugreifen. Die Komponenten setzen die folgende Funktionalität um:

- a) Verwaltung der Identitäten der Datenschutz-Akteure;
- b) Verwaltung der Identitäten der Akteure, die die IKT-Systeme verwenden;
- c) Bereitstellung dieser Informationen für andere Komponenten in den IKT-Systemen; und
- d) Verwaltung der Zuordnungen zwischen den Hauptidentitäten von personenbezogenen Daten und Pseudonymen für die Pseudonymisierung von personenbezogenen Daten.

Die Schicht für die Identitäts- und Zugangsverwaltung stellt Identitätsinformationen für Komponenten in anderen Schichten bereit, die diese benötigen. Es ist zu beachten, dass dieses Dokument keine Angaben zu den anzuwendenden Verfahren des Identitätsmanagements festlegt.

8.2.3.2 Identitätsmanagementsystem

Allgemeines: Diese Komponente kann mehrere Zwecke haben, die jeweils von einem eigenen Identitätsmanagementsystem umgesetzt werden können.

Erstens kann die Komponente die Identitäten der Betroffenen verwalten, deren personenbezogene Daten im IKT-System verarbeitet werden. Zweitens kann die Komponente die Identitäten der Benutzer der IKT-Systeme verwalten, die personenbezogene Daten verarbeiten. Drittens kann die Komponente die Identitäten der IKT-Systeme der Datenschutz-Akteure verwalten. Dies würde es den IKT-Systemen verschiedener Datenschutz-Akteure ermöglichen, sich bei der Übertragung personenbezogener Daten gegenseitig zu authentifizieren. Diese Aufzählung von Beispielen erhebt keinen Anspruch auf Vollständigkeit.

Mechanismen, um die Art und Genauigkeit der zugrunde liegenden Identitätsinformationen zu behandeln, werden in diesem Dokument nicht definiert. Die Funktionalität der Identitätsmanagementkomponente ist für alle Akteure ähnlich.

8.2.3.3 Pseudonymisierungsschema

- Allgemeines: Wenn Pseudonymisierung in der Verarbeitung personenbezogener Daten verwendet wird, sollten die beteiligten IKT-Systeme über Funktionen zur Verwaltung der einzelnen verwendeten Fälle der Pseudonymisierungsfunktion verfügen.

Die Komponente für das Pseudonymisierungsschema in der Schicht für die Identitäts- und Zugangsverwaltung enthält Informationen über das implementierte Pseudonymisierungsschema und dessen Parameter. Wenn z. B. ein Verschlüsselungsschema verwendet wird, speichert diese Komponente die verwendeten Schlüssel.

Die zugehörige Komponente zur Pseudonymisierung von personenbezogenen Daten in der pbD-Schicht wird verwendet, um die eigentlichen Transformationen an personenbezogenen Daten durchzuführen.

- Betroffene Person: Wenn im IKT-System der betroffenen Person Pseudonymisierung verwendet wird, sollte das System über eine Beschreibung des implementierten Pseudonymisierungsschemas verfügen. Die Pseudonymisierungskomponente in der pbD-Schicht des IKT-Systems der betroffenen Person sollte dann dieses Pseudonymisierungsschema auf personenbezogene Daten anwenden.

- Verantwortliche Stelle: Pseudonymisierungsschemata können vom IKT-System der verantwortlichen Stelle verwaltet werden. In diesem Fall überträgt das IKT-System der verantwortlichen Stelle Informationen über die verwendeten Pseudonymisierungsschemata an die IKT-Systeme der Betroffenen und Auftragsdatenverarbeiter. Dies kann erforderlich sein, um sicherzustellen, dass die pseudonymisierten personenbezogenen Daten aus dem IKT-System der betroffenen Person in den IKT-Systemen der verantwortlichen Stelle und des Auftragsdatenverarbeiters verarbeitet werden können. Es ist auch zu beachten, dass mehrere Instanzen eines Pseudonymisierungsschemas notwendig sein können, um z. B. personenbezogene Daten für verschiedene Auftragsdatenverarbeiter unterschiedlich zu pseudonymisieren.
- Auftragsdatenverarbeiter: Wenn der Auftragsdatenverarbeiter die Pseudonymisierung nach den Anweisungen der verantwortlichen Stelle durchführen muss, muss er auch diese Komponente zur Verwaltung der Schemata umsetzen.

8.2.3.4 Zugangskontrolle

Allgemeines: Zugangskontrollmechanismen sollten sicherstellen, dass der Zugriff auf die Funktionen des IKT-Systems für die Verarbeitung von personenbezogenen Daten nur innerhalb der durch die Datenschutzanforderungen festgelegten Einschränkungen gewährt wird. Wenn z. B. die Erhebung von personenbezogenen Daten bei der betroffenen Person über ein Webformular erfolgt und sich über einen bestimmten Zeitraum erstreckt, sollte der Zugriff auf das Webformular nur während dieses Zeitraums möglich sein. In diesem Beispiel sollte das IKT-System der verantwortlichen Stelle den Zugriff der betroffenen Person auf das pbD-Erfassungsformular beschränken.

Die Funktionalität der Komponente für Zugangskontrolle ist für alle Akteure ähnlich. Die Regeln und Verfahren für die Zugangskontrolle in jedem IKT-System leiten sich aus den Datenschutzanforderungen ab.

8.2.3.5 Authentifizierung

Allgemeines: Die Authentifizierung ist eine wichtige Sicherheitskomponente eines IKT-Systems, das personenbezogene Daten verarbeitet. Sie kann die Vertraulichkeit und Integrität der vom System erhobenen, gespeicherten und verarbeiteten pbD sicherstellen.

Die Authentifizierungskomponente kann mehrere Zwecke haben. Erstens kann sie die Authentifizierung der Benutzer, die das IKT-System bedienen, übernehmen. Zweitens kann sie die gegenseitige Authentifizierung von IKT-Systemen oder deren Komponenten als Teil eines sicheren Zugriffs und Transfers personenbezogener Daten handhaben. Diese Aufzählung von Beispielen erhebt keinen Anspruch auf Vollständigkeit.

Die Regeln und Verfahren, die bei jeder Bereitstellung des IKT-Systems verwendet werden, sollten separat betrachtet werden, wobei die Sicherheitsziele des Akteurs, der das IKT-System nutzt, berücksichtigt werden müssen.

Beispielsweise sollte das IKT-System der betroffenen Person die das System nutzenden Betroffenen authentifizieren. Ebenso sollte das IKT-System der betroffenen Person die verantwortliche Stelle authentifizieren, bevor die personenbezogenen Daten an das IKT-System der verantwortlichen Stelle übertragen werden.

Die Funktionalität der Authentifizierungskomponente ist in den IKT-Systemen aller Akteure ähnlich.

8.2.3.6 Autorisierung

Allgemeines: In IKT-Systemen, in denen der Zugriff jedes Akteurs eingeschränkt ist, sollte ein Autorisierungssystem vorhanden sein. Nur autorisierte Benutzer des IKT-Systems sollten Zugang zu personenbezogenen Daten erhalten. Zum Beispiel können die Betroffenen, auf die die Verarbeitung personenbezogener Daten abzielt, auf die ihnen zugehörigen personenbezogenen Daten zugreifen.

Die Funktionalität der Autorisierungskomponente ist für alle Akteure ähnlich. Die Regeln und Verfahren für die Authentifizierung in jedem IKT-System leiten sich aus den Datenschutzanforderungen ab.

8.2.3.7 Beziehung zwischen Datenschutzprinzipien und Komponenten in der Schicht für Identitäts- und Zugangsverwaltung

Tabelle 2 zeigt eine beispielhafte Zuordnung von den Datenschutzprinzipien der ISO/IEC 29100 zu den Komponenten der Schicht für Identitäts- und Zugangsverwaltung. Ein „X“ in der Tabelle zeigt eine Beziehung zwischen einer Komponente der Schicht und einem Prinzip an. Diese Beziehung ist jedoch nur als Beispiel dargestellt.

8.2.4 Schicht der personenbezogenen Daten

Die Komponenten in der Schicht der personenbezogenen Daten sollten die folgenden Funktionalitäten umsetzen:

- Erhebung und Übertragung personenbezogener Daten;
- Verarbeitung von personenbezogenen Daten, einschließlich sicherer Verarbeitung, und Präsentation;
- Speicherung und Archivierung der personenbezogenen Daten; und
- Auditierung der personenbezogenen Daten und Protokollierung der darauf stattfindenden Transaktionen.

Tabelle 2 — Beispiel für die Beziehung zwischen den Datenschutzprinzipien und den Komponenten in der Schicht für Identitäts- und Zugangsverwaltung

Komponenten	Prinzipien										
	Einwilligung und Wahlfreiheit	Zulässigkeit des Zwecks und Zweckbestimmung	Beschränkung der Erhebung	Datensparsamkeit	Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung	Genauigkeit und Qualität	Offenheit, Transparenz und Benachrichtigung	Persönliche Teilnahme und Zugang	Verantwortlichkeit	Maßnahmen zur Informationssicherheit	Einhaltung
Identitätsmanagement-system					X		X			X	
Pseudonymisierungs-schema				X	X				X	X	
Zugangskontrolle					X	X		X	X	X	
Authentifizierung					X	X		X	X	X	
Autorisierung					X	X		X	X	X	

Dieses Dokument schlägt nur allgemeine Anforderungen an das pbD-Management vor und überlässt die Einzelheiten dem Anwendungsentwickler. Einschlägige Datenschutzvorkehrungen (oder -maßnahmen) sollten ergriffen werden, um das Risiko von Datenschutzverletzungen bei der Verarbeitung personenbezogener Daten zu verringern.

Die Schicht der personenbezogenen Daten verwendet Informationen aus der Schicht für die Datenschutzeinstellungen, um die Maßnahmen in den Datenschutzanforderungen durchzusetzen, die sich auf die Verarbeitung personenbezogener Daten beziehen.

8.2.4.1 pbD-Management

- Allgemeines: Jedes IKT-System, das personenbezogene Daten verarbeitet, sollte bestimmte grundlegende Merkmale für das Management personenbezogener Daten im IKT-System aufweisen. Dazu gehören Eingabe, Zugriff, Aktualisierung und Löschung personenbezogener Daten. Bei Bedarf sollte das IKT-System in der Lage sein, einen kontinuierlichen Prozess zu unterstützen, der die Erhebung und Verarbeitung personenbezogener Daten während der gesamten Lebensdauer des Systems vorsieht.
- Betroffene Person: Der Schwerpunkt der Komponente für das pbD-Management des IKT-Systems der betroffenen Person liegt auf der Erhebung und lokalen Verarbeitung personenbezogener Daten, die von der betroffenen Person erhoben werden.
- Verantwortliche Stelle: Die Komponente für das pbD-Management des IKT-Systems der verantwortlichen Stelle sollte in der Lage sein, personenbezogene Daten mit den IKT-Systemen der Betroffenen (Erhebung personenbezogener Daten) und Auftragsdatenverarbeiter (zur Delegation der Verarbeitung) auszutauschen. Es ist zu beachten, dass die Datenschutzrichtlinie, die Verwendung verschiedener Technologien zum Datenschutz und andere Faktoren die im IKT-System der verantwortlichen Stelle verfügbaren pbD-Managementinstrumente einschränken können. So kann dem IKT-System der verantwortlichen Stelle beispielsweise untersagt werden, personenbezogene Daten hinzuzufügen oder mit anderen Informationen zu verknüpfen.
- Auftragsdatenverarbeiter: Die Komponente für das pbD-Management des IKT-Systems des Auftragsdatenverarbeiters verarbeitet die von der verantwortlichen Stelle erhaltenen personenbezogenen Daten.

8.2.4.2 Übertragung personenbezogener Daten

Allgemeines: Die pbD-Übertragungskomponente ist für den Austausch personenbezogener Daten zwischen den IKT-Systemen der verschiedenen Datenschutz-Akteure zuständig. Die Übertragung personenbezogener Daten sollte eine gegenseitige Authentisierung und Verschlüsselung zwischen dem Quell- und Zielpunkt beinhalten, um die Übertragung personenbezogener Daten zu schützen und ihre Vertraulichkeit sicherzustellen. In diesem Fall sollte die pbD-Übertragungskomponente die Komponenten „Authentifizierung“ und „Verschlüsselung personenbezogener Daten“ verwenden.

8.2.4.3 Validierung personenbezogener Daten

- Allgemeines: Die zu verarbeitenden personenbezogenen Daten sollten auf die Genauigkeit der Daten und die Korrektheit des Formats validiert werden. Die Komponente sollte über ausreichende Informationen zum Datenmodell und zum Bereich der zulässigen Werte verfügen, um den Datenschutz-Akteur, der das IKT-System nutzt, vor möglichen Fehlern bei der Eingabe von personenbezogenen Daten zu warnen.
- Betroffene Person: Das IKT-System der betroffenen Person führt eine Validierung der von der betroffenen Person oder den Betroffenen mittels IKT-System erhobenen Daten durch.
- Verantwortliche Stelle: Selbst wenn das IKT-System der betroffenen Person dazu bestimmt ist, eine Validierung der personenbezogenen Daten durchzuführen, sollte das IKT-System der verantwortlichen Stelle dasselbe tun und möglicherweise zusätzliche Prüfungen durchführen, um die Genauigkeit der Daten und die Korrektheit des Formats der personenbezogenen Daten sicherzustellen. Das IKT-System der verantwortlichen Stelle kann auch globale Prüfungen auf Ausreißer und statistische Abweichungen durchführen.

- Auftragsdatenverarbeiter: Das IKT-System des Auftragsdatenverarbeiters sollte ähnliche Aufgaben wie das IKT-System der verantwortlichen Stelle erfüllen.

8.2.4.4 Pseudonymisierung personenbezogener Daten

- Allgemeines: Die Pseudonymisierungskomponente in der Schicht der personenbezogenen Daten verwendet ein Pseudonymisierungsschema, wie in der Schicht für die Identitäts- und Zugangsverwaltung beschrieben, um die Zuordnungsmerkmale, die die wahre Identität der Betroffenen offenbaren, durch Pseudonyme zu ersetzen, die die wahren Identitäten verbergen.

Der andere Weg, um die Ziele der Pseudonymisierung zu erreichen, kann oft durch eine Teil-anonymisierung der Informationen erreicht werden.

Beispiele dafür, wann Pseudonymisierung verwendet werden kann, sind Fälle, in denen

- a) die Identität der betroffenen Person nicht erforderlich ist, um die Ziele der Verarbeitung personenbezogener Daten zu erreichen, und
 - b) das pseudonyme Zuordnungsmerkmal für die Verarbeitung personenbezogener Daten erforderlich ist (z. B. zur Verknüpfung mehrerer Datenbanken oder zur Re-Identifizierung einer Person).
- Betroffene Person: Das IKT-System der betroffenen Person führt eine Pseudonymisierung an den erhobenen personenbezogenen Daten durch, bevor diese an das IKT-System der verantwortlichen Stelle gesendet werden.
 - Verantwortliche Stelle: Die Pseudonymisierungskomponente im IKT-System der verantwortlichen Stelle kann für die Verarbeitung der pseudonymisierten Identitäten bei personenbezogenen Daten verwendet werden, die vom IKT-System der betroffenen Person erhalten wurden. Wenn das Pseudonymisierungsschema auf einer Zwei-Wege-Funktion basiert, die von der betroffenen Person und der verantwortlichen Stelle gemeinsam genutzt wird, dann kann letztere die personenbezogenen Daten bei Bedarf auch re-identifizieren. Das IKT-System der verantwortlichen Stelle kann auch Pseudonymisierung auf personenbezogene Daten anwenden, die an das IKT-System des Auftragsdatenverarbeiters übertragen werden. Bei der Offenlegung personenbezogener Daten gegenüber verschiedenen Akteuren sollten unterschiedliche oder unterschiedlich parametrisierte Pseudonymisierungsfunktionen verwendet werden.

Wenn die personenbezogenen Daten z. B. an die IKT-Systeme mehrerer Auftragsdatenverarbeiter übertragen werden, sollten für die an die einzelnen Auftragsdatenverarbeiter übergebenen personenbezogenen Daten unterschiedliche Pseudonymisierungsfunktionen verwendet werden, um das Risiko geheimer Absprachen zwischen den Auftragsdatenverarbeitern zu verringern. Die verantwortliche Stelle führt ein Register der Auftragsdatenverarbeiter und ihrer jeweiligen Pseudonymisierungsschlüssel. Darüber hinaus sollte jedes Ereignis der Offenlegung personenbezogener Daten von beiden Seiten der Offenlegungstransaktion protokolliert werden — in den IKT-Systemen sowohl der verantwortlichen Stelle als auch des Auftragsdatenverarbeiters.

- Auftragsdatenverarbeiter: Das IKT-System des Auftragsdatenverarbeiters kann eine Pseudonymisierung durchführen, wenn es von der verantwortlichen Stelle dazu angewiesen wird.

8.2.4.5 Anonymisierung personenbezogener Daten

Allgemeines: Der Anonymisierungsprozess übernimmt personenbezogene Daten und löscht alle persönlichen Zuordnungsmerkmale oder verändert sie auf andere Weise irreversibel, so dass eine betroffene Person nicht mehr direkt oder indirekt von der verantwortlichen Stelle allein oder in Zusammenarbeit mit einer anderen Partei identifiziert werden kann

Beispiele für Anonymisierungsverfahren umfassen:

- a) Verallgemeinerung der personenbezogenen Daten, wodurch die Informationen unpräziser werden, z. B. Gruppierung kontinuierlicher Werte oder Ersetzen kategorischer Werte durch allgemeinere Begriffe;
- b) Unterdrückung der personenbezogenen Daten — Löschen eines gesamten Datensatzes oder bestimmter Teile von Datensätzen, die ihn identifizierbar machen würden;
- c) Einbringen von Störfaktoren in die personenbezogenen Daten — Hinzufügen von kleinen Abweichungen in ausgewählten Informationsfeldern wie Gewicht, Größe oder Alter;
- d) Vertauschen der personenbezogenen Daten — Austausch bestimmter pbD-Felder eines Datensatzes mit denselben pbD-Feldern eines anderen ähnlichen Datensatzes (z. B. Vertauschen der Postleitzahlen zweier Datensätze); und
- e) Ersetzen der personenbezogenen Daten durch den Durchschnittswert — Ersetzen jedes Wertes der personenbezogenen Daten innerhalb der geclusterten Datensätze durch den Durchschnittswert für die gesamte Gruppe der personenbezogenen Daten.

Es gibt Verfahren, die eine Möglichkeit zur Re-Identifizierung der mit den Daten verbundenen betroffenen Person zulassen. Solche Verfahren sind für die Anwendung in dieser Komponente nicht geeignet. Darüber hinaus gibt es Anonymisierungsverfahren, die personenbezogene Daten versehentlich so umwandeln können, dass sie eine andere betroffene Person identifizieren. Die Qualität des verwendeten Anonymisierungsverfahrens sollte bewertet werden, bevor es in die Gestaltung des IKT-Systems einbezogen wird.

Personenbezogene Daten können durch das IKT-System eines jeden Datenschutz-Akteurs anonymisiert werden, bevor sie an die IKT-Systeme anderer Datenschutz-Akteure übertragen werden.

8.2.4.6 Secret Sharing (Geheimnisteilung)

- Allgemeines: Secret Sharing ist ein Verfahren zur Aufteilung von pbD-Werten in Teilmengen, die einzeln keine Informationen über den ursprünglichen Wert erkennen lassen. Secret Sharing kann für die Erhebung personenbezogener Daten verwendet werden, um das Risiko einer Datenschutzverletzung zu verringern. Secret Sharing bietet einen besseren Datenschutz, wenn es auf dem IKT-System der betroffenen Person durchgeführt und in Verbindung mit einer sicheren Mehrparteienberechnung verwendet wird.

Secret Sharing kann verwendet werden, um das Risiko von Insiderangriffen zu verringern, da eine Partei mit Zugriff auf eine Teilmenge eines pbD-Wertes den ursprünglichen Wert nicht in Erfahrung bringen kann. Dies macht Insider-Angriffe deutlich komplexer. Um optimale Ergebnisse zu erzielen, erfordert Secret Sharing, dass es mehr als eine Instanz jedes Akteurs im System gibt. Jede Instanz sollte eine begrenzte Anzahl von Teilmengen speichern und verarbeiten.

- Betroffene Person: Das IKT-System der betroffenen Person kann Secret Sharing mit den von Betroffenen erhobenen personenbezogenen Daten durchführen. Die sich daraus ergebenden Teilmengen werden dann an die verantwortlichen Stellen übertragen.
- Verantwortliche Stelle: Das IKT-System der verantwortlichen Stelle kann Secret Sharing verwenden, um vom IKT-System der betroffenen Person eingegangene Teilmengen von pbD zu verarbeiten oder um Secret Sharing an reinen pbD durchzuführen, bevor diese an das IKT-System des Auftragsdatenverarbeiters übertragen werden.
- Auftragsdatenverarbeiter: Das IKT-System des Auftragsdatenverarbeiters kann Secret Sharing für einen von zwei Zwecken verwenden. Der erste besteht darin, dass die Teilmengen der pbD vor der Verarbeitung gespeichert oder geladen werden. In diesem Fall werden die personenbezogenen Daten in

Form von Teilmengen gespeichert, aber vor der Verarbeitung rekonstruiert. Der zweite besteht darin, sie in Verbindung mit sicherer Mehrparteienberechnung zu verwenden. In diesem Fall ist es möglich, Berechnungen direkt an Teilmengen der pbD durchzuführen.

8.2.4.7 Verschlüsselung personenbezogener Daten

Allgemeines: pbD-Verschlüsselungskomponenten sollten Mechanismen zur Verschlüsselung von personenbezogenen Daten bieten, bevor diese gespeichert werden. Bei der Gestaltung eines IKT-Systems sollte auch festgelegt werden, welche gespeicherten personenbezogenen Daten verschlüsselt werden müssen. Je nach Datenschutzanforderungen können die Kodierungsschlüssel von den IKT-Systemen gemeinsam genutzt werden, so dass jedes von ihnen die personenbezogenen Daten entschlüsseln und entsprechend darauf zugreifen kann. Wenn ein sicheres Berechnungsverfahren verwendet wird, das in der Lage ist, verschlüsselte personenbezogene Daten zu verarbeiten, müssen die Informationen nicht entschlüsselt werden, um verarbeitet zu werden.

Die Komponentendienste umfassen die Schlüsselverwaltung, die Verschlüsselung von personenbezogenen Daten innerhalb von Datenbanken und die Verschlüsselung gespeicherter personenbezogener Daten wie Backup-Dateien und Archive.

Die Verschlüsselung personenbezogener Daten kann zum Schutz gespeicherter personenbezogener Daten verwendet werden. Dies kann zu zwei Zwecken geschehen. Erstens kann man personenbezogene Daten verschlüsselt speichern, um unbefugten Zugriff darauf zu verhindern. Wenn sie verarbeitet werden müssen, werden sie mit dem entsprechenden Entschlüsselungscode entschlüsselt. Die Verschlüsselung personenbezogener Daten reduziert das Sicherheitsrisiko von Datenverletzungen durch Backups. Die zur Verschlüsselung verwendeten Schlüssel sollten getrennt von den verschlüsselten personenbezogenen Daten aufbewahrt werden.

Zusätzlich können personenbezogene Daten verschlüsselt werden, um sie für die Verarbeitung in verschlüsselter Form vorzubereiten, wobei sichere Berechnungsverfahren wie die homomorphe Verschlüsselung verwendet werden.

In allen Fällen sollten geeignete Schlüssellängen so definiert werden, dass aktuelle und zukünftige Rechnerkapazitäten diesen Schlüssel nicht brechen können.

8.2.4.8 Nutzung personenbezogener Daten

Allgemeines: Um personenbezogene Daten in Berechnungen oder Analysen verwenden zu können, sollte das IKT-System des Akteurs eine Komponente zur Nutzung personenbezogener Daten einsetzen. Diese Komponente realisiert die Geschäftslogik der pbD-Verarbeitung. Es ist zu beachten, dass einige pbD-Nutzungsszenarien mit sicheren Berechnungen umgesetzt werden können, um das Risiko der Weitergabe personenbezogener Daten zu verringern.

8.2.4.9 Sichere Berechnung

Verantwortliche Stelle und Auftragsdatenverarbeiter: Sichere Berechnungen können verwendet werden, damit verantwortliche Stellen und Auftragsdatenverarbeiter personenbezogene Daten verarbeiten können, ohne Zugriff auf die Eingabewerte zu haben. Stattdessen führen sichere Berechnungsverfahren Berechnungen mit personenbezogenen Daten durch, die durch Technologien zum Datenschutz wie Verschlüsselung oder Secret Sharing umgewandelt wurden.

Eine Teilmenge der sicheren Berechnungsverfahren, bekannt als sichere Mehrparteienberechnung, ist ein Verfahren, bei dem mehrere Parteien gemeinsam einen Wert auf der Grundlage von individuell gehaltenen geheimen Informationsteilen berechnen können, ohne diese Geheimnisse dabei gegenseitig aufzudecken. Für einen optimalen Schutz vor Datenschutzverletzungen sollte eine sichere Mehrparteienberechnung mehrere verantwortliche Stellen oder Auftragsdatenverarbeiter und deren IKT-Systeme mit ihren jeweiligen geheimen Informationen umfassen

Sichere Berechnungen können das Risiko von pbD-Lecks aus dem IKT-System des Akteurs verringern, da personenbezogene Daten dem Datenverarbeiter nicht in eindeutiger Form zur Verfügung gestellt werden.

8.2.4.10 Abfrageverwaltung

Allgemeines: Die Komponente zur Abfrageverwaltung des IKT-Systems der verantwortlichen Stelle und/oder des Auftragsdatenverarbeiters wird zur Filterung eingehender Anfragen eingesetzt. Zum Beispiel kann ein Dienst die Beantwortung einer statistischen Abfrage verweigern, wenn nicht genügend Eingaben für diese Abfrage vorhanden sind. Obwohl die verweigte Antwort auf eine Abfrage immer noch einige Informationen für den abfragenden Datenschutz-Akteur bereitstellt, sollte das Verfahren in bestimmten Szenarien dennoch in Betracht gezogen werden.

Die Abfrageverwaltung ist ein spezielles Verfahren, das in Data-Mining-Anwendungen zur Minimierung der Verarbeitung personenbezogener Daten eingesetzt wird. Dieses Verfahren erleichtert die Bereitstellung von pbD-Analysediensten, ohne den Missbrauch von personenbezogenen Daten zu riskieren und ohne die Präzision der Data-Mining-Algorithmen zu gefährden. Der Prozess der Abfrageverwaltung sollte verwendet werden, um sicherzustellen, dass nur eine für die jeweiligen Prozesse ausreichende personenbezogene Datenmenge verarbeitet wird.

Zu den Verfahren der Abfrageverwaltung gehören die Begrenzung der Größe von Abfrageergebnissen, die Kontrolle der Überlappung zwischen aufeinanderfolgenden Abfragen, das Führen von Audit-Trails aller beantworteten Abfragen und die ständige Überprüfung auf mögliche Datenschutzverletzungen, die Unterdrückung von pbD-Zellen kleiner Größe und das Clustern von Einheiten in sich gegenseitig ausschließende atomare Populationen.

8.2.4.11 Inventarisierung personenbezogener Daten

Allgemeines: Die Komponente für die Inventarisierung personenbezogener Daten bietet eine Übersicht über die im IKT-System gespeicherten personenbezogenen Daten. Die Informationen aus dem pbD-Kategorisierungssystem sollten verwendet werden, um die im System gespeicherten pbD-Werte zu kategorisieren. Das Identitätsmanagementsystem sollte verwendet werden, um die betroffene Person zu ermitteln, die sich auf ein bestimmtes pbD-Element bezieht. Die Komponente für die Inventarisierung personenbezogener Daten sollte in der Lage sein, dem Datenschutz-Akteur, der das IKT-System nutzt, mindestens die folgenden Metriken zur Verfügung zu stellen:

- a) die Menge an personenbezogenen Daten im System (Anzahl der Datensätze, Metadaten über die Datensätze); und
- b) die Anzahl der Betroffenen, die Informationen zur Verfügung gestellt haben.

Abhängig von den Datenschutzanforderungen kann diese Komponente zusätzliche Informationen bereitstellen, wie z. B. die Liste der Betroffenen.

Die Komponente für die Inventarisierung personenbezogener Daten hat bei allen Akteuren eine ähnliche Funktion — sie soll einen Überblick darüber verschaffen, wie viele personenbezogene Daten lokal aufbewahrt werden und wer die jeweiligen Betroffenen sind. Das IKT-System der verantwortlichen Stelle sollte diese Funktionalität erweitern, indem es Aufzeichnungen über die Verarbeitung personenbezogener Daten durch die IKT-Systeme der Auftragsdatenverarbeiter führt. Dies sollte in Zusammenarbeit mit den jeweiligen Komponenten für das pbD-Management und die Archivierung im IKT-System des Auftragsdatenverarbeiters erfolgen.

8.2.4.12 Offenlegung personenbezogener Daten

- Verantwortliche Stelle: Die Komponente zur Offenlegung personenbezogener Daten ist für die Verwaltung der Offenlegung personenbezogener Daten durch die verantwortliche Stelle zuständig. Dies kann die Vorbereitung von personenbezogenen Daten beinhalten, bevor sie das IKT-System der verantwortlichen Stelle verlassen. Beispielsweise kann die verantwortliche Stelle personenbezogene Daten mit der entsprechenden Komponente pseudonymisieren oder anonymisieren, bevor sie sie an einen Auftragsdatenverarbeiter sendet. Die Offenlegung von personenbezogenen Daten erfordert häufig die Verwendung der Komponente zur Übertragung personenbezogener Daten.

Wenn bei der Offenlegung von personenbezogenen Daten eine Pseudonymisierung verwendet wird, sollte das Protokoll auch eine Beschreibung der Pseudonymisierungsfunktion enthalten, die zur Offenlegung der personenbezogenen Daten verwendet wurde. In diesem Fall sollten bei der Offenlegung unterschiedliche Pseudonymisierungsfunktionen verwendet werden, da dies die Verknüpfbarkeit offengelegter Datenbanken einschränkt, indem dasselbe Zuordnungsmerkmal nicht demselben Pseudonym zugeordnet wird.

- Auftragsdatenverarbeiter: Personenbezogene Daten können vom IKT-System des Auftragsdatenverarbeiters auf ähnliche Weise offengelegt werden wie im IKT-System der verantwortlichen Stelle. Eine solche Offenlegung sollte nach den Anweisungen der verantwortlichen Stelle durchgeführt werden.

8.2.4.13 Archivierung und Aufbewahrung personenbezogener Daten

Allgemeines: Wenn personenbezogene Daten nicht aktiv verwendet werden und für die Archivierung vorgesehen sind, sollten sie für die Archivierung vorbereitet werden. Die Komponente zur Archivierung und Aufbewahrung sollte sicherstellen, dass das Archiv ausreichend geschützt ist und dass die Archivierungs- und Aufbewahrungsverfahren eingehalten werden. Verschlüsselung, Secret Sharing und Pseudonymisierung können verwendet werden, um archivierte personenbezogene Daten vor unbefugter Verarbeitung zu schützen. Es ist wichtig zu wissen, welcher Kodierungsschlüssel, welches Secret-Sharing-Schema oder welches Pseudonymisierungsschema während des Prozesses verwendet wurde, um personenbezogene Daten später wiederherstellen zu können.

Wenn die Aufbewahrungsfrist für personenbezogene Daten abgelaufen ist, sollte diese Komponente die Anonymisierung oder sichere Löschung der personenbezogenen Daten aus dem System planen.

8.2.4.14 Audit-Protokollierung

Die Komponente für die Audit-Protokollierung sollte jede mit personenbezogenen Daten durchgeführte Transaktion protokollieren. Diese Komponente sollte mit jeder anderen Komponente integriert werden, damit sie alle relevanten Aktivitäten protokollieren kann.

Die Identität des Akteurs oder der Akteure, die auf personenbezogene Daten zugreifen, pbD-Transaktionen einleiten oder aus pbD-Transaktionen resultierende personenbezogene Daten erhalten, sollte im Transaktionsprotokoll aufgezeichnet werden. Dazu gehört die Integration der Audit-Protokollierung mit den Modulen der Authentifizierung, Autorisierung und pbD-Schicht. Es sollten sichere Protokollierungsverfahren verwendet werden, um eine Manipulation der Protokolleinträge zu verhindern.

8.2.4.15 Beziehung zwischen den Datenschutzprinzipien und den Komponenten der Schicht der personenbezogenen Daten

Tabelle 3 zeigt eine beispielhafte Zuordnung von den Datenschutzprinzipien der ISO/IEC 29100 zu den Komponenten der pbD-Schicht. Ein „X“ in der Tabelle zeigt eine Beziehung zwischen einer Komponente der Schicht und einem Prinzip an. Diese Beziehung ist jedoch nur als Beispiel dargestellt.

Tabelle 3 — Beispiel für die Beziehung zwischen den Datenschutzprinzipien und den Komponenten in der Schicht der personenbezogenen Daten

Komponenten	Prinzipien										
	Einwilligung und Wahlfreiheit	Zulässigkeit des Zwecks und Zweckbestimmung	Beschränkung der Erhebung	Datensparsamkeit	Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung	Genauigkeit und Qualität	Offenheit, Transparenz und Benachrichtigung	Persönliche Teilnahme und Zugang	Verantwortlichkeit	Maßnahmen zur Informationssicherheit	Einhaltung
pbD-Management	X	X	X	X	X		X	X			
Übertragung personenbezogener Daten	X	X		X	X		X	X			
Validierung personenbezogener Daten						X					
Pseudonymisierung personenbezogener Daten				X						X	
Anonymisierung personenbezogener Daten				X						X	
Secret Sharing (Geheimnisteilung)				X						X	
Verschlüsselung personenbezogener Daten				X						X	
Nutzung personenbezogener Daten	X	X		X	X	X	X				
Sichere Berechnung				X						X	
Abfrageverwaltung				X	X					X	
Inventarisierung personenbezogener Daten				X	X		X		X		
Offenlegung personenbezogener Daten	X	X		X	X		X				
Archivierung und Aufbewahrung personenbezogener Daten	X	X		X	X		X				
Audit-Protokollierung									X	X	

8.3 Akteursansicht

8.3.1 Allgemeines

Die Akteursansicht veranschaulicht, wie die Komponenten im Architekturrahmenwerk dieses Dokuments in den IKT-Systemen eines bestimmten Datenschutz-Akteurs eingesetzt werden. Für jeden Akteur gibt die Ansicht eine Teilmenge von Komponenten an, die für die Bereitstellung im IKT-System dieses Akteurs geeignet sind. Der Entwickler verwendet diese Ansicht, um zu entscheiden, welche Komponenten in die Architektur des IKT-Systems eines Datenschutz-Akteurs aufgenommen werden sollten.