

DIN EN ISO/IEC 29151:2022-07 (D)

Informationstechnik - Sicherheitsverfahren - Leitfaden für den Schutz
personenbezogener Daten (ISO/IEC 29151:2017); Deutsche Fassung EN ISO/IEC
29151:2022

Inhalt	Seite
Europäisches Vorwort.....	7
Vorwort	8
Einleitung	9
1 Anwendungsbereich.....	12
2 Normative Verweisungen	12
3 Begriffe und Abkürzungen	12
3.1 Begriffe	12
3.2 Abkürzungen	13
4 Übersicht.....	13
4.1 Ziele des Schutzes von pbD	13
4.2 Anforderung an den Schutz von pbD.....	13
4.3 Maßnahmen	14
4.4 Auswahl von Maßnahmen	14
4.5 Entwicklung organisationsspezifischer Leitfäden	15
4.6 Erwägungen zur Lebensdauer.....	15
4.7 Aufbau dieser Spezifikation.....	15
5 Sicherheitsleitlinien	16
5.1 Managementvorgaben zur Informationssicherheit.....	16
5.1.1 Einleitung.....	16
5.1.2 Informationssicherheitsleitlinien.....	16
5.1.3 Überprüfung der Informationssicherheitsrichtlinien.....	16
6 Organisation der Informationssicherheit	16
6.1 Interne Organisation	16
6.1.1 Einleitung.....	16
6.1.2 Informationssicherheitsrollen und -verantwortlichkeiten.....	16
6.1.3 Aufgabentrennung	17
6.1.4 Kontakt mit Behörden	18
6.1.5 Kontakt mit speziellen Interessensgruppen	18
6.1.6 Informationssicherheit im Projektmanagement	18
6.2 Mobilgeräte und Telearbeit	18
6.2.1 Einleitung.....	18
6.2.2 Richtlinie zu Mobilgeräten	18
6.2.3 Telearbeit.....	19
7 Personalsicherheit.....	19
7.1 Vor der Beschäftigung.....	19
7.1.1 Einleitung.....	19
7.1.2 Sicherheitsüberprüfung.....	19
7.1.3 Beschäftigungs- und Vertragsbedingungen.....	19
7.2 Während der Anstellung	19
7.2.1 Einleitung.....	19
7.2.2 Verantwortlichkeiten der Leitung.....	19
7.2.3 Informationssicherheits-bewusstsein, -ausbildung und -schulung.....	19

7.2.4	Maßregelungsprozess.....	19
7.3	Beendigung und Änderung der Beschäftigung	20
7.3.1	Einleitung.....	20
7.3.2	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung.....	20
8	Verwaltung der Werte	20
8.1	Verantwortlichkeit für Werte	20
8.1.1	Einleitung.....	20
8.1.2	Inventarisierung der Werte.....	20
8.1.3	Zuständigkeit für Werte.....	21
8.1.4	Zulässiger Gebrauch von Werten.....	21
8.1.5	Rückgabe von Werten.....	21
8.2	Informationsklassifizierung.....	21
8.2.1	Einleitung.....	21
8.2.2	Klassifizierung von Information	21
8.2.3	Kennzeichnung von Information	22
8.2.4	Handhabung von Werten.....	22
8.3	Handhabung von Datenträgern	22
8.3.1	Einleitung.....	22
8.3.2	Verwaltung von Wechseldatenträgern	22
8.3.3	Entsorgung von Datenträgern.....	23
8.3.4	Transport von Datenträgern	23
9	Zugangssteuerung.....	23
9.1	Geschäftsanforderung an die Zugangssteuerung	23
9.1.1	Einleitung.....	23
9.1.2	Zugangssteuerungsrichtlinie.....	23
9.1.3	Zugang zu Netzwerken und Netzwerkdiensten.....	23
9.2	Benutzerzugangsverwaltung.....	23
9.2.1	Einleitung.....	23
9.2.2	Registrierung und Deregistrierung von Benutzern	24
9.2.3	Zuteilung von Benutzerzugängen	24
9.2.4	Verwaltung privilegierter Zugangsrechte.....	24
9.2.5	Verwaltung geheimer Authentifizierungsdaten von Benutzern.....	24
9.2.6	Überprüfung von Benutzerzugangsrechten	24
9.2.7	Entziehung oder Anpassung von Zugangsrechten.....	25
9.3	Benutzerverantwortlichkeiten.....	25
9.3.1	Einleitung.....	25
9.3.2	Gebrauch geheimer Authentisierungsinformation.....	25
9.4	Zugangssteuerung für Systemen und Anwendungen	25
9.4.1	Einleitung.....	25
9.4.2	Informationszugangsbeschränkung	25
9.4.3	Sichere Anmeldeverfahren	25
9.4.4	System zur Verwaltung von Kennwörtern.....	26
9.4.5	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	26
9.4.6	Zugangssteuerung für Quellcode von Programmen	26
10	Kryptographie	26
10.1	Kryptographische Maßnahmen.....	26
10.1.1	Einleitung.....	26
10.1.2	Richtlinie zum Gebrauch von kryptographischen Maßnahmen	26
10.1.3	Schlüsselverwaltung	26
11	Physische und umgebungsbezogene Sicherheit.....	26
11.1	Sicherheitsbereiche.....	26
11.1.1	Einleitung.....	26
11.1.2	Physische Sicherheitsperimeter	26
11.1.3	Physische Zutrittssteuerung.....	26
11.1.4	Sicherung von Büros, Räumen und Einrichtungen.....	26
11.1.5	Schutz vor externen und umweltbedingten Bedrohungen.....	27

11.1.6	Arbeit in Sicherheitsbereichen	27
11.1.7	Anlieferungs- und Ladebereiche	27
11.2	Geräte und Betriebsmittel	27
11.2.1	Einleitung.....	27
11.2.2	Platzierung und Schutz von Geräten und Betriebsmitteln	27
11.2.3	Versorgungseinrichtungen	27
11.2.4	Sicherheit der Verkabelung.....	27
11.2.5	Instandhalten von Geräten und Betriebsmitteln.....	27
11.2.6	Entfernen von Werten.....	27
11.2.7	Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten	27
11.2.8	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	27
11.2.9	Unbeaufsichtigte Benutzergeräte	28
11.2.10	Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren.....	28
12	Betriebssicherheit.....	28
12.1	Betriebsabläufe und -verantwortlichkeiten.....	28
12.1.1	Einleitung.....	28
12.1.2	Dokumentierte Betriebsabläufe.....	28
12.1.3	Änderungssteuerung.....	28
12.1.4	Kapazitätssteuerung	28
12.1.5	Trennung von Entwicklungs-, Test- und Betriebsumgebungen.....	28
12.2	Schutz vor Schadsoftware.....	29
12.2.1	Einleitung.....	29
12.2.2	Maßnahmen gegen Schadsoftware	29
12.3	Datensicherung.....	29
12.3.1	Einleitung.....	29
12.3.2	Sicherung von Information	29
12.4	Protokollierung und Überwachung.....	29
12.4.1	Einleitung.....	29
12.4.2	Ereignisprotokollierung	29
12.4.3	Schutz der Protokollinformationen	30
12.4.4	Administratoren- und Bedienerprotokolle	30
12.4.5	Uhrensynchronisation	30
12.5	Steuerung von Software im Betrieb.....	30
12.5.1	Einleitung.....	30
12.5.2	Installation von Software auf Systemen im Betrieb.....	31
12.6	Handhabung technischer Schwachstellen.....	31
12.6.1	Einleitung.....	31
12.6.2	Handhabung von technischen Schwachstellen.....	31
12.6.3	Einschränkung von Softwareinstallation	31
12.7	Audit von Informationssystemen.....	31
12.7.1	Einleitung.....	31
12.7.2	Maßnahmen für Audits von Informationssystemen	31
13	Kommunikationssicherheit.....	31
13.1	Netzwerksicherheitsmanagement.....	31
13.1.1	Einleitung.....	31
13.1.2	Netzwerksteuerungsmaßnahmen	31
13.1.3	Sicherheit von Netzwerkdiensten.....	31
13.1.4	Trennung in Netzwerken	31
13.2	Informationsübertragung.....	32
13.2.1	Einleitung.....	32
13.2.2	Richtlinien und Verfahren für die Informationsübertragung	32
13.2.3	Vereinbarungen zum Informationstransfer	32
13.2.4	Elektronische Nachrichtenübermittlung.....	32
13.2.5	Vertraulichkeits- oder Geheimhaltungsvereinbarungen.....	32
14	Anschaffung, Entwicklung und Instandhalten von Systemen	32
14.1	Sicherheitsanforderungen für Informationssysteme.....	32

14.1.1	Einleitung.....	32
14.1.2	Analyse und Spezifikation von Informationssicherheitsanforderungen.....	32
14.1.3	Sicherung von Anwendungsdiensten in öffentlichen Netzwerken	33
14.1.4	Schutz der Transaktionen bei Anwendungsdiensten.....	33
14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen	33
14.2.1	Einleitung.....	33
14.2.2	Richtlinie für sichere Entwicklung	33
14.2.3	Verfahren zur Verwaltung von Systemänderungen.....	33
14.2.4	technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform	33
14.2.5	Beschränkung von Änderungen an Software-Paketen	33
14.2.6	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme	33
14.2.7	Sichere Entwicklungsumgebung	33
14.2.8	Ausgegliederte Entwicklung.....	34
14.2.9	Testen der Systemsicherheit	34
14.2.10	Systemabnahmetest	34
14.3	Testdaten	34
14.3.1	Einleitung.....	34
14.3.2	Schutz von Testdaten	34
15	Lieferantenbeziehungen	34
15.1	Informationssicherheit in Lieferantenbeziehungen	34
15.1.1	Einleitung.....	34
15.1.2	Informationssicherheitsrichtlinie für Lieferantenbeziehungen	34
15.1.3	Behandlung von Sicherheit in Lieferantenvereinbarungen.....	35
15.1.4	Lieferkette für Informations- und Kommunikationstechnologie.....	36
15.2	Steuerung der Dienstleistungserbringung von Lieferanten	36
15.2.1	Einleitung.....	36
15.2.2	Überwachung und Überprüfung von Lieferantendienstleistungen.....	36
15.2.3	Handhabung der Änderungen von Lieferantendienstleistungen.....	36
16	Handhabung von Informationssicherheitsvorfällen	36
16.1	Handhabung von Informationssicherheitsvorfällen und Verbesserungen.....	36
16.1.1	Einleitung.....	36
16.1.2	Verantwortlichkeiten und Verfahren	36
16.1.3	Meldung von Informationssicherheitsereignissen	37
16.1.4	Meldung von Schwächen in der Informationssicherheit.....	37
16.1.5	Beurteilung von und Entscheidung über Informationssicherheitsereignisse	38
16.1.6	Reaktion auf Informationssicherheitsvorfälle	38
16.1.7	Erkenntnisse aus Informationssicherheitsvorfällen.....	38
16.1.8	Sammeln von Beweismaterial.....	38
17	Informationssicherheitsaspekte beim Business Continuity Management.....	38
17.1	Aufrechterhalten der Informationssicherheit.....	38
17.1.1	Einleitung.....	38
17.1.2	Planung zur Aufrechterhaltung der Informationssicherheit.....	38
17.1.3	Umsetzen der Aufrecht-erhaltung der Informations-sicherheit	38
17.1.4	Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit.....	38
17.2	Redundanzen.....	38
17.2.1	Einleitung.....	38
17.2.2	Verfügbarkeit von informationsverarbeitenden Einrichtungen	38
18	Compliance.....	39
18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen	39
18.1.1	Einleitung.....	39
18.1.2	Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen	39
18.1.3	geistige Eigentumsrechte	40
18.1.4	Schutz von Aufzeichnungen	40
18.1.5	Privatsphäre und Schutz von personenbezogener Information.....	40
18.1.6	Regelungen bezüglich kryptographischer Maßnahmen	40
18.2	Überprüfungen der Informationssicherheit	40

18.2.1	Einleitung.....	40
18.2.2	unabhängige Überprüfung der Informationssicherheit.....	40
18.2.3	Einhaltung von Sicherheitsrichtlinien und -standards.....	40
18.2.4	Überprüfung der Einhaltung von technischen Vorgaben.....	40
Anhang A Erweiterter Kontrollsatz für den Datenschutz (Dieser Anhang ist integraler Bestandteil dieser Empfehlung Internationalen Norm.).....		
		41
A.1	Allgemeines.....	41
A.2	Allgemeine Leitlinien für die Nutzung und den Schutz von pbD.....	41
A.3	Einwilligung und Wahlfreiheit.....	42
A.3.1	Einwilligung	42
A.3.2	Wahl.....	44
A.4	Zulässigkeit des Zwecks und Spezifikation.....	45
A.4.1	Zulässigkeit des Zwecks	45
A.4.2	Spezifikation des Zwecks	46
A.5	Beschränkung der Erhebung.....	47
A.6	Datensparsamkeit.....	48
A.7	Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung	50
A.7.1	Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung	50
A.7.2	Sicheres Löschen temporärer Dateien	52
A.7.3	Mitteilung über die Offenlegung von pbD	52
A.7.4	Aufzeichnung der Offenlegung von pbD.....	52
A.7.5	Offenlegung der Verarbeitung von pbD durch Subunternehmer	53
A.8	Genauigkeit und Qualität.....	53
A.9	Offenheit, Transparenz und Benachrichtigung	55
A.9.1	Datenschutzmitteilung	55
A.9.2	Offenheit und Transparenz	56
A.10	Beteiligung und Zugang der betroffenen Person	57
A.10.1	Zugang der betroffenen Person	57
A.10.2	Abhilfe und Beteiligung.....	58
A.10.3	Behandlung von Beschwerden.....	59
A.11	Verantwortlichkeit	60
A.11.1	Lenkung.....	60
A.11.2	Datenschutz-Folgenabschätzung.....	61
A.11.3	Datenschutzanforderung für Auftragnehmer und Auftragsdatenverarbeiter	61
A.11.4	Überwachung und Prüfung des Datenschutzes	62
A.11.5	Datenschutzaufklärung und -schulung	63
A.11.6	Berichterstattung zum Datenschutz	63
A.12	Informationssicherheit	64
A.13	Einhaltung der Datenschutzpflichten	65
A.13.1	Compliance	65
A.13.2	Beschränkungen der grenzüberschreitenden Datenübertragung in einigen Ländern.....	65
Literaturhinweise		66