DIN EN ISO/IEC 27701:2026-02 (D)

Informationssicherheit, Cybersicherheit und Datenschutz - Datenschutz-Managementsysteme - Anforderungen und Hinweise (ISO/IEC 27701:2025); Deutsche Fassung EN ISO/IEC 27701:2025

Inhalt

Seite

Europäisches Vorwort 7
Vorwort 8
Einleitung 9
1 Anwendungsbereich 10
2 Normative Verweisungen 10
3 Begriffe und Abkürzungen 10
4 Kontext der Organisation 14
4.1 Verstehen der Organisation und ihres Kontextes 14
4.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien 15
4.3 Festlegung des Anwendungsbereichs des Datenschutz-Managementsystems 15
4.4 Datenschutz-Managementsystem 16
5 Führung 16
5.1 Führung und Verpflichtung 16
5.2 Datenschutzpolitik 17
5.3 Rollen, Verantwortlichkeiten und Befugnisse 17
6 Planung 17
6.1 Maßnahmen zum Umgang mit Risiken und Chancen 17
6.1.1 Allgemeines 17
6.1.2 Datenschutz-Risikobeurteilung 18
6.1.3 Datenschutz-Risikobehandlung 19
6.2 Datenschutzziele und Planung zu deren Erreichung 20
6.3 Planung von Änderungen 21
7 Unterstützung 21
7.1 Ressourcen 21
7.2 Kompetenz 21
7.3 Bewusstsein 21
7.4 Kommunikation 22
7.5 Dokumentierte Information 22
7.5.1 Allgemeines 22
7.5.2 Erstellen und Aktualisieren dokumentierter Information 22
7.5.3 Lenkung dokumentierter Information 23
8 Betrieb 23
8.1 Betriebliche Planung und Steuerung 23
8.2 Datenschutz-Risikobeurteilung 23
8.3 Datenschutz-Risikobehandlung 24
9 Leistungsbewertung 24
9.1 Überwachung, Messung, Analyse und Bewertung 24
9.2 Internes Audit 24
9.2.1 Allgemeines 24
9.2.2 Internes Auditprogramm 24
9.3 Managementbewertung 25

9.3.1 Allgemeines ... 25
9.3.2 Eingaben für die Managementbewertung ... 25
9.3.3 Ergebnisse der Managementbewertung ... 25

10 Verbesserung ... 26
10.1 Fortlaufende Verbesserung ... 26
10.2 Nichtkonformität und Korrekturmaßnahmen ... 26

11 Weitere Informationen zu Anhängen ... 26

Anhang A (normativ) DSMS-Referenzmaßnahmenziele und -Maßnahmen für verantwortliche Stellen und Auftragsverarbeiter ... 27

Anhang B (normativ) Hinweis zur Umsetzung für verantwortliche Stellen und Auftragsverarbeiter ... 39
B.1 Hinweis zur Umsetzung für verantwortliche Stellen ... 39
B.1.1 Allgemeines ... 39
B.1.2 Bedingungen für die Erhebung und Verarbeitung ... 39
B.1.3 Verpflichtungen gegenüber betroffenen Personen ... 44
B.1.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen ... 50
B.1.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten ... 53
B.2 Hinweis zur Umsetzung für Auftragsverarbeiter ... 55
B.2.1 Allgemeines ... 55
B.2.2 Bedingungen für die Erhebung und Verarbeitung ... 55
B.2.3 Verpflichtungen gegenüber betroffenen Personen ... 57
B.2.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen ... 58
B.2.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten ... 60
B.3 Hinweis zur Umsetzung für verantwortliche Stellen und Auftragsverarbeiter ... 63
B.3.1 Zielsetzung ... 63
B.3.2 Allgemeines ... 63
B.3.3 Informationssicherheitspolitik und -richtlinien ... 63
B.3.4 Informationssicherheitsrollen und -verantwortlichkeiten ... 64
B.3.5 Klassifizierung von Informationen ... 65
B.3.6 Kennzeichnung von Informationen ... 65
B.3.7 Informationsübermittlung ... 65
B.3.8 Identitätsmanagement ... 65
B.3.9 Zugangsrechte ... 66
B.3.10 Behandlung von Informationssicherheit in Lieferantenvereinbarungen ... 66
B.3.11 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen ... 67
B.3.12 Reaktion auf Informationssicherheitsvorfälle ... 67
B.3.13 Juristische, gesetzliche, regulatorische und vertragliche Anforderungen ... 69
B.3.14 Schutz von Aufzeichnungen ... 70
B.3.15 Unabhängige Überprüfung der Informationssicherheit ... 70
B.3.16 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit ... 71
B.3.17 Informationssicherheitsbewusstsein, -ausbildung und -schulung ... 71
B.3.18 Vertraulichkeits- oder Geheimhaltungsvereinbarungen ... 71
B.3.19 Aufgeräumte Arbeitsumgebung und Bildschirmsperren ... 72
B.3.20 Speichermedien ... 72
B.3.21 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln ... 73
B.3.22 Endpunktgeräte des Benutzers ... 73
B.3.23 Sichere Authentifizierung ... 73
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 Entwicklungsgrundsätze ... 77
B.3.30 Ausgegliederte Entwicklung ... 77
B.3.31 Testdaten ... 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 **27**

Tabelle A.2 — Maßnahmenziele und Maßnahmen für Auftragsverarbeiter **31**

Tabelle A.3 — Maßnahmenziele und Maßnahmen für verantwortliche Stellen und Auftragsverarbeiter **33**

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 dieses Dokuments zu den Artikeln der DSGVO **82**

Tabelle E.1 — Zuordnung von ISO/IEC 27701 zu 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 **92**