

DIN EN ISO/IEC 27701:2021-07 (D)

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

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

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

7.2.4	Einholung und Aufzeichnung der Einwilligung	42
7.2.5	Datenschutz-Folgenabschätzung.....	42
7.2.6	Verträge mit Auftragsverarbeitern	43
7.2.7	Gemeinsame verantwortliche Stelle	43
7.2.8	Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten	44
7.3	Verpflichtungen gegenüber betroffenen Personen.....	45
7.3.1	Bestimmung und Erfüllung von Verpflichtungen gegenüber betroffenen Personen.....	45
7.3.2	Bestimmen von Informationen für betroffene Personen.....	46
7.3.3	Bereitstellen von Informationen für betroffene Personen.....	47
7.3.4	Bereitstellung eines Mechanismus zur Änderung oder zum Widerruf der Einwilligung	47
7.3.5	Bereitstellung eines Mechanismus zur Ablehnung der Verarbeitung personenbezogener Daten	48
7.3.6	Zugriff, Korrektur und/oder Löschung	48
7.3.7	Verpflichtungen von verantwortlichen Stellen, Dritte zu informieren	49
7.3.8	Bereitstellung einer Kopie der verarbeiteten personenbezogenen Daten	49
7.3.9	Handhabung von Anfragen.....	50
7.3.10	Automatisierte Entscheidungsfindung.....	50
7.4	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen.....	51
7.4.1	Beschränkte Erhebung	51
7.4.2	Beschränkte Verarbeitung	51
7.4.3	Genauigkeit und Qualität.....	51
7.4.4	Ziele der Sparsamkeit personenbezogener Daten	52
7.4.5	Entpersonalisierung personenbezogener Daten und Löschung am Ende der Verarbeitung.....	53
7.4.6	Temporäre Dateien.....	53
7.4.7	Aufbewahrung.....	53
7.4.8	Entsorgung.....	54
7.4.9	Maßnahmen zur Übertragung personenbezogener Daten	54
7.5	Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten	54
7.5.1	Ermittlung der Grundlage für die Übertragung von personenbezogenen Daten zwischen Rechtssystemen	54
7.5.2	Länder und internationale Organisationen, an die personenbezogene Daten übertragen werden können	55
7.5.3	Aufzeichnungen über die Übertragung von personenbezogenen Daten.....	55
7.5.4	Aufzeichnungen der Offenlegung von personenbezogenen Daten für Dritte	55
8	Zusätzliche Leitlinie für Auftragsverarbeiter nach ISO/IEC 27002	56
8.1	Allgemeines.....	56
8.2	Bedingungen für die Erhebung und Verarbeitung	56
8.2.1	Kundenvereinbarung.....	56
8.2.2	Ziele der Organisation	57
8.2.3	Verwendung für Marketing und Werbung.....	57
8.2.4	Verstoßende Anweisung.....	57
8.2.5	Kundenverpflichtungen	58
8.2.6	Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten	58
8.3	Verpflichtungen gegenüber betroffenen Personen.....	58
8.3.1	Verpflichtungen gegenüber betroffenen Personen.....	58
8.4	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen.....	59
8.4.1	Temporäre Dateien.....	59
8.4.2	Rückgabe, Übertragung oder Entsorgung von personenbezogenen Daten.....	59
8.4.3	Maßnahmen zur Übertragung personenbezogener Daten	60
8.5	Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten	60
8.5.1	Grundlage für die Übertragung von personenbezogenen Daten zwischen Rechtssystemen	60
8.5.2	Länder und internationale Organisationen, an die personenbezogene Daten übertragen werden können	61

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