ILNAS-EN 17529:2022 - Preview only Copy via ILNAS e-Shop

ILNAS

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

ILNAS-EN 17529:2022

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

Data protection and privacy by design and by default

Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

05/2022

Avant-propos national

Cette Norme Européenne EN 17529:2022 a été adoptée comme Norme Luxembourgeoise ILNAS-EN 17529:2022.

Toute personne intéressée, membre d'une organisation basée au Luxembourg, peut participer gratuitement à l'élaboration de normes luxembourgeoises (ILNAS), européennes (CEN, CENELEC) et internationales (ISO, IEC) :

- Influencer et participer à la conception de normes
- Anticiper les développements futurs
- Participer aux réunions des comités techniques

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

ILNAS-EN 17529:2022 - Preview only Copy via ILNAS e-Shop

CETTE PUBLICATION EST PROTÉGÉE PAR LE DROIT D'AUTEUR
Aucun contenu de la présente publication ne peut être reproduit ou utilisé sous quelque forme ou par quelque procédé que ce soit - électronique, mécanique, photocopie ou par d'autres moyens sans autorisation préalable !

NORME EUROPÉENNE

EUROPÄISCHE NORM

EUROPEAN STANDARD

EN 17529

Mai 2022

ICS 35.030

Version Française

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

Datenschutz by Design und als Grundeinstellung

Data protection and privacy by design and by default

La présente Norme européenne a été adoptée par le CEN le 5 décembre 2021.

Les membres du CEN et CENELEC sont tenus de se soumettre au Règlement Intérieur du CEN/CENELEC, qui définit les conditions dans lesquelles doit être attribué, sans modification, le statut de norme nationale à la Norme européenne. Les listes mises à jour et les références bibliographiques relatives à ces normes nationales peuvent être obtenues auprès du Centre de Gestion du CEN-CENELEC ou auprès des membres du CEN et CENELEC.

La présente Norme européenne existe en trois versions officielles (allemand, anglais, français). Une version dans une autre langue faite par traduction sous la responsabilité d'un membre du CEN et CENELEC dans sa langue nationale et notifiée au Centre de Gestion du CEN-CENELEC, a le même statut que les versions officielles.

Les membres du CEN et du CENELEC sont les organismes nationaux de normalisation et les comités électrotechniques nationaux des pays suivants: Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République de Macédoine du Nord, République de Serbie, République Tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Suisse et Turquie.

ILNAS-EN 17529:2022 - Preview only Copy via ILNAS e-Shop

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

© 2022 CEN/CENELEC Tous droits d'exploitation sous quelque forme et de quelque manière que ce soit réservés dans le monde entier aux membres nationaux du CEN et aux membres du CENELEC.

Sommaire

Page

Avant-propos européen 4
Introduction 5
1 Domaine d'application 7
2 Références normatives 7
3 Termes, définitions et abréviations 7
3.1 Termes et définitions 7
3.2 Abréviations 8
4 Généralités 8
4.1 Mise en place des bases pour une protection des données et de la vie privée dès la conception et par défaut 8
4.2 Structure pour la décomposition des produits et services en catégories applicables 10
4.2.1 Introduction 10
4.2.2 Décomposition des produits 10
4.2.3 Décomposition des services 11
4.3 Autodéclaration et niveaux de réalisation 12
5 Développement de produits et services conçus en prenant en compte le respect de la vie privée 14
5.1 Leadership et connaissance du marché 14
5.2 Préparation 15
5.3 Conception 15
5.3.1 Détermination des exigences en matière de DPPbDD 15
5.3.2 Développement 17
5.3.3 Production et prestation de service 17
5.3.4 Mise sur le marché des produits et services 17
5.4 Évaluation des performances 17
5.5 Amélioration 17
6 Exigences relatives à la capacité de protection des données applicables à la conception des produits et des services 18
6.1 Accès 18
6.1.1 Accès aux données 18
6.1.2 Copie de données 18
6.2 Responsabilité 19
6.3 Exactitude 19
6.4 Désidentification des données 21
6.5 Minimisation des données 22
6.6 Portabilité des données 23
6.7 Confidentialité 24
6.8 Suppression 26
6.9 Consentement et enfants 27
6.9.1 Détermination de l'âge de l'utilisateur 27
6.9.2 Seuil d'âge configurable pour les enfants 28
6.10 Sécurité de l'information 28

ILNAS-EN 17529:2022 - Preview only Copy via ILNAS e-Shop

6.10.1 Traitement non autorisé ou illégal 28
6.10.2 Pertes de données 31
6.10.3 Objectifs de protection de l'information 32
6.10.4 Restauration 33
6.11 Licéité 34
6.11.1 Divulgation des données 34
6.11.2 Consentement 34
6.12 Objection au traitement 34
6.13 Prise de décision automatisée 35
6.14 Restriction du traitement 36
6.15 Limitation du stockage 37
6.16 Transparence 38
6.16.1 Informations 38
6.16.2 Enregistrement des activités de traitement 41

7 Exigences relatives à l'autodéclaration d'une conception qui tient compte de la protection de la vie privée 42
7.1 Exigences relatives aux processus 42
7.1.1 Préparation fondée sur les exigences applicables aux composantes des produit et éléments de service 42
7.1.2 Considérations supplémentaires relatives aux DPIA 42
7.1.3 Détermination du niveau de réalisation 43
7.2 Notification d'autodéclaration 44

Annexe A (informative) Mise en correspondance de l'applicabilité entre les exigences de l'Article 6 et les composantes ou éléments 45

Annexe B (informative) Approche en vue d'une spécification 58

Annexe C (informative) Lignes directrices relatives à l'EN ISO 9001 61

Annexe ZA (informative) Relation entre la présente Norme européenne et les exigences concernées de protection des données dès la conception et par défaut du Règlement UE 2016/679 66

Bibliographie 68

ILNAS-EN 17529:2022 - Preview only Copy via ILNAS e-Shop

Avant-propos européen

Le présent document (EN 17529:2022) a été élaboré par le GT 5 « Gestion de l'identité, de la protection de la vie privée et des données » du CEN/CENELEC JTC 13 « Cybersécurité et protection des données », dont le secrétariat est tenu par le DIN.

Cette Norme européenne devra recevoir le statut de norme nationale, soit par publication d'un texte identique, soit par entérinement, au plus tard en novembre 2022, et toutes les normes nationales en contradiction devront être retirées au plus tard en novembre 2022.

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. Le CEN ne saurait être tenu pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

Le présent document a été élaboré dans le cadre du programme de travail du CEN/CLC/JTC 13, non seulement en tant que premier livrable requis par le mandat M/530 donné au CEN et au CENELEC par la Commission européenne, mais aussi pour être suffisamment générique pour s'appliquer à une variété de domaines autres que l'industrie de la sécurité, qui était au cœur du mandat.

Pour la relation avec le ou les Règlements UE, voir l'Annexe ZA informative, qui fait partie intégrante du présent document.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve sur le site web du CEN.

Selon le Règlement intérieur du CEN/CENELEC, les organismes de normalisation nationaux des pays suivants sont tenus de mettre cette Norme européenne en application : Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République de Macédoine du Nord, République Tchèque, Roumanie, Royaume-Uni, Serbie, Slovaquie, Slovénie, Suède, Suisse et Turquie.

ILNAS-EN 17529:2022 - Preview only Copy via ILNAS e-Shop

Introduction

0.1 Généralités

Le présent document fournit aux développeurs de composants et de sous-systèmes un processus formalisé disponible dès l'origine pour identifier les objectifs et les exigences en matière de protection de la vie privée, ainsi que les recommandations nécessaires à l'évaluation associée. Il fournit en outre une aide à la compréhension de la responsabilité et des obligations en cascade des fabricants et des fournisseurs de services (référence au RGPD et, le cas échéant, référence à l'Article 25, ainsi qu'aux règles applicables aux applications gouvernementales).

Le règlement général sur la protection des données (RGPD), dans son article vingt-cinq, charge les responsables du traitement des données, et implicitement les fabricants, de mettre en œuvre la protection des données, dès la conception et par défaut.

L'objectif du présent document est de préciser les exigences auxquelles doivent se conformer les fabricants et/ou les fournisseurs de services pour mettre en œuvre la protection des données et de la vie privée dès la conception et par défaut (Data protection and Privacy by Design and by Default, DPPbDD), dès le début du développement de leurs produits et services, c'est-à-dire avant (ou indépendamment de) toute intégration dans une application spécifique, afin de s'assurer qu'ils sont aussi prêts que possible à respecter la vie privée sur les marchés visés.

Le système de management de la qualité de l'EN ISO 9001 fournit un cadre au processus par lequel les produits et services peuvent prendre en compte la protection des données et de la vie privée dès leur conception. L'Annexe C précise comment l'EN ISO 9001 peut être interprétée et étendue pour être utilisée dans ce domaine, si nécessaire. Des objectifs et exigences de contrôle, que le fabricant de composants ou le fournisseur de sous-services ou de sous-systèmes logiciels peut choisir de mettre en œuvre, ont été dérivés du règlement général sur la protection des données. Ces clauses sont applicables au marché du B2B, puisque les fabricants qui intègrent ces sous-ensembles dans des systèmes plus importants devront tenir compte des limites et des capacités de chaque composant, dans le cadre de la conception de leur système. Enfin, un mécanisme d'autodéclaration est spécifié. Ce mécanisme peut être utilisé par les fabricants de composants et les fournisseurs de services afin d'attester auprès des intégrateurs des capacités, protections et limitations de ces composants ou services.

À certaines fins de traitement et pour certaines catégories de données à caractère personnel, une évaluation d'impact de la protection des données (data protection impact assessment, DPIA) selon l'EN ISO/IEC 29134 doit être réalisée et, outre les exigences spécifiées dans le présent document, le plan de traitement résultant de la DPIA doit également être mis en œuvre.

Le présent document est destiné à être utilisé par des fabricants, des fournisseurs, des développeurs de matériel et de logiciels fournissant des produits et des services aux intégrateurs de systèmes qui ont, eux-mêmes, vocation à offrir des produits et des services destinés à être utilisés par des responsables de traitement des données et des sous-traitants de données. Il permet aux intégrateurs de systèmes de sélectionner et d'utiliser correctement les offres des fournisseurs et des fabricants de sous-systèmes et de composants, lors du développement de systèmes pouvant être soumis à des exigences en matière de protection des données.

ILNAS-EN 17529:2022 - Preview only Copy via ILNAS e-Shop

0.2 Compatibilité avec les normes de systèmes de management

Le présent document applique le cadre élaboré par le CEN/CENELEC et l'ISO afin d'améliorer l'harmonisation entre ses normes de systèmes de management. Toutefois, ce document ne constitue pas en lui-même une norme de système de management.

Le présent document permet aux organisations d'aligner ou d'intégrer leurs considérations de développement relatives à la protection des données sur les exigences des normes de systèmes de management.

ILNAS-EN 17529:2022 - Preview only Copy via ILNAS e-Shop

1 Domaine d'application

Le présent document spécifie les exigences auxquelles doivent se conformer les fabricants et/ou les fournisseurs de services pour mettre en œuvre la protection des données et de la vie privée dès la conception et par défaut (DPPbDD) dès le début du développement de leurs produits et services, c'est-à-dire avant (ou indépendamment de) toute intégration dans une application spécifique, afin de s'assurer qu'ils sont aussi prêts que possible à respecter la vie privée. Le document s'applique à l'ensemble des secteurs d'activité, y compris à celui de la sécurité.

2 Références normatives

Le présent document ne contient aucune référence normative.

3 Termes, définitions et abréviations

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

— IEC Electropedia : disponible à l'adresse https://www.electropedia.org/

— ISO Online browsing platform : disponible à l'adresse https://www.iso.org/obp

3.1.1
protection des données dès la conception
mesures techniques et organisationnelles conçues en vue de mettre en œuvre les principes de la protection des données

Note 1 à l'article : Les mesures doivent être mises en œuvre de manière efficace et intégrer les moyens de protection nécessaires dans le traitement.

3.1.2
protection des données par défaut
mesures techniques et organisationnelles conçues afin de garantir que seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées

Note 1 à l'article : Il convient que de telles mesures couvrent au moins le volume des données à caractère personnel collectées, l'étendue de leur traitement, leur période de stockage et leur accessibilité.

3.1.3
évaluation d'impact de la protection des données
DPIA [data protection impact assessment]
processus global visant à identifier, analyser, évaluer, consulter, communiquer et planifier le traitement des impacts potentiels sur la vie privée au regard du traitement des données à caractère personnel, dans le cadre plus large du système de management des risques d'une organisation

Note 1 à l'article : Adapté de l'ISO/IEC 29134:2017, 3.7.

3.1.4
conçu en prenant en compte le respect de la vie privée
attribut d'un produit ou d'un service utilisé pour le traitement des données à caractère personnel, indiquant que les exigences en matière de protection des données ont été prises en compte lors de la conception et de la préconfiguration, et que les exigences fonctionnelles défavorables à la vie privée n'ont été inclues que dans la mesure où elles étaient nécessaires à la finalité prévue du produit ou du service

ILNAS-EN 17529:2022 - Preview only Copy via ILNAS e-Shop