

DIN ISO/IEC 27018

ICS 35.030

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

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)

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)

Gesamtumfang 37 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

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

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.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. DIN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Für die in diesem Dokument zitierten internationalen Dokumente wird im Folgenden auf die entsprechende deutschen Dokumente hingewiesen:

ISO/IEC 17788	siehe	DIN ISO/IEC 17788
ISO/IEC 17789	siehe	DIN ISO/IEC 17789
ISO/IEC 27001:2013	siehe	DIN ISO/IEC 27001:2015-03
ISO/IEC 27002:2013	siehe	DIN ISO/IEC 27002:2016-11
ISO/IEC 27040	siehe	DIN EN ISO/IEC 27040

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 27040, *Informationstechnik — IT-Sicherheitsverfahren — Speichersicherheit*

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

DIN ISO/IEC 17789, *Informationstechnik — Cloud Computing — Referenzarchitektur*

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

DIN ISO/IEC 27002:2016-11, *Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für das Informationssicherheits-Management (ISO/IEC 27002:2013 + Cor.1:2014 + Cor.2:2015)*

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Internationale Organisationen, staatlich und nicht-staatlich, in Liaison mit ISO und IEC, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames technisches Komitee (JTC, en: joint technical committee), ISO/IEC JTC 1, eingerichtet.

Die zur Erarbeitung und künftigen Revision dieses Dokumentes verwendeten Regeln sind in den ISO/IEC Direktiven Teil 1 beschrieben. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen Dokumentenarten beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Regeln der ISO/IEC Direktiven Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Einzelheiten zu Patentrechten, die während der Erarbeitung des Dokumentes identifiziert werden, werden in der Einleitung und/oder in der ISO-Liste der erhaltenen Patentdeklarationen (siehe www.iso.org/patents) angegeben.

Alle in diesem Dokument verwendeten Markennamen stellen eine Informationen für den Leser dar und stellen keine Anerkennung derselben dar.

Bezüglich einer Erklärung der Bedeutung ISO-spezifischer Ausdrücke im Zusammenhang mit Konformitätsbewertung sowie Informationen über die Einhaltung der Prinzipien der Welthandelsorganisation (WTO) zu technischen Handelshemmnissen (TBT) seitens ISO siehe folgende URL: Foreword - Supplementary information.

Das für dieses Dokument verantwortliche Komitee ist ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security techniques*.

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 Verweisungen 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 (pBD) 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]

3.4

Betroffene/r

(en: PII principal)

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

2) Wird demnächst veröffentlicht.

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.