EESTI STANDARD EVS-EN 17529:2022

LÕIMELINE JA VAIKELINE ANDMEKAITSE JA PRIVAATSUS

Data protection and privacy by design and by default

EESTI STANDARDI EESSÕNA	NATIONAL FOREWORD
See Eesti standard EVS-EN 17529:2022 sisaldab Euroopa standardi EN 17529:2022 ingliskeelset teksti.	This Estonian standard EVS-EN 17529:2022 consists of the English text of the European standard EN 17529:2022.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 18.05.2022.	Date of Availability of the European standard is 18.05.2022.
Standard on kättesaadav Eesti Standardimis-ja Akrediteerimiskeskusest.	The standard is available from the Estonian Centre for Standardisation and Accreditation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.030

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

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