

E DIN EN ISO/IEC 27018:2026-08 (D/E)

Erscheinungsdatum: 2026-07-03

Informationssicherheit, Cybersicherheit und Datenschutz - Leitlinien zum Schutz personenbezogener Daten (PD) in öffentlichen Clouds, die als Auftragsverarbeiter für PD tätig sind (ISO/IEC 27018:2025); Deutsche und Englische Fassung prEN ISO/IEC 27018:2026

Information security, cybersecurity and privacy protection - Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors (ISO/IEC 27018:2025); German and English version prEN ISO/IEC 27018:2026

Inhalt

Seite

| | |
|--|----|
| Europäisches Vorwort | 5 |
| Vorwort | 6 |
| Einleitung | 7 |
| 1 Anwendungsbereich | 11 |
| 2 Normative Verweisungen | 11 |
| 3 Begriffe | 11 |
| 4 Überblick | 13 |
| 4.1 Aufbau dieses Dokuments | 13 |
| 4.2 Maßnahmengestaltung | 22 |
| 5 Organisatorische Maßnahmen | 23 |
| 5.1 Informationssicherheitspolitik und -richtlinien | 23 |
| 5.2 Informationssicherheitsrollen und -verantwortlichkeiten | 23 |
| 5.3 Funktionstrennung | 24 |
| 5.4 Verantwortlichkeiten des Managements | 24 |
| 5.5 Kontakt zu Behörden | 24 |
| 5.6 Kontakt mit speziellen Interessengruppen | 24 |
| 5.7 Informationen über die Bedrohungslage | 24 |
| 5.8 Informationssicherheit im Projektmanagement | 24 |
| 5.9 Inventar der Informationen und anderer damit verbundener Werte | 24 |
| 5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten | 24 |
| 5.11 Rückgabe von Werten | 24 |
| 5.12 Klassifizierung von Informationen | 24 |
| 5.13 Kennzeichnung von Informationen | 24 |
| 5.14 Informationsübermittlung | 24 |
| 5.15 Zugangskontrolle | 25 |
| 5.16 Identitätsmanagement | 25 |
| 5.17 Authentisierungsinformationen | 25 |
| 5.18 Zugangsrechte | 25 |
| 5.19 Informationssicherheit in Lieferantenbeziehungen | 25 |
| 5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen | 25 |
| 5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette | 25 |
| 5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen | 26 |
| 5.23 Informationssicherheit für die Nutzung von Cloud-Diensten | 26 |
| 5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen | 26 |
| 5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse | 26 |
| 5.26 Reaktion auf Informationssicherheitsvorfälle | 26 |
| 5.27 Erkenntnisse aus Informationssicherheitsvorfällen | 26 |
| 5.28 Sammeln von Beweismaterial | 26 |
| 5.29 Informationssicherheit bei Störungen | 26 |
| 5.30 IKT-Bereitschaft für Business-Continuity | 26 |
| 5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen | 26 |
| 5.32 geistige Eigentumsrechte | 27 |

| | | |
|------|--|----|
| 5.33 | Schutz von Aufzeichnungen | 27 |
| 5.34 | Datenschutz und Schutz personenbezogener Daten (pbD) | 27 |
| 5.35 | unabhängige Überprüfung der Informationssicherheit | 27 |
| 5.36 | Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit | 27 |
| 5.37 | dokumentierte Betriebsabläufe | 27 |
| 6 | Personenbezogene Maßnahmen | 27 |
| 6.1 | Sicherheitsüberprüfung | 27 |
| 6.2 | Beschäftigungs- und Vertragsbedingungen | 27 |
| 6.3 | Informationssicherheitsbewusstsein, -ausbildung und -schulung | 27 |
| 6.4 | Maßregelungsverfahren | 28 |
| 6.5 | Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung | 28 |
| 6.6 | Vertraulichkeits- oder Geheimhaltungsvereinbarungen | 28 |
| 6.7 | Remote-Arbeit | 28 |
| 6.8 | Meldung von Informationssicherheitsereignissen | 28 |
| 7 | Physische Maßnahmen | 28 |
| 7.1 | Physische Sicherheitsperimeter | 28 |
| 7.2 | Physischer Zutritt | 28 |
| 7.3 | Sicherung von Büros, Räumen und Einrichtungen | 28 |
| 7.4 | Physische Sicherheitsüberwachung | 28 |
| 7.5 | Schutz vor physischen und umweltbedingten Bedrohungen | 28 |
| 7.6 | Arbeit in Sicherheitsbereichen | 29 |
| 7.7 | Aufgeräumte Arbeitsumgebung und Bildschirmsperren | 29 |
| 7.8 | Platzierung und Schutz der Geräte und Betriebsmittel | 29 |
| 7.9 | Sicherheit von Werten außerhalb der Räumlichkeiten | 29 |
| 7.10 | Speichermedien | 29 |
| 7.11 | Versorgungseinrichtungen | 29 |
| 7.12 | Sicherheit der Verkabelung | 29 |
| 7.13 | Instandhalten von Geräten und Betriebsmitteln | 29 |
| 7.14 | Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln | 29 |
| 8 | Technologische Maßnahmen | 29 |
| 8.1 | Endgeräte des Benutzers | 29 |
| 8.2 | Privilegierte Zugangsrechte | 29 |
| 8.3 | Informationszugangsbeschränkung | 30 |
| 8.4 | Zugriff auf den Quellcode | 30 |
| 8.5 | Sichere Authentisierung | 30 |
| 8.6 | Kapazitätssteuerung | 30 |
| 8.7 | Schutz gegen Schadsoftware | 30 |
| 8.8 | Handhabung von technischen Schwachstellen | 30 |
| 8.9 | Konfigurationsmanagement | 30 |
| 8.10 | Löschung von Informationen | 30 |
| 8.11 | Datenmaskierung | 30 |
| 8.12 | Verhinderung von Datenlecks | 30 |
| 8.13 | Sicherung von Information | 31 |
| 8.14 | Redundanz von informationsverarbeitenden Einrichtungen | 31 |
| 8.15 | Protokollierung | 31 |
| 8.16 | Überwachung von Aktivitäten | 32 |
| 8.17 | Uhrensynchronisation | 32 |
| 8.18 | Gebrauch von Hilfsprogrammen mit privilegierten Rechten | 32 |
| 8.19 | Installation von Software auf Systemen in Betrieb | 32 |
| 8.20 | Netzwerksicherheit | 32 |
| 8.21 | Sicherheit von Netzwerkdiensten | 32 |
| 8.22 | Trennung von Netzwerken | 32 |
| 8.23 | Webfilterung | 32 |
| 8.24 | Verwendung von Kryptographie | 33 |
| 8.25 | sicherer Softwareentwicklungslebenszyklus | 33 |
| 8.26 | Anforderungen an die Anwendungssicherheit | 33 |
| 8.27 | Sichere Systemarchitektur und Entwicklungsgrundsätze | 33 |

| | | |
|---|---|-----------|
| 8.28 | Sichere Codierung | 33 |
| 8.29 | Sicherheitsprüfung bei Entwicklung und Abnahme | 33 |
| 8.30 | ausgegliederte Entwicklung | 33 |
| 8.31 | Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen | 33 |
| 8.32 | Änderungsmanagement | 34 |
| 8.33 | Prüfinformationen | 34 |
| 8.34 | Schutz der Informationssysteme während Audit-Prüfungen | 34 |
| Anhang A (informativ) Erweiterungssatz von durch den Public-Cloud-Auftragsverarbeiter umzusetzenden Datenschutzmaßnahmen | | 35 |
| A.1 | Allgemeines | 35 |
| A.2 | Einwilligung und Wahlfreiheit | 35 |
| A.2.1 | Verpflichtung zur Zusammenarbeit, wenn es um die Rechte des/der Betroffenen geht | 35 |
| A.3 | Zulässigkeit und Spezifikation des Zwecks | 35 |
| A.3.1 | Zweck des Public-Cloud-Auftragsverarbeiters von personenbezogenen Daten | 35 |
| A.3.2 | Kommerzielle Nutzung durch den Public-Cloud-Auftragsverarbeiter | 36 |
| A.4 | Beschränkung der Erhebung | 36 |
| A.5 | Minimierung der Datenmenge | 36 |
| A.5.1 | Sicheres Löschen temporärer Dateien | 36 |
| A.6 | Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung | 37 |
| A.6.1 | Mitteilung über die Offenlegung von pbD | 37 |
| A.6.2 | Aufzeichnung der Offenlegung von pbD | 37 |
| A.7 | Genauigkeit und Qualität | 37 |
| A.8 | Offenheit, Transparenz und Benachrichtigung | 37 |
| A.8.1 | Offenlegung der im Unterauftrag ausgeführten Verarbeitung von pbD | 37 |
| A.9 | Persönliche Teilnahme und Zugang | 38 |
| A.10 | Verantwortlichkeit | 38 |
| A.10.1 | Benachrichtigung über eine personenbezogene Daten betreffende Datenschutzverletzung | 38 |
| A.10.2 | Aufbewahrungszeitraum für administrative Sicherheitsricht- und -Anleitungen | 39 |
| A.10.3 | Rückgabe, Übertragung und Löschung von pbD | 39 |
| A.11 | Informationssicherheit | 40 |
| A.11.1 | Vertraulichkeits- oder Geheimhaltungsvereinbarungen | 40 |
| A.11.2 | Beschränkung der Erstellung von ausgedruckten Materialien | 40 |
| A.11.3 | Überwachung und Protokollierung von Datenwiederherstellungsprozessen | 40 |
| A.11.4 | Schutz von Daten auf Datenträgern, die die eigenen Räumlichkeiten verlassen | 40 |
| A.11.5 | Nutzung von unverschlüsselten tragbaren Speichermedien und Geräten | 40 |
| A.11.6 | Verschlüsselung von über öffentliche Datenübertragungsnetzwerke gesendeten pbD | 41 |
| A.11.7 | Sichere Entsorgung von ausgedruckten Materialien | 41 |
| A.11.8 | Eindeutige Nutzung von User-IDs | 41 |
| A.11.9 | Verwaltung von User-IDs | 41 |
| A.11.10 | Datensätze von berechtigten Benutzern | 41 |
| A.11.11 | Vertragsmaßnahmen | 42 |
| A.11.12 | Im Unterauftrag erfolgende Verarbeitung von personenbezogenen Daten | 42 |
| A.11.13 | Zugang zu Daten in bereits genutzten Datenspeichern | 42 |
| A.12 | Einhaltung der Datenschutzpflichten | 43 |
| A.12.1 | Geographischer Standort von pbD | 43 |
| A.12.2 | Vorgesehener Bestimmungsort von pbD | 43 |
| Anhang B (informativ) Übereinstimmung zwischen diesem Dokument und der ersten Ausgabe ISO/IEC 27018:2019 | | 44 |
| Literaturhinweise | | 48 |

Tabellen

| | | |
|-------------|---|----|
| Tabelle 1 | — Ablageort der öffentliche Cloud Diensteanbieter-spezifischen Anleitung und weitere Informationen zur Umsetzung der Datenschutzmaßnahmen in ISO/IEC 27002:2022 | 14 |
| Tabelle B.1 | — Übereinstimmung zwischen Maßnahmen in diesem Dokument und Maßnahmen in ISO/IEC 27018:2019 | 44 |