SLOVENSKI STANDARD
SIST EN 17799:2024

01-april-2024

Zahteve za varstvo osebnih podatkov za postopke obdelave

Personal data protection requirements for processing operations

Anforderungen an den Datenschutz bei Verarbeitungsvorgängen

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

Ta slovenski standard je istoveten z: **EN 17799:2023**

ICS:

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

SIST EN 17799:2024 **en,fr,de**

EUROPEAN STANDARD **EN 17799**

NORME EUROPÉENNE

EUROPÄISCHE NORM October 2023

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 European Standard was approved by CEN on 4 September 2023.

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, Türkiye and United Kingdom.

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

Ref. No. EN 17799:2023 E

Contents

Page

European foreword

This document (EN 17799:2023) has been prepared by Technical Committee CEN/CLC/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 April 2024, and conflicting national standards shall be withdrawn at the latest by April 2024.

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.

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, Türkiye and the United Kingdom.

Introduction

Personal data protection is regulated throughout European Union according to laws, the most important of which is the EU Regulation 2016/679 (hereafter referred to as “Regulation” or “GDPR”). 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.

Moreover, the Regulation refers to the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with the regulation of processing operations by controllers and processors.

Those efforts will also provide a solid basis for GDPR conformance and alignment of the European data protection landscape with global standards. The focus of those standards is fundamentally different since they are aimed to a management system and not to services and processes as the current document is.

ISO/IEC 27701 has been adopted as an EN, and CEN/CLC JTC 13 is undertaking a new work item on its “Refinements in European context”. Those efforts will also provide a solid support 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 at a management system and not to services and processes as the current document.

1 Scope

This document specifies baseline requirements intended to support the data protection certification mechanism requested by Article 42 of the GDPR to demonstrate compliance 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 supporting such organizations in demonstrating compliance with the EU personal data protection normative framework

This document is applicable to all of an organization's processing activities or to a specific subset of these if such a decision does not involve failure to conform with the EU 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 27000:2020, *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 27000:2020 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
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]

3.2
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 effectively supported when demonstrating compliance with EU 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.

This document is completed by Annex A which summarizes the applicability of the document clauses to controllers and processors.

NOTE This document can't provide direct coverage of all the requirements within EU and applicable national personal data protection normative framework but is structured to contribute establishing a baseline to allow their effective fulfilment.

5 Planning

5.1 General

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

NOTE All seven principles listed within article 5 of the Regulation are considered within this and following chapters, inside dedicated paragraphs or spread in other.

5.2 Understanding the needs and expectations of interested parties

The controller or, where applicable and consistent with the circumstances of the data processing, the 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;

c) the mandatory requirements of any applicable legislation 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 physical locations, organizational structure (including all interested parties identified in 5.2), information systems and other relevant involved supporting assets.

5.3.2 Records of data processing activities

The controller or processor shall, to the extent of their applicable responsibilities, 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 name and contact details of the controller of the processing and, where applicable, of the joint controller and the data protection officer;

2) the processes which use personal data;

3) the sources from which personal data originate (only applicable to controllers);

4) the categories of data subjects and personal data being processed (only applicable to controllers);

5) the categories of processing carried out on behalf of each controller (only applicable to processors);

6) the identified legal basis for the processing (see 5.3.3) (only applicable to controllers);

7) the purposes of the processing (only applicable to controllers);

8) the categories of recipients of personal data, including categories of third parties;

10) the information systems involved in the storage of personal data;

11) the general description of technical and organisational security measures used to protect personal data (ensuring the existence of this description is not itself a security hazard);

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

13) the retention period of personal data or the criteria used for determining such period and the type of measures taken at the end of the period;

14) the physical locations where processing takes place.

NOTE This section is intended to support article 30of the Regulation.

5.3.3 Identification of the legal basis

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

NOTE 1 Article 6 of the Regulation specifies the acceptable legal basis for processing personal data.

When special categories of personal data are processed, the controller shall identify, communicate and document the legal basis for the processing of personal data.

NOTE 2 Article 9 of the Regulation specifies the acceptable legal basis for processing special categories of personal data.