

DIN ISO/IEC 27018:2017-08 (D)

Informationstechnik - Sicherheitsverfahren - Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung (ISO/IEC 27018:2014)

Inhalt	Seite
Nationales Vorwort	4
Nationaler Anhang NA (informativ) Literaturhinweise	4
Vorwort	5
0 Einleitung.....	6
0.1 Hintergrund und Kontext	6
0.2 Maßnahmen zum Schutz personenbezogener Daten für Öffentliche-Cloud-Computing-Dienste	7
0.3 Anforderungen zum Schutz personenbezogener Daten	7
0.4 Auswahl und Umsetzung von Maßnahmen in einer Cloud-Computing-Umgebung.....	8
0.5 Entwicklung weiterer Leitfäden.....	9
0.6 Berücksichtigung von Lebenszyklen.....	9
1 Anwendungsbereich.....	10
2 Normative Verweisungen	10
3 Begriffe	11
4 Übersicht.....	12
4.1 Aufbau dieser Norm.....	12
4.2 Kategorien von Sicherheitsmaßnahmen	13
5 Informationssicherheitsrichtlinien.....	14
5.1 Managementausrichtung zur Informationssicherheit.....	14
6 Organisation der Informationssicherheit	15
6.1 Interne Organisation.....	15
6.2 Mobilgeräte und von zuhause Arbeiten („Teleworking“)	15
7 Personalsicherheit.....	16
7.1 Vor Beginn eines Anstellungsverhältnisses.....	16
7.2 Während des Anstellungsverhältnisses.....	16
7.3 Beendigung und Änderung des Anstellungsverhältnisses.....	16
8 Verwaltung der Werte	16
9 Zugangsprüfung.....	17
9.1 Geschäftliche Anforderungen in Bezug auf die Zugangsprüfung.....	17
9.2 Benutzerzugangsverwaltung.....	17
9.3 Benutzerverantwortlichkeiten	18
9.4 Zugangssteuerung für Systeme und Anwendungen.....	18
10 Kryptographie	19
10.1 Kryptographische Maßnahmen.....	19
11 Physische und umgebungsbezogene Sicherheit.....	19
11.1 Sicherheitsbereiche	19
11.2 Geräte und Betriebsmittel.....	19
12 Betriebssicherheit.....	20
12.1 Betriebsabläufe und -verantwortlichkeiten.....	20

12.2	Schutz vor Schadsoftware.....	21
12.3	Datensicherung.....	21
12.4	Protokollierung und Überwachung.....	22
12.5	Steuerung von Software im Betrieb	23
12.6	Handhabung technischer Schwachstellen.....	23
12.7	Audit von Informationssystemen.....	23
13	Kommunikationssicherheit.....	23
13.1	Netzwerksicherheitsmanagement.....	23
13.2	Informationsübertragung	23
14	Anschaffung, Entwicklung und Instandhaltung von Systemen.....	24
15	Lieferantenbeziehungen.....	24
16	Handhabung von Informationssicherheitsvorfällen	24
16.1	Handhabung von Informationssicherheitsvorfällen und Verbesserungen.....	24
17	Informationssicherheitsaspekte des Managements zur Aufrechterhaltung des Geschäfts im Krisenfall	25
18	Regelkonformität.....	26
18.1	Einhaltung von rechtlichen und vertraglichen Anforderungen.....	26
18.2	Überprüfungen der Informationssicherheit	26
Anhang A (normativ) Erweiterungssatz von durch den		
	Öffentlichen-Cloud-Auftragsdatenverarbeiter umzusetzenden Datenschutzmaßnahmen.....	27
A.1	Einwilligung und Wahlmöglichkeit.....	27
A.2	Zulässigkeit des Zwecks und Zweckbestimmung	27
A.3	Erhebungsbeschränkung.....	28
A.4	Datenvermeidung und Datensparsamkeit.....	28
A.5	Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung	29
A.6	Genauigkeit und Qualität.....	29
A.7	Offenheit, Transparenz und Benachrichtigung.....	30
A.8	Persönliche Teilnahme und Zugang.....	30
A.9	Verantwortlichkeit	30
A.10	Informationssicherheit	32
A.11	Einhaltung der Datenschutzpflichten.....	36
	Literaturhinweise.....	37