DIN EN ISO/IEC 27701

ICS 35.030 Einsprüche bis 2021-02-11

Entwurf

Sicherheitstechniken – Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz – Anforderungen und Richtlinien (ISO/IEC 27701:2019); Deutsche und Englische Fassung prEN ISO/IEC 27701:2020

Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines (ISO/IEC 27701:2019); German and English version prEN ISO/IEC 27701:2020

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 et anglaise prEN ISO/IEC 27701:2020

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-12-11 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

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

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

Gesamtumfang 160 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

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 prEN ISO/IEC 27701:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

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

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

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

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

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

– Entwurf –

2020-12

prEN ISO/IEC 27701:2020

Titel de:	Sicherheitstechniken — Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz — Anforderungen und Richtlinien (ISO/IEC 27701:2019)
Titel en:	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines (ISO/IEC 27701:2019)
Titel fr:	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)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

Inhalt

Seite

Europäisches Vorwort ... 6

Vorwort ... 7

Einleitung ... 8

1 Anwendungsbereich ... 10

2 Normative Verweisungen ... 10

3 Begriffe ... 10

4 Allgemeines ... 11
4.1 Aufbau dieses Dokuments ... 11
4.2 Anwendung der Anforderungen von ISO/IEC 27001:2013 ... 11
4.3 Anwendung der Anleitungen von ISO/IEC 27002:2013 ... 12
4.4 Kunde ... 13

5 PIMS-spezifische Anforderungen in Bezug auf ISO/IEC 27001 ... 13
5.1 Allgemeines ... 13
5.2 Kontext der Organisation ... 14
5.2.1 Verstehen der Organisation und ihres Kontextes ... 14
5.2.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien ... 14
5.2.3 Festlegung des Anwendungsbereichs des Informationssicherheitsmanagementsystems ... 15
5.2.4 Managementsystem für Informationssicherheit ... 15
5.3 Führung ... 15
5.3.1 Führung und Verpflichtung ... 15
5.3.2 Politik ... 15
5.3.3 Organisatorische Rollen, Verantwortlichkeiten und Befugnisse ... 15
5.4 Planung ... 15
5.4.1 Aktionen zum Umgang mit Risiken und Chancen ... 15
5.4.2 Informationssicherheitsziele und Planung zu deren Erreichung ... 16
5.5 Unterstützung ... 17
5.5.1 Ressourcen ... 17
5.5.2 Kompetenz ... 17
5.5.3 Bewusstsein ... 17
5.5.4 Kommunikation ... 17
5.5.5 Dokumentierte Information ... 17
5.6 Betrieb ... 17
5.6.1 Betriebliche Planung und Steuerung ... 17
5.6.2 Beurteilung von Informationssicherheitsrisiken ... 17
5.6.3 Informationssicherheitsrisikobehandlung ... 17
5.7 Leistungsbewertung ... 18
5.7.1 Überwachung, Messung, Analyse und Bewertung ... 18
5.7.2 Internes Audit ... 18
5.7.3 Managementbewertung ... 18
5.8 Verbesserung ... 18
5.8.1 Nichtkonformität und Korrekturmaßnahmen ... 18
5.8.2 Fortlaufende Verbesserung ... 18

6 PIMS-spezifische Anleitungen in Bezug auf ISO/IEC 27002 ... 18
6.1 Allgemeines ... 18

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

6.2 Informationssicherheitsrichtlinien ... 18
6.2.1 Vorgaben der Leitung für Informationssicherheit ... 18
6.3 Organisation der Informationssicherheit ... 19
6.3.1 Interne Organisation ... 19
6.3.2 Mobilgeräte und Telearbeit ... 20
6.4 Personalsicherheit ... 20
6.4.1 Vor Beginn eines Anstellungsverhältnisses ... 20
6.4.2 Während des Anstellungsverhältnisses ... 21
6.4.3 Beendigung und Änderung des Anstellungsverhältnisses ... 21
6.5 Verwaltung der Werte ... 21
6.5.1 Verantwortlichkeit für Werte ... 21
6.5.2 Informationsklassifizierung ... 22
6.5.3 Handhabung von Datenträgern ... 22
6.6 Zugangssteuerung ... 24
6.6.1 Geschäftsanforderungen an die Zugangsteuerung ... 24
6.6.2 Benutzerzugangsverwaltung ... 24
6.6.3 Benutzerverantwortlichkeiten ... 25
6.6.4 Zugangssteuerung für Systeme und Anwendungen ... 25
6.7 Kryptographie ... 26
6.7.1 Kryptographische Maßnahmen ... 26
6.8 Physische und umgebungsbezogene Sicherheit ... 26
6.8.1 Sicherheitsbereiche ... 26
6.8.2 Einrichtung ... 27
6.9 Betriebssicherheit ... 28
6.9.1 Betriebsabläufe und -verantwortlichkeiten ... 28
6.9.2 Schutz vor Schadsoftware ... 29
6.9.3 Datensicherung ... 29
6.9.4 Protokollierung und Überwachung ... 30
6.9.5 Steuerung von Software im Betrieb ... 31
6.9.6 Handhabung technischer Schwachstellen ... 31
6.9.7 Überlegungen für Audits von Informationssystemen ... 31
6.10 Kommunikationssicherheit ... 31
6.10.1 Netzwerksicherheitsmanagement ... 31
6.10.2 Informationsübertragung ... 32
6.11 Anschaffung, Entwicklung und Instandhaltung von Systemen ... 32
6.11.1 Sicherheitsanforderungen an Informationssysteme ... 32
6.11.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen ... 33
6.11.3 Testdaten ... 35
6.12 Lieferantenbeziehungen ... 35
6.12.1 Informationssicherheit in Lieferantenbeziehungen ... 35
6.12.2 Steuerung der Dienstleistungserbringung von Lieferanten ... 36
6.13 Handhabung von Informationssicherheitsvorfällen ... 36
6.13.1 Handhabung von Informationssicherheitsvorfällen und -verbesserungen ... 36
6.14 Informationssicherheitsaspekte beim Business Continuity Management ... 39
6.14.1 Aufrechterhalten der Informationssicherheit ... 39
6.14.2 Redundanzen ... 39
6.15 Einhaltung ... 39
6.15.1 Einhaltung gesetzlicher und vertraglicher Anforderungen ... 39
6.15.2 Überprüfungen der Informationssicherheit ... 40

7 Zusätzliche Anleitung für PII-Beauftragte nach ISO/IEC 27002 ... 41
7.1 Allgemeines ... 41
7.2 Bedingungen für die Erhebung und Verarbeitung ... 41
7.2.1 Identifizieren und Dokumentieren des Zwecks ... 41
7.2.2 Identifizieren der rechtmäßigen Grundlage ... 42
7.2.3 Bestimmen, wann und wie die Einwilligung einzuholen ist ... 43

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

7.2.4 Einholung und Aufzeichnung der Einwilligung 43
7.2.5 Datenschutz-Folgenabschätzung 44
7.2.6 Verträge mit PII-Verarbeitern 44
7.2.7 Gemeinsamer PII-Beauftragter 45
7.2.8 Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten 46
7.3 Verpflichtungen gegenüber betroffenen Personen 46
7.3.1 Bestimmung und Erfüllung von Verpflichtungen gegenüber betroffenen Personen 46
7.3.2 Bestimmen von Informationen für betroffene Personen 47
7.3.3 Bereitstellen von Informationen für betroffene Personen 48
7.3.4 Bereitstellung eines Mechanismus zur Änderung oder zum Widerruf der Einwilligung 48
7.3.5 Bereitstellung eines Mechanismus zur Ablehnung der PII-Verarbeitung 49
7.3.6 Zugriff, Korrektur und/oder Löschung 49
7.3.7 Verpflichtungen von PII-Beauftragten, Dritte zu informieren 50
7.3.8 Bereitstellung einer Kopie der verarbeiteten personenbezogenen Daten 50
7.3.9 Handhabung von Anfragen 51
7.3.10 Automatisierte Entscheidungsfindung 51
7.4 Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen 52
7.4.1 Beschränkte Erhebung 52
7.4.2 Beschränkte Verarbeitung 52
7.4.3 Genauigkeit und Qualität 53
7.4.4 Ziele der Sparsamkeit personenbezogener Daten 53
7.4.5 Entpersonalisierung personenbezogener Daten und Löschung am Ende der Verarbeitung 54
7.4.6 Temporäre Dateien 54
7.4.7 Aufbewahrung 54
7.4.8 Entsorgung 55
7.4.9 Maßnahmen zur Übertragung personenbezogener Daten 55
7.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten 55
7.5.1 Ermittlung der Grundlage für die Übertragung von personenbezogenen Daten zwischen Rechtssystemen 56
7.5.2 Länder und internationale Organisationen, an die personenbezogene Daten übertragen werden können 56
7.5.3 Aufzeichnungen über die Übertragung von personenbezogenen Daten 56
7.5.4 Aufzeichnungen der Offenlegung von personenbezogenen Daten für Dritte 57

8 Zusätzliche Anleitung für PII-Verarbeiter nach ISO/IEC 27002 57
8.1 Allgemeines 57
8.2 Bedingungen für die Erhebung und Verarbeitung 57
8.2.1 Kundenvereinbarung 57
8.2.2 Ziele der Organisation 58
8.2.3 Verwendung für Marketing und Werbung 58
8.2.4 Verstoßende Anweisung 59
8.2.5 Kundenverpflichtungen 59
8.2.6 Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten 59
8.3 Verpflichtungen gegenüber betroffenen Personen 59
8.3.1 Verpflichtungen gegenüber betroffenen Personen 60
8.4 Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen 60
8.4.1 Temporäre Dateien 60
8.4.2 Rückgabe, Übertragung oder Entsorgung von personenbezogenen Daten 61
8.4.3 Maßnahmen zur Übertragung personenbezogener Daten 61
8.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten 62

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

8.5.1 Grundlage für die Übertragung von personenbezogenen Daten zwischen Rechtssystemen ... 62
8.5.2 Länder und internationale Organisationen, an die personenbezogene Daten übertragen werden können ... 62
8.5.3 Aufzeichnungen der Offenlegung von personenbezogenen Daten für Dritte ... 63
8.5.4 Benachrichtigung über Anträge auf Offenlegung von personenbezogenen Daten ... 63
8.5.5 Rechtsverbindliche Offenlegung von personenbezogenen Daten ... 63
8.5.6 Offenlegung von Unterauftragnehmern, die zur Verarbeitung von personenbezogenen Daten eingesetzt werden ... 64
8.5.7 Einschaltung eines Unterauftragnehmers mit der Verarbeitung von personenbezogenen Daten ... 64
8.5.8 Wechsel des Unterauftragnehmers zur Verarbeitung von personenbezogenen Daten ... 65

Anhang A (normativ) PIMS-spezifische Referenzmaßnahmenziele und -Maßnahmen (PII-Beauftragter) ... 66

Anhang B (normativ) PIMS-spezifische Referenzmaßnahmenziele und -Maßnahmen (PII-Verarbeiter) ... 70

Anhang C (informativ) Zuordnung zu ISO/IEC 29100 ... 73

Anhang D (informativ) Zuordnung zur Datenschutz-Grundverordnung ... 76

Anhang E (informativ) Zuordnung zu ISO/IEC 27018 und ISO/IEC 29151 ... 80

Anhang F (informativ) Anwendung von ISO/IEC 27701 auf ISO/IEC 27001 und ISO/IEC 27002 ... 83
F.1 Anwendung dieses Dokuments ... 83
F.2 Beispiel für die Präzisierung von Sicherheitsnormen ... 84

Literaturhinweise ... 85

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

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 prEN ISO/IEC 27701:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 27701:2019 wurde von CEN als prEN ISO/IEC 27701:2020 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

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).

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.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

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 PII zu, ebenso wie die Anzahl der Situationen, in denen eine Organisation mit anderen Organisationen bei der Verarbeitung von PII zusammenarbeiten muss. Der Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung von PII 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 PII-Beauftragten (einschließlich den gemeinsamen PII-Beauftragten) und PII-Verarbeitern (einschließlich denjenigen, die PII-Verarbeiter im Unterauftrag einsetzen und denjenigen, die personenbezogene Daten als Unterauftragnehmer für PII-Verarbeiter 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.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

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

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

1 Anwendungsbereich

Dieses Dokument legt Anforderungen fest und bietet eine Anleitung 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 Anleitung für PII-Beauftragte und PII-Verarbeiter, die für die PII-Verarbeitung 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 PII-Beauftragte und/oder PII-Verarbeiter 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
gemeinsamer PII-Beauftragter
PII-Beauftragter, der gemeinsam mit einem oder mehreren anderen PII-Beauftragten 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

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

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 Anleitung 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 PII-Beauftragter oder als PII-Verarbeiter 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 Anleitung und weitere Informationen zu den Informationssicherheitsmaßnahmen in ISO/IEC 27002 sowie eine PIMS-spezifische Anleitung für eine Organisation, die entweder als PII-Beauftragter oder als PII-Verarbeiter 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 Anleitung oder weitere Informationen gibt.

Abschnitt 7 enthält eine zusätzliche Anleitung nach ISO/IEC 27002 für PII-Beauftragte, und Abschnitt 8 enthält eine zusätzliche Anleitung nach ISO/IEC 27002 für PII-Verarbeiter.

Anhang A listet die PIMS-spezifischen Maßnahmenziele und Maßnahmen für eine Organisation auf, die als PII-Beauftragter tätig ist (unabhängig davon, ob sie einen PII-Verarbeiter beschäftigt oder nicht und ob sie gemeinsam mit einem anderen PII-Beauftragten handelt oder nicht).

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

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

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	Leistungsbewertung	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 Anleitungen von ISO/IEC 27002:2013

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

Tabelle 2 — Stellen der PIMS-spezifischen Anleitungen 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	Informationssicherheits-richtlinien	6.2	zusätzliche Anleitung
6	Organisation der Informationssicherheit	6.3	zusätzliche Anleitung
7	Personalsicherheit	6.4	zusätzliche Anleitung
8	Verwaltung der Werte	6.5	zusätzliche Anleitung
9	Zugangssteuerung	6.6	zusätzliche Anleitung
10	Kryptographie	6.7	zusätzliche Anleitung
11	physische und umgebungsbezogene Sicherheit	6.8	zusätzliche Anleitung
12	Betriebssicherheit	6.9	zusätzliche Anleitung
13	Kommunikationssicherheit	6.10	zusätzliche Anleitung
14	Anschaffung, Entwicklung und Instandhaltung von Systemen	6.11	zusätzliche Anleitung

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

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

ANMERKUNG Die erweiterte Interpretation von „Informationssicherheit“ nach 6.1 gilt immer, auch wenn es keine PIMS-spezifische Anleitung 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 einem PII-Beauftragten hat (z. B. der Kunde des PII-Beauftragten);

ANMERKUNG 1 Dies kann bei einer Organisation der Fall sein, die ein gemeinsamer Datenbeauftragter 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 ein PII-Beauftragter, der einen Vertrag mit einem PII-Verarbeiter hat (z. B. der Kunde des PII-Verarbeiters); oder

c) als ein PII-Verarbeiter, der einen Vertrag mit einem Unterauftragnehmer für die PII-Verarbeitung hat (z. B. der Kunde des unterbeauftragten PII-Subverarbeiters).

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).

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

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 PII-Beauftragter (einschließlich als gemeinsamer PII-Beauftragter) und/oder als PII-Verarbeiter 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 PII-Beauftragter und als PII-Verarbeiter), 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 PII-Beauftragte, PII-Verarbeiter 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 Anleitung 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.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

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, Abschnitte 4 bis 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.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

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.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

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.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

5.7 Leistungsbewertung

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 Anleitungen in Bezug auf ISO/IEC 27002

6.1 Allgemeines

Die Anleitungen 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 Anleitung auch für PII-Beauftragte und PII-Verarbeiter.

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 Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen:

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

Zusätzliche Anleitung 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 ein PII-Beauftragter oder ein PII-Verarbeiter, 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, Anleitungen 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 Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen:

Zusätzliche Anleitung 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 einen PII-Beauftragten 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,

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

— 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, Anleitungen 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, Anleitungen 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, Anleitungen 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, Anleitungen 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 Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen.

Zusätzliche Anleitung 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, Anleitungen 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, Anleitungen zur Umsetzung und sonstigen Informationen.

AVA Documents Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

6.4.1.2 Beschäftigungs- und Vertragsbedingungen

Es gelten die in ISO/IEC 27002:2013, 7.1.2 angegebenen Maßnahmen, Anleitungen 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, Anleitungen 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 Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen.

Zusätzliche Anleitung 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, Anleitungen 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, Anleitungen 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, Anleitungen 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, Anleitungen zur Umsetzung und sonstigen Informationen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

6.5.1.3 Zulässiger Gebrauch von Werten

Es gelten die in ISO/IEC 27002:2013, 8.1.3 angegebenen Maßnahmen, Anleitungen 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, Anleitungen 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 Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen.

Zusätzliche Anleitung 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 PII 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 Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen.

Zusätzliche Anleitung 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, Anleitungen 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 Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen.

Zusätzliche Anleitung 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

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

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 Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen.

Zusätzliche Anleitung 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 Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen.

Zusätzliche Anleitung 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 bei der Übertragung 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.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

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, Anleitungen 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, Anleitungen 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 Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen.

Zusätzliche Anleitung 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 PII 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 PII verarbeitende Systeme und Dienste an Benutzer wieder ausgeben.

In dem Fall, dass die Organisation die PII-Verarbeitung 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 Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen.

Zusätzliche Anleitung 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 PII 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.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

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 PII-Verarbeitung 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 stellen, z. B. durch die Vergabe von Administratorrechten zur Verwaltung oder Beendigung von Zugangsrechten. Solche Fälle sollten in die dokumentierten Informationen aufgenommen werden.

6.6.2.3 Verwaltung privilegierter Zugangsrechte

Es gelten die in ISO/IEC 27002:2013, 9.2.3 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen:

6.6.2.4 Verwaltung geheimer Authentisierungsinformationen von Benutzern

Es gelten die in ISO/IEC 27002:2013, 9.2.4 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.6.2.5 Überprüfung von Benutzerzugangsrechten

Es gelten die in ISO/IEC 27002:2013, 9.2.5 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen:

6.6.2.6 Entzug oder Anpassung von Zugangsrechten

Es gelten die in ISO/IEC 27002:2013, 9.2.6 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.6.3 Benutzerverantwortlichkeiten

6.6.3.1 Gebrauch geheimer Authentisierungsinformationen

Es gelten die in ISO/IEC 27002:2013, 9.3.1 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.6.4 Zugangssteuerung für Systeme und Anwendungen

6.6.4.1 Informationszugangsbeschränkung

Es gelten die in ISO/IEC 27002:2013, 9.4.1 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.6.4.2 Sichere Anmeldeverfahren

Es gelten die in ISO/IEC 27002:2013, 9.4.2 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen.

Zusätzliche Anleitung zur Umsetzung für 9.4.2, Sichere Anmeldeverfahren, der ISO/IEC 27002:2013:

Wenn vom Kunden gefordert, sollte die Organisation die Möglichkeit für sichere Anmeldeverfahren für alle Benutzerkonten unter der Aufsicht des Kunden bereitstellen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

6.6.4.3 System zur Verwaltung von Kennwörtern

Es gelten die in ISO/IEC 27002:2013, 9.4.3 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.6.4.4 Gebrauch von Hilfsprogrammen mit privilegierten Rechten

Es gelten die in ISO/IEC 27002:2013, 9.4.4 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.6.4.5 Zugangssteuerung für Quellcode von Programmen

Es gelten die in ISO/IEC 27002:2013, 9.4.5 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.7 Kryptographie

6.7.1 Kryptographische Maßnahmen

6.7.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen

Es gelten die in ISO/IEC 27002:2013, 10.1.1 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen.

Zusätzliche Anleitung zur Umsetzung für 10.1.1, Richtlinie zum Gebrauch von kryptographischen Maßnahmen, der ISO/IEC 27002:2013:

Einige Rechtssysteme können den Gebrauch von kryptographischen Verfahren zum Schutz bestimmter Arten personenbezogener Daten verlangen, wie z. B. Gesundheitsdaten, Einwohnermeldenummern, Passnummern und Führerscheinnummern.

Die Organisation sollte dem Kunden Informationen zu den Umständen zur Verfügung stellen, unter denen er kryptographische Mittel anwendet, um die von ihm verarbeiteten personenbezogenen Daten zu schützen. Die Organisation sollte dem Kunden außerdem Informationen zu den von ihm bereitgestellten Kapazitäten zur Verfügung stellen, die dem Kunden bei der Anwendung seiner eigenen kryptographischen Schutzmaßnahmen helfen können.

6.7.1.2 Schlüsselverwaltung

Es gelten die in ISO/IEC 27002:2013, 10.1.2 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.8 Physische und umgebungsbezogene Sicherheit

6.8.1 Sicherheitsbereiche

6.8.1.1 Physische Sicherheitsperimeter

Es gelten die in ISO/IEC 27002:2013, 11.1.1 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.8.1.2 Physische Zutrittssteuerung

Es gelten die in ISO/IEC 27002:2013, 11.1.2 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

6.8.1.3 Sichern von Büros, Räumen und Einrichtungen

Es gelten die in ISO/IEC 27002:2013, 11.1.3 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.8.1.4 Schutz vor externen und umweltbedingten Bedrohungen

Es gelten die in ISO/IEC 27002:2013, 11.1.4 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.8.1.5 Arbeiten in Sicherheitsbereichen

Es gelten die in ISO/IEC 27002:2013, 11.1.5 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.8.1.6 Anlieferungs- und Ladebereiche

Es gelten die in ISO/IEC 27002:2013, 11.1.6 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.8.2 Einrichtung

6.8.2.1 Platzierung und Schutz der Einrichtung

Es gelten die in ISO/IEC 27002:2013, 11.2.1 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.8.2.2 Versorgungseinrichtungen

Es gelten die in ISO/IEC 27002:2013, 11.2.2 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.8.2.3 Sicherheit der Verkabelung

Es gelten die in ISO/IEC 27002:2013, 11.2.3 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.8.2.4 Instandhaltung von Geräten und Betriebsmitteln

Es gelten die in ISO/IEC 27002:2013, 11.2.4 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.8.2.5 Entfernen von Werten

Es gelten die in ISO/IEC 27002:2013, 11.2.5 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.8.2.6 Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten

Es gelten die in ISO/IEC 27002:2013, 11.2.6 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.8.2.7 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

Es gelten die in ISO/IEC 27002:2013, 11.2.7 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

Zusätzliche Anleitung zur Umsetzung für 11.2.7, Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln, der ISO/IEC 27002:2013:

Die Organisation sollte sicherstellen, dass bei jeder Neuzuweisung von Speicherplatz alle personenbezogenen Daten, die sich zuvor auf diesem Speicherplatz befanden, nicht zugänglich sind.

Bei Löschung von in einem Informationssystem gespeicherten personenbezogenen Daten können Leistungsprobleme bedeuten, dass eine explizite Löschung dieser Daten praktisch unmöglich ist. Dies bringt das Risiko, dass andere Benutzer auf die personenbezogenen Daten zugreifen können, mit sich. Dieses Risiko sollte durch entsprechende technische Maßnahmen vermieden werden.

Für die sichere Entsorgung oder Wiederverwendung sollten Geräte und Betriebsmittel, die Speichermedien enthalten, die möglicherweise personenbezogene Daten enthalten können, so behandelt werden, als sei dies der Fall.

6.8.2.8 Unbeaufsichtigte Benutzergeräte

Es gelten die in ISO/IEC 27002:2013, 11.2.8 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.8.2.9 Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren

Es gelten die in ISO/IEC 27002:2013, 11.2.9 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen.

Zusätzliche Anleitung zur Umsetzung für 11.2.9, Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren, der ISO/IEC 27002:2013:

Die Organisation sollte die Erstellung von ausgedruckten Materialien einschließlich PII auf das zur Erfüllung des identifizierten Verarbeitungszwecks erforderliche Minimum beschränken.

6.9 Betriebssicherheit

6.9.1 Betriebsabläufe und -verantwortlichkeiten

6.9.1.1 Dokumentieren von Betriebsabläufen

Es gelten die in ISO/IEC 27002:2013, 12.1.1 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.9.1.2 Änderungsmanagement

Es gelten die in ISO/IEC 27002:2013, 12.1.2 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.9.1.3 Kapazitätssteuerung

Es gelten die in ISO/IEC 27002:2013, 12.1.3 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.9.1.4 Trennung von Entwicklungs-, Prüf- und Betriebsumgebungen

Es gelten die in ISO/IEC 27002:2013, 12.1.4 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

6.9.2 Schutz vor Schadsoftware

6.9.2.1 Maßnahmen gegen Schadsoftware

Es gelten die in ISO/IEC 27002:2013, 12.2.1 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.9.3 Datensicherung

6.9.3.1 Sicherung von Informationen

Es gelten die in ISO/IEC 27002:2013, 12.3.1 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen:

Zusätzliche Anleitung zur Umsetzung für 12.3.1, Sicherung von Informationen, der ISO/IEC 27002:2013:

Die Organisation sollte über eine Richtlinie verfügen, die die Anforderungen an die Sicherung, Wiederbeschaffung und Wiederherstellung personenbezogener Daten (die Teil einer allgemeinen Richtlinie für die Sicherung von Informationen sein kann) sowie alle sonstigen Anforderungen (z. B. vertragliche und/oder rechtliche Anforderungen) bezüglich der Löschung von PII anspricht, die in den zu Sicherungsanforderungen gespeicherten Informationen enthalten sind.

Die diesbezüglichen PII-spezifischen Verantwortlichkeiten können vom Kunden abhängen. Die Organisation sollte sicherstellen, dass der Kunde über die Grenzen des Dienstes bezüglich der Datensicherung informiert wurde.

Wenn die Organisation explizit Sicherungs- und Wiederherstellungsdienste für Kunden anbietet, sollte die Organisation ihnen klare Informationen über ihre Fähigkeiten in Bezug auf die Sicherung und Wiederherstellung von personenbezogenen Daten zur Verfügung stellen.

Einige Rechtssysteme stellen bestimmte Anforderungen bezüglich der Häufigkeit von Sicherungen personenbezogener Daten, der Häufigkeit von Überprüfungen und Tests von Datensicherungen oder hinsichtlich der Wiederherstellungsverfahren für personenbezogene Daten. Organisationen, die in diesen Rechtssystemen tätig sind, sollten die Einhaltung dieser Anforderungen nachweisen.

Es kann Gelegenheiten geben, bei denen die personenbezogenen Daten wiederhergestellt werden müssen, vielleicht aufgrund einer Systemstörung, eines Angriffs oder einer Katastrophe. Wenn personenbezogene Daten wiederhergestellt werden (in der Regel von Sicherungsdatenträgern), müssen Prozesse vorhanden sein, die sicherstellen, dass die personenbezogenen Daten in einen Zustand versetzt werden, in dem die Integrität dieser Daten gewährleistet werden kann und/oder in dem deren Ungenauigkeit und/oder Unvollständigkeit festgestellt und Prozesse zu deren Behebung eingerichtet werden (was die betroffene Person einbeziehen kann).

Die Organisation sollte über ein Verfahren und ein Protokoll für die Wiederherstellung personenbezogener Daten verfügen. Das Datenwiederherstellungsprotokoll sollte mindestens folgende Angaben enthalten:

— den Namen der für die Wiederherstellung verantwortlichen Person;

— eine Beschreibung der wiederhergestellten personenbezogenen Daten.

Einige Rechtssysteme schreiben den Inhalt der Datenwiederherstellungsprotokolle vor. Organisationen sollten in der Lage sein, die Einhaltung aller anwendbaren auf das jeweilige Rechtssystem zugeschnittenen Anforderungen an den Inhalt von Wiederherstellungsprotokollen zu dokumentieren. Die Schlussfolgerungen solcher Beratungen sollten in dokumentierte Informationen aufgenommen werden.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

Der Einsatz von Unterauftragnehmern zur Aufbewahrung von replizierten oder Sicherungskopien der verarbeiteten personenbezogenen Daten wird durch die Maßnahmen in diesem Dokument abgedeckt, die für die Verarbeitung von personenbezogenen Daten durch Unterauftragnehmer gelten (siehe 6.5.3.3, 6.12.1.2). Wenn Datenträger im Zusammenhang mit Sicherungen und Wiederherstellungen physisch transportiert werden, wird dies ebenfalls von den Maßnahmen in diesem Dokument abgedeckt (6.10.2.1).

6.9.4 Protokollierung und Überwachung

6.9.4.1 Ereignisprotokollierung

Es gelten die in ISO/IEC 27002:2013, 12.4.1 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen:

Zusätzliche Anleitung zur Umsetzung für 12.4.1, Ereignisprotokollierung, der ISO/IEC 27002:2013:

Es sollte ein Prozess eingeführt werden, um Ereignisprotokolle mittels kontinuierlichen, automatisierten Überwachungs- und Alarmierungsprozessen oder manuell mit festgelegten, dokumentierten Intervallen auf Unregelmäßigkeiten zu überprüfen und entsprechende Abhilfemaßnahmen vorzuschlagen.

Wenn möglich, sollten Ereignisprotokolle den Zugriff auf personenbezogene Daten aufzeichnen, einschließlich Angaben darüber, wer, wann, auf welche personenbezogenen Daten der betroffenen Person zugegriffen hat und welche Änderungen (wenn überhaupt) infolge des Ereignisses vorgenommen wurden (Ergänzungen, Änderungen oder Streichungen).

Falls mehrere Dienstleister an der Bereitstellung von Diensten beteiligt sind, kann für die Umsetzung dieser Anleitung die Ausübung unterschiedlicher oder verteilter Rollen erforderlich sein. Diese Rollen sollten klar definiert und in die dokumentierten Informationen aufgenommen werden, und es sollte eine Vereinbarung über einen Protokollzugang zwischen den Anbietern getroffen werden.

Anleitung zur Umsetzung für PII-Verarbeiter:

Die Organisation sollte Kriterien dafür festlegen, ob, wann und in welcher Weise Protokolldaten dem Kunden zur Verfügung gestellt oder von ihm genutzt werden können. Diese Kriterien sollten dem Kunden zur Verfügung gestellt werden.

Wenn die Organisation ihren Kunden den Zugriff auf von der Organisation kontrollierte Protokollaufzeichnungen ermöglicht, sollte die Organisation angemessene Maßnahmen einführen, um sicherzustellen, dass der Kunde nur auf Aufzeichnungen zugreifen kann, die sich auf die Aktivitäten dieses Kunden beziehen, nicht auf Protokollaufzeichnungen, die sich auf die Aktivitäten anderer Kunden beziehen, und dass er die Protokolle in keiner Weise ändern kann.

6.9.4.2 Schutz der Protokollinformationen

Es gelten die in ISO/IEC 27002:2013, 12.4.2 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen:

Zusätzliche Anleitung zur Umsetzung für 12.4.2, Schutz der Protokollinformationen, der ISO/IEC 27002:2013:

Für die Sicherheitsüberwachung beispielsweise und die Betriebsdiagnostik aufgezeichnete Protokollinformationen können PII enthalten. Es sollten Maßnahmen, wie z. B. eine Zugangskontrolle (siehe ISO/IEC 27002:2013, 9.2.3), eingeführt werden, um sicherzustellen, dass die protokollierten Informationen nur bestimmungsgemäß genutzt werden.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

Es sollte ein vorzugsweise automatisches Verfahren eingeführt werden, um sicherzustellen, dass die protokollierten Informationen entweder gelöscht oder nach dem Aufbewahrungsplan (siehe 7.4.7) de-identifiziert werden.

6.9.4.3 Administratoren- und Bedienerprotokolle

Es gelten die in ISO/IEC 27002:2013, 12.4.3 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.9.4.4 Uhrensynchronisation

Es gelten die in ISO/IEC 27002:2013, 12.4.4 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.9.5 Steuerung von Software im Betrieb

6.9.5.1 Installation von Software auf Systemen im Betrieb

Es gelten die in ISO/IEC 27002:2013, 12.5.1 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.9.6 Handhabung technischer Schwachstellen

6.9.6.1 Handhabung von technischen Schwachstellen

Es gelten die in ISO/IEC 27002:2013, 12.6.1 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.9.6.2 Einschränkung von Softwareinstallation

Es gelten die in ISO/IEC 27002:2013, 12.6.2 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.9.7 Überlegungen für Audits von Informationssystemen

6.9.7.1 Maßnahmen für Audits von Informationssystemen

Es gelten die in ISO/IEC 27002:2013, 12.7.1 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.10 Kommunikationssicherheit

6.10.1 Netzwerksicherheitsmanagement

6.10.1.1 Netzwerksteuerungsmaßnahmen

Es gelten die in ISO/IEC 27002:2013, 13.1.1 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.10.1.2 Sicherheit in Netzwerkdiensten

Es gelten die in ISO/IEC 27002:2013, 13.1.2 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

6.10.1.3 Trennung in Netzwerken

Es gelten die in ISO/IEC 27002:2013, 13.1.3 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.10.2 Informationsübertragung

6.10.2.1 Richtlinien und Verfahren für die Informationsübertragung

Es gelten die in ISO/IEC 27002:2013, 13.2.1 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen:

Zusätzliche Anleitung zur Umsetzung für 13.2.1, Richtlinien und Verfahren für die Informationsübertragung, der ISO/IEC 27002:2013:

Die Organisation sollte Verfahren in Betracht ziehen, um sicherzustellen, dass die Regeln im Zusammenhang mit der Verarbeitung von personenbezogenen Daten im gesamten System und gegebenenfalls außerhalb des Systems durchgesetzt werden.

6.10.2.2 Informationsübertragungsabsprachen

Es gelten die in ISO/IEC 27002:2013, 13.2.2 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.10.2.3 Elektronische Nachrichtenübermittlung

Es gelten die in ISO/IEC 27002:2013, 13.2.3 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.10.2.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

Es gelten die in ISO/IEC 27002:2013, 13.2.4 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen:

Zusätzliche Anleitung zur Umsetzung für 13.2.4, Vertraulichkeits- oder Geheimhaltungsvereinbarungen, der ISO/IEC 27002:2013:

Die Organisation sollte sicherstellen, dass Personen, die unter ihrer Aufsicht arbeiten und Zugang zu personenbezogenen Daten haben, einer Geheimhaltungspflicht unterliegen. Die Vertraulichkeitsvereinbarung, ob Teil eines Vertrags oder separat, sollte die Dauer der einzuhaltenden Verpflichtungen festlegen.

Wenn es sich bei der Organisation um einen PII-Verarbeiter handelt, sollte eine Vertraulichkeitsvereinbarung, in welcher Form auch immer, zwischen der Organisation, ihren Mitarbeitern und ihren Vertretern sicherstellen, dass Mitarbeiter und Vertreter die Richtlinien und Verfahren bezüglich der Datenverarbeitung und des Datenschutzes einhalten.

6.11 Anschaffung, Entwicklung und Instandhaltung von Systemen

6.11.1 Sicherheitsanforderungen an Informationssysteme

6.11.1.1 Analyse und Spezifikation von Informationssicherheitsanforderungen

Es gelten die in ISO/IEC 27002:2013, 14.1.1 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

6.11.1.2 Sicherung von Anwendungsdiensten in öffentlichen Netzwerken

Es gelten die in ISO/IEC 27002:2013, 14.1.2 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen:

Zusätzliche Anleitung zur Umsetzung für 14.1.2, Sicherung von Anwendungsdiensten in öffentlichen Netzwerken, der ISO/IEC 27002:2013:

Die Organisation sollte sicherstellen, dass personenbezogene Daten, die über nicht vertrauenswürdige Datenübertragungsnetzwerke übertragen werden, für die Übertragung verschlüsselt werden.

Nicht vertrauenswürdige Netzwerke können das öffentliche Internet und andere Einrichtungen außerhalb der betrieblichen Kontrolle der Organisation umfassen.

ANMERKUNG In einigen Fällen, z. B. beim Austausch von E-Mails, kann aufgrund der inhärenten Eigenschaften von nicht vertrauenswürdigen Datenübertragungsnetzwerken für eine wirksame Übertragung die Offenlegung bestimmter Kopfzeilen- oder Verkehrsdaten erforderlich sein.

6.11.1.3 Schutz der Transaktionen bei Anwendungsdiensten

Es gelten die in ISO/IEC 27002:2013, 14.1.3 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.11.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen

6.11.2.1 Richtlinie für sichere Entwicklung

Es gelten die in ISO/IEC 27002:2013, 14.2.1 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen:

Zusätzliche Anleitung zur Umsetzung für 14.2.1, Richtlinie für sichere Entwicklung, der ISO/IEC 27002:2013:

Die Richtlinien für die Systementwicklung und -gestaltung sollten eine Anleitung für die Bearbeitung des PII-Bedarfs durch die Organisation enthalten, die auf den Verpflichtungen gegenüber den betroffenen Personen und/oder den geltenden Gesetzen bzw. Vorschriften sowie auf den Arten der von der Organisation durchgeführten Verarbeitung basiert. Abschnitt 7 und Abschnitt 8 enthalten Maßnahmen für die Verarbeitung von personenbezogenen Daten, die bei der Entwicklung von Richtlinien für den Datenschutz bei der Systemgestaltung nützlich sein können.

Richtlinien, die zum Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen beitragen, sollten die folgenden Aspekte berücksichtigen:

a) Anleitung zum Datenschutz und zur Umsetzung der Datenschutzprinzipien (siehe ISO/IEC 29100) im Lebenszyklus der Software-Entwicklung;

b) Anforderungen an den Schutz der Privatsphäre und von personenbezogenen Daten in der Gestaltungsphase, die auf dem Ergebnis einer Risikobewertung für die Privatsphäre und/oder einer Folgenabschätzung der Privatsphäre beruhen können (siehe 7.2.5);

c) PII-Schutz-Kontrollpunkte innerhalb der Projekt-Meilensteine;

d) erforderliche Kenntnisse über den Schutz der Privatsphäre und von personenbezogenen Daten;

e) Minimieren der Verarbeitung von personenbezogenen Daten durch datenschutzfreundliche Voreinstellungen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

6.11.2.2 Verfahren zur Verwaltung von Systemänderungen

Es gelten die in ISO/IEC 27002:2013, 14.2.2 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.11.2.3 Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform

Es gelten die in ISO/IEC 27002:2013, 14.2.3 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.11.2.4 Beschränkungen von Änderungen an Softwarepaketen

Es gelten die in ISO/IEC 27002:2013, 14.2.4 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.11.2.5 Technische Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme

Es gelten die in ISO/IEC 27002:2013, 14.2.5 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen:

Zusätzliche Anleitung zur Umsetzung für 14.2.5, Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme, der ISO/IEC 27002:2013:

Systeme und/oder Komponenten im Zusammenhang mit der Verarbeitung von personenbezogenen Daten sollten nach den Grundsätzen des Schutzes der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen konzipiert sein und die Umsetzung einschlägiger Maßnahmen (wie in Abschnitt 7 und Abschnitt 8 jeweils für PII-Beauftragte und PII-Verarbeiter beschrieben) vorwegnehmen und erleichtern, insbesondere so, dass die Erhebung und Verarbeitung von personenbezogenen Daten in diesen Systemen auf das für die festgelegten Zwecke der Verarbeitung von PII erforderliche Maß beschränkt ist (siehe 7.2).

Beispielsweise sollte eine Organisation, die personenbezogene Daten verarbeitet, sicherstellen, dass sie auf der Grundlage des jeweiligen Rechtssystems nach einem bestimmten Zeitraum diese Daten vernichtet. Das System, das diese personenbezogenen Daten verarbeitet, sollte so gestaltet sein, dass es diese Löschungsanforderung erleichtert.

6.11.2.6 Sichere Entwicklungsumgebung

Es gelten die in ISO/IEC 27002:2013, 14.2.6 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.11.2.7 Ausgegliederte Entwicklung

Es gelten die in ISO/IEC 27002:2013, 14.2.7 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen:

Zusätzliche Anleitung zur Umsetzung für 14.2.7, Ausgegliederte Entwicklung, der ISO/IEC 27002:2013:

Dieselben Prinzipien (siehe 6.11.2.5) des Schutzes der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen sollten gegebenenfalls auch auf ausgegliederte Informationssysteme angewandt werden.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

6.11.2.8 Testen der Systemsicherheit

Es gelten die in ISO/IEC 27002:2013, 14.2.8 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.11.2.9 Systemabnahmetest

Es gelten die in ISO/IEC 27002:2013, 14.2.9 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.11.3 Testdaten

6.11.3.1 Schutz von Testdaten

Es gelten die in ISO/IEC 27002:2013, 14.3.1 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen:

Zusätzliche Anleitung zur Umsetzung für 14.3.1, Schutz von Testdaten, der ISO/IEC 27002:2013:

Personenbezogene Daten sollten nicht für Testzwecke verwendet werden; es sollten falsche oder synthetische Daten verwendet werden. Falls sich die Nutzung von personenbezogenen Daten für Testzwecke nicht vermeiden lässt, sollten technische und organisatorische Maßnahmen, die den in der Produktionsumgebung verwendeten gleichwertig sind, umgesetzt werden, um die Risiken zu minimieren. Falls solche gleichwertigen Maßnahmen nicht durchführbar sind, sollte eine Risikobeurteilung vorgenommen und als Grundlage für die Auswahl geeigneter mildernder Maßnahmen herangezogen werden.

6.12 Lieferantenbeziehungen

6.12.1 Informationssicherheit in Lieferantenbeziehungen

6.12.1.1 Informationssicherheitsrichtlinie für Lieferantenbeziehungen

Es gelten die in ISO/IEC 27002:2013, 15.1.1 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.12.1.2 Behandlung von Sicherheit in Lieferantenvereinbarungen

Es gelten die in ISO/IEC 27002:2013, 15.1.2 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen:

Zusätzliche Anleitung zur Umsetzung für 15.1.2, Behandlung von Sicherheit in Lieferanten-vereinbarungen, der ISO/IEC 27002:2013:

Die Organisation sollte in Vereinbarungen mit Lieferanten festlegen, ob PII verarbeitet werden und welche technischen und organisatorischen Mindestmaßnahmen der Lieferant erfüllen muss, damit die Organisation ihren Verpflichtungen zur Informationssicherheit und zum Schutz der PII nachkommen kann (siehe 7.2.6 und 8.2.1).

In Lieferantenvereinbarungen sollten die Verantwortlichkeiten zwischen der Organisation, ihren Partnern, ihren Lieferanten und ihren jeweiligen Dritten (Kunden, Lieferanten usw.) unter Berücksichtigung der Art der verarbeiteten PII klar zugewiesen werden.

Die Vereinbarungen zwischen der Organisation und ihren Lieferanten sollten einen Mechanismus vorsehen, der sicherstellt, dass die Organisation die Einhaltung aller geltenden Gesetze und/oder Vorschriften

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

unterstützt und verwaltet. Die Vereinbarungen sollten eine unabhängig geprüfte und für den Kunden annehmbare Einhaltung vorsehen.

ANMERKUNG Für solche Auditzwecke kann die Einhaltung einschlägiger und anwendbarer Sicherheits- und Datenschutznormen wie ISO/IEC 27001 oder dieses Dokument in Betracht gezogen werden.

Anleitung zur Umsetzung für PII-Verarbeiter

Die Organisation sollte in Verträgen mit allen Lieferanten festlegen, dass personenbezogene Daten nur auf ihre Anweisung hin verarbeitet werden.

6.12.1.3 Lieferkette für Informations- und Kommunikationstechnologie

Es gelten die in ISO/IEC 27002:2013, 15.1.3 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.12.2 Steuerung der Dienstleistungserbringung von Lieferanten

6.12.2.1 Überwachung und Überprüfung von Lieferantendienstleistungen

Es gelten die in ISO/IEC 27002:2013, 15.2.1 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.12.2.2 Handhabung der Änderungen von Lieferantendienstleistungen

Es gelten die in ISO/IEC 27002:2013, 15.2.2 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.13 Handhabung von Informationssicherheitsvorfällen

6.13.1 Handhabung von Informationssicherheitsvorfällen und -verbesserungen

6.13.1.1 Verantwortlichkeiten und Verfahren

Es gelten die in ISO/IEC 27002:2013, 16.1.1 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen.

Zusätzliche Anleitung zur Umsetzung für 16.1.1, Verantwortlichkeiten und Verfahren, der ISO/IEC 27002:2013:

Als Teil des Gesamtprozesses für das Management von Informationssicherheitsvorfällen sollte die Organisation Verantwortlichkeiten und Verfahren für die Identifizierung und Aufzeichnung von Verstößen der PII festlegen. Darüber hinaus sollte die Organisation Verantwortlichkeiten und Verfahren in Bezug auf die Benachrichtigung der erforderlichen Parteien über die Verstöße gegen personenbezogene Daten (einschließlich des Zeitpunkts solcher Benachrichtigungen) und die Offenlegung gegenüber den Behörden festlegen, wobei die geltenden Gesetze und/oder Vorschriften zu berücksichtigen sind.

Einige Rechtssysteme ordnen besondere Vorschriften für die Reaktion auf Verstöße an, einschließlich der Benachrichtigung. Organisationen, die in diesen Rechtssystemen tätig sind, sollten sicherstellen, dass sie die Einhaltung dieser Vorschriften nachweisen können.

6.13.1.2 Meldung von Informationssicherheitsereignissen

Es gelten die in ISO/IEC 27002:2013, 16.1.2 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

6.13.1.3 Meldung von Schwächen in der Informationssicherheit

Es gelten die in ISO/IEC 27002:2013, 16.1.3 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.13.1.4 Beurteilung von und Entscheidungen über Informationssicherheitsereignisse

Es gelten die in ISO/IEC 27002:2013, 16.1.4 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.13.1.5 Reaktion auf Informationssicherheitsvorfälle

Es gelten die in ISO/IEC 27002:2013, 16.1.5 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen.

Zusätzliche Anleitung zur Umsetzung für 16.1.5, Reaktion auf Informationssicherheitsvorfälle, der ISO/IEC 27002:2013:

Anleitung zur Umsetzung für PII-Beauftragte

Ein Vorfall, der personenbezogene Daten betrifft, sollte eine Überprüfung durch die Organisation als Teil ihrer Prozesse zur Handhabung von Informationssicherheitsvorfällen nach sich ziehen, um festzustellen, ob ein PII-bedingter Verstoß stattgefunden hat, der eine Reaktion erfordert.

Ein Ereignis hat nicht notwendigerweise eine solche Überprüfung zur Folge.

ANMERKUNG 1 Ein Informationssicherheitsereignis führt nicht notwendigerweise zu einem tatsächlichen oder mit hoher Wahrscheinlichkeit nicht autorisierten Zugriff auf personenbezogene Daten oder auf Geräte oder Einrichtungen der Organisation, in denen personenbezogene Daten gespeichert sind. Dazu können unter anderem Pings und andere Broadcast-Angriffe auf Firewalls oder Edge-Server, Port-Scans, erfolglose Anmeldeversuche, Denial-of-Service-Angriffe und Packet-Sniffing gehören.

Wenn es zu einem Verstoß im Umgang mit personenbezogene Daten gekommen ist, sollten die Reaktionsverfahren entsprechende Benachrichtigungen und Aufzeichnungen enthalten.

Einige Rechtssysteme definieren Fälle, wann die Aufsichtsbehörde über den Verstoß benachrichtigt werden sollte, und wann die betroffenen Personen benachrichtigt werden sollten.

Benachrichtigungen sollten klar sein und können erforderlich sein.

ANMERKUNG 2 Die Benachrichtigung kann Details enthalten wie z. B.:

— eine Kontaktstelle, bei der weitere Informationen erhältlich sind;

— eine Beschreibung und die wahrscheinlichen Folgen des Verstoßes;

— eine Beschreibung des Verstoßes einschließlich der Anzahl der betroffenen Personen sowie der Anzahl der betroffenen Aufzeichnungen;

— getroffene oder geplante Maßnahmen.

ANMERKUNG 3 Informationen über das Management von Sicherheitsvorfällen sind in der Reihe ISO/IEC 27035 zu finden.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

Wenn gegen den Umgang mit personenbezogenen Daten verstoßen wurde, sollte eine Aufzeichnung mit ausreichenden Informationen geführt werden, um einen Bericht für regulatorische und/oder forensische Zwecke zur Verfügung zu stellen, wie z. B.:

— eine Beschreibung des Vorfalls;

— den Zeitraum;

— die Folgen für den Vorfall;

— den Namen des Verfassers;

— an wen der Vorfall gemeldet wurde;

— zur Behebung des Problems ergriffene Maßnahmen (einschließlich der verantwortlichen Person und der wiederhergestellten Daten);

— die Tatsache, dass der Vorfall zur Nichtverfügbarkeit, zum Verlust, zur Offenlegung oder zur Änderung von personenbezogenen Daten geführt hat.

Im Falle eines Verstoßes im Umgang mit personenbezogenen Daten sollte dieser Datensatz auch eine Beschreibung der kompromittierten personenbezogenen Daten enthalten, sofern sie bekannt sind; und falls Benachrichtigungen durchgeführt wurden, die unternommenen Schritte, um betroffene Personen, Aufsichtsbehörden oder Kunden zu benachrichtigen.

Anleitung zur Umsetzung für PII-Verarbeiter

Vorgaben zur Benachrichtigung über einen Verstoß gegen personenbezogene Daten sollten Teil des Vertrags zwischen der Organisation und dem Kunden sein. In diesem Vertrag sollte festgelegt sein, in welcher Weise die Organisation die Informationen bereitstellt, die der Kunde benötigt, um seiner Verpflichtung zur Benachrichtigung der zuständigen Behörden nachzukommen. Diese Verpflichtung zur Benachrichtigung erstreckt sich nicht auf einen Verstoß, der vom Kunden oder einem/einer Betroffenen verursacht wurde oder der innerhalb von Systemkomponenten aufgetreten ist, für die diese verantwortlich sind. Der Vertrag sollte auch erwartete und extern vorgegebene Grenzen für die Reaktionszeiten bei der Benachrichtigung festlegen.

In einigen Rechtssystemen sollte der PII-Verarbeiter den PII-Beauftragten über das Vorliegen eines Verstoßes ohne unnötige Verzögerung (d. h. so bald wie möglich) benachrichtigen, vorzugsweise sobald diese entdeckt wird, damit der PII-Beauftragte die geeigneten Maßnahmen ergreifen kann.

Wenn gegen den Umgang mit personenbezogenen Daten verstoßen wurde, sollte eine Aufzeichnung mit ausreichenden Informationen geführt werden, um einen Bericht für regulatorische und/oder forensische Zwecke zur Verfügung zu stellen, wie z. B.:

— eine Beschreibung des Vorfalls;

— den Zeitraum;

— die Folgen für den Vorfall;

— den Namen des Verfassers;

— an wen der Vorfall gemeldet wurde;

— zur Behebung des Problems ergriffene Maßnahmen (einschließlich der verantwortlichen Person und der wiederhergestellten Daten);

— die Tatsache, dass der Vorfall zur Nichtverfügbarkeit, zum Verlust, zur Offenlegung oder zur Änderung von personenbezogenen Daten geführt hat.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

Im Falle eines Verstoßes im Zusammenhang mit personenbezogenen Daten sollte dieser Datensatz auch Folgendes enthalten: eine Beschreibung der kompromittierten personenbezogenen Daten, sofern bekannt, die Angabe, ob jemand benachrichtigt wurde, und die zur Benachrichtigung des Kunden und/oder der Regulierungsbehörden ergriffenen Maßnahmen.

In einigen Rechtssystemen können die geltenden Gesetze und/oder Vorschriften von der Organisation verlangen, die zuständigen Regulierungsbehörden (z. B. Datenschutz-Aufsichtsbehörde) im Falle eines Verstoßes gegen personenbezogene Daten direkt zu benachrichtigen.

6.13.1.6 Erkenntnisse aus Informationssicherheitsvorfällen

Es gelten die in ISO/IEC 27002:2013, 16.1.6 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.13.1.7 Sammeln von Beweismaterial

Es gelten die in ISO/IEC 27002:2013, 16.1.7 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen:

6.14 Informationssicherheitsaspekte beim Business Continuity Management

6.14.1 Aufrechterhalten der Informationssicherheit

6.14.1.1 Planung der Aufrechterhaltung der Informationssicherheit

Es gelten die in ISO/IEC 27002:2013, 17.1.1 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.14.1.2 Umsetzung der Aufrechterhaltung der Informationssicherheit

Es gelten die in ISO/IEC 27002:2013, 17.1.2 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.14.1.3 Überprüfen, Erneuern und Bewerten der Aufrechterhaltung der Informationssicherheit

Es gelten die in ISO/IEC 27002:2013, 17.1.3 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.14.2 Redundanzen

6.14.2.1 Verfügbarkeit von informationsverarbeitenden Einrichtungen

Es gelten die in ISO/IEC 27002:2013, 17.2.1 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.15 Einhaltung

6.15.1 Einhaltung gesetzlicher und vertraglicher Anforderungen

6.15.1.1 Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen

Es gelten die in ISO/IEC 27002:2013, 18.1.1 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

Zusätzliche weitere Informationen für 18.1.1, Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen, der ISO/IEC 27002:2013:

Die Organisation sollte alle möglichen rechtlichen Sanktionen (die sich aus der Nichterfüllung einiger Verpflichtungen ergeben können) im Zusammenhang mit der Verarbeitung von personenbezogenen Daten ermitteln, einschließlich erheblicher Bußgelder direkt von der örtlichen Aufsichtsbehörde. In einigen Rechtssystemen können Internationale Normen wie dieses Dokument als Grundlage für einen Vertrag zwischen der Organisation und dem Kunden verwendet werden, in dem die jeweiligen Verantwortlichkeiten für die Sicherheit, die Privatsphäre und den Schutz der personenbezogenen Daten dargelegt werden. Die Vertragsbedingungen können eine Grundlage für vertragliche Sanktionen im Falle eines Verstoßes gegen diese Pflichten bilden.

6.15.1.2 Geistige Eigentumsrechte

Es gelten die in ISO/IEC 27002:2013, 18.1.2 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.15.1.3 Schutz von Aufzeichnungen

Es gelten die in ISO/IEC 27002:2013, 18.1.3 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen.

Zusätzliche Anleitung zur Umsetzung für 18.1.3, Schutz von Aufzeichnungen, der ISO/IEC 27002:2013:

Es kann eine Überprüfung von aktuellen und historischen Richtlinien und Verfahren erforderlich sein, z. B. im Falle der Behandlung von Kundenbeschwerden und der Untersuchung durch eine Aufsichtsbehörde.

Die Organisation sollte Kopien ihrer Datenschutzrichtlinien und der damit verbundenen Verfahren für einen Zeitraum aufbewahren, der in ihrem Aufbewahrungsplan festgelegt ist (siehe 7.4.7). Dazu gehört auch die Speicherung früherer Versionen dieser Dokumente, wenn sie aktualisiert werden.

6.15.1.4 Privatsphäre und Schutz von personenbezogenen Informationen

Es gelten die in ISO/IEC 27002:2013, 18.1.4 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.15.1.5 Regelungen bezüglich kryptographischer Maßnahmen

Es gelten die in ISO/IEC 27002:2013, 18.1.5 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.15.2 Überprüfungen der Informationssicherheit

6.15.2.1 Unabhängige Überprüfung der Informationssicherheit

Es gelten die in ISO/IEC 27002:2013, 18.2.1 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen:

Zusätzliche Anleitung zur Umsetzung für 18.2.1, Unabhängige Überprüfung der Informationssicherheit, der ISO/IEC 27002:2013:

Wenn eine Organisation als PII-Verarbeiter tätig ist und wenn individuelle Kundenaudits unpraktisch sind oder die Sicherheitsrisiken erhöhen können, sollte die Organisation den Kunden vor Abschluss und für die Dauer eines Vertrags unabhängige Nachweise dafür zur Verfügung stellen, dass die Informationssicherheit in Übereinstimmung mit den Richtlinien und Verfahren der Organisation umgesetzt und betrieben wird. Ein

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

entsprechendes unabhängiges Audit, so wie es von der Organisation ausgewählt wurde, sollte üblicherweise ein annehmbares Verfahren sein, um dem Interesse des Kunden an der Überprüfung der Verarbeitungsvorgänge der Organisation Rechnung zu tragen, wenn es die Bedürfnisse der erwarteten Benutzer abdeckt und wenn die Ergebnisse in ausreichend transparenter Weise zur Verfügung gestellt werden.

6.15.2.2 Einhaltung von Sicherheitsrichtlinien und -standards

Es gelten die in ISO/IEC 27002:2013, 18.2.2 angegebenen Maßnahmen, Anleitungen zur Umsetzung und sonstigen Informationen.

6.15.2.3 Überprüfung der Einhaltung von technischen Vorgaben

Es gelten die in ISO/IEC 27002:2013, 18.2.3 und in der folgenden zusätzlichen Anleitung angegebenen Maßnahmen, Anleitungen zur Umsetzung und weitere Informationen:

Zusätzliche Anleitung zur Umsetzung für 18.2.3, Überprüfung der Einhaltung von technischen Vorgaben, der ISO/IEC 27002:2013:

Als Teil der technischen Überprüfungen der Einhaltung von Sicherheitsrichtlinien und -standards sollte die Organisation Verfahren zur Überprüfung dieser Tools und Komponenten im Zusammenhang mit der Verarbeitung von personenbezogenen Daten einbeziehen. Dies kann Folgendes umfassen:

— laufende Überwachung, um zu überprüfen, dass nur eine zulässige Verarbeitung stattfindet; und/oder

— spezifische Penetrationstests oder Anfälligkeitsprüfungen (z. B. können de-identifizierte Datensätze einem motivierten Eindringungstest unterzogen werden, um zu überprüfen, ob die Entpersonalisierungsverfahren den organisatorischen Anforderungen entsprechen).

7 Zusätzliche Anleitung für PII-Beauftragte nach ISO/IEC 27002

7.1 Allgemeines

Die Anleitung in Abschnitt 6 und die Ergänzungen in diesem Abschnitt bilden die PIMS-spezifische Anleitung für PII-Beauftragte. Die in diesem Abschnitt dokumentierte Anleitung für die Umsetzung bezieht sich auf die in Anhang A aufgeführten Maßnahmen.

7.2 Bedingungen für die Erhebung und Verarbeitung

Zielsetzung: Bestimmen und Dokumentieren, dass die Verarbeitung rechtmäßig ist, mit einer rechtlichen Grundlage nach den geltenden Rechtssystemen und mit klar definierten und legitimen Zwecken.

7.2.1 Identifizieren und Dokumentieren des Zwecks

Maßnahme

Die Organisation sollte die spezifischen Zwecke, für die die personenbezogenen Daten verarbeitet werden, identifizieren und dokumentieren.

Anleitung zur Umsetzung

Die Organisation sollte sicherstellen, dass betroffene Personen den Zweck verstehen, zu dem ihre personenbezogenen Daten verarbeitet werden. Es liegt in der Verantwortung der Organisation, dies klar zu dokumentieren und den betroffenen Personen mitzuteilen. Ohne eine eindeutige Erklärung des Verarbeitungszwecks können Einwilligung und Wahlfreiheit nicht angemessen erteilt werden.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

Die Dokumentation des Zwecks bzw. der Zwecke der Verarbeitung von personenbezogenen Daten sollte hinreichend deutlich und detailliert sein, damit sie in den erforderlichen Informationen, die den betroffenen Personen zur Verfügung gestellt werden müssen, verwendet werden kann (siehe 7.3.2). Dazu gehören Informationen, die zur Einholung der Einwilligung erforderlich sind (siehe 7.2.3), sowie Aufzeichnungen über Richtlinien und Verfahren (siehe 7.2.8).

Weitere Informationen

Bei der Bereitstellung von Cloud-Computing-Diensten können die Taxonomie und die Definitionen in ISO/IEC 19944 hilfreich sein, um Begriffe für die Beschreibung des Zwecks der Verarbeitung von personenbezogenen Daten zu liefern.

7.2.2 Identifizieren der rechtmäßigen Grundlage

Maßnahme

Die Organisation sollte die geeignete rechtmäßige Grundlage für die Verarbeitung von personenbezogenen Daten für die identifizierten Zwecke bestimmen, dokumentieren und einhalten.

Anleitung zur Umsetzung

Einige Rechtssysteme verlangen, dass die Organisation in der Lage sein muss, nachzuweisen, dass die Rechtmäßigkeit der Verarbeitung vor der Verarbeitung ordnungsgemäß festgestellt wurde.

Die rechtliche Grundlage für die Verarbeitung von personenbezogenen Daten kann Folgendes umfassen:

— die Einwilligung betroffener Personen;

— die Erfüllung eines Vertrags;

— die Einhaltung einer gesetzlichen Verpflichtung;

— den Schutz grundlegender Interessen von betroffenen Personen;

— die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt;

— berechtigte Interessen des PII-Beauftragten.

Die Organisation sollte diese Grundlage für jede PII-Verarbeitungsaktivität dokumentieren (siehe 7.2.8).

Zu den rechtmäßigen Interessen der Organisation können z. B. Ziele der Informationssicherheit gehören, die gegen die Verpflichtungen gegenüber betroffenen Personen im Hinblick auf den Datenschutz abgewogen werden sollten.

Wann immer spezielle Kategorien von personenbezogenen Daten definiert werden, entweder durch die Art der personenbezogenen Daten (z. B. Gesundheitsinformationen) oder durch die betroffenen Personen (z. B. personenbezogene Daten, die sich auf Kinder beziehen), sollte die Organisation diese Kategorien von personenbezogenen Daten in ihre Klassifikationsschemata aufnehmen.

Die Klassifikation von PII, die in diese Kategorien fällt, kann sich von einem Rechtssystem zum anderen unterscheiden und zwischen verschiedenen Rechtsvorschriften, die für verschiedene Geschäftsarten gelten, variieren, so dass sich die Organisation der Klassifikation(en) bewusst sein muss, die für die durchgeführte PII-Verarbeitung gelten.

Auch die Verwendung spezieller Kategorien von PII kann strengeren Kontrollen unterliegen.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

Eine Änderung oder Erweiterung der Zwecke für die Verarbeitung von PII kann eine Aktualisierung und/oder Überarbeitung der Rechtsgrundlage erfordern. Sie kann auch die Einholung einer zusätzlichen Einwilligung der betroffenen Person erfordern.

7.2.3 Bestimmen, wann und wie die Einwilligung einzuholen ist

Maßnahme

Die Organisation sollte ein Verfahren festlegen und dokumentieren, mit dem sie nachweisen kann, ob, wann und wie die Einwilligung zur Verarbeitung von personenbezogenen Daten von den betroffenen Personen eingeholt wurde.

Anleitung zur Umsetzung

Die Einwilligung kann für die Verarbeitung von personenbezogenen Daten erforderlich sein, sofern keine anderen rechtmäßigen Gründe vorliegen. Die Organisation sollte klar dokumentieren, wann die Einwilligung eingeholt werden muss und welche Voraussetzungen dafür erfüllt sein müssen. Es kann nützlich sein, den/die Zweck(e) für die Verarbeitung mit Informationen darüber zu korrelieren, ob und wie die Einwilligung eingeholt wird.

Einige Rechtssysteme haben spezifische Anforderungen an die Art und Weise, wie die Einwilligung eingeholt und aufgezeichnet wird (z. B. nicht gebündelt mit anderen Vereinbarungen). Darüber hinaus können bestimmte Arten der Datenerfassung (z. B. für wissenschaftliche Forschung) und bestimmte Arten von betroffenen Personen, wie z. B. Kinder, zusätzlichen Anforderungen unterworfen werden. Die Organisation sollte solche Anforderungen berücksichtigen und dokumentieren, wie Mechanismen für die Einwilligung diese Anforderungen erfüllen.

7.2.4 Einholung und Aufzeichnung der Einwilligung

Maßnahme

Die Organisation sollte die Einwilligung der betroffenen Personen nach den dokumentierten Prozessen einholen und aufzeichnen.

Anleitung zur Umsetzung

Die Organisation sollte die Einwilligung von betroffenen Personen einholen und aufzeichnen, so dass sie auf Anfrage Einzelheiten der erteilten Einwilligung mitteilen kann (z. B. den Zeitpunkt, zu dem die Einwilligung erteilt wurde, die Identifizierung der betroffenen Person und die Einwilligungserklärung).

Die Informationen, die der betroffenen Person vor dem Einwilligungsverfahren zur Verfügung gestellt werden, sollten der Anleitung in 7.3.3 folgen.

Die Einwilligung sollte

— freiwillig erteilt,

— spezifisch in Bezug auf den Zweck der Verarbeitung, und

— eindeutig und explizit sein.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2021-01

7.2.5 Datenschutz-Folgenabschätzung

Maßnahme

Die Organisation sollte immer dann, wenn eine neue Verarbeitung von personenbezogenen Daten oder Änderungen an der bestehenden Verarbeitung von personenbezogenen Daten geplant ist, die Notwendigkeit einer Datenschutz-Folgenabschätzung prüfen und gegebenenfalls umsetzen.

Anleitung zur Umsetzung

Die Verarbeitung von personenbezogenen Daten erzeugt Risiken für betroffene Personen. Diese Risiken sollten durch eine Datenschutz-Folgenabschätzung beurteilt werden. Einige Rechtssysteme definieren Fälle, für die eine Datenschutz-Folgenabschätzung vorgeschrieben ist. Zu den Kriterien können die automatisierte Entscheidungsfindung, die rechtliche Auswirkungen auf betroffene Personen hat, eine groß angelegte Verarbeitung von personenbezogenen Daten (z. B. gesundheitsbezogene Informationen, ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten oder biometrische Daten) oder die systematische Überwachung eines öffentlich zugänglichen Bereichs in großem Maßstab gehören.

Die Organisation sollte die Elemente bestimmen, die für den Abschluss einer Datenschutz-Folgenabschätzung notwendig sind. Dazu kann eine Liste der verarbeiteten Arten von personenbezogenen Daten gehören, wo die personenbezogenen Daten gespeichert sind und wohin sie übertragen werden können. Datenflussdiagramme und Datenkarten können in diesem Zusammenhang ebenfalls hilfreich sein (siehe 7.2.8 für Einzelheiten zu Aufzeichnungen über die Verarbeitung von personenbezogenen Daten, die über Auswirkungen auf den Datenschutz oder andere Risikobewertungen informieren können).

Weitere Informationen

Anleitungen zu Datenschutz-Folgenabschätzungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten können ISO/IEC 29134 entnommen werden.

7.2.6 Verträge mit PII-Verarbeitern

Maßnahme

Die Organisation sollte einen schriftlichen Vertrag mit jedem von ihr eingesetzten PII-Verarbeiter haben und sicherstellen, dass ihre Verträge mit PII-Verarbeitern die Umsetzung der entsprechenden Maßnahmen in Anhang B vorsehen.

Anleitung zur Umsetzung

Der Vertrag zwischen der Organisation und jedem PII-Verarbeiter, der in ihrem Namen personenbezogene Daten verarbeitet, sollte den PII-Verarbeiter verpflichten, die entsprechenden Maßnahmen nach Anhang B umzusetzen, wobei der Prozess der Risikobewertung der Informationssicherheit (siehe 5.4.1.2) und der Umfang der Verarbeitung von personenbezogenen Daten durch den PII-Verarbeiter (siehe 6.12) zu berücksichtigen sind. Standardmäßig sollten alle in Anhang B aufgeführten Maßnahmen als relevant angenommen werden. Wenn die Organisation beschließt, vom PII-Verarbeiter nicht zu verlangen, eine Maßnahme aus Anhang B umzusetzen, sollte sie ihren Ausschluss begründen (siehe 5.4.1.3).

Ein Vertrag kann die Verantwortlichkeiten jeder Partei unterschiedlich definieren, aber um mit diesem Dokument im Einklang zu sein, sollten alle Maßnahmen berücksichtigt und in die dokumentierten Informationen aufgenommen werden.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

7.2.7 Gemeinsamer PII-Beauftragter

Maßnahme

Die Organisation sollte die jeweiligen Rollen und Verantwortlichkeiten für die Verarbeitung von personenbezogenen Daten (einschließlich Datenschutz und Sicherheitsanforderungen) mit jedem gemeinsamen PII-Beauftragten festlegen.

Anleitung zur Umsetzung

Die Rollen und Verantwortlichkeiten für die Verarbeitung von personenbezogenen Daten sollten auf transparente Weise festgelegt werden.

Diese Rollen und Verantwortlichkeiten sollten in einem Vertrag oder einem ähnlichen verbindlichen Dokument dokumentiert werden, das die Bedingungen für die gemeinsame Verarbeitung von personenbezogenen Daten enthält. In einigen Rechtssystemen wird eine solche Vereinbarung als Vereinbarung über die gemeinsame Nutzung von Daten bezeichnet.

Eine Vereinbarung für einen gemeinsamen PII-Beauftragten kann Folgendes enthalten (diese Liste ist weder endgültig noch erschöpfend):

— Zweck der gemeinsamen Nutzung von personenbezogenen Daten/Beziehung des gemeinsamen PII-Beauftragten;

— Identität der Organisationen (PII-Beauftragte), die Teil der Beziehung des gemeinsamen PII-Beauftragten sind;

— Kategorien von personenbezogenen Daten, die im Rahmen der Vereinbarung geteilt und/oder übertragen und verarbeitet werden sollen;

— Überblick über die Verarbeitungsvorgänge (z. B. Weitergabe, Verwendung);

— Beschreibung der jeweiligen Rollen und Verantwortlichkeiten;

— Verantwortung für die Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen zum Datenschutz;

— Definition der Verantwortung im Falle eines Verstoßes gegen personenbezogene Daten (z. B. wer benachrichtigt, wann, gegenseitige Information);

— Bedingungen für die Aufbewahrung und/oder Entsorgung von personenbezogenen Daten;

— Haftung für die Nichteinhaltung der Vereinbarung;

— wie Verpflichtungen gegenüber betroffenen Personen erfüllt werden;

— wie betroffenen Personen Informationen über das Wesen der Vereinbarung zwischen den gemeinsamen PII-Beauftragten bereitgestellt werden;

— wie betroffene Personen andere Informationen erhalten können, zu deren Erhalt sie berechtigt sind; und

— eine Kontaktstelle für betroffene Personen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01

7.2.8 Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten

Maßnahme

Die Organisation sollte die notwendigen Aufzeichnungen zur Unterstützung ihrer Verpflichtungen für die Verarbeitung von personenbezogenen Daten festlegen und sicher aufbewahren.

Anleitung zur Umsetzung

Eine Möglichkeit, Aufzeichnungen über die Verarbeitung von personenbezogenen Daten zu führen, besteht darin, über ein Inventar oder eine Liste der PII-Verarbeitungsaktivitäten, die die Organisation durchführt, zu verfügen. Solch ein Inventar kann Folgendes umfassen:

— die Art der Verarbeitung;

— den Zweck für die Verarbeitung;

— eine Beschreibung der Kategorien von personenbezogenen Daten und betroffenen Personen (z. B. Kinder);

— die Kategorien von Empfängern, denen personenbezogene Daten offengelegt wurden oder werden, einschließlich der Empfänger in Drittländern oder internationalen Organisationen;

— eine allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen; und

— einen Bericht zur Datenschutz-Folgenabschätzung.

Ein solches Inventar sollte einen Eigentümer haben, der für dessen Genauigkeit und Vollständigkeit verantwortlich ist.

7.3 Verpflichtungen gegenüber betroffenen Personen

Zielsetzung: Sicherstellen, dass betroffene Personen angemessene Informationen über die Verarbeitung ihrer personenbezogenen Daten erhalten, und Erfüllen aller anderen anwendbaren Verpflichtungen gegenüber betroffenen Personen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten.

7.3.1 Bestimmung und Erfüllung von Verpflichtungen gegenüber betroffenen Personen

Maßnahme

Die Organisation sollte ihre rechtlichen, behördlichen und geschäftlichen Verpflichtungen gegenüber den betroffenen Personen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten festlegen und dokumentieren und die Mittel zur Erfüllung dieser Verpflichtungen bereitstellen.

Anleitung zur Umsetzung

Die Verpflichtungen gegenüber betroffenen Personen und die Mittel zu ihrer Unterstützung sind von Rechtssystem zu Rechtssystem unterschiedlich.

Die Organisation sollte sicherstellen, dass sie die geeigneten Mittel zur Verfügung stellt, um den Verpflichtungen gegenüber den betroffenen Personen auf zugängliche Weise und rechtzeitig nachzukommen. Der betroffenen Person sollte eine klare Dokumentation zur Verfügung gestellt werden, aus

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2021-01