ILNAS

Institut luxembourgeois de la normalisation de l'accréditation, de la sécurité et qualité des produits et services
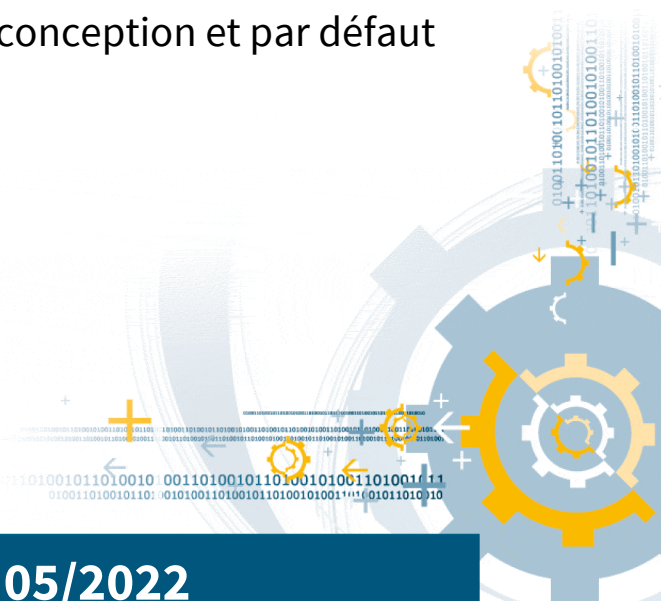
ILNAS-EN 17529:2022

Data protection and privacy by design and by default

Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

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

05/2022

National Foreword

This European Standard EN 17529:2022 was adopted as Luxembourgish Standard ILNAS-EN 17529:2022.

Every interested party, which is member of an organization based in Luxembourg, can participate for FREE in the development of Luxembourgish (ILNAS), European (CEN, CENELEC) and International (ISO, IEC) standards:

- Participate in the design of standards
- Foresee future developments
- Participate in technical committee meetings

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

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 17529

May 2022

ICS 35.030

English version

Data protection and privacy by design and by default

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

Datenschutz by Design und als Grundeinstellung

This European Standard was approved by CEN on 5 December 2021.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

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

Ref. No. EN 17529:2022 E

Contents

Page

European foreword

This document (EN 17529:2022) has been prepared by WG 5 "Data Protection, Privacy and Identity Management" of the CEN/CENELEC JTC 13 "Cybersecurity and Data Protection", the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by November 2022, and conflicting national standards shall be withdrawn at the latest by November 2022.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document has been prepared as part of CEN/CLC JTC 13 work programme, not only as the first deliverable called by mandate M/530 given to CEN and CENELEC by the European Commission, but also to be generic enough to be applicable to a variety of domains other than the security industry, which was in focus of the mandate.

For relationship with EU Regulation(s), see informative Annex ZA, which is an integral part of this document.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN website.

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

0.1 General

This document provides the component and subsystems developers with an early formalized process for identification of privacy objectives and requirements, as well as the necessary guidance on associated assessment. It further provides support for understanding the cascaded liability and obligation of manufacturers and service providers (Reference to GDPR and as applicable reference to Article 25, as well as to rules applicable to governmental applications).

The General Data Protection Regulation, in its Art. Twenty-five charges data controllers, and implicitly manufacturers, with implementing Data Protection by design and by default.

The aim of this document is to give requirements to manufacturers and/or service providers to implement Data protection and Privacy by Design and by Default (DPPbDD) early in the development of their products and services, i.e. before (or independently of) any specific application integration, to make sure that they are as privacy ready as possible with regard to the anticipated markets.

The quality management system of EN ISO 9001 provides a process framework through which products and services can incorporate Data protection and privacy by design. Annex C shows how EN ISO 9001 can be interpreted and extended for use in this domain where necessary. Control objectives and requirements have been derived from the General Data Protection Regulation, which the component manufacturer or software sub-systems or sub-service provider may choose to address. These clauses are applicable to the B2B market, since manufacturers composing these sub-components in larger systems will need to understand the limits and capabilities of each component, as part of their system design. Finally, a self-declaration mechanism is specified which can be used by component manufacturers and service providers as part of their attestation to system integrators of the capabilities, protections and limitations of that component or service.

For some purposes of processing and for some categories of personal data, a data protection impact assessment (DPIA) according to EN ISO/IEC 29134 needs to be conducted and in addition to the requirements given in this document, the treatment plan resulting from the DPIA needs to be fulfilled as well.

This document is intended to be used by manufacturers, suppliers, hard- and software developers providing products and services to system integrators who themselves intend to offer products and services to be used by data controllers and data processors. It allows system integrators to select and correctly use the offerings of sub-system and component suppliers and manufacturers when developing systems that may have data protection requirements.

0.2 Compatibility with management system standards

This document applies the framework developed by CEN/CENELEC and ISO to improve alignment among its Management System Standards. However, this document itself does not represent a Management System standard.

This document supports an organization to align or integrate its development considerations on data protection with the requirements of Management System standards.

1 Scope

This document specifies requirements for manufacturers and/or service providers to implement Data protection and Privacy by Design and by Default (DPPbDD) early in their development of their products and services, i.e. before (or independently of) any specific application integration, to make sure that they are as privacy ready as possible. This document is applicable to all business sectors, including the security industry.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the following term and definitions apply.

— IEC Electropedia: available at https://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1.1
data protection by design
technical and organizational measures designed to implement data protection principles

Note 1 to entry: The measures shall be implemented in an effective manner and to integrate the necessary safeguards into the processing.

3.1.2
data protection by default
technical and organizational measures for ensuring that only personal data which are necessary for each specific purpose of the processing are processed

Note 1 to entry: Such measures should cover at least the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

3.1.3
data protection impact assessment
DPIA
overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of personal data, framed within an organization's broader risk management framework

Note 1 to entry: Adapted from ISO/IEC 29134:2017, 3.7.

3.1.4
privacy-aware
attribute of a product or service for the processing of personal data, meaning that data protection requirements were considered in the design and pre-configuration and that privacy adverse functional requirements were only made as far as necessary for the intended purpose of the product or service

3.1.5
special categories of personal data
data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

[SOURCE: GDPR Article 9, Clause 1]

3.2 Abbreviated terms

DPPbDD   Data protection and Privacy by Design and by Default

DPIA   Data protection impact assessment

GDPR   EU General Data Protection Regulation 679/2016

GSMA   Global system of mobile communication association

ISACA   Information Systems Audit and Control Association

LoA   Level of Achievement

4 General

4.1 Preparing the grounds for data protection and privacy by design and by default

Alongside the broadly formulated expectations in terms of protecting personal data during data processing procedures, data protection and privacy by design and by default relate to the ability of the intended technical systems and components to be able to support this protection. Reference is made to consideration reason 78, sentence 4 for adopting of the GDPR. Yet, manufacturers do not have an obligation under the GDPR. Other instruments are therefore required to guide them in a process through which their products or services are designed to be data protection and privacy by design and default friendly for a maximum of use cases, as per the anticipated market. An underlying set of requirements consistent with the company's quality process is detailed hereafter. Anticipated benefits are for the end-users (customers/data controllers) ease to implement their privacy duties and for the manufacturer a competitive edge.

The GDPR contains many legal provisions for consideration by data controllers and processors; such provisions rely largely on the diverse functional and operational conditions in which it is anticipated that the product or service will be used. In this context and to support the providers of products and services in their assessment, the obligations of data controllers were generically analysed to determine whether they contain, explicitly or implicitly, the need for functional capabilities in support of data controllers' obligations.

The following principles are expected for data protection and privacy by design and by default:

1) DPPbDD should be proactive and preventative, not reactive and remedial.

2) Default settings and configuration should be secure and privacy-aware.

3) Data protection and privacy should be incorporated into design.

4) DPPbDD seeks full functionality in accommodation of legitimate interests and objectives, no trade-offs.

5) DPPbDD should concern the entire data lifecycle.