

# DIN EN ISO/IEC 27018:2020-08 (D)

Informationstechnik - Sicherheitsverfahren - Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung (ISO/IEC 27018:2019); Deutsche Fassung EN ISO/IEC 27018:2020

---

| Inhalt   | Seite |
|--|-------|
| Europäisches Vorwort.....  | 5     |
| Vorwort.....   | 6     |
| Einleitung.....  | 7     |
| 1 Anwendungsbereich.....   | 11    |
| 2 Normative Verweisungen.....  | 11    |
| 3 Begriffe.....  | 11    |
| 4 Übersicht.....   | 13    |
| 4.1 Aufbau dieses Dokuments.....   | 13    |
| 4.2 Kategorien von Maßnahmen.....  | 14    |
| 5 Informationssicherheitsrichtlinien.....  | 15    |
| 5.1 Managementausrichtung zur Informationssicherheit.....                              | 15    |
| 5.1.1 Richtlinien für die Informationssicherheit.....                                  | 15    |
| 5.1.2 Überprüfung der Richtlinien für die Informationssicherheit.....                  | 16    |
| 6 Organisation der Informationssicherheit.....   | 16    |
| 6.1 Interne Organisation.....  | 16    |
| 6.1.1 Mit der Informationssicherheit verbundene Aufgaben und Verantwortlichkeiten..... | 16    |
| 6.1.2 Funktionstrennung.....   | 16    |
| 6.1.3 Kontakt zu Behörden.....   | 16    |
| 6.1.4 Kontakt zu speziellen Interessengruppen.....                                     | 16    |
| 6.1.5 Informationssicherheit im Projektmanagement.....                                 | 16    |
| 6.2 Mobilgeräte und von zuhause Arbeiten („Teleworking“ ).....                         | 16    |
| 7 Personalsicherheit.....  | 16    |
| 7.1 Vor Beginn eines Anstellungsverhältnisses.....                                     | 16    |
| 7.2 Während des Anstellungsverhältnisses.....  | 16    |
| 7.2.1 Managementverantwortlichkeiten.....  | 17    |
| 7.2.2 Sensibilisierung, Ausbildung und Schulung zur Informationssicherheit.....        | 17    |
| 7.2.3 Disziplinarverfahren.....  | 17    |
| 7.3 Beendigung und Änderung des Anstellungsverhältnisses.....                          | 17    |
| 8 Verwaltung der Werte.....  | 17    |
| 9 Zugangssteuerung.....  | 17    |
| 9.1 Geschäftliche Anforderungen in Bezug auf die Zugangsprüfung.....                   | 17    |
| 9.2 Benutzerzugangsverwaltung.....   | 17    |
| 9.2.1 Registrierung und Deregistrierung von Benutzern.....                             | 18    |
| 9.2.2 Zuteilung von Benutzerzugängen.....  | 18    |
| 9.2.3 Verwaltung privilegierter Zugangsrechte.....                                     | 18    |
| 9.2.4 Verwaltung geheimer Authentifizierungsdaten von Benutzern.....                   | 18    |
| 9.2.5 Überprüfung von Benutzerzugangsrechten.....                                      | 18    |
| 9.2.6 Entzug oder Anpassung von Zugangsrechten.....                                    | 18    |
| 9.3 Benutzerverantwortlichkeiten.....  | 18    |
| 9.3.1 Gebrauch geheimer Authentifizierungsdaten.....                                   | 19    |

|        |   |    |
|--------|---|----|
| 9.4    | Zugangssteuerung für Systeme und Anwendungen.....                                     | 19 |
| 9.4.1  | Informationszugangsbeschränkung .....   | 19 |
| 9.4.2  | Sichere Anmeldeverfahren .....  | 19 |
| 9.4.3  | System zur Verwaltung von Kennwörtern .....   | 19 |
| 9.4.4  | Gebrauch von Hilfsprogrammen mit privilegierten Rechten .....                         | 19 |
| 9.4.5  | Zugangssteuerung für Quellcode von Programmen .....                                   | 19 |
| 10     | Kryptographie .....   | 19 |
| 10.1   | Kryptographische Maßnahmen.....   | 19 |
| 10.1.1 | Richtlinie zum Gebrauch von kryptographischen Maßnahmen .....                         | 19 |
| 10.1.2 | Schlüsselverwaltung .....   | 20 |
| 11     | Physische und umgebungsbezogene Sicherheit.....                                       | 20 |
| 11.1   | Sicherheitsbereiche.....  | 20 |
| 11.2   | Geräte und Betriebsmittel.....  | 20 |
| 11.2.1 | Platzierung und Schutz von Geräten und Betriebsmitteln .....                          | 20 |
| 11.2.2 | Versorgungseinrichtungen .....  | 20 |
| 11.2.3 | Sicherheit der Verkabelung .....  | 20 |
| 11.2.4 | Instandhaltung von Geräten und Betriebsmitteln .....                                  | 20 |
| 11.2.5 | Entfernen von Werten .....  | 20 |
| 11.2.6 | Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten ..... | 20 |
| 11.2.7 | Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln .....        | 21 |
| 11.2.8 | Unbeaufsichtigte Benutzergeräte .....   | 21 |
| 11.2.9 | Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren.....            | 21 |
| 12     | Betriebssicherheit .....  | 21 |
| 12.1   | Betriebsabläufe und -verantwortlichkeiten.....  | 21 |
| 12.1.1 | Dokumentierte Bedienabläufe .....   | 21 |
| 12.1.2 | Änderungssteuerung.....   | 21 |
| 12.1.3 | Kapazitätssteuerung .....   | 21 |
| 12.1.4 | Trennung von Entwicklungs-, Test- und Betriebsumgebungen.....                         | 21 |
| 12.2   | Schutz vor Schadsoftware.....   | 22 |
| 12.3   | Datensicherung.....   | 22 |
| 12.3.1 | Sicherung von Informationen .....   | 22 |
| 12.4   | Protokollierung und Überwachung.....  | 23 |
| 12.4.1 | Ereignisprotokollierung .....   | 23 |
| 12.4.2 | Schutz der Protokollinformation .....   | 23 |
| 12.4.3 | Administratoren- und Bedienerprotokolle .....   | 23 |
| 12.4.4 | Uhrensynchronisation.....   | 23 |
| 12.5   | Steuerung von Software im Betrieb .....   | 24 |
| 12.6   | Handhabung technischer Schwachstellen.....  | 24 |
| 12.7   | Audit von Informationssystemen.....   | 24 |
| 13     | Kommunikationssicherheit.....   | 24 |
| 13.1   | Netzwerksicherheitsmanagement.....  | 24 |
| 13.2   | Informationsübertragung .....   | 24 |
| 13.2.1 | Richtlinien und Verfahren zur Informationsübertragung.....                            | 24 |
| 13.2.2 | Vereinbarungen zur Informationsübertragung.....                                       | 24 |
| 13.2.3 | Elektronische Nachrichtenübermittlung.....  | 24 |
| 13.2.4 | Vertraulichkeits- oder Geheimhaltungsvereinbarungen.....                              | 24 |
| 14     | Anschaffung, Entwicklung und Instandhaltung von Systemen.....                         | 24 |
| 15     | Lieferantenbeziehungen .....  | 25 |
| 16     | Handhabung von Informationssicherheitsvorfällen .....                                 | 25 |
| 16.1   | Handhabung von Informationssicherheitsvorfällen und Verbesserungen.....               | 25 |
| 16.1.1 | Verantwortlichkeiten und Verfahren .....  | 25 |
| 16.1.2 | Meldung von Informationssicherheitsereignissen .....                                  | 25 |
| 16.1.3 | Meldung von Schwächen in der Informationssicherheit.....                              | 25 |
| 16.1.4 | Beurteilung von und Entscheidung über Informationssicherheitsereignisse(n) .....      | 25 |

|   |   |    |
|---|---|----|
| 16.1.5  | Reaktion auf Informationssicherheitsvorfälle .....                      | 25 |
| 16.1.6  | Erkenntnisse aus Informationssicherheitsvorfällen .....                 | 26 |
| 16.1.7  | Sammeln von Beweismaterial.....   | 26 |
| 17  | Informationssicherheitsaspekte beim Business Continuity Management..... | 26 |
| 18  | Compliance .....  | 26 |
| 18.1  | Einhaltung von rechtlichen und vertraglichen Anforderungen.....         | 26 |
| 18.2  | Überprüfungen der Informationssicherheit.....                           | 26 |
| 18.2.1  | Unabhängige Überprüfung der Informationssicherheit.....                 | 26 |
| 18.2.2  | Einhaltung von Sicherheitsrichtlinien und -standards .....              | 26 |
| 18.2.3  | Überprüfung der Einhaltung von technischen Vorgaben.....                | 26 |
| Anhang A (normativ) Erweiterungssatz von durch den Public-Cloud-Auftragsdatenverarbeiter<br>umzusetzenden Datenschutzmaßnahmen..... |   | 27 |
| Literaturhinweise .....   |   | 37 |