Belgische Norm

ISO/IEC 29100:2011
ISO/IEC 29100:2011/Amd 1:2018
EN ISO/IEC 29100:2020
NBN EN ISO/IEC 29100:2020

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

Gültig ab 29-07-2020

ICS: 35.030

Bureau for Standarisation
Jozef II-straat 40 bus 6
1000 Brussel

T. +32 2 738 01 11
F. +32 2 733 42 64
info@nbn.be

BTW BE0880.857.592
IBAN BE41 0003 2556 2110
BIC Code BPOTBEB1

www.nbn.be

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 29100

Juni 2020

ICS 35.030

Deutsche Fassung

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

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

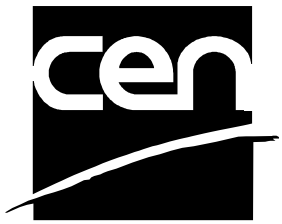
Technologies de l'information - Techniques de sécurité - Cadre privé (ISO/IEC 29100:2011, y compris Amd 1:2018)

Diese Europäische Norm wurde vom CEN am 31. 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

Bilder

Tabellen

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) erarbeitet und als EN ISO/IEC 29100:2020 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 Dezember 2020, und etwaige entgegenstehende nationale Normen müssen bis Dezember 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 29100:2011, einschließlich Amd 1:2018, wurde von CEN als EN ISO/IEC 29100:2020 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.

Internationale Normen werden in Übereinstimmung mit den Gestaltungsregeln 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 gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security techniques,* erarbeitet.

Vorwort der Änderung 1

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 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.

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 diesem Dokument 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.

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. Dieses Dokument ist jedoch weder als globale Modellrichtlinie noch als gesetzliches Rahmenwerk vorgesehen.

1 Anwendungsbereich

Diese Internationale Norm enthält ein Rahmenwerk für Datenschutz, das

— eine gemeinsame Terminologie zum Datenschutz festlegt,

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

— Überlegungen zum Datenschutz 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 von der verantwortlichen Stelle 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

zurückgezogen