

DIN ISO/IEC 27018



ICS 35.030

Einsprüche bis 2017-01-18

Entwurf

**Informationstechnik –
Sicherheitsverfahren –
Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen
Cloud-Diensten als Auftragsdatenverarbeitung (ISO/IEC 27018:2014);
Text Deutsch und Englisch**

Information technology –

Security techniques –

Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (ISO/IEC 27018:2014);

Text in German and English

Technologies de l'information –

Techniques de sécurité –

Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme des processeur de PII (ISO/IEC 27018:2014);

Texte en allemand et anglais

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2016-11-18 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 67 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Inhalt

	Seite
Nationales Vorwort.....	4
Nationaler Anhang NA (informativ) Literaturhinweise	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	8
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	14
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

Nationales Vorwort

Die zugrunde liegende internationale Norm wurde von ISO/IEC JTC 1/SC 27 (International Organization for Standardization/International Electrotechnical Commission – Joint Technical Committee 1 “Information Technology”/Subcommittee 27 “Security techniques”) erarbeitet.

Die Deutsche Fassung wurde vom DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), Arbeitskreis NA 043-01-27-05 AK „Identitätsmanagement und Datenschutz-Technologien“ erarbeitet.

Wird in diesem Dokument ein Handelsname verwendet, so dient dies nur zur Information der Anwender und stellt keine Anerkennung dar.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung des ISO/IEC 27018 entsprechend der diesbezüglich durch ISO erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen ISO-Text.

Für die in diesem Dokument zitierte Internationale Norm wird im Folgenden auf die entsprechende Deutsche Norm hingewiesen:

ISO/IEC 17788	siehe	DIN ISO/IEC 17788
ISO/IEC 27000:2014	siehe	DIN ISO/IEC 27000 (in Überarbeitung)
ISO/IEC 27001:2013	siehe	DIN ISO/IEC 27001
ISO/IEC 27002:2013	siehe	DIN ISO/IEC 27002 (in Überarbeitung)

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN ISO/IEC 17788, *Informationstechnik — Cloud Computing — Übersicht und Vokabular (ISO/IEC 17788)*

DIN ISO/IEC 27000, *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Überblick und Terminologie (ISO/IEC 27001)*

DIN ISO/IEC 27001:2015-03, *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Anforderungen (ISO/IEC 27001:2013 + Cor. 1:2014)*

DIN ISO/IEC 27002:2014-02, *Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für das Informationssicherheits-Management (ISO/IEC FDIS 27002:2013)*

Informationstechnik — Sicherheitsverfahren — Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung

0 Einleitung

0.1 Hintergrund und Kontext

Cloud-Dienstleister, die im Rahmen eines Vertrages mit ihren Kunden personenbezogene Daten (pbD; en: Personally Identifiable Information, PII) verarbeiten, müssen ihre Dienste so betreiben, dass es beiden Parteien möglich ist, die Anforderungen der geltenden Gesetze und Vorschriften zum Schutz personenbezogener Daten zu erfüllen. Die Anforderungen und die Art und Weise, wie diese Anforderungen zwischen dem Cloud-Dienstleister und seinen Kunden aufgeteilt werden, variieren je nach rechtlicher Zuständigkeit und entsprechend den Bedingungen des zwischen Cloud-Dienstleister und Kunden geschlossenen Vertrags. Gesetze, die vorschreiben, wie pbD verarbeitet (d.h. erhoben, genutzt, übertragen und gelöscht) werden dürfen, werden häufig als Datenschutzgesetze bezeichnet; pbD werden häufig als persönliche Daten, personenbezogene Informationen oder Personalien bezeichnet. Die Pflichten, die der Auftragsdatenverarbeiter zu erfüllen hat, variieren ebenfalls je nach rechtlicher Zuständigkeit, was es den Unternehmen, die Cloud-Dienste bereitstellen, erschwert, über Ländergrenzen hinweg zu operieren.

Ein Öffentlicher-Cloud-Dienstleister ist dann ein Auftragsdatenverarbeiter (en: PII Processor), wenn er für einen Cloud-Dienstleistungskunden nach dessen Anweisungen personenbezogene Daten verarbeitet. Der mit dem Öffentlichen-Cloud-Auftragsdatenverarbeiter (en: public cloud PII processor) in vertraglicher Beziehung stehende Cloud-Dienstleistungskunde kann eine natürliche Person, ein/e Betroffene/r (en: PII principal), der/die seine/ihre eigenen pbD in der Cloud verarbeitet, oder eine Organisation oder eine verantwortliche Stelle (en: PII controller) sein, die pbD für und zu viele(n) Betroffene(n) verarbeitet. Der Cloud-Dienstleistungskunde kann einem oder mehreren der mit ihm verbundenen Cloud-Service-Nutzer die Berechtigung erteilen, die ihm im Rahmen seines Vertrages mit dem Öffentlichen-Cloud-Auftragsdatenverarbeiter zur Verfügung gestellten Dienste zu nutzen. Dabei ist zu beachten, dass der Cloud-Dienstleistungskunde die Verfügungsgewalt über die Verarbeitung und Nutzung der Daten hat. Ein Cloud-Dienstleistungskunde, der außerdem eine verantwortliche Stelle ist, kann weiter gefassten Verpflichtungen zum Schutz personenbezogener Daten unterliegen als der Öffentliche-Cloud-Auftragsdatenverarbeiter. Ob sich weiterhin zwischen verantwortlicher Stelle und Auftragsdatenverarbeiter unterscheiden lässt, hängt davon ab, ob der Öffentliche-Cloud-Auftragsdatenverarbeiter mit der Datenverarbeitung keine Ziele verbindet, die über die vom Cloud-Dienstleistungskunden festgelegten Ziele in Bezug auf die von ihm verarbeiteten pbD und die zur Umsetzung der Ziele des Cloud-Dienstleistungskunden erforderlichen Prozesse hinausgehen.

ANMERKUNG Falls der Öffentliche-Cloud-Auftragsdatenverarbeiter Kontodaten des Cloud-Dienstleistungskunden verarbeitet, kann er in diesem Zusammenhang als verantwortliche Stelle fungieren. Die damit verbundenen Aktivitäten werden von der vorliegenden Internationalen Norm nicht abgedeckt.

Zweck dieser Internationalen Norm bei Anwendung im Zusammenhang mit den in ISO/IEC 27002 festgelegten Informationssicherheitszielen und -maßnahmen ist, eine gemeinsame Menge von Sicherheitskategorien und -maßnahmen zu erstellen, die von einem als Auftragsdatenverarbeiter auftretenden Öffentlichen-Cloud-Computing-Dienstleister implementiert werden können. Sie hat die Ziele:

- dem Öffentlichen-Cloud-Dienstleister dabei zu helfen, seine für das Auftreten als Auftragsdatenverarbeiter geltenden Pflichten zu erfüllen, unabhängig davon, ob diese Pflichten dem Auftragsdatenverarbeiter direkt oder aufgrund des Vertrages obliegen;

- den Öffentlichen-Cloud-Auftragsdatenverarbeiter in die Lage zu versetzen, in maßgeblichen Zusammenhängen transparent zu sein, so dass Cloud-Dienstleistungskunden eine gut geführte cloudbasierte Verarbeitung von personenbezogenen Daten auswählen können;
- den Cloud-Dienstleistungskunden und den Öffentlichen-Cloud-Auftragsdatenverarbeiter beim Eingehen einer vertraglichen Vereinbarung zu unterstützen;
- dem Cloud-Dienstleistungskunden ein Verfahren zu bieten, um seine Rechte und Pflichten zur Prüfung und Regelkonformität ausüben zu können, wenn individuelle Prüfungen der verwalteten Daten in einer von mehreren Parteien genutzten, virtualisierten Server-(Cloud-)Umgebung technisch nicht praktikabel sind und die Risiken für die bereits angewendeten Sicherheitskontrollen im physikalischen und logischen Netzwerk erhöhen können.

Diese Internationale Norm ersetzt keine geltenden Gesetze oder Vorschriften, kann aber bei der Bereitstellung eines gemeinsamen Regelkonformitätsrahmenwerks für Öffentliche Cloud-Dienstleister und besonders für die im multinationalen Rahmen Agierenden von Nutzen sein.

0.2 Maßnahmen zum Schutz personenbezogener Daten für Öffentliche-Cloud-Computing-Dienste

Diese Internationale Norm wurde entwickelt, um von Organisationen als Referenz für die Auswahl von Maßnahmen zum Schutz personenbezogener Daten bei der Implementierung eines auf ISO/IEC 27001 basierenden Informationssicherheitsmanagementsystems für das Cloud-Computing oder als Anleitungsdokument für die Umsetzung von allgemein anerkannten Maßnahmen zum Schutz personenbezogener Daten bei Organisationen zu dienen, die als Öffentliche-Cloud-Auftragsdatenverarbeiter auftreten. Im Besonderen basiert diese Internationale Norm auf ISO/IEC 27002, wobei sie das (die) spezielle(n) Risikoumfeld(er) berücksichtigt, das (die) sich aus den Anforderungen zum Schutz personenbezogener Daten ergibt (ergeben) und für Öffentliche-Cloud-Computing-Dienstleister gelten kann (können), die als Auftragsdatenverarbeiter auftreten.

Organisationen, die ISO/IEC 27001 implementieren, schützen in der Regel ihre eigenen Informationswerte. Im Zusammenhang mit den Anforderungen zum Schutz von personenbezogenen Daten für einen als Auftragsdatenverarbeiter auftretenden Öffentlichen-Cloud-Dienstleister schützt die Organisation jedoch die ihr von ihren Kunden anvertrauten Informationswerte. Die Umsetzung der in ISO/IEC 27002 festgelegten Maßnahmen durch den Öffentlichen-Cloud-Auftragsdatenverarbeiter ist sowohl für diesen Zweck geeignet als auch notwendig. Diese Internationale Norm erweitert die in ISO/IEC 27002 festgelegten Maßnahmen, um dem seinem Wesen nach verteilten Risiko und dem Vorliegen einer vertraglichen Beziehung zwischen dem Cloud-Dienstleistungskunden und dem Öffentlichen-Cloud-Auftragsdatenverarbeiter Rechnung zu tragen. Diese Internationale Norm erweitert ISO/IEC 27002 auf zwei Weisen:

- für einige der nach ISO/IEC 27002 bereits bestehenden Maßnahmen werden Anleitungen für die Implementierung des Schutzes von personenbezogenen Daten in der Öffentlichen Cloud gegeben; und
- Anhang A enthält eine Reihe von zusätzlichen Maßnahmen und zugehörigen Anleitungen, deren Zweck ist, den Anforderungen zum Schutz personenbezogener Daten in der Öffentlichen Cloud gerecht zu werden, die von den nach ISO/IEC 27002 bereits bestehenden Maßnahmen nicht abgedeckt werden.

Die meisten der in dieser Internationalen Norm festgelegten Maßnahmen und Anleitungen gelten auch für verantwortliche Stellen. Die betreffende verantwortliche Stelle unterliegt jedoch in den meisten Fällen weiteren Verpflichtungen, die in diesem Dokument nicht festgelegt sind.

0.3 Anforderungen zum Schutz personenbezogener Daten

Von entscheidender Bedeutung ist, dass die betreffende Organisation ihre Anforderungen für den Schutz personenbezogener Daten benennt. Die drei wichtigsten Quellen, aus denen sich Anforderungen ergeben, sind:

- a) **Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen:** Eine Quelle sind die rechtlichen, gesetzlichen, regulatorischen und vertraglichen Anforderungen und Verpflichtungen, die von der Organisation, ihren Handels- und Vertragspartnern und den Dienstleistern erfüllt werden müssen, und deren soziokulturelle Verantwortlichkeiten und die Betriebsumgebung. Es sollte beachtet werden, dass die geltenden Gesetze und Vorschriften und die vom Auftragsdatenverarbeiter eingegangenen vertraglichen Verpflichtungen zur Auswahl spezieller Maßnahmen verpflichten und bestimmte Kriterien für die Einrichtung dieser Maßnahmen nötig machen können. Diese Anforderungen können von einem Rechtsraum zum nächsten variieren.
- b) **Risiken:** Eine weitere Quelle leitet sich aus der Bewertung der sich im Zusammenhang mit pbD für die Organisation ergebenden Risiken unter Berücksichtigung der allgemeinen Geschäftsstrategie und der Ziele der Organisation ab. Im Rahmen einer Risikobewertung werden Bedrohungen ermittelt, die Wahrscheinlichkeit des Eintretens und die Verwundbarkeit dafür beurteilt und die möglichen Auswirkungen abgeschätzt. ISO/IEC 27005 enthält Anleitungen für das Management von Informationssicherheitsrisiken, einschließlich Ratschlägen für die Risikobewertung sowie für die Annahme, Kommunikation, Überwachung und Überprüfung von Risiken. ISO/IEC 29134 enthält Anleitungen für die Datenschutz-Folgenabschätzung.
- c) **Unternehmensrichtlinien:** Während sich viele der von einer Unternehmensrichtlinie abgedeckten Aspekte aus gesetzlichen und soziokulturellen Verpflichtungen ableiten, kann eine Organisation auch aus freien Stücken beschließen, strengere Kriterien als die aus den Anforderungen von a) abgeleiteten anzulegen.

0.4 Auswahl und Umsetzung von Maßnahmen in einer Cloud-Computing-Umgebung

Maßnahmen können aus dieser Internationalen Norm ausgewählt werden (die in Form von Verweisen die Maßnahmen von ISO/IEC 27002 einschließt, wodurch sich ein gemeinsamer Satz von Referenzmaßnahmen für den/die durch den Anwendungsbereich festgelegte(n) Bereich/Anwendung ergibt). Falls erforderlich, können die Maßnahmen auch aus anderen Sätzen von Maßnahmen ausgewählt werden, oder es können neue Maßnahmen entwickelt werden, um bestimmten Bedürfnissen gerecht zu werden.

ANMERKUNG Ein von einem Öffentlichen-Cloud-Auftragsdatenverarbeiter bereitgestellter Dienst für die Verarbeitung von personenbezogenen Daten, lässt sich besser als Cloud-Computing-Anwendung ansehen, als ein Anwendungsbereich an sich. Dennoch wird in der vorliegenden Internationalen Norm, die Benennung „bereichsspezifisch“ verwendet, weil dies die in den anderen Normen der Reihe ISO/IEC 27000 verwendete konventionelle Benennung ist.

Die Auswahl der Maßnahmen hängt von organisatorischen Entscheidungen auf der Grundlage der Kriterien für die Annahme des Risikos, der Optionen für die Risikobehandlung und des allgemeinen auf die Organisation und aufgrund vertraglicher Vereinbarungen ihre Kunden und Lieferanten angewendeten Ansatzes für das Risikomanagement und unterliegt außerdem allen einschlägigen nationalen und internationalen Gesetzen und Vorschriften. Falls eine der in dieser Internationalen Norm festgelegten Maßnahmen nicht gewählt wird, muss dies dokumentiert und begründet werden.

Darüber hinaus hängen die Auswahl und die Umsetzung von Maßnahmen von den tatsächlichen Aufgaben des Öffentlichen-Cloud-Anbieters im Zusammenhang mit der Gesamt-Referenzarchitektur für das Cloud Computing ab (siehe ISO/IEC 17789). An der Bereitstellung der Infrastruktur und der Anwendungsdienste in einer Cloud-Computing-Umgebung können viele verschiedene Organisationen beteiligt sein. In einigen Fällen können ausgewählte Maßnahmen ausschließlich für eine bestimmte Dienstkategorie der Cloud-Computing-Referenzarchitektur anwendbar sein. In anderen Fällen können die mit der Umsetzung von

Sicherheitsmaßnahmen verbundenen Rollen verteilt sein. In den vertraglichen Vereinbarungen müssen die mit dem Datenschutz verbundenen Verantwortlichkeiten aller an der Bereitstellung oder Nutzung der Cloud-Dienste beteiligten Organisationen, einschließlich des Öffentlichen-Cloud-Auftragsverarbeiters von personenbezogenen Daten, seiner Unterauftragnehmer und des Cloud-Dienstleistungskunden eindeutig festgelegt werden.

Die in dieser Internationalen Norm festgelegten Maßnahmen können als Leitlinien und als für die meisten Organisationen anwendbar angesehen werden. Sie werden im Folgenden in Verbindung mit Anleitungen zur Umsetzung näher erläutert. Die Umsetzung kann vereinfacht werden, wenn die Anforderungen an den Schutz personenbezogener Daten bereits beim Design des Informationssystems, der Dienste und der Operationen des Öffentlichen-Cloud-Auftragsverarbeiters von personenbezogenen Daten berücksichtigt werden. Dies ist Bestandteil des häufig als „Privacy by Design“ bezeichneten Konzepts. In den Literaturhinweisen sind einschlägige Dokumente, wie z. B. ISO/IEC 29101, aufgeführt.

0.5 Entwicklung weiterer Leitfäden

Diese Internationale Norm kann als Ausgangspunkt für die Entwicklung von Leitfäden zum Schutz personenbezogener Daten angesehen werden. Es sind möglicherweise nicht alle der in diesem Leitfaden angegebenen Maßnahmen und Anleitungen anwendbar. Unter Umständen können weitere Maßnahmen und Leitfäden erforderlich sein, die in der vorliegenden Internationalen Norm nicht enthalten sind. Bei der Ausarbeitung von Dokumenten, die weitere Leitfäden oder Maßnahmen enthalten, kann die Aufnahme von Verweisen auf Abschnitte dieser Internationalen Norm von Nutzen sein, sofern diese anwendbar sind, um die Prüfung auf Regelkonformität durch Auditoren und Geschäftspartner zu erleichtern.

0.6 Berücksichtigung von Lebenszyklen

Personenbezogene Daten haben einen natürlichen Lebenszyklus, der von der Erhebung und Erstellung über die Speicherung, Verarbeitung, Nutzung und Übertragung bis zur letztendlichen Zerstörung oder zum Zerfall reicht. Die für personenbezogene Daten bestehenden Risiken können über ihre Lebensdauer variieren, in gewissem Maß ist Datenschutz jedoch in allen Phasen wichtig.

Die Anforderungen zum Schutz personenbezogener Daten müssen beim Management bestehender und neuer Informationssysteme über deren gesamten Lebenszyklus hinweg berücksichtigt werden.

1 Anwendungsbereich

Diese Internationale Norm legt allgemein anerkannte Maßnahmenziele, Maßnahmen und Richtlinien für die Umsetzung von Maßnahmen zum Schutz personenbezogener Daten (pD) nach den in ISO/IEC 29100 festgelegten Datenschutzprinzipien für die Öffentliche-Cloud-Umgebung fest.

Im Besonderen sind in dieser Internationalen Norm auf ISO/IEC 27002 basierende Richtlinien festgelegt, die die gesetzlichen Anforderungen für den Schutz personenbezogener Daten berücksichtigen, die im Kontext der Informationssicherheits-Risikoumgebung(en) eines Anbieters von Öffentlichen-Cloud-Diensten anwendbar sein können.

Diese Internationale Norm ist auf alle Arten und Größen von Organisationen, einschließlich öffentlicher und privater Unternehmen, öffentlicher Stellen und gemeinnütziger Organisation, anwendbar, die als Auftragsdatenverarbeiter anderen Organisationen im Rahmen eines Vertrags Informationsverarbeitungsdienste mittels Cloud Computing zur Verfügung stellen.

Die in dieser Internationalen Norm festgelegten Leitfäden können auch für Organisationen von Bedeutung sein, die als verantwortliche Stellen fungieren; diese verantwortlichen Stellen können jedoch weiteren Gesetzen, Vorschriften und Verpflichtungen zum Schutz von personenbezogenen Daten unterliegen, die nicht für Auftragsdatenverarbeiter gelten. Diese Internationale Norm ist nicht dafür vorgesehen, auch derartige zusätzliche Verpflichtungen abzudecken.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 17788 | Rec. ITU-T Y.3500, *Information technology — Cloud-computing — Overview and vocabulary*¹⁾

ISO/IEC 27000:2014, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

1) Wird demnächst veröffentlicht.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 17788 und ISO/IEC 27000 sowie die folgenden Begriffe.

3.1

Bruch der Vertraulichkeit, Integrität oder Verfügbarkeit

Datenschutz-Verletzung

(en: data breach)

Sicherheitsverletzung, die versehentlich oder rechtswidrig zur Zerstörung, zum Verlust, zur Veränderung oder zur unberechtigten Offenlegung von oder zum Zugriff auf geschützte(n) Daten bei deren Übertragung, Speicherung oder sonstiger Verarbeitung führt

[QUELLE: ISO/IEC 27040:—²⁾ 3.7]

3.2

personenbezogene Daten

pbD

(en: personally identifiable information, PII)

alle Daten bzw. Informationen die

- a) zur Identifizierung des/der Betroffenen, auf den/die sich die Informationen beziehen, verwendet werden können; oder
- b) die direkt oder indirekt mit einem/einer Betroffenen verknüpft sind oder werden können

Anmerkung 1 zum Begriff: Um festzustellen, ob ein/e Betroffene/r identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von Betroffenen, Verantwortlichen oder anderen Interessengruppen des Datenschutzes (en: privacy stakeholders), die im Besitz der Daten sind, oder von einer beliebigen anderen Partei zur Identifizierung der betreffenden natürlichen Person nachvollziehbarerweise angewendet werden können.

[QUELLE: ISO/IEC 29100:2011, 2.9]

Anmerkung 2 zum Begriff: Diese Definition wurde aufgenommen, um den Begriff der personenbezogenen Daten seiner Anwendung in dieser Internationalen Norm entsprechend zu definieren. Ein Öffentlicher-Cloud-Auftragsdatenverarbeiter ist in der Regel nicht in der Lage, genau zu wissen, ob die von ihm verarbeiteten Informationen in irgendeine festgelegte Kategorie fallen, es sei denn, der Cloud-Dienstleistungskunde hat diesbezüglich für Transparenz gesorgt.

3.3

verantwortliche Stelle

(en: PII controller)

Betroffene/r, Verantwortliche/r oder andere Interessengruppe/n des Datenschutzes, der oder die die Zwecke und Mittel für die Verarbeitung personenbezogener Daten festlegt/festlegen, ausgenommen natürliche Personen, die Daten für persönliche Zwecke nutzen

Anmerkung 1 zum Begriff: In einigen Fällen weist eine verantwortliche Stelle andere (z.B. Auftragsdatenverarbeiter) an, personenbezogene Daten in ihrem Namen zu verarbeiten, während die Verantwortung für die Verarbeitung weiterhin bei der verantwortlichen Stelle liegt.

[QUELLE: ISO/IEC 29100:2011, 2.10]

2) Wird demnächst veröffentlicht.

3.4

Betroffene/r

(en: PII principal)

natürliche Person, auf die sich die personenbezogene(n) Information/Daten (pbD) bezieht (beziehen)

Anmerkung 1 zum Begriff: Abhängig von der Rechtsprechung und der jeweiligen Gesetzgebung zum Schutz personenbezogener Daten und zum Schutz der Privatsphäre kann im Englischen anstelle der Benennung „PII principal“ auch das Synonym „data subject“ verwendet werden.

[QUELLE: ISO/IEC 29100:2011, 2.11]

3.5

Auftragsdatenverarbeiter

(en: PII processor)

Betroffene, Verantwortliche und andere Interessengruppen des Datenschutzes, die personenbezogene Daten (pbD) im Namen und nach den Anweisungen einer verantwortlichen Stelle verarbeiten

[QUELLE: ISO/IEC 29100:2011, 2.12]

3.6

Verarbeitung von personenbezogenen Daten

(en: processing of PII)

Operation oder Reihe von Operationen, die auf personenbezogene Daten (pbD) angewendet wird

Anmerkung 1 zum Begriff: Beispiele für Operationen zur Verarbeitung von pbD sind unter anderen: die Erhebung, Speicherung, Änderung, Auswertung, Beratung, Offenlegung, Anonymisierung, Pseudonymisierung, Verbreitung oder sonstige Verfügbarmachung, Löschung oder Zerstörung von pbD.

[QUELLE: ISO/IEC 29100:2011, 2.23]

3.7

Öffentlicher-Cloud-Dienstleister

Partei, die dem Öffentlichen-Cloud-Modell entsprechend Cloud-Dienste bereitstellt

4 Übersicht

4.1 Aufbau dieser Norm

Diese Internationale Norm ist ähnlich gegliedert wie ISO/IEC 27002. Wo immer die in ISO/IEC 27002 festgelegten Zielsetzungen und Maßnahmen anwendbar sind, ohne dass weitere Informationen erforderlich sind, wird im vorliegenden Dokument nur auf ISO/IEC 27002 verwiesen. Weitere Maßnahmen für den Datenschutz bei Cloud-Dienstleistern und entsprechende Anleitungen zu deren Umsetzung sind in Anhang A (normativ) beschrieben.

Falls für bestimmte Maßnahmen zusätzliche Anleitungen für den Schutz von personenbezogenen Daten bei Cloud-Dienstleistern erforderlich sind, werden diese unter der Überschrift *Anleitung für die Umsetzung von Datenschutzmaßnahmen bei Öffentlichen-Cloud-Anwendungen* angegeben. Sofern maßgeblich, werden in einigen Fällen unter der Überschrift *Weitere Informationen für den Datenschutz bei Öffentlichen-Cloud-Anwendungen* weitere Informationen gegeben, die die zusätzliche Anleitung ergänzen.

Wie sich Tabelle 1 entnehmen lässt, sind derartige bereichsspezifische Anleitungen und Informationen in den in ISO/IEC 27002 definierten Kategorien enthalten. Die mit ISO/IEC 27002 abgeglichenen Abschnittsnummern sind wie in der Tabelle angegeben.

Tabelle 1 — Stellen in ISO/IEC 27002, an denen bereichsspezifische Anleitungen und weitere Informationen zur Umsetzung der Datenschutzmaßnahmen angegeben sind

Abschnittsnummer	Überschrift	Bemerkungen
5	Informationssicherheitsrichtlinien	Enthält bereichsspezifische Anleitungen für die Umsetzung und weitere Informationen.
6	Organisation der Informationssicherheit	Enthält bereichsspezifische Anleitungen für die Umsetzung.
7	Personalsicherheit	Enthält bereichsspezifische Anleitungen für die Umsetzung und weitere Informationen.
8	Verwaltung der Werte	Enthält keine weiteren bereichsspezifischen Anleitungen für die Umsetzung oder weitere Informationen.
9	Zugangsprüfung	Enthält bereichsspezifische Anleitungen für die Umsetzung sowie eine Verweisung auf eine oder mehrere Maßnahme(n) in Anhang A.
10	Kryptographie	Enthält bereichsspezifische Anleitungen für die Umsetzung.
11	Physische und umgebungsbezogene Sicherheit	Enthält bereichsspezifische Anleitungen für die Umsetzung sowie eine Verweisung auf eine oder mehrere Maßnahme(n) in Anhang A.
12	Betriebssicherheit	Enthält bereichsspezifische Anleitungen für die Umsetzung.
13	Kommunikationssicherheit	Enthält bereichsspezifische Anleitungen für die Umsetzung sowie eine Verweisung auf eine oder mehrere Maßnahme(n) in Anhang A.
14	Anschaffung, Entwicklung und Instandhaltung von Systemen	Enthält keine weiteren bereichsspezifischen Anleitungen für die Umsetzung oder weitere Informationen.
15	Lieferantenbeziehungen	Enthält keine weiteren bereichsspezifischen Anleitungen für die Umsetzung oder weitere Informationen.
16	Handhabung von Informationssicherheitsvorfällen	Enthält bereichsspezifische Anleitungen für die Umsetzung.
17	Informationssicherheitsaspekte des Managements zur Aufrechterhaltung des Geschäfts im Krisenfall	Enthält keine weiteren bereichsspezifischen Anleitungen für die Umsetzung oder weitere Informationen.
18	Regelkonformität	Enthält bereichsspezifische Anleitungen für die Umsetzung sowie eine Verweisung auf eine oder mehrere Maßnahme(n) in Anhang A.

4.2 Kategorien von Sicherheitsmaßnahmen

In Übereinstimmung mit ISO/IEC 27002 enthält jede Hauptkategorie von Sicherheitsmaßnahmen:

- a) ein Maßnahmenziel, das angibt, was zu erreichen ist; und
- b) eine oder mehrere Maßnahmen, die angewendet werden können, um dieses Maßnahmenziel zu erreichen.

Die Beschreibungen der Sicherheitsmaßnahmen sind wie folgt strukturiert:

Maßnahme

Definiert die spezifische Aussage der Maßnahme zur Erfüllung des Maßnahmenziels.

Anleitung für die Umsetzung von Datenschutzmaßnahmen bei Öffentlichen-Cloud-Anwendungen

Enthält weitere detaillierte Informationen, um die Umsetzung der Maßnahme und das Erreichen der Maßnahmenziele zu unterstützen. Die Anleitung ist möglicherweise nicht in allen Situationen geeignet oder ausreichend und erfüllt möglicherweise nicht die spezifischen Anforderungen der Organisation an die Sicherheitsmaßnahmen. Daher können alternative oder zusätzliche Maßnahmen oder andere Formen der Risikobehandlung (Vermeidung, Verlagerung oder Annahme von Risiken) angemessen sein.

Weitere Informationen zum Datenschutz bei Öffentlichen-Cloud-Anwendungen

Enthält weitere Informationen, die möglicherweise berücksichtigt werden müssen, wie z.B. rechtliche Erwägungen und Verweisungen auf andere Normen.

5 Informationssicherheitsrichtlinien

5.1 Managementausrichtung zur Informationssicherheit

Es gilt das in ISO/IEC 27002:2013, 5.1 festgelegte Ziel.

5.1.1 Richtlinien für die Informationssicherheit

Es gelten die Maßnahme 5.1.1 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002. Außerdem gilt die folgende bereichsspezifische Anleitung.

Anleitung für die Umsetzung von Datenschutzmaßnahmen bei Öffentlichen-Cloud-Anwendungen

Die Informationssicherheitsrichtlinien sollten durch eine Aussage ergänzt werden, der sich entnehmen lässt, dass die Einhaltung der geltenden Gesetze zum Schutz von personenbezogenen Daten sowie der zwischen dem Öffentlichen-Cloud-Auftragsdatenverarbeiter und dessen Kunden (Cloud-Dienstleistungskunden) vereinbarten Vertragsbedingungen unterstützt und als Verpflichtung angesehen wird.

In den Vertragsvereinbarungen sollten die zwischen dem Öffentlichen-Cloud-Auftragsdatenverarbeiter, seinen Unterauftragnehmern und dem Cloud-Dienstleistungskunden aufgeteilten Verantwortlichkeiten unter Berücksichtigung der Art des betreffenden Cloud-Dienstes (z.B. IaaS-, PaaS- oder SaaS-Dienst, Kategorie der Cloud-Computing-Referenzarchitektur) eindeutig festgelegt sein. So kann z.B. die Zuordnung der Verantwortung für Maßnahmen, die die Anwendungsschicht betreffen, variieren, je nachdem, ob der Öffentliche-Cloud-Auftragsdatenverarbeiter einen SaaS-Dienst oder eher einen PaaS- oder IaaS-Dienst zur Verfügung stellt, auf den der Cloud-Dienstleistungskunde seine eigenen Anwendungen – gegebenenfalls schichtweise – aufbauen kann.

Weitere Informationen zum Datenschutz bei Öffentlichen-Cloud-Anwendungen

In einigen Rechtssystemen unterliegt der Öffentliche-Cloud-Auftragsdatenverarbeiter den Gesetzen zum Schutz personenbezogener Daten direkt. In anderen gelten diese Gesetze nur für die verantwortliche Stelle.

Durch den Vertrag zwischen dem Cloud-Dienstleistungskunden und dem Öffentlichen-Cloud-Auftragsdatenverarbeiter wird ein Verfahren festgelegt, das sicherstellt, dass der Öffentliche-Cloud-Auftragsdatenverarbeiter verpflichtet ist, die Einhaltung zu unterstützen und zu verwalten. Der Vertrag kann verlangen, dass die Einhaltung der Anforderungen, z. B. durch Umsetzung der entsprechenden in dieser Internationalen Norm und in ISO/IEC 27002 festgelegten Maßnahmen, von unabhängiger Seite in einer für den Cloud-Dienstleistungskunden annehmbaren Art und Weise überprüft wird.

5.1.2 Überprüfung der Richtlinien für die Informationssicherheit

Es gelten die Maßnahme 5.1.2 und die in ISO/IEC 27002 angegebenen zugehörigen Anleitungen zur Umsetzung.

6 Organisation der Informationssicherheit

6.1 Interne Organisation

Es gilt das in ISO/IEC 27002:2013, 6.1 festgelegte Ziel.

6.1.1 Mit der Informationssicherheit verbundene Aufgaben und Verantwortlichkeiten

Es gelten die Maßnahme 6.1.1 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002. Außerdem gilt die folgende bereichsspezifische Anleitung.

Anleitung für die Umsetzung von Datenschutzmaßnahmen bei Öffentlichen-Cloud-Anwendungen

Der Öffentliche-Cloud-Auftragsdatenverarbeiter sollt eine Anlaufstelle benennen, an die sich der Cloud-Dienstleistungskunde bezüglich der Verarbeitung von pbD im Rahmen des Vertrages wenden kann.

6.1.2 Funktionstrennung

Es gelten die Maßnahme 6.1.2 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

6.1.3 Kontakt zu Behörden

Es gelten die Maßnahme 6.1.3 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

6.1.4 Kontakt zu speziellen Interessengruppen

Es gelten die Maßnahme 6.1.4 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

6.1.5 Informationssicherheit im Projektmanagement

Es gelten die Maßnahme 6.1.5 und die zugehörige in ISO/IEC 27002 angegebene Anleitung zur Umsetzung.

6.2 Mobilgeräte und von zuhause Arbeiten („Teleworking“)

Es gelten das Ziel und der Inhalt von ISO/IEC 27002:2013, 6.2.

7 Personalsicherheit

7.1 Vor Beginn eines Anstellungsverhältnisses

Es gelten das Ziel und der Inhalt von ISO/IEC 27002:2013, 7.1.

7.2 Während des Anstellungsverhältnisses

Es gilt das in ISO/IEC 27002:2013, 7.2 festgelegte Ziel.

7.2.1 Managementverantwortlichkeiten

Es gelten die Maßnahme 7.2.1 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

7.2.2 Sensibilisierung, Ausbildung und Schulung zur Informationssicherheit

Es gelten die Maßnahme 7.2.2 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002. Außerdem gilt die folgende bereichsspezifische Anleitung.

Anleitung für die Umsetzung von Datenschutzmaßnahmen bei Öffentlichen-Cloud-Anwendungen

Es sollten Maßnahmen ergriffen werden, um sicherzustellen, dass sich alle betreffenden Mitarbeiter der möglichen Folgen von Verstößen gegen die Regeln und Verfahren zu Datenschutz oder Informationssicherheit, besonders gegen diejenigen zum Umgang mit pbD, für den Öffentlichen-Cloud-Auftragsdatenverarbeiter (z.B. rechtliche Folgen, Geschäftsverlust und Schaden für die Marke oder den Ruf), den Mitarbeiter (z.B. disziplinarische Folgen) und die/den Betroffene/n (z.B. körperliche, materielle oder psychische Folgen) bewusst sind.

Weitere Informationen zum Datenschutz bei Öffentlichen-Cloud-Anwendungen

In einigen Rechtssystemen können dem Öffentlichen-Cloud-Auftragsdatenverarbeiter rechtliche Sanktionen, einschließlich empfindlicher Geldstrafen, von der örtlich zuständigen Datenschutz-Aufsichtsbehörde direkt auferlegt werden. In anderen Rechtssystemen sollte die Anwendung von Internationalen Normen wie der vorliegenden bei der Abfassung des Vertrags zwischen dem Öffentlichen-Cloud-Auftragsdatenverarbeiter und dem Cloud-Dienstleistungskunde helfen, eine Basis für vertragliche Sanktionen im Falle eines Verstoßes gegen die Sicherheitsregeln und -verfahren festzulegen.

7.2.3 Disziplinarverfahren

Es gelten die Maßnahme 7.2.3 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

7.3 Beendigung und Änderung des Anstellungsverhältnisses

Es gelten das Ziel und der Inhalt von ISO/IEC 27002:2013, 7.3.

8 Verwaltung der Werte

Es gelten die Ziele und der Inhalt von ISO/IEC 27002:2013, Abschnitt 8.

9 Zugangsprüfung

9.1 Geschäftliche Anforderungen in Bezug auf die Zugangsprüfung

Es gelten das Ziel und der Inhalt von ISO/IEC 27002:2013, 9.1.

9.2 Benutzerzugangsverwaltung

Es gilt das in ISO/IEC 27002:2013, 9.2 festgelegte Ziel. Die folgende bereichsspezifische Anleitung gilt auch für die Umsetzung aller unter diesen Abschnitt (9.2) fallenden Maßnahmen.

Anleitung für die Umsetzung von Datenschutzmaßnahmen bei Öffentlichen-Cloud-Anwendungen

Im Kontext der Dienstekategorien der Cloud-Computing-Referenzarchitektur kann der Cloud-Dienstleistungskunde für einige oder alle Aspekte des Zugangsmanagements für die in seinem Zuständigkeitsbereich aktiven Cloud-Service-Nutzer verantwortlich sein. Falls angemessen, sollte der Öffentliche-Cloud-Auftragsdatenverarbeiter dem Cloud-Dienstleistungskunden ermöglichen, die Zugangsrechte der in seinem Zuständigkeitsbereich aktiven Cloud-Service-Nutzer, z.B. durch die Vergabe von Administratorrechten für die Verwaltung oder Beendigung von Zugangsrechten, selbst zu verwalten.

9.2.1 Registrierung und Deregistrierung von Benutzern

Es gelten die Maßnahme 9.2.1 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002. Außerdem gilt die folgende bereichsspezifische Anleitung.

Anleitung für die Umsetzung von Datenschutzmaßnahmen bei Öffentlichen-Cloud-Anwendungen

Die Verfahren für die Registrierung und Deregistrierung von Benutzern sollten den Fall einer Kompromittierung der Benutzerzugangskontrolle, z.B. durch die Verfälschung oder Kompromittierung von Kennwörtern oder sonstigen Benutzerregistrierungsdaten (z.B. in Folge unbeabsichtigter Offenlegung), einbeziehen.

ANMERKUNG Einzelne Rechtssysteme können bestimmte Anforderungen bezüglich der Häufigkeit von Überprüfungen auf ungenutzte Zugangsdaten stellen. Organisationen, die in diesen Rechtssystemen agieren, sollten sicherstellen, dass sie diese Anforderungen erfüllen.

9.2.2 Zuteilung von Benutzerzugängen

Es gelten die Maßnahme 9.2.2 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

9.2.3 Verwaltung privilegierter Zugangsrechte

Es gelten die Maßnahme 9.2.3 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

9.2.4 Verwaltung geheimer Authentifizierungsdaten von Benutzern

Es gelten die Maßnahme 9.2.4 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

9.2.5 Überprüfung von Benutzerzugangsrechten

Es gelten die Maßnahme 9.2.5 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

9.2.6 Entzug oder Anpassung von Zugangsrechten

Es gelten die Maßnahme 9.2.6 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

9.3 Benutzerverantwortlichkeiten

Es gilt das in ISO/IEC 27002:2013, 9.3 festgelegte Ziel.

9.3.1 Gebrauch geheimer Authentifizierungsdaten

Es gelten die Maßnahme 9.3.1 und die in ISO/IEC 27002 angegebene zugehörige Umsetzungsanleitung.

9.4 Zugangssteuerung für Systeme und Anwendungen

Es gilt das in ISO/IEC 27002:2013, 9.4 festgelegte Ziel.

9.4.1 Informationszugangsbeschränkung

Es gelten die Maßnahme 9.4.1 und die in ISO/IEC 27002 angegebene zugehörige Umsetzungsanleitung.

ANMERKUNG Weitere Maßnahmen und Anleitungen für die Informationszugangsbeschränkung finden sich in A.10.13.

9.4.2 Sichere Anmeldeverfahren

Es gelten die Maßnahme 9.4.2 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002. Außerdem gilt die folgende bereichsspezifische Anleitung.

Anleitung für die Umsetzung von Datenschutzmaßnahmen bei Öffentlichen-Cloud-Anwendungen

Falls erforderlich, sollte der Öffentliche-Cloud-Auftragsdatenverarbeiter sichere Anmeldeverfahren für alle vom Cloud-Dienstleistungskunden beantragten Konten für in dessen Zuständigkeitsbereich aktive Cloud-Service-Nutzer zur Verfügung stellen.

9.4.3 System zur Verwaltung von Kennwörtern

Es gelten die Maßnahme 9.4.3 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

9.4.4 Gebrauch von Hilfsprogrammen mit privilegierten Rechten

Es gelten die Maßnahme 9.4.4 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

9.4.5 Zugangssteuerung für Quellcode von Programmen

Es gelten die Maßnahme 9.4.5 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

10 Kryptographie

10.1 Kryptographische Maßnahmen

Es gilt das in ISO/IEC 27002:2013, 10.1 festgelegte Ziel.

10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen

Es gelten die Maßnahme 10.1.1 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002. Außerdem gilt die folgende bereichsspezifische Anleitung.

Anleitung für die Umsetzung von Datenschutzmaßnahmen bei Öffentlichen-Cloud-Anwendungen

Der Öffentliche-Cloud-Auftragsdatenverarbeiter sollte dem Cloud-Dienstleistungskunden Informationen zu den Umständen zur Verfügung stellen, unter denen er kryptographische Mittel anwendet, um die von ihm verarbeiteten pbD zu schützen. Der Öffentliche-Cloud-Auftragsdatenverarbeiter sollte dem Cloud-Dienstleistungskunden außerdem Informationen zu den von ihm bereitgestellten Kapazitäten zur Verfügung stellen, die dem Cloud-Dienstleistungskunden bei der Anwendung seiner eigenen kryptographischen Schutzmaßnahmen helfen können.

ANMERKUNG Einige Rechtssysteme verlangen die Anwendung von kryptographischen Verfahren zum Schutz bestimmter Arten von pbD, wie z. B. Gesundheitsdaten von Betroffenen, Einwohnermeldenummern, Pass-Nummern und Führerscheinnummern.

10.1.2 Schlüsselverwaltung

Es gelten die Maßnahme 10.1.2 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

11 Physische und umgebungsbezogene Sicherheit

11.1 Sicherheitsbereiche

Es gelten das Ziel und der Inhalt von ISO/IEC 27002:2013, 11.1.

11.2 Geräte und Betriebsmittel

Es gilt das in ISO/IEC 27002:2013, 11.2 festgelegte Ziel.

11.2.1 Platzierung und Schutz von Geräten und Betriebsmitteln

Es gelten die Maßnahme 11.2.1 und die in ISO/IEC 27002 angegebene zugehörige Umsetzungsanleitung.

11.2.2 Versorgungseinrichtungen

Es gelten die Maßnahme 11.2.2 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

11.2.3 Sicherheit der Verkabelung

Es gelten die Maßnahme 11.2.3 und die in ISO/IEC 27002 angegebene zugehörige Umsetzungsanleitung.

11.2.4 Instandhaltung von Geräten und Betriebsmitteln

Es gelten die Maßnahme 11.2.4 und die in ISO/IEC 27002 angegebene zugehörige Umsetzungsanleitung.

11.2.5 Entfernen von Werten

Es gelten die Maßnahme 11.2.5 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

11.2.6 Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten

Es gelten die Maßnahme 11.2.6 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

11.2.7 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

Es gelten die Maßnahme 11.2.7 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002. Außerdem gilt die folgende bereichsspezifische Anleitung.

Anleitung für die Umsetzung von Datenschutzmaßnahmen bei Öffentlichen-Cloud-Anwendungen

Für die Zwecke der sicheren Entsorgung oder Wiederverwendung sollten Geräte und Betriebsmittel, die Speichermedien enthalten, die möglicherweise pbD enthalten können, so behandelt werden, als sei dies der Fall.

ANMERKUNG Weitere Maßnahmen und Anleitungen für die sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln finden sich in A.10.13.

11.2.8 Unbeaufsichtigte Benutzergeräte

Es gelten die Maßnahme 11.2.8 und die in ISO/IEC 27002 angegebene zugehörige Umsetzungsanleitung.

11.2.9 Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren

Es gelten die Maßnahme 11.2.9 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

12 Betriebssicherheit

12.1 Betriebsabläufe und -verantwortlichkeiten

Es gilt das in ISO/IEC 27002:2013, 12.1 festgelegte Ziel.

12.1.1 Dokumentierte Bedienabläufe

Es gelten die Maßnahme 12.1.1 und die in ISO/IEC 27002 angegebene zugehörige Umsetzungsanleitung.

12.1.2 Änderungssteuerung

Es gelten die Maßnahme 12.1.2 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

12.1.3 Kapazitätssteuerung

Es gelten die Maßnahme 12.1.3 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

12.1.4 Trennung von Entwicklungs-, Test- und Betriebsumgebungen

Es gelten die Maßnahme 12.1.4 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002. Außerdem gilt die folgende bereichsspezifische Anleitung.

Anleitung für die Umsetzung von Datenschutzmaßnahmen bei Öffentlichen-Cloud-Anwendungen

Falls sich die Nutzung von pbD für Testzwecke nicht vermeiden lässt, sollte eine Risikobewertung durchgeführt werden. Und es sollten technische und organisatorische Maßnahmen umgesetzt werden, um die dabei ermittelten Risiken auf ein Minimum zu reduzieren.

12.2 Schutz vor Schadsoftware

Es gelten das Ziel und der Inhalt von ISO/IEC 27002:2013, 12.2.

12.3 Datensicherung

Es gilt das in ISO/IEC 27002:2013, 12.3 festgelegte Ziel.

12.3.1 Sicherung von Informationen

Es gelten die Maßnahme 12.3.1 und die in ISO/IEC 27002 angegebene zugehörige Umsetzungsanleitung. Außerdem gilt die folgende bereichsspezifische Anleitung.

Anleitung für die Umsetzung von Datenschutzmaßnahmen bei Öffentlichen-Cloud-Anwendungen

Informationsverarbeitungssysteme, die auf dem Cloud-Computing-Modell basieren, führen zusätzliche oder alternative Verfahren für die Datensicherung außerhalb des ursprünglichen Standorts zum Schutz gegen Datenverlust ein, die die Aufrechterhaltung von Datenverarbeitungsoperationen sicherstellen bzw. es ermöglichen, die betreffenden Datenverarbeitungsoperationen nach einem Störereignis wiederaufzunehmen. Um die Sicherung und/oder Wiederherstellung der Daten zu ermöglichen, sollten mehrere Kopien davon an physikalisch und/oder logisch getrennten Stellen (die sich innerhalb des Informationsverarbeitungssystems selbst befinden können) erzeugt oder aufbewahrt werden.

Die diesbezüglichen pbD-spezifischen Verantwortlichkeiten können beim Cloud-Dienstleistungskunden liegen. Falls der Öffentliche-Cloud-Auftragsdatenverarbeiter dem Cloud-Dienstleistungskunden ausdrücklich auch Sicherungs- und Wiederherstellungsdienste zur Verfügung stellt, sollte er dem Cloud-Dienstleistungskunden auch klare Informationen über das Leistungsspektrum seines Cloud-Dienstes in Bezug auf die Sicherung und Wiederherstellung der Daten des Cloud-Dienstleistungskunden zur Verfügung stellen.

ANMERKUNG 1 Einige Rechtssysteme können besondere Anforderungen bezüglich der Häufigkeit der Datensicherung stellen. Organisationen, die in diesen Rechtssystemen agieren, sollten sicherstellen, dass sie diese Anforderungen erfüllen.

Es sollten Verfahren eingeführt werden, die die Wiederaufnahme von Datenverarbeitungsoperationen innerhalb eines festgelegten, dokumentierten Zeitraums nach einem Störereignis ermöglichen.

Die Sicherungs- und Wiederherstellungsverfahren sollten in festgelegten, dokumentierten Intervallen überprüft werden.