

E DIN EN ISO/IEC 27701:2024-09 (D/E)

Erscheinungsdatum: 2024-08-23

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

Inhalt	Seite
Europäisches Vorwort.....	8
Vorwort.....	9
Einleitung.....	10
1 Anwendungsbereich.....	11
2 Normative Verweisungen.....	11
3 Begriffe und Abkürzungen.....	11
4 Kontext der Organisation.....	15
4.1 Verstehen der Organisation und ihres Kontextes.....	15
4.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien.....	16
4.3 Festlegung des Anwendungsbereichs des Managementsystems für Datenschutzinformationen.....	17
4.4 Managementsystem für Datenschutzinformationen.....	17
5 Führung.....	17
5.1 Führung und Verpflichtung.....	17
5.2 Datenschutzrichtlinie.....	18
5.3 Rollen, Verantwortlichkeiten und Befugnisse.....	18
6 Planung.....	18
6.1 Aktionen zum Umgang mit Risiken und Chancen.....	18
6.1.1 Allgemeines.....	18
6.1.2 Datenschutz-Folgenabschätzung.....	19
6.1.3 Datenschutz-Risikobehandlung.....	20
6.2 Datenschutzziele und Planung zu deren Erreichung.....	21
6.3 Planung von Änderungen.....	21
7 Unterstützung.....	21
7.1 Ressourcen.....	21
7.2 Kompetenz.....	22
7.3 Bewusstsein.....	22
7.4 Kommunikation.....	22
7.5 Dokumentierte Information.....	22
7.5.1 Allgemeines.....	22
7.5.2 Erstellen und Aktualisieren dokumentierter Informationen.....	23
7.5.3 Lenkung dokumentierter Information.....	23
8 Betrieb.....	24
8.1 Betriebliche Planung und Steuerung.....	24
8.2 Datenschutz-Risikobeurteilung.....	24
8.3 Datenschutz-Risikobehandlung.....	24

9	Bewertung der Leistung.....	24
9.1	Überwachung, Messung, Analyse und Bewertung.....	24
9.2	Internes Audit.....	25
9.2.1	Allgemeines.....	25
9.2.2	Internes Auditprogramm.....	25
9.3	Managementbewertung.....	25
9.3.1	Allgemeines.....	25
9.3.2	Eingaben für die Managementbewertung.....	25
9.3.3	Ergebnisse der Managementbewertung.....	26
10	Verbesserung.....	26
10.1	Fortlaufende Verbesserung.....	26
10.2	Nichtkonformität und Korrekturmaßnahmen.....	26
11	Weitere Informationen zu Anhängen.....	27
Anhang A (normativ) PIMS-Referenzmaßnahmenziele und -Maßnahmen für verantwortliche Stellen und Auftragsverarbeiter.....		28
Anhang B (normativ) Leitlinie zur Umsetzung für verantwortliche Stellen und Auftragsverarbeiter.....		40
B.1	Leitlinie zur Umsetzung für verantwortliche Stellen.....	40
B.1.1	Allgemeines.....	40
B.1.2	Bedingungen für die Erhebung und Verarbeitung.....	40
B.1.3	Verpflichtungen gegenüber betroffenen Personen.....	45
B.1.4	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen.....	51
B.1.5	Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten.....	54
B.2	Leitlinie zur Umsetzung für Auftragsverarbeiter.....	56
B.2.1	Allgemeines.....	56
B.2.2	Bedingungen für die Erhebung und Verarbeitung.....	56
B.2.3	Verpflichtungen gegenüber betroffenen Personen.....	58
B.2.4	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen.....	59
B.2.5	Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten.....	60
B.3	Leitlinie zur Umsetzung für verantwortliche Stellen und Auftragsverarbeiter.....	64
B.3.1	Zielsetzung.....	64
B.3.2	Allgemeines.....	64
B.3.3	Richtlinien für die Informationssicherheit.....	64
B.3.4	Informationssicherheitsrollen und -verantwortlichkeiten.....	65
B.3.5	Klassifizierung von Informationen.....	65
B.3.6	Kennzeichnung von Informationen.....	66
B.3.7	Informationsübertragung.....	66
B.3.8	Identitätsmanagement.....	66
B.3.9	Zugangsrechte.....	67
B.3.10	Behandlung von Informationssicherheit in Lieferantenvereinbarungen.....	67
B.3.11	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen.....	68
B.3.12	Reaktion auf Informationssicherheitsvorfälle.....	68
B.3.13	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen.....	70
B.3.14	Schutz von Aufzeichnungen.....	71
B.3.15	Unabhängige Überprüfung der Informationssicherheit.....	71
B.3.16	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit.....	71
B.3.17	Informationssicherheitsbewusstsein, -ausbildung und -schulung.....	72
B.3.18	Vertraulichkeits- oder Geheimhaltungsvereinbarungen.....	72
B.3.19	Aufgeräumte Arbeitsumgebung und Bildschirmsperren.....	72
B.3.20	Speichermedien.....	73
B.3.21	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln.....	73
B.3.22	Endpunktgeräte des Benutzers.....	74
B.3.23	Sichere Authentifizierung.....	74
B.3.24	Sicherung von Informationen.....	74
B.3.25	Protokollierung.....	75
B.3.26	Verwendung von Kryptographie.....	76

B.3.27 Lebenszyklus einer sicheren Entwicklung.....	76
B.3.28 Anforderungen an die Anwendungssicherheit.....	77
B.3.29 Sichere Systemarchitektur und technische Grundsätze.....	77
B.3.30 Ausgegliederte Entwicklung.....	78
B.3.31 Prüfinformationen.....	78
Anhang C (informativ) Zuordnung zu ISO/IEC 29100.....	79
Anhang D (informativ) Zuordnung zur Datenschutz-Grundverordnung.....	82
Anhang E (informativ) Zuordnung zu ISO/IEC 27018 und ISO/IEC 29151.....	86
Anhang F (informativ) Übereinstimmung mit ISO/IEC 27701:2019.....	89
Literaturhinweise.....	98

Tabellen

Tabelle A.1 — Maßnahmenziele und Maßnahmen für verantwortliche Stellen.....	28
Tabelle A.2 — Maßnahmenziele und Maßnahmen für Auftragsverarbeiter.....	31
Tabelle A.3 — Maßnahmenziele und Maßnahmen für verantwortliche Stellen und Auftragsverarbeiter.....	34
Tabelle C.1 — Zuordnung von Maßnahmen für verantwortliche Stellen und ISO/IEC 29100.....	79
Tabelle C.2 — Zuordnung von Maßnahmen für Auftragsverarbeiter und ISO/IEC 29100.....	80
Tabelle D.1 — Zuordnung der Struktur von ISO/IEC 27701 auf die Artikel der DSGVO.....	82
Tabelle E.1 — Zuordnung der ISO/IEC 27701 auf ISO/IEC 27018 und ISO/IEC 29151.....	86
Tabelle F.1 — Übereinstimmung zwischen Maßnahmen in diesem Dokument und Maßnahmen in ISO/IEC 27701:2019.....	89
Tabelle F.2 — Übereinstimmung zwischen Maßnahmen in ISO/IEC 27701:2019 und Maßnahmen in diesem Dokument.....	93