SLOVENSKI STANDARD
SIST EN 17529:2022

01-september-2022

Varstvo podatkov in zasebnosti z načrtovanjem in kot privzeto

Data protection and privacy by design and by default

Datenschutz by Design und als Grundeinstellung

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

Ta slovenski standard je istoveten z: **EN 17529:2022**

ICS:

35.030	Informacijska varnost	IT Security

SIST EN 17529:2022 **en,fr,de**

EUROPEAN STANDARD **EN 17529**

NORME EUROPÉENNE

EUROPÄISCHE NORM 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of an identical text or by endorsement, at the latest by November 2022, and conflicting national standards shall be withdrawn at the latest by November 2022.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.

6) DPPbDD should be visible and transparent and subject to independent verification.

7) The interests of the individual should be kept uppermost by offering strong defaults, appropriate notice and be kept user-centric by offering user-friendly options, even if such provisions appear as less privacy-friendly.

8) DPPbDD controls should be effective.

9) DPPbDD measures should be designed to be robust and be able to scale up in accordance with increases in risk of breach of the data protection principles.

10) DPPdDD measures should be regularly assessed.

When understanding data protection by design in the utmost possible way, consideration needs to be given not only to the moment of supplying and providing. The whole lifecycle of both, the personal data and the product and/or service needs to be considered as well.

Special attention should be drawn to maintenance activities as well as to the general conditions, under which a reuse of products could happen. Furthermore, the service includes the operation of processing as a processor on data controllers behalf. Some requirements of this document will draw attention to this scenarios.

If the service provider needs to be seen as a data controller, additional organizational and technical measures should be put into place and be governed by an appropriated Management system, e.g. EN ISO/IEC 27701. These organizational and technical measures will be out of scope for this document.

This document provides in 4.2 a structure for splitting up integrated products and services into layers, which may be used to modulate them into building blocks that need to fulfil the same set of requirements. Any reasonable approach may be taken to describing the system architecture, provided it allows a mapping of the data protection concerns onto the architecture. When designing a major component from sub-systems and services, it may be necessary for the overarching system architecture decomposition to leverage the descriptions of the included components. Such approaches may draw on opaque or transparent models for the component elements. In 4.3 the conformity scheme for a self-declaration is provided.

In Clause 5, the requirements for an exemplar process of privacy-aware development of products and services are provided.

In Clause 6, there are basic requirements on the design of products and services provided. Application is specified to the respective product perspectives and service elements specified in 4.2 and control objectives give reference to the GDPR.

Clause 7 provides guidelines to the process of self-declaration and the requirements to determine the level of achievement.

In the Annexes A, B and C, detailed information is given on the mapping of basic requirements to product perspectives or service elements on the definition of privacy by design and on guidance for applying EN ISO 9001 as a management system to the development. Additionally, the Annex ZA contains the conformity statement for EU Mandate M/530.

4.2 Structure for disassembling product and service into applicable categories

4.2.1 Introduction

As it does not seem practical to build requirements directly for products and for services, that can highly differ in submodule assembly, architecture and bundling, a set of module categories is specified in the next two clauses. Any complex product or service under this document can be decomposed into

component parts or layers. These can be used to represent products and services. The structural decomposition is divided into product and service issues for ease of description.

4.2.2 Product perspectives

The module categories, of which a product can consist, are specified as follows:

1) Component perspective — mainly physical submodules like microprocessors and microcontrollers, DRAM-Modules, Interface controllers, media drives, physical storage media, sensors, actuators or power supply. This perspective can include connectivity drivers and small programs as e.g. for upgrading or dynamic connection.

2) Device perspective — bare bone with chassis, shielding, display, keyboards and casing. The device perspective integrates components from the component perspective and is adding programs for BIOS and boot capabilities.

3) Operating system perspective — software perspective with programs supporting the configuration of the device, the basic interaction with the user, like keyboard input and output via display or printer, the support of user authentication, the administration of the device itself and its interconnectivity with networks and with tools supporting local activities on the device.

4) Communication perspective — Connectivity components emulating physical links (wired or wireless) for the purpose of information transmission. This perspective is similar to the component perspective, but differs regarding specific concerns related with the aspect of the network it builds.

5) Storage perspective — logical perspective for the management of storage locations on connected physical storage media via the component perspective. This includes locally or remotely connected media, raid or cluster architectures, NAS or SAN concepts as well as fileservers and cloud storage.

6) User Interface perspective — logical perspective for the management of user interaction with a device or service, which is not on Operating system perspective. This perspective also includes portals and, up to a certain degree, content management systems.

7) Integrated system perspective — this perspective applies, when a product is an integration of more than one device. It requires a communication model between the devices with specified protocols and transmission management. Integrated systems are expected to demonstrate the capabilities and default settings for an appropriate network security.

8) Application perspective — software perspective providing the expected functionality of a device or an integrated system.

9) Business process perspective — logical perspective above the application perspective that is managing information exchange between many devices, integrated systems or even organizations.

10) System management perspective — logical perspective for the management of Operation and information security regarding the devices, integrated systems, applications, Storages and/or communication flows.

4.2.3 Service elements

The module categories, of which a service can consist, are specified as follows:

1) Service management element — human based service of configuration, operation control and incident response.

2) Self-service element — application service to provide the customer or the user with tools to configure other product or service elements.

3) Integration service element — customer specific service of making subsystems interoperable, normally organized within a dedicated project under a customer specified management framework.

4) Transmission service element — service that interconnects transmission lines via organizational boarders.

5) Update service element — Program code updates, these may be provided, for example, proactively by humans, reactively through an automated system, or published for downloading.

6) Cloud service element — service providing operation facilities either on infrastructure level, platform level or on application level.

7) Content service element — service providing additional data (e.g.: news, scoring figures, addresses), sometimes with the possibility to enhance collected personal data.

8) Outsourced business process element — functional data processing either customer specific or as a normalized offer to similar clients.

9) Output service element — services receiving customer data for the purpose of producing output media (e.g.: photo calendars or marketing mails).

10) Maintenance service element — service reacting on demand of users and/or customers in order to keep products and services usable over lifetime, including collect or bring-in services and device swaps.

11) Security as a service element —services evaluating systems, traffic and log entries in order to detect, prevent or react on vulnerabilities and security breaches.

12) Media recovery services element — service on customer owned physical storage media for the purpose of recovering the information contained in them.

13) Media destruction service element — physical destruction of storage media in a way that is unable for recovery of data, normally applied at the end of lifecycle.

14) System remarketing service element — service on products by cleaning, reconstruction and re-licensing in order to give the product a second life with another customer.

4.3 Self-declaration and levels of achievement

Although the consideration of data protection and privacy by design within an organization's quality management system could be seen as a prerequisite to deliver DPPbDD, it would not be sufficient to conform with the respective processes in order to build privacy-aware products and services. It is also indispensable for the product or service to conform with the specific requirements applicable to any of the perspectives the product or elements the service is built of in order to fulfil the data protection and privacy by design and by default principles.

In practice, it would be reasonable sometimes to find a trade-off between market needs or customer expressed requirements and the principles and requirements. This will lower the level of safeguarding for the data subject but will not result in a product or service that is privacy-unaware. As another example, an organization could plan to provide a product or service for the processing of special categories of data under lawful circumstances, and it applies additional measures or functions retrieved from a data

protection impact assessment. One state of being privacy-aware will not reflect the enhanced level of safeguarding needed and demonstrated by additional effort.

Suppliers of sub-components, and providers of services to system integrators, may wish to address specific data protection needs, while ignoring others. For example, a data storage component might provide guarantees w.r.t the completeness and timeliness of deletion but be intended only to hold encrypted data with no on-device decryption. As such, this device could not allow for correction of personal data, since it would be holding blocks of bits – a higher level privacy-aware service would need to replace the stored content. The self-declaration mechanism allows a component manufacturer to identify those facets of data protection that are the market focus for their product."

In order to reflect the potential for incomplete addressing of data protection concerns, the practise of trade-offs and the need for adequacy in special processing conditions, six levels of achievement have been specified in Table 1 below.

Table 1 — Definitions of achievement levels

Achievement	Sub-level achievement	Level of achievement	Prerequisites
The requirements are fully applied. No trade-offs were made. Special categories of personal data are about to be processed and additional design concerns were made accordingly.	Special categories of personal data protection and privacy are considered by design and by default.	A	Data protection impact assessment was conducted and appropriate design concerns were applied.
The requirements are fully applied. No trade-offs were made. Purpose fits to protection level.	Data protection and privacy are considered by design and by default.	B	The requirements are fully applied. No trade-offs were made. Uppermost consideration of data subject interests is confirmed.

Achievement	Sub-level achievement	Level of achievement	Prerequisites
Trade-offs were made when applying the requirements	The design is privacy-aware	C	Requirement fulfilment rate is 95 % ≤ *x* < 100 %
	The design is mostly privacy-aware	D	Requirement fulfilment rate is 80 % ≤ *x* < 95 %
	Considerations to a privacy-aware design were made in general	E	Requirement fulfilment rate is 50 % ≤ *x* < 80 %
The application of requirements is underperforming		Z	Requirement fulfilment rate is lower than 50 %

Achievements need to be demonstrated by conformance to the selected data protection capability requirements in Clause 6 and their mapping onto an architectural model of the component, service or sub-system. One approach to this is demonstrated using the example of product perspectives and/or service elements throughout this document. An equivalent mapping of data protection requirements to architectural components could be used to develop an equivalent system for sub-systems that are composed from multiple parts, or from base level components for which a non-layered (e.g. service-oriented architecture) approach is prefered. In case of some particular processing likely to result in a high risk to the rights and freedoms of the data subjects, a data protection impact assessment (DPIA) shall be conducted and the outcome shall be considered within the design as well. This DPIA shall be conducted and recorded. An example of a DPIA is provided by EN ISO/IEC 29134.

Component suppliers and sub-system service providers will be permitted to label their product or service by self-declaration as privacy-aware together with the level of achievement, to inform potential system integrators, as long as they are able to demonstrate conformance to the requirements as provided in Clause 7.

Where a component or sub-system or service is offered to system integrators with a self-declaration at achievement level C, D, E or Z, there should be accompanying documentation to assist the system integrator in understanding which data protection controls are, and are not, offered by this component.

This document focuses on B2B activity, supporting the component and subsystems developers in addressing specific data protection issues. Products and services achieving level A or B should satisfy all of the requirements laid out in Clause 6. However, those requirements do not represent all of the data protection baseline embodied by the GDPR in full detail. It should not therefore, be assumed that a level A or B self-declaration represents full satisfaction of the GDPR requirements. Further analysis would be needed, based on the actual product, before such an assessment could be justified.

5 Privacy-aware development of products and services

5.1 Leadership and market intelligence

5.1.1 The organization shall establish and maintain an understanding that data protection and privacy by design and by default are an imperative to the development and provision of any of its products and services that may potentially have privacy implications.

NOTE This means that data protection and privacy by design and by default is reflected in the senior management commitment, expressed in written policies and the respective responsibilities and accountability is allocated to the appropriate organizational roles.

5.1.2 To ensure a proper match between the variety of use cases implied by the targeted market and their implication in the activation of the GDPR provisions, the organization shall select, train and fully inform staff in charge of the process below on the GDPR, ensuring they have a comprehensive view of all the usage conditions relative to the different segments covered by the marketing plans.

NOTE This comprehensive functional view applies to all the process described in present Clause 5, keeping in mind that the privacy analysis relative to the specific procurement of a product or a system is outside the scope of this document.

5.2 Preparation

5.2.1 The organization shall determine if the product and/or service to be provided includes an active role in the processing of personal data.

NOTE An active role is to be considered, if the personal data are processed on products or services where the customer and/or user does not have the full and only control of collecting, storing, sharing and deletion of this personal data.

5.2.2 In order to address the impact of products and services on the privacy of a data subject, the organization shall specify an appropriate methodology and the structure of the impact assessment report.

NOTE EN ISO/IEC 29134 provides guidance on the privacy impact assessment

5.2.3 The organization shall provide the development units with access to sufficient human resources of the appropriate competence in legal and technical expertise in the field of privacy.

NOTE If there is appointed one for the organization, the data protection officer is expected to get involved in the design process. It is to be ensured that no conflicts of interest arise. Another option could be to have a dedicated privacy engineer role in the development unit.

5.2.4 The organization shall assess, and where necessary amend, its existing development process for the fit to the requirements of this document.

5.3 Design

5.3.1 Determination of DPPbDD requirements

5.3.1.1 Basic design requirements

5.3.1.1.1 The person responsible for the product and/or service design shall logically disassemble the intended market offer into the perspectives and elements it is composed of.

NOTE The perspectives and elements are specified in Clause 4.2.

5.3.1.1.2 For each perspective and element identified as being part of the intended market offer, all the basic requirements from Clause 6 applying to this perspective or element shall be identified.

NOTE Annex A, Tables A.1 and A.2 provides mapping tables for the applicable basic requirements to a specific product perspective or service element.

5.3.1.2 Enhanced design requirements when processing of personal data are included

5.3.1.2.1 In case the organization has confirmed to take an active role in the processing of personal data for the intended market offer, the person responsible for the product and/or service design shall consider implementing appropriate technical and organizational measures.