EUROPEAN DATA PROTECTION SUPERVISOR

Leitlinien zum Schutz personenbezogener Daten für die Bereiche IT-Governance und IT-Management der EU-Institutionen

März 2018

INHALT

ZUSAMMENFASSUNG

Die Verordnung (EG) Nr. 45/2001 (im Folgenden „Verordnung“) bildet den gesetzlichen Rahmen für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Europäischen Union (EU-Institutionen).

Die EU-Institutionen nutzen Informationssysteme und Datenbanken für verschiedene operative und administrative Aufgaben. In vielen dieser Informationssysteme werden personenbezogene Daten verarbeitet, weshalb es enorm wichtig ist, dass die Systeme der Verordnung in vollem Umfang Rechnung tragen. Darüber hinaus ist in der Datenschutz-Grundverordnung (DSGVO) der Datenschutz durch Technikgestaltung erstmals verbindlich vorgeschrieben. Infolgedessen müssen der Datenschutz und der Schutz der Privatsphäre künftig in die Designvorgaben und Architektur von Informations- und Kommunikationssystemen und -technologien integriert werden. Ähnliche Verpflichtungen kommen auf die Organe und Einrichtungen der EU zu.

Die vorliegenden Leitlinien dienen dazu, den EU-Institutionen praktische Hinweise zur Verarbeitung personenbezogener Daten über den Lebenszyklus eines Informationssystems hinweg zu geben, damit gewährleistet ist, dass die für die Verarbeitung Verantwortlichen ihren gesetzlichen Pflichten nachkommen können. Die Verantwortung für die ordnungsgemäße Verarbeitung personenbezogener Daten gemäß den Datenschutzbestimmungen liegt jedoch weiterhin bei den EU-Institutionen selbst.

Die Leitlinien befassen sich mit den Datenschutzaspekten der Verarbeitung personenbezogener Daten in Informationssystemen.

Sie enthalten 26 Empfehlungen, die die EU-Institutionen dabei unterstützen sollen, ihre Rechenschaftspflicht bei der Entwicklung, beim Betrieb und bei der Pflege der von ihnen verwendeten Informationssysteme und Datenbanken zu verbessern.

Die Liste der in diesen Leitlinien empfohlenen Aktivitäten und Maßnahmen erhebt keinen Anspruch auf Vollständigkeit oder Ausschließlichkeit. Die EU-Institutionen können sich unter Berücksichtigung ihres spezifischen Bedarfs auch für andere, nicht in diesem Dokument aufgeführte Maßnahmen entscheiden, die gleichermaßen wirksam sind. In diesem Fall müssen sie demonstrieren können, auf welche Weise diese Maßnahmen einen gleichwertigen Schutz personenbezogener Daten bieten.

1. EINLEITUNG

1 Diese Leitlinien dienen dazu, die Einrichtungen und Organe der EU (im Folgenden „EU-Institutionen“) beim Entwurf und der Einrichtung eines internen Kontrollsystems[1] für das Management und die Governance ihrer IT-Systeme[2] zu unterstützen, um zu gewährleisten, dass die Prozesse und Systeme über ihren Lebenszyklus hinweg den in der Verordnung (EG) Nr. 45/2001[3] (im Folgenden „Verordnung“) dargelegten rechtlichen Verpflichtungen hinsichtlich der Verarbeitung personenbezogener Daten Rechnung tragen. Die vorliegenden Leitlinien ergänzen die Leitlinien des EDSB zu spezifischen IT-Bereichen, etwa zu mobilen Geräten[4], zu Online-Diensten[5], zu mobilen Apps[6] und zum Cloud-Computing[7].

2 Als unabhängige Aufsichtsbehörde mit Zuständigkeit für die Verarbeitung personenbezogener Daten durch die EU-Institutionen kann der Europäische Datenschutzbeauftragte (EDSB) unter anderem Leitlinien zu bestimmten Themen im Zusammenhang mit der Verarbeitung personenbezogener Daten herausgeben.[8] Die vorliegenden Leitlinien sind das Ergebnis eines Prozesses, in dessen Rahmen die EU-Institutionen konsultiert wurden.

3 Für das Management von IT-Systemen gibt es bewährte Verfahren, nämlich den „Datenschutz durch Technikgestaltung“ und den „Datenschutz durch

[1] Der in diesen Leitlinien verfolgte Ansatz ist mit dem überarbeiteten internen Kontrollrahmen der Europäischen Kommission (C(2017) 2373) vereinbar, der interne Kontrollen in fünf Komponenten und 17 Grundsätze unterteilt. Die Rechenschaftspflicht und das Risikomanagement bilden sowohl für den Kontrollrahmen als auch den Datenschutz zentrale Grundsätze. Für die Bereiche Governance und Management sind prinzipiell zwar alle Grundsätze relevant, IT-gestützte Prozesse werden allerdings vornehmlich in Grundsatz 11, der sich mit der Kontrolle der Technologie- und IT-Sicherheit befasst, und Grundsatz 13, der dem Informations- und Dokumentenmanagement und insbesondere den Datenschutzbestimmungen gewidmet ist, angesprochen.

[2] Die Begriffe „Informationssystem“ und „IT-System“ werden im gesamten Text dieser Leitlinien synonym verwendet.

[3] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8 vom 12.1.2001, S. 1.

[4] Leitlinien zum Schutz personenbezogener Daten auf von den EU-Organen genutzten mobilen Geräten (Leitlinien für mobile Geräte), 17. Dezember 2015.

[5] Leitlinien zum Schutz personenbezogener Daten, die über von den EU-Organen bereitgestellte Online-Dienste verarbeitet werden, 7. November 2016.

[6] Leitlinien zum Schutz personenbezogener Daten, die in von den EU-Organen bereitgestellten mobilen Anwendungen verarbeitet werden, 7. November 2016.

[7] Leitlinien zum Schutz personenbezogener Daten, die in von den EU-Organen bereitgestellten Cloud-Computing-Diensten verarbeitet werden, 16. März 2018.

[8] In Ausübung der Befugnisse gemäß Artikel 41 Absatz 2 und Artikel 46 Buchstabe d der Verordnung.

datenschutzfreundliche Voreinstellungen“, die gewährleisten sollen, dass personenbezogene Daten gemäß den Datenschutzgrundsätzen verarbeitet werden[9].

4 Für die Einrichtung eines wirksamen internen Kontrollsystems ist die Führungsebene einer Institution verantwortlich. Es wird als gute Praxis angesehen, dass die Führungsebene ihre „Rechenschaftspflicht“ dadurch demonstriert, dass sie ihre Pflichten vollumfänglich wahrnimmt.

5 Nach dem Erlass der Datenschutz-Grundverordnung (DSGVO)[10] sind die Grundsätze der Rechenschaftspflicht sowie des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen auch für die EU-Institutionen zunehmend wichtiger geworden, da der Unionsgesetzgeber diese Grundsätze in der DSGVO als rechtliche Verpflichtung verankert und erklärt hat[11], dass auch die Datenschutzvorschriften für die EU-Institutionen entsprechend angepasst werden sollten, damit dieselben Grundsätze angewendet werden, und zwar idealerweise gleichzeitig mit der Verordnung.[12]

6 Es ist unmöglich, in diesen Leitlinien alle Hinweise aufzuführen, die für die Einführung des Datenschutzes durch Technikgestaltung in bestimmten IT-Lösungen nötig sind, da jeder einzelne technische Kontext die Konzeption und Umsetzung konkreter technischer Maßnahmen erfordert. Die Einführung der Rechenschaftspflicht für den Schutz der Privatsphäre und den Datenschutz in die Prozesse des IT-Managements und der IT-Governance ist jedoch unerlässlich, um diesen und anderen Verpflichtungen auch künftig nachkommen zu können.

7 Die Leitlinien sollten von Datenschutzbeauftragten und Datenschutzkoordinatoren oder -ansprechpartnern in jeder EU-Institution, vom IT-Personal und von Mitarbeitern in anderen Dienststellen, die mit der Entwicklung und dem Betrieb von IT-Systemen befasst sind, sowie von allen Personen, die Verantwortung für die EU-Institutionen in ihrer Rolle als für die Verarbeitung Verantwortliche tragen, berücksichtigt werden. Sie

---

[9] Es wird erwartet, dass der Europäische Datenschutzausschuss noch genauere Empfehlungen zu den Grundsätzen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen erarbeiten wird, zu denen auch der EDSB einen Beitrag leisten wird. Überdies plant der EDSB die Veröffentlichung einer Stellungnahme zu künftigen Strategien, um ein umfassenderes Konzept des „eingebauten Datenschutzes“ zu entwickeln.

[10] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S. 1-88.

[11] Erwägungsgrund 17 DSGVO.

[12] Zum Zeitpunkt der Veröffentlichung dieser Leitlinien war das Legislativverfahren zu dem neuen Instrument, das die Verordnung (EG) Nr. 45/2001 ersetzen soll, noch im Gang. Allerdings ist schon jetzt klar, dass die maßgeblichen Bestimmungen der DSGVO auch mit Blick auf die EU-Organe Anwendung finden werden. Die vorliegende Version der Leitlinien verweist, wo immer angemessen, auf die DSGVO. Nach Veröffentlichung der neuen Datenschutzverordnung wird eine aktualisierte Version mit Verweisen auf die neue Verordnung vorgelegt.

helfen der oberen Führungsebene zudem dabei, von höchster Stelle der Organisation aus eine Datenschutzkultur zu fördern.

8 Auch wenn der Zweck dieser Leitlinien darin besteht, den EU-Institutionen die Erfüllung ihrer Pflichten zu erleichtern, liegt die Verantwortung für ihre Anwendung allein in den Händen der EU-Institutionen. Die Liste der in diesen Leitlinien empfohlenen Maßnahmen erhebt keinen Anspruch auf Vollständigkeit oder Ausschließlichkeit. Die Maßnahmen sind flexibel genug gehalten, um den EU-Institutionen zu erlauben, den erwarteten Prozess der Rechenschaftspflicht bereits jetzt einzuleiten und sich gleichzeitig mit Blick auf die Zukunft auf die erwarteten Änderungen der Rechtsvorschriften einzustellen. Die EU-Institutionen können sich unter Berücksichtigung ihres spezifischen Bedarfs auch für andere, nicht in diesem Dokument aufgeführte Maßnahmen entscheiden, die gleichermaßen wirksam sind. Ihre Wirksamkeit ist schriftlich zu begründen.

2. ANWENDUNGSBEREICH UND AUFBAU DER LEITLINIEN

2.1. Anwendungsbereich

9 Die Verordnung definiert die Pflichten der in den EU-Institutionen für die Verarbeitung Verantwortlichen mit Blick auf personenbezogene Daten, die in den EU-Institutionen verarbeitet werden, und gewährt natürlichen Personen auf dem Rechtsweg durchsetzbare Datenschutzrechte.

10 Bei der Verarbeitung personenbezogener Daten in den Informationssystemen der EU müssen die Bestimmungen der Verordnung in vollem Umfang eingehalten werden.

11 Diese Leitlinien enthalten Empfehlungen, die die es den EU-Institutionen ermöglichen sollen, ihre Rechenschaftspflicht für den Datenschutz über den Lebenszyklus ihrer Informationssysteme hinweg, also von der Entwicklung über den Betrieb und die Pflege bis hin zur Entsorgung der bestehenden Systeme, zu erhöhen. Sie unterstützen die Einrichtung eines internen Kontrollsystems für die IT-Governance und das IT-Management, das dem für die Verarbeitung Verantwortlichen hilft, die Verordnung einzuhalten und die Einhaltung der Bestimmungen zu überprüfen und nachzuweisen.

12 Die in diesen Leitlinien vorgeschlagenen Maßnahmen behandeln keine technischen Aspekte der Entwicklung von IT-Systemen für einen bestimmten Zweck oder unter Einsatz einer bestimmten Technologie. Diese Fragen behandelt der EDSB auch weiterhin in themenspezifischen Leitlinien (etwa zu den Bereichen mobile Anwendungen, Online-Dienste, mobile Geräte und Cloud-Computing).

2.2. Aufbau der Leitlinien

13 In Kapitel 1 wird der Zweck der Leitlinien erörtert.

14 In Kapitel 2 sind Anwendungsbereich und Aufbau des Dokuments beschrieben.

15 Kapitel 3 enthält allgemeine Definitionen der Begriffe Rechenschaftspflicht, IT-Governance und IT-Management.

16 Kapitel 4 erläutert den Rechtsrahmen für den Datenschutz und bietet eine Übersicht über die allgemein anerkannten Datenschutzgrundsätze, die während des gesamten Lebenszyklus eines Informationssystems zu berücksichtigen sind.

17 In Kapitel 5 wird erklärt, wie sich die Datenschutzanforderungen in die Lebenszyklen eines Informationssystems einbinden lassen.[13]

[13] Der Lebenszyklus des IT-Systemmodells, das in diesem Dokument als Bezugspunkt verwendet wird, beruht auf dem RUP@EC®- IBM® Rational Unified Process®.

3. ZENTRALE KONZEPTE: IT-GOVERNANCE, IT-MANAGEMENT, RECHENSCHAFTSPFLICHT

3.1. IT-Governance und IT-Management

18 Die Begriffe „IT-Governance“ und „IT-Management“ beziehen sich auf zentrale Funktionsbereiche in einer Organisation. Die Funktionsträger müssen sicherstellen, dass die IT-Umgebung der Organisation deren Ziele unterstützt.

19 *Das von der ISACA[14] eingerichtete IT Governance Institute (ITGI)* definiert IT-Governance wie folgt:

> *Die IT-Governance liegt in der Verantwortung des Aufsichtsrats und der Geschäftsleitung. Sie ist integraler Bestandteil der Unternehmensführung und setzt sich aus den Führungs- und Organisationsstrukturen und -prozessen zusammen, die gewährleisten, dass die IT-Systeme der Organisation deren Strategien und Ziele unterstützen und erweitern.*

20 Die IT-Governance ist strategisch ausgerichtet (was ist zu tun?), während das IT-Management taktischer Natur ist (wie sieht die Umsetzung aus?). Das IT-Management besteht aus verschiedenen Prozessen und Funktionen.

21 Für die praktische Umsetzung von IT-Management und IT-Governance stehen einige bewährte Verfahren zur Verfügung, etwa die Information Technology Infrastructure Library[15] für das Management und COBIT (Control Objectives for IT and related Technology) für die Governance.

22 Laut COBIT[16] besteht ein klarer Unterschied zwischen Governance und Management:

> *Die Governance stellt sicher, dass die Bedürfnisse, Bedingungen und Möglichkeiten der Stakeholder evaluiert werden, damit es möglich ist, ausgewogene, vereinbarte Unternehmensziele festzulegen, die Richtung durch Priorisierung und Entscheidungsfindung vorzugeben sowie die Performance und Compliance anhand der vereinbarten Richtung und Ziele zu überwachen.*
>
> *Beim Management geht es um die Planung, Ausarbeitung, Durchführung und Überwachung von Aktivitäten im Einklang mit der Richtung, die vom*

---

[14] Die ISACA (Information Systems Audit and Control Association) ist ein gemeinnütziger unabhängiger Verband, der Fachkräfte in den Bereichen Informationssicherheit, Assurance, Risikomanagement und Governance vertritt. Das von der ISACA eingerichtete ITGI konzentriert sich auf Forschungen zur IT-Governance und auf verwandte Themen.

[15] Die Information Technology Infrastructure Library (ITIL) ist eine Sammlung von Best-Practice-Ansätzen für das IT-Service-Management, die einen IT-Dienste-Zyklus widerspiegelt. Die ITIL bietet Anleitungen zu Herangehensweisen, Funktionen, Rollen und Prozessen. Demgegenüber besteht die ISO 20000 aus einer Norm mit Verhaltenskodex, wobei die ISO 20000-1 die Anforderungen an einen Diensteanbieter definiert, der Managed Services erbringen möchte, und die ISO 20000-2 den Verhaltenskodex enthält.

[16] COBIT ist das Rahmenwerk für Governance und Management der Unternehmens-IT, das von einer globalen Taskforce und einem Entwicklungsteam der ISACA erarbeitet wurde.

Governance-Gremium zur Verwirklichung der Unternehmensziele vorgegeben wurde.

23 Aufgrund der in mehreren EU-Institutionen vorgenommenen Zentralisierung von IT-Funktionen ist es wichtiger geworden, geeignete Governance-Strukturen einzurichten, um zu gewährleisten, dass die Bedürfnisse und Anliegen der Teile der Organisation, die nicht mehr über separate, dezentralisierte Infrastrukturen verfügen, bei der Governance der allgemeinen IT-Infrastruktur angemessen berücksichtigt werden. Die Rechenschaftspflicht für den IT-Bereich sollte sich in der Governance-Struktur und den zugehörigen Prozessen widerspiegeln.

24 Die Strukturen und Prozesse der IT-Governance sind so zu konzipieren, dass die Datenschutzgrundsätze eingehalten und wirksam umgesetzt werden. Ferner sollten sie organisatorische und personelle Aspekte behandeln, etwa die klare Festlegung der Rollen und Zuständigkeiten sowie die Aufklärung sämtlicher Mitarbeiter über die geltenden Datenschutzbestimmungen und -strategien.

25 Die datenschutzrelevanten Rollen auf verschiedenen Ebenen innerhalb einer EU-Institution, etwa in Direktoraten oder Referaten, sollten ebenso wie die Verteilung der Zuständigkeiten in der IT-Governance- und -Managementstruktur der Institution eindeutig definiert sein.

3.2. Rechenschaftspflicht im Bereich des Datenschutzes

26 Der Begriff der „Rechenschaftspflicht“ taucht in vielen verschiedenen Zusammenhängen auf. Er wurde in den letzten Jahren weiterentwickelt und beschreibt nun ein umfassendes Konzept zur Erfüllung der Datenschutzbestimmungen, das über die reine Einhaltung des Gesetzeswortlauts hinausgeht.

27 In einer Stellungnahme der Artikel-29-Datenschutzgruppe[17] heißt es, dass bei der Rechenschaftspflicht *die Betonung darauf liege, zu zeigen, wie die Rechenschaftspflicht ausgeübt wird, und dies auch nachweisen zu können*.

28 Der EDSB erklärt in seiner Stellungnahme[18] zum Datenschutzreformpaket, dass der Grundsatz der Rechenschaftspflicht der Verantwortung des für die Verarbeitung Verantwortlichen größeres Gewicht verleihe. Der für die Verarbeitung Verantwortliche müsse durch geeignete Strategien und Maßnahmen allgemein sicherstellen, dass personenbezogene Daten in Übereinstimmung mit den Datenschutzvorschriften verarbeitet werden und er den *Nachweis dafür erbringen* könne; zudem müsse er die Wirksamkeit der Maßnahmen überprüfen.

29 Diese Überprüfung kann durch interne Ressourcen, etwa die Compliance-Abteilung einer Organisation und/oder die interne Revision, sowie durch externe Ressourcen, etwa

[17] Stellungnahme 3/2010 der Artikel-29-Datenschutzgruppe zum Grundsatz der Rechenschaftspflicht.

[18] Stellungnahme des EDSB vom 7.3.2012 zum Datenschutzreformpaket.

Organisationen, die Zertifizierungen, Verhaltenskodizes, externe Prüfungen usw. anbieten, vorgenommen werden.

30 Artikel 5 DSGVO[19] zielt auf die Rechenschaftspflicht ab, indem vorgegeben wird, dass *der Verantwortliche für die Datenschutzgrundsätze der „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz", „Zweckbindung", „Datenminimierung", „Richtigkeit", „Speicherbegrenzung" und Sicherheit („Integrität und Vertraulichkeit") verantwortlich ist und deren Einhaltung nachweisen können muss.*

31 Die Rechenschaftspflicht hängt von der höchsten Führungsebene einer Organisation ab, die sicherstellen muss, dass die gesamte Organisation ihre Verpflichtungen erfüllt.

R1: Es ist äußerst wichtig, dass die Führungsebene die Datenschutzgrundsätze unmissverständlich unterstützt.

32 Die Führungsebene kann ihre Verantwortung für die Umsetzung ihrer Strategien mit Hilfe einer eindeutigen Definition von Mandat und Befugnissen delegieren.

R2: Die obere Führungsebene hat die Verantwortung für den Datenschutz zu tragen, unabhängig davon, ob sie für spezifische Verarbeitungsvorgänge die Rolle des Verantwortlichen ausfüllt oder nicht. Auch wenn sie nicht selbst in der Rolle des Verantwortlichen ist, sollte die obere Führungsebene besondere Verantwortung für die Einhaltung der Datenschutzvorschriften übernehmen, etwa indem sie geeignete Organisationsstrukturen und -verfahren einrichtet, damit das operative Management über die Mittel und Befugnisse verfügt, die zur Wahrnehmung der Rolle des Verantwortlichen nötig sind, und eine wirksame Einhaltung der Bestimmungen sicherstellen kann.

33 Obwohl die Verordnung vorsieht, dass der für die Verarbeitung Verantwortliche allein für den Datenschutz verantwortlich ist, muss die obere Führungsebene mit Einführung der Rechenschaftspflicht dem für ihre Institution Verantwortlichen alles an die Hand geben, was zur Kontrolle der Verarbeitungsvorgänge und zur Behebung von Problemen nötig ist.

R3: Die obere Führungsebene sollte eine für den Datenschutz zuständige Person[20] (z. B. einen Datenschutzbeauftragten oder Datenschutzkoordinator) ernennen und dieser ein Mandat zur Umsetzung der Datenschutzmaßnahmen erteilen.

34 Der Datenschutzbeauftragte oder Datenschutzkoordinator sollte die für die Verarbeitung Verantwortlichen nicht nur zu ihrem Verantwortungsbereich beraten, er muss darüber hinaus befugt sein, Informationen über die Verarbeitungsvorgänge

[19] Wie bereits in Punkt 5 erläutert, hat der Unionsgesetzgeber erklärt, dass die für die EU-Institutionen geltenden Datenschutzvorschriften entsprechend angepasst werden sollten, damit sie im Idealfall gleichzeitig mit der DSGVO angewandt werden können.

[20] Weitere Einzelheiten zur Rolle des Datenschutzbeauftragten finden sich in den Leitlinien der Artikel-29-Datenschutzgruppe in Bezug auf Datenschutzbeauftragte („DSB").

einzuholen, um seine Aufgaben ordnungsgemäß wahrnehmen zu können, sowie der oberen Führungsebene alle Beobachtungen zu Umständen mitzuteilen, die im Verlauf der Verarbeitungsvorgänge auftreten und sich auf die Rechte der betroffenen Personen bei der Verarbeitung ihrer personenbezogenen Daten auswirken könnten.

35 Alle Mitarbeiter, die an den betreffenden Vorgängen beteiligt sind, müssen den Anweisungen der für den Datenschutz zuständigen Person, was die korrekte Anwendung der von der Organisation festgelegten Strategien angeht, Folge leisten.

R4: Sämtliche Mitarbeiter sollten gut über die bestehenden Datenschutzstrategien und -verfahren Bescheid wissen. Dies lässt sich beispielsweise durch verpflichtende Einführungskurse, die Bereitstellung von Informationsmaterial oder Auffrischungsprogramme gewährleisten.

36 Die Führungsebene kann sich nur dann darauf verlassen, dass ihre Strategien ordnungsgemäß umgesetzt werden, wenn deren Wirksamkeit regelmäßig überprüft wird.

R5: Die mit dem Datenschutz verbundenen Strategien, Verfahren, Zuständigkeiten und Funktionen sollten regelmäßig überwacht und aufrechterhalten werden.

37 Der für die IT-Governance Verantwortliche sollte sich bewusst sein, dass auch Schatten-IT[21] existieren kann. Um diesem Problem zu begegnen, müssen die Mitarbeiter entsprechend sensibilisiert werden, um zu gewährleisten, dass sämtliche Maßnahmen zur Einhaltung der Vorschriften tatsächlich alle (wesentlichen) Systeme abdecken. Die obere Führungsebene sollte über Probleme mit Schatten-IT und die damit verbundenen Risiken aufgeklärt werden.

3.3. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

38 Gemäß Artikel 25 DSGVO „*trifft der Verantwortliche (...) geeignete technische und organisatorische Maßnahmen (…), die dafür ausgelegt sind, die Datenschutzgrundsätze (...) wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen*“. Der Verantwortliche kommt dieser Verpflichtung sowohl „zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung“ nach, also wenn die Verarbeitungssysteme entworfen, entwickelt und getestet werden, als auch „*zum*

[21] Der Begriff „Schatten-IT“ bezieht sich auf IT-Systeme, die nicht in den Verantwortungsbereich der IT-Hauptfunktion der Organisation fallen, sondern von einer anderen operativen oder administrativen Einheit für deren eigene Zwecke verwaltet und geregelt werden. Eine solch separate Organisation erschwert häufig die Einhaltung der von der Organisation vorgegebenen Regeln. Auch IT-Systeme, die von Beschäftigten mit oder ohne förmliche Genehmigung der Organisation verwendet werden, gelten als „Schatten-IT“. Dazu zählen insbesondere mobile Privatgeräte in Verbindung mit dem BYOD-Konzept („Bring Your Own Device“), zu denen Empfehlungen in den Leitlinien des EDSB zu mobilen Geräten zu finden sind.

Zeitpunkt der eigentlichen Verarbeitung“, d. h. wenn sich das System im Produktivbetrieb befindet.

39 Ferner stellt er sicher, dass „*durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden*“ (Datenschutz durch datenschutzfreundliche Voreinstellungen).

40 Der Verantwortliche kann diesen Verpflichtungen nur nachkommen, wenn die Prozesse im Bereich IT-Governance und IT-Management sowie bei der Systementwicklung so organisiert sind, dass bei jedem einzelnen Schritt Datenschutzüberlegungen zum Tragen kommen.

41 In Abschnitt 5 wird erläutert, wie diese Verpflichtungen in jeder Phase des Lebenszyklus eines IT-Systems und bei den entsprechenden horizontalen Abläufen zu berücksichtigen sind. Es beginnt damit, dass in der Konzeptionsphase die wichtigsten Datenschutzanforderungen in die Projektcharta aufgenommen werden. Danach müssen im Rahmen der Systemanforderungen die funktionalen und nichtfunktionalen Datenschutzanforderungen definiert werden. Anschließend werden geeignete Garantien und Maßnahmen in das Design integriert und in der Testphase geprüft und geeignete Schritte wie Meldungen und Überwachungsprozesse in die Betriebsabläufe eingebaut. Wenn das System schließlich in den Produktivmodus übergeht, werden Nutzern und anderen maßgeblichen Mitarbeitern geeignete Schulungen angeboten. Bei der Beschaffung von IT-Systemen und -Dienstleistungen wird von den EU-Institutionen genauso wie von anderen öffentlichen Einrichtungen erwartet, dass in ihren Leistungsbeschreibungen auch Datenschutzaspekte erwähnt werden,[22] um die Produkthersteller und Dienstleistungserbringer zu ermutigen, den Datenschutz durch Technikgestaltung bei ihren Entwicklungsprozessen zu berücksichtigen. Dies soll dazu beitragen, die neuesten technischen Möglichkeiten in diesem Datenschutzbereich zu fördern.

42 Für die EU-Institutionen ist der Datenschutz durch Technikgestaltung insbesondere bei Systemen relevant, die eine direkte Interaktion mit Nutzern innerhalb oder außerhalb der EU-Institutionen ermöglichen. Gegebenenfalls sollten alle Verarbeitungsvorgänge auf das absolut notwendige Maß begrenzt werden, was „*die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre*

[22] Mit Blick auf die Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die auf der Verarbeitung personenbezogener Daten beruhen oder die zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller bzw. Anbieter dieser Produkte, Anwendungen und Dienste dazu ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung von Produkten, Diensten und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sollten auch im Zusammenhang mit öffentlichen Ausschreibungen Berücksichtigung finden.

Zugänglichkeit“[23] für Einzelpersonen oder Organisationen angeht. Dies sollte auch für alle Tracking-Funktionen gelten, etwa im Kontext von Online-Diensten oder mobilen Apps.

[23] Artikel 25 Absatz 2 DSGVO.

4. RECHTSRAHMEN FÜR DEN DATENSCHUTZ

43 Dieser Abschnitt enthält einen kurzen Überblick über die wichtigsten Datenschutzkonzepte, die bei allen Prozessen im Bereich IT-Management und IT-Governance berücksichtigt werden sollten.

44 In diesen Leitlinien werden über die Verordnung hinaus auch in der DSGVO enthaltene Konzepte berücksichtigt, die mit der Anpassung der Verordnung an die DSGVO für die EU-Institutionen verpflichtend werden. Diese Konzepte ergänzen und stärken die in der Verordnung dargelegten Grundsätze, zudem sind sie vollständig mit dem geltenden Rahmen vereinbar. Sie werden bereits jetzt als bewährte Verfahren angesehen und können im Kontext des derzeitigen Rechtsrahmens angewendet werden.

Personenbezogene Daten

45 Gemäß Artikel 2 der Verordnung bezeichnet der Begriff personenbezogene Daten alle Informationen über eine bestimmte oder bestimmbare natürliche Person (nachstehend „betroffene Person“ genannt); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.[24]

Betroffene Person

46 Die betroffene Person ist die Person, deren personenbezogene Daten erhoben, gespeichert oder verarbeitet werden.

Für die Verarbeitung Verantwortlicher

47 Der für die Verarbeitung Verantwortliche ist das Organ oder die Einrichtung der EU, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Zu den Aufgaben des Verantwortlichen zählen insbesondere die Gewährleistung der Datenqualität und die Meldung der Verarbeitungsvorgänge an den Datenschutzbeauftragten. Der für die Verarbeitung Verantwortliche ist ferner für die Sicherheitsmaßnahmen zum Schutz der Daten verantwortlich.

Auftragsverarbeiter

48 Der Begriff „Auftragsverarbeiter“ bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet.

[24] Weitere Informationen und Beispiele finden sich unter dem Eintrag zu personenbezogenen Daten im EDSB-Glossar und in der Stellungnahme 4/2007 der Artikel-29-Datenschutzgruppe zum Begriff „personenbezogene Daten“.

Rechtsgrundlage für die Verarbeitung personenbezogener Daten

49 Artikel 5 der Verordnung enthält die Rechtsgrundlage, nach der die Verarbeitung personenbezogener Daten gestattet ist:

1. Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die aufgrund der Verträge zur Gründung der Europäischen Gemeinschaften im öffentlichen Interesse liegt.
2. Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt.
3. Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Antrag der betroffenen Person erfolgen.
4. Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben.
5. Die Verarbeitung ist für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich.

4.1. Datenschutzanforderungen

50 Die nachstehende Liste vermittelt einen kurzen Überblick über die allgemein anerkannten Datenschutzgrundsätze.

51 Diese Grundsätze, die von Anfang an das Gerüst für den Datenschutz bildeten, sind in die Verordnung integriert. Sie sind im Folgenden nach dem Vorbild von Artikel 5 DSGVO dargelegt.

1. **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**[25]

- Durchgängige Transparenz der Datenverarbeitung gegenüber den betroffenen Personen
- Information der betroffenen Personen über die Verarbeitung, z. B. über ihren Zweck und die Identität des Verantwortlichen
- Klare Angaben gegenüber den betroffenen Personen dazu, auf welche Weise, in welchem Umfang und zu welchem Zweck ihre personenbezogenen Daten verarbeitet werden
- Sicherstellung, dass eine eindeutige Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten existiert und dass die Verarbeitung nicht über die in dieser Rechtsgrundlage genannten Grenzen hinausgeht
- Wenn laut Rechtsgrundlage eine Einwilligung erforderlich ist, muss diese zweckgebunden sein und dokumentiert werden, und es muss möglich sein, sie zu widerrufen[26]
- Wahrung der Rechte des Einzelnen auf Zugang und Berichtigung seiner Daten

[25] Siehe auch Abschnitt 5.6.1: Information der betroffenen Personen und Transparenz.

[26] Siehe auch den Eintrag zum Thema Einwilligung im EDSB-Glossar.

- Entwicklung von Verfahren und Anleitungen, in denen eindeutig erklärt wird, wie betroffene Personen ihr Recht auf Zugang und Berichtigung ihrer Daten in jeder Phase der Verarbeitung wahrnehmen können
- Einrichtung von Funktionen im IT-System, die den Zugang, die Änderung oder das Sperren von Daten sowie einen Widerspruch gegen die Verarbeitung ermöglichen
- Festlegung interner Regeln zur Prüfung der Gültigkeit der Rechtsgrundlage im Fall von Änderungen, z. B. bei Widerruf der Einwilligung[27]

2. Zweckbindung

- Verarbeitung personenbezogener Daten nur für festgelegte, eindeutige und legitime sowie begrenzte Zwecke
- Begrenzung der Verarbeitung von Daten in einem IT-System auf den ursprünglich festgelegten Zweck
- Gewährleistung der Zweckbindung, wenn Daten verschiedener Art erhoben und zu unterschiedlichen Zwecken verarbeitet werden
- Festlegung interner Regeln für die fallweise Bewertung der Kompatibilitätsanforderungen[28], um eine Änderung des Zwecks zu ermöglichen
- Klare Mitteilung an die betroffenen Personen im Fall einer Änderung des ursprünglich festgelegten Zwecks für die Verarbeitung ihrer personenbezogenen Daten

3. Datenminimierung

- Sicherstellung, dass die personenbezogenen Daten dem Zweck angemessen und erheblich sind und nicht über das für die Zwecke der Verarbeitung notwendige Maß hinausgehen
- Begrenzung der Kategorien personenbezogener Daten, die für die Verarbeitung ausgewählt werden, auf eine Datensammlung, die unmittelbar für die ursprünglich festgelegten Zwecke relevant ist
- Inbetrachtziehung und Verwendung spezieller Technologien zum Schutz der Privatsphäre, sofern machbar, die die übermäßige Nutzung personenbezogener Daten vermeiden helfen oder den Einsatz anonymisierter Daten ermöglichen

4. Richtigkeit

- Sicherstellung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind

[27] Siehe auch den Eintrag zum Thema Einwilligung im EDSB-Glossar.

[28] Stellungnahme 3/2013 der Artikel-29-Datenschutzgruppe zur Zweckbindung.

- Einführung von Prozessen zur Gewährleistung und Aufrechterhaltung der Richtigkeit der verarbeiteten Daten, etwa indem die Qualität der in das System eingegebenen Daten vor ihrer Verarbeitung automatisch überprüft wird
- Sicherstellung, dass betroffene Personen die Möglichkeit haben, unrichtige Daten zu berichtigen

5. Speicherbegrenzung

- Keine längere Speicherung personenbezogener Daten als für den ursprünglich festgelegten Zweck erforderlich
- Vorabfestlegung der Speicherfristen für Daten, die in einer Form gespeichert sind, die eine Identifizierung der betroffenen Personen zulässt
- Sicherstellung, dass die erforderlichen Speicherfristen den Zwecken der Datenerhebung angemessen und begrenzt sind Getrennte Zuordnung und Verwaltung der Speicherfristen für Daten, die für unterschiedliche Zwecke erhoben wurden
- Ergreifung besonderer Vorsichtsmaßnahmen, wenn personenbezogene Daten auf Papier gespeichert sind, da ihre Existenz nur schwer nachzuverfolgen ist
- Gestaltung von IT-Systemmerkmalen, die eine Verwaltung der Speicherfristen und die Durchführung der nach ihrem Ablauf notwendigen Maßnahmen (Löschung oder Anonymisierung) erlauben

6. Integrität und Vertraulichkeit

- Gewährleistung der Sicherheit der personenbezogenen Daten
- Bewertung der Sicherheitsrisiken und Planung von Maßnahmen zur Eindämmung der Risiken[29]
- Bewusstsein, dass ein Papierausdruck andere für das IT-System eingerichtete Maßnahmen zur Risikoeindämmung wie Zugangskontrolllisten unterlaufen kann
- Auf der Risikobewertung basierende Gestaltung und Umsetzung organisatorischer und technischer Maßnahmen, um die Risiken auf ein annehmbares Maß zurückzustufen, Verarbeitungsvorgänge zu vermeiden, die keine wirksame Eindämmung erlauben, und um zu gewährleisten, dass das verantwortliche Management eine eindeutige Entscheidung darüber trifft, welche Risiken aus welchen Gründen akzeptabel sind. Da Datenschutzrisiken mit den Grundrechten anderer Personen verzahnt sind, ist eine Auslagerung der Risiken (Versicherung) eine weniger gangbare Option als in anderen Risikobereichen.

[29] Siehe unter anderem die Leitlinien des EDSB zu Sicherheitsmaßnahmen bei der Verarbeitung personenbezogener Daten.

7. Rechenschaftspflicht

- Sicherstellung, dass die Einhaltung der oben aufgeführten Grundsätze nachgewiesen werden kann

52 Über diese Grundsätze hinaus sind die für die Verarbeitung Verantwortlichen dazu verpflichtet, die Rechte der betroffenen Personen auf Zugang, Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerspruch gegen die Verarbeitung zu wahren, insbesondere bei einer automatisierten Entscheidungsfindung.

53 Der für die Verarbeitung Verantwortliche muss seiner Verpflichtung nachkommen, personenbezogene Daten nur dann an Einrichtungen in Drittländern zu übermitteln, wenn ein angemessenes[30] Schutzniveau garantiert ist.[31]

[30] Siehe das Positionspapier des EDSB zur Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen durch Organe und Einrichtungen der EU.

[31] Siehe auch Anhang 1: Verarbeitung durch externe Organisationen und Übermittlung personenbezogener Daten.

5. DATENSCHUTZANFORDERUNGEN IM LEBENSZYKLUS VON IT-SYSTEMEN

54 In diesem Kapitel ist die Verarbeitung personenbezogener Daten über den Lebenszyklus eines IT-Systems[32] hinweg beschrieben, von der Entwicklung über den Betrieb bis hin zur Pflege des Systems. Daneben werden auch horizontale Prozesse wie das Projektmanagement betrachtet.

55 Die

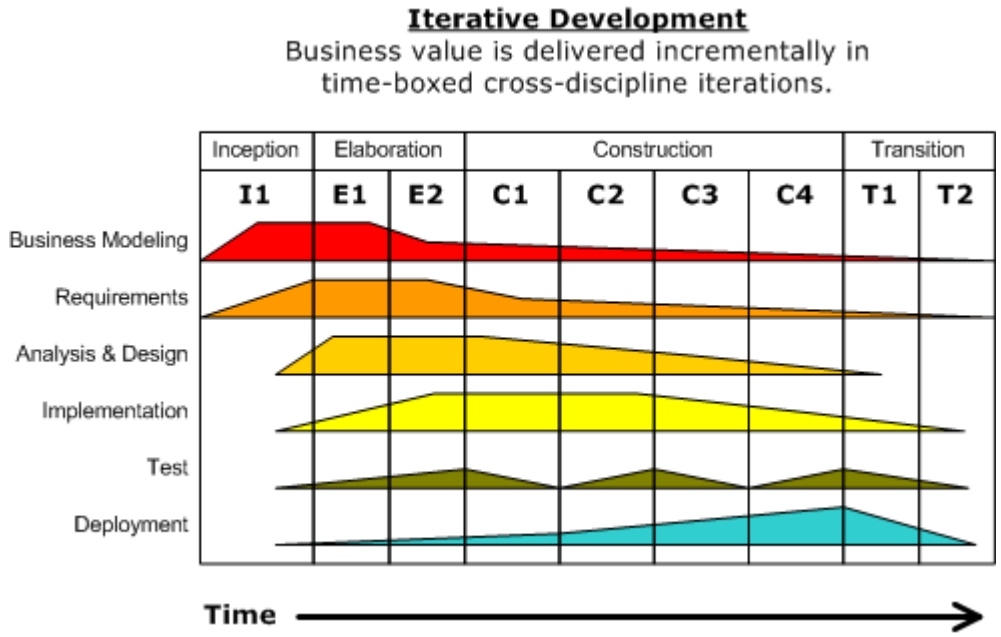

Abbildung 1: Lebenszyklusphasen (Quelle: Dutchguilder, gemeinfreies Werk)

Iterative Development	Iterative Entwicklung
Business value is delivered incrementally in time/boxed cross/discipline iterations.	Der Geschäftswert wird inkrementell durch disziplinenübergreifende Iterationen in festen Zeitfenstern erzielt.
Inception	Konzeption
Elaboration	Entwurf
Construction	Konstruktion
Transition	Übergabe

[32] Der Lebenszyklus des IT-Systems, das hier als Bezugspunkt verwendet wird, beruht auf dem RUP@EC®-IBM® Rational Unified Process®, einer speziell auf die Europäische Kommission abgestimmten Entwicklungsmethodik.

I1	I1
E1, E2	E1, E2
C1, C2, C3, C4	C1, C2, C3, C4
T1, T2	T1, T2
Business modeling	Geschäftsprozessmodellierung
Requirements	Anforderungen
Analysis & Design	Analyse u. Design
Implementation	Implementierung
Test	Test
Deployment	Auslieferung
Time	Zeitachse

in Anhang 2 beigefügte Tabelle enthält die (im Folgenden aufgeführten) Empfehlungen, die für die Datenschutzanforderungen in den einzelnen Lebenszyklusphasen eines IT-Systems relevant sind.

5.1. Konzeption (Start)

56 In der Konzeptionsphase geht es darum, den Projektumfang festzulegen und sich über die wichtigsten Projektanforderungen zu einigen.

57 Die für den Datenschutz zuständige Person (z. B. der Datenschutzbeauftragte oder Datenschutzkoordinator) sollte bei einem IT-Projekt als Interessenträger angesehen werden, da sie unter anderem dabei helfen kann, als ein Endprodukt des Projekts den Schutz aller personenbezogenen Daten, die in dem betreffenden IT-System verarbeitet werden, zu erleichtern. Der Datenschutzbeauftragte/Datenschutzkoordinator sollte von Beginn der Konzeptionsphase an in das Projekt eingebunden werden.

R6: Zunächst sollte bestimmt werden, ob Daten, die in dem betreffenden IT-System verarbeitet werden, personenbezogene Daten sind oder ob sie infolge der Verarbeitung zu personenbezogenen Daten werden können.

58 Wenn die Verarbeitung personenbezogener Daten vorgesehen ist, sollte die Rechtsgrundlage für die Verarbeitung bestimmt werden.

59 Die Datenschutzrisiken und anwendbaren Schutzmaßnahmen sollten auf hoher Ebene bestimmt werden.

R7: Die wichtigsten Datenschutzanforderungen („High-Level Requirements“) sollten in einer Projektcharta aufgeführt werden. Dieses Dokument dient der Beschreibung des Projektumfangs und der wichtigsten Anforderungen, die sich aus der Konzeptionsphase ergeben.

60 In dieser Phase sollten die wichtigsten Risiken[33], die bei der Verarbeitung personenbezogener Daten auftreten könnten, betrachtet werden. Angesichts der bevorstehenden Überarbeitung der rechtlichen Verpflichtungen wird empfohlen, eine sogenannte Datenschutz-Folgenabschätzung gemäß DSGVO vorzunehmen.

61 Während der gesamten Projektdauer sollte ein Risikomanagementprozess angewendet werden.[34]

5.2. Entwurf (Plan)

62 In der Entwurfsphase werden die Arbeitsschritte festgelegt, die in den anschließenden Projektphasen durchzuführen sind. In diesen Phasen wird anhand der zu ermittelnden Anforderungen ein künftiges IT-System entworfen.

5.2.1. Ermittlung der Anforderungen

R8: Die Datenschutzanforderungen sollten bei den Interessenträgern ermittelt und während der IT-Systemspezifikation dokumentiert werden.

63 Die Anforderungen sollten aufrechterhalten und anhand der üblichen Projektzyklusmethodik überprüft werden. Der Projektmanager sollte die für den Datenschutz zuständige Person (etwa den Datenschutzbeauftragten oder den Datenschutzkoordinator) konsultieren, um einen umfassenden Überblick über die Datenschutzanforderungen zu erhalten.

64 Es gibt funktionale und nichtfunktionale Anforderungen an den Datenschutz.[35] Zu den funktionalen Anforderungen zählen insbesondere die Leistungsmerkmale, die nötig sind, um die Rechte der betroffenen Personen, etwa das Recht auf Auskunft (Artikel 15 DSGVO), auf Datenübertragbarkeit (Artikel 18F DSGVO), auf Berichtigung (Artikel 16 DSGVO) und auf Löschung (Artikel 17 DSGVO), zu wahren, sowie Funktionen, die die Speicherbegrenzung gewährleisten (Artikel 5 Buchstabe e DSGVO). Zu den nichtfunktionalen Anforderungen zählen die Einhaltung der Grundsätze der Datenminimierung und der Zweckbindung (Artikel 5 Buchstaben b und

[33] In den Leitlinien des EDSB zu den Sicherheitsvorkehrungen bei der Verarbeitung personenbezogener Daten wird der Begriff Risiko als „Auswirkung von Unsicherheit auf Ziele“ definiert. Die wichtigsten Risiken werden in der Konzeptionsphase ermittelt. Die umfassende Risikobewertung findet in der Planungsphase statt und wird über den gesamten Projektzyklus hinweg fortgeführt.

[34] Ebd.

[35] Die nichtfunktionalen Anforderungen werden nach ISO 25010 auch als Qualitätsanforderungen aufgefasst.

c DSGVO), die beim Entwurf der Datenstrukturen eines Systems zu berücksichtigen sind, sowie weiter gefasste Ziele wie die Sicherheit und Prüfbarkeit.

65 Die Integration der Datenschutzanforderungen in dieser Phase ist die Voraussetzung dafür, dass in der Designphase geeignete Entscheidungen getroffen werden können.

5.2.2. Design

66 In der Designphase wird festgelegt, auf welche Weise die Umsetzung der Anforderungen im System erfolgt. Dazu werden die Bausteine und Funktionalitäten des Systems sowie ihre Wechselwirkung definiert. In dieser Phase werden zum Beispiel die Sicherheitsvorkehrungen bestimmt, die für den Schutz der zu verarbeitenden Daten nötig sind.

67 Es ist wichtig, dass das an einem IT-Projekt beteiligte technische Personal und die Datenschutzexperten mit den neuesten Entwicklungen im Bereich der bestehenden Technologien und Produkte vertraut sind, die die Einhaltung der Datenschutzanforderungen und deren Umsetzung ermöglichen.

68 Mit dem neuen Datenschutzrahmen werden der „Datenschutz durch Technikgestaltung“ sowie Technologien zum Schutz der Privatsphäre zu obligatorischen Instrumenten zur Verbesserung des Schutzniveaus.[36] Im Rahmen des Designprozesses müssen alle funktionalen und nichtfunktionalen Datenschutzanforderungen berücksichtigt werden. Die Entscheidungen über das Design erfordern zudem eine genaue Betrachtung der Datenschutzfunktionen der gewählten technischen Konzepte. Es sollten wiederverwendbare Module und Funktionen gewählt werden, damit keine Verarbeitungsvorgänge – und auch keine Datenerhebungen – durchgeführt werden, die für die Zwecke des Systems nicht erforderlich sind. Zum Beispiel sollten die Designer nicht auf Funktionsbibliotheken zugreifen, die mit dem Ziel entwickelt wurden, möglichst viele Daten zu sammeln oder die Aktivitäten der Nutzer im Detail aufzuzeichnen, die in einem anderen Zusammenhang zum Anlegen von Profilen verwendet werden könnten. Ferner sollten die Designer Tools vermeiden, die personenbezogene Daten an Dritte weiterleiten. Wann immer Technologien vorhanden sind, die einen besseren Datenschutz ermöglichen, sind diese Technologien vorzuziehen, bei denen der Schutz der Privatsphäre geringer ist. Ein solcher Ansatz ermöglicht die Entwicklung von IT-Systemen, die flexibel genug sind, um einen angemessenen Schutz personenbezogener Daten zu gewährleisten.

69 Wenn der Umfang der Verarbeitung von der betroffenen Person bestimmt werden kann, sind die Initialisierungswerte für die einschlägigen Parameter so zu wählen, dass die geringste Zahl an Verarbeitungsvorgängen durchgeführt, dem Nutzer jedoch die

[36] Die Datenschutz-Grundverordnung (DSGVO) verpflichtet Verantwortliche und Auftragsverarbeiter erstmals dazu, Datenschutz durch Technikgestaltung zu betreiben.

Möglichkeit gegeben wird, sich für eine umfangreichere Verarbeitung zu entscheiden, so dass er eine echte Wahl hat.

70 In Artikel 22 Absatz 2 der Verordnung sind neben verschiedenen Sicherheitszielen auch allgemeine Risiken aufgeführt, die eingedämmt werden müssen. Der für die Verarbeitung Verantwortliche ergreift Maßnahmen, um die Ziele zu erfüllen und die Risiken zu mindern und damit einen möglichen Verlust der Vertraulichkeit, Integrität und Verfügbarkeit zu verhindern, der eine Gefahr für personenbezogene Daten darstellen kann. Die Wahl der Gegenmaßnahmen hängt vom Ergebnis der spezifischen Risikobewertung ab.[37]

71 Durch Zugangskontrollen wird beispielsweise gewährleistet, dass nur befugte Personen Daten im System lesen, ändern oder löschen können. Diese Kontrollen tragen vom Standpunkt der Sicherheit gesehen zur Vertraulichkeit und Integrität der Daten bei. Wenn in einem IT-System personenbezogene Daten verarbeitet werden, sollten die eingebauten Kontrollen zudem sicherstellen, dass die Nutzer zur Erfüllung ihrer Aufgaben nur auf bestimmte Daten Zugriff haben. Die Zugangskontrollen können somit sicherstellen helfen, dass die Nutzung personenbezogener Daten auf die zulässigen Zwecke beschränkt ist (Zweckbindung) und die Daten vor dem Zugang durch Unbefugte und vor Manipulation geschützt sind.

R9: Wenn in einem IT-System besonders sensible (personenbezogene) Daten, etwa zur körperlichen oder geistigen Gesundheit, zur ethnischen Herkunft, zu politischen oder religiösen Überzeugungen oder zu Vorstrafen, verarbeitet werden, sollten zusätzliche Schutzvorkehrungen getroffen werden, etwa in Form einer Verschlüsselung oder von mehrstufigen Zugangskontrollen, um die Risiken der Verarbeitung zu mindern.

72 Es können verschiedene Maßnahmen ergriffen werden, um Sicherheit zu erzielen. Für den Zugang zu personenbezogenen Dateien können besondere Passwörter verlangt werden. Zur Identifizierung befugter Nutzer sollten eindeutige Anmeldeverfahren sowie Protokolldateien eingeführt werden, in denen der Zugriff auf Dateien und die Änderung von Daten aufgezeichnet werden.

R10: Beim Entwurf eines IT-Systems sollten geeignete Maßnahmen geplant werden, die es erlauben, die Speicherfrist angemessen zu verwalten und die nach deren Ablauf erforderlichen Maßnahmen (wie Anonymisierung oder Löschung) zu ergreifen.

73 Die Artikel-29-Datenschutzgruppe kommt in ihrer Stellungnahme 5/2014[38] „*zu dem Schluss, dass Anonymisierungstechniken geeignet sind, Garantien für den Schutz der*

[37] Siehe unter anderem die Leitlinien des EDSB zu Sicherheitsmaßnahmen bei der Verarbeitung personenbezogener Daten.

[38] Stellungnahme 5/2014 der Artikel 29-Datenschutzgruppe zu Anonymisierungstechniken.

Privatsphäre zu schaffen, und eingesetzt werden können, um wirksame Anonymisierungsverfahren zu entwickeln. Dies gilt allerdings nur, wenn ihre Anwendung ordnungsgemäß geplant wird. Das bedeutet, dass die Voraussetzungen (Kontext) und die Zielsetzung(en) des Anonymisierungsverfahrens klar festgelegt werden müssen, um die angestrebte Anonymisierung zu erreichen und zugleich zweckmäßige Daten hervorzubringen. Die Wahl der am besten geeigneten Lösung sollte auf der Grundlage einer Einzelfallbewertung erfolgen, nach Möglichkeit unter Heranziehung einer Kombination verschiedener Techniken und unter Berücksichtigung der in dieser Stellungnahme herausgearbeiteten praktischen Empfehlungen."

5.3. Konstruktion und Entwicklung (Durchführung)

74 In der Entwicklungsphase wird der Code geschrieben. Ferner wird bei Systemen, die auch Hardware umfassen, deren Design und Konfiguration in die Überlegungen mit einbezogen, damit die aus der Risikobewertung erwachsenden Anforderungen erfüllt werden können.

R11: Es ist wichtig, dass das Entwicklungsteam und die Interessenträger eine gemeinsame Verständnisgrundlage besitzen. Die Datenschutzgesetze und -bestimmungen sollten dem Entwicklungsteam schon vor Beginn der Entwicklungsphase bewusst sein. Dies lässt sich etwa dadurch sicherstellen, dass der Datenschutzbeauftragte Schulungen für bestehende und neue Entwicklungsteams organisiert oder gleichwertige Maßnahmen ergriffen werden.

75 Das Entwicklungsteam sollte die Systementwicklung auf leicht verständliche und umfassende Art und Weise dokumentieren.

5.4. Test (Prüfung)

76 Die Testphase gibt Aufschluss darüber, ob das in Entwicklung befindliche System alle Anforderungen erfüllt.

77 Die Datenschutzanforderungen sollten anhand von Testfällen und Testszenarien betrachtet werden.

78 In den Tests sollten sämtliche Datenschutzanforderungen geprüft werden, etwa ob eine erschöpfende und eindeutige Datenschutzerklärung existiert, ob Funktionen für die Verwaltung der Datenqualität und von Cookies sowie datenschutzfreundliche Voreinstellungen vorhanden sind und ob die IT-Sicherheitsanforderungen erfüllt wurden.

79 Ein integrierter Ansatz bei den Sicherheitstests (der statische Code-Analysen für den Bereich der Sicherheit und dynamische Ansätze wie Penetrationstests umfasst) kann in der Entwicklungsphase eine wesentliche Rolle spielen.

R12: Für die Tests sind Verfahren und Anweisungen zu entwickeln, die die Einhaltung der Datenschutzanforderungen gewährleisten.

80 In der Testphase sollte die Erhebung personenbezogener Echtdaten vermieden werden, da diese Daten nicht für andere Zwecke als den ursprünglichen Erhebungszweck verwendet werden dürfen und ihr Einsatz in einer Testumgebung dazu führen könnte, dass die personenbezogenen Daten unbefugten Personen zugänglich gemacht werden.

81 Nach Möglichkeit sollten künstlich generierte Testdaten verwendet werden oder Testdaten, die von Echtdaten ohne Änderung ihrer Struktur abgeleitet wurden und keine personenbezogenen Daten mehr aufweisen. Verschiedene solcher Techniken wurden bereits erfolgreich angewandt.[39]

82 Wenn eine gründliche und umsichtige Analyse zeigt, dass die generierten Testdaten keine hinreichende Gewähr für die Gültigkeit der Tests bieten können, muss umfassend entschieden und dokumentiert werden, welche Echtdaten – in möglichst begrenztem Umfang – im Test verwendet werden sollten und welche zusätzlichen technischen und organisatorischen Schutzvorkehrungen für die Testumgebung einzurichten sind. Besondere Datenkategorien dürfen bei Tests mit Echtdaten nur mit der ausdrücklichen Einwilligung der betreffenden Personen verwendet werden.

R13: Bei der Simulation einer Liveumgebung sollte die Erhebung personenbezogener Echtdaten vermieden werden.

83 Beim Testen eines IT-Systems sollten wirksame Schutzvorkehrungen getroffen werden. Falls für den Test die Verwendung personenbezogener Echtdaten nötig ist, sollten die Daten anonymisiert werden. Als Alternative sollte das Anlegen simulierter Datensätze zur allgemeinen Verwendung durch die Entwickler in Betracht gezogen werden.

84 Sollte der Fall eintreten, dass personenbezogene Daten bei der Entwicklung oder in der Testumgebung verwendet werden müssen, gelten die für die Produktivumgebung maßgeblichen Anforderungen.

85 Falls ein externer Auftragsverarbeiter an den Tests beteiligt ist, sollte den Daten, die für den Test zur Verfügung gestellt werden, besondere Aufmerksamkeit zuteil werden. Generell sollten keine personenbezogenen Echtdaten für diesen Zweck verwendet werden.

86 Auftragnehmer sollten lediglich Zugang zu den Testumgebungen haben. Falls ihr Zugang zur Produktivumgebung nötig ist, sollten ausschließlich zugriffsberechtigte IT-Systemadministratoren[40] der betreffenden Institution nach Durchführung geeigneter Verfahrensprüfungen auf Anweisung des Auftragnehmers Handlungen ausführen.

[39] Verschiedene Entwicklungsumgebungen enthalten Techniken und Tools für die Testdatengenerierung.

[40] IT-Administratorrechte sollten nur nach einer entsprechenden Entscheidung des Systemeigners eingerichtet werden.

Wenn es nur externe IT-Systemadministratoren gibt, sollte der für die Verarbeitung Verantwortliche sicherstellen, dass der Auftragnehmer die geltenden Datenschutzbestimmungen einhält.

5.5. Übergabe und Auslieferung (Aktion)

87 In dieser Phase besteht das Hauptziel darin, das System von der Entwicklungs- in die Produktivphase zu überführen. Die Nutzer sollten das System verstehen. Zu den Maßnahmen in dieser Phase sollte daher auch die Aufklärung von Endnutzern und Systempflegern über den Datenschutz gehören.

R14: Endnutzer, Systemadministratoren und die für die Systempflege zuständigen Mitarbeiter sollten sich der Datenschutzbestimmungen bewusst sein.

5.6. Betrieb und Pflege

88 Nachdem ein IT-System die Akzeptanztests durchlaufen hat und für die Produktivphase freigegeben wurde, geht es in den Regelbetrieb der Organisation über. Das Entwicklungsteam gibt die Verantwortung an das für den Systembetrieb zuständige Team weiter. Entwicklungskapazitäten werden nur noch für Pflegezwecke bereitgehalten, d. h. für die Berichtigung von Fehlern, die im Produktivbetrieb entdeckt wurden, und für begrenzte Systemanpassungen, falls sich die Anforderungen ändern.

89 Im Gegensatz zur Systementwicklung, die gewöhnlich anhand von Projekten abläuft und zahlreiche Einzelmaßnahmen umfasst, ist der Systembetrieb ein täglich stattfindender Arbeitsprozess, bei dem bestimmte Schritte in regelmäßigen Intervallen kontinuierlich wiederholt werden (z. B. Backup, Vorbereitung, Releasewechsel usw.).

90 Der Betrieb sollte sich auf eine umfassende und aktuelle Dokumentation der Systemverfahren gründen, zu denen unter anderem die besonderen Anforderungen an die Verarbeitung personenbezogener Daten zählen.

91 Falls noch nicht geschehen, sollte die Organisation ermitteln, in welchen ihrer bereits vorhandenen IT-Systeme personenbezogene Daten verarbeitet werden und welcher Art diese Daten sind (z. B. sensible Daten wie Gesundheitsdaten). Dadurch lassen sich die mit der Verarbeitung der personenbezogenen Daten verbundenen Risiken bestimmen, so dass ein geeignetes internes Kontrollsystem eingerichtet werden kann, das die Einhaltung der Datenschutzbestimmungen gewährleistet.

92 Die Bewertung der Risiken, die sich aus dem Systembetrieb ergeben, sollte regelmäßig überprüft und aktualisiert werden. Die Einbindung dieser Aufgabe in das regelmäßige Risikomanagement der Organisation, die das System betreibt, hat sich hier als wirksame Praxis erwiesen.

R15: Der für die Verarbeitung Verantwortliche sollte dem Datenschutzbeauftragten der Institution jede Verarbeitung personenbezogener Daten in einer Datenbank oder einem IT-System melden.[41]

93 Die Datenschutzerklärungen sollten regelmäßig überprüft werden, falls Änderungen vorgenommen oder zusätzliche Dienste angeboten werden, die die Verarbeitung personenbezogener Daten mit einschließen.

R16: Die maximale Speicherfrist für Daten auf Speichermedien sollte so festgelegt werden, dass sie den vertraglichen, gesetzlichen und regulatorischen Anforderungen entspricht. Die Speicherfrist kann je nach Speicherzweck variieren.[42]

5.6.1. Information der betroffenen Personen und Transparenz

94 Die Institution ist verpflichtet, den Nutzer eines IT-Systems zumindest über folgende Aspekte eines Verarbeitungsvorgangs zu informieren:

a. die Identität der Institution sowie jeder anderen Institution oder Einrichtung, mit der sie die Verantwortung für die Verarbeitung teilt, sowie Angaben dazu, wie die Institution im Fall von Anfragen, Ersuchen und Beschwerden kontaktiert werden kann

b. welche personenbezogenen Daten verarbeitet werden

c. warum (zu welchen Zwecken) die Institution die Daten erhebt und weiterverarbeitet

d. die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten, indem die Dienststellen oder die Kategorien der Mitarbeiter angegeben werden, die Zugang zu den Daten haben

e. die Datenübermittlung an andere Institutionen oder Einrichtungen, zusammen mit den Gründen für die Übermittlung

f. klare Hinweise darauf, welche Angaben verpflichtend und welche freiwillig sind, selbst wenn ein Online-Formular existiert, in dem verpflichtende und freiwillige Angaben kenntlich gemacht sind

95 Die Informationen für die betroffenen Personen sollten ...

a. einfach und direkt von der Homepage und jeder anderen Seite aus zugänglich sein, die dazu benutzt wird, personenbezogene Daten zu erheben und zu verarbeiten

b. in klaren Worten und einfacher Sprache verfasst sein,

[41] Diese Meldung muss gemäß Artikel 25 der Verordnung (EG) Nr. 45/2001 erfolgen.

[42] Für einen Backup-Speicher werden normalerweise andere Zugangskontrollen festgelegt als für ein normales Betriebssystem, so dass sich die Risiken unterscheiden.

c. deutlich von anderen Rechtshinweisen und Grundsatzinformationen unterscheidbar sein.

96 Die Institutionen sollten es Menschen mit Behinderungen[43] ermöglichen, ihre Recht als betroffene Personen umfassend zu verstehen und wirksam wahrzunehmen, wenn ihre personenbezogenen Daten durch IT-Dienste verarbeitet werden.

> R17: Die Institution sollte geeignete Informationshinweise zu den Verarbeitungsvorgängen erstellen und den betroffenen Personen über Informationskanäle zugänglich machen.

97 Die Eignung des jeweiligen Informationskanals hängt von der Art des IT-Systems und den Interaktionen der betroffenen Personen mit der Institution ab. Wenn während der Datenverarbeitung direkter Zugang zum System besteht (z. B. Zugang von Mitarbeitern zu internen Verwaltungssystemen oder Zugang von externen Interessenträgern zu Online-Diensten), sollte auf der Benutzeroberfläche des Systems eine Funktion angebracht sein, über die Angaben zur Verarbeitung abgerufen werden können.

98 Wenn keine direkte Interaktion mit dem IT-System für die betroffenen Personen möglich ist, müssen die organisatorischen Prozesse so gestaltet sein, dass die Informationen zum richtigen Zeitpunkt angezeigt werden. (Wenn Daten etwa mit Hilfe eines Formulars erhoben werden, könnte das Formular die Informationen oder einen Hinweis auf die Informationsquelle enthalten.)

99 Die Institution muss außerdem in der Lage sein, die einschlägigen Informationen auf Anfrage bereitzustellen, etwa durch Angabe einer E-Mail-Adresse für allgemeine Anfragen oder über einen Online-Dienst. Ferner muss sie ein Verfahren einrichten, das es ihr erlaubt, innerhalb einer angemessenen Frist auf Anfragen zu reagieren.

5.6.2. Zugangsverwaltung[44]

100 Es sollte deutlich gemacht werden, wer der Systemeigner ist und somit die Verantwortung dafür trägt, dass das System regelmäßigen Risikomanagementmaßnahmen unterzogen wird. Der Systemeigner ist ferner dafür verantwortlich, dass angemessene Zugangskontrollen sowie andere Kontrollen zur Risikominderung aufrechterhalten werden und dass ordnungsgemäß mit IT-Sicherheitsvorfällen umgegangen und das IT-System korrekt entsorgt wird.

> R18: Der Systemeigner sollte Verfahren zur Benutzerverwaltung sowie Genehmigungsverfahren, etwa hinsichtlich der Zugangsgewährung zum System, festlegen und anwenden.

[43] Siehe zu Online-Diensten zum Beispiel die Seite http://www.w3.org/WAI/intro/accessibility.php.

[44] Informationen über die erforderlichen Kontrollmaßnahmen finden sich zum Beispiel in COBIT 5: Rahmenwerk für Governance und Management der Unternehmens-IT.

101 Das Management sollte die Zugangsverfahren und ihre wirksame Umsetzung regelmäßig überprüfen.

102 Der Zugang zu personenbezogenen Daten ist allgemein nach dem Least-Privilege-Prinzip zu gewähren, d. h. Nutzer und Administratoren sollten nur die Zugangsrechte erhalten, die zur Ausführung ihrer Aufgaben unbedingt nötig sind.

5.6.3. Änderungsverwaltung

103 Es sollten Kontrollen eingerichtet werden, die den Zugang zu Systemkomponenten begrenzen und Änderungen durch Unbefugte verhindern.

R19: Es sollten formelle Verfahren für die Änderungsverwaltung festgelegt und angewendet werden, damit alle Anträge auf Änderungen im Informationssystem einheitlich gehandhabt werden.

104 Verfahren für die Änderungsverwaltung sollten auch für beauftragte Dienstleister (etwa Systementwickler oder Application-Service-Provider) bereitgestellt werden.

105 Falls der Zweck der Verarbeitung personenbezogener Daten in irgendeiner Weise geändert wird, sind die betroffenen Personen darüber zu informieren und über die Rechtsgrundlage für den geänderten Zweck aufzuklären. Die Datenschutzanforderungen sollten unter Mithilfe des Datenschutzbeauftragten oder einer Person mit gleichwertiger Funktion analysiert werden.

5.6.4. Sicherheitskontrollen

R20: Der Zugriff auf Dateien mit personenbezogenen Daten sollte ständig überwacht werden.

Beispiel: Treten beim Betrieb eines Systems Fehler auf, sollte die Verwendung von personenbezogenen Echtdaten zur Fehlerbeseitigung vermieden werden. Auf jeden Fall ist von dem für die Verarbeitung Verantwortlichen, sofern erforderlich, eine Genehmigung einzuholen. Darüber hinaus müssen das Genehmigungsverfahren und die Fehlerbeseitigungsmaßnahmen dokumentiert werden, um Nachprüfbarkeit herzustellen. Die Menge der für Tests verwendeten personenbezogenen Daten sollte möglichst klein gehalten werden, wobei strikt der Grundsatz „Kenntnis nur, wenn nötig“ gelten sollte.

106 Die Institutionen sollten den Schutz ihrer IT-Systeme durch geeignete Sicherheitstechnologien und die Umsetzung der im Lauf der Bewertung der Sicherheitsrisiken ermittelten Maßnahmen zur Risikominderung sicherstellen und dafür sorgen, dass diese immer auf dem neuesten Stand sind, um neu aufkommende Bedrohungen abwehren zu können.

107 Die Informationssysteme sollten Prüfprotokolle erstellen, die notwendig sind, um die Abfolge von Ereignissen oder von Änderungen im IT-System zu rekonstruieren.

108 Falls bei den Sicherheitskontrollen Protokolle angelegt werden, ist zu prüfen, ob diese Protokolle personenbezogene Daten enthalten und daher in die Risikobewertung einbezogen werden müssen. Zweck und Speicherfrist müssen daher genau definiert sein.

109 Die Umsetzung der IT-Sicherheitsmaßnahmen sollte aktiv getestet und überwacht werden.

5.6.5. Datenaustausch

110 Es ist wichtig, die verschiedenen Szenarien zu ermitteln, in denen eine Sekundärnutzung oder ein Datenaustausch mit Dritten stattfinden kann. Die damit verbundenen Risiken sollten identifiziert werden, da dies bei der Definition und Gestaltung von Maßnahmen zur Risikominderung von Nutzen ist.

111 Detaillierte technische und praktische Empfehlungen zu der Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen durch die EU-Institutionen finden sich im einschlägigen Positionspapier des EDSB[45] sowie in Anhang 2 unter dem Punkt „Verarbeitung durch externe Organisationen und Übermittlungen personenbezogener Daten“.

R21: Personenbezogene Daten sollten ausschließlich über sichere Online-Kanäle übermittelt werden. Dies kann über vertrauenswürdige Netze, über einen Kanal, in dem die Daten verschlüsselt werden, oder mittels gleichwertiger Verfahren geschehen.

Beispiel: Werden personenbezogene Daten über öffentliche Netze wie das Internet versendet, müssen sie gegen die inhärenten Risiken dieser Netze wie das Abfangen von Daten geschützt werden.

Verschlüsselungstools sollten korrekt konfiguriert und die zugehörigen Chiffrierschlüssel sicher verwaltet werden.

112 Eine manuelle Datenübermittlung mittels nicht gesicherter Wechseldatenträger wie Speichersticks sollte ohne starke Verschlüsselung vermieden werden.

113 Die Übertragung personenbezogener Daten in einen Cloud- oder Online-Speicher, für den keine geeigneten Rahmenregelungen zur Zugangsberechtigung existieren, sollte

[45] Positionspapier des EDSB vom 14. Juli 2014 zur Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen durch Organe und Einrichtungen der EU.

vermieden werden. Die Nutzung von Anwendungen wie „Dropbox“ oder „Google Drive“ sollte geeigneten Risikomanagementmaßnahmen unterliegen.[46]

Beispiel: E-Mail- und Textverarbeitungsprogramme

Alle Institutionen verwenden E-Mail- und Textverarbeitungsprogramme. Sie sollten so konfiguriert werden, dass nur die unbedingt erforderlichen personenbezogenen Daten übermittelt werden. Dazu könnte es nötig werden, verborgene personenbezogene Daten vor ihrer Übermittlung aus Dateien zu entfernen.

114 Die für die Verarbeitung Verantwortlichen sollten bei Verwendung solcher Softwareprogramme alle erforderlichen Schutzvorkehrungen zu personenbezogenen Daten (HR-Daten, Gesundheitsdaten usw.) treffen.

R22: Institutionen, die sensible personenbezogene Daten per E-Mail übermitteln,[47] sollten sich über die inhärenten Datenschutzprobleme dieser Technologie im Klaren sein und diese in ihrer Risikobewertung berücksichtigen. Sie sollten gewährleisten, dass eine solche Übermittlung sicher ist, etwa durch die Verschlüsselung von Dateien oder die Verwendung einer sicheren E-Mail-Funktion, mit der sich Daten und Anhänge verschlüsseln lassen, oder durch die Versendung der Daten nur über vertrauenswürdige Netze.

115 Es sollten zusätzliche Maßnahmen erwogen werden, um das Kopieren von in Anwendungen gespeicherten personenbezogenen Daten in Textverarbeitungsprogramme auszuschließen.

5.6.6. Entsorgung[48]

R23: Es sollten Verfahren festgelegt und angewendet werden, die gewährleisten, dass die Anforderungen an den Schutz personenbezogener Daten erfüllt sind, wenn die Software und die Hardware entsorgt oder an einen anderen Ort verbracht werden.

116 Wenn ein IT-System veraltet ist bzw. verlagert oder nicht mehr benutzt wird, sollte besondere Aufmerksamkeit darauf verwendet werden, zu verhindern, dass personenbezogene Daten auf irgendeine Weise unbefugt offengelegt werden könnten.

117 Bei der Entsorgung eines IT-Systems sollten die vereinbarten Speicherfristen eingehalten werden.

---

[46] Denken Sie daran, dass es bei der Nutzung solcher Dienste zur Übermittlung personenbezogener Daten in ein Drittland kommen kann. Weitere Informationen finden sich in Anhang 1.

[47] Technisch gesehen enthält jede E-Mail personenbezogene Daten. Diese Empfehlung bezieht sich daher auf zusätzliche personenbezogene Daten in der eigentlichen Nachricht oder im Betreff.

[48] Informationen über die erforderlichen Kontrollmaßnahmen finden sich zum Beispiel in COBIT 5: Rahmenwerk für Governance und Management der Unternehmens-IT.

118 Der Zugriff auf veraltete Systeme mit personenbezogenen Daten sollte aufgehoben werden, falls kein Zugang mehr nötig oder nicht zu rechtfertigen ist.

119 Zur Entfernung elektronischer Dateien, die personenbezogene Daten enthalten, sollten Verfahren eingerichtet und Anleitungen verfasst werden. Darüber hinaus sollten Verfahren zur sicheren Entsorgung von Hardware (z. B. Speichermedien) eingerichtet werden.

5.7. Horizontale Prozesse

5.7.1. Beschaffung und Outsourcing

120 Wenn die Entwicklung eines IT-Systems geplant ist, muss entschieden werden, ob Arbeiten ausgelagert werden oder ob für das System Standardsoftware angeschafft werden soll. Sobald diese Entscheidung gefallen ist, wird ein Beschaffungsvorgang eingeleitet.

R24: In der Leistungsbeschreibung und den sonstigen Vertragsbedingungen sollten die technischen und organisatorischen Schutzvorkehrungen beschrieben sein, die der Auftragnehmer treffen sollte, um den Schutz der zu verarbeitenden personenbezogenen Daten, etwa in der Testphase, zu gewährleisten.

121 Hierzu können spezielle Mustervertragsklauseln für Datenschutzanforderungen verwendet werden. Personenbezogene Daten, die im Zusammenhang mit Beschaffungs- und den entsprechenden Auswahlverfahren verarbeitet werden, sind den Datenschutzbestimmungen gemäß zu schützen.[49]

122 Der Datenschutzbeauftragte/Datenschutzkoordinator sollte in den Beschaffungsvorgang eingebunden werden, damit seine Sachkenntnis zum Tragen kommen kann.

123 Falls entschieden wird, das IT-System, seine Entwicklung oder andere Teile des Prozesses auszulagern, sollte das IT-Management die zusätzlichen Risiken und die Grenzen der Eindämmung dieser Risiken berücksichtigen. Die Verantwortung liegt auch im Fall des Outsourcings weiterhin beim IT-Management als dem für die Verarbeitung Verantwortlichen. Das gesamte IT-Management sollte zudem sicherstellen, dass der Auftragnehmer alle zutreffenden Empfehlungen so weit wie möglich umsetzt.[50]

124 Die in Artikel 25 DSGVO vorgesehene Verpflichtung, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu betreiben, richtet sich lediglich an die für die Verarbeitung Verantwortlichen und gilt nicht direkt

[49] Leitlinien des EDSB zur Verarbeitung personenbezogener Daten im Rahmen der Vergabe von öffentlichen Aufträgen und Zuschüssen sowie der Auswahl und des Einsatzes von Experten.

[50] Ausführliche Informationen zum Outsourcing finden sich in Anhang 1.

für die Hersteller von Standardprodukten und die Anbieter von Standarddienstleistungen. In Erwägungsgrund 78 DSGVO wird allerdings betont, dass die Hersteller und Anbieter dazu ermutigt werden sollten, die Datenschutzgrundsätze bei der Entwicklung und Gestaltung zu berücksichtigen. Im selben Erwägungsgrund heißt es weiter: „*Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte auch bei öffentlichen Ausschreibungen Rechnung getragen werden.*“ Die EU-Institutionen sollten daher sicherstellen, dass sie ihre Beschaffungsverfahren für IT-Lösungen entsprechend ausgestalten.

5.7.2. Projektmanagement

125 Projektmanagement ist die Anwendung von Kenntnissen, Fertigkeiten, Instrumenten und Methoden auf Projektmaßnahmen zur Erfüllung der Projektanforderungen.[51]

5.7.2.1. Rollen und Zuständigkeiten

126 Die für den Datenschutz zuständige Person, z. B. der Datenschutzbeauftragte/Datenschutzkoordinator, sollte in jedes neue IT-Projekt eingebunden werden, bei dem in allen Projektphasen personenbezogene Daten verarbeitet werden, sowie bei der Ermittlung vorhandener Datenbanken oder Anwendungen helfen, in denen eine solche Verarbeitung stattfindet. Sie sollte gebeten werden, die Datenschutzanforderungen zu erläutern und dabei zu helfen, die angemessene Gestaltung und wirksame Umsetzung der Anforderungen auf eine Weise, die die Einhaltung der Datenschutzgesetze gewährleistet, zu überprüfen.

127 Sie sollte auch in der Konzeptionsphase eines Projekts um Rat gebeten werden, wenn bestimmt werden muss, ob es sich bei den in dem IT-System verarbeiteten Daten um personenbezogene Daten handelt oder nicht.

128 Ebenso wichtig ist ihre Unterstützung bei der Ermittlung und Bewertung sämtlicher Risiken, die mit der Verarbeitung personenbezogener Daten einhergehen.

R25: Der Projektmanager eines in Entwicklung befindlichen IT-Projekts oder der Systemeigner sollte eine angemessene Kommunikation mit der für den Datenschutz zuständigen Person (Datenschutzbeauftragter/Datenschutzkoordinator) sicherstellen.

129 Der Projektmanager sollte ferner dafür sorgen, dass die Datenschutzanforderungen, die bei der für den Datenschutz zuständigen Person erfragt wurden, umfassend analysiert und im System umgesetzt werden. Diese Anforderungen werden zu Beginn einer Projektphase (Konzeption und Entwurf) ermittelt.

[51] Definition des PMI (Project Management Institute).

5.7.2.2. Schulung zu den Datenschutzanforderungen

130 Der Projektmanager, das Projektteam (einschließlich des Entwicklungsteams) und die für den Betrieb und die Systempflege zuständigen Mitarbeiter sollten an einer gemeinsam mit dem Datenschutzbeauftragten organisierten Schulung zu den geltenden Datenschutzbestimmungen teilnehmen oder nachweisen können, dass sie die notwendigen Kenntnisse auf andere, gleichwertige Art erworben haben. Außerdem sollten sie über Technologien zum Schutz der Privatsphäre Bescheid wissen und ein Konzept für den Datenschutz durch Technikgestaltung verfolgen.

5.8. Standardsoftware

131 Standardsoftware ist auf dem Markt erhältlich.

132 Beim Erwerb sollte der gesamte Lebenszyklus einer Standardsoftware betrachtet werden: Beschreibung der Anforderungen, Wahl eines geeigneten Produkts, Installation und kundenspezifische Anpassung, Test, Produktionsfreigabe sowie Lizenzverwaltung und Entsorgung.

133 Die Inbetriebnahme der Standardsoftware lässt sich in folgende Phasen unterteilen:

a. Planung: Vor Auswahl der Standardsoftware sollte eine Liste mit den Anforderungen erstellt werden. Anhand dieser Liste lässt sich eine objektive und transparente Wahl der Software treffen. Falls eine eher komplexe Software gewählt wird, sollte in dieser Phase auch die für die Beschaffung verantwortliche Person hinzugezogen werden. Siehe die Abschnitte 5.1 und 5.2 sowie die Empfehlungen E6, E7, E8, E9 und E10.

b. Erwerb/Anschaffung: Anhand der erstellten Anforderungsliste kann geprüft werden, welches auf dem Markt befindliche Produkt die am besten geeigneten Funktionalitäten bietet. Siehe Abschnitt 5.7.1, Anhang 1 und Empfehlung E24.

c. Implementierung/Test: Die in der Dokumentation zu der Standardsoftware beschriebenen Funktionalitäten müssen getestet werden. Siehe die Abschnitte 5.4 und 5.5 sowie die Empfehlungen E12, E13 und E14.

d. Kundenspezifische Anpassung: Im Normalfall muss die Software an die Bedürfnisse und die rechtlichen Verpflichtungen der jeweiligen Institution angepasst werden.

e. Installation: Es ist wichtig, eine wirksame Lizenz- und Versionsverwaltung der Standardsoftware zu betreiben.

f. Betrieb und Pflege: Die während der Installation festgelegten Verfahren und Regeln müssen aufrechterhalten und regelmäßig überprüft werden. Siehe die Abschnitte 5.6, 5.6.2, 5.6.3, 5.6.4 und 5.6.5 sowie die Empfehlungen E15, E16, E17, E18, E19, E20, E21 und E22.

g. Entsorgung: Die angemessene Entsorgung der Standardsoftware erfordert häufig komplexe und umfangreiche Vorgänge. Siehe Abschnitt 5.6.6 sowie Empfehlung E23.

6. DAS MODELL DER DREI VERTEIDIGUNGSLINIEN

134 Das international anerkannte Modell der „Three Lines of Defence“ (drei Verteidigungslinien)[52] ist ein bewährtes Verfahren, um die Aufsicht über eine Organisation zu verbessern. Dieses Modell kann auch für den Datenschutzbereich als Orientierung dienen, da es bei der Einrichtung eines geeigneten Governance-Rahmens und der Stärkung der Rechenschaftspflicht innerhalb der Organisation behilflich sein kann.

135 Das Modell sieht drei Verteidigungslinien vor:

1. das operative Management
2. die Risikomanagement- und Compliance-Funktionen
3. die interne Revision

136 Dem Modell zufolge gibt die obere Führungsebene „den Ton an der Spitze“ der Organisation vor. Sie sollte allen Interessenträgern, die mit personenbezogenen Daten in Berührung kommen können, die Bedeutung des Schutzes dieser Daten verdeutlichen. Die obere Führungsebene sollte besondere Verantwortung für den Datenschutz übernehmen und eine für den Datenschutz zuständige Person bestimmen.

137 Um die Einhaltung der Datenschutzbestimmungen nachzuweisen und die Wirksamkeit der ergriffenen Maßnahmen zu prüfen, legt das operative Management geeignete Verfahren sowie die jeweiligen Rollen und Zuständigkeiten fest und führt Maßnahmen zur Kontrolle der Verfahren ein. All diese Elemente sind Bestandteil des internen Kontrollsystems einer Organisation. Die internen Kontrollsysteme sollten so beschaffen sein, dass die der betreffenden Einrichtung beim Erreichen ihrer Ziele helfen.[53]

138 Interne Kontrollen können unter anderem Strategien, Verfahren, technische und organisatorische Schutzmaßnahmen, Datenschutz-Folgenabschätzungen, Verhaltenskodizes sowie Sicherheits- und Datenschutzzertifizierungen umfassen.

139 Die Compliance-Funktionen in einer Organisation überwachen, ob die Kontrollen den einschlägigen Datenschutzbestimmungen Rechnung tragen, während die Revisoren dafür zuständig sind, der oberen Führungsebene die Wirksamkeit und Effizienz der Kontrollen unabhängig zu bestätigen.

140 Es wird empfohlen, bei der Erstellung eines Arbeitsplans für die interne Revision dafür zu sorgen, dass die Planungen auch die Prozesse und Funktionen innerhalb der Einrichtung in Verbindung mit der Verarbeitung personenbezogener Daten sowie die Zuständigkeiten für den Schutz der personenbezogenen Daten abdecken.

---

[52] Positionspapier der IIA: The Three Lines of Defense in Effective Risk Management and Control, Altamonte Springs, FL: The Institute of Internal Auditors Inc, Januar 2013.

[53] Eine weit gefasste Definition der internen Kontrolle ist in der Haushaltsordnung (Artikel 32 Absatz 2) zu finden. Diese Definition ist eng an die Standarddefinition des Committee of Sponsoring Organizations of the Treadway Commission (COSO) der internen Kontrolle angelehnt.

141 Bei einer solchen Revision wird bewertet, inwieweit das interne Kontrollsystem wirksam und geeignet ist, die Risiken von Verstößen gegen die Datenschutzbestimmungen zu minimieren.

R26: Die internen Revisoren sollten in die Bewertung des internen Kontrollsystems eingebunden werden, das zur Einhaltung der Datenschutzbestimmungen eingerichtet wurde.

ANHÄNGE

Anhang 1: Verarbeitung durch externe Organisationen und Übermittlung personenbezogener Daten

Allgemeine Erwägungen

142 Falls IT-Dienste von Dritten erbracht werden, müssen die EU-Institutionen die Risiken für den Datenschutz sowie die Verlässlichkeit dieser Dritten mit Blick auf die Datenschutz- und Informationsrisiken bewerten.

143 Wenn EU-Institutionen die Dienste eines Auftragnehmers oder einer anderen externen Organisation zur Wahrnehmung ihrer Aufgaben in Anspruch nehmen, kann es sein, dass von den Institutionen erhobene personenbezogene Daten von institutionsfremden Organisationen verarbeitet werden. In diesem Fall handelt die externe Organisation im Auftrag der Institution als Auftragsverarbeiter, so dass Artikel 23 der Verordnung zur Anwendung kommt.

144 Sollte die externe Organisation die von EU-Institutionen erhobenen personenbezogenen Daten jedoch für ihre eigenen Zwecke verarbeiten, ist sie darüber hinaus als für die Verarbeitung Verantwortlicher anzusehen, dem Daten übermittelt oder zugänglich gemacht werden. Für diese Übermittlung personenbezogener Daten[54] gelten die Bestimmungen der Artikel 7, 8 und 9 der Verordnung.

145 Die Mitarbeiter der externen Organisation sollten der Vereinbarung über Sicherheitsüberprüfungen unterliegen, um sicherzugehen, dass sie, was den Zugriff auf personenbezogene Daten angeht, als verlässlich angesehen werden können.

146 Gemäß der Verordnung sind in beiden Fällen Gründe für die Zulässigkeit der Verarbeitung personenbezogener Daten durch die externe Organisation sowie besondere Garantien erforderlich. Die Institution muss die Rolle der vorgesehenen externen Organisation, die an der Verarbeitung personenbezogener Daten mitwirken soll, definieren. Besondere Sorgfalt ist bei Übermittlung personenbezogener Daten an Länder außerhalb der EU/des EWR und an internationale Organisationen nötig.

---

[54] Eine Übermittlung personenbezogener Daten beinhaltet normalerweise folgende Elemente: Mitteilung, Weitergabe oder sonstige Bereitstellung personenbezogener Daten, vorgenommen mit dem Wissen oder in der Absicht eines der Verordnung unterworfenen Übermittlers, dass der oder die Empfänger Zugriff darauf haben. Diese Elemente gelten für die Übermittlung innerhalb von oder zwischen Organen und Einrichtungen der Union (Artikel 7), die Übermittlung an Empfänger, die der Richtlinie 95/46/EG / DSGVO unterworfen sind (Artikel 8), und die Übermittlung an Drittländer und internationale Organisationen (Artikel 9). Der Begriff deckt sowohl beabsichtigte Übermittlungen als auch den zugelassenen Zugriff auf die Daten durch die Empfänger ab. Aufgrund der Bedingungen „Wissen“ und „Absicht“ sind Fälle des ungesetzlichen Zugriffs (z. B. Hacking) ausgeschlossen. Siehe Abschnitt 3.1. im Positionspapier des EDSB zur Übermittlung personenbezogener Daten an Drittländer.

147 Wenn Daten einer externen Organisation außerhalb der EU zugänglich gemacht werden, gilt Artikel 9 der Verordnung, und zwar unabhängig davon, ob der Empfänger als Auftragsverarbeiter oder als zusätzlicher für die Verarbeitung Verantwortlicher handelt. Detaillierte Empfehlungen zur Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen durch EU-Institutionen finden sich auch im einschlägigen Positionspapier des EDSB.[55]

Externe Organisation als Auftragsverarbeiter

148 Wenn die externe Organisation als Auftragsverarbeiter für die EU-Institution fungiert, gilt hinsichtlich der Beziehung zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter sowie der Verpflichtungen des Auftragsverarbeiters Artikel 23 der Verordnung.[56]

149 Wenn der Auftragsverarbeiter eine außerhalb der EU ansässige externe Organisation ist, gilt neben Artikel 23 der Verordnung zusätzlich auch Artikel 9. Wenn eine nicht in der EU ansässige Organisation IT-Dienste erbringt, ist es wichtig, bei der Wahl des Auftragsverarbeiters die Bestimmungen von Artikel 9 zu berücksichtigen und das Schutzniveau zu prüfen, das der Auftragsverarbeiter in Bezug auf personenbezogene Daten bietet.

150 Die Institution muss sicherstellen, dass der externe Auftragsverarbeiter gemäß Artikel 23 der Verordnung nur in ihrem Auftrag und auf ihre Weisung handelt. Dies muss in einem Vertrag zwischen der Institution und dem Auftragsverarbeiter schriftlich niedergelegt werden, wobei der Vertrag klare Datenschutzvorgaben, etwa zur Sicherheit sowie zu den technischen und organisatorischen Maßnahmen enthalten muss, die der Auftragsverarbeiter gemäß den Artikeln 21 and 22 der Verordnung zu treffen hat.

151 Die Institution muss dem Auftragsverarbeiter von einer IT-Risikobewertung ausgehend klare Anweisungen zu den Sicherheitsanforderungen und Schutzmaßnahmen geben und sich vergewissern, dass der Auftragsverarbeiter diese Maßnahmen tatsächlich eingerichtet hat.

Externe Organisation als für die Verarbeitung Verantwortlicher

152 Die EU-Institutionen sollten es grundsätzlich vermeiden, externe Einrichtungen in die Lage zu versetzen, als für die Verarbeitung personenbezogener Daten Verantwortlicher zu fungieren, es sei denn, dies ist zum Erreichen ihrer institutionellen Ziele erforderlich, zum Beispiel wenn die EU-Institution mit einer internationalen Organisation im humanitären oder einem anderen Bereich zusammenarbeitet.

---

[55] Positionspapier vom 14. Juli 2014 zur Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen durch Organe und Einrichtungen der EU.

[56] Die Artikel 7 und 8 der Verordnung sind nicht anwendbar, wenn EU-Institutionen einem in der EU ansässigen Auftragsverarbeiter Daten zugänglich machen, da dieser direkt der Verantwortung des für die Verarbeitung Verantwortlichen untersteht.

153 Die Artikel 7, 8 und 9 der Verordnung regeln die Übermittlung personenbezogener Daten. Die Institutionen dürfen personenbezogene Daten nur dann übermitteln, wenn die Erfordernis dazu besteht. Die Empfänger der gemäß den Artikeln 7, 8 oder 9 der Verordnung übermittelten personenbezogenen Daten dürfen diese Daten nur für die Zwecke verarbeiten, für die sie übermittelt wurden.

154 Wenn eine externe Organisation als für die Verarbeitung Verantwortlicher fungiert, d. h. die Daten für ihre eigenen Zwecke verarbeitet, sollte sie sämtliche mit dieser Verantwortung einhergehenden Pflichten übernehmen, also auch die Verpflichtung, personenbezogene Daten nur an Empfänger zu übermitteln, wenn ein angemessenes Schutzniveau besteht und die Übermittlung ausschließlich die Wahrnehmung von Aufgaben des für die Verarbeitung Verantwortlichen ermöglichen soll.

155 Die Institutionen sollten betroffenen Personen gegenüber folgende Angaben machen, um Transparenz in Bezug auf ihre IT-Dienste herzustellen:

a. Welche Verarbeitungsvorgänge werden von der Organisation in ihrer Rolle als Auftragsverarbeiter und welche in ihrer Rolle als für die Verarbeitung Verantwortlicher durchgeführt?

b. Welche Datenschutzpraktiken verfolgt die externe Organisation in ihrer Rolle als für die Verarbeitung Verantwortlicher?

Anhang 2: Datenschutzempfehlungen zu den verschiedenen Phasen im Lebenszyklus eines IT-Systems

Phasen im Lebenszyklus eines IT-Systems	Prozesse und Teilprozesse	Empfehlungen	Allgemeine Empfehlung
Konzeption		**E6:** Zunächst sollte bestimmt werden, ob Daten, die in dem betreffenden IT-System verarbeitet werden, personenbezogene Daten sind oder ob sie infolge der Verarbeitung zu personenbezogenen Daten werden können**.**	**In jeder Phase des Lebenszyklus eines IT-Systems sollten die allgemein anerkannten Datenschutzgrundsätze eingehalten werden (siehe Abschnitt 4.1)**
		E7: Die wichtigsten Datenschutzanforderungen („High-Level Requirements“) sollten in einer Projektcharta aufgeführt werden. Dieses Dokument dient der Beschreibung des Projektumfangs und der wichtigsten Anforderungen, die sich aus der Konzeptionsphase ergeben.	
Entwurf	Ermittlung der Anforderungen	**E8:** Die Datenschutzanforderungen sollten bei den Interessenträgern ermittelt und während der IT-Systemspezifikation dokumentiert werden.	
	Design	**E9:** Wenn in einem IT-System besonders sensible (personenbezogene) Daten, etwa zur körperlichen oder geistigen Gesundheit, zur ethnischen Herkunft, zu politischen oder religiösen Überzeugungen oder zu Vorstrafen, verarbeitet werden, sollten zusätzliche Schutzvorkehrungen getroffen werden, etwa in Form einer Verschlüsselung oder von mehrstufigen Zugangskontrollen, um die Risiken der Verarbeitung zu mindern.	
		E10: Beim Entwurf eines IT-Systems sollten geeignete Maßnahmen geplant werden, die es erlauben, die Speicherfrist angemessen zu verwalten und die nach deren Ablauf erforderlichen Maßnahmen (wie Anonymisierung oder Löschung) zu ergreifen.	
	Entwicklung	**E11:** Es ist wichtig, dass das Entwicklungsteam und die	

Phasen im Lebenszyklus eines IT-Systems	Prozesse und Teilprozesse	Empfehlungen	Allgemeine Empfehlung
Konstruktion		Interessenträger eine gemeinsame Verständnisgrundlage besitzen. Die Datenschutzgesetze und -bestimmungen sollten dem Entwicklungsteam schon vor Beginn der Entwicklungsphase bewusst sein. Dies lässt sich etwa dadurch sicherstellen, dass der Datenschutzbeauftragte Schulungen für bestehende und neue Entwicklungsteams organisiert oder gleichwertige Maßnahmen ergriffen werden.	
	Test	**E12:** Für die Tests sind Verfahren und Anweisungen zu entwickeln, die die Einhaltung der Datenschutzanforderungen gewährleisten.	
		E13: Bei der Simulation einer Liveumgebung sollte die Erhebung personenbezogener Echtdaten vermieden werden.	
Übergabe und Auslieferung		**E14:** Endnutzer, Systemadministratoren und die für die Systempflege zuständigen Mitarbeiter sollten sich der Datenschutzbestimmungen bewusst sein.	
Betrieb und Pflege		**E15: Der für die Verarbeitung Verantwortliche sollte dem Datenschutzbeauftragten der Institution jede Verarbeitung personenbezogener Daten in einer Datenbank oder einem IT-System melden.**	
		E16: Die maximale Speicherfrist für Daten auf Speichermedien sollte so festgelegt werden, dass sie den vertraglichen, gesetzlichen und regulatorischen Anforderungen entspricht. Die Speicherfrist kann je nach Speicherzweck variieren.	
	Information der betroffenen Personen und Transparenz	**E17:** Die Institution sollte geeignete Informationshinweise zu den Verarbeitungsvorgängen erstellen und den betroffenen Personen über Informationskanäle zugänglich machen.	
	Zugangsverwaltung	**E18:** Der Systemeigner sollte Verfahren zur Benutzerverwaltung sowie Genehmigungsverfahren, etwa	

Phasen im Lebenszyklus eines IT-Systems	Prozesse und Teilprozesse	Empfehlungen	Allgemeine Empfehlung
		hinsichtlich der Zugangsgewährung zum System, festlegen und anwenden.	
	Änderungsverwaltung	**E19:** Es sollten formelle Verfahren für die Änderungsverwaltung festgelegt und angewendet werden, damit alle Anträge auf Änderungen im Informationssystem einheitlich gehandhabt werden.	
	Sicherheitskontrollen	**E20:** Der Zugriff auf Dateien mit personenbezogenen Daten sollte ständig überwacht werden.	
	Datenaustausch	**E21:** Personenbezogene Daten sollten ausschließlich über sichere Online-Kanäle übermittelt werden. Dies kann über vertrauenswürdige Netze, über einen Kanal, in dem die Daten verschlüsselt werden, oder mittels gleichwertiger Verfahren geschehen.	
		E22: Institutionen, die sensible personenbezogene Daten per E-Mail übermitteln, sollten sich über die inhärenten Datenschutzprobleme dieser Technologie im Klaren sein und diese in ihrer Risikobewertung berücksichtigen. Sie sollten gewährleisten, dass eine solche Übermittlung sicher ist, etwa durch die Verschlüsselung von Dateien oder die Verwendung einer sicheren E-Mail-Funktion, mit der sich Daten und Anhänge verschlüsseln lassen, oder durch die Versendung der Daten nur über vertrauenswürdige Netze.	
	Entsorgung	**E23:** Es sollten Verfahren festgelegt und angewendet werden, die gewährleisten, dass die Anforderungen an den Schutz personenbezogener Daten erfüllt sind, wenn die Software und die Hardware entsorgt oder an einen anderen Ort verbracht werden.	
Horizontale Prozesse	Beschaffung	**E24:** In der Leistungsbeschreibung und den sonstigen Vertragsbedingungen sollten die technischen und organisatorischen Schutzvorkehrungen	

Phasen im Lebenszyklus eines IT-Systems	Prozesse und Teilprozesse	Empfehlungen	Allgemeine Empfehlung
		beschrieben sein, die der Auftragnehmer treffen sollte, um den Schutz der zu verarbeitenden personenbezogenen Daten, etwa in der Testphase, zu gewährleisten.	
	Projektmanagement	**E25:** Der Projektmanager eines in Entwicklung befindlichen IT-Projekts oder der Systemeigner sollte eine angemessene Kommunikation mit der für den Datenschutz zuständigen Person (Datenschutzbeauftragter/Datenschutzkoordinator) sicherstellen.	
	Governance	**E1:** Es ist äußerst wichtig, dass die Führungsebene die Datenschutzgrundsätze unmissverständlich unterstützt.	
		E2: Wenn die obere Führungsebene die Rolle des für die Verarbeitung Verantwortlichen ausfüllt, hat sie die Verantwortung für den Datenschutz zu tragen. Falls sie nicht in der Rolle des Verantwortlichen ist, sollte die obere Führungsebene dennoch besondere Verantwortung für den Datenschutz übernehmen, um die Einhaltung der Datenschutzvorschriften zu gewährleisten.	
		E3: Die obere Führungsebene sollte die Verantwortung für den Datenschutz übernehmen und ferner eine für den Datenschutz zuständige Person (z. B. einen Datenschutzbeauftragten oder Datenschutzkoordinator) ernennen und dieser ein Mandat zur Umsetzung der Datenschutzmaßnahmen erteilen.	
		E4: Sämtliche Mitarbeiter sollten gut über die bestehenden Datenschutzstrategien und -verfahren Bescheid wissen. Dies lässt sich beispielsweise durch verpflichtende Einführungskurse, die Bereitstellung von Informationsmaterial oder Auffrischungsprogramme gewährleisten.	
		E5: Die mit dem Datenschutz verbundenen Strategien, Verfahren, Zuständigkeiten und Funktionen sollten regelmäßig überwacht und aufrechterhalten werden.	

Phasen im Lebenszyklus eines IT-Systems	Prozesse und Teilprozesse	Empfehlungen	Allgemeine Empfehlung
		E26: Die internen Revisoren sollten in die Bewertung des internen Kontrollsystems eingebunden werden, das zur Einhaltung der Datenschutzbestimmungen eingerichtet wurde.	