

E DIN EN ISO/IEC 29151:2025-02 (D/E)

Erscheinungsdatum: 2025-01-10

Informationstechnik - Sicherheitsverfahren - Leitfaden für den Schutz
personenbezogener Daten (ISO/IEC DIS 29151:2024); Deutsche und Englische
Fassung prEN ISO/IEC 29151:2024

Information security, cybersecurity and privacy protection - Controls and guidance
for personally identifiable information protection (ISO/IEC DIS 29151:2024); German
and English version prEN ISO/IEC 29151:2024

Inhalt	Seite
Europäisches Vorwort.....	9
Einleitung	10
1 Anwendungsbereich.....	14
2 Normative Verweisungen	14
3 Begriffe und Abkürzungen	14
3.1 Begriffe	14
3.2 Abkürzungen	15
4 Übersicht.....	16
4.1 Ziele des Schutzes von pbd	16
4.2 Anforderung an den Schutz von pbd.....	16
4.3 Maßnahmen	16
4.4 Auswahl von Maßnahmen	17
4.5 Entwicklung organisationspezifischer Leitfäden	17
4.6 Erwägungen zur Lebensdauer.....	17
4.7 Aufbau dieses Dokuments	18
5 Organisatorische Maßnahmen.....	25
5.1 Informationssicherheitsleitlinien.....	25
5.2 Informationssicherheitsrollen und -verantwortlichkeiten.....	25
5.3 Aufgabentrennung	26
5.4 Verantwortlichkeiten der Leitung.....	26
5.5 Kontakt mit Behörden	26
5.6 Kontakt mit speziellen Interessengruppen	26
5.7 Informationen über Bedrohungen	27
5.8 Informationssicherheit im Projektmanagement.....	27
5.9 Inventar der Informationen und anderen damit verbundenen Werte.....	27
5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten.....	28
5.11 Rückgabe von Werten	28
5.12 Klassifizierung von Information.....	28
5.13 Kennzeichnung von Information.....	29
5.14 Informationsübertragung.....	29
5.15 Zugangssteuerung.....	29
5.16 Identitätsmanagement	29
5.17 Informationen zur Authentifizierung.....	29
5.18 Zugangsrechte	29
5.19 Informationssicherheit in Lieferantenbeziehungen.....	30
5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen	30
5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette	31
5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	31

5.23	Informationssicherheit für die Nutzung von Cloud-Diensten.....	31
5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	31
5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse	32
5.26	Reaktion auf Informationssicherheitsvorfälle	32
5.27	Erkenntnisse aus Informationssicherheitsvorfällen.....	33
5.28	Sammeln von Beweismaterial.....	33
5.29	Informationssicherheit bei Störungen	33
5.30	IKT-Bereitschaft für Business Continuity.....	33
5.31	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	33
5.32	Geistige Eigentumsrechte	34
5.33	Schutz von Aufzeichnungen	34
5.34	Datenschutz und Schutz personenbezogener Daten (pBD).....	34
5.35	Unabhängige Überprüfung der Informationssicherheit.....	34
5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit.....	35
5.37	Dokumentierte Betriebsabläufe.....	35
6	Personenbezogene Maßnahmen.....	35
6.1	Sicherheitsüberprüfung.....	35
6.2	Beschäftigungs- und Vertragsbedingungen.....	35
6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung.....	35
6.4	Maßregelungsprozess.....	36
6.5	Verantwortlichkeiten nach Beendigung oder Änderung des Beschäftigungsverhältnisses.....	36
6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen.....	36
6.7	Telearbeit	36
6.8	Meldung von Informationssicherheitsereignissen	36
7	Physische Maßnahmen.....	37
7.1	Physische Sicherheitsperimeter	37
7.2	Physischer Zutritt.....	37
7.3	Sicherung von Büros, Räumen und Einrichtungen.....	37
7.4	Physische Sicherheitsüberwachung.....	37
7.5	Schutz vor physischen und umweltbedingten Bedrohungen	37
7.6	Arbeit in Sicherheitsbereichen.....	37
7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren.....	37
7.8	Platzierung und Schutz von Geräten und Betriebsmitteln	37
7.9	Sicherheit von Werten außerhalb der Räumlichkeiten.....	37
7.10	Speichermedien.....	37
7.11	Versorgungseinrichtungen	38
7.12	Sicherheit der Verkabelung.....	38
7.13	Instandhaltung von Geräten und Betriebsmitteln	38
7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	38
8	Technische Maßnahmen.....	39
8.1	Endpunktgeräte des Benutzers	39
8.2	Privilegierte Zugangsrechte	39
8.3	Informationszugangsbeschränkung	39
8.4	Zugriff auf den Quellcode.....	40
8.5	Sichere Authentifizierung.....	40
8.6	Kapazitätssteuerung	40
8.7	Schutz gegen Schadsoftware.....	40
8.8	Handhabung von technischen Schwachstellen.....	40
8.9	Konfigurationsmanagement.....	40
8.10	Löschung von Informationen	40
8.11	Datenmaskierung.....	40
8.12	Verhinderung von Datenlecks	40
8.13	Sicherung von Information	40
8.14	Verfügbarkeit von informationsverarbeitenden Einrichtungen	41
8.15	Protokollierung	41
8.16	Überwachung von Aktivitäten	41

8.17	Uhrensynchronisation	42
8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	42
8.19	Installation von Software auf Betriebssystemen	42
8.20	Netzwerksicherheit	42
8.21	Sicherheit von Netzwerkdiensten	42
8.22	Trennung von Netzwerken.....	42
8.23	Webfilterung	42
8.24	Verwendung von Kryptographie	42
8.25	Lebenszyklus einer sicheren Entwicklung.....	42
8.26	Anforderungen an die Anwendungssicherheit.....	42
8.27	Sichere Systemarchitektur und technische Grundsätze.....	42
8.28	Sichere Programmierung.....	43
8.29	Sicherheitsprüfung bei Entwicklung und Abnahme	43
8.30	Ausgegliederte Entwicklung	43
8.31	Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen	43
8.32	Änderungssteuerung.....	43
8.33	Prüfinformationen	43
8.34	Schutz der Informationssysteme während der Überwachungsprüfung	43
Anhang A (normativ) Erweiterter Kontrollsatz für den Datenschutz (Dieser Anhang ist integraler Bestandteil dieser Empfehlung Internationalen Norm.).....		
A.1	Allgemeines	44
A.2	Allgemeine Leitlinien für die Nutzung und den Schutz von pbD.....	44
A.3	Einwilligung und Wahlfreiheit.....	45
A.3.1	Einwilligung	45
A.3.2	Wahl.....	47
A.4	Zulässigkeit des Zwecks und Spezifikation.....	48
A.4.1	Zulässigkeit des Zwecks.....	48
A.4.2	Spezifikation des Zwecks Maßnahme.....	49
A.5	Beschränkung der Erhebung.....	50
A.6	Datensparsamkeit.....	51
A.7	Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung	52
A.7.1	Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung	52
A.7.2	Sicheres Löschen temporärer Dateien	54
A.7.3	Mitteilung über die Offenlegung von pbD	55
A.7.4	Aufzeichnung der Offenlegung von pbD.....	55
A.7.5	Offenlegung der Verarbeitung von pbD durch Subunternehmer	56
A.8	Genauigkeit und Qualität.....	56
A.9	Offenheit, Transparenz und Benachrichtigung	57
A.9.1	Datenschutzmitteilung	57
A.9.2	Offenheit und Transparenz.....	58
A.10	Beteiligung und Zugang der betroffenen Person	59
A.10.1	Zugang der betroffenen Person	59
A.10.2	Behebung	61
A.10.3	Behandlung von Beschwerden.....	62
A.11	Verantwortlichkeit	62
A.11.1	Lenkung.....	62
A.11.2	Datenschutz-Folgenabschätzung.....	63
A.11.3	Datenschutzanforderung für Auftragnehmer und Auftragsdatenverarbeiter	64
A.11.4	Überwachung und Prüfung des Datenschutzes	65
A.11.5	Datenschutzaufklärung und -schulung	65
A.11.6	Berichterstattung zum Datenschutz	66
A.12	Informationssicherheit	66
A.13	Einhaltung der Datenschutzpflichten	67
A.13.1	Compliance	67
A.13.2	Beschränkungen der grenzüberschreitenden Datenübertragung in einigen Ländern.....	68

Anhang B (informativ) Übereinstimmung von ISO/IEC 29151:202X (dieses Dokument) mit ISO/IEC 29151:2017 (Dieser Anhang ist nicht integraler Bestandteil dieser Empfehlung Internationalen Norm.)	69
Literaturhinweise	73

Bilder

Bild 1 — Zusammenhang zwischen diesem Dokument und anderen ISO/IEC-Normen	12
--	-----------

Tabellen

Tabelle 1 — Ort der datenschutzspezifischen Anleitung und weiteren Informationen zur Implementierung von Maßnahmen in ISO/IEC 27002:2022	19
Tabelle B.1 —Übereinstimmung zwischen Maßnahmen in diesem Dokument und Maßnahmen in ISO/ IEC 29151:2017	69