SIST

SLOVENSKI STANDARD
SIST EN 17740:2024

01-april-2024

Zahteve za poklicne profile pri obdelavi in varovanju osebnih podatkov

Requirements for professional profiles related to personal data processing and protection

Anforderungen an Berufsprofile im Zusammenhang mit der Verarbeitung und dem Schutz personenbezogener Daten

Exigences relatives aux profils de professionnels en lien avec le traitement et la protection de données à caractère personnel

Ta slovenski standard je istoveten z: EN 17740:2023

ICS:

03.100.30	Vodenje ljudi	Management of human resources
35.030	Informacijska varnost	IT Security

SIST EN 17740:2024 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 17740

October 2023

ICS 03.100.30; 35.030

English version

Requirements for professional profiles related to personal data processing and protection

Exigences relatives aux profils de professionnels en lien avec le traitement et la protection de données à caractère personnel

Anforderungen an Berufsprofile im Zusammenhang mit der Verarbeitung und dem Schutz personenbezogener Daten

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 17740:2023 E

Contents

Page

European foreword

This document (EN 17740:2023) 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

The definition of requirements for professional profiles in the field of processing and protection of personal data are necessary to establish the fundamental set of knowledges, skills and competences that distinguish such profiles.

The standard applies to the professional profiles in the identified area, regardless of the working methods and type of employment relationship. Tasks and activities related to the profession are described on the basis of all functions actually performed by professionals working in the field of processing and protection of personal data in different work contexts. These functions are varied and concern technical, administrative, cultural, scientific and legal aspects.

This document adopts the reference European framework for the definition of competences and related skills: EN 16234-1. For related ICT-oriented profiles, such as for example the system administrator, please refer to CEN CWA 16458-1.

The profiles specified in this document are not intended to be exhaustive and are applicable regardless of the work placement of the subjects operating in the sector.

The main intended audience of this document comprises professionals seeking guidance regarding their professional development, enterprises defining their internal data protection organization and related hiring requirements, bodies providing personnel training, accreditation and certification services.

Methodological approach

Within the development of this document the principles and indications set out in Recommendation 2008 / C111 / 01 (European Qualification Framework - EQF) and Recommendation 2009 / C 155/02 (European Credit System for Vocational Education and Training - ECVET) were first considered.

From a methodological point of view, it was established in particular that:

- the basic terms and definitions (Clause 3) adopted are, for the most part, derived from the EQF, ECVET and the relevant terminology commonly used in the European Community;

- the specific terms and definitions of the subject “protection of personal data” are consistent with those set out in EU 2016/679 Regulation;

- for the description of the requirements of knowledge, skills and competence of a specific professional profile, it is necessary to start from a preliminary identification of the tasks and specific activities of the professional profile (Clause 4);

- the requirements of the specific professional profile are specified in terms of knowledge, skills and competence (Clause 5) and the personal ability expected have also been identified, as far as applicable. An indication of the levels associated with the specific professional activity, using the e-CF levels which are directly mapped to the ones within the European Qualifications Framework (EQF), is also provided;

- the useful elements regarding the applicable assessment methods are specified (Clause 7). These elements have been developed taking into due consideration what already consolidated within voluntary technical standardization, also with reference to the normative corpus concerning the conformity assessment (EN ISO/IEC 17000 series);

- in Annex A (informative) skills and knowledges applicable to the development of the profiles are listed;

- in Annex B (normative) requirements for access to professional profiles are specified.

Furthermore, as far as relevant, the guidelines specified in the CEN Guide 14 were also followed.

1 Scope

This document specifies the requirements related to the professional activity of persons active in the processing and protection of personal data, namely the intellectual profession that is pursued at different levels of complexity and in different organizational contexts, both public and private.

These requirements are specified, starting from the specific tasks and activities identified, in terms of knowledge, skills and competence, in accordance with the European Qualifications Framework - EQF and are expressed in such a way as to facilitate and contribute to harmonize, as far as possible, evaluation and validation processes of learning outcomes.

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 16234-1, *e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all sectors - Part 1: Framework*

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

EN ISO/IEC 29100, *Information technology – Security techniques – Privacy framework*

CEN CWA 16458-3, *European ICT Professional Role Profiles – Part 3: Methodology documentation*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 16234-1, EN ISO/IEC 27000, EN ISO/IEC 29100 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
formal learning
learning process deriving from training activities, intentional and structured, carried out by entities / institutions of education and training recognized by a competent authority

Note 1 to entry: Formal learning can involve the issues of certificate with legal value .

3.2
informal learning
learning process deriving from work experiences, from family life and also from leisure time

Note 1 to entry: Informal learning is not a deliberately structured activity and sometimes learning is not intentional.

3.3
non-formal learning
learning process resulting from training activities, intentional and structured, implemented in any field other than formal

Note 1 to entry: Such a training does not issue a certificate with legal value.

3.4
audit
systematic, independent and documented process for obtaining audit evidence (records, statements of facts or other relevant and verifiable information) and evaluating them objectively, in order to establish to what extent the audit criteria (policies, procedures or requirements used as a reference) have been met

3.5
validation of learning outcomes
process confirming that certain assessed learning outcomes, obtained by a learner, correspond to the results required for a specified qualification or part of it

Note 1 to entry: Certification in accordance with EN ISO/IEC 17024 is an evaluation and validation process.

Note 2 to entry: The recognition of learning outcomes, according to defined rules, by subjects or other organizations in charge, is also a process of evaluation and validation.

3.6
Privacy Impact Assessment
PIA
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

[SOURCE: ISO/IEC 29134:2017, 3.7]

3.7
Privacy Level Agreement
PLA
level of protection of personal data ensured by a supplier in the provision of services to its customers, conceptually similar to an SLA

3.8
qualification
formal result of an assessment and validation process, obtained when a competent and impartial organization states that the learning outcomes of an individual are compliant with technical standards

Note 1 to entry: Definition adapted from the EQF, Annex I, definition a).

3.9
Service Level Agreement
SLA
Document that defines the technical support or business performance objectives, including measures for performance and consequences for failure the provider of a service can provide its clients

[SOURCE: ISO/IEC 27039 :2015, 2.27]

3.10
evaluation of learning outcomes
Methods and processes used to define the extent to which a person has effectively achieved one specific knowledge, skill or competence

4 Professional profile tasks and specific activities

4.1 General

The professional operating in the processing and protection of personal data performs a wide range of activities, frequently transversal to other business processes, both with respect to the life cycle of the processing - from design to cessation - and with respect to the examined topics, technological, organizational, legal or otherwise.

The professional working in the field of processing and protection of personal data thus contributes to the management or the verification of a more or less extensive set of processes and information systems involved in the processing of personal data, on behalf of natural or legal persons, such as entities, institutions, associations, public or private. Legal entities of different sizes may decide either to collapse related professional profiles into one (e.g. data protection manager and data protection specialist or a data protection auditor with another auditor) or to have several instances of the same profile within different responsibility areas, such as geographical or organizational ones. In all cases the separation between control-related profiles like auditor and data protection officer and the other ones should be preserved.

At the time of publication of this document, the maintenance, updating and development of the skills necessary for the professional activity of the subjects, operating in the processing and protection of personal data, are not subject to a detailed training path herewith specified. The professional is however required to follow autonomous or guided paths of continuous professional updating, consistent with the provisions of paragraph 6.4 and Annex B.

If professionals have already followed previous training courses, not aligned with the indications of this document, it shall be necessary to carry out an analytical comparison between the path already followed by the candidate for certification and the path illustrated in this document, assuming the related responsibilities.

4.2 Introduction to professional profiles

A series of considerations of an introductory nature and preliminary to the description of the main professional profiles, referred to in Clause 6 of this document, is listed below in order to facilitate their understanding.

Data protection officer

It is a profile corresponding to the professional profile described in EU Regulation 2016/679, art. 39. It is possible to assign to the profile different tasks and other tasks included in other managerial level profiles, if no conflict of interest is present.

Data protection manager

It is a profile corresponding to professionals with a very high level of knowledge, skills and competences in a specific organizational context (both a functional area of the organization and a specific sector), to ensure the adoption of appropriate organizational measures in the processing of personal data.

Data protection specialist

It is a profile corresponding to professionals able to support the Data protection officer and / or the Data protection manager in developing the appropriate technical and organizational measures for the processing of personal data.

Data protection engineer

It is a profile corresponding to professionals who are designing and building systems that process personal data, who have a specialist knowledge of, and responsibility for, related data protection issues. They can work alongside other software and systems engineers and related technical disciplines, as well as with other data protection-devoted profiles in an organization both developing and operating those systems.

Data protection auditor

It is a profile corresponding to independent professionals with knowledge and skills in the IT / technology sector and legal / organizational activities, able to carry out processing and protection of personal data, which can still make use of data protection specialists in both areas to carry out audit assignments.

4.3 Tasks and activities of the professional operating in the processing and protection of personal data

The profile of the professional operating in the field of processing and protection of personal data includes a series of fundamental tasks which, without pretending exhaustiveness, are described in the following Clause 5 (see item "Main tasks").

A professional operating in the processing and protection of personal data are intended as a person who has a profile that complies with the aforementioned tasks, and performs, or has the necessary preparation, to achieve the "Expected Results".

5 Knowledge, skills and competencies associated with professional activity

5.1 General

Each professional profile in this chapter is structured with a short description synthesizing it, the pursued mission, the deliverables of which they are accountable, responsible or contributor, the specific performed main tasks, competences defined according to EN 16234-1 and CWA 16458-3 are identified within the "Competences e-CF" table with related skills and knowledge and the KPIs measuring their performance.

5.2 Data protection officer professional profile

5.2.1 Short description

Advises controllers or processors for the application of EU Regulation 2016/679 or other applicable data protection legislation.

5.2.2 Mission

Advises controllers or processors with respect to the risks of data processing activities to ensure compliance with EU Regulation 2016/679 and other local data protection provisions.

5.2.3 Deliverables[1]

This profile is accountable for the following deliverables:

- Regular risk-based reports on compliance with laws regarding personal data protection.
- Documentation in support of the request for consultation addressed to data protection authorities, according to the development of data protection impact assessment .
- Requests for consultation with data protection authorities on specific application issues.
- Documentation supporting the interface with the data protection authorities (requests for information, assessment procedures or testing etc.).
- Documentation (including forms) supporting the interface with the interested parties.
- Indicators on the protection of personal data.
- Advice with respect to inquiries regarding data protection law and its application.

This profile is responsible for the following deliverables:

- Opinions on data protection impact assessments pursuant to Regulation 2016/679.

This profile is a contributor for the following deliverables:

- Attribution of responsibilities in the processing and protection of personal data.
- Budget for the protection of personal data.
- Policy for the protection of personal data.
- Data protection notices.
- Requirements for the processing and protection of personal data.
- Operating procedures for processing and protection of personal data.
- Development of a Data protection impact assessment.
- Evaluation of the risk related to information security.
- Risk management plan related to information security.
- Codes of conduct.
- Answers to data subject exercising their rights.
- Audit program for the protection and processing of personal data.
- Training program, professional development and awareness.

[1] Please note that all professional profiles herewith described are not related to legal responsibilities, but only to operating responsibilities.

- Notification of incidents that result in a violation of personal data (to data protection authorities).

5.2.4 Main tasks

The main tasks associated to this profile are:

- inform and provide advice to controllers or processors, as well as to employees involved in processing of personal data, about the obligations arising from this Regulation as well as from other Union or Member State data protection provisions;
- monitor compliance with the Regulation, other Union or Member State or other provisions on data protection and the policies of the controller or data controller, regarding the protection of personal data, including the assignment of responsibilities, the awareness and training of personnel involved in the processing and related control activities;
- provide, if requested, an opinion on the impact assessment on data protection and monitor its performance;
- cooperate with the supervisory authority;
- act as a contact point for the supervisory authority for matters related to processing.

The following Table 1 shows the assigned competencies and required levels according to the e-CF provided in EN 16234-1.

Table 1 — assigned competencies and required levels according to the e-CF provided in EN 16234-1

e-CF competence	*Level*
D.8. Contract Management	3
D.9. Personnel Development	3
E.3. Risk management	4
E.4. Relationship Management	4
E.8. Information Security Management	3

5.2.5 Skills

Skills associated to this profile are:

- Analyse personal data processing and evaluate their compliance to applicable legal requirements
- Verify the application of data protection by design and protection by default
- Verify the appropriate application of data protection principles
- Identify roles, responsibilities and legal basis for the processing of personal data
- Contribute to the strategy for the processing and protection of personal data
- Contribute to provision of correct information to data subjects
- Manage the application of codes of conduct and certification applicable to the processing and protection of personal data

- Ability to communicate
- Analytical skills
- Self management and stress control
- Self-development capacity
- Control capacity
- Persuasion capacity
- Conflict management capacity
- Initiative
- Eligibility for negotiation
- Organization skills
- Perspective thinking
- Planning and scheduling
- Constructive attitude in solving problems
- Tenacity
- S1 - address CPD needs of staff to meet organisational requirements
- S5 - analyse the company critical assets and identify weaknesses and vulnerability to intrusion or attack
- S19 - anticipate required changes to the organization's information security strategy and formulate new plans
- S21 - apply mitigation and contingency actions
- S23 - apply relevant standards, best practices and legal requirements for information security
- S40 – coach
- S45 - compose, document and catalogue essential processes and procedures
- S52 - communicate and promote the organization's risk analysis outcomes and risk management processes
- S55 - communicate good and bad news to avoid surprises
- S66 - establish a risk management plan to feed and produce preventative action plans
- S91 - ensure that IPR and privacy issues are respected
- S111 - identify competence and skill gaps