DIN EN ISO/IEC 27018

DIN

ICS 35.030

Entwurf

Einsprüche bis 2020-03-10
Vorgesehen als 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 und Englische Fassung prEN 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 and English version prEN 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 et anglaise prEN ISO/IEC 27018:2020

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-01-10 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, Saatwinkler Damm 42/43, 13627 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 73 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27018:2020-02

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) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als prEN ISO/IEC 27018:2020 durch das Technische Komitee CEN/TC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN 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).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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

ISO/IEC 17088	siehe	DIN ISO/IEC 17088
ISO/IEC 27000	siehe	DIN EN ISO/IEC 27000
ISO/IEC 27002:2013	siehe	DIN EN ISO/IEC 27002:2017-06
ISO/IEC 17789	siehe	DIN ISO/IEC 17789
ISO/IEC 27001	siehe	DIN EN ISO/IEC 27001
ISO/IEC 27040	siehe	DIN EN ISO/IEC 27040

Änderungen

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

a) Korrektur eines redaktionellen Fehlers in Anhang A.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27018:2020-02

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN ISO/IEC 17088, *Informationstechnik — Cloud Computing — Übersicht und Vokabular*

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

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

DIN EN ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — 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*

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27018:2020-02

— Leerseite —

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27018:2020-02

– Entwurf –

CEN/TC 13

Datum: 2020-01

prEN ISO/IEC 27018:2020

CEN/TC 13

Sekretariat: DIN

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

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)

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: CEN-Umfrage
Dokument-Sprache: D

STD Version 2.9p

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27018:2020-02

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 Sicherheitsmaßnahmen **15**

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“) **17**

7 Personalsicherheit **17**
7.1 Vor Beginn eines Anstellungsverhältnisses **17**
7.2 Während des Anstellungsverhältnisses **17**
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 **18**
9.1 Geschäftliche Anforderungen in Bezug auf die Zugangsprüfung **18**
9.2 Benutzerzugangsverwaltung **18**
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 **19**
9.3 Benutzerverantwortlichkeiten **19**
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**

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27018:2020-02

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 ... 20
10.1 Kryptographische Maßnahmen ... 20
10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen ... 20
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 ... 21
11.2.6 Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten ... 21
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 ... 22
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 ... 24
12.4.4 Uhrensynchronisation ... 24
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 ... 25
13.2.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen ... 25

14 Anschaffung, Entwicklung und Instandhaltung von Systemen ... 25

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 ... 26
16.1.3 Meldung von Schwächen in der Informationssicherheit ... 26
16.1.4 Beurteilung von und Entscheidung über Informationssicherheitsereignisse(n) ... 26
16.1.5 Reaktion auf Informationssicherheitsvorfälle ... 26

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27018:2020-02

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 27
18.2.3 Überprüfung der Einhaltung von technischen Vorgaben 27

Anhang A (normativ) Erweiterungssatz von durch den Öffentlichen-Cloud-Auftragsdatenverarbeiter umzusetzenden Datenschutzmaßnahmen 28

Literaturhinweise 38

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27018:2020-02

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) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als prEN ISO/IEC 27018:2020 durch das Technische Komitee CEN/TC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Anerkennungsnotiz

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

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27018:2020-02

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.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27018:2020-02

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-ienstleistungskunden 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 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 Öffentlichen-Cloud-Computing-Dienstleister implementiert werden können. Es 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;

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27018:2020-02

— 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.

Dieses Dokument kann 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

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 Öffentliche-Cloud-Auftragsdatenverarbeiter auftreten. Im Besonderen basiert dieses Dokument auf ISO/IEC 27002, wobei es 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. 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 Öffentlichen-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.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27018:2020-02

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 Verweisungen 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 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.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27018:2020-02

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 diesem Dokument 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 (siehe [9] in den Literaturhinweisen).

0.5 Entwicklung weiterer Leitfäden

Dieses Dokument 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 im vorliegenden Dokument nicht enthalten sind. Bei der Ausarbeitung von Dokumenten, die weitere Leitfäden oder Maßnahmen enthalten, kann die Aufnahme von Verweisungen auf Abschnitte des vorliegenden Dokuments 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.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27018:2020-02

1 Anwendungsbereich

Dieses Dokument 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 diesem Dokument 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.

Dieses Dokument 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 diesem Dokument 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. Dieses Dokument ist nicht dafür vorgesehen, auch derartige zusätzliche Verpflichtungen abzudecken.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. 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, *Information technology — Cloud computing — Overview and vocabulary*

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

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

3 Begriffe

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

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— ISO Online Browsing Platform: verfügbar unter https://www.iso.org/obp

— IEC Electropedia: verfügbar unter http://www.electropedia.org/

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27018:2020-02

3.1
Bruch der Vertraulichkeit, Integrität oder Verfügbarkeit
Datenschutz-Verletzung
(en: data breach)
Beeinträchtigung der Sicherheit, die zur zufälligen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, zur unberechtigten Offenlegung von oder den Zugang zu geschützten Daten führt, die übertragen, gespeichert oder anderweitig verarbeitet werden

[QUELLE: ISO/IEC 27040:2015, 3.7]

3.2
personenbezogene Daten
pbD
(en: personally identifiable information, PII)
sämtliche Informationen, die (a) verwendet werden können, um der natürlichen Person, auf die sich solche Informationen beziehen, zu identifizieren, oder die (b) im direkten oder indirekten Zusammenhang mit einer natürlichen Person stehen oder stehen könnten

Anmerkung 1 zum Begriff: Die „natürliche Person“ in der Definition entspricht der/dem *Betroffenen* (3.4). 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 angewendet werden können, um eine Verbindung zwischen den pbD und der natürlichen Person herzustellen.

Anmerkung 2 zum Begriff: Diese Definition wurde aufgenommen, um den Begriff der personenbezogenen Daten seiner Anwendung in diesem Dokument entsprechend zu definieren. Ein Öffentlicher-Cloud-*Auftragsdatenverarbeiter* (3.5) 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.

[QUELLE: ISO/IEC 29100:2011/Amd 1:2018, 2.9, modifiziert – Anmerkung 2 zum Begriff wurde hinzugefügt.]

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 (pbD)* (3.2) 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* (3.5)] 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 *personenbezogenen Daten (pbD)* (3.2) 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]

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27018:2020-02

3.5
Auftragsdatenverarbeiter
(en: PII processor)
Betroffene, Verantwortliche und andere Interessengruppen des Datenschutzes, die *personenbezogene Daten (pbD)* (3.2) im Namen und nach den Anweisungen einer *verantwortlichen Stelle* (3.3) 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)* (3.2) 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 dieses Dokuments

Dieses Dokument 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 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 zum 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 Tabelle 1 angegeben.

Dieses Dokument muss in Verbindung mit ISO/IEC 27001 verwendet werden, und die in Anhang A genannten zusätzlichen Maßnahmen müssen im Rahmen der Implementierung eines Informationssicherheits Managementsystems gemäß ISO/IEC 27001 für die Umsetzung berücksichtigt werden.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27018:2020-02

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

Abschnitts-nummer	Überschrift	Bemerkungen
5	Informationssicherheitsrichtlinien	enthält bereichsspezifische Anleitungen für die Umsetzung und weitere Informationen.
6	Organisation der Informations-sicherheit	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	Zugangssteuerung	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 Informations-sicherheitsvorfällen	enthält bereichsspezifische Anleitungen für die Umsetzung.
17	Informationssicherheitsaspekte des beim Business Continuity Management	enthält keine weiteren bereichsspezifischen Anleitungen für die Umsetzung oder weitere Informationen.
18	Compliance	enthält bereichsspezifische Anleitungen für die Umsetzung sowie eine Verweisung auf eine oder mehrere Maßnahme(n) in Anhang A.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27018:2020-02

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 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.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27018:2020-02

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 können diese Gesetze nur für die verantwortliche Stelle gelten.

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 diesem Dokument 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 sollte 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.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27018:2020-02

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 dem vorliegenden Dokument bei der Abfassung des Vertrags zwischen dem Öffentlichen-Cloud-Auftragsdaten-verarbeiter 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.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27018:2020-02

9 Zugangssteuerung

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 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. Es liegt in der Verantwortung der Organisationen, die in diesen Rechtssystemen agieren, diese Anforderungen zu 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.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27018:2020-02