E DIN EN ISO/IEC 27701:2021-01 (D/E)

Erscheinungsdatum: 2020-12-11

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

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

Inhalt

Seite

Europäisches Vorwort 6

Vorwort 7

Einleitung 8

1 Anwendungsbereich 10

2 Normative Verweisungen 10

3 Begriffe 10

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

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

5.7.3 Managementbewertung 18
5.8 Verbesserung 18
5.8.1 Nichtkonformität und Korrekturmaßnahmen 18
5.8.2 Fortlaufende Verbesserung 18

6 PIMS-spezifische Anleitungen in Bezug auf ISO/IEC 27002 18
6.1 Allgemeines 18
6.2 Informationssicherheitsrichtlinien 18
6.2.1 Vorgaben der Leitung für Informationssicherheit 18
6.3 Organisation der Informationssicherheit 19
6.3.1 Interne Organisation 19
6.3.2 Mobilgeräte und Telearbeit 20
6.4 Personalsicherheit 20
6.4.1 Vor Beginn eines Anstellungsverhältnisses 20
6.4.2 Während des Anstellungsverhältnisses 21
6.4.3 Beendigung und Änderung des Anstellungsverhältnisses 21
6.5 Verwaltung der Werte 21
6.5.1 Verantwortlichkeit für Werte 21
6.5.2 Informationsklassifizierung 22
6.5.3 Handhabung von Datenträgern 22
6.6 Zugangssteuerung 24
6.6.1 Geschäftsanforderungen an die Zugangsteuerung 24
6.6.2 Benutzerzugangsverwaltung 24
6.6.3 Benutzerverantwortlichkeiten 25
6.6.4 Zugangssteuerung für Systeme und Anwendungen 25
6.7 Kryptographie 26
6.7.1 Kryptographische Maßnahmen 26
6.8 Physische und umgebungsbezogene Sicherheit 26
6.8.1 Sicherheitsbereiche 26
6.8.2 Einrichtung 27
6.9 Betriebssicherheit 28
6.9.1 Betriebsabläufe und -verantwortlichkeiten 28
6.9.2 Schutz vor Schadsoftware 29
6.9.3 Datensicherung 29
6.9.4 Protokollierung und Überwachung 30
6.9.5 Steuerung von Software im Betrieb 31
6.9.6 Handhabung technischer Schwachstellen 31
6.9.7 Überlegungen für Audits von Informationssystemen 31
6.10 Kommunikationssicherheit 31
6.10.1 Netzwerksicherheitsmanagement 31
6.10.2 Informationsübertragung 32
6.11 Anschaffung, Entwicklung und Instandhaltung von Systemen 32
6.11.1 Sicherheitsanforderungen an Informationssysteme 32
6.11.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen 33
6.11.3 Testdaten 35
6.12 Lieferantenbeziehungen 35
6.12.1 Informationssicherheit in Lieferantenbeziehungen 35
6.12.2 Steuerung der Dienstleistungserbringung von Lieferanten 36
6.13 Handhabung von Informationssicherheitsvorfällen 36
6.13.1 Handhabung von Informationssicherheitsvorfällen und -verbesserungen 36
6.14 Informationssicherheitsaspekte beim Business Continuity Management 39
6.14.1 Aufrechterhalten der Informationssicherheit 39
6.14.2 Redundanzen 39
6.15 Einhaltung 39
6.15.1 Einhaltung gesetzlicher und vertraglicher Anforderungen 39
6.15.2 Überprüfungen der Informationssicherheit 40

7 Zusätzliche Anleitung für PII-Beauftragte nach ISO/IEC 27002 41
7.1 Allgemeines 41

7.2 Bedingungen für die Erhebung und Verarbeitung 41
7.2.1 Identifizieren und Dokumentieren des Zwecks 41
7.2.2 Identifizieren der rechtmäßigen Grundlage 42
7.2.3 Bestimmen, wann und wie die Einwilligung einzuholen ist 43
7.2.4 Einholung und Aufzeichnung der Einwilligung 43
7.2.5 Datenschutz-Folgenabschätzung 44
7.2.6 Verträge mit PII-Verarbeitern 44
7.2.7 Gemeinsamer PII-Beauftragter 45
7.2.8 Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten 46
7.3 Verpflichtungen gegenüber betroffenen Personen 46
7.3.1 Bestimmung und Erfüllung von Verpflichtungen gegenüber betroffenen Personen 46
7.3.2 Bestimmen von Informationen für betroffene Personen 47
7.3.3 Bereitstellen von Informationen für betroffene Personen 48
7.3.4 Bereitstellung eines Mechanismus zur Änderung oder zum Widerruf der Einwilligung 48
7.3.5 Bereitstellung eines Mechanismus zur Ablehnung der PII-Verarbeitung 49
7.3.6 Zugriff, Korrektur und/oder Löschung 49
7.3.7 Verpflichtungen von PII-Beauftragten, Dritte zu informieren 50
7.3.8 Bereitstellung einer Kopie der verarbeiteten personenbezogenen Daten 50
7.3.9 Handhabung von Anfragen 51
7.3.10 Automatisierte Entscheidungsfindung 51
7.4 Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen 52
7.4.1 Beschränkte Erhebung 52
7.4.2 Beschränkte Verarbeitung 52
7.4.3 Genauigkeit und Qualität 53
7.4.4 Ziele der Sparsamkeit personenbezogener Daten 53
7.4.5 Entpersonalisierung personenbezogener Daten und Löschung am Ende der Verarbeitung 54
7.4.6 Temporäre Dateien 54
7.4.7 Aufbewahrung 54
7.4.8 Entsorgung 55
7.4.9 Maßnahmen zur Übertragung personenbezogener Daten 55
7.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten 55
7.5.1 Ermittlung der Grundlage für die Übertragung von personenbezogenen Daten zwischen Rechtssystemen 56
7.5.2 Länder und internationale Organisationen, an die personenbezogene Daten übertragen werden können 56
7.5.3 Aufzeichnungen über die Übertragung von personenbezogenen Daten 56
7.5.4 Aufzeichnungen der Offenlegung von personenbezogenen Daten für Dritte 57

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

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

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

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

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

Anhang D (informativ) Zuordnung zur Datenschutz-Grundverordnung 76

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

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

Literaturhinweise 85