

DIN EN ISO/IEC 27018

ICS 35.030

Ersatz für
DIN ISO/IEC 27018:2017-08

**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**

Information technology –
Security techniques –

Code of practice for protection of personally identifiable information (PII) in public clouds
acting as PII processors (ISO/IEC 27018:2019);
German version EN ISO/IEC 27018:2020

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 processeur de PII (ISO/IEC 27018:2019);
Version allemande EN ISO/IEC 27018:2020

Gesamtumfang 41 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC 27018:2019 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 27018:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitskreis NA 043-01-27-05 AK „Identitätsmanagement und Datenschutz-Technologien“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

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

ISO/IEC 17788	siehe	DIN ISO/IEC 17788
ISO/IEC 17789	siehe	DIN ISO/IEC 17789
ISO/IEC 27000	siehe	DIN EN ISO/IEC 27000
ISO/IEC 27001	siehe	DIN EN ISO/IEC 27001
ISO/IEC 27002:2013	siehe	DIN EN ISO/IEC 27002:2017-06
ISO/IEC 27040	siehe	DIN EN ISO/IEC 27040

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Änderungen

Gegenüber DIN ISO/IEC 27018:2017-08 wurden folgende Änderungen vorgenommen:

- a) Korrektur eines redaktionellen Fehlers in Anhang A;
- b) redaktionelle Überarbeitung der Norm.

Frühere Ausgaben

DIN ISO/IEC 27018: 2017-08

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 27000, *Informationstechnik — Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Überblick und Terminologie*

DIN EN ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheits-managementsysteme — Anforderungen*

DIN EN ISO/IEC 27002:2017-06, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017*

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

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

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

— Leerseite —

Deutsche Fassung

Informationstechnik —
Sicherheitsverfahren —
Leitfaden zum Schutz personenbezogener Daten (PII) in
öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung
(ISO/IEC 27018:2019)

Information technology —
Security techniques —
Code of practice for protection of personally
identifiable information (PII) in public clouds acting as
PII processors (ISO/IEC 27018:2019)

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
processeur de PII (ISO/IEC 27018:2019)

Diese Europäische Norm wurde vom CEN am 3. Mai 2020 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute und elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

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 umzusetzenden Datenschutzmaßnahmen.....		27
Literaturhinweise.....		37

Europäisches Vorwort

Der Text von ISO/IEC 27018:2019 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 27018:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis November 2020, und etwaige entgegenstehende nationale Normen müssen bis November 2020 zurückgezogen werden.

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

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 27018:2019 wurde von CEN als EN ISO/IEC 27018:2020 ohne irgendeine Abänderung genehmigt.

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. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames Technisches Komitee, ISO/IEC JTC 1 (JTC, en: Joint Technical Committee), eingerichtet.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln 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. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security techniques* erarbeitet.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO/IEC 27018:2014), die geringfügig überarbeitet wurde. Die wesentliche Änderung im Vergleich zur Vorgängerausgabe ist die Korrektur eines redaktionellen Fehlers in Anhang A.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

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 Public-Cloud-Diensteanbieter ist dann ein Auftragsdatenverarbeiter (en: PII Processor), wenn er für einen Cloud-Dienstleistungskunden nach dessen Anweisungen personenbezogene Daten verarbeitet. Der mit dem Public-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, eine verantwortliche Stelle (en: PII controller) sein, die pbD für und von 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 Public-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 Public-Cloud-Auftragsdatenverarbeiter. Die Beibehaltung der Unterscheidung zwischen verantwortlicher Stelle und Auftragsdatenverarbeiter hängt davon ab, ob der Public-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 Public-Cloud-Auftragsdatenverarbeiter Kontodaten des Cloud-Dienstleistungskunden verarbeitet, kann er in diesem Zusammenhang als verantwortliche Stelle fungieren. Die damit verbundenen Aktivitäten werden von diesem Dokument nicht abgedeckt.

Zweck dieses Dokuments 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 Public-Cloud-Computing-Dienstleister implementiert werden können. Es hat die Ziele:

- dem Public-Cloud-Diensteanbieter 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 Public-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 Public-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.

Dieses Dokument kann bei der Bereitstellung eines gemeinsamen Regelkonformitätsrahmenwerks für Public-Cloud-Dienstleister und besonders für die im multinationalen Rahmen Agierenden von Nutzen sein.

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

Dieses Dokument 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 Informationssicherheits-Managementsystems für das Cloud-Computing oder als Anleitungsdokument für die Umsetzung von allgemein anerkannten Maßnahmen zum Schutz personenbezogener Daten bei Organisationen zu dienen, die als Public-Cloud-Auftragsdatenverarbeiter auftreten. Im Besonderen basiert dieses Dokument auf ISO/IEC 27002, wobei es das bzw. die speziellen Risikoumfelder berücksichtigt, das/die sich aus den Anforderungen zum Schutz personenbezogener Daten ergibt (ergeben) und für Public-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 Public-Cloud-Diensteanbieter schützt die Organisation jedoch die ihr von ihren Kunden anvertrauten Informationswerte. Die Umsetzung der in ISO/IEC 27002 festgelegten Maßnahmen durch den Public-Cloud-Auftragsdatenverarbeiter ist sowohl für diesen Zweck geeignet als auch notwendig. Dieses Dokument 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 Public-Cloud-Auftragsdatenverarbeiter Rechnung zu tragen. Dieses Dokument 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 diesem Dokument 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 diesem Dokument ausgewählt werden (das 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 Public-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 im vorliegenden Dokument 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 ab. Sie unterliegt außerdem allen einschlägigen nationalen und internationalen Gesetzen und Vorschriften. Falls eine der in diesem Dokument festgelegten Maßnahmen nicht gewählt wird, muss dies dokumentiert und begründet werden.