

# E DIN EN ISO/IEC 29151:2025-07 (D/E)

Informationssicherheit, Cybersicherheit und Datenschutz - Maßnahmen und Anleitung für den Schutz personenbezogener Daten (ISO/IEC DIS 29151:2025); Deutsche und Englische Fassung prEN ISO/IEC 29151:2025

Information security, cybersecurity and privacy protection - Controls and guidance for personally identifiable information protection (ISO/IEC DIS 29151:2025); German and English version prEN ISO/IEC 29151:2025

---

Inhalt	Seite
Europäisches Vorwort . . . . .	6
Vorwort . . . . .	7
Einleitung . . . . .	9
1 Anwendungsbereich . . . . .	12
2 Normative Verweisungen . . . . .	12
3 Begriffe und Abkürzungen . . . . .	12
3.1 Begriffe . . . . .	12
3.2 Abkürzungen . . . . .	13
4 Übersicht . . . . .	14
4.1 Schutz von pbD . . . . .	14
4.2 Anforderung an den Schutz von pbD . . . . .	14
4.3 Von der Datenschutz-Risikobeurteilung abgeleitete Maßnahmen . . . . .	14
4.4 Auswahl von Maßnahmen . . . . .	15
4.5 Entwicklung organisationsspezifischer Leitfäden . . . . .	15
4.6 Erwägungen zur Lebensdauer . . . . .	15
4.7 Aufbau dieses Dokuments . . . . .	16
5 Organisatorische Maßnahmen . . . . .	21
5.1 Informationssicherheitsleitlinien . . . . .	21
5.2 Informationssicherheitsrollen und -verantwortlichkeiten . . . . .	21
5.3 Aufgabentrennung . . . . .	22
5.4 Verantwortlichkeiten der Leitung . . . . .	23
5.5 Kontakt mit Behörden . . . . .	23
5.6 Kontakt mit speziellen Interessengruppen . . . . .	23
5.7 Informationen über Bedrohungen . . . . .	23
5.8 Informationssicherheit im Projektmanagement . . . . .	23
5.9 Inventar der Informationen und anderen damit verbundenen Werte . . . . .	23
5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten . . . . .	24
5.11 Rückgabe von Werten . . . . .	24
5.12 Klassifizierung von Information . . . . .	24
5.13 Kennzeichnung von Information . . . . .	25
5.14 Informationsübertragung . . . . .	25
5.15 Zugangssteuerung . . . . .	25
5.16 Identitätsmanagement . . . . .	25
5.17 Informationen zur Authentifizierung . . . . .	26
5.18 Zugangsrechte . . . . .	26
5.19 Informationssicherheit in Lieferantenbeziehungen . . . . .	26
5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen . . . . .	26
5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette . . . . .	27
5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen . . . . .	27
5.23 Informationssicherheit für die Nutzung von Cloud-Diensten . . . . .	27
5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen . . . . .	27
5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse . . . . .	28
5.26 Reaktion auf Informationssicherheitsvorfälle . . . . .	29
5.27 Erkenntnisse aus Informationssicherheitsvorfällen . . . . .	29

5.28	Sammeln von Beweismaterial . . . . .	29
5.29	Informationssicherheit bei Störungen . . . . .	29
5.30	IKT-Bereitschaft für Business Continuity . . . . .	29
5.31	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen . . . . .	30
5.32	Geistige Eigentumsrechte . . . . .	30
5.33	Schutz von Aufzeichnungen . . . . .	30
5.34	Datenschutz und Schutz personenbezogener Daten (pbd) . . . . .	30
5.35	Unabhängige Überprüfung der Informationssicherheit . . . . .	30
5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit . . . . .	31
5.37	Dokumentierte Betriebsabläufe . . . . .	31
6	Personenbezogene Maßnahmen . . . . .	31
6.1	Sicherheitsüberprüfung . . . . .	31
6.2	Beschäftigungs- und Vertragsbedingungen . . . . .	31
6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung . . . . .	31
6.4	Maßregelungsprozess . . . . .	32
6.5	Verantwortlichkeiten nach Beendigung oder Änderung des Beschäftigungsverhältnisses . . . . .	32
6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen . . . . .	32
6.7	Telearbeit . . . . .	32
6.8	Meldung von Informationssicherheitsereignissen . . . . .	33
7	Physische Maßnahmen . . . . .	33
7.1	Physische Sicherheitsperimeter . . . . .	33
7.2	Physischer Zutritt . . . . .	33
7.3	Sicherung von Büros, Räumen und Einrichtungen . . . . .	33
7.4	Physische Sicherheitsüberwachung . . . . .	33
7.5	Schutz vor physischen und umweltbedingten Bedrohungen . . . . .	33
7.6	Arbeit in Sicherheitsbereichen . . . . .	33
7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren . . . . .	33
7.8	Platzierung und Schutz von Geräten und Betriebsmitteln . . . . .	33
7.9	Sicherheit von Werten außerhalb der Räumlichkeiten . . . . .	33
7.10	Speichermedien . . . . .	33
7.11	Versorgungseinrichtungen . . . . .	34
7.12	Sicherheit der Verkabelung . . . . .	34
7.13	Instandhaltung von Geräten und Betriebsmitteln . . . . .	34
7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln . . . . .	34
8	Technische Maßnahmen . . . . .	35
8.1	Endpunktgeräte des Benutzers . . . . .	35
8.2	Privilegierte Zugangsrechte . . . . .	35
8.3	Informationszugangsbeschränkung . . . . .	35
8.4	Zugriff auf den Quellcode . . . . .	35
8.5	Sichere Authentifizierung . . . . .	36
8.6	Kapazitätssteuerung . . . . .	36
8.7	Schutz gegen Schadsoftware . . . . .	36
8.8	Handhabung von technischen Schwachstellen . . . . .	36
8.9	Konfigurationsmanagement . . . . .	36
8.10	Löschung von Informationen . . . . .	36
8.11	Datenmaskierung . . . . .	36
8.12	Verhinderung von Datenlecks . . . . .	36
8.13	Sicherung von Information . . . . .	36
8.14	Verfügbarkeit von informationsverarbeitenden Einrichtungen . . . . .	37
8.15	Protokollierung . . . . .	37
8.16	Überwachung von Aktivitäten . . . . .	37
8.17	Uhrensynchronisation . . . . .	37
8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten . . . . .	37
8.19	Installation von Software auf Betriebssystemen . . . . .	38
8.20	Netzwerksicherheit . . . . .	38
8.21	Sicherheit von Netzwerkdiensten . . . . .	38
8.22	Trennung von Netzwerken . . . . .	38
8.23	Webfilterung . . . . .	38
8.24	Verwendung von Kryptographie . . . . .	38
8.25	Sicherer Entwicklungslebenszyklus . . . . .	38
8.26	Anforderungen an die Anwendungssicherheit . . . . .	38
8.27	Sichere Systemarchitektur und technische Grundsätze . . . . .	38
8.28	Sichere Programmierung . . . . .	38

8.29	Sicherheitsprüfung bei Entwicklung und Abnahme . . . . .	38
8.30	Ausgegliederte Entwicklung . . . . .	39
8.31	Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen . . . . .	39
8.32	Änderungssteuerung . . . . .	39
8.33	Prüfinformationen . . . . .	39
8.34	Schutz der Informationssysteme während der Überwachungsprüfung . . . . .	39
<b>Anhang A (normativ) Erweiterter Kontrollsatz für den Datenschutz . . . . .</b>		<b>40</b>
A.1	Allgemeines . . . . .	40
A.2	Allgemeine Leitlinien für die Nutzung und den Schutz von pbD . . . . .	40
A.3	Einwilligung und Wahlfreiheit . . . . .	41
A.3.1	Einwilligung . . . . .	41
A.3.2	Wahl . . . . .	43
A.4	Zulässigkeit des Zwecks und Spezifikation . . . . .	44
A.4.1	Zulässigkeit des Zwecks . . . . .	44
A.4.2	Spezifikation des Zwecks . . . . .	45
A.5	Beschränkung der Erhebung . . . . .	45
A.6	Datensparsamkeit . . . . .	46
A.7	Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung . . . . .	48
A.7.1	Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung . . . . .	48
A.7.2	Sicheres Löschen temporärer Dateien . . . . .	50
A.7.3	Mitteilung über die Offenlegung von pbD . . . . .	50
A.7.4	Aufzeichnung der Offenlegung von pbD . . . . .	51
A.7.5	Offenlegung der Verarbeitung von pbD durch Subunternehmer . . . . .	51
A.8	Genauigkeit und Qualität . . . . .	52
A.9	Offenheit, Transparenz und Benachrichtigung . . . . .	53
A.9.1	Datenschutzmitteilung . . . . .	53
A.9.2	Offenheit und Transparenz . . . . .	54
A.10	Beteiligung und Zugang der betroffenen Person . . . . .	55
A.10.1	Zugang der betroffenen Person . . . . .	55
A.10.2	Behebung . . . . .	56
A.10.3	Behandlung von Beschwerden . . . . .	57
A.11	Verantwortlichkeit . . . . .	57
A.11.1	Lenkung . . . . .	57
A.11.2	Datenschutz-Folgenabschätzung . . . . .	58
A.11.3	Datenschutzanforderung für Auftragnehmer und Auftragsdatenverarbeiter . . . . .	59
A.11.4	Überwachung und Prüfung des Datenschutzes . . . . .	60
A.11.5	Datenschutzaufklärung und -schulung . . . . .	60
A.11.6	Berichterstattung zum Datenschutz . . . . .	61
A.12	Informationssicherheit . . . . .	61
A.13	Einhaltung der Datenschutzpflichten . . . . .	62
A.13.1	Compliance . . . . .	62
A.13.2	Beschränkungen der grenzüberschreitenden Datenübertragung in einigen Ländern . . . . .	63
<b>Anhang B (informativ) Übereinstimmung zwischen diesem Dokument und ISO/ IEC 29151:2017 . . . . .</b>		<b>64</b>
<b>Literaturhinweise . . . . .</b>		<b>68</b>

## Bilder

<b>Bild 1 — Zusammenhang zwischen diesem Dokument und anderen Internationalen Normen . . . . .</b>	<b>10</b>
--	-----------

## Tabellen

<b>Tabelle 1 — Ort der datenschutzspezifischen Anleitung und weiteren Informationen zur Implementierung von Maßnahmen in ISO/IEC 27002:2022 . . . . .</b>	<b>17</b>
<b>Tabelle B.1 — Übereinstimmung zwischen Maßnahmen in diesem Dokument und Maßnahmen in ISO/ IEC 29151:2017 . . . . .</b>	<b>64</b>