

STN	Požiadavky na ochranu osobných údajov pri spracovateľských operáciách	STN EN 17799 97 4169
------------	--	--

Personal data protection requirements for processing operations

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 12/23

Obsahuje: EN 17799:2023

137930

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2024
Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii v znení neskorších predpisov.

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**

EN 17799:2023 (E)

Contents	Page
European foreword	4
Introduction	5
1 Scope.....	6
2 Normative references.....	6
3 Terms and definitions	6
4 Overview	7
5 Planning	7
5.1 General.....	7
5.2 Understanding the needs and expectations of interested parties	7
5.3 Scope of personal data processing activities	7
5.3.1 General.....	7
5.3.2 Records of data processing activities	8
5.3.3 Identification of the legal basis	8
5.3.4 Data minimization	9
5.3.5 Retention periods	9
5.4 Policy for personal data protection.....	9
5.5 Roles and responsibilities	10
5.5.1 General.....	10
5.5.2 Internal roles.....	11
5.5.3 External roles	11
5.6 Risk management	12
5.6.1 General.....	12
5.6.2 Data protection risk assessment and impact analysis	12
5.6.3 Evaluation of the impact on data protection.....	13
5.6.4 Risk treatment and treatment plan.....	14
5.7 Personal data protection by design and by default.....	14
6 Operational activities.....	15
6.1 General.....	15
6.2 Data protection notices and consent	15
6.2.1 Data protection notices	15
6.2.2 Consent	15
6.3 Update of roles.....	16
6.4 Personal data protection.....	16
6.4.1 Erasure of data.....	16
6.4.2 Implementation and maintenance of security measures.....	16
6.4.3 Management of personal data breaches.....	17
6.5 Data subjects' requests for the application of their rights.....	18
6.5.1 General.....	18
6.5.2 Data access	18
6.5.3 Correction.....	18
6.5.4 Erasure.....	19
6.5.5 Restriction of processing	19
6.5.6 Data portability	19
6.5.7 Objections.....	19

6.5.8	Automated decisions, including profiling.....	20
6.5.9	Complaints and appeals	20
6.6	Training and awareness.....	20
7	Control	20
7.1	General	20
7.2	Internal audits	20
7.3	Periodical report.....	21
7.4	Nonconformities and corrective actions.....	22
	Annex A (informative) Controllers and processors requirements mapping	23
	Bibliography	25

EN 17799:2023 (E)**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.

EN 17799:2023 (E)

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*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN