

DIN EN ISO/IEC 27701

ICS 35.030

**Sicherheitstechniken –
Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management
von Informationen zum Datenschutz –
Anforderungen und Leitlinien (ISO/IEC 27701:2019);
Deutsche Fassung EN ISO/IEC 27701:2021**

Security techniques –
Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management –
Requirements and guidelines (ISO/IEC 27701:2019);
German version EN ISO/IEC 27701:2021

Techniques de sécurité –
Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection
de la vie privée –
Exigences et lignes directrices (ISO/IEC 27701:2019);
Version allemande EN ISO/IEC 27701:2021

Gesamtumfang 88 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC 27701:2019 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 27701:2021 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

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

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

ISO/IEC 27000	siehe	DIN EN ISO/IEC 27000
ISO/IEC 27001:2013	siehe	DIN EN ISO/IEC 27001:2017-06
ISO/IEC 27002:2013	siehe	DIN EN ISO/IEC 27002:2017-06
ISO/IEC 27018	siehe	DIN EN ISO/IEC 27018
ISO/IEC 29100	siehe	DIN EN ISO/IEC 29100
ISO/IEC 29101	siehe	DIN EN ISO/IEC 29101
ISO/IEC 29134	siehe	DIN EN ISO/IEC 29134

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 27000, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Überblick und Terminologie*

DIN EN ISO/IEC 27001:2017-06, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27001:2017*

DIN EN ISO/IEC 27002:2017-06, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017*

DIN EN ISO/IEC 27018, *Informationstechnik — Sicherheitsverfahren — Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung*

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

DIN EN ISO/IEC 29101, *Informationstechnik — Sicherheitstechniken — Rahmenwerk für Datenschutz*

DIN EN ISO/IEC 29134, *Informationstechnik — Sicherheitsverfahren — Leitlinien für die Datenschutz-Folgenabschätzung*

— Leerseite —

Deutsche Fassung

Sicherheitstechniken —
Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das
Management von Informationen zum Datenschutz —
Anforderungen und Leitlinien (ISO/IEC 27701:2019)

Security techniques —
Extension to ISO/IEC 27001 and ISO/IEC 27002
for privacy information management —
Requirements and guidelines (ISO/IEC 27701:2019)

Techniques de sécurité —
Extension d'ISO/IEC 27001 et ISO/IEC 27002 au
management de la protection de la vie privée —
Exigences et lignes directrices (ISO/IEC 27701:2019)

Diese Europäische Norm wurde vom CEN am 12. April 2021 angenommen.

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

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

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



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

Inhalt

	Seite
Europäisches Vorwort	6
Vorwort	7
Einleitung	8
1 Anwendungsbereich	9
2 Normative Verweisungen	9
3 Begriffe	9
4 Allgemeines	10
4.1 Aufbau dieses Dokuments	10
4.2 Anwendung der Anforderungen von ISO/IEC 27001:2013	10
4.3 Anwendung der Leitlinien von ISO/IEC 27002:2013	11
4.4 Kunde	12
5 PIMS-spezifische Anforderungen in Bezug auf ISO/IEC 27001	12
5.1 Allgemeines	12
5.2 Kontext der Organisation	13
5.2.1 Verstehen der Organisation und ihres Kontextes	13
5.2.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien	13
5.2.3 Festlegung des Anwendungsbereichs des Informationssicherheitsmanagementsystems	14
5.2.4 Managementsystem für Informationssicherheit	14
5.3 Führung	14
5.3.1 Führung und Verpflichtung	14
5.3.2 Politik	14
5.3.3 Organisatorische Rollen, Verantwortlichkeiten und Befugnisse	14
5.4 Planung	14
5.4.1 Aktionen zum Umgang mit Risiken und Chancen	14
5.4.2 Informationssicherheitsziele und Planung zu deren Erreichung	15
5.5 Unterstützung	16
5.5.1 Ressourcen	16
5.5.2 Kompetenz	16
5.5.3 Bewusstsein	16
5.5.4 Kommunikation	16
5.5.5 Dokumentierte Information	16
5.6 Betrieb	16
5.6.1 Betriebliche Planung und Steuerung	16
5.6.2 Beurteilung von Informationssicherheitsrisiken	16
5.6.3 Informationssicherheitsrisikobehandlung	16
5.7 Bewertung der Leistung	17
5.7.1 Überwachung, Messung, Analyse und Bewertung	17
5.7.2 Internes Audit	17
5.7.3 Managementbewertung	17
5.8 Verbesserung	17
5.8.1 Nichtkonformität und Korrekturmaßnahmen	17
5.8.2 Fortlaufende Verbesserung	17
6 PIMS-spezifische Leitlinien in Bezug auf ISO/IEC 27002	17
6.1 Allgemeines	17

6.2	Informationssicherheitsrichtlinien.....	17
6.2.1	Vorgaben der Leitung für Informationssicherheit.....	17
6.3	Organisation der Informationssicherheit	18
6.3.1	Interne Organisation.....	18
6.3.2	Mobilgeräte und Telearbeit.....	19
6.4	Personalsicherheit.....	19
6.4.1	Vor Beginn eines Anstellungsverhältnisses	19
6.4.2	Während des Anstellungsverhältnisses.....	20
6.4.3	Beendigung und Änderung des Anstellungsverhältnisses.....	20
6.5	Verwaltung der Werte	20
6.5.1	Verantwortlichkeit für Werte	20
6.5.2	Informationsklassifizierung.....	21
6.5.3	Handhabung von Datenträgern.....	21
6.6	Zugangssteuerung.....	22
6.6.1	Geschäftsanforderungen an die Zugangssteuerung	22
6.6.2	Benutzerzugangsverwaltung	23
6.6.3	Benutzerverantwortlichkeiten	24
6.6.4	Zugangssteuerung für Systeme und Anwendungen	24
6.7	Kryptographie	25
6.7.1	Kryptographische Maßnahmen	25
6.8	Physische und umgebungsbezogene Sicherheit	25
6.8.1	Sicherheitsbereiche.....	25
6.8.2	Geräte und Betriebsmittel.....	26
6.9	Betriebssicherheit.....	27
6.9.1	Betriebsabläufe und -verantwortlichkeiten.....	27
6.9.2	Schutz vor Schadsoftware	27
6.9.3	Datensicherung	28
6.9.4	Protokollierung und Überwachung.....	29
6.9.5	Steuerung von Software im Betrieb.....	30
6.9.6	Handhabung technischer Schwachstellen.....	30
6.9.7	Überlegungen für Audits von Informationssystemen.....	30
6.10	Kommunikationssicherheit.....	30
6.10.1	Netzwerksicherheitsmanagement.....	30
6.10.2	Informationsübertragung	30
6.11	Anschaffung, Entwicklung und Instandhaltung von Systemen.....	31
6.11.1	Sicherheitsanforderungen an Informationssysteme	31
6.11.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen.....	32
6.11.3	Testdaten.....	34
6.12	Lieferantenbeziehungen.....	34
6.12.1	Informationssicherheit in Lieferantenbeziehungen	34
6.12.2	Steuerung der Dienstleistungserbringung von Lieferanten.....	35
6.13	Handhabung von Informationssicherheitsvorfällen.....	35
6.13.1	Handhabung von Informationssicherheitsvorfällen und -verbesserungen	35
6.14	Informationssicherheitsaspekte beim Business Continuity Management	38
6.14.1	Aufrechterhalten der Informationssicherheit.....	38
6.14.2	Redundanzen	38
6.15	Einhaltung	38
6.15.1	Einhaltung gesetzlicher und vertraglicher Anforderungen	38
6.15.2	Überprüfungen der Informationssicherheit	39
7	Zusätzliche Leitlinie für verantwortliche Stellen nach ISO/IEC 27002	40
7.1	Allgemeines	40
7.2	Bedingungen für die Erhebung und Verarbeitung.....	40
7.2.1	Identifizieren und Dokumentieren des Zwecks.....	40
7.2.2	Identifizieren der rechtmäßigen Grundlage	41
7.2.3	Bestimmen, wann und wie die Einwilligung einzuholen ist	42

7.2.4	Einholung und Aufzeichnung der Einwilligung	42
7.2.5	Datenschutz-Folgenabschätzung	42
7.2.6	Verträge mit Auftragsverarbeitern	43
7.2.7	Gemeinsame verantwortliche Stelle	43
7.2.8	Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten	44
7.3	Verpflichtungen gegenüber betroffenen Personen	45
7.3.1	Bestimmung und Erfüllung von Verpflichtungen gegenüber betroffenen Personen	45
7.3.2	Bestimmen von Informationen für betroffene Personen	46
7.3.3	Bereitstellen von Informationen für betroffene Personen	47
7.3.4	Bereitstellung eines Mechanismus zur Änderung oder zum Widerruf der Einwilligung	47
7.3.5	Bereitstellung eines Mechanismus zur Ablehnung der Verarbeitung personenbezogener Daten	48
7.3.6	Zugriff, Korrektur und/oder Löschung	48
7.3.7	Verpflichtungen von verantwortlichen Stellen, Dritte zu informieren	49
7.3.8	Bereitstellung einer Kopie der verarbeiteten personenbezogenen Daten	49
7.3.9	Handhabung von Anfragen	50
7.3.10	Automatisierte Entscheidungsfindung	50
7.4	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen	51
7.4.1	Beschränkte Erhebung	51
7.4.2	Beschränkte Verarbeitung	51
7.4.3	Genauigkeit und Qualität	51
7.4.4	Ziele der Sparsamkeit personenbezogener Daten	52
7.4.5	Entpersonalisierung personenbezogener Daten und Löschung am Ende der Verarbeitung	53
7.4.6	Temporäre Dateien	53
7.4.7	Aufbewahrung	53
7.4.8	Entsorgung	54
7.4.9	Maßnahmen zur Übertragung personenbezogener Daten	54
7.5	Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten	54
7.5.1	Ermittlung der Grundlage für die Übertragung von personenbezogenen Daten zwischen Rechtssystemen	54
7.5.2	Länder und internationale Organisationen, an die personenbezogene Daten übertragen werden können	55
7.5.3	Aufzeichnungen über die Übertragung von personenbezogenen Daten	55
7.5.4	Aufzeichnungen der Offenlegung von personenbezogenen Daten für Dritte	55
8	Zusätzliche Leitlinie für Auftragsverarbeiter nach ISO/IEC 27002	56
8.1	Allgemeines	56
8.2	Bedingungen für die Erhebung und Verarbeitung	56
8.2.1	Kundenvereinbarung	56
8.2.2	Ziele der Organisation	57
8.2.3	Verwendung für Marketing und Werbung	57
8.2.4	Verstoßende Anweisung	57
8.2.5	Kundenverpflichtungen	58
8.2.6	Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten	58
8.3	Verpflichtungen gegenüber betroffenen Personen	58
8.3.1	Verpflichtungen gegenüber betroffenen Personen	58
8.4	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen	59
8.4.1	Temporäre Dateien	59
8.4.2	Rückgabe, Übertragung oder Entsorgung von personenbezogenen Daten	59
8.4.3	Maßnahmen zur Übertragung personenbezogener Daten	60
8.5	Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten	60
8.5.1	Grundlage für die Übertragung von personenbezogenen Daten zwischen Rechtssystemen	60

8.5.2	Länder und internationale Organisationen, an die personenbezogene Daten übertragen werden können	61
8.5.3	Aufzeichnungen der Offenlegung von personenbezogenen Daten für Dritte	62
8.5.4	Benachrichtigung über Anträge auf Offenlegung von personenbezogenen Daten	62
8.5.5	Rechtsverbindliche Offenlegung von personenbezogenen Daten.....	62
8.5.6	Offenlegung von Unterauftragnehmern, die zur Verarbeitung von personenbezogenen Daten eingesetzt werden	63
8.5.7	Einschaltung eines Unterauftragnehmers mit der Verarbeitung von personenbezogenen Daten	63
8.5.8	Wechsel des Unterauftragnehmers zur Verarbeitung von personenbezogenen Daten.....	64
Anhang A (normativ) PIMS-spezifische Referenzmaßnahmenziele und -Maßnahmen (verantwortliche Stelle).....		65
Anhang B (normativ) PIMS-spezifische Referenzmaßnahmenziele und -Maßnahmen (Auftragsverarbeiter)		69
Anhang C (informativ) Zuordnung zu ISO/IEC 29100.....		72
Anhang D (informativ) Zuordnung zur Datenschutz-Grundverordnung		75
Anhang E (informativ) Zuordnung zu ISO/IEC 27018 und ISO/IEC 29151		79
Anhang F (informativ) Anwendung von ISO/IEC 27701 auf ISO/IEC 27001 und ISO/IEC 27002		82
F.1	Anwendung dieses Dokuments	82
F.2	Beispiel für die Präzisierung von Sicherheitsnormen.....	83
Literaturhinweise.....		84

Europäisches Vorwort

Der Text von ISO/IEC 27701:2019 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 27701:2021 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Oktober 2021, und etwaige entgegenstehende nationale Normen müssen bis Oktober 2021 zurückgezogen werden.

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

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

Anerkennungsnotiz

Der Text von ISO/IEC 27701:2019 wurde von CEN als EN ISO/IEC 27701:2021 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.

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) oder in der IEC-Liste der erhaltenen Patenterklärungen (siehe <http://patents.iec.ch>).

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/TC JTC 1, *Information technology*, Unterkomitee SC 27, *Security techniques* erarbeitet.

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

0.1 Allgemeines

Fast jede Organisation verarbeitet personenbezogene Daten (PII, en: Personally Identifiable Information). Darüber hinaus nehmen die Menge und die Arten der verarbeiteten personenbezogenen Daten zu, ebenso wie die Anzahl der Situationen, in denen eine Organisation mit anderen Organisationen bei der Verarbeitung von personenbezogenen Daten zusammenarbeiten muss. Der Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung von personenbezogenen Daten ist ein gesellschaftliches Bedürfnis sowie Gegenstand spezieller Gesetze und/oder Vorschriften auf der ganzen Welt.

Das in ISO/IEC 27001 definierte Managementsystem für Informationssicherheit (ISMS, en: Information Security Management System) ist so konzipiert, dass branchenspezifische Anforderungen hinzugefügt werden können, ohne dass ein neues Managementsystem entwickelt werden muss. ISO-Managementsystemnormen, einschließlich der branchenspezifischen Normen, sind so konzipiert, dass sie entweder getrennt oder als kombiniertes Managementsystem umgesetzt werden können.

Die Anforderungen und Leitlinien für den Schutz personenbezogener Daten variieren je nach dem Kontext der Organisation, insbesondere dort, wo nationale Gesetze und/oder Vorschriften bestehen. Die ISO/IEC 27001 verlangt, dass dieser Kontext verstanden und berücksichtigt wird. Dieses Dokument beinhaltet eine Zuordnung:

- zum Rahmenwerk für Datenschutz und zu den in ISO/IEC 29100 definierten Grundsätzen;
- zur ISO/IEC 27018;
- zur ISO/IEC 29151; und
- zur EU-Datenschutz-Grundverordnung.

Diese müssen jedoch unter Umständen interpretiert werden, um die lokalen Gesetze und/oder Vorschriften zu berücksichtigen.

Dieses Dokument kann von verantwortlichen Stellen (einschließlich den gemeinsamen verantwortlichen Stellen) und Auftragsverarbeitern (einschließlich denjenigen, die Auftragsverarbeiter im Unterauftrag einsetzen und denjenigen, die personenbezogene Daten als Unterauftragnehmer für Auftragsverarbeiter verarbeiten) verwendet werden.

Eine Organisation, die die Anforderungen in diesem Dokument erfüllt, wird einen dokumentierenden Nachweis darüber erbringen, wie sie mit der Verarbeitung personenbezogener Daten umgeht. Dieser Nachweis kann verwendet werden, um Vereinbarungen mit Geschäftspartnern zu erleichtern, bei denen die Verarbeitung von personenbezogenen Daten für beide Seiten von Bedeutung ist. Dies kann auch bei den Beziehungen zu anderen interessierten Parteien hilfreich sein. Die Verwendung dieses Dokuments in Verbindung mit ISO/IEC 27001 kann, falls gewünscht, eine unabhängige Verifizierung dieses Nachweises liefern.

Dieses Dokument wurde ursprünglich als ISO/IEC 27552 entwickelt.

0.2 Kompatibilität mit anderen Managementsystemnormen

Dieses Dokument wendet das von ISO entwickelte Rahmenwerk an, um die Angleichung zwischen ihren Managementsystemnormen zu verbessern.

Dieses Dokument ermöglicht es einer Organisation, ihr Managementsystem für Informationen zum Datenschutz an die Anforderungen anderer Managementsystemnormen anzugleichen oder es entsprechend zu integrieren.

1 Anwendungsbereich

Dieses Dokument legt Anforderungen fest und bietet eine Leitlinie für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Managementsystems für Informationen zum Datenschutz (PIMS, en: Privacy Information Management System) in Form einer Erweiterung der ISO/IEC 27001 und ISO/IEC 27002 für das Datenschutzmanagement im Kontext der Organisation.

Dieses Dokument legt die PIMS-bezogenen Anforderungen fest und bietet eine Leitlinie für verantwortliche Stellen und Auftragsverarbeiter, die für die Verarbeitung von personenbezogenen Daten verantwortlich und rechenschaftspflichtig sind.

Dieses Dokument ist auf alle Arten und Größen von Organisationen, einschließlich öffentlicher und privater Unternehmen, öffentlicher Stellen und gemeinnütziger Organisationen, anwendbar, die verantwortliche Stellen und/oder Auftragsverarbeiter im Rahmen eines ISMS 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 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

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

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 27000; ISO/IEC 29100 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>

3.1

gemeinsame verantwortliche Stelle

verantwortliche Stelle, die gemeinsam mit einer oder mehreren anderen verantwortlichen Stellen die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten festlegt

3.2

Managementsystem für Datenschutzinformationen

PIMS; en: privacy information management system

Managementsystem für Informationssicherheit, das sich mit dem Schutz der durch die Verarbeitung personenbezogener Daten möglicherweise beeinträchtigten Privatsphäre befasst

4 Allgemeines

4.1 Aufbau dieses Dokuments

Dies ist ein branchenspezifisches Dokument, das sich auf ISO/IEC 27001:2013 und ISO/IEC 27002:2013 bezieht.

Dieses Dokument konzentriert sich auf die PIMS-spezifischen Anforderungen. Die Übereinstimmung mit diesem Dokument basiert auf der Einhaltung dieser Anforderungen und der Anforderungen in ISO/IEC 27001:2013. Dieses Dokument erweitert die Anforderungen von ISO/IEC 27001:2013, um neben der Informationssicherheit auch den Schutz der Privatsphäre von betroffenen Personen zu berücksichtigen, die durch die Verarbeitung personenbezogener Daten möglicherweise beeinträchtigt ist. Zum besseren Verständnis sind eine Leitlinie zur Umsetzung und weitere Informationen zu den Anforderungen enthalten.

Abschnitt 5 enthält PIMS-spezifische Anforderungen und weitere Informationen zu den Anforderungen an die Informationssicherheit nach ISO/IEC 27001, die für eine Organisation gelten, die entweder als verantwortliche Stelle oder als Auftragsverarbeiter tätig ist.

ANMERKUNG 1 Der Vollständigkeit halber enthält Abschnitt 5 einen Unterabschnitt für jeden der Abschnitte, die Anforderungen in ISO/IEC 27001:2013 enthalten, selbst in Fällen, in denen es keine PIMS-spezifischen Anforderungen oder weitere Informationen gibt.

Abschnitt 6 enthält eine PIMS-spezifische Leitlinie und weitere Informationen zu den Informationssicherheitsmaßnahmen in ISO/IEC 27002 sowie eine PIMS-spezifische Leitlinie für eine Organisation, die entweder als verantwortliche Stelle oder als Auftragsverarbeiter fungiert.

ANMERKUNG 2 Der Vollständigkeit halber enthält Abschnitt 6 einen Unterabschnitt für jeden der Abschnitte, die Zielsetzungen oder Maßnahmen in ISO/IEC 27002:2013 enthalten, selbst in Fällen, in denen es keine PIMS-spezifische Leitlinie oder weitere Informationen gibt.

Abschnitt 7 enthält eine zusätzliche Leitlinie nach ISO/IEC 27002 für verantwortliche Stellen, und Abschnitt 8 enthält eine zusätzliche Leitlinie nach ISO/IEC 27002 für Auftragsverarbeiter.

Anhang A listet die PIMS-spezifischen Maßnahmenziele und Maßnahmen für eine Organisation auf, die als verantwortliche Stelle tätig ist (unabhängig davon, ob sie einen Auftragsverarbeiter beschäftigt oder nicht und ob sie gemeinsam mit einer anderen verantwortliche Stelle handelt oder nicht).

Anhang B listet die PIMS-spezifischen Maßnahmenziele und Maßnahmen für eine Organisation auf, die als Auftragsverarbeiter tätig ist (unabhängig davon, ob sie die Verarbeitung personenbezogener Daten an einen getrennten Auftragsverarbeiter vergibt oder nicht und einschließlich denjenigen, die personenbezogene Daten als Unterauftragnehmer für Auftragsverarbeiter verarbeiten).

Anhang C enthält eine Zuordnung zu ISO/IEC 29100.

Anhang D enthält eine Zuordnung der Maßnahmen in diesem Dokument zur EU-Datenschutz-Grundverordnung.

Anhang E enthält eine Zuordnung zu ISO/IEC 27018 und ISO/IEC 29151.

Anhang F erläutert, wie ISO IEC 27001 und ISO/IEC 27002 auf den Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten ausgedehnt werden.

4.2 Anwendung der Anforderungen von ISO/IEC 27001:2013

Tabelle 1 zeigt die Stellen der PIMS-spezifischen Anforderungen in diesem Dokument in Bezug auf ISO/IEC 27001.

Tabelle 1 — Stellen der PIMS-spezifischen Anforderungen und weitere Informationen zur Umsetzung der Datenschutzmaßnahmen in ISO/IEC 27001:2013

Abschnitt in ISO/IEC 27001:2013	Überschrift	Unterabschnitt in diesem Dokument	Bemerkungen
4	Kontext der Organisation	5.2	zusätzliche Anforderungen
5	Führung	5.3	keine PIMS-spezifischen Anforderungen
6	Planung	5.4	zusätzliche Anforderungen
7	Unterstützung	5.5	keine PIMS-spezifischen Anforderungen
8	Betrieb	5.6	keine PIMS-spezifischen Anforderungen
9	Bewertung der Leistung	5.7	keine PIMS-spezifischen Anforderungen
10	Verbesserung	5.8	keine PIMS-spezifischen Anforderungen

ANMERKUNG Die erweiterte Interpretation von „Informationssicherheit“ nach 5.1 gilt immer, auch wenn keine PIMS-spezifischen Anforderungen bestehen.

4.3 Anwendung der Leitlinien von ISO/IEC 27002:2013

Tabelle 2 gibt die Stellen der PIMS-spezifischen Leitlinien in diesem Dokument in Bezug auf ISO/IEC 27002 an.

Tabelle 2 — Stellen der PIMS-spezifischen Leitlinien und weitere Informationen zur Umsetzung der Datenschutzmaßnahmen in ISO/IEC 27002:2013

Abschnitt in ISO/IEC 27002:2013	Überschrift	Unterabschnitt in diesem Dokument	Bemerkungen
5	Informationssicherheitsrichtlinien	6.2	zusätzliche Leitlinie
6	Organisation der Informationssicherheit	6.3	zusätzliche Leitlinie
7	Personalsicherheit	6.4	zusätzliche Leitlinie
8	Verwaltung der Werte	6.5	zusätzliche Leitlinie
9	Zugangssteuerung	6.6	zusätzliche Leitlinie
10	Kryptographie	6.7	zusätzliche Leitlinie
11	physische und umgebungsbezogene Sicherheit	6.8	zusätzliche Leitlinie
12	Betriebssicherheit	6.9	zusätzliche Leitlinie
13	Kommunikationssicherheit	6.10	zusätzliche Leitlinie
14	Anschaffung, Entwicklung und Instandhaltung von Systemen	6.11	zusätzliche Leitlinie

Abschnitt in ISO/IEC 27002:2013	Überschrift	Unterabschnitt in diesem Dokument	Bemerkungen
15	Lieferantenbeziehungen	6.12	zusätzliche Leitlinie
16	Handhabung von Informationssicherheitsvorfällen	6.13	zusätzliche Leitlinie
17	Informationssicherheitsaspekte beim Business Continuity Management	6.14	keine PIMS-spezifische Leitlinie
18	Einhaltung	6.15	zusätzliche Leitlinie

ANMERKUNG Die erweiterte Interpretation von „Informationssicherheit“ nach 6.1 gilt immer, auch wenn es keine PIMS-spezifische Leitlinie gibt.

4.4 Kunde

Je nach der Rolle der Organisation (siehe 5.2.1) kann der Begriff „Kunde“ wie folgt verstanden werden:

- a) entweder als eine Organisation, die einen Vertrag mit einer verantwortlichen Stelle hat (z. B. der Kunde der verantwortlichen Stelle);

ANMERKUNG 1 Dies kann bei einer Organisation der Fall sein, die eine gemeinsame verantwortliche Stelle ist.

ANMERKUNG 2 Eine natürliche Person, die in einer Business-to-Consumer-Beziehung mit einer Organisation steht, wird in diesem Dokument als „betroffene Person“ bezeichnet.

- b) als eine verantwortliche Stelle, die einen Vertrag mit einem Auftragsverarbeiter hat (z. B. der Kunde des Auftragsverarbeiters); oder
- c) als ein Auftragsverarbeiter, der einen Vertrag mit einem Unterauftragnehmer für die Verarbeitung personenbezogener Daten hat (z. B. der Kunde des unterbeauftragten Auftragsverarbeiters).

ANMERKUNG 3 Wenn in Abschnitt 6 auf „Kunde“ Bezug genommen wird, können die entsprechenden Bestimmungen in den Kontexten a), b) oder c) anwendbar sein.

ANMERKUNG 4 Wenn in Abschnitt 7 und Anhang A auf „Kunde“ Bezug genommen wird, sind die Bestimmungen über die Beziehungen im Kontext a) anwendbar.

ANMERKUNG 5 Wenn in Abschnitt 8 und Anhang B auf „Kunde“ Bezug genommen wird, können die Bestimmungen über die Beziehungen in den Kontexten b) und/oder c) anwendbar sein.

5 PIMS-spezifische Anforderungen in Bezug auf ISO/IEC 27001

5.1 Allgemeines

Die Anforderungen von ISO/IEC 27001:2013, in denen „Informationssicherheit“ erwähnt wird, müssen auf den Schutz der Privatsphäre ausgedehnt werden, die durch die Verarbeitung personenbezogener Daten möglicherweise beeinträchtigt wird.

ANMERKUNG Wenn in der Praxis „Informationssicherheit“ in ISO/IEC 27001:2013 verwendet wird, gilt stattdessen „Informationssicherheit und Datenschutz“ (siehe Anhang F).

5.2 Kontext der Organisation

5.2.1 Verstehen der Organisation und ihres Kontextes

Eine Anforderung zusätzlich zu ISO/IEC 27001:2013, 4.1, lautet:

Die Organisation muss ihre Rolle als verantwortliche Stelle (einschließlich als gemeinsame verantwortliche Stelle) und/oder als Auftragsverarbeiter bestimmen.

Die Organisation muss externe und interne Faktoren bestimmen, die für ihren Kontext relevant sind und sich auf ihre Fähigkeit auswirken, das/die beabsichtigte(n) Ergebnis(se) ihres PIMS zu erreichen. Diese können beispielsweise Folgendes beinhalten:

- geltende Datenschutzgesetze;
- geltende Vorschriften;
- geltende Gerichtsentscheidungen;
- anwendbarer organisatorischer Kontext, Unternehmenssteuerung, Richtlinien und Verfahren;
- geltende Verwaltungsentscheidungen;
- anwendbare vertragliche Anforderungen.

Wenn die Organisation in beiden Rollen tätig ist (z. B. als verantwortliche Stelle und als Auftragsverarbeiter), müssen getrennte Rollen bestimmt werden, die jeweils Gegenstand einer separaten Reihe von Maßnahmen sind.

ANMERKUNG Die Rolle der Organisation kann für jeden Vorgang der Verarbeitung personenbezogener Daten unterschiedlich sein, da sie davon abhängt, wer die Zwecke und Mittel der Verarbeitung bestimmt.

5.2.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien

Eine Anforderung zusätzlich zu ISO/IEC 27001:2013, 4.2, lautet:

Die Organisation muss zu ihren interessierten Parteien (siehe ISO/IEC 27001:2013, 4.2) diejenigen Parteien zählen, die Interessen oder Verantwortlichkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten haben, einschließlich der betroffenen Personen.

ANMERKUNG 1 Andere interessierte Parteien können Kunden (siehe 4.4), Aufsichtsbehörden, andere verantwortliche Stellen, Auftragsverarbeiter und ihre Unterauftragnehmer sein.

ANMERKUNG 2 Anforderungen, die für die Verarbeitung personenbezogener Daten relevant sind, können durch gesetzliche und behördliche Anforderungen, durch vertragliche Verpflichtungen und durch selbst auferlegte organisatorische Ziele bestimmt werden. Die in ISO/IEC 29100 festgelegten Datenschutzgrundsätze bieten eine Leitlinie für die Verarbeitung personenbezogener Daten.

ANMERKUNG 3 Als ein Element zum Nachweis der Einhaltung der Verpflichtungen der Organisation können einige interessierte Parteien erwarten, dass die Organisation im Einklang mit bestimmten Normen steht, wie z. B. dem in diesem Dokument festgelegten Managementsystem und/oder einer entsprechenden Reihe von Spezifikationen. Diese Parteien können eine unabhängig geprüfte Einhaltung dieser Normen fordern.

5.2.3 Festlegung des Anwendungsbereichs des Informationssicherheitsmanagementsystems

Eine Anforderung zusätzlich zu ISO/IEC 27001:2013, 4.3, lautet:

Bei der Festlegung des Anwendungsbereichs des PIMS muss die Organisation die Verarbeitung personenbezogener Daten einbeziehen.

ANMERKUNG Die Festlegung des Anwendungsbereichs des PIMS kann eine Überarbeitung des Anwendungsbereichs des Managementsystems für Informationssicherheit aufgrund der erweiterten Interpretation des Begriffs „Informationssicherheit“ nach 5.1 erfordern.

5.2.4 Managementsystem für Informationssicherheit

Eine Anforderung zusätzlich zu ISO/IEC 27001:2013, 4.4, lautet:

Die Organisation muss ein PIMS in Übereinstimmung mit den Anforderungen der ISO/IEC 27001:2013, Abschnitt 4 bis Abschnitt 10, erweitert um die Anforderungen in Abschnitt 5, einrichten, umsetzen, aufrechterhalten und fortlaufend verbessern.

5.3 Führung

5.3.1 Führung und Verpflichtung

Es gelten die in ISO/IEC 27001:2013, 5.1, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.3.2 Politik

Es gelten die in ISO/IEC 27001:2013, 5.2, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.3.3 Organisatorische Rollen, Verantwortlichkeiten und Befugnisse

Es gelten die in ISO/IEC 27001:2013, 5.3, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.4 Planung

5.4.1 Aktionen zum Umgang mit Risiken und Chancen

5.4.1.1 Allgemeines

Es gelten die in ISO/IEC 27001:2013, 6.1.1, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.4.1.2 Beurteilung von Informationssicherheitsrisiken

Es gelten die in ISO/IEC 27001:2013, 6.1.2, genannten Anforderungen mit den folgenden Präzisierungen:

ISO/IEC 27001:2013, 6.1.2 c) 1), wird wie folgt präzisiert:

Die Organisation muss das Verfahren zur Risikobeurteilung der Informationssicherheit anwenden, um die Risiken im Zusammenhang mit dem Verlust der Vertraulichkeit, Integrität und Verfügbarkeit im Rahmen des PIMS zu ermitteln.

Die Organisation muss ein Verfahren zur Risikobeurteilung des Datenschutzes anwenden, um Risiken im Zusammenhang mit der Verarbeitung von personenbezogenen Daten im Rahmen des PIMS zu ermitteln.

Die Organisation muss während der gesamten Risikobeurteilungsprozesse sicherstellen, dass die Beziehung zwischen Informationssicherheit und Datenschutz angemessen gehandhabt wird.

ANMERKUNG Die Organisation kann entweder einen integrierten Prozess zur Risikobeurteilung der Informationssicherheit und des Datenschutzes oder zwei getrennte Verfahren für die Informationssicherheit und die mit der Verarbeitung personenbezogener Daten verbundenen Risiken anwenden.

ISO/IEC 27001:2013, 6.1.2 d) 1), wird wie folgt präzisiert:

Die Organisation muss die möglichen Folgen sowohl für die Organisation als auch für die betroffenen Personen beurteilen, die sich ergeben würden, wenn die in ISO/IEC 27001:2013, 6.1.2 c), wie oben präzisiert, identifizierten Risiken eintreten würden.

5.4.1.3 Informationssicherheitsrisikobehandlung

Es gelten die in ISO/IEC 27001:2013, 6.1.3, genannten Anforderungen mit den folgenden Ergänzungen:

ISO/IEC 27001:2013, 6.1.3 c), wird wie folgt präzisiert:

Die in ISO/IEC 27001:2013, 6.1.3 b), festgelegten Maßnahmen müssen mit den Maßnahmen in Anhang A und/oder Anhang B und ISO/IEC 27001:2013, Anhang A, verglichen werden, um zu überprüfen, dass keine notwendigen Maßnahmen ausgelassen wurden.

Bei der Beurteilung der Anwendbarkeit der Maßnahmenziele und Maßnahmen aus ISO/IEC 27001:2013 Anhang A, für die Behandlung von Risiken müssen die Maßnahmenziele und Maßnahmen sowohl im Zusammenhang mit Risiken für die Informationssicherheit als auch mit Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich Risiken für betroffene Personen, berücksichtigt werden.

ISO/IEC 27001:2013, 6.1.3 d), wird wie folgt präzisiert:

Erstellung einer Erklärung zur Anwendbarkeit, die Folgendes enthält:

- die notwendigen Maßnahmen [siehe ISO/IEC 27001:2013, 6.1.3 b) und c)];
- Begründung für ihre Aufnahme;
- ob die notwendigen Maßnahmen umgesetzt sind oder nicht; und
- die Begründung für den Ausschluss einer der Maßnahmen in Anhang A und/oder Anhang B und ISO/IEC 27001:2013, Anhang A, entsprechend der Bestimmung der Rolle der Organisation (siehe 5.2.1).

Nicht alle in den Anhängen aufgeführten Maßnahmenziele und Maßnahmen müssen in einer PIMS-Umsetzung enthalten sein. Ein Ausschluss kann u. a. dann begründet sein, wenn die Maßnahmen nach der Risikobeurteilung nicht als notwendig erachtet werden und wenn sie nach den Gesetzen und/oder Vorschriften, einschließlich der auf die betroffene Person anwendbaren Maßnahmen, nicht erforderlich sind (oder Ausnahmen davon unterliegen).

5.4.2 Informationssicherheitsziele und Planung zu deren Erreichung

Es gelten die in ISO/IEC 27001:2013, 6.2, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.5 Unterstützung

5.5.1 Ressourcen

Es gelten die in ISO/IEC 27001:2013, 7.1, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.5.2 Kompetenz

Es gelten die in ISO/IEC 27001:2013, 7.2, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.5.3 Bewusstsein

Es gelten die in ISO/IEC 27001:2013, 7.3, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.5.4 Kommunikation

Es gelten die in ISO/IEC 27001:2013, 7.4, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.5.5 Dokumentierte Information

5.5.5.1 Allgemeines

Es gelten die in ISO/IEC 27001:2013, 7.5.1, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.5.5.2 Erstellen und Aktualisieren

Es gelten die in ISO/IEC 27001:2013, 7.5.2, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.5.5.3 Lenkung dokumentierter Information

Es gelten die in ISO/IEC 27001:2013, 7.5.3, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.6 Betrieb

5.6.1 Betriebliche Planung und Steuerung

Es gelten die in ISO/IEC 27001:2013, 8.1, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.6.2 Beurteilung von Informationssicherheitsrisiken

Es gelten die in ISO/IEC 27001:2013, 8.2, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.6.3 Informationssicherheitsrisikobehandlung

Es gelten die in ISO/IEC 27001:2013, 8.3, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.7 Bewertung der Leistung

5.7.1 Überwachung, Messung, Analyse und Bewertung

Es gelten die in ISO/IEC 27001:2013, 9.1, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.7.2 Internes Audit

Es gelten die in ISO/IEC 27001:2013, 9.2, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.7.3 Managementbewertung

Es gelten die in ISO/IEC 27001:2013, 9.3, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.8 Verbesserung

5.8.1 Nichtkonformität und Korrekturmaßnahmen

Es gelten die in ISO/IEC 27001:2013, 10.1, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

5.8.2 Fortlaufende Verbesserung

Es gelten die in ISO/IEC 27001:2013, 10.2, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

6 PIMS-spezifische Leitlinien in Bezug auf ISO/IEC 27002

6.1 Allgemeines

Die Leitlinien von ISO/IEC 27002:2013, in denen „Informationssicherheit“ erwähnt wird, sollten auf den Schutz der Privatsphäre ausgedehnt werden, die durch die Verarbeitung personenbezogener Daten möglicherweise beeinträchtigt wird.

ANMERKUNG 1 Wenn in der Praxis „Informationssicherheit“ in ISO/IEC 27002:2013 verwendet wird, gilt stattdessen „Informationssicherheit und Datenschutz“ (siehe Anhang F).

Alle Maßnahmenziele und Maßnahmen sollten sowohl im Zusammenhang mit den Risiken für die Informationssicherheit als auch mit den Risiken für den Datenschutz in Bezug auf die Verarbeitung personenbezogener Daten beachtet werden.

ANMERKUNG 2 Sofern nicht anderweitig durch besondere Bestimmungen in Abschnitt 6 festgelegt oder von der Organisation nach den anwendbaren Rechtssystemen bestimmt, gilt dieselbe Leitlinie auch für verantwortliche Stellen und Auftragsverarbeiter.

6.2 Informationssicherheitsrichtlinien

6.2.1 Vorgaben der Leitung für Informationssicherheit

6.2.1.1 Richtlinien für die Informationssicherheit

Es gelten die in ISO/IEC 27002:2013, 5.1.1, und in der folgenden zusätzlichen Leitlinie angegebenen Maßnahmen, Leitlinien zur Umsetzung und weitere Informationen:

Zusätzliche Leitlinie zur Umsetzung für 5.1.1, Richtlinien für die Informationssicherheit, der ISO/IEC 27002:2013:

Die Organisation sollte entweder durch die Erarbeitung separater Datenschutzrichtlinien oder durch die Erweiterung der Informationssicherheitsrichtlinien eine Erklärung über die Unterstützung und Verpflichtung zur Einhaltung der geltenden Datenschutzgesetze und/oder -vorschriften und der zwischen der Organisation und ihren Partnern, ihren Unterauftragnehmern und ihren anwendbaren Dritten (Kunden, Lieferanten usw.) vereinbarten Vertragsbedingungen abgeben, in der die Verantwortlichkeiten zwischen ihnen klar zugeordnet werden sollten.

Zusätzliche weitere Informationen für 5.1.1, Richtlinien für die Informationssicherheit, der ISO/IEC 27002:2013:

Jede Organisation, die personenbezogene Daten verarbeitet, sei es eine verantwortliche Stelle oder ein Auftragsverarbeiter, sollte bei der Erarbeitung und Pflege von Informationssicherheitsrichtlinien die geltenden Datenschutzgesetze und/oder -vorschriften berücksichtigen.

6.2.1.2 Überprüfung der Informationssicherheitsrichtlinien

Es gelten die in ISO/IEC 27002:2013, 5.1.2, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen:

6.3 Organisation der Informationssicherheit

6.3.1 Interne Organisation

6.3.1.1 Informationssicherheitsrollen und -verantwortlichkeiten

Es gelten die in ISO/IEC 27002:2013, 6.1.1, und in der folgenden zusätzlichen Leitlinie angegebenen Maßnahmen, Leitlinien zur Umsetzung und weitere Informationen:

Zusätzliche Leitlinie zur Umsetzung für 6.1.1, Informationssicherheitsrollen und -verantwortlichkeiten, der ISO/IEC 27002:2013:

Die Organisation sollte eine Anlaufstelle benennen, an die sich der Kunde bezüglich der Verarbeitung personenbezogener Daten wenden kann. Wenn es sich bei der Organisation um eine verantwortliche Stelle handelt, wird eine Kontaktstelle für betroffene Personen bezüglich der Bearbeitung ihrer personenbezogene Daten benannt (siehe 7.3.2).

Die Organisation sollte eine oder mehrere Personen ernennen, die für die Entwicklung, Umsetzung, Aufrechterhaltung und Überwachung eines organisationsweiten Steuerungs- und Datenschutzprogramms verantwortlich sind, um die Einhaltung aller geltenden Gesetze und Vorschriften bezüglich der Verarbeitung personenbezogener Daten sicherzustellen.

Die verantwortliche Person sollte gegebenenfalls:

- unabhängig sein und direkt der entsprechenden Managementebene der Organisation Bericht erstatten, um ein effektives Management von Datenschutzrisiken sicherzustellen;
- am Management aller Themen im Zusammenhang mit der Bearbeitung personenbezogener Daten beteiligt sein;
- Experte auf dem Gebiet der Datenschutzgesetze, -vorschriften und -praxis sein;
- als Kontaktstelle für Aufsichtsbehörden fungieren;

- die oberste Führungsebene und die Mitarbeiter der Organisation über ihre Verpflichtungen in Bezug auf die Verarbeitung von personenbezogenen Daten informieren;
- Auskunft in Bezug auf die von der Organisation durchgeführten Datenschutz-Folgenabschätzungen geben.

ANMERKUNG Eine solche Person wird in einigen Rechtssystemen als Datenschutzbeauftragter bezeichnet. Diese legen fest, wann eine solche Position erforderlich ist, sowie ihre Stellung und Rolle. Diese Position kann durch einen Mitarbeiter besetzt oder ausgegliedert werden.

6.3.1.2 Aufgabentrennung

Es gelten die in ISO/IEC 27002:2013, 6.1.2, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen.

6.3.1.3 Kontakt zu Behörden

Es gelten die in ISO/IEC 27002:2013, 6.1.3, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen.

6.3.1.4 Kontakt zu speziellen Interessensgruppen

Es gelten die in ISO/IEC 27002:2013, 6.1.4, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen.

6.3.1.5 Informationssicherheit im Projektmanagement

Es gelten die in ISO/IEC 27002:2013, 6.1.5, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen.

6.3.2 Mobilgeräte und Telearbeit

6.3.2.1 Richtlinie zu Mobilgeräten

Es gelten die in ISO/IEC 27002:2013, 6.2.1, und in der folgenden zusätzlichen Leitlinie angegebenen Maßnahmen, Leitlinien zur Umsetzung und weitere Informationen.

Zusätzliche Leitlinie zur Umsetzung für 6.2.1, Richtlinien zu Mobilgeräten, der ISO/IEC 27002:2013:

Die Organisation sollte sicherstellen, dass die Verwendung von Mobilgeräten nicht zu einer Beeinträchtigung der personenbezogenen Daten führt.

6.3.2.2 Telearbeit

Es gelten die in ISO/IEC 27002:2013, 6.2.2, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen.

6.4 Personalsicherheit

6.4.1 Vor Beginn eines Anstellungsverhältnisses

6.4.1.1 Sicherheitsüberprüfung

Es gelten die in ISO/IEC 27002:2013, 7.1.1, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen.

6.4.1.2 Beschäftigungs- und Vertragsbedingungen

Es gelten die in ISO/IEC 27002:2013, 7.1.2, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen.

6.4.2 Während des Anstellungsverhältnisses

6.4.2.1 Verantwortlichkeiten des Managements

Es gelten die in ISO/IEC 27002:2013, 7.2.1, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen.

6.4.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung

Es gelten die in ISO/IEC 27002:2013, 7.2.2, und in der folgenden zusätzlichen Leitlinie angegebenen Maßnahmen, Leitlinien zur Umsetzung und weitere Informationen.

Zusätzliche Leitlinie zur Umsetzung für 7.2.2, Informationssicherheitsbewusstsein, -ausbildung und -schulung, der ISO/IEC 27002:2013:

Es sollten Maßnahmen ergriffen werden, einschließlich der Sensibilisierung für die Meldung von Vorfällen, um sicherzustellen, dass sich das zuständige Personal über die möglichen Folgen für die Organisation (z. B. rechtliche Folgen, Geschäftsverlust und Schaden für die Marke oder den Ruf), für den Mitarbeiter (z. B. disziplinarische Folgen) und für die betroffene Person (z. B. körperliche, materielle und psychische Folgen) von Verstößen gegen die Regeln und Verfahren zu Datenschutz oder Informationssicherheit, besonders gegen diejenigen zum Umgang mit personenbezogenen Daten, bewusst ist.

ANMERKUNG Solche Maßnahmen können die Anwendung einer geeigneten regelmäßigen Schulung für Personal, das Zugang zu personenbezogenen Daten hat, einschließen.

6.4.2.3 Disziplinarverfahren

Es gelten die in ISO/IEC 27002:2013, 7.2.3, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen.

6.4.3 Beendigung und Änderung des Anstellungsverhältnisses

6.4.3.1 Verantwortlichkeiten bei Beendigung oder Änderung des Anstellungsverhältnisses

Es gelten die in ISO/IEC 27002:2013, 7.3.1, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen.

6.5 Verwaltung der Werte

6.5.1 Verantwortlichkeit für Werte

6.5.1.1 Inventarisierung der Werte

Es gelten die in ISO/IEC 27002:2013, 8.1.1, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen.

6.5.1.2 Zuständigkeit für Werte

Es gelten die in ISO/IEC 27002:2013, 8.1.2, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen.

6.5.1.3 Zulässiger Gebrauch von Werten

Es gelten die in ISO/IEC 27002:2013, 8.1.3, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen.

6.5.1.4 Rückgabe von Werten

Es gelten die in ISO/IEC 27002:2013, 8.1.4, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen.

6.5.2 Informationsklassifizierung

6.5.2.1 Klassifizierung von Informationen

Es gelten die in ISO/IEC 27002:2013, 8.2.1, und in der folgenden zusätzlichen Leitlinie angegebenen Maßnahmen, Leitlinien zur Umsetzung und weitere Informationen.

Zusätzliche Leitlinie zur Umsetzung für 8.2.1, Klassifizierung von Informationen, der ISO/IEC 27002:2013:

Das Informationsklassifizierungssystem der Organisation sollte die personenbezogenen Daten ausdrücklich als Teil des von ihr umgesetzten Programms betrachten. Die Berücksichtigung personenbezogener Daten innerhalb des gesamten Klassifizierungssystems ist wesentlich für das Verständnis, welche personenbezogenen Daten die Organisation verarbeitet (z. B. Art, spezielle Kategorien), wo solche personenbezogene Daten gespeichert sind und durch welche Systeme sie fließen können.

6.5.2.2 Kennzeichnung von Informationen

Es gelten die in ISO/IEC 27002:2013, 8.2.2, und in der folgenden zusätzlichen Leitlinie angegebenen Maßnahmen, Leitlinien zur Umsetzung und weitere Informationen.

Zusätzliche Leitlinie zur Umsetzung für 8.2.2, Kennzeichnung von Informationen, der ISO/IEC 27002:2013:

Die Organisation sollte sicherstellen, dass die unter ihrer Aufsicht stehenden Personen über die Definition von personenbezogenen Daten und darüber informiert werden, wie Informationen, die personenbezogene Daten sind, erkannt werden können.

6.5.2.3 Handhabung von Werten

Es gelten die in ISO/IEC 27002:2013, 8.2.3, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen.

6.5.3 Handhabung von Datenträgern

6.5.3.1 Handhabung von Wechseldatenträgern

Es gelten die in ISO/IEC 27002:2013, 8.3.1, und in der folgenden zusätzlichen Leitlinie angegebenen Maßnahmen, Leitlinien zur Umsetzung und weitere Informationen.

Zusätzliche Leitlinie zur Umsetzung für 8.3.1, Handhabung von Wechseldatenträgern, der ISO/IEC 27002:2013:

Die Organisation sollte jede Verwendung von Wechseldatenträgern und/oder -geräten zur Speicherung von personenbezogenen Daten dokumentieren. Soweit möglich, sollte die Organisation physische Wechseldatenträger und/oder -geräte verwenden, die eine Verschlüsselung bei der Speicherung von

personenbezogenen Daten ermöglichen. Unverschlüsselte Datenträger sollten nur dort verwendet werden, wo es unvermeidlich ist, und in Fällen, in denen unverschlüsselte Datenträger und/oder -geräte verwendet werden, sollte die Organisation Verfahren und Gegenmaßnahmen (z. B. manipulationssichere Verpackung) einführen, um die Risiken für die personenbezogenen Daten zu mindern.

Zusätzliche weitere Informationen für 8.3.1, Handhabung von Wechseldatenträgern, der ISO/IEC 27002:2013:

Wechseldatenträger, die außerhalb der physischen Grenzen der Organisation mitgenommen werden, sind anfällig für Verlust, Beschädigung und unangemessenen Zugang. Die Verschlüsselung von Wechseldatenträgern bietet einen zusätzlichen Schutz für personenbezogene Daten, der die Risiken für die Sicherheit und den Datenschutz verringert, falls die Wechseldatenträger kompromittiert werden sollten.

6.5.3.2 Entsorgung von Datenträgern

Es gelten die in ISO/IEC 27002:2013, 8.3.2, und in der folgenden zusätzlichen Leitlinie angegebenen Maßnahmen, Leitlinien zur Umsetzung und weitere Informationen.

Zusätzliche Leitlinie zur Umsetzung für 8.3.2, Entsorgung von Datenträgern, der ISO/IEC 27002:2013:

Wenn Wechselmedien, auf denen personenbezogene Daten gespeichert sind, entsorgt werden, sollten sichere Entsorgungsverfahren in die dokumentierten Informationen aufgenommen und umgesetzt werden, um sicherzustellen, dass auf zuvor gespeicherte personenbezogene Daten nicht zugegriffen werden kann.

6.5.3.3 Transport von physischen Datenträgern

Es gelten die in ISO/IEC 27002:2013, 8.3.3, und in der folgenden zusätzlichen Leitlinie angegebenen Maßnahmen, Leitlinien zur Umsetzung und weitere Informationen.

Zusätzliche Leitlinie zur Umsetzung für 8.3.3, Transport von Datenträgern, der ISO/IEC 27002:2013:

Wenn für die Übertragung von Informationen physische Datenträger eingesetzt werden, sollte ein System zur Protokollierung des Ein- und Ausgangs von personenbezogenen Daten enthaltenden physischen Datenträgern eingeführt werden, bei dem der Datenträgertyp, die autorisierten Sender/Empfänger, das Datum und die Uhrzeit sowie die Anzahl der physischen Datenträger aufgezeichnet werden. Wenn möglich, sollten zusätzliche Maßnahmen wie z. B. Verschlüsselung umgesetzt werden, um sicherzustellen, dass auf die Daten nur am Bestimmungsort und nicht auf dem Transportweg zugegriffen werden kann.

Die Organisation sollte physische Datenträger mit personenbezogenen Daten vor Verlassen des Geländes einem Genehmigungsverfahren unterziehen und sicherstellen, dass die personenbezogenen Daten für niemanden außer autorisiertem Personal zugänglich sind.

ANMERKUNG Eine mögliche Maßnahme, um sicherzustellen, dass personenbezogene Daten auf physischen Datenträgern, die die Räumlichkeiten der Organisation verlassen, nicht allgemein zugänglich sind, besteht darin, die betreffenden personenbezogenen Daten zu verschlüsseln und die Entschlüsselungsmöglichkeiten auf autorisiertes Personal zu beschränken.

6.6 Zugangssteuerung

6.6.1 Geschäftsanforderungen an die Zugangsteuerung

6.6.1.1 Zugangssteuerungsrichtlinie

Es gelten die in ISO/IEC 27002:2013, 9.1.1, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen.

6.6.1.2 Zugang zu Netzwerken und Netzwerkdiensten

Es gelten die in ISO/IEC 27002:2013, 9.1.2, angegebenen Maßnahmen, Leitlinien zur Umsetzung und sonstigen Informationen.

6.6.2 Benutzerzugangsverwaltung

6.6.2.1 Registrierung und Registrierungsaufhebung von Benutzern

Es gelten die in ISO/IEC 27002:2013, 9.2.1, und in der folgenden zusätzlichen Leitlinie angegebenen Maßnahmen, Leitlinien zur Umsetzung und weitere Informationen.

Zusätzliche Leitlinie zur Umsetzung für 9.2.1, Registrierung und Registrierungsaufhebung von Benutzern, der ISO/IEC 27002:2013:

Die Verfahren für die Registrierung und Registrierungsaufhebung von Benutzern, die personenbezogene Daten verarbeitende Systeme und Dienste verwalten oder betreiben, sollten den Fall einer Kompromittierung der Benutzerzugangskontrolle für diese Benutzer, z. B. durch die Verfälschung oder Kompromittierung von Kennwörtern oder sonstigen Benutzerregistrierungsdaten (z. B. in Folge unbeabsichtigter Offenlegung), einbeziehen.

Die Organisation sollte keine deaktivierten oder erloschenen Benutzer-IDs für personenbezogene Daten verarbeitende Systeme und Dienste an Benutzer wieder ausgeben.

In dem Fall, dass die Organisation die Verarbeitung personenbezogener Daten als Dienstleistung anbietet, kann der Kunde für einige oder alle Aspekte der Benutzer-ID-Verwaltung verantwortlich sein. Solche Fälle sollten in die dokumentierten Informationen aufgenommen werden.

Einige Rechtssysteme stellen bestimmte Anforderungen bezüglich der Häufigkeit von Überprüfungen auf ungenutzte Zugangsdaten im Zusammenhang mit Systemen, die personenbezogene Daten verarbeiten. Organisationen, die in diesen Rechtssystemen tätig sind, sollten die Einhaltung dieser Anforderungen berücksichtigen.

6.6.2.2 Zuteilung von Benutzerzugängen

Es gelten die in ISO/IEC 27002:2013, 9.2.2, und in der folgenden zusätzlichen Leitlinie angegebenen Maßnahmen, Leitlinien zur Umsetzung und weitere Informationen.

Zusätzliche Leitlinie zur Umsetzung für 9.2.2, Zuteilung von Benutzerzugängen, der ISO/IEC 27002:2013:

Die Organisation sollte eine genaue, aktuelle Aufzeichnung der Benutzerprofile führen, die für die zum Zugriff auf das Informationssystem und die darin enthaltenen personenbezogenen Daten berechtigten Benutzer erstellt wurden. Dieses Profil umfasst den Datensatz zum betreffenden Benutzer, einschließlich Benutzer-ID, die für die Umsetzung der identifizierten technischen Maßnahmen zur Gewährung eines berechtigten Zugangs erforderlich sind.

Durch die Umsetzung individueller Benutzerzugangs-IDs können entsprechend konfigurierte Systeme identifizieren, wer auf personenbezogene Daten zugegriffen hat und welche Ergänzungen, Löschungen oder Änderungen sie vorgenommen haben. Neben dem Schutz der Organisation sind auch die Benutzer geschützt, da sie erkennen können, was sie verarbeitet haben und was nicht.

In dem Fall, dass die Organisation die Verarbeitung personenbezogener Daten als Dienstleistung anbietet, kann der Kunde für einige oder alle Aspekte der Zugangsverwaltung verantwortlich sein. Gegebenenfalls sollte die Organisation dem Kunden die Mittel zur Durchführung der Zugangsverwaltung zur Verfügung