ILNAS

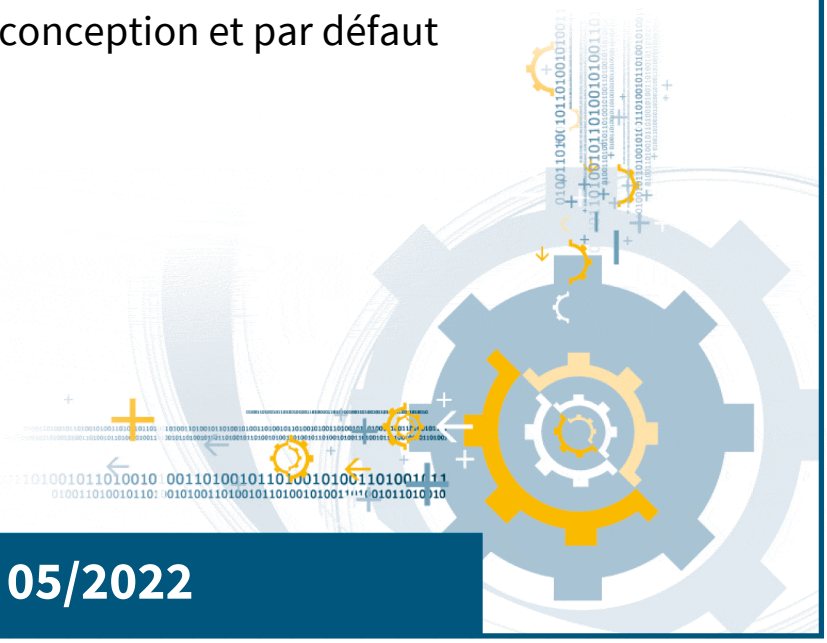
Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN 17529:2022

Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Data protection and privacy by design and by default

Protection des données et de la vie privée dès la conception et par défaut



05/2022

Nationales Vorwort

Diese Europäische Norm EN 17529:2022 wurde als luxemburgische Norm ILNAS-EN 17529:2022 übernommen.

Alle interessierten Personen, welche Mitglied einer luxemburgischen Organisation sind, können sich kostenlos an der Entwicklung von luxemburgischen (ILNAS), europäischen (CEN, CENELEC) und internationalen (ISO, IEC) Normen beteiligen:

- Inhalt der Normen beeinflussen und mitgestalten
- Künftige Entwicklungen vorhersehen
- An Sitzungen der technischen Komitees teilnehmen

https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html

EUROPÄISCHE NORM
EUROPEAN STANDARD
NORME EUROPÉENNE

EN 17529

Mai 2022

ICS 35.030

Deutsche Fassung

Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Data protection and privacy by design and by default

Protection des données et de la vie privée dès la conception et par défaut

Diese Europäische Norm wurde vom CEN am 5. Dezember 2021 angenommen.

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

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

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

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

Inhalt

Seite

Europäisches Vorwort

Dieses Dokument (EN 17529:2022) wurde von WG 5 „Datensicherheit, Datenschutz und Identitätsmanagement“ des Technischen Komitees CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis November 2022, und etwaige entgegenstehende nationale Normen müssen bis November 2022 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.

Dieses Dokument wurde im Rahmen des Arbeitsprogramms von CEN/CLC/JTC 13 erarbeitet, und zwar nicht nur als erstes Ergebnis des Normungsauftrags M/530, der von der Europäischen Kommission an CEN und CENELEC erteilt wurde, sondern auch mit dem Ziel, generisch genug zu sein, damit es auf eine Vielzahl anderer Bereiche außer der Sicherheitsindustrie, die im Fokus des Normungsauftrags stand, anwendbar ist.

Zum Zusammenhang mit EU-Verordnungen siehe informativen Anhang ZA, der Bestandteil dieses Dokuments ist.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

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.

Einleitung

0.1 Allgemeines

Dieses Dokument stellt den Entwicklern von Komponenten und Teilsystemen einen frühzeitig formalisierten Prozess zur Identifizierung von Datenschutzzielsetzungen und -anforderungen sowie die notwendige Anleitung für die damit verbundene Abschätzung bereit. Darüber hinaus bietet es Unterstützung für das Verständnis der kaskadierten Haftung und Verpflichtung von Herstellern und Diensterbringern (Verweisung auf DSGVO, insbesondere auf Artikel 25 sowie auf die für staatliche Anwendungen geltenden Regeln).

Die Datenschutz-Grundverordnung beauftragt in Art. 25 die für die Datenverarbeitung Verantwortlichen und implizit die Hersteller mit der Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.

Ziel dieses Dokuments ist es, den Herstellern und/oder Diensterbringern Anforderungen an die Hand zu geben, damit sie Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (DSTV) frühzeitig in der Entwicklung ihrer Produkte und Dienste umsetzen, d. h. vor (oder unabhängig von) einer bestimmten Anwendungsintegration, um sicherzustellen, dass sie im Hinblick auf die zu erwartenden Märkte möglichst datenschutzfähig sind.

Das Qualitätsmanagementsystem nach EN ISO 9001 bietet einen Prozessrahmen, durch den Produkte und Dienstleistungen den Datenschutz und den Schutz der Privatsphäre durch Technikgestaltung berücksichtigen können. Anhang C zeigt, wie EN ISO 9001 für die Anwendung in diesem Bereich interpretiert und gegebenenfalls erweitert werden kann. Aus der Datenschutz-Grundverordnung wurden Maßnahmenziele und Anforderungen abgeleitet, die der Komponentenhersteller bzw. der Anbieter von Software-Teilsystemen oder Subdiensten möglicherweise ansprechen möchte. Diese Abschnitte sind auf den B2B-Markt anwendbar, da Hersteller, die diese Teilkomponenten in größeren Systemen zusammensetzen, die Grenzen und Fähigkeiten jeder Komponente als Teil ihres Systemdesigns verstehen müssen. Schließlich wird ein Mechanismus zur Eigenerklärung festgelegt, der von Komponentenherstellern und Diensterbringern im Rahmen ihrer Attestierung von Fähigkeiten, Schutzmaßnahmen und Einschränkungen dieser Komponente oder dieses Dienstes gegenüber Systemintegratoren verwendet werden kann.

Für einige Zwecke der Verarbeitung und für einige Kategorien personenbezogener Daten muss eine Datenschutz-Folgenabschätzung (DSFA) nach EN ISO/IEC 29134 durchgeführt werden, und zusätzlich zu den in diesem Dokument aufgeführten Anforderungen muss auch der aus der DSFA resultierende Behandlungsplan erfüllt werden.

Dieses Dokument ist für die Verwendung durch Hersteller, Lieferanten, Hard- und Softwareentwickler bestimmt, die Produkte und Dienste für Systemintegratoren bereitstellen, die ihrerseits beabsichtigen, Produkte und Dienste für die Verwendung durch für die Datenverarbeitung Verantwortliche und Auftragsverarbeiter anzubieten. Es ermöglicht Systemintegratoren, die Angebote von Teilsystem- und Komponentenlieferanten und -herstellern auszuwählen und richtig zu nutzen, wenn sie Systeme entwickeln, die möglicherweise Datenschutzanforderungen haben.

0.2 Kompatibilität mit Managementsystemnormen

Dieses Dokument wendet das von CEN/CENELEC und ISO entwickelte Rahmenwerk an, um die Angleichung zwischen ihren Managementsystemnormen zu verbessern. Dieses Dokument selbst stellt jedoch keine Managementsystemnorm dar.

Dieses Dokument unterstützt eine Organisation dabei, ihre Entwicklungsüberlegungen zum Datenschutz an die Anforderungen von Managementsystemnormen anzugleichen oder sie entsprechend zu integrieren.

1 Anwendungsbereich

Dieses Dokument legt Anforderungen an Hersteller und/oder Diensterbringer fest, Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (DSTV) frühzeitig in der Entwicklung ihrer Produkte und Dienste umzusetzen, d. h. vor (oder unabhängig von) einer bestimmten Anwendungsintegration, um sicherzustellen, dass sie so datenschutzfähig wie möglich sind. Dieses Dokument ist anwendbar für alle Wirtschaftszweige, einschließlich der Sicherheitsindustrie.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

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

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

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

3.1.1
Datenschutz durch Technikgestaltung
technische und organisatorische Maßnahmen zur Umsetzung der Datenschutzgrundsätze

Anmerkung 1 zum Begriff: Die Maßnahmen müssen in wirksamer Weise implementiert und die erforderlichen Schutzvorkehrungen in der Verarbeitung getroffen werden.

3.1.2
Datenschutz durch datenschutzfreundliche Voreinstellungen
technische und organisatorische Maßnahmen, um sicherzustellen, dass nur solche personenbezogenen Daten, die für jeden spezifischen Zweck der Verarbeitung notwendig sind, verarbeitet werden

Anmerkung 1 zum Begriff: Solche Maßnahmen sollten mindestens die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, die Speicherfrist und ihre Zugänglichkeit umfassen.

3.1.3
Datenschutz-Folgenabschätzung
DSFA
Gesamtprozess aus Identifizieren, Analysieren, Bewerten, Beraten, Kommunizieren und Planen der Behandlung von möglichen Datenschutzfolgen unter Bezug auf die Verarbeitung personenbezogener Daten, eingebettet in das unternehmensweite Rahmenwerk zum Risikomanagement

Anmerkung 1 zum Begriff: Basierend auf ISO/IEC 29134:2017, 3.7.

3.1.4
datenschutzbewusst
Attribut eines Produkts oder Dienstes für die Verarbeitung personenbezogener Daten, was bedeutet, dass die Datenschutzanforderungen bei der Technikgestaltung und Vorkonfiguration berücksichtigt wurden und datenschutzwidrige funktionale Anforderungen nur insoweit gestellt wurden, wie dies für den beabsichtigten Zweck des Produkts oder Dienstes unerlässlich ist