SLOVENSKI STANDARD
oSIST prEN 17529:2020

01-september-2020

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: **prEN 17529**

ICS:

35.030 Informacijska varnost IT Security

oSIST prEN 17529:2020 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 17529

June 2020

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 draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/CLC/JTC 13.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CEN and CENELEC 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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

Contents

Page

European foreword

This document (prEN 17529:2020) 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 document is currently submitted to the CEN Enquiry.

This document has been prepared under a mandate given to CEN and CENELEC by the European Commission and the European Free Trade Association. This project is developed as part of CEN/CLC/JTC 13 work programme in fulfilment of Standardization Request M/530.

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

Introduction

0.1 General

This document provides the component and subsystems developers with an early formalized process for identification of privacy objects 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 23, as well as to rules applicable to governmental applications).

The General Data Protection Regulation, in its Art. 25 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 (DPbDD) early in the development of their products and services, i.e. before (or independently of) any specific application or 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 is building the framework for the process to provide products and services that incorporate Data protection and privacy by design. Enhancements are made to EN ISO 9001 where necessary. Additionally, and as applicable in this preliminary generic phase for the product or service, specific control objectives and requirements were derived from the General Data Protection Regulation, the respective supplier or service provider is expected to fulfil. Finally, a self-declaration mechanism is defined to be applied, when feasible pending the variety of anticipated use cases, for accordingly designed products and services in order to provide orientation to data controllers, to data subjects and to the society.

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 get fulfilled as well.

This document is intended for the use by manufacturers, suppliers, hard- and software developers, system integrators providing products and services for the use by as data controller, and for the use by controllers when selecting products and services for data processing.

0.2 Compatibility with other management system standards

This document applies the framework developed by CEN/CENELEC and ISO to improve alignment among its Management System Standards.

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

1 Scope

This document provides requirements for manufacturers and/or service providers to implement Data protection and Privacy by Design and by Default (DPbDD) 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. The document will be applicable to all business sectors, including the security industry.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN ISO/IEC 29134, *Information technology — Security techniques — Guidelines for privacy impact assessment (ISO/IEC 29134)*

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 http://www.electropedia.org/

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

3.1.1
data protection by design
technical and organisational 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 organisational 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 personally identifiable information, framed within an organization's broader risk management framework

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

3.1.4
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

DPbDD	Data protection and Privacy by Design and by Default
DPIA	Data protection impact assessment
GDPR	EU General Data Protection Regulation
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. 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 if they contain, explicitly or implicitly, the need for functional capabilities in support of data controllers obligation.

The following principles will be considered foundational for Data protection and privacy by design and by default:

1) DPbDD shall be proactive and preventative, not reactive and remedial.

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

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

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

5) DPbDD will concern the entire data lifecycle.

6) DPbDD shall 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) DPbDD measures shall be effective.

9) DPbDD measures shall 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) DPdDD measures shall 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 frame 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 himself, 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. In 4.3 the conformity scheme for a self-declaration is provided.

In Clause 5, the requirements for a 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 and service layers defined 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 or service layers on the definition of privacy by design and on guidance for applying 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, set of module categories is defined in the next two clauses. Any market product or service under this document needs to be seen as a combination of some of this categories in the understanding of adding layers to get the full picture. Therefore, the terms “product layer” and “service layer” will be used for these categories.

4.2.2 Product layers

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

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

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

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

5) Storage layer — logical layer for the management of storage locations on connected physical storage media via the component layer. 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 layer — logical layer for the management of user interaction with a device or service, which is not on Operating system layer. This layer also includes portals and, up to a certain degree, content management systems.

7) Integrated system layer — this layer 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 shall demonstrate the capabilities and default settings for an appropriate network security.

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

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

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

4.2.3 Service layers

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

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

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

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

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

5) Update service layer — Program code updates provided human based proactive, automated reactive or by only making the updates available for download.

6) Cloud service layer — service providing operation facilities either on infrastructure level or on application level.

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

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

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

10) Maintenance service layer — 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 layer — semi-automated services evaluating systems, traffic and log entries in order to detect, prevent or react on vulnerabilities and security breaches.

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

13) Media destruction service layer — 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 layer — service on products by cleaning, reconstruction and re-licensing in order to give the product a second live 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 DPbDD, 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 layers the product or 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.

In order to reflect both, the practise of trade-offs and the need for adequacy in special processing conditions, six levels of achievement have been defined 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 is 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 is 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.
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 requirements applicable from the correct set of product and/or service layers. 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.

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

5 Process for a privacy aware development of products and services

5.1 Leadership and market intelligence

5.1.1 The organization shall establish and maintain the understanding of data protection and privacy by design and by default being an imperative to the development and provision of its products and services.

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 and its functional logic a comprehensive view of all the usage conditions relative to the different segments covered by the marketing plans.

This comprehensive functional view shall apply 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 business model includes an active role in the processing of personal data.

NOTE An active role needs 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 define an appropriate methodology and the structure of the 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.

If there is appointed one for the organization, the data protection officer should get involved in the design process. 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 DPbPP 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 layers it is composed of.

NOTE The layers are defined in Clause 4.2.

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

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

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 take into consideration to implement appropriate technical and organisational measures.

NOTE 1 EN ISO/IEC 27701, extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management, provides respective requirements and guidelines.

If there is one, the data protection officer of the organization should get informed and consulted for the appropriate measures to implement on the processing.

NOTE 2 Reference is made to GDPR Article 25.

5.3.1.3 Impact driven design requirements

5.3.1.3.1 The person responsible for the product and/or service design shall determine, if the data collected, processed and/or transmitted include so called “special categories of personal data” as defined in GDPR Article 9, or personal data relating to criminal convictions and offences.

NOTE Reference is made to GDPR Articles 9 and 10.

5.3.1.3.2 In case of the special categories of personal data are confirmed, the person responsible for the product and/or service design shall conduct a data protection impact assessment (DPIA) in accordance to the provisions made in 5.2.2.

NOTE Reference is made to GDPR Article 35. There could be further cases when a DPIA needs to be conducted as well.

5.3.1.3.3 If the DPIA comes to the conclusion that additional requirements shall be raised against the design and the default setting of the product and/or service, the person responsible for the product and/or service design shall ensure that these requirements will get considered under the development as well.

5.3.1.4 Specific branches or consumer related design requirements

5.3.1.4.1 If a product /and/or sevice is intended to be provided to specific categories of data subjects, the person responsible for the product and/or service design shall determine if there are specific expectations to the privacy-aware design and default configuration.

5.3.1.4.2 Any of these expectations shall be covered by either an existing or a new requirement to the design and the default setting of the product and/or service. The person responsible for the product and/or service design shall ensure that these requirements will get considered under the development as well.

NOTE In a certain branch, use case or environment, customer and/or consumer expectation on a privacy-aware design and default could be far more in detail than the legal expectation from GDPR.

5.3.2 Development

5.3.2.1 The person responsible for the product and/or service development shall ensure that all the design requirements kept up in 5.3.1 will get considered in the development phase of the product or service.

5.3.2.2 The person responsible for the product and/or service development shall ensure that best effort is made to implement adequate functions, measures and controls in the respective product and/or service in order to fulfil the requirements mentioned in 5.3.2.1.

5.3.2.3 The person responsible for the product and/or service development shall define the utmost privacy-aware default settings possible for any configurable function coming with the product and/or service under development.