DIN EN ISO/IEC 27701

DIN

ICS 35.030

Entwurf

Einsprüche bis 2024-10-23
Vorgesehen als Ersatz für
DIN EN ISO/IEC 27701:2021-07

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Datenschutz-Informationsmanagementsysteme – Anforderungen und Leitlinien (ISO/IEC DIS 27701:2024); Deutsche und Englische Fassung prEN ISO/IEC 27701:2024

Information security, cybersecurity and privacy protection –
Privacy information management systems –
Requirements and guidance (ISO/IEC DIS 27701:2024);
German and English version prEN ISO/IEC 27701:2024

Sécurité de l'information, cybersécurité et protection de la vie privée –
Systèmes de management de la protection de la vie privée –
Exigences et recommandations (ISO/IEC DIS 27701:2024);
Version allemande et anglaise prEN ISO/IEC 27701:2024

Anwendungswarnvermerk

Dieser Entwurf mit Erscheinungsdatum 2024-08-23 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil das beabsichtigte Dokument 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 Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

Es wird gebeten, mit den Kommentaren zu diesem Entwurf jegliche relevanten Patentrechte, die bekannt sind, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 176 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Nationales Vorwort

Der Text von ISO/IEC DIS 27701:2024 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 27701.2:2024 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ 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 27001	siehe	DIN EN ISO/IEC 27001
ISO/IEC 27002	siehe	DIN EN ISO/IEC 27002
ISO/IEC 27018	siehe	DIN EN ISO/IEC 27018
ISO/IEC 29100	siehe	DIN EN ISO/IEC 29100
ISO/IEC 29101	siehe	DIN EN ISO/IEC 29101
ISO/IEC 29134	siehe	DIN EN ISO/IEC 29134
ISO/IEC 29151	siehe	DIN EN ISO/IEC 29151
ISO/IEC 29184	siehe	DIN EN ISO/IEC 29184
ISO 31000	siehe	DIN ISO 31000

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

Änderungen

Gegenüber DIN EN ISO/IEC 27701:2021-07 wurden folgende Änderungen vorgenommen:

a) diese zweite Ausgabe annulliert und ersetzt die erste Ausgabe (ISO/IEC 27701:2019), die als eigenständiges Managementsystem neu formuliert wurde;

b) Dokument redaktionell überarbeitet.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO/IEC 27001, *Informationssicherheit, Cybersicherheit und Datenschutz — Informationssicherheitsmanagementsysteme — Anforderungen*

DIN EN ISO/IEC 27002, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Informationssicherheitsmaßnahmen*

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

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

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

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

DIN EN ISO/IEC 29151, *Informationstechnik — Sicherheitsverfahren — Leitfaden für den Schutz personenbezogener Daten*

DIN EN ISO/IEC 29184, *Informationstechnologie — Online-Datenschutzerklärung und Einwilligung*

DIN ISO 31000, *Risikomanagement — Leitlinien*

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

– Leerseite –

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

– Entwurf –

Juli 2024

prEN ISO/IEC 27701

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Datenschutz-Informationsmanagementsysteme – Anforderungen und Leitlinien (ISO/IEC DIS 27701:2024)

Information security, cybersecurity and privacy protection – Privacy information management systems – Requirements and guidance (ISO/IEC DIS 27701:2024)

Sécurité de l'information, cybersécurité et protection de la vie privée – Systèmes de management de la protection de la vie privée – Exigences et recommandations (ISO/IEC DIS 27701:2024)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Inhalt

Seite

Europäisches Vorwort 5
Vorwort 6
Einleitung 7
1 Anwendungsbereich 8
2 Normative Verweisungen 8
3 Begriffe und Abkürzungen 8
4 Kontext der Organisation 12
4.1 Verstehen der Organisation und ihres Kontextes 12
4.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien 12
4.3 Festlegung des Anwendungsbereichs des Managementsystems für Datenschutzinformationen 13
4.4 Managementsystem für Datenschutzinformationen 14
5 Führung 14
5.1 Führung und Verpflichtung 14
5.2 Datenschutzrichtlinie 14
5.3 Rollen, Verantwortlichkeiten und Befugnisse 15
6 Planung 15
6.1 Aktionen zum Umgang mit Risiken und Chancen 15
6.1.1 Allgemeines 15
6.1.2 Datenschutz-Folgenabschätzung 15
6.1.3 Datenschutz-Risikobehandlung 16
6.2 Datenschutzziele und Planung zu deren Erreichung 17
6.3 Planung von Änderungen 18
7 Unterstützung 18
7.1 Ressourcen 18
7.2 Kompetenz 18
7.3 Bewusstsein 18
7.4 Kommunikation 19
7.5 Dokumentierte Information 19
7.5.1 Allgemeines 19
7.5.2 Erstellen und Aktualisieren dokumentierter Informationen 19
7.5.3 Lenkung dokumentierter Information 19
8 Betrieb 20
8.1 Betriebliche Planung und Steuerung 20
8.2 Datenschutz-Risikobeurteilung 20
8.3 Datenschutz-Risikobehandlung 20
9 Bewertung der Leistung 20
9.1 Überwachung, Messung, Analyse und Bewertung 20
9.2 Internes Audit 21
9.2.1 Allgemeines 21
9.2.2 Internes Auditprogramm 21
9.3 Managementbewertung 21
9.3.1 Allgemeines 21
9.3.2 Eingaben für die Managementbewertung 22
9.3.3 Ergebnisse der Managementbewertung 22
10 Verbesserung 22
10.1 Fortlaufende Verbesserung 22
10.2 Nichtkonformität und Korrekturmaßnahmen 22
11 Weitere Informationen zu Anhängen 23
Anhang A (normativ) PIMS-Referenzmaßnahmenziele und -Maßnahmen für verantwortliche Stellen und Auftragsverarbeiter 24

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Anhang B (normativ) **Leitlinie zur Umsetzung für verantwortliche Stellen und Auftragsverarbeiter** 36
B.1 Leitlinie zur Umsetzung für verantwortliche Stellen 36
B.1.1 Allgemeines 36
B.1.2 Bedingungen für die Erhebung und Verarbeitung 36
B.1.3 Verpflichtungen gegenüber betroffenen Personen 40
B.1.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen . . 46
B.1.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten 49
B.2 Leitlinie zur Umsetzung für Auftragsverarbeiter 51
B.2.1 Allgemeines 51
B.2.2 Bedingungen für die Erhebung und Verarbeitung 51
B.2.3 Verpflichtungen gegenüber betroffenen Personen 53
B.2.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen . . 54
B.2.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten 55
B.3 Leitlinie zur Umsetzung für verantwortliche Stellen und Auftragsverarbeiter 58
B.3.1 Zielsetzung 58
B.3.2 Allgemeines 58
B.3.3 Richtlinien für die Informationssicherheit 59
B.3.4 Informationssicherheitsrollen und -verantwortlichkeiten 59
B.3.5 Klassifizierung von Informationen 60
B.3.6 Kennzeichnung von Informationen 60
B.3.7 Informationsübertragung 60
B.3.8 Identitätsmanagement 60
B.3.9 Zugangsrechte 61
B.3.10 Behandlung von Informationssicherheit in Lieferantenvereinbarungen 61
B.3.11 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen 62
B.3.12 Reaktion auf Informationssicherheitsvorfälle 62
B.3.13 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen 64
B.3.14 Schutz von Aufzeichnungen 65
B.3.15 Unabhängige Überprüfung der Informationssicherheit 65
B.3.16 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit . . 65
B.3.17 Informationssicherheitsbewusstsein, -ausbildung und -schulung 66
B.3.18 Vertraulichkeits- oder Geheimhaltungsvereinbarungen 66
B.3.19 Aufgeräumte Arbeitsumgebung und Bildschirmsperren 66
B.3.20 Speichermedien 66
B.3.21 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln 67
B.3.22 Endpunktgeräte des Benutzers 68
B.3.23 Sichere Authentifizierung 68
B.3.24 Sicherung von Informationen 68
B.3.25 Protokollierung 69
B.3.26 Verwendung von Kryptographie 70
B.3.27 Lebenszyklus einer sicheren Entwicklung 70
B.3.28 Anforderungen an die Anwendungssicherheit 71
B.3.29 Sichere Systemarchitektur und technische Grundsätze 71
B.3.30 Ausgegliederte Entwicklung 71
B.3.31 Prüfinformationen 72
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) **Übereinstimmung mit ISO/IEC 27701:2019** 83
Literaturhinweise 91

Tabellen

Tabelle A.1 — Maßnahmenziele und Maßnahmen für verantwortliche Stellen 24

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Tabelle A.2 — Maßnahmenziele und Maßnahmen für Auftragsverarbeiter 27
Tabelle A.3 — Maßnahmenziele und Maßnahmen für verantwortliche Stellen und Auftragsverarbeiter 30
Tabelle C.1 — Zuordnung von Maßnahmen für verantwortliche Stellen und ISO/IEC 29100 73
Tabelle C.2 — Zuordnung von Maßnahmen für Auftragsverarbeiter und ISO/IEC 29100 75
Tabelle D.1 — Zuordnung der Struktur von ISO/IEC 27701 auf die Artikel der DSGVO 76
Tabelle E.1 — Zuordnung der ISO/IEC 27701 auf ISO/IEC 27018 und ISO/IEC 29151 80
Tabelle F.1 —Übereinstimmung zwischen Maßnahmen in diesem Dokument und Maßnahmen in ISO/IEC 27701:2019 83
Tabelle F.2 —Übereinstimmung zwischen Maßnahmen in ISO/IEC 27701:2019 und Maßnahmen in diesem Dokument 87

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Europäisches Vorwort

Der Text von ISO/IEC DIS 27701.2:2024 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 27701.2:2024 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 DIS 27701.2:2024 wurde von CEN als prEN ISO/IEC 27701:2024 ohne irgendeine Abänderung genehmigt.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

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-Directives, 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-Directives, Teil 2 erarbeitet (siehe www.iso.org/directives oder www.iec.ch/members_experts/refdocs).

ISO und IEC weisen auf die Möglichkeit hin, dass die Anwendung dieses Dokuments mit der Verwendung eines oder mehrerer Patente verbunden sein kann. ISO und IEC beziehen jedoch in dieser Hinsicht keinerlei Stellung bezüglich Nachweis, Gültigkeit oder Anwendbarkeit jeglicher beanspruchten Patentrechte. Zum Zeitpunkt der Veröffentlichung dieses Dokuments lag ISO und IEC keine Mitteilung über ein Patent bzw. mehrere Patente vor, welche/s zur Umsetzung dieses Dokuments erforderlich sein könnte/n. Anwender werden jedoch darauf hingewiesen, dass dies möglicherweise nicht der aktuelle Informationsstand ist. Dieser kann jedoch der Patentdatenbank unter www.iso.org/patents und https://patents.iec.ch entnommen werden. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

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. In der IEC, siehe www.iec.ch/understanding-standards.

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

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO/IEC 27701:2019), die zu einem eigenständigen Managementsystem umgestaltet wurde.

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

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Einleitung

0.1 Allgemeines

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

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.

ANMERKUNG Diese können interpretiert werden, um die lokalen Gesetze oder Vorschriften zu berücksichtigen.

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

Durch Erfüllung der Anforderungen in diesem Dokument kann eine Organisation einen 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 kann eine unabhängige Verifizierung dieses Nachweises liefern.

Dieses Dokument wurde ursprünglich als ISO/IEC 27552 entwickelt.

0.2 Kompatibilität mit anderen Managementsystemnormen

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

Dieses Dokument ermöglicht es einer Organisation, ihr Managementsystem für Informationen zum Datenschutz an die Anforderungen anderer Managementsystemnormen anzugleichen oder es entsprechend zu integrieren, insbesondere an das in ISO/IEC 27001 festgelegte Informationssicherheitsmanagementsystem.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

1 Anwendungsbereich

Dieses Dokument legt Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Managementsystems für Datenschutzinformationen (PIMS) fest.

Es wird eine Anleitung bereitgestellt, um die Umsetzung der Anforderungen in diesem Dokument zu unterstützen.

Dieses Dokument ist für verantwortliche Stellen und Auftragsverarbeiter gedacht, die für die Verarbeitung von personenbezogenen Daten verantwortlich und rechenschaftspflichtig sind.

Dieses Dokument ist für alle Arten und Größen von Organisationen, einschließlich öffentlicher und privater Unternehmen, öffentlicher Stellen und gemeinnütziger Organisationen anwendbar.

2 Normative Verweisungen

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

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

3 Begriffe und Abkürzungen

Für die Anwendung dieses Dokuments gelten die Begriffe nach 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 https://www.electropedia.org/

3.1
Organisation
Person oder Personengruppe, die eigene Funktionen mit Verantwortlichkeiten, Befugnissen und Beziehungen hat, um ihre *Ziele* (3.6) zu erreichen

Anmerkung 1 zum Begriff: Der Begriff Organisation umfasst unter anderem Einzelunternehmer, Gesellschaft, Konzern, Firma, Unternehmen, Behörde, Handelsgesellschaft, Wohltätigkeitsorganisation, Institution, oder Teile oder eine Kombination der genannten, ob eingetragen oder nicht, öffentlich oder privat.

Anmerkung 2 zum Begriff: Wenn die Organisation Teil einer größeren Instanz ist, bezieht sich der Ausdruck „Organisation“ nur auf den Teil der größeren Instanz, der in den Anwendungsbereich des *Managementsystems* (3.4) für Datenschutzinformationen fällt.

3.2
interessierte Partei (Vorzugsbenennung)
Stakeholder (zugelassene Benennung)
Person oder *Organisation* (3.1), die eine Entscheidung oder Tätigkeit beeinflussen kann, die davon beeinflusst sein kann oder die sich davon beeinflusst fühlen kann

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

3.3
oberste Leitung
Person oder Personengruppe, die eine *Organisation* (3.1) auf der obersten Ebene führt und steuert

Anmerkung 1 zum Begriff: Die oberste Leitung ist innerhalb der Organisation in der Lage, Verantwortung zu delegieren und Ressourcen bereitzustellen.

Anmerkung 2 zum Begriff: Wenn der Anwendungsbereich des *Managementsystems* (3.4) nur einen Teil einer Organisation umfasst, bezieht sich „oberste Leitung" auf diejenigen, die diesen Teil führen und steuern.

3.4
Managementsystem
Satz zusammenhängender oder sich gegenseitig beeinflussender Elemente einer *Organisation* (3.1), um *Leitlinien* (3.5), *Ziele* (3.6) und *Prozesse* (3.8) zum Erreichen dieser Ziele festzulegen

Anmerkung 1 zum Begriff: Ein Managementsystem kann eine oder mehrere Disziplinen behandeln.

Anmerkung 2 zum Begriff: Die Elemente des Managementsystems beinhalten die Struktur der Organisation, Rollen und Verantwortlichkeiten, Planung sowie Betrieb.

3.5
Leitlinie
Absichten und Ausrichtung einer *Organisation* (3.1), wie sie von der *obersten Leitung* (3.3) formell ausgedrückt sind

3.6
Ziel
zu erreichendes Ergebnis

Anmerkung 1 zum Begriff: Ein Ziel kann strategisch, taktisch oder operativ sein.

Anmerkung 2 zum Begriff: Ziele können sich auf verschiedene Disziplinen beziehen (z. B. Finanz-, Gesundheits- und Sicherheits- und Umweltziele). Sie können z. B. organisationsweit gelten, oder für ein Projekt, ein Produkt oder einen *Prozess* (3.8) spezifisch sein.

Anmerkung 3 zum Begriff: Ein Ziel kann auf andere Weise ausgedrückt werden, z. B. als beabsichtigtes Ergebnis, als Zweck, als betriebliches Kriterium, als Ziel für den Schutz personenbezogener Daten oder durch die Verwendung anderer Wörter mit ähnlicher Bedeutung (en: aim, goal, target).

Anmerkung 4 zum Begriff: Im Kontext von *Managementsystemen für Datenschutzinformationen* (3.22) werden Sicherheitsziele von *Organisationen* (3.1) im Einklang mit ihren *Leitlinien* (3.5) zum Schutz personenbezogener Daten gesetzt, um bestimmte Ergebnisse zu erreichen.

3.7
Risiko
Auswirkung von Ungewissheit

Anmerkung 1 zum Begriff: Eine Auswirkung ist eine Abweichung vom Erwarteten – in positiver oder negativer Hinsicht.

Anmerkung 2 zum Begriff: Ungewissheit ist der Zustand des auch teilweisen Fehlens von Informationen im Hinblick auf das Verständnis eines Ereignisses oder Wissen über ein Ereignis, seine Folgen oder seine Wahrscheinlichkeit.

Anmerkung 3 zum Begriff: Risiko wird häufig durch Bezugnahme auf mögliche Ereignisse (definiert in ISO Guide 73) und Folgen (definiert in ISO Guide 73) oder durch eine Kombination beider charakterisiert.

Anmerkung 4 zum Begriff: Risiko wird oft häufig mittels der Folgen eines Ereignisses (einschließlich Veränderungen der Umstände) in Verbindung mit der Wahrscheinlichkeit (wie in ISO Guide 73 definiert) des Eintretens beschrieben.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

3.8
Prozess
Satz zusammenhängender oder sich gegenseitig beeinflussender Tätigkeiten, der Eingaben verwendet oder umwandelt, um ein Ergebnis bereitzustellen

Anmerkung 1 zum Begriff: Ob das Ergebnis eines Prozesses als Ausgabe, Produkt oder Dienstleistung bezeichnet wird, ist abhängig vom Kontext der Verweisung.

3.9
Kompetenz
Fähigkeit, Wissen und Fertigkeiten anzuwenden, um beabsichtigte Ergebnisse zu erzielen

3.10
dokumentierte Information
Information, die von einer *Organisation* (3.1) gelenkt und aufrechterhalten werden muss, und das Medium, auf dem sie enthalten ist

Anmerkung 1 zum Begriff: Dokumentierte Information kann in jeglichem Format oder Medium vorliegen sowie aus jeglicher Quelle stammen.

Anmerkung 2 zum Begriff: Dokumentierte Information kann sich beziehen auf: – das *Managementsystem (*3.4), einschließlich damit in Zusammenhang stehender *Prozesse* (3.8); – Informationen, die für den Betrieb der Organisation geschaffen wurden (Dokumentation); – Nachweise erreichter Ergebnisse (Aufzeichnungen).

3.11
Leistung
messbares Ergebnis

Anmerkung 1 zum Begriff: Leistung kann sich entweder auf quantitative oder qualitative Feststellungen beziehen.

Anmerkung 2 zum Begriff: Leistung kann sich auf das Führen und Steuern von Tätigkeiten, *Prozessen* (3.8), Produkten, Dienstleistungen, Systemen oder *Organisationen* (3.1) beziehen.

3.12
fortlaufende Verbesserung
wiederkehrende Tätigkeit zum Steigern der *Leistung* (3.11)

3.13
Wirksamkeit
Ausmaß, in dem geplante Tätigkeiten verwirklicht und geplante Ergebnisse erreicht werden

3.14
Anforderung
Erfordernis oder Erwartung, das oder die festgelegt, üblicherweise vorausgesetzt oder verpflichtend ist

Anmerkung 1 zum Begriff: „Üblicherweise vorausgesetzt“ bedeutet, dass es für die *Organisation* (3.1) und andere *interessierte Parteien* (3.2) übliche oder allgemeine Praxis ist, dass das entsprechende Erfordernis oder die entsprechende Erwartung vorausgesetzt wird.

Anmerkung 2 zum Begriff: Eine festgelegte Anforderung ist eine, die z. B. in *dokumentierter Information* (3.10) enthalten ist.

3.15
Konformität
Erfüllung einer *Anforderung* (3.14)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

3.16
Nichtkonformität
Nichterfüllung einer *Anforderung* (3.14)

3.17
Korrekturmaßnahme
Maßnahme zum Beseitigen der Ursache(n) einer *Nichtkonformität* (3.16) und zum Verhindern des erneuten Auftretens

3.18
Audit
systematischer und unabhängiger *Prozess* (3.8) zum Erlangen von Auditnachweisen und zu deren objektiver Auswertung, um zu bestimmen, inwieweit Auditkriterien erfüllt sind

Anmerkung 1 zum Begriff: Ein Audit kann ein internes Audit (Erstparteien-Audit) oder externes Audit (Zweit- oder Drittparteien-Audit) sein und es kann ein kombiniertes Audit sein (Verbindung zweier oder mehrerer Disziplinen).

Anmerkung 2 zum Begriff: Ein internes Audit wird von der *Organisation* (3.1) selbst durchgeführt, oder von einer externen Stelle in ihrem Auftrag.

Anmerkung 3 zum Begriff: „Auditnachweise“ und „Auditkriterien“ sind in ISO 19011 definiert.

3.19
Messung
Prozess (3.8) zum Bestimmen eines Wertes

3.20
Überwachung
Bestimmung des Zustands eines Systems, eines *Prozesses* (3.8) oder einer Tätigkeit

Anmerkung 1 zum Begriff: Zum Bestimmen des Zustands kann es erforderlich sein, zu prüfen, zu beaufsichtigen oder kritisch zu beobachten.

3.21
gemeinsame verantwortliche Stelle
verantwortliche Stelle, die gemeinsam mit einer oder mehreren anderen verantwortlichen Stellen die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten festlegt

3.22
Kunde
Person oder *Organisation* (3.1), die ein Produkt oder einen Dienst erhalten könnte oder erhält, das/der für diese Person oder *Organisation* (3.1) gedacht oder erforderlich ist

BEISPIEL Verbraucher, Kunde, Endnutzer, Einzelhändler, Empfänger eines Produkts oder Dienstes von einem internen *Prozess* (3.8), Begünstigter und Einkäufer.

Anmerkung 1 zum Begriff: Ein Kunde kann sich innerhalb oder außerhalb der Organisation befinden.

Anmerkung 2 zum Begriff: Ein Kunde kann eine *Organisation* (3.1) sein, die einen Vertrag mit einer verantwortlichen Stelle hat, eine verantwortliche Stelle, die einen Vertrag mit einem Auftragsverarbeiter hat, oder ein Auftragsverarbeiter, der einen Vertrag mit einem Unterauftragnehmer für die Verarbeitung personenbezogener Daten hat (weitere Informationen siehe 4.2).

3.23
Managementsystem für Datenschutzinformationen
PIMS, en: Privacy Information Management System
Managementsystem (3.4), das sich mit dem Schutz der durch die Verarbeitung personenbezogener Daten möglicherweise beeinträchtigten Privatsphäre befasst

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

3.24
Informationssicherheitsprogramm
Reihe von Leitlinien (3.5), Zielen (3.6) und Prozessen (3.8), die entwickelt wurden, um Risiken (3.7) für die Werte einer Organisation (3.1) zu verwalten und so die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen

Anmerkung 1 zum Begriff: Ein Informationssicherheitsprogramm kann beispielsweise ein Managementsystem für Informationssicherheit sein, z. B. auf der Basis von ISO/IEC 27001.

3.25
Erklärung zur Anwendbarkeit
Dokumentation aller notwendigen Maßnahmen und Begründung der Aufnahme oder des Ausschlusses von Maßnahmen

Anmerkung 1 zum Begriff: Organisationen benötigen möglicherweise nicht alle in Anhang A aufgeführten Maßnahmen oder können sogar die Liste in Anhang A durch zusätzliche, durch die Organisation selbst eingeführte Maßnahmen erweitern.

4 Kontext der Organisation

4.1 Verstehen der Organisation und ihres Kontextes

Die Organisation muss externe und interne Themen bestimmen, die für ihren Zweck maßgeblich sind und sich auf ihre Fähigkeit auswirken, das/die beabsichtigte(n) Ergebnis(se) ihres Managementsystems für Datenschutzinformationen zu erreichen.

Die Organisation muss bestimmen, ob der Klimawandel ein maßgebliches Thema für sie ist.

Die Organisation muss bestimmen, ob sie als verantwortliche Stelle (einschließlich als gemeinsame verantwortliche Stelle) oder als Auftragsverarbeiter fungiert.

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

ANMERKUNG 1 Externe und interne Themen können unter anderem Folgendes umfassen:

— 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 (d. h. als verantwortliche Stelle und als Auftragsverarbeiter), müssen getrennte Rollen bestimmt werden, die jeweils Gegenstand einer separaten Reihe von Maßnahmen sind.

ANMERKUNG 2 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.

4.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien

Die Organisation muss Folgendes bestimmen:

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

— die interessierten Parteien, die für ihr Managementsystem für Datenschutzinformationen relevant sind;

— die relevanten Anforderungen dieser interessierten Parteien;

— welche dieser Anforderungen durch das Managementsystem für Datenschutzinformationen erfüllt werden.

ANMERKUNG 1 Maßgebliche interessierte Parteien können Anforderungen im Zusammenhang mit dem Klimawandel haben.

Die Organisation muss zu ihren interessierten Parteien diejenigen Parteien zählen, die Interessen oder Verantwortlichkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten haben, einschließlich der betroffenen Personen.

ANMERKUNG 2 Andere interessierte Parteien können Kunden (siehe 4.2), Aufsichtsbehörden, andere verantwortliche Stellen, Auftragsverarbeiter und ihre Unterauftragnehmer sein.

Je nach der Rolle der Organisation kann der Begriff „Kunde“ wie folgt verstanden werden:

a) als eine Organisation, die einen Vertrag mit einer verantwortlichen Stelle hat (z. B. der Kunde der verantwortlichen Stelle, der Fall, dass eine Organisation eine gemeinsame verantwortliche Stelle ist);

b) als eine verantwortliche Stelle, die einen Vertrag mit einem Auftragsverarbeiter hat (z. B. der Kunde des Auftragsverarbeiters); oder

c) als ein Auftragsverarbeiter, der einen Vertrag mit einem Unterauftragnehmer für die Verarbeitung personenbezogener Daten hat (z. B. der Kunde des unterbeauftragten Auftragsverarbeiters).

ANMERKUNG 3 Eine natürliche Person, die in einer Business-to-Consumer-Beziehung mit einer Organisation steht, wird in diesem Dokument als „betroffene Person“ bezeichnet.

ANMERKUNG 4 Anforderungen, die für die Verarbeitung personenbezogener Daten relevant sind, können durch gesetzliche und behördliche Anforderungen, durch vertragliche Verpflichtungen und durch selbst auferlegte organisatorische Ziele bestimmt werden. Die in ISO/IEC 29100 festgelegten Datenschutzgrundsätze bieten eine Leitlinie für die Verarbeitung personenbezogener Daten.

ANMERKUNG 5 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 oder einer entsprechenden Reihe von Spezifikationen. Diese Parteien können eine unabhängig geprüfte Einhaltung dieser Normen fordern.

4.3 Festlegung des Anwendungsbereichs des Managementsystems für Datenschutzinformationen

Die Organisation muss die Grenzen und die Anwendbarkeit des Managementsystems für Datenschutzinformationen bestimmen, um dessen Anwendungsbereich festzulegen.

Bei der Festlegung des Anwendungsbereichs muss die Organisation Folgendes berücksichtigen:

— die unter 4.1 aufgeführten externen und internen Themen;

— die unter 4.2 aufgeführten Anforderungen.

Der Anwendungsbereich des Datenschutzinformationssystems der Organisation muss als dokumentierte Information verfügbar sein und gepflegt werden.

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

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

4.4 Managementsystem für Datenschutzinformationen

Die Organisation muss entsprechend den Anforderungen dieses Dokuments ein Managementsystem für Datenschutzinformationen aufbauen, verwirklichen, aufrechterhalten und fortlaufend verbessern, einschließlich der benötigten Prozesse und ihrer Wechselwirkungen.

5 Führung

5.1 Führung und Verpflichtung

Die oberste Leitung muss in Bezug auf das Managementsystem für Datenschutzinformationen Führung und Verpflichtung zeigen, indem sie:

— sicherstellt, dass die Datenschutzrichtlinie (siehe 5.2) und Datenschutzziele (siehe 6.2) festgelegt und mit der strategischen Ausrichtung der Organisation vereinbar sind;

— die Integration der Anforderungen an das Managementsystem für Datenschutzinformationen in die Geschäftsprozesse der Organisation sicherstellt;

— sicherstellt, dass die für das Managementsystem für Datenschutzinformationen erforderlichen Ressourcen zur Verfügung stehen;

— die Bedeutung eines wirksamen Datenschutzmanagements sowie die Wichtigkeit der Erfüllung der Anforderungen des Managementsystems für Datenschutzinformationen vermittelt;

— sicherstellt, dass das Managementsystem für Datenschutzinformationen sein beabsichtigtes Ergebnis bzw. seine beabsichtigten Ergebnisse erzielt;

— Personen anleitet und unterstützt, damit diese zur Wirksamkeit des Managementsystems für Datenschutzinformationen beitragen können;

— fortlaufende Verbesserung fördert;

— andere relevante Rollen unterstützt, um deren Führungsrolle in deren jeweiligen Verantwortungsbereichen deutlich zu machen.

ANMERKUNG Wenn in diesem Dokument das Wort „Geschäft“ (en: business) verwendet wird, kann dieses im weiteren Sinne verstanden werden und bezieht sich auf Tätigkeiten, die für die Zwecke der Organisation bzw. deren Existenz entscheidend sind.

5.2 Datenschutzrichtlinie

Die oberste Leitung muss eine Datenschutzrichtlinie vorgeben, die:

a) für den Zweck der Organisation angemessen ist;

b) einen Rahmen zum Festlegen von Datenschutzzielen bietet;

c) eine Verpflichtung zur Erfüllung anwendbarer Anforderungen enthält;

d) eine Verpflichtung zur fortlaufenden Verbesserung des Managementsystems für Datenschutzinformationen enthält.

Die Datenschutzrichtlinie muss:

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

— als dokumentierte Information verfügbar sein;

— innerhalb der Organisation bekanntgemacht werden;

— für interessierte Parteien verfügbar sein, soweit angemessen.

5.3 Rollen, Verantwortlichkeiten und Befugnisse

Die oberste Leitung muss sicherstellen, dass die Verantwortlichkeiten und Befugnisse für relevante Rollen zugewiesen und innerhalb der Organisation bekannt gemacht werden.

Die oberste Leitung muss die Verantwortlichkeit und Befugnis zuweisen für:

a) das Sicherstellen, dass das Managementsystem für Datenschutzinformationen die Anforderungen dieses Dokuments erfüllt;

b) das Berichten an die oberste Leitung über die Leistung des Managementsystems für Datenschutzinformationen.

6 Planung

6.1 Aktionen zum Umgang mit Risiken und Chancen

6.1.1 Allgemeines

Bei Planungen für das Managementsystem für Datenschutzinformationen muss die Organisation die in 4.1 genannten Themen und die in 4.2 genannten Anforderungen berücksichtigen sowie die Risiken und Chancen bestimmen, die behandelt werden müssen, um:

— sicherzustellen, dass das Managementsystem für Datenschutzinformationen seine angestrebten Ergebnisse erzielen kann;

— unerwünschte Auswirkungen zu verhindern oder zu verringern;

— fortlaufende Verbesserung zu erreichen.

Die Organisation muss planen:

a) Maßnahmen zum Umgang mit diesen Risiken und Chancen;

b) wie

— die Maßnahmen in die Prozesse des Managementsystems für Datenschutzinformationen der Organisation integriert und dort umgesetzt werden;

— die Wirksamkeit dieser Maßnahmen bewertet wird.

6.1.2 Datenschutz-Folgenabschätzung

Die Organisation muss einen Prozess zur Datenschutz-Risikobeurteilung festlegen und anwenden, der:

a) Datenschutzrisikokriterien festlegt und aufrechterhält, die Folgendes beinhalten:

   1) Kriterien für die Risikoakzeptanz; und

   2) Kriterien für die Durchführung von Datenschutz-Risikobeurteilungen;

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

b) sicherstellt, dass wiederholte Datenschutz-Risikobeurteilungen zu konsistenten, gültigen und vergleichbaren Ergebnissen führen;

c) die Datenschutzrisiken identifiziert:

   1) die in Zusammenhang mit dem Schutz personenbezogener Daten und mit Informationssicherheitsrisiken innerhalb des Geltungsbereichs des Managementsystems für Datenschutzinformationen stehen; und

   2) die Risikoeigentümer identifizieren;

d) die Datenschutzrisiken identifiziert, die:

   1) eine Einschätzung der potenziellen Folgen für die Organisation und die betroffenen Personen bei Eintritt der nach 6.1.2 c) 1) identifizierten Risiken ermöglichen;

   2) eine Abschätzung der realistischen Eintrittswahrscheinlichkeiten der nach 6.1.2 c) 1) identifizierten Risiken ermöglichen; und

   3) Bestimmung des Risikoniveaus ermöglichen;

e) die Datenschutzrisiken abschätzt, die:

   1) die einen Vergleich der Ergebnisse der Risikoanalyse mit den nach 6.1.2 a) festgelegten Risikokriterien ermöglichen; und

   2) die eine Priorisierung der analysierten Risiken für die Risikobehandlung ermöglichen.

Die Organisation muss dokumentierte Informationen über den Prozess zur Datenschutz-Folgenabschätzung aufbewahren.

ANMERKUNG Weitere Informationen zum Prozess der Datenschutz-Folgenabschätzung siehe ISO/IEC 27557.

6.1.3 Datenschutz-Risikobehandlung

Die Organisation muss einen Datenschutz-Risikobehandlungsprozess definieren und anwenden, um Risiken im Zusammenhang mit der Verarbeitung von personenbezogenen Daten (einschließlich Risiken für betroffene Personen und die Sicherheit der personenbezogenen Daten) zu behandeln, indem sie:

a) angemessene Optionen für die Datenschutz-Risikobehandlung unter Berücksichtigung der Ergebnisse der Risikobeurteilung auswählt;

b) alle Maßnahmen, die zur Umsetzung der gewählte(n) Option(en) für die Datenschutz-Risikobehandlung erforderlich sind, festlegt;

   ANMERKUNG 1 Organisationen können Maßnahmen nach Bedarf gestalten oder aus einer beliebigen Quelle auswählen.

c) das von der Organisation umgesetzte Informationssicherheitsprogramm identifiziert und dokumentiert, einschließlich der angemessenen Sicherheitsmaßnahmen;

   ANMERKUNG 2 ISO/IEC 27002 enthält eine Liste von möglichen Informationssicherheitsmaßnahmen. Wenn das Informationssicherheitsprogramm auf ISO/IEC 27001 beruht, werden Anwender dieses Dokuments auf ISO/IEC 27002 verwiesen, um sicherzustellen, dass keine wichtigen Informationssicherheitsmaßnahmen übersehen werden.

d) die nach 6.1.3 b) festgelegten Maßnahmen mit den Maßnahmen in Anhang A vergleicht und überprüft, dass keine erforderlichen Maßnahmen ausgelassen wurden;

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

ANMERKUNG 3 Anhang A enthält eine Liste von möglichen Maßnahmen für den Datenschutz. Anwender dieses Dokuments werden auf Anhang A verwiesen, um sicherzustellen, dass keine wichtigen Maßnahmen für den Datenschutz übersehen werden.

ANMERKUNG 4 Die in Anhang A aufgeführten Maßnahmen für den Datenschutz sind nicht erschöpfend und können bei Bedarf durch zusätzliche Maßnahmen für den Datenschutz ergänzt werden.

ANMERKUNG 5 Organisationen können bei der Betrachtung der Sicherheit der Verarbeitung personenbezogener Daten die Sicherheit und den Datenschutz auf einheitliche Weise behandeln, indem sie beispielsweise die Risikobeurteilungen für Sicherheit und Datenschutz miteinander kombinieren, oder sie können sie als getrennte Entitäten mit Überlappungsbereichen behandeln.

e) eine Erklärung zur Anwendbarkeit erstellen, die Folgendes enthält:

   — die erforderlichen Maßnahmen (siehe 6.1.3 b), c) und d));

   — die Begründung für ihre Aufnahme;

   — ob die notwendigen Maßnahmen umgesetzt sind oder nicht; und

   — Gründe für die Nichteinbeziehung von Maßnahmen aus Anhang A.

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

f) einen Plan zur Datenschutz-Risikobehandlung ausarbeitet;

g) die Genehmigung der Risikoeigentümer für den Plan zur Datenschutz-Risikobehandlung und die Akzeptanz der Restrisiken einholt; und

h) die Leitlinien in Anhang B für die Umsetzung der in b) und c) festgelegten Maßnahmen berücksichtigt.

Die Organisation muss dokumentierte Informationen über den Informationsdatenschutz-Risikobehandlungsprozess aufbewahren.

6.2 Datenschutzziele und Planung zu deren Erreichung

Die Organisation muss Datenschutzziele für relevante Funktionen und Ebenen festlegen.

Die Datenschutzziele müssen:

a) mit der Datenschutzrichtlinie (siehe 5.2) konsistent sein;

b) messbar sein (sofern machbar);

c) anwendbare Anforderungen berücksichtigen;

d) überwacht werden;

e) kommuniziert werden;

f) soweit erforderlich, aktualisiert werden;

g) als dokumentierte Information verfügbar sein.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Bei der Planung zum Erreichen der Datenschutzziele muss die Organisation bestimmen:

— was getan werden wird;

— welche Ressourcen erforderlich sein werden;

— wer verantwortlich sein wird;

— wann es abgeschlossen sein wird;

— wie die Ergebnisse bewertet werden.

6.3 Planung von Änderungen

Wenn die Organisation feststellt, dass Änderungen am Managementsystem für Datenschutzinformationen erforderlich sind, müssen diese Änderungen geplant durchgeführt werden.

7 Unterstützung

7.1 Ressourcen

Die Organisation muss die erforderlichen Ressourcen für den Aufbau, die Umsetzung, die Aufrechterhaltung und die fortlaufende Verbesserung des Managementsystems für Datenschutzinformationen bestimmen und bereitstellen.

7.2 Kompetenz

Die Organisation muss:

— für Personen, die unter ihrer Aufsicht Tätigkeiten verrichten, welche die Datenschutzleistung der Organisation beeinflussen, die erforderliche Kompetenz bestimmen;

— sicherstellen, dass diese Personen auf Grundlage angemessener Ausbildung, Schulung oder Erfahrung kompetent sind;

— wenn erforderlich, Maßnahmen einleiten, um die benötigte Kompetenz zu erwerben, und die Wirksamkeit der getroffenen Maßnahmen bewerten.

Es müssen angemessene dokumentierte Informationen als Nachweis der Kompetenz verfügbar sein.

ANMERKUNG Geeignete Maßnahmen können zum Beispiel sein: Schulung, Mentoring oder Versetzung von gegenwärtig angestellten Personen; oder Anstellung oder Beauftragung kompetenter Personen.

7.3 Bewusstsein

Personen, die unter Aufsicht der Organisation Tätigkeiten verrichten, müssen sich bewusst sein über:

— die Datenschutzrichtlinie (siehe 5.2);

— ihren Beitrag zur Wirksamkeit des Managementsystems für Datenschutzinformationen, einschließlich der Vorteile einer verbesserten Datenschutzleistung;

— die Folgen einer Nichterfüllung der Anforderungen des Managementsystems für Datenschutzinformationen.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

7.4 Kommunikation

Die Organisation muss die interne und externe Kommunikation in Bezug auf das Managementsystem für Datenschutzinformationen bestimmen, einschließlich:

— zu welchen Themen sie kommunizieren wird;

— wann zu kommunizieren ist;

— mit wem zu kommunizieren ist;

— wie zu kommunizieren ist.

7.5 Dokumentierte Information

7.5.1 Allgemeines

Das Managementsystem für Datenschutzinformationen der Organisation muss beinhalten:

a) die von diesem Dokument geforderte dokumentierte Information;

b) dokumentierte Informationen, welche die Organisation als notwendig für die Wirksamkeit des Managementsystems für Datenschutzinformationen bestimmt hat.

ANMERKUNG Der Umfang dokumentierter Informationen für ein Managementsystem für Datenschutzinformationen kann sich von Organisation zu Organisation unterscheiden, und zwar aufgrund:

— der Größe der Organisation und der Art ihrer Tätigkeiten, Prozesse, Produkte und Dienstleistungen;

— der Komplexität ihrer Prozesse und deren Wechselwirkungen;

— der Kompetenz der Personen.

7.5.2 Erstellen und Aktualisieren dokumentierter Informationen

Beim Erstellen und Aktualisieren dokumentierter Informationen muss die Organisation Folgendes sicherstellen:

— eine angemessene Kennzeichnung und Beschreibung (z. B. Titel, Datum, Autor oder Referenznummer);

— ein angemessenes Format (z. B. Sprache, Softwareversion, Graphiken) und Medium (z. B. Papier, elektronisch);

— eine angemessene Überprüfung und Genehmigung im Hinblick auf Eignung und Angemessenheit.

7.5.3 Lenkung dokumentierter Information

Die für das Managementsystem für Datenschutzinformationen erforderliche und von diesem Dokument geforderte dokumentierte Information muss gelenkt werden, um sicherzustellen, dass sie:

a) verfügbar und zur Verwendung geeignet ist, wo und wann sie benötigt wird;

b) angemessen geschützt wird (z. B. vor Verlust der Vertraulichkeit, unsachgemäßem Gebrauch oder Integritätsverlust).

Zur Lenkung dokumentierter Information muss die Organisation, falls zutreffend, folgende Tätigkeiten berücksichtigen:

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

— Verteilung, Zugriff, Bereitstellung und Verwendung;

— Ablage/Speicherung und Erhaltung, einschließlich Erhaltung der Lesbarkeit;

— Überwachung von Änderungen (z. B. Versionskontrolle);

— Aufbewahrung und Verfügung über den weiteren Verbleib.

Dokumentierte Information externer Herkunft, die von der Organisation als notwendig für Planung und Betrieb des Managementsystems für Datenschutzinformationen bestimmt wurde, muss angemessen gekennzeichnet und gelenkt werden.

ANMERKUNG Zugriff kann eine Entscheidung voraussetzen, mit der die Erlaubnis erteilt wird, dokumentierte Information lediglich zu lesen oder die Erlaubnis und Befugnis zum Lesen und Ändern dokumentierter Information.

8 Betrieb

8.1 Betriebliche Planung und Steuerung

Die Organisation muss die Prozesse zur Erfüllung der Anforderungen und zur Durchführung der in Abschnitt 6 bestimmten Maßnahmen planen, verwirklichen und steuern, indem sie:

— Kriterien für die Prozesse festlegt;

— die Steuerung der Prozesse in Übereinstimmung mit den Kriterien durchführt.

Dokumentierte Information muss im notwendigen Umfang verfügbar sein, so dass darauf vertraut werden kann, dass die Prozesse wie geplant durchgeführt wurden.

Die Organisation muss geplante Änderungen überwachen sowie die Folgen unbeabsichtigter Änderungen beurteilen und, falls notwendig, Maßnahmen ergreifen, um jegliche negativen Auswirkungen zu vermindern.

Die Organisation muss sicherstellen, dass extern bereitgestellte Prozesse, Produkte oder Dienstleistungen, die für das Managementsystem für Datenschutzinformationen relevant sind, kontrolliert werden.

8.2 Datenschutz-Risikobeurteilung

Die Organisation muss in geplanten Abständen Datenschutz-Risikobeurteilungen vornehmen oder immer dann, wenn erhebliche Änderungen vorgeschlagen werden oder auftreten. Dabei sind die in 6.1.2 a) festgelegten Kriterien zu berücksichtigen.

Die Organisation muss dokumentierte Information über die Ergebnisse der Datenschutz-Risikobeurteilungen aufbewahren.

8.3 Datenschutz-Risikobehandlung

Die Organisation muss den Plan für die Datenschutz-Risikobehandlung umsetzen.

Die Organisation muss dokumentierte Information über die Ergebnisse der Datenschutz-Risikobehandlung aufbewahren.

9 Bewertung der Leistung

9.1 Überwachung, Messung, Analyse und Bewertung

Die Organisation muss Folgendes bestimmen:

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

— was überwacht und gemessen werden muss;

— die Methoden zur Überwachung, Messung, Analyse und Bewertung, sofern zutreffend, um gültige Ergebnisse sicherzustellen;

— wann die Überwachung und Messung durchzuführen ist;

— wann die Ergebnisse der Überwachung und Messung zu analysieren und zu bewerten sind.

Es müssen dokumentierte Informationen als Nachweis der Ergebnisse verfügbar sein.

Die Organisation muss die Datenschutzleistung und die Wirksamkeit des Managementsystems für Datenschutzinformationen bewerten.

9.2 Internes Audit

9.2.1 Allgemeines

Die Organisation muss in geplanten Abständen interne Audits durchführen, um Informationen darüber zu erhalten, ob das Managementsystem für Datenschutzinformationen:

a) folgende Anforderungen erfüllt:

— die Anforderungen der Organisation an ihr Managementsystem für Datenschutzinformationen;

— die Anforderungen dieses Dokuments;

b) wirksam umgesetzt und aufrechterhalten wird.

9.2.2 Internes Auditprogramm

Die Organisation muss ein oder mehrere Auditprogramme planen, aufbauen, verwirklichen und aufrechterhalten, einschließlich der Häufigkeit von Audits, Methoden, Verantwortlichkeiten, Anforderungen an die Planung sowie Berichterstattung.

Beim Aufbauen der internen Auditprogramme muss die Organisation die Bedeutung der betroffenen Prozesse und die Ergebnisse vorheriger Audits berücksichtigen.

Die Organisation muss:

a) für jedes Audit die Auditziele, -kriterien sowie den Umfang festlegen;

b) Auditoren so auswählen und Audits so durchführen, dass die Objektivität und Unparteilichkeit des Auditprozesses sichergestellt sind;

c) sicherstellen, dass die Ergebnisse von Audits der zuständigen Leitung berichtet werden.

Es müssen dokumentierte Informationen als Nachweis der Umsetzung der Auditprogramme und der Auditergebnisse verfügbar sein.

9.3 Managementbewertung

9.3.1 Allgemeines

Die oberste Leitung muss das Managementsystem für Datenschutzinformationen der Organisation in geplanten Abständen bewerten, um dessen fortdauernde Eignung, Angemessenheit und Wirksamkeit sicherzustellen.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

9.3.2 Eingaben für die Managementbewertung

Die Managementbewertung muss Folgendes umfassen:

a) den Status von Maßnahmen vorheriger Managementbewertungen;

b) Veränderungen bei externen und internen Themen, die das Managementsystem für Datenschutzinformationen betreffen;

c) Veränderungen bei den Erfordernissen und Erwartungen von interessierten Parteien, die relevant für das Managementsystem für Datenschutzinformationen sind;

d) Informationen über die Leistung des Managementsystems für Datenschutzinformationen, einschließlich Entwicklungen bei:

— Nichtkonformitäten und Korrekturmaßnahmen;

— Überwachungs- und Messergebnissen;

— Auditergebnissen;

d) Chancen zur fortlaufenden Verbesserung.

9.3.3 Ergebnisse der Managementbewertung

Die Ergebnisse der Managementbewertung müssen Entscheidungen zu Möglichkeiten der fortlaufenden Verbesserung sowie zu jeglichem Änderungsbedarf am Managementsystem für Datenschutzinformationen enthalten.

Es müssen dokumentierte Informationen als Nachweis der Ergebnisse von Managementbewertungen verfügbar sein.

10 Verbesserung

10.1 Fortlaufende Verbesserung

Die Organisation muss die Eignung, Angemessenheit und Wirksamkeit ihres Managementsystems für Datenschutzinformationen fortlaufend verbessern.

10.2 Nichtkonformität und Korrekturmaßnahmen

Liegt eine Nichtkonformität vor, muss die Organisation:

a) darauf reagieren und falls zutreffend:

— Maßnahmen zur Überwachung und zur Korrektur ergreifen;

— mit den Folgen umgehen;

b) die Notwendigkeit von Maßnahmen zur Beseitigung der Ursachen von Nichtkonformitäten bewerten, damit diese nicht erneut oder an anderer Stelle auftreten, und zwar durch:

— Überprüfen der Nichtkonformität;

— Bestimmen der Ursachen der Nichtkonformität;

— Bestimmen, ob vergleichbare Nichtkonformitäten bestehen oder möglicherweise auftreten können;

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

c) jede erforderliche Maßnahme ergreifen;

d) die Wirksamkeit aller ergriffenen Korrekturmaßnahmen überprüfen;

e) sofern erforderlich, das Managementsystem für Datenschutzinformationen ändern.

Korrekturmaßnahmen müssen den Auswirkungen der aufgetretenen Nichtkonformitäten angemessen sein.

Es müssen dokumentierte Informationen als Nachweis von Folgendem verfügbar sein:

— der Art der Nichtkonformität sowie jeder daraufhin getroffenen Maßnahme;

— der Ergebnisse jeder Korrekturmaßnahme.

11 Weitere Informationen zu Anhängen

Anhang A listet die PIMS-Referenzmaßnahmenziele und -Maßnahmen für eine Organisation auf, die als verantwortliche Stelle (unabhängig davon, ob sie einen Auftragsverarbeiter beschäftigt oder nicht, und ob sie mit einer anderen verantwortlichen Stelle zusammenarbeitet oder nicht) oder als Auftragsverarbeiter tätig ist (unabhängig davon, ob sie die Verarbeitung personenbezogener Daten an einen getrennten Auftragsverarbeiter vergibt oder nicht und einschließlich derjenigen, die personenbezogene Daten als Unterauftragnehmer für Auftragsverarbeiter verarbeiten), oder als Auftragsverarbeiter oder beides.

Anhang B listet die Leitlinien zur Umsetzung für das Managementsystem für Datenschutzinformationen zur Umsetzung der in Anhang A aufgelisteten Maßnahmen.

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 zeigt die Übereinstimmung zwischen den Maßnahmen in dieser Ausgabe von ISO/IEC 27701 und der vorherigen Ausgabe 2019.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Anhang A
(normativ)

PIMS-Referenzmaßnahmenziele und -Maßnahmen für verantwortliche Stellen und Auftragsverarbeiter

Dieser Anhang ist zur Verwendung durch Organisationen bestimmt, die als verantwortliche Stellen oder Auftragsverarbeiter oder beides tätig sind.

Nicht alle in diesem Anhang aufgeführten Maßnahmenziele und Maßnahmen müssen in der PIMS-Umsetzung enthalten sein. Eine Begründung für den Ausschluss von Maßnahmenzielen muss in der Erklärung zur Anwendbarkeit enthalten sein (siehe 6.1.3 f)). Ein Ausschluss kann u. a. dann begründet sein, wenn die Maßnahmen nach der Risikobeurteilung nicht als notwendig erachtet werden und wenn sie nach den geltenden Gesetzen oder Vorschriften nicht erforderlich sind (oder Ausnahmen davon unterliegen).

Tabelle A.1 ist für verantwortliche Stellen gedacht, Tabelle A.2 ist für Auftragsverarbeiter gedacht und Tabelle A.3 bezieht sich auf Sicherheitsmaßnahmen sowohl für verantwortliche Stellen als auch für Auftragsverarbeiter

ANMERKUNG Die Verweisungen in der Spalte „Maßnahmenverweisung“ in Tabelle A.1, Tabelle A.2 und Tabelle A.3 beziehen sich auf die entsprechenden Abschnittsnummern in Anhang B (z. B. ist die Anleitung für die Maßnahme A.1.2.2 in B.1.2.2 zu finden).

Tabelle A.1 — Maßnahmenziele und Maßnahmen für verantwortliche Stellen

Bedingungen für die Erhebung und Verarbeitung Zielsetzung: Bestimmen und Dokumentieren, dass die Verarbeitung rechtmäßig ist, mit einer rechtlichen Grundlage nach den geltenden Rechtssystemen, mit klar definierten und legitimen Zwecken.		
Maßnahmenverweisung	Maßnahmenüberschrift	Maßnahme
A.1.2.2	Identifizieren und Dokumentieren des Zwecks	Die Organisation muss die spezifischen Zwecke, für die die personenbezogenen Daten verarbeitet werden, identifizieren und dokumentieren.
A.1.2.3	Identifizieren der rechtmäßigen Grundlage	Die Organisation muss die geeignete rechtmäßige Grundlage für die Verarbeitung von personenbezogenen Daten für die identifizierten Zwecke bestimmen, dokumentieren und einhalten.
A.1.2.4	Bestimmen, wann und wie die Einwilligung einzuholen ist	Die Organisation muss 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.
A.1.2.5	Einholung und Aufzeichnung der Einwilligung	Die Organisation muss die Einwilligung der betroffenen Personen nach den dokumentierten Prozessen einholen und aufzeichnen.

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Tabelle A.1 (*fortgesetzt*)

A.1.2.6	Datenschutz-Folgenabschätzung	Die Organisation muss 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 bewerten und gegebenenfalls umsetzen.
A.1.2.7	Verträge mit Auftragsverarbeitern	Die Organisation muss einen schriftlichen Vertrag mit jedem von ihr eingesetzten Auftragsverarbeiter haben und sicherstellen, dass ihre Verträge mit Auftragsverarbeitern die Umsetzung der entsprechenden Maßnahmen in Anhang A vorsehen (siehe Tabelle A.2).
A.1.2.8	Gemeinsame verantwortliche Stelle	Die Organisation muss die jeweiligen Rollen und Verantwortlichkeiten für die Verarbeitung von personenbezogenen Daten (einschließlich Datenschutz und Sicherheitsanforderungen) mit jeder gemeinsamen verantwortlichen Stelle festlegen.
A.1.2.9	Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten	Die Organisation muss die notwendigen Aufzeichnungen zur Unterstützung ihrer Verpflichtungen für die Verarbeitung von personenbezogenen Daten festlegen und sicher aufbewahren.
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.		
A.1.3.2	Bestimmung und Erfüllung von Verpflichtungen gegenüber betroffenen Personen	Die Organisation muss 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.
A.1.3.3	Bestimmen von Informationen für betroffene Personen	Die Organisation muss die Informationen, die den betroffenen Personen bezüglich der Verarbeitung ihrer personenbezogenen Daten und des Zeitpunkts einer solchen Bereitstellung zur Verfügung zu stellen sind, festlegen und dokumentieren.
A.1.3.4	Bereitstellen von Informationen für betroffene Personen	Die Organisation muss den betroffenen Personen klare und leicht zugängliche Informationen zur Identifizierung der verantwortlichen Stelle und zur Beschreibung der Verarbeitung ihrer personenbezogenen Daten zur Verfügung stellen.
A.1.3.5	Bereitstellung eines Mechanismus zur Änderung oder zum Widerruf der Einwilligung	Die Organisation muss einen Mechanismus zur Verfügung stellen, mit dem betroffene Personen ihre Einwilligung ändern oder widerrufen können.
A.1.3.6	Bereitstellung eines Mechanismus zur Ablehnung der Verarbeitung personenbezogener Daten	Die Organisation muss einen Mechanismus zur Verfügung stellen, mit dem betroffene Personen die Verarbeitung ihrer personenbezogenen Daten ablehnen können.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2024-09

Tabelle A.1 (*fortgesetzt*)

A.1.3.7	Zugriff, Korrektur oder Löschung	Die Organisation muss Richtlinien, Verfahren oder Mechanismen umsetzen, um ihren Verpflichtungen gegenüber den betroffenen Personen nachzukommen, auf ihre personenbezogenen Daten zuzugreifen, sie zu korrigieren oder zu löschen.
A.1.3.8	Verpflichtungen von verantwortlichen Stellen, Dritte zu informieren	Die Organisation muss Dritte, mit denen personenbezogene Daten geteilt wurden, über jede Änderung, jeden Widerruf oder Einwände bezüglich der geteilten personenbezogenen Daten informieren und entsprechende Richtlinien, Verfahren oder Mechanismen umsetzen.
A.1.3.9	Bereitstellung einer Kopie der verarbeiteten personenbezogenen Daten	Die Organisation muss in der Lage sein, eine Kopie der personenbezogenen Daten, die auf Anfrage der betroffenen Person verarbeitet werden, zur Verfügung zu stellen.
A.1.3.10	Handhabung von Anfragen	Die Organisation muss Richtlinien und Verfahren für die Handhabung von und Reaktion auf rechtmäßige(n) Anfragen betroffener Personen definieren und dokumentieren.
A.1.3.11	Automatisierte Entscheidungsfindung	Die Organisation muss Verpflichtungen, einschließlich rechtlicher Verpflichtungen, gegenüber den betroffenen Personen identifizieren und ansprechen, die sich aus Entscheidungen der Organisation ergeben, die sich auf die betroffene Person beziehen und ausschließlich auf der automatischen Verarbeitung von personenbezogenen Daten beruhen.
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen Zielsetzung: Sicherstellen, dass Prozesse und Systeme so gestaltet sind, dass die Erhebung und Verarbeitung von personenbezogenen Daten (einschließlich Nutzung, Offenlegung, Aufbewahrung, Übertragung und Entsorgung) auf das für den ermittelten Zweck erforderliche Maß beschränkt sind.		
A.1.4.2	Beschränkte Erhebung	Die Organisation muss die Erhebung von personenbezogenen Daten auf das Minimum beschränken, das für die ermittelten Zwecke relevant, verhältnismäßig und notwendig ist.
A.1.4.3	Beschränkte Verarbeitung	Die Organisation muss die Verarbeitung von personenbezogenen Daten auf das beschränken, was für die ermittelten Zwecke angemessen, relevant und notwendig ist.
A.1.4.4	Genauigkeit und Qualität	Die Organisation muss sicherstellen und dokumentieren, dass die personenbezogenen Daten während ihres gesamten Lebenszyklus so genau, vollständig und aktuell sind, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.
A.1.4.5	Ziele der Sparsamkeit personenbezogener Daten	Die Organisation muss Ziele der Datensparsamkeit definieren und dokumentieren, und welche Mechanismen (wie z. B. die Entpersonalisierung) zur Erreichung dieser Ziele eingesetzt werden.
A.1.4.6	Entpersonalisierung personenbezogener Daten und Löschung am Ende der Verarbeitung	Die Organisation muss personenbezogene Daten entweder löschen oder in einer Form wiedergeben, die eine Identifizierung oder Neuidentifizierung der betroffenen Personen nicht zulässt, sobald die ursprünglichen personenbezogenen Daten für den/die ermittelten Zweck(e) nicht mehr erforderlich sind.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Tabelle A.1 (*fortgesetzt*)

A.1.4.7	Temporäre Dateien	Die Organisation muss sicherstellen, dass temporäre Dateien, die als Ergebnis der Verarbeitung von personenbezogenen Daten erstellt wurden, innerhalb eines festgelegten, dokumentierten Zeitraums nach dokumentierten Verfahren entsorgt (z. B. gelöscht oder vernichtet) werden.
A.1.4.8	Aufbewahrung	Die Organisation darf personenbezogene Daten nicht länger aufbewahren, als es für die Zwecke, für die die personenbezogenen Daten verarbeitet werden, erforderlich ist.
A.1.4.9	Entsorgung	Die Organisation muss über dokumentierte Richtlinien, Verfahren oder Mechanismen für die Entsorgung von personenbezogenen Daten verfügen.
A.1.4.10	Maßnahmen zur Übertragung personenbezogener Daten	Die Organisation muss personenbezogene Daten, die über ein Datenübertragungsnetzwerk übertragen werden (z. B. an eine andere Organisation gesendet), geeigneten Maßnahmen unterziehen, die sicherstellen sollen, dass die Daten ihren vorgesehenen Bestimmungsort erreichen.
Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten Zielsetzung: Zu bestimmen, ob und zu dokumentieren, wann personenbezogene Daten weitergegeben, an andere Rechtssysteme oder Dritte übertragen oder in Übereinstimmung mit den geltenden Verpflichtungen offengelegt werden.		
A.1.5.2	Ermittlung der Grundlage für die Übertragung von personenbezogenen Daten zwischen Rechtssystemen	Die Organisation muss die relevante Grundlage für die Übertragung von personenbezogenen Daten zwischen verschiedenen Rechtssystemen ermitteln und dokumentieren.
A.1.5.3	Länder und internationale Organisationen, an die personenbezogene Daten übertragen werden können	Die Organisation muss die Länder und internationalen Organisationen angeben und dokumentieren, an die personenbezogene Daten möglicherweise übertragen werden können.
A.1.5.4	Aufzeichnungen über die Übertragung von personenbezogenen Daten	Die Organisation muss Übertragungen von personenbezogenen Daten an oder von Dritten aufzeichnen und die Zusammenarbeit mit diesen Parteien sicherstellen, um zukünftige Anfragen in Bezug auf Verpflichtungen gegenüber den betroffenen Personen zu unterstützen.
A.1.5.5	Aufzeichnungen der Offenlegung von personenbezogenen Daten für Dritte	Die Organisation muss die Offenlegung von personenbezogenen Daten gegenüber Dritten aufzeichnen unter Angabe, welche personenbezogenen Daten an wen und zu welchem Zeitpunkt offengelegt wurden.

Tabelle A.2 — Maßnahmenziele und Maßnahmen für Auftragsverarbeiter

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.		
Maßnahmenverweisung	Maßnahmenüberschrift	Maßnahme

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Tabelle A.2 (*fortgesetzt*)

A.2.2.2	Kundenvereinbarung	Die Organisation muss, wo dies relevant ist, sicherstellen, dass der Vertrag zur Verarbeitung von personenbezogenen Daten bei der Rolle der Organisation durch Hilfestellung bei den Verpflichtungen des Kunden ansetzt (unter Berücksichtigung der Art der Verarbeitung und der der Organisation zur Verfügung stehenden Informationen).
A.2.2.3	Ziele der Organisation	Die Organisation muss sicherstellen, dass personenbezogene Daten, die im Namen eines Kunden verarbeitet werden, nur für die Ziele verarbeitet werden, die in den dokumentierten Anweisungen des Kunden zum Ausdruck kommen.
A.2.2.4	Verwendung für Marketing und Werbung	Die Organisation darf personenbezogene Daten, die im Rahmen eines Vertrags verarbeitet werden, nicht für Marketing- und Werbezwecke verwenden, ohne nachzuweisen, dass die vorherige Einwilligung der jeweiligen betroffenen Person eingeholt wurde. Die Organisation darf die Erteilung einer solchen Einwilligung nicht zur Bedingung für den Erhalt der Dienstleistung machen.
A.2.2.5	Verstoßende Anweisung	Die Organisation muss den Kunden informieren, wenn ihrer Meinung nach eine Verarbeitungsanweisung gegen geltende Gesetze oder Vorschriften verstößt.
A.2.2.6	Kundenverpflichtungen	Die Organisation muss dem Kunden die entsprechenden Informationen zur Verfügung stellen, so dass der Kunde die Einhaltung seiner Verpflichtungen nachweisen kann.
A.2.2.7	Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten	Die Organisation muss die notwendigen Aufzeichnungen zum Nachweis der Einhaltung ihrer Verpflichtungen (wie im anwendbaren Vertrag festgelegt) für die Verarbeitung von personenbezogenen Daten, die im Namen eines Kunden durchgeführt wird, festlegen und führen.
Verpflichtungen gegenüber betroffenen Personen Zielsetzung: Sicherstellen, dass betroffene Personen die angemessenen 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.		
A.2.3.2	Einhaltung von Verpflichtungen gegenüber betroffenen Personen	Die Organisation muss dem Kunden die Mittel zur Verfügung stellen, um seinen Verpflichtungen in Bezug auf betroffene Personen nachzukommen.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Tabelle A.2 (*fortgesetzt*)

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen Zielsetzung: Sicherstellen, dass Prozesse und Systeme so gestaltet sind, dass die Erhebung und Verarbeitung von personenbezogenen Daten (einschließlich Nutzung, Offenlegung, Aufbewahrung, Übertragung und Entsorgung) auf das für den ermittelten Zweck erforderliche Maß beschränkt sind.		
A.2.4.2	Temporäre Dateien	Die Organisation muss sicherstellen, dass temporäre Dateien, die als Ergebnis der Verarbeitung von personenbezogenen Daten erstellt wurden, innerhalb eines festgelegten, dokumentierten Zeitraums nach dokumentierten Verfahren entsorgt (z. B. gelöscht oder vernichtet) werden.
A.2.4.3	Rückgabe, Übertragung oder Entsorgung von personenbezogenen Daten	Die Organisation muss die Möglichkeit bieten, personenbezogene Daten auf sichere Art und Weise zurückzugeben, zu übertragen oder zu entsorgen. Sie muss ihre Richtlinie auch dem Kunden zur Verfügung stellen.
A.2.4.4	Maßnahmen zur Übertragung personenbezogener Daten	Die Organisation muss personenbezogene Daten, die über ein Datenübertragungsnetzwerk übertragen werden, geeigneten Maßnahmen unterziehen, die sicherstellen sollen, dass die Daten ihren vorgesehenen Bestimmungsort erreichen.
Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten Zielsetzung: Zu bestimmen, ob und zu dokumentieren, wann personenbezogene Daten weitergegeben, an andere Rechtssysteme oder Dritte übertragen oder in Übereinstimmung mit den geltenden Verpflichtungen offengelegt werden.		
A.2.5.2	Grundlage für die Übertragung von personenbezogenen Daten zwischen Rechtssystemen	Die Organisation muss den Kunden rechtzeitig über die Grundlage für Übertragungen von personenbezogenen Daten zwischen Rechtssystemen und über alle diesbezüglich geplanten Änderungen informieren, so dass dieser die Möglichkeit hat, diese Änderungen abzulehnen oder den Vertrag zu kündigen.
A.2.5.3	Länder und internationale Organisationen, an die personenbezogene Daten übertragen werden können	Die Organisation muss die Länder und internationalen Organisationen angeben und dokumentieren, an die personenbezogene Daten möglicherweise übertragen werden können.
A.2.5.4	Aufzeichnungen der Offenlegung von personenbezogenen Daten für Dritte	Die Organisation muss die Offenlegung von personenbezogenen Daten gegenüber Dritten aufzeichnen unter Angabe, welche personenbezogenen Daten an wen und wann offengelegt wurden.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Tabelle A.2 (*fortgesetzt*)

A.2.5.5	Benachrichtigung über Anträge auf Offenlegung von personenbezogenen Daten	Die Organisation muss den Kunden über alle rechtsverbindlichen Anträge auf Offenlegung von personenbezogenen Daten informieren.
A.2.5.6	Rechtsverbindliche Offenlegung von personenbezogenen Daten	Die Organisation muss alle Anträge auf Offenlegungen von personenbezogenen Daten, die nicht rechtsverbindlich sind, ablehnen, den entsprechenden Kunden konsultieren, bevor sie derartige Offenlegungen vornimmt und alle vertraglich vereinbarten Anträge auf Offenlegungen von personenbezogenen Daten, die vom entsprechenden Kunden autorisiert sind, annimmt.
A.2.5.7	Offenlegung von Unterauftragnehmern, die zur Verarbeitung von personenbezogenen Daten eingesetzt werden	Die Organisation muss dem Kunden jede Inanspruchnahme von Subunternehmern zur Verarbeitung von personenbezogenen Daten vorab offenlegen.
A.2.5.8	Einschaltung eines Unterauftragnehmers mit der Verarbeitung von personenbezogenen Daten	Die Organisation muss nur einen Unterauftragnehmer mit der Verarbeitung von personenbezogenen Daten nach dem Kundenvertrag beauftragen.
A.2.5.9	Wechsel des Unterauftragnehmers zur Verarbeitung von personenbezogenen Daten	Im Falle einer allgemeinen schriftlichen Genehmigung muss die Organisation den Kunden über alle beabsichtigten Änderungen bezüglich der Hinzufügung oder des Wechsels von Unterauftragnehmern zur Verarbeitung von personenbezogenen Daten informieren, um dem Kunden die Möglichkeit zu geben, diese Änderungen abzulehnen.

Tabelle A.3 — Maßnahmenziele und Maßnahmen für verantwortliche Stellen und Auftragsverarbeiter

Sicherheitsüberlegungen für verantwortlichen Stellen und Auftragsverarbeiter Zielsetzung: Sicherstellen der Sicherheit der Verarbeitung personenbezogener Daten.		
Maßnahmenverweisung	Maßnahmenüberschrift	Maßnahme
A.3.3	Richtlinien für die Informationssicherheit	Informationssicherheitsrichtlinien für die Verarbeitung personenbezogener Daten müssen definiert, von der Geschäftsleitung genehmigt, veröffentlicht, dem zuständigen Personal und den interessierten Parteien mitgeteilt und von diesen zur Kenntnis genommen sowie in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Tabelle A.3 (*fortgesetzt*)

A.3.4	Informationssicherheitsrollen und -verantwortlichkeiten	Die Aufgaben und Zuständigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten im Bereich der Informationssicherheit müssen entsprechend den Erfordernissen der Organisation definiert und zugewiesen werden.
A.3.5	Klassifizierung von Informationen	Informationen müssen entsprechend den Informationssicherheitsanforderungen der Organisation unter Berücksichtigung des Schutzes personenbezogener Daten auf der Grundlage von Vertraulichkeit, Integrität, Verfügbarkeit und relevanten Anforderungen der interessierten Parteien klassifiziert werden.
A.3.6	Kennzeichnung von Informationen	Ein angemessener Satz von Verfahren zur Kennzeichnung von Informationen, der den Schutz personenbezogener Daten berücksichtigt, muss entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt werden.
A.3.7	Informationsübertragung	Für alle Arten von Übertragungseinrichtungen innerhalb der Organisation und zwischen der Organisation und anderen Parteien müssen für die Verarbeitung personenbezogener Daten Regeln, Verfahren oder Vereinbarungen zur Informationsübermittlung vorhanden sein.
A.3.8	Identitätsmanagement	Der gesamte Lebenszyklus von Identitäten in Bezug auf die Verarbeitung personenbezogener Daten muss verwaltet werden.
A.3.9	Zugangsrechte	Zugangsrechte zu personenbezogenen Informationen und anderen zugehörigen Werten in Zusammenhang mit der Verarbeitung personenbezogener Daten müssen in Übereinstimmung mit den themenspezifischen Richtlinien und Regeln der Organisation für die Zugangssteuerung bereitgestellt, überprüft, geändert und entfernt werden.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2024-09

Tabelle A.3 (*fortgesetzt*)

A.3.10	Behandlung von Informationssicherheit in Lieferantenvereinbarungen	Je nach Art der Lieferantenbeziehung müssen die entsprechenden Anforderungen an die Informationssicherheit für die Verarbeitung personenbezogener Daten festgelegt und mit jedem Lieferanten vereinbart werden.
A.3.11	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	Die Organisation muss die Handhabung von Informationssicherheitsvorfällen in Zusammenhang mit der Auftragsverarbeitung planen und vorbereiten, indem sie Prozesse, Rollen und Verantwortlichkeiten für die Handhabung von Vorfällen definiert, einführt und kommuniziert.
A.3.12	Reaktion auf Informationssicherheitsvorfälle	Auf Informationssicherheitsvorfälle in Zusammenhang mit der Auftragsverarbeitung muss entsprechend den dokumentierten Verfahren reagiert werden.
A.3.13	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	Rechtliche, gesetzliche, behördliche und vertragliche Anforderungen, die für die Informationssicherheit in Zusammenhang mit der Auftragsverarbeitung relevant sind, und die Vorgehensweise der Organisation zur Erfüllung dieser Anforderungen müssen ermittelt, dokumentiert und auf dem neuesten Stand gehalten werden.
A.3.14	Schutz von Aufzeichnungen	Aufzeichnungen in Zusammenhang mit der Auftragsverarbeitung müssen vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt sein.
A.3.15	Unabhängige Überprüfung der Informationssicherheit	Die Vorgehensweise der Organisation für die Handhabung der Informationssicherheit in Zusammenhang mit der Auftragsverarbeitung und deren Umsetzung einschließlich der Mitarbeiter, Prozesse und Technologien, müssen auf unabhängige Weise in planmäßigen Abständen oder jeweils bei erheblichen Änderungen überprüft werden.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Tabelle A.3 (*fortgesetzt*)

A.3.16	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	Die Einhaltung der Informationssicherheitspolitik der Organisation, der themenspezifischen Richtlinien, Regeln und Normen in Zusammenhang mit der Auftragsverarbeitung muss regelmäßig überprüft werden.
A.3.17	Informationssicherheitsbewusstsein, ausbildung und -schulung	Das Personal der Organisation und relevante interessierte Parteien müssen ein angemessenes Bewusstsein für die Informationssicherheit, eine entsprechende Ausbildung und Schulung sowie regelmäßige Aktualisierungen der Informationssicherheitspolitik der Organisation, themenspezifischer Richtlinien und Verfahren erhalten, die für ihr berufliches Arbeitsgebiet in Zusammenhang mit der Auftragsverarbeitung relevant sind.
A.3.18	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche die Erfordernisse der Organisation an den Schutz von personenbezogenen Daten widerspiegeln, müssen identifiziert, dokumentiert, regelmäßig überprüft und von den Mitarbeitern und anderen interessierten Parteien unterzeichnet werden.
A.3.19	Aufgeräumte Arbeitsumgebung und Bildschirmsperren	Es müssen klare Regeln für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechseldatenträgern und klare Regeln für Bildschirmsperren für informationsverarbeitende Einrichtungen festgelegt und angemessen durchgesetzt werden.
A.3.20	Speichermedien	Speichermedien mit personenbezogenen Daten müssen während ihres gesamten Lebenszyklus – Erwerb, Verwendung, Transport und Entsorgung – in Übereinstimmung mit dem Klassifizierungsschema und den Handhabungsanforderungen der Organisation verwaltet werden.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Tabelle A.3 (*fortgesetzt*)

A.3.21	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	Arten von Geräten und Betriebsmitteln, die Speichermedien mit personenbezogenen Daten enthalten, müssen überprüft werden, um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind.
A.3.22	Endpunktgeräte des Benutzers	Personenbezogene Daten, die auf Endpunktgeräten der Benutzer gespeichert sind, von ihnen verarbeitet werden oder über sie zugänglich sind, müssen geschützt werden.
A.3.23	Sichere Authentifizierung	Sichere Authentifizierungstechnologien und Verfahren in Zusammenhang mit der Auftragsverarbeitung müssen auf Grundlage von Informationszugangsbeschränkungen umgesetzt werden.
A.3.24	Sicherung von Informationen	Sicherungskopien von personenbezogenen Daten und Software und Systemen, die in Zusammenhang mit der Auftragsverarbeitung stehen, müssen gepflegt und regelmäßig geprüft werden.
A.3.25	Protokollierung	Protokolle, die Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse in Zusammenhang mit der Auftragsverarbeitung aufzeichnen, müssen erstellt, gespeichert, geschützt und analysiert werden.
A.3.26	Verwendung von Kryptographie	Es müssen Regeln für den wirksamen Einsatz von Kryptographie in Zusammenhang mit der Auftragsverarbeitung, einschließlich der Verwaltung kryptographischer Schlüssel, festgelegt und umgesetzt werden.
A.3.27	Lebenszyklus einer sicheren Entwicklung	Regeln für die sichere Entwicklung von Software und Systemen in Zusammenhang mit der Auftragsverarbeitung müssen festgelegt und angewendet werden.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Tabelle A.3 (*fortgesetzt*)

A.3.28	Anforderungen an die Anwendungssicherheit	Die Anforderungen an die Informationssicherheit in Zusammenhang mit der Auftragsverarbeitung müssen bei der Entwicklung oder Beschaffung von Anwendungen ermittelt, spezifiziert und genehmigt werden.
A.3.29	Sichere Systemarchitektur und technische Grundsätze	Grundsätze für die Entwicklung sicherer Systeme in Zusammenhang mit der Verarbeitung personenbezogener Daten müssen festgelegt, dokumentiert, aktuell gehalten und bei allen Entwicklungsaktivitäten eines Informationssystems angewendet werden.
A.3.30	Ausgegliederte Entwicklung	Die Organisation muss die Aktivitäten im Zusammenhang mit der ausgegliederten Systementwicklung für die Verarbeitung personenbezogener Daten leiten, überwachen und überprüfen.
A.3.31	Prüfinformationen	Die Prüfinformationen in Zusammenhang mit der Auftragsverarbeitung müssen in geeigneter Weise ausgewählt, geschützt und verwaltet werden.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2024-09

Anhang B
(normativ)

Leitlinie zur Umsetzung für verantwortliche Stellen und Auftragsverarbeiter

B.1 Leitlinie zur Umsetzung für verantwortliche Stellen

B.1.1 Allgemeines

Die Ergänzungen in diesem Abschnitt bilden die PIMS-Leitlinie für verantwortliche Stellen. Die in diesem Abschnitt dokumentierte Leitlinie für die Umsetzung bezieht sich auf die in Tabelle A.1 aufgeführten Maßnahmen.

B.1.2 Bedingungen für die Erhebung und Verarbeitung

B.1.2.1 Zielsetzung

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

B.1.2.2 Identifizieren und Dokumentieren des Zwecks

Maßnahme

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

Leitlinie 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.

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 B.1.3.3). Dazu gehören Informationen, die zur Einholung der Einwilligung erforderlich sind (siehe B.1.2.4), sowie dokumentierte Informationen über Richtlinien und Verfahren (siehe B.1.2.9).

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.

B.1.2.3 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.

Leitlinie zur Umsetzung

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

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 der verantwortlichen Stelle.

Die Organisation sollte diese Grundlage für jede Verarbeitungsaktivität personenbezogener Daten dokumentieren (siehe B.1.2.9).

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 personenbezogenen Daten, 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 Verarbeitung personenbezogener Daten gelten.

Auch die Verwendung spezieller Kategorien von personenbezogenen Daten kann strengeren Maßnahmen unterliegen.

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

B.1.2.4 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.

Leitlinie 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 Anforderungen für die Einholung der Einwilligung gelten. Es kann nützlich sein, den/die Zweck(e) für die Verarbeitung mit Informationen darüber zu korrelieren, ob und wie die Einwilligung eingeholt wird.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

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.

B.1.2.5 Einholung und Aufzeichnung der Einwilligung

Maßnahme

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

Leitlinie 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 Leitlinie in B.1.3.4 folgen.

Die Einwilligung sollte:

— freiwillig erteilt;

— spezifisch in Bezug auf den Zweck der Verarbeitung; und

— eindeutig und explizit sein.

B.1.2.6 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 bewerten und gegebenenfalls umsetzen.

Leitlinie 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 besonderer Kategorien 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 B.1.2.9 für Einzelheiten zu dokumentierten Informationen über die Verarbeitung von personenbezogenen Daten, die über Auswirkungen auf den Datenschutz oder andere Risikobewertungen informieren können).

Weitere Informationen

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

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

B.1.2.7 Verträge mit Auftragsverarbeitern

Maßnahme

Die Organisation sollte einen schriftlichen Vertrag mit jedem von ihr eingesetzten Auftragsverarbeiter haben und sicherstellen, dass ihre Verträge mit Auftragsverarbeitern die Umsetzung der entsprechenden Maßnahmen in Anhang A vorsehen (siehe Tabelle A.2).

Leitlinie zur Umsetzung

Der Vertrag zwischen der Organisation und jedem Auftragsverarbeiter, der in ihrem Namen personenbezogene Daten verarbeitet, sollte den Auftragsverarbeiter verpflichten, die entsprechenden Maßnahmen nach Anhang A umzusetzen (siehe Tabelle A.2), wobei der Prozess der Risikobewertung der Informationssicherheit (siehe 6.1.2) und der Umfang der Verarbeitung von personenbezogenen Daten durch den Auftragsverarbeiter zu berücksichtigen sind. Standardmäßig sollten alle in Anhang A (siehe Tabelle A.2) aufgeführten Maßnahmen als relevant angenommen werden. Wenn die Organisation beschließt, vom Auftragsverarbeiter nicht zu verlangen, eine Maßnahme aus Anhang A (siehe Tabelle A.2) umzusetzen, sollte sie ihren Ausschluss begründen (siehe 6.1.3).

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.

B.1.2.8 Gemeinsame verantwortliche Stelle

Maßnahme

Die Organisation sollte die jeweiligen Rollen und Verantwortlichkeiten für die Verarbeitung von personenbezogenen Daten (einschließlich Datenschutz und Sicherheitsanforderungen) mit jeder gemeinsamen verantwortlichen Stelle festlegen.

Leitlinie 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 eine gemeinsame verantwortliche Stelle kann Folgendes enthalten (diese Liste ist weder endgültig noch erschöpfend):

— Zweck der gemeinsamen Nutzung von personenbezogenen Daten/Beziehung der gemeinsamen verantwortlichen Stelle;

— Identität der Organisationen (verantwortliche Stellen), die Teil der Beziehung der gemeinsamen verantwortlichen Stelle sind;

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

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

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

— 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 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 verantwortlichen Stellen bereitgestellt werden;

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

— eine Kontaktstelle für betroffene Personen.

B.1.2.9 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.

Leitlinie zur Umsetzung

Eine Möglichkeit, dokumentierte Informationen über die Verarbeitung von personenbezogenen Daten zu führen, besteht darin, über ein Inventar oder eine Liste der Verarbeitungsaktivitäten personenbezogener Daten, 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.

B.1.3 Verpflichtungen gegenüber betroffenen Personen

B.1.3.1 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.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

B.1.3.2 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.

Leitlinie 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 der hervorgeht, inwieweit und wie die Verpflichtungen ihr gegenüber erfüllt werden, sowie eine aktuelle Kontaktstelle, an die sie ihre Anfragen richten kann.

Die Kontaktstelle sollte in ähnlicher Weise angegeben werden wie bei der Erhebung von personenbezogenen Daten und Einwilligungen (z. B. wenn personenbezogene Daten per E-Mail oder über eine Website erhoben werden, sollte die Kontaktstelle per E-Mail oder über die Website angegeben werden, nicht über eine Alternative wie Telefon oder Fax).

B.1.3.3 Bestimmen von Informationen für betroffene Personen

Maßnahme

Die Organisation sollte die Informationen, die den betroffenen Personen bezüglich der Verarbeitung ihrer personenbezogenen Daten und des Zeitpunkts einer solchen Bereitstellung zur Verfügung zu stellen sind, festlegen und dokumentieren.

Leitlinie zur Umsetzung

Die Organisation sollte die gesetzlichen, behördlichen oder geschäftlichen Anforderungen festlegen, wann Informationen der betroffenen Person bereitgestellt werden sollen (z. B. vor der Verarbeitung, innerhalb einer bestimmten Zeit ab dem Zeitpunkt, zu dem sie angefordert werden) und welche Art von Informationen bereitgestellt werden sollen.

Je nach den Anforderungen können die Informationen in Form einer Mitteilung erfolgen. Beispiele für Arten von Informationen, die den betroffenen Personen zur Verfügung gestellt werden können, sind:

— Informationen über den Zweck der Verarbeitung (siehe B.1.2.2);

— Kontaktdaten für die verantwortliche Stelle oder ihrer Vertreter;

— Informationen über die rechtmäßige Grundlage für die Verarbeitung (siehe B.1.2.3);

— Informationen darüber, woher die personenbezogenen Daten bezogen wurden, wenn nicht direkt von der betroffenen Person;

— Informationen darüber, ob die Bereitstellung von personenbezogenen Daten eine gesetzliche oder vertragliche Anforderung ist, und gegebenenfalls die möglichen Folgen einer Nichtbereitstellung von personenbezogenen Daten;

— Informationen über die Verpflichtungen gegenüber betroffenen Personen, wie in B.1.3.2 festgelegt, und darüber, wie betroffene Personen davon profitieren können, insbesondere in Bezug auf den Zugang, die

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27701:2024-09

Änderung, die Berichtigung, die Beantragung der Löschung, den Erhalt einer Kopie ihrer personenbezogenen Daten und die Ablehnung der Verarbeitung;

— Informationen darüber, wie die betroffene Person ihre Einwilligung widerrufen kann (siehe B.1.3.5);

— Informationen über die Übertragung von personenbezogenen Daten;

— Informationen über Empfänger oder Kategorien von Empfängern von personenbezogenen Daten;

— Informationen über den Zeitraum, für den die personenbezogenen Daten aufbewahrt werden;

— Informationen über den Einsatz der automatisierten Entscheidungsfindung auf der Grundlage der automatisierten Verarbeitung von personenbezogenen Daten;

— Informationen über das Recht, eine Beschwerde einzureichen, und darüber, wie eine solche Beschwerde eingereicht werden kann;

— Informationen über die Häufigkeit, mit der Informationen zur Verfügung gestellt werden (z. B. JIT-Benachrichtigung (JIT, en: Just In Time), von der Organisation festgelegte Häufigkeit).

Die Organisation sollte aktualisierte Informationen bereitstellen, wenn die Zwecke für die Verarbeitung von personenbezogenen Daten geändert oder erweitert werden.

B.1.3.4 Bereitstellen von Informationen für betroffene Personen

Maßnahme

Die Organisation sollte den betroffenen Personen klare und leicht zugängliche Informationen zur Identifizierung der verantwortlichen Stelle und zur Beschreibung der Verarbeitung ihrer personenbezogenen Daten zur Verfügung stellen.

Leitlinie zur Umsetzung

Die Organisation sollte die in B.1.3.3 beschriebenen Informationen den betroffenen Personen in zeitnaher, prägnanter, vollständiger, transparenter, verständlicher und leicht zugänglicher Form und in klarer und verständlicher Sprache entsprechend der Zielgruppe zur Verfügung stellen.

Gegebenenfalls sollten die Informationen zum Zeitpunkt der Erhebung personenbezogener Daten angegeben werden. Sie sollten auch dauerhaft zugänglich sein.

ANMERKUNG Symbole und Bilder können für die betroffene Person hilfreich sein, indem sie einen visuellen Überblick über die beabsichtigte Verarbeitung geben.

B.1.3.5 Bereitstellung eines Mechanismus zur Änderung oder zum Widerruf der Einwilligung

Maßnahme

Die Organisation sollte einen Mechanismus zur Verfügung stellen, mit dem betroffene Personen ihre Einwilligung ändern oder widerrufen können.

Leitlinie zur Umsetzung

Die Organisation sollte die betroffenen Personen jederzeit über ihre Rechte in Bezug auf den Widerruf der Einwilligung (die je nach Rechtssystem unterschiedlich sein können) informieren und den Mechanismus dafür bereitstellen. Der für den Widerruf verwendete Mechanismus hängt vom Rechtssystem ab; er sollte, wenn möglich, mit den für die Einholung der Einwilligung verwendeten Mechanismen übereinstimmen. Wenn die Einwilligung beispielsweise per E-Mail oder über eine Website eingeholt wird, sollte der Mechanismus für den Widerruf der Einwilligung derselbe sein und nicht eine Alternativlösung wie Telefon oder Fax.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Die Änderung der Einwilligung kann auch Einschränkungen für die Verarbeitung von personenbezogenen Daten beinhalten, was in einigen Fällen die Einschränkung der Löschung der personenbezogenen Daten durch die verantwortliche Stelle beinhalten kann.

Einige Rechtssysteme legen Beschränkungen dafür fest, wann und wie eine betroffene Person ihre Einwilligung ändern oder widerrufen kann.

Die Organisation sollte jeden Antrag auf Widerruf oder Änderung der Einwilligung in ähnlicher Weise wie die Aufzeichnung der Einwilligung selbst aufzeichnen.

Jede Änderung der Einwilligung sollte über geeignete Systeme an autorisierte Benutzer und an relevante Dritte weitergegeben werden.

Die Organisation sollte eine Reaktionszeit festlegen, und Anfragen sollten dementsprechend behandelt werden.

Zusätzliche Informationen

Wenn die Einwilligung für eine bestimmte Verarbeitung von personenbezogenen Daten widerrufen wird, sollte üblicherweise die gesamte Verarbeitung von personenbezogenen Daten, die vor dem Widerruf durchgeführt wurde, als angemessen betrachtet werden, aber die Ergebnisse einer solchen Verarbeitung sollten nicht für eine neue Verarbeitung verwendet werden. Wenn beispielsweise eine betroffene Person ihre Einwilligung zur Profilerstellung widerruft, sollte ihr Profil nicht weiter verwendet oder konsultiert werden.

B.1.3.6 Bereitstellung eines Mechanismus zur Ablehnung der Verarbeitung personenbezogener Daten

Maßnahme

Die Organisation sollte einen Mechanismus zur Verfügung stellen, mit dem betroffene Personen die Verarbeitung ihrer personenbezogenen Daten ablehnen können.

Leitlinie zur Umsetzung

Einige Rechtssysteme räumen den betroffenen Personen das Recht ein, die Verarbeitung ihrer personenbezogenen Daten abzulehnen. Organisationen, die den Gesetzen oder den Vorschriften solcher Rechtssysteme unterliegen, sollten sicherstellen, dass sie Aufzeichnungen über betroffene Personen führen, die dieses Recht auszuüben.

Die Organisation sollte die rechtlichen und behördlichen Anforderungen in Bezug auf Einwände der betroffenen Personen gegen die Verarbeitung dokumentieren (z. B. Ablehnung in Bezug auf die Verarbeitung von personenbezogenen Daten für Direktmarketingzwecke). Die Organisation sollte den Betroffenen Informationen über die Möglichkeit, in solchen Situationen Einspruch einzulegen, zur Verfügung stellen. Die Mechanismen zum Einspruch können unterschiedlich sein, sollten aber mit der Art des angebotenen Dienstes konsistent sein (z. B. sollten Online-Dienste diese Möglichkeit online zur Verfügung stellen).

B.1.3.7 Zugriff, Korrektur oder Löschung

Maßnahme

Die Organisation sollte Richtlinien, Verfahren oder Mechanismen umsetzen, um ihren Verpflichtungen gegenüber den betroffenen Personen nachzukommen, auf ihre personenbezogenen Daten zuzugreifen, sie zu korrigieren oder zu löschen.

Leitlinie zur Umsetzung

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Die Organisation sollte Richtlinien, Verfahren oder Mechanismen umsetzen, die es den betroffenen Personen ermöglichen, Zugang zu ihren personenbezogenen Daten zu erhalten, sie zu korrigieren und zu löschen, falls dies verlangt wird und ohne unnötige Verzögerung.

Die Organisation sollte eine Reaktionszeit festlegen, und Anfragen sollten dementsprechend behandelt werden.

Alle Korrekturen oder Löschungen sollten über das System oder an autorisierte Benutzer verbreitet und an Dritte (siehe B.1.3.8) weitergegeben werden, an die die personenbezogenen Daten übertragen wurden.

ANMERKUNG Dokumentierte Informationen, die von der in B.1.5.4 festgelegten Maßnahme erzeugt werden, können in dieser Hinsicht hilfreich sein.

Die Organisation sollte Richtlinien, Verfahren oder Mechanismen für den Gebrauch umsetzen, wenn es zu einem Streit über die Genauigkeit oder Korrektur der Daten durch die betroffene Person kommen kann. Zu diesen Richtlinien, Verfahren oder Mechanismen sollte es gehören, die betroffene Person darüber zu informieren, welche Änderungen vorgenommen wurden und aus welchen Gründen keine Korrekturen vorgenommen werden können (sofern dies der Fall ist).

Einige Rechtssysteme legen Beschränkungen dafür fest, wann und wie eine betroffene Person die Berichtigung oder Löschung ihrer personenbezogenen Daten beantragen kann. Die Organisation sollte diese Einschränkungen als anwendbar festlegen und sich darüber auf dem Laufenden halten.

B.1.3.8 Verpflichtungen von verantwortlichen Stellen, Dritte zu informieren

Maßnahme

Die Organisation sollte Dritte, mit denen personenbezogene Daten geteilt wurden, über jede Änderung, jeden Widerruf oder Ablehnungen bezüglich der geteilten personenbezogenen Daten informieren und entsprechende Richtlinien, Verfahren oder Mechanismen umsetzen.

Leitlinie zur Umsetzung

Die Organisation sollte unter Berücksichtigung der verfügbaren Technologie geeignete Schritte unternehmen, um Dritte über jede Änderung oder jeden Widerruf der Einwilligung oder über Ablehnungen bezüglich der gemeinsamen personenbezogenen Daten zu informieren.

ANMERKUNG 1 Es können gesetzliche Anforderungen gelten.

Die Organisation sollte aktive Kommunikationskanäle mit Dritten festlegen und aufrechterhalten. Zusammenhängende Verantwortlichkeiten können den Personen zugewiesen werden, die für ihren Betrieb und ihre Instandhaltung verantwortlich sind. Wenn Dritte informiert werden, sollte die Organisation deren Empfangsbestätigung über den Erhalt der Informationen überwachen.

ANMERKUNG 2 Änderungen, die sich aus den Verpflichtungen gegenüber den betroffenen Personen ergeben, können eine Änderung oder einen Widerruf der Einwilligung, Anträge auf Berichtigung, Löschung oder Einschränkungen der Verarbeitung oder Einwände gegen die Verarbeitung von personenbezogenen Daten auf Antrag der betroffenen Person umfassen.

B.1.3.9 Bereitstellung einer Kopie der verarbeiteten personenbezogenen Daten

Maßnahme

Die Organisation sollte in der Lage sein, eine Kopie der personenbezogenen Daten, die auf Anfrage der betroffenen Person verarbeitet werden, zur Verfügung zu stellen.

Leitlinie zur Umsetzung

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

Die Organisation sollte eine Kopie der personenbezogenen Daten zur Verfügung stellen, die in einem strukturierten, gebräuchlichen und für die betroffene Person zugänglichen Format verarbeitet wird.

Einige Rechtssysteme definieren Fälle, in denen die Organisation eine Kopie der verarbeiteten personenbezogenen Daten in einem Format zur Verfügung stellen sollte, das die Übertragbarkeit auf die betroffenen Personen oder auf die empfangenden verantwortlichen Stellen ermöglicht (typischerweise strukturiert, gebräuchlich und maschinenlesbar).

Die Organisation sollte sicherstellen, dass alle Kopien von personenbezogenen Daten, die einer betroffenen Person zur Verfügung gestellt werden, sich speziell auf diese betroffene Person beziehen.

Wenn die angeforderten personenbezogenen Daten vorbehaltlich der Richtlinie zur Aufbewahrung und Entsorgung (wie in B.1.4.8 beschrieben) bereits gelöscht wurden, sollte die verantwortliche Stelle die betroffene Person darüber informieren, dass die angeforderten personenbezogenen Daten gelöscht wurden.

In Fällen, in denen die Organisation nicht mehr in der Lage ist, die betroffene Person zu ermitteln (z. B. als Ergebnis eines Entpersonalisierungsprozesses), sollte die Organisation nicht versuchen, die betroffenen Personen allein aus dem Grund der Umsetzung dieser Maßnahme (erneut) zu ermitteln. In einigen Rechtssystemen kann durch rechtmäßige Anfragen jedoch verlangt werden, dass zusätzliche Informationen von der betroffenen Person angefordert werden, um eine erneute Identifizierung und anschließende Offenlegung zu ermöglichen.

Wo dies technisch machbar ist, sollte die Übertragung einer Kopie der personenbezogenen Daten von einer Organisation direkt an eine andere Organisation möglich sein, wenn die betroffene Person dies wünscht.

B.1.3.10 Handhabung von Anfragen

Maßnahme

Die Organisation sollte Richtlinien und Verfahren für die Handhabung von und Reaktion auf rechtmäßige(n) Anfragen betroffener Personen definieren und dokumentieren.

Leitlinie zur Umsetzung

Zu den berechtigten Anfragen können Anfragen für eine Kopie der verarbeiteten personenbezogenen Daten oder Anfragen für die Einreichung einer Beschwerde gehören.

Einige Rechtssysteme erlauben es der Organisation, in bestimmten Fällen (z. B. bei übermäßigen oder wiederholten Anfragen) eine Gebühr zu erheben.

Anfragen sollten innerhalb der angemessen definierten Antwortzeiten bearbeitet werden.

Einige Rechtssysteme definieren Antwortzeiten, die von der Komplexität und Anzahl der Anfragen abhängen, sowie Anforderungen, die betroffenen Personen über jede Verzögerung zu informieren. Die entsprechenden Reaktionszeiten sollten in der Datenschutzrichtlinie definiert werden.

B.1.3.11 Automatisierte Entscheidungsfindung

Maßnahme

Die Organisation sollte Verpflichtungen, einschließlich rechtlicher Verpflichtungen, gegenüber den betroffenen Personen identifizieren und ansprechen, die sich aus Entscheidungen der Organisation ergeben, die sich auf die betroffene Person beziehen und ausschließlich auf der automatischen Verarbeitung von personenbezogenen Daten beruhen.

Leitlinie zur Umsetzung

Einige Rechtssysteme definieren spezifische Verpflichtungen gegenüber betroffenen Personen, wenn eine Entscheidung, die ausschließlich auf der automatisierten Verarbeitung von personenbezogenen Daten beruht, sie

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09

erheblich beeinträchtigt, wie z. B. die Benachrichtigung über eine vorhandene automatisierte Entscheidungsfindung, die es den betroffenen Personen ermöglicht, gegen eine solche Entscheidungsfindung Einspruch zu erheben, oder die Erwirkung menschlichen Eingreifens.

ANMERKUNG In einigen Rechtssystemen kann die Verarbeitung von personenbezogenen Daten nicht vollständig automatisiert werden.

Organisationen, die in diesen Rechtssystemen tätig sind, sollten die Einhaltung dieser Verpflichtungen berücksichtigen.

B.1.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

B.1.4.1 Zielsetzung

Sicherstellen, dass Prozesse und Systeme so gestaltet sind, dass die Erhebung und Verarbeitung von personenbezogenen Daten (einschließlich Nutzung, Offenlegung, Aufbewahrung, Übertragung und Entsorgung) auf das für den ermittelten Zweck erforderliche Maß beschränkt sind.

B.1.4.2 Beschränkte Erhebung

Maßnahme

Die Organisation sollte die Erhebung von personenbezogenen Daten auf das Minimum beschränken, das für die ermittelten Zwecke relevant, verhältnismäßig und notwendig ist.

Leitlinie zur Umsetzung

Die Organisation sollte die Erhebung von personenbezogenen Daten auf das beschränken, was in Bezug auf die ermittelten Zwecke angemessen, relevant und notwendig ist. Dazu gehört die Begrenzung der Menge an personenbezogenen Daten, die die Organisation indirekt (z. B. über Weblogs, Systemprotokolle) erhebt.

Datenschutz durch datenschutzfreundliche Voreinstellungen bedeutet, dass bei bestehender Optionalität in der Erhebung und Verarbeitung von personenbezogenen Daten jede Option standardmäßig deaktiviert und nur durch ausdrückliche Wahl der betroffenen Person aktiviert werden sollte.

B.1.4.3 Beschränkte Verarbeitung

Maßnahme

Die Organisation sollte die Verarbeitung von personenbezogenen Daten auf das beschränken, was für die ermittelten Zwecke angemessen, relevant und notwendig ist.

Leitlinie zur Umsetzung

Die beschränkte Verarbeitung von personenbezogenen Daten sollte durch Informationssicherheits- und Datenschutzrichtlinien (siehe 5.2) zusammen mit dokumentierten Verfahren für deren Annahme und Einhaltung gehandhabt werden.

Die Verarbeitung von personenbezogenen Daten, einschließlich:

— der Datenoffenlegung;

— des Zeitraums der Speicherung personenbezogener Daten; und

— wer in der Lage ist, auf die personenbezogenen Daten zuzugreifen;

sollte standardmäßig auf das im Verhältnis zu den ermittelten Zwecken erforderliche Minimum beschränkt werden.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27701:2024-09