SLOVENSKI STANDARD
oSIST prEN 17799:2022

01-februar-2022

Zahteve za varstvo osebnih podatkov za postopke obdelave

Personal data protection requirements for processing operations

Anforderungen an den Datenschutz bei Verarbeitungsvorgängen

Ta slovenski standard je istoveten z: **prEN 17799**

ICS:

03.160	Pravo. Uprava	Law. Administration
35.020	Informacijska tehnika in tehnologija na splošno	Information technology (IT) in general

oSIST prEN 17799:2022 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 17799

December 2021

ICS 03.120.20; 03.160

English version

Personal data protection requirements for processing operations

Exigences de protection des données à caractère personnel pour les opérations de traitement

Anforderungen an den Datenschutz bei Verarbeitungsvorgängen

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

Ref. No. prEN 17799:2021 E

Contents

Page

European foreword

This document (prEN 17799:2021) has been prepared by Technical Committee CEN/CLC/JTC 13 “Cybersecurity and Data Protection”, the secretariat of which is held by DIN.

This document is currently submitted to the CEN Enquiry.

Introduction

Personal data protection is regulated throughout Europe according to laws, the most important of which is the European Regulation 2016/679 (hereafter referred to as “Regulation”). This regulates the protection of natural persons with regard to the processing of personal data but does not contextualise it in a set of consequential or related activities and refers specifically to mechanisms for the certification of personal data protection for demonstrating compliance with the Regulation.

ISO/IEC 27701 is undergoing the process for adoption as an EN, and CEN/CLC JTC 13 is undertaking a new work item on “enhancing ISO/IEC 27701 for the EU context”. Those efforts will also provide a solid basis for GDPR conformance and alignment of the European data protection landscape with global norms. The focus of those standards is however fundamentally different since they are aimed to a management system and not to services and processes as the current document.

1 Scope

This document specifies baseline requirements for demonstrating processing activities compliance with the European personal data protection normative framework in accordance with EN ISO/IEC 17065. It does not however apply to products or management systems destined for processing personal data.

This document is applicable to all organizations which, as personal data controllers and/or processors, process personal data, and its objective is to provide a set of requirements enabling such organizations to conform effectively with the European personal data protection normative framework.

An organization can decide that the standard is applicable only to a specific subset of its processing activities if such a decision does not involve failure to conform with the European personal data protection normative framework.

This document also provides indications for conformity assessment with the aforementioned requirements.

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.

ISO/IEC 27000, *Information technology - Security techniques - Information security management systems - Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

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

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

3.1
supervisory authority
independent public authority which is established by a Member State pursuant to Article 51

[SOURCE: European Regulation 2016/679]

3.2
supervisory authority concerned
supervisory authority which is concerned by the processing of personal data because: (a) the controller or processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority

[SOURCE: European Regulation 2016/679]

3.3
consent
consent of the data subject
any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

[SOURCE: European Regulation 2016/679]

3.4
personal data
any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

[SOURCE: European Regulation 2016/679]

3.5
profiling
any form of automated processing of personal data used to evaluate certain aspects relating to a natural person, in particular to analyse or to predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

[SOURCE: European Regulation 2016/679]

3.6
processor
natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

[SOURCE: European Regulation 2016/679]

3.7
processing
any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

[SOURCE: European Regulation 2016/679]

3.8
controller
natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

[SOURCE: European Regulation 2016/679]

3.9
third party
the natural or legal person, public authority, agency or other body other than a data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data

[SOURCE: European Regulation 2016/679]

3.10
impact
data protection impact
anything that has an effect on the protection of a data subject and/or group of data subjects

[SOURCE: ISO/IEC 27557]

3.11
consequence
outcome of an event affecting organizational objectives

[SOURCE: ISO/IEC 27557]

4 Overview

This document specifies baseline requirements for the processing of personal data so that an organization, whether controller or processor, is able to attain compliance with the European and applicable national personal data protection normative framework. The separation between controller and processor activities is based on the requirements within the aforementioned normative framework but processors might be delegated more activities by the related controllers, therefore transferring the applicability of related additional requirements set forth in this document to them.

The present document is completed by Annex A which contains the indications for conformity assessment to the requirements of the document.

5 Planning

5.1 General

This clause sets out the activities which a controller or processor shall perform, in order to carry out the protection of personal data in a systematic and organized way within processing activities. They shall be implemented periodically or after relevant changes such as modifications to the law or corporate organization, structural changes in information technology or its characteristics.

5.2 Understanding the needs and expectations of interested parties

The controller or processor shall determine:

a) all interested parties, involved in personal data processing activities including data subjects, processors and controllers; and

b) the requirements of such interested parties related to personal data processing activities;

the mandatory requirements of the normative reference framework of national laws and the contractual obligations.

5.3 Scope of personal data processing activities

5.3.1 General

The controller shall determine the limits and applicability of the personal data processing, documenting: records of data processing activities, their legal basis, the locations, organizational structure (including all interested parties identified in 5.1), information systems and main involved supporting assets.

5.3.2 Records of data processing activities

The controller or processor shall identify the personal data and their flow related to each processing and shall keep them updated in personal data processing activity records. In particular, the controller or processor shall establish and maintain up-to-date records of data processing activities identifying:

1) the controller of the processing;

2) the processes which use personal data;

3) the sources of processed personal data;

4) the processed personal data and related categories;

5) the purposes of the use of the personal data;

6) the recipients of personal data, including third parties;

7) the role (controller, processor or joint controller of the processing of the organization;

8) the information systems involved in the archiving of personal data;

9) any transfers of personal data to third parties, international organizations or other countries;

10) the storage period of personal data or the criteria used for determining such period and the measures taken at the end of the period;

11) the locations where processing takes place.

NOTE This is in line with article 30 of the Regulation.

5.3.3 Identification of the legal basis

The controller shall define the legal basis for the processing of personal data and communicate them to the data subjects. The controller shall document the legal basis.

NOTE The legal basis contained in article 6 of the Regulation are as follows:

— the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

— processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

— processing is necessary for compliance with a legal obligation to which the controller is subject;

— processing is necessary for protecting the vital interests of the data subject or of another natural person;