DIN EN ISO/IEC 29100

ICS 35.030 Einsprüche bis 2020-04-14

Entwurf

Informationstechnik – Sicherheitsverfahren – Rahmenwerk für Datenschutz (ISO/IEC 29100:2011, einschließlich Amd 1:2018); Deutsche und Englische Fassung prEN ISO/IEC 29100:2020

Information technology –
Security techniques –
Privacy framework (ISO/IEC 29100:2011, including Amd 1:2018);
German and English version prEN ISO/IEC 29100:2020

Technologies de l'information –
Techniques de sécurité –
Cadre privé (ISO/IEC 29100:2011 y compris Amd 1:2018);
Version allemande et anglaise prEN ISO/IEC 29100:2020

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-02-14 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)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29100:2020-03

Nationales Vorwort

Der Text von ISO/IEC 29100:2011 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 29100:2020 durch das Technische Komitee CEN/TC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Für die deutsche Mitarbeit ist der Arbeitskreis NA 043-01-27-05 AK „Identitätsmanagement und Datenschutz-Technologien“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) verantwortlich.

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 31000 siehe DIN ISO 31000

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN ISO 31000, *Risikomanagement — Leitlinien*

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29100:2020-03

– Entwurf –

CEN/TC 13

Datum: 2020-01

prEN ISO/IEC 29100:2020

CEN/TC 13

Sekretariat: DIN

Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Datenschutz (ISO/IEC 29100:2011/Amd.1:2018)

Technologies de l'information — Techniques de sécurité — Cadre privé (ISO/IEC 29100:2011/Amd.1:2018)

Information technology — Security techniques — Privacy framework (ISO/IEC 29100:2011/Amd.1:2018)

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 29100:2020-03

Inhalt

Seite

Europäisches Vorwort **3**

Vorwort **4**

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29100:2020-03

Europäisches Vorwort

Der Text von ISO/IEC 29100:2011/Amd.1:2018 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 29100:2020 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 29100:2011/Amd.1:2018 wurde von CEN als prEN ISO/IEC 29100:2020 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29100:2020-03

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsorganisationen (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von Technischen Komitees von ISO durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO stehen, nehmen ebenfalls an der Arbeit teil. ISO arbeitet bei allen elektrotechnischen Themen eng mit der Internationalen Elektrotechnischen Kommission (IEC) zusammen.

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. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen ISO-Dokumentenarten 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 ist 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, *Security techniques,* erarbeitet.

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 29100:2020-03

Einleitung, dritter Absatz, erster Satz

„Internationale Norm“ ist durch „Dokument“ zu ersetzen:

In einigen Rechtssystemen könnten die Verweisungen auf Datenschutzanforderungen in diesem Dokument so verstanden werden, dass sie eine Ergänzung zu gesetzlichen Anforderungen zum Schutz von pbD darstellen.

Einleitung, letzter Absatz

„Internationale Norm“ ist durch „Dokument“ zu ersetzen:

Einige Rechtssysteme könnten die Einhaltung eines oder mehrerer der Dokumente, auf die in ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 (WG 5 SD2) – Official Privacy Documents References [3] verwiesen wird, oder sonstiger geltender Gesetze und Vorschriften fordern. Dieses Dokument ist jedoch weder als globale Modellrichtlinie noch als gesetzliches Rahmenwerk vorgesehen.

2.6

Die Definition von „identifizieren“ ist zu löschen:

2.6

(zurückgezogen)

2.7

Die Definition von „Identität“ ist zu löschen:

2.7

(zurückgezogen)

2.9

Der terminologische Eintrag ist wie folgt zu ändern:

2.9
personenbezogene Daten
pbD
(en: personally identifiable information, PII)
sämtliche Informationen, die (a) verwendet werden können, um die natürliche 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 Die „natürliche Person“ in der Definition entspricht der betroffenen Person (2.11). Um festzustellen, ob eine betroffene Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die vom Datenschutz-Akteur, der im Besitz der Daten ist, oder von einer beliebigen anderen Partei angewendet werden können, um eine Verbindung zwischen den pbD und der natürlichen Person herzustellen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29100:2020-03

2.20

Der terminologische Eintrag ist wie folgt zu ändern:

2.20
Datenschutz-Folgenabschätzung
DSFA
Datenschutz-Risikobeurteilung
Gesamtprozess aus Identifizieren, Analysieren, Bewerten, Beraten, Kommunizieren und Planen der Behandlung von möglichen Datenschutzfolgen unter Bezug auf die Verarbeitung personenbezogener Daten, eingebettet in den unternehmensweiten Rahmen zum Risikomanagement

[QUELLE: ISO/IEC 29134:2017, 3.7, modifiziert – „Datenschutz-Folgenabschätzung“ wurde als zulässige Benennung hinzugefügt]

4.5, letzter Absatz, zweiter Anstrich

Dieser wird durch folgenden Text ersetzt, um den Anstrich mit dem Text in Bild 1 zu vereinheitlichen:

— Vertragsfaktoren wie Vereinbarungen zwischen mehreren verschiedenen Akteuren, Firmenrichtlinien und verbindlichen Unternehmensregeln;

4.5.2, zweiter Absatz

Der Absatz wird durch folgenden ersetzt:

Im Prinzip sollte jede Partei, die Zugang zu pbD hat, formell von dem/den jeweiligen pbD-Beauftragten auf ihre Verpflichtungen hingewiesen werden, zum Beispiel durch den Abschluss von Vereinbarungen mit Dritten. Solche Vereinbarungen enthalten wahrscheinlich eine Reihe von Datenschutzanforderungen, die Empfänger von pbD berücksichtigen müssen. In einigen Rechtssystemen könnten nationale und regionale Behörden rechtliche und vertragliche Mittel geschaffen haben, die die Übertragung von pbD an Dritte ermöglichen.

4.5.3, zweiter Absatz

Der Absatz wird durch folgenden ersetzt:

Viele geschäftliche Faktoren haben keine direkte Auswirkung auf Datenschutzanforderungen als solche. Die vorgesehene Nutzung von pbD wird voraussichtlich die Umsetzung von Datenschutzrichtlinien sowie die Wahl von Steuerungsmaßnahmen für den Datenschutz einer Organisation beeinflussen. Die Organisation sollte jedoch die Datenschutzprinzipien, denen sie beipflichtet, deshalb nicht ändern. So kann es für einen Dienstleister zum Beispiel notwendig sein, um eine bestimmte Dienstleistung anbieten zu können, zusätzliche pbD zu erheben oder weiteren seiner Angestellten zu erlauben, gewisse Arten von pbD zu verarbeiten. Ein pbD-Beauftragter, der den in diesem Rahmenwerk enthaltenen Prinzipien beipflichtet, sollte trotzdem sorgfältig beurteilen, welche Arten von pbD unbedingt erforderlich sind, um den Dienst zu erbringen (Grundsatz der Beschränkung der Erhebung) und die Verarbeitung von pbD durch seine Mitarbeiter auf das zur Erfüllung ihrer Aufgaben erforderliche Maß beschränken (Grundsatz der Datensparsamkeit).

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29100:2020-03

5.1, erster Absatz, erster Satz

„Staaten, Länder“ wird durch „Länder“ ersetzt:

> Die in dieser Norm beschriebenen Datenschutzprinzipien wurden aus bestehenden Prinzipien abgeleitet, die von einer Reihe von Ländern und internationaler Organisationen entwickelt wurden. Dieses Rahmenwerk legt den Schwerpunkt auf die Verwirklichung der Datenschutzprinzipien in IKT-Systemen und die Entwicklung von Datenschutz-Managementsystemen, die innerhalb der IKT-Systeme der Organisation implementiert werden müssen. Diese Datenschutzprinzipien sollten verwendet werden, um die Entwicklung und Verwirklichung von Datenschutzprinzipien und Steuerungsmaßnahmen für den Datenschutz anzuleiten. Zusätzlich können sie als Grundlage bei der Überwachung und Messung von Leistungs-, Leistungsvergleichs- und Auditingaspekten von Datenschutz-Managementprogrammen in einer Organisation verwendet werden.

5.5, Aufzählung

Die Liste wird durch folgende ersetzt:

— die pbD, die verarbeitet werden, sowie die Anzahl von Datenschutz-Akteuren und Personen, denen pbD offengelegt werden oder denen erlaubt wird, diese zu verarbeiten, minimieren,

— die Anwendung eines „Need-to-know“-Prinzips sicherstellen (d. h. man sollte nur die pbD verarbeiten dürfen, die für die Erfüllung der offiziellen Aufgaben im Rahmen des legitimen Zwecks der Verarbeitung von pbD erforderlich sind),

— nach Möglichkeit Interaktionen und Transaktionen nutzen oder als Standardoptionen anbieten, die nicht die Identifizierung betroffener Personen beinhalten, die die Beobachtbarkeit ihres Verhaltens verringern und die die Verknüpfbarkeit der erhobenen pbD einschränken und

— pbD sicher vernichten, wann immer dies praktisch möglich ist, insbesondere, wenn der Zweck der Verarbeitung der pbD endet und keine gesetzlichen Anforderungen an ihre Aufbewahrung bestehen.

5.8, zweite Liste, letzter Punkt

„pbD-Daten“ wird durch „pbD“ ersetzt:

— die angegebenen Anforderungen an die Aufbewahrung und Entsorgung von pbD.

5.9, Liste, Punkt 3

„persönliche Daten“ wird durch „pbD“ ersetzt:

— die Bereitstellung jeglicher Änderung, Berichtigung oder Löschung an pbD-Verarbeiter und Dritte, an die pbD weitergegeben wurden, sofern diese bekannt sind; und

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29100:2020-03

— Leerseite —

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29100:2020-03

– Entwurf –

CEN/TC 13

Datum: 2020-01

prEN ISO/IEC 29100:2020

CEN/TC 13

Sekretariat: DIN

Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Datenschutz (ISO/IEC 29100:2011, einschließlich Amd 1:2018)

Technologies de l'information — Techniques sécurité — Cadre privé (ISO/IEC 29100:2011 y compris Amd 1:2018)

Information technology — Security techniques — Privacy framework (ISO/IEC 29100:2011, including Amd 1:2018)

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 29100:2020-03

Inhalt

Seite

Europäisches Vorwort **4**

Vorwort **5**

Einleitung **6**

1 Anwendungsbereich **8**

2 Begriffe **8**

3 Symbole und Abkürzungen **12**

4 Grundlegende Elemente des Rahmenwerks für Datenschutz **12**
4.1 Überblick über das Rahmenwerk für Datenschutz **12**
4.2 Akteure und Rollen **12**
4.2.1 Betroffene Personen **13**
4.2.2 pbD-Beauftragte **13**
4.2.3 pbD-Verarbeiter **13**
4.2.4 Dritte **13**
4.3 Interaktionen **13**
4.4 Erkennen von pbD **15**
4.4.1 Zuordnungsmerkmale **15**
4.4.2 Sonstige Unterscheidungsmerkmale **15**
4.4.3 Daten, die mit einer betroffenen Person verbunden sind oder verbunden werden könnten **17**
4.4.4 Pseudonymisierte Daten **17**
4.4.5 Metadaten **18**
4.4.6 Nicht angeforderte pbD **18**
4.4.7 Sensible pbD **18**
4.5 Datenschutzanforderungen **18**
4.5.1 Gesetzliche und regulatorische Faktoren **20**
4.5.2 Vertragliche Faktoren **21**
4.5.3 Geschäftliche Faktoren **21**
4.5.4 Weitere Faktoren **21**
4.6 Datenschutzrichtlinien **22**
4.7 Steuerungsmaßnahmen für den Datenschutz **23**

5 Die Datenschutzprinzipien aus ISO/IEC 29100 ..... **23**
5.1 Überblick über die Datenschutzprinzipien **23**
5.2 Einwilligung und Wahlfreiheit **24**
5.3 Zulässigkeit des Zwecks und Zweckbestimmung **25**
5.4 Beschränkung der Erhebung **25**
5.5 Datensparsamkeit **26**
5.6 Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung **26**
5.7 Genauigkeit und Qualität **26**
5.8 Offenheit, Transparenz und Benachrichtigung **27**
5.9 Persönliche Teilnahme und Zugang **28**
5.10 Verantwortlichkeit **28**
5.11 Informationssicherheit **29**
5.12 Einhaltung der Datenschutzpflichten **30**

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29100:2020-03

Anhang A (informativ) Übereinstimmung zwischen Begriffen aus ISO/IEC 29100 und Begriffen aus ISO/IEC 27000 ..... **31**

Literaturhinweise **32**

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29100:2020-03

Europäisches Vorwort

Der Text von ISO/IEC 29100:2011 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 29100:2020 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 29100:2011 wurde von CEN als prEN ISO/IEC 29100:2020 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29100:2020-03

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.

Internationale Normen werden nach den Regeln der ISO/IEC-Direktiven, Teil 2 erarbeitet.

Die Hauptaufgabe des Gemeinsamen Technischen Komitees ist es, Internationale Normen zu erarbeiten. Die vom Gemeinsamen Technischen Komitee verabschiedeten Internationalen Normentwürfe werden den nationalen Mitgliedern zur Abstimmung vorgelegt. Die Veröffentlichung als Internationale Norm erfordert Zustimmung von mindestens 75 % der abstimmenden nationalen Mitglieder.

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.

ISO/IEC 29100 wurde vom Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security techniques,* erarbeitet.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29100:2020-03

Einleitung

Diese Internationale Norm enthält ein hochrangiges Rahmenwerk für den Schutz personenbezogener Daten (pbD) in Systemen der Informations- und Kommunikationstechnik (IKT). Sie ist allgemeiner Natur und bettet organisatorische, technische und verfahrenstechnische Aspekte in ein allgemeines Rahmenwerk für Datenschutz ein.

Das Rahmenwerk für Datenschutz ist vorgesehen, um Organisationen dabei zu unterstützen, ihre Datenschutzanforderungen im Zusammenhang mit pbD in einer IKT-Umgebung festzulegen, indem

— eine gemeinsame Terminologie für den Schutz personenbezogener Daten festgelegt wird,

— die Akteure und ihre Rollen bei der Verarbeitung von pbD festgelegt werden,

— Datenschutzanforderungen beschrieben werden und

— auf bekannte Datenschutzprinzipien verwiesen wird.

In einigen Rechtssystemen könnten die Verweisungen auf Datenschutzanforderungen in dieser Internationalen Norm so verstanden werden, dass sie eine Ergänzung zu gesetzlichen Anforderungen zum Schutz von pbD darstellen. Aufgrund der steigenden Anzahl an Informations- und Kommunikationstechnologien, die pbD verarbeiten, ist es wichtig, über internationale Informationssicherheitsstandards zu verfügen, die ein gemeinsames Verständnis für den Schutz von pbD schaffen. Diese Internationale Norm soll bestehende Sicherheitsstandards verbessern, indem sie einen für die Verarbeitung von pbD relevanten Schwerpunkt setzt.

Die zunehmende kommerzielle Nutzung und der steigende kommerzielle Wert von pbD, die Weitergabe von pbD zwischen verschiedenen Rechtssystemen und die wachsende Komplexität von IKT-Systemen können es einer Organisation erschweren, den Schutz personenbezogener Daten sicherzustellen und die verschiedenen geltenden Gesetze einzuhalten. Datenschutz-Akteure können verhindern, dass Unsicherheit und Misstrauen entstehen, indem sie mit Fragen zum Schutz personenbezogener Daten ordnungsgemäß umgehen und Fälle von Missbrauch von pbD vermeiden.

Die Verwendung dieser Internationalen Norm wird

— die Entwicklung, der Einführung, dem Betrieb und der Aufrechterhaltung von IKT-Systemen erleichtern, die pbD verarbeiten und schützen,

— innovative Lösungen voranbringen, um den Schutz von pbD innerhalb von IKT-Systemen zu ermöglichen und

— die Programme zum Schutz personenbezogener Daten von Organisationen durch den Einsatz bewährter Vorgehensweisen verbessern.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29100:2020-03

Das in dieser Internationalen Norm enthaltene Rahmenwerk für Datenschutz kann als Grundlage für zusätzliche Normungsinitiativen zum Schutz personenbezogener Daten dienen, zum Beispiel

— als technische Referenzarchitektur,

— bei der Umsetzung und Verwendung spezifischer Technologien für den Schutz personenbezogener Daten und eines umfassenden Managements für den Schutz personenbezogener Daten,

— für Steuerungsmaßnahmen für den Datenschutz bei der Datenverarbeitung im Auftrag,

— bei Beurteilungen von Datenschutzrisiken oder

— für spezifische technische Spezifikationen.

Einige Rechtssysteme könnten die Einhaltung eines oder mehrerer der Dokumente, auf die in ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 (WG 5 SD2) – *Official Privacy Documents References* [3] verwiesen wird, oder sonstiger geltender Gesetze und Vorschriften fordern. Diese Internationale Norm ist jedoch weder als globale Modellrichtlinie noch als gesetzliches Rahmenwerk vorgesehen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29100:2020-03

1 Anwendungsbereich

Diese Internationale Norm enthält ein Rahmenwerk für Datenschutz, das

— eine gemeinsame Terminologie zum Schutz personenbezogener Daten festlegt,

— die handelnden Stellen und ihre Rollen bei der Verarbeitung von personenbezogenen Daten (pbD) festlegt,

— Überlegungen zum Schutz personenbezogener Daten beschreibt und

— Verweisungen auf bekannte Datenschutzprinzipien für Informationstechnologie enthält.

Diese Internationale Norm gilt für natürliche Personen und Organisationen, die mit Festlegung, Bereitstellung, Aufbau, Entwurf, Entwicklung, Prüfung, Aufrechterhaltung, Verwaltung und Betrieb von Informations- und Kommunikationstechniksystemen befasst sind, wenn Steuerungsmaßnahmen für den Datenschutz für die Verarbeitung von pbD erforderlich sind.

2 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ANMERKUNG Um die Verwendung der Familie Internationaler Normen ISO/IEC 27000 im spezifischen Kontext des Schutzes personenbezogener Daten zu vereinfachen und Datenschutzkonzepte im Kontext von ISO/IEC 27000 zu integrieren, enthält Anhang A die Begriffe von ISO/IEC 27000, die den Begriffen von ISO/IEC 29100 entsprechen, die in dieser Internationalen Norm verwendet werden.

2.1
Anonymität
Informationsmerkmal, das es nicht erlaubt, eine betroffene Person direkt oder indirekt zu identifizieren

2.2
Anonymisierung
Prozess, durch den personenbezogene Daten (pbD) unwiderruflich so verändert werden, dass eine betroffene Person nicht mehr direkt oder indirekt vom pbD-Beauftragten alleine oder in Zusammenarbeit mit einer anderen Partei identifiziert werden kann

2.3
anonymisierte Daten
Daten, die als Ergebnis eines Anonymisierungsprozesses personenbezogener Daten erzeugt werden

2.4
Einwilligung
die freiwillig erteilte, spezifische und informierte Zustimmung der betroffenen Person zur Verarbeitung ihrer pbD

2.5
Identifizierbarkeit
Bedingung, die dazu führt, dass eine betroffene Person direkt oder indirekt auf der Grundlage von gegebenen pbD identifiziert wird

2.6
identifizieren
eine Verbindung zwischen einer betroffenen Person und pbD oder einem Satz von pbD herstellen

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29100:2020-03

2.7
Identität
Satz von Attributen, die es ermöglichen, die betroffene Person zu identifizieren

2.8
Opt-in
Verfahren oder Politik, nach dem bzw. der die betroffene Person eine Maßnahme ergreifen muss, um eine ausdrückliche vorherige Einwilligung in die Verarbeitung ihrer pbD für einen bestimmten Zweck zu erteilen

ANMERKUNG Ein anderer Begriff, der für das Datenschutzprinzip ‚Einwilligung und Wahlfreiheit' häufig verwendet wird, ist „Opt-out". Dieser beschreibt ein Verfahren oder eine Politik, nach dem bzw. der die betroffene Person eine getrennte Maßnahme ergreifen muss, um ihre Einwilligung zurückzuhalten oder zu entziehen oder einer bestimmten Art von Verarbeitung zu widersprechen. Die Verwendung einer Opt-out-Politik geht davon aus, dass der pbD-Beauftragte das Recht hat, die pbD in der beabsichtigten Weise zu verarbeiten. Dieses Recht kann durch eine Maßnahme der betroffenen Person impliziert werden, die sich von der Einwilligung unterscheidet (z. B. durch eine Bestellung in einem Online-Shop).

2.9
personenbezogene Daten
pbD
(en: personally identifiable information, PII)
Daten, die (a) dazu verwendet werden können, die betroffene Person, auf die sie sich beziehen, zu identifizieren, oder (b) direkt oder indirekt mit einer betroffenen Person verknüpft sind oder verknüpft werden können

ANMERKUNG Um festzustellen, ob eine betroffene Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise vom Datenschutz-Akteur, der im Besitz der Daten ist, oder von einer beliebigen anderen Partei angewendet werden können, um die natürliche Person zu identifizieren.

2.10
pbD-Beauftragter
(en: PII controller)
Datenschutz-Akteur (oder Datenschutz-Akteure), der/die die Zwecke und Mittel für die Verarbeitung der personenbezogenen Daten (pbD) festlegt/festlegen, ausgenommen natürliche Personen, die Daten für persönliche Zwecke nutzen

ANMERKUNG In einigen Fällen weist ein pbD-Beauftragter andere (z. B. pbD-Verarbeiter) an, personenbezogene Daten in seinem Namen zu verarbeiten, während die Verantwortung für die Verarbeitung weiterhin beim pbD-Beauftragten liegt.

2.11
betroffene Person
(en: PII principal)
natürliche Person, auf die sich die personenbezogenen Daten (pbD) beziehen

ANMERKUNG Abhängig von der Rechtsprechung und der jeweiligen Gesetzgebung zum Datenschutz und zum Schutz personenbezogener Daten kann im Englischen anstelle der Benennung „PII principal" auch das Synonym „data subject" verwendet werden.

2.12
pbD-Verarbeiter
(en: PII processor)
Datenschutz-Akteur, der personenbezogene Daten (pbD) im Auftrag eines pbD-Beauftragten sowie in Übereinstimmung mit dessen Anweisungen verarbeitet

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29100:2020-03

2.13
Datenschutzverletzung
Situation, in der personenbezogene Daten unter Nichteinhaltung einer oder mehrerer relevanter Anforderungen an den Schutz der Privatsphäre verarbeitet werden

2.14
Steuerungsmaßnahmen für den Datenschutz
Maßnahmen, durch die Datenschutzrisiken behandelt werden, indem ihre Wahrscheinlichkeit oder ihre Folgen verringert werden

ANMERKUNG 1 Steuerungsmaßnahmen für den Datenschutz beinhalten organisatorische, physische und technische Maßnahmen, z. B. Richtlinien, Verfahren, Leitfäden, Verträge, Managementpraktiken oder Organisationsstrukturen.

ANMERKUNG 2 Steuerung wird auch als Synonym für Vorkehrungen oder Gegenmaßnahmen verwendet.

2.15
Technologie zum Schutz personenbezogener Daten
PET
(en: privacy enhancing technology)
Steuerungsmaßnahme für den Datenschutz, bestehend aus Maßnahmen, Produkten oder Dienstleistungen der Informations- und Kommunikationstechnik (IKT), die die Privatsphäre schützen, indem die personenbezogenen Daten (pbD) eliminiert oder reduziert werden, oder indem eine unnötige und/oder unerwünschte Verarbeitung von pbD verhindert wird, ohne dass die Funktionsweise des IKT-Systems verlorengeht

ANMERKUNG 1 Beispiele für PET sind unter anderem Anonymisierungs- und Pseudonymisierungswerkzeuge, die pbD eliminieren, reduzieren, maskieren oder de-identifizieren oder die eine unnötige, unbefugte und/oder unerwünschte Verarbeitung von pbD verhindern.

ANMERKUNG 2 Maskieren ist der Prozess, mit dem pbD-Elemente verdeckt werden.

2.16
Datenschutzrichtlinie
allgemeine Absicht und Richtung, Regeln und Verpflichtungen, so wie sie vom pbD-Beauftragten für die Verarbeitung von pbD in einem bestimmten Rahmen formal formuliert wurden

2.17
Datenschutzpräferenzen
spezifische Entscheidungen, die eine betroffene Person darüber trifft, wie ihre pbD für einen bestimmten Zweck verarbeiten werden soll

2.18
Datenschutzprinzipien
eine Reihe gemeinsamer Werte für den Schutz personenbezogener Daten (pbD) in Systemen der Informations- und Kommunikationstechnik

2.19
Datenschutzrisiken
Auswirkung von Unsicherheit auf den Schutz personenbezogener Daten

ANMERKUNG 1 Risiko wird in ISO Guide 73 und ISO 31000 als „Auswirkung von Unsicherheit auf Ziele“ definiert.

ANMERKUNG 2 Unsicherheit ist der Zustand des auch teilweisen Fehlens von Daten im Hinblick auf das Verständnis eines Ereignisses oder Wissen über ein Ereignis, seine Folgen oder seine Wahrscheinlichkeit.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29100:2020-03

2.20
Datenschutz-Risikobeurteilung
Gesamtprozess von Risikoidentifizierung, Risikoanalyse und Risikobewertung hinsichtlich der Verarbeitung personenbezogener Daten (pbD)

ANMERKUNG Dieser Prozess ist auch als Datenschutz-Folgenabschätzung bekannt.

2.21
Datenschutzanforderungen
Reihe von Anforderungen, die eine Organisation bei der Verarbeitung personenbezogener Daten (pbD) hinsichtlich des Schutzes personenbezogener Daten berücksichtigen muss

2.22
Datenschutz-Akteur
natürliche oder juristische Person, Behörde, Agentur oder jegliche andere Stelle, welche eine mit der Verarbeitung personenbezogener Daten (pbD) zusammenhängende Entscheidung oder Tätigkeit beeinflussen kann oder durch eine solche Entscheidung oder Aktivität betroffen ist oder sich dadurch betroffen fühlen kann

2.23
Verarbeitung von personenbezogenen Daten
(en: processing of PII)
Operation oder Reihe von Operationen, die auf personenbezogene Daten (pbD) angewendet wird

ANMERKUNG Beispiele für Vorgänge zur Verarbeitung von pbD sind unter anderen: die Erhebung, Speicherung, Änderung, Auswertung, Hinzuziehung, Offenlegung, Anonymisierung, Pseudonymisierung, Verbreitung oder sonstige Verfügbarmachung, Löschung oder Zerstörung von pbD.

2.24
Pseudonymisierung
Prozess, der auf personenbezogene Daten (pbD) angewendet wird und bei dem identifizierende Daten durch einen Aliasnamen ersetzt werden

ANMERKUNG 1 Eine Pseudonymisierung kann durch die betroffenen Personen selbst oder durch pbD-Beauftragte erfolgen. Eine Pseudonymisierung kann von betroffenen Personen verwendet werden, um eine Ressource oder einen Dienst konsistent zu nutzen, ohne dieser Ressource oder diesem Dienst (oder verschiedenen Diensten) ihre Identität offenzulegen, wobei sie jedoch für diese Verwendung verantwortlich gemacht werden.

ANMERKUNG 2 Eine Pseudonymisierung schließt die Möglichkeit nicht aus, dass es neben dem pbD-Beauftragten (eine eingeschränkte Reihe von) Datenschutz-Akteure(n) der pseudonymisierten Daten gibt, die die Identität der betroffenen Person auf der Grundlage des Aliasnamens und der damit verbundenen Daten ermitteln können.

2.25
sekundäre Nutzung
die Verarbeitung personenbezogener Daten (pbD) unter Bedingungen, die von den ursprünglichen Bedingungen abweichen

ANMERKUNG Bedingungen, die von den ursprünglichen Bedingungen abweichen, könnten zum Beispiel ein neuer Zweck für die Verarbeitung der pbD, ein neuer Empfänger der pbD usw. sein.

2.26
sensible pbD
Kategorie personenbezogener Daten (pbD), die entweder ihrer Art nach sensibel sind, wie z. B. solche, die sich auf den intimsten Bereich der betroffenen Personen beziehen, oder die einen erheblichen Einfluss auf die betroffene Person haben könnten

ANMERKUNG In einigen Rechtsprechungen oder in spezifischen Kontexten werden sensible pbD unter Bezugnahme auf die Art der pbD definiert und können aus pbD bestehen, die die ethnische Herkunft, politische Meinungen oder religiöse oder andere Überzeugungen, geschützte Daten zu Gesundheit, Sexualleben oder strafrechtlichen Verurteilungen sowie andere pbD, die als sensibel definiert werden könnten, offenbaren.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 29100:2020-03

2.27
Dritter
Datenschutz-Akteur, bei dem es sich nicht um die betroffene Person, den pbD-Beauftragten und den pbD-Verarbeiter sowie die natürlichen Personen, die zur Verarbeitung der Daten im Auftrag des pbD-Beauftragten oder des pbD-Verarbeiters ermächtigt sind, handelt

3 Symbole und Abkürzungen

Die folgenden Abkürzungen sind in ISO/IEC 29100 üblich.

IKT Informations- und Kommunikationstechnik (en: Information and Communication Technology, ICT)

PET Technologie zum Schutz personenbezogener Daten (en: Privacy Enhancing Technology)

pbD personenbezogene Daten (en: Personally Identifiable Information, PII)

4 Grundlegende Elemente des Rahmenwerks für Datenschutz

4.1 Überblick über das Rahmenwerk für Datenschutz

Die folgenden Komponenten beziehen sich auf den Schutz und die Verarbeitung von pbD in IKT-Systemen und bilden den in dieser Internationalen Norm beschriebenen Rahmen für den Datenschutz:

— Akteure und Rollen;

— Interaktionen;

— Erkennen von pbD;

— Datenschutzanforderungen;

— Datenschutzrichtlinien;

— Steuerungsmaßnahmen für den Datenschutz.

Bei der Entwicklung dieses Rahmenwerks für Datenschutz wurden Begriffe, Definitionen und Empfehlungen aus anderen offiziellen Quellen berücksichtigt. Diese Quellen sind im ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 (WG 5 SD2) – *Official Privacy Documents References* [3] zu finden.

4.2 Akteure und Rollen

Für die Zwecke dieser Norm ist es wichtig, die Akteure bei der Verarbeitung von pbD zu identifizieren. Es gibt vier Arten von Akteuren, die an der Verarbeitung von pbD beteiligt sein können: betroffene Personen, pbD-Beauftragte, pbD-Verarbeiter und Dritte.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 29100:2020-03