SLOVENSKI STANDARD
SIST-TP CEN/CLC/TR 17919:2023

01-maj-2023

Varstvo podatkov in zasebnosti z načrtovanjem in kot privzeto - Tehnično poročilo o uporabnosti v industriji videonadzora - Stanje tehnike

Data protection and privacy by design and by default - Technical Report on applicability to the videosurveillance industry - State of the art

Videoüberwachung

Protection des données et de la vie privée dès la conception et par défaut - Rapport technique sur l'applicabilité au secteur de la vidéosurveillance - État de l'art

Ta slovenski standard je istoveten z: **CEN/CLC/TR 17919:2023**

ICS:

35.030	Informacijska varnost	IT Security

SIST-TP CEN/CLC/TR 17919:2023 **en,fr,de**

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER REPORT

CEN/CLC/TR 17919

February 2023

ICS 35.030

English version

Data protection and privacy by design and by default - Technical Report on applicability to the video surveillance industry - State of the art

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen - Technischer Bericht über die Anwendbarkeit in der Videoüberwachungsindustrie - Stand der Technik

This Technical Report was approved by CEN on 9 January 2023. It has been drawn up by the Technical Committee CEN/CLC/JTC 13.

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. CEN/CLC/TR 17919:2023 E

Contents

Page

European foreword

This document (CEN/CLC/TR 17919:2023) has been prepared by Technical Committee CEN/CLC/JTC 013 “Cybersecurity and Data protection”, the secretariat of which is held by DIN.

This document has been prepared in complement of EN 17529*: Data protection and privacy by design and by default 2021*, under mandate M530 given to CEN/CENELEC by the European Commission.

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.

Introduction

This document explains how EN 17529, “Data Protection and Privacy by Design and by Default”, is applicable to the video-surveillance industry, a security industry which is permanently serving the objectives of its various customers, themselves subject to a balance between privacy and security expectations, eventually changing with the political, local and conjunctural situations.

EN 17529 defines the process through which the developers and/or manufacturers of all types of products and services make sure that the end-users thereof will be encouraged and be able to use them in compliance with the applicable privacy rules, directly or after an appropriate set-up. Concretely, implementing this standard will allow this industry sector to provide its customers (and especially their data controllers) with solutions designed with the necessary options and flexibility to comply with their privacy protection obligations over the lifetime of the delivered solutions.

It should be noted that in parallel to this report, the European Data Protection Board (EDPB) has published its *Guidelines 3/2019 on processing of personal data through video devices*, version 2.0, which provide an official interpretation of the use of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) applied to video-surveillance systems.

1 Scope

This document illustrates, through a review of the state of the art, the applicability of the EN 17529 to the domain of the video-surveillance industries, a security industrial domain which is serving the objectives of its various customers, themselves subject to a delicate balance between privacy and security objectives eventually changing with the political, local and conjunctural situations.

Implementing this standard will allow this industry to provide its customers with solutions designed with the necessary options and flexibility to contribute to their privacy protection obligations over the lifetime of the delivered solution.

The present document considers at this stage the core video-surveillance solutions consisting in up to:

- A number of cameras (fixed or PTZ);
- A Video Management System (VMS) including its storage capability;
- A display and replay capability:

  Basic video analytics allowing automatic detection in the video of each camera of simple geometric situations (movement detection, line crossing, etc.), but excluding embedded tools allowing automated distinguishing, direct identification or tracking of individuals;
- IP interfacing with external (not included) terminals.

This basic set-up may be expanded in future versions.

The “off-the-shelf” system and sub-system manufacturers are the core targets of this document; companies doing systems installation may be indirectly addressed, but service providers eventually running the systems are not covered.

2 Normative references

The following documents are referred to in the text in such a way that some, or all, of their content constitutes references for 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 17529:2022, *Data protection and privacy by design and by default*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 17529 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
pan-tilt and zoom
PTZ
capacity of a camera to be controlled remotely regarding direction and zoom

4 High level objectives

Referring on the main body of EN 17529 and based on the state of the art, the present TR details how it is possible for a manufacturer of a video-surveillance system to take into consideration as part of the quality process followed by its product line, the provisions of EN 17529 making sure that its different potential end-users can easily and are encouraged to comply with their data protection and privacy obligations.

To do so, the different prescriptions of EN 17529:2022, Clause 6, will be translated into features and set-up of a video-surveillance system, while as per the core principle of EN 17529, the manufacturer can have a formal process through which all such prescriptions are considered (in existence, performance, set-up, etc.) with regard to the privacy requirements, for each system delivered.

It must be noted:

- That, nevertheless, the product will be delivered, maintained and disposed in compliance with the written configuration request established by the customer, who remains the sole accountable entity, even if this may not correspond to an optimum privacy set-up or configuration among the options proposed by the vendor; this is especially true as video-surveillance systems are often used in governmental security missions covered by dedicated regulations,

- That this document applies to digital, analogue and hybrid systems (containing both digital and analogue technologies). It might not be possible to fully decompose these systems into the functional perspectives envisaged in the example presentation given in EN 17529. System integrators and manufacturers may need to map their system architectures directly to the data protection and privacy requirements, using a more natural decomposition into parts as appropriate for their system,

- That in many countries, video-surveillance has been subject to local privacy regulations for many years and that accordingly at least some of the prescriptions discussed hereafter are covered by legacy implementations,

- And finally that in parallel to the preparation of this TR, the European Data Protection Board (EDPB) has published the *Guidelines 3/2019 on processing of personal data through video devices*, Version 2.0, which provide an official interpretation of the use of the GDPR applied to video-surveillance systems, which, as such, prevails on interpretations which may result of provisions of the standard and of this TR.

5 Guidelines regarding the process to follow

The main body of EN 17529 details, in its Clause 5, process to follow in a comprehensive detailed and generic manner.

As clearly demonstrated in the EDPB Guidelines, the video-surveillance domain requires a detailed functional analysis for each individual use case to be able to identify the set of the GDPR (and of Clause 6 below) provisions applicable.

It is worth remembering as well that, although not all the video-surveillance systems are digital, privacy regulations might remain applicable.

As stated in 5.1.2 of EN 17529 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 is encouraged to select, train and fully inform staff in charge of the process below on

- Applicable legislation, e.g. the GDPR and its functional logic, and

- A comprehensive view of all the usage conditions relative to the different segments covered by the marketing plans.

This comprehensive functional view applies to the full process described in 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 standard.

To do so, like for quality, the manufacturer can establish a documented process for the design and the production of the video-surveillance systems (including the cameras, the camera software and the VMS), with, typically, as an output the following documents:

— A general description of the system,

— Risk assessment report covering the different anticipated use cases,

— Technical requirements, including the security and privacy ones,

— The architecture of the system,

— A description of the manufacturing controls,

— User manual,

— Test reports, including the security test reports (IT vulnerability assessment).

It must be noted that accordingly, and unless the organization develops extremely specific video-surveillance systems, representing the solutions in terms of the perspective-based decomposition required by the standard, self-declaration, as well as PIA, are almost impossible to achieve during the development phase covered by the standard.

Considering the nature of a video-surveillance system, as described in Clause 1, the efforts of the organization can concentrate on the basic requirements on the design listed in Clause 6 hereafter and it is the proper response to these basic requirements, that the compliance to the standard is due to ensure.

6 Verification of the ability to comply with the applicable privacy provisions[1]

6.1 Access

6.1.1 Access to data

6.1.1.1 Control objective:

A video-surveillance system being by essence designed to monitor a field of view without any discrimination, its designer can only provide indirect tools to the controllers, for helping them in providing capabilities for the data subject to access his/her data, as applicable.

6.1.1.2 Implementation in support to access to data by the data subjects

To support the data controllers of their future customers, which will implement its systems, by informing the potential data subjects of the existence of the system and of their rights, a good practice is that the manufacturers provide on their website models of posters to be installed in the area covered by the video-surveillance system, indicating that the area is monitored by video-surveillance and leaving a position to indicate how to contact the data controller in charge, who may give access to relevant footage.

Also, to support the future data controllers in retrieving information requested by the data subjects, it is recommended that each video-surveillance system be designed to allow search in the collected videos by time and camera location.

[1] For the reader's convenience, the numbering in this clause is the same as that of Clause 6 of EN 17529.

6.1.1.3 Account for each data subject involved (not applicable)

Each camera being able to monitor passively a large number of individuals, which are not discriminated in the scenes, any attempt to create files per data subject would generate an unnecessary and illegitimate processing of personal data.

6.1.2 Copy of data

6.1.2.1 Control objective:

The objective is to ensure that the video-surveillance system will be designed to allow export of clips in a non-proprietary format, by the data controllers (and data processors) in response to the requests of the data subjects.

6.1.2.2 Implementation of the export to the benefit of data subjects

Video-surveillance systems are commonly designed to allow the export without quality degradation of a clip representing one of the video streams for a limited duration in the form of a file with a format accepted by most commercial player (typically H264), this export being possible electronically or through the transfer of a removable memory (like a USB key). (see also IEC 62676 series of standards)

A single frame of a single camera being potentially able to show in detail many data subjects, export to one of them is acceptable only if all the other individuals visible in the scenes are anonymized. It is recommended that the video-surveillance export functionality be accordingly designed to be fitted with dynamic masking and one or more of such masking solutions be proposed by default with each system.

6.2 Accountability

6.2.1 Control objective

Ensure that nothing in the design of the video-surveillance system may mislead the data controller to the point where he or she could be unable to demonstrate compliance to the rules detailed in this section.

6.2.2 Accurate, transparent and easy to understand documentation

It is key that each video-surveillance system be provided with a documentation describing without ambiguity all its functionalities, which may impact privacy aspects; the manufacturer will also be prepared to propose the relevant training to the end-users (including their data controller) and to update duly the documentation, whenever a change to the system is introduced.

6.3 Accuracy

6.3.1 Control objective

The principle of enabling the data controller to update or append recordings is contrary to the video-surveillance key role, i.e. providing evidence of a presence or of a fact.

6.3.2 Corrections in the recorded videos (not applicable)

In fact, a video-surveillance system collects images of what happens at a given place and time. It is the interpretation of such images, eventually linked to the identity of an individual which might require updates or corrections, but it is not part of what a manufacturer of video-surveillance can influence.

To ensure that the recorded material has not been manipulated, the signature proposed by IEC 62676-2-32, 9.4 can be provided, to be activated as required by the data controller.

6.3.3 Dynamic masking (related consideration)

In some special circumstances, and as already discussed in 6.1.2.2, a dynamic masking can be made available, allowing the data controller to hide persons, groups of persons or privacy sensitive material.