

DOCUMENT ON VIDEO SURVEILLANCE at Fondazione Bruno Kessler

drawn up pursuant to EU Regulation no. 679/2016, to the Provision of the Personal Data Protection Authority of April 8, 2010 and to Guidelines 3/2019 of the European Committee for Data Protection

REV E DATA	CREATION	REVIEW	APPROVAL	Changes from the previous edition
Rev. 02 del 04/09/2026	Responsabile Videosorveglianza	DPO, A1	Responsabile del Servizio Patrimonio con determina n. 07 del 04/09/2026	Premessa e Artt. 1, 3, 4, 5, 6, 7, 8
Rev. 01 del 31/01/2022	Responsabile Videosorveglianza	DPO, A1	Responsabile del Servizio Patrimonio con determina n. 02/2022 del 31/01/2022	Premessa e Artt. 1, 2, 3, 4, 5, 6, 7, 8
Rev. 00 del 23/01/2018	Responsabile Videosorveglianza	Unità Prevenzione della Corruzione, Trasparenza e Privacy, A1	Responsabile del Servizio IT, Infrastrutture e Patrimonio con determina n. 01/2018 del 22 gennaio 2018	Nuova adozione

Introduction

With this Document, Fondazione Bruno Kessler (hereinafter FBK or Data Controller), with its registered office at Via Santa Croce 77, Trento, Italy, acting as the **Data Controller**, intends to provide detailed information regarding the processing of personal data consisting of images captured by the video surveillance system installed at the Foundation's premises, in accordance with Article 13 of Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR).

This Document is published on the FBK's website and made available at the entrance of each of its premises.

Appropriate information notices containing concise and relevant information on the processing activities are displayed at the monitored areas or in the immediate vicinity of the cameras. These notices are designed and positioned so as to be clearly visible before entering any area subject to video surveillance.

The processing of personal data through the video surveillance system is carried out in compliance with the principles established by the GDPR, including lawfulness, fairness, transparency, data minimisation, purpose limitation, integrity and confidentiality.

In accordance with the principles of privacy by design and privacy by default, the video surveillance system has been designed and is managed so as to limit the collection of images exclusively to those areas that are strictly necessary for achieving the stated security purposes.

The Data Controller also adopts a risk-based approach to the processing of personal data, periodically reviewing and updating its technical and organisational measures in order to ensure continued compliance with the applicable data protection legislation.

The **Data Protection Officer** (DPO) designated by the Data Controller pursuant to Article 37 of the GDPR can be contacted through the following channels: +39.0461.314.370 - privacy@fbk.eu.

1. Place of data processing

The video surveillance systems are installed at FBK premises:

- A. Operational premises in via Sommarive 18, Povo (TN)
- B. Operational premises at Villa Tambosi - Strada delle Tabarelle 286, Villazzano (TN)
- C. Registered office in via Santa Croce 77, Trento (TN)
- D. Operational premises in via alla Cascata 56/C, Povo (TN)
- E. Offices in vicolo Dallapiccola 12, Trento (TN)

The cameras are installed exclusively in areas that are relevant for security purposes, such as building entrances, outdoor areas, parking facilities, common areas, special-purpose rooms and access points to the Foundation's premises. The cameras are not specifically intended to monitor workstations or employees' work activities.

The processing of personal data takes place within the territory of the **European Union**. Should the processing activities involve the transfer or processing of personal data outside the European Union, and in the absence of an adequacy decision adopted by the European Commission, the Foundation will implement appropriate additional safeguards to ensure a level of protection essentially equivalent to that guaranteed within the European Union. In such cases, the Foundation will comply with the applicable legislation governing transfers of personal data to third countries, as

set out in Chapter V of the General Data Protection Regulation (GDPR), including, where applicable, the use of the European Commission's Standard Contractual Clauses (SCCs).

2. Purpose of data processing.

The processing of the data captured has the following purposes:

- a. safety and security from illegal and fraudulent behavior of natural persons who attend the Foundation's offices;
- b. protection from theft and vandalism of both corporate and third party assets;
- c. unauthorized access control.

3. Legal basis for data processing.

The processing of personal data is conducted in compliance with art. 4 of Law no. 300/1970 (Workers' Statute) and having a specific trade union agreement for the installation of the video surveillance system been signed.

The legal basis for the processing of personal data is the legitimate interest pursued by the Data Controller in operating a video surveillance system to ensure the security of its premises and the safety of individuals, as well as to protect the Foundation's assets and technological infrastructure.

Please note that providing the data is a required condition to access the Foundation's offices. Pursuant to the Provision of the Data Protection Authority on video surveillance of April 8, 2010, the consent of the data subjects is not required for the pursuit of the purposes of protecting the Foundation's property and the protection and safety of persons.

The Foundation undertakes to respect the principle of purpose limitation of processed data: therefore unnecessary uses are excluded and redundancies avoided. It is deemed necessary to use the video surveillance system because of:

- the high value of the equipment present in the Foundation's premises;
- the value of the information processed and stored on the Foundation's premises;
- the number of Users who access the Foundation's premises;
- the condition of isolation of the area surrounding the perimeter of some of the Foundation's locations;
- some premises of the Foundation being open to the public;
- the potential nature of the Foundation as a "sensitive target";
- previous cases of vandalism in the premises and in the immediate vicinity of the Foundation and the risk of recurrence.

The data collected are those strictly necessary to achieve the purposes set out in point 1 and those in support of civil trial proceedings to protect people and property from possible aggression, theft, robbery, damage and vandalism.

4. Processing methods and data storage period

The video surveillance system consists of cameras outside and inside the buildings identified in the following plans:

- Operational premises in via Sommarive 18, Povo:

- a) GENERAL POVO: A00
 - b) BLD N: A01, A02, A03, A04, A05, A06
 - c) BLD O: A02, A03, A04, A05, A06
 - d) BLD E: A03, A04, A05, A06
- Operational premises in via alla Cascata 56/C: A00, A01, A02, A03, A04, A05, A06, A07
 - Operational premises at Villa Tambosi - Strada delle Tabarelle 286, Villazzano:
 - a) GENERAL VILLAZZANO: A00
 - b) BLD VT: A01, A02, A03, A04
 - c) BLD RT: A00
 - Main offices in via Santa Croce 77, Trento: A00, A01, A02, A03, A04
 - Operational offices in vicolo Dallapiccola 12, Trento: A01

All information relating to the system is detailed in the document "Rete Impianti FBK.xlsx".

All the above documents are constantly updated and stored by the Corporate Assets Service in the shared folder "Patrimonio CAD".

The building plans include the following legend:

LEGENDA IMPIANTI ELETTRICI - TVCC	
SIMBOLO	DENOMINAZIONE
 X	Telecamera DOME PTZ
 X	Telecamera Fissa - Accessi Interni
 X	Telecamera Fissa - Perimetrali
 X	Postazione fissa Client visualizzazione immagini

Based on the legend, the type of camera installed can be identified in the above plans.

A) The system consists of different types of cameras and a single video recorder:

- Fixed and Dome digital cameras, associated with an NVR video recorder (see Milestone) located in the West building server room at the Povo Hub.
- The images recorded can be viewed with a software requiring authentication (Username and Password).
- The images are recorded H24 with Motion Detection function.
- Image retention has been set to a maximum of 120 hours.
- Dome type cameras are controlled by the designated officers only from the Povo

porter's lodge through keyboards and joysticks.

B) The images captured by the system are screened live through monitors positioned in the following reception areas:

- 1) Povo Hub (Guardiola):
 - All the images of the Povo Hub (EAST-NORTH-WEST building)
 - All the images of the Trento offices - via Santa Croce
 - All the images of the Trento offices - Vicolo Dallapiccola
 - All the images of the Villazzano offices
 - All the images of the Via alla Cascata offices
- 2) Trento offices:
 - Images of the Trento offices only
- 3) Villazzano offices:
 - All the images of the Villazzano offices
- 4) Palazzine alla Cascata:
 - Images of via alla Cascata offices only

The monitors are positioned in such a way that they are not visible to third parties.

Data is processed on subjects authorized to carry out these tasks, in accordance with the law, through the use of manual and automated systems, with logic designed to ensure data confidentiality, integrity and availability.

The Video Surveillance System Manager, appointed by the Board of Directors, designates the Authorized Data Processors who have access to the monitors or system management, providing them with appropriate guidance.

No automated decision-making process nor profiling activity is expected.

Considering the relevant security needs, images are stored for a maximum period of 120 hours. The images will be automatically deleted after this period, unless otherwise ordered by the judicial police.

5.Data communication

Without prejudice to disclosures made in compliance with legal or contractual obligations, the personal data collected and processed may be disclosed to the competent authorities upon their formal request for the purposes of the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security.

Personal data is not subject to disclosure.

6. Data Subject Rights

Data subjects may exercise the following rights referred to in Articles 15 et seq. of the GDPR in relation to their personal data:

- **Right to be informed:** this Privacy Notice is intended to provide data subjects with information regarding the processing of their personal data.
- **Right of access:** data subjects have the right to receive a copy of the personal data undergoing processing and to make a Subject Access Request.
- **Right to rectification:** where personal data are inaccurate or incomplete, data subjects have the right to obtain their rectification and/or completion.
- **Right to restriction of processing:** data subjects have the right to request the restriction or suppression of their personal data. This means that they may request the Data Controller to limit the way in which their personal data are processed or to delete them, where the applicable legal conditions are met.
- **Right to erasure ("right to be forgotten"):** data subjects have the right to obtain the erasure of their personal data. However, the Data Controller will retain personal data where there is a valid legal basis for doing so.
- **Right to object:** data subjects have the right to object, at any time, to the processing of their personal data, subject to the conditions laid down by the GDPR.

To exercise the above rights, data subjects may contact the Video Surveillance System Manager at: videosorveglianza@fbk.eu.

Data subjects also have the right to lodge a complaint with the competent Supervisory Authority. Information on the national supervisory authorities is available on the website of the European Data Protection Board (EDPB): https://edpb.europa.eu/about-edpb/about-edpb/members_en.

7. Security Measures

Personal data are processed by means of manual and automated systems designed to ensure their confidentiality, integrity and availability.

The Foundation implements appropriate technical and organisational measures to ensure the security of personal data processed through the video surveillance system.

Such measures include, among others:

- restricting access to the system exclusively to authorised personnel;
- the use of secure authentication mechanisms;
- the protection of the supporting IT infrastructure;
- periodic monitoring of the proper functioning of the video surveillance system.

8. Monitoring and Risk Assessment

The Data Controller carries out periodic checks to verify compliance with the applicable legal provisions and to ensure that authorised personnel comply with the instructions provided.

These reviews also take into account the Foundation's internal procedures on personal data protection, as well as the guidance provided by the Corruption Prevention, Transparency and Privacy Unit and the Data Protection Officer (DPO).

The video surveillance system is subject to periodic reviews to ensure that the processing remains proportionate to the purposes pursued and does not give rise to excessive risks for the rights and freedoms of data subjects.

The Data Controller has carried out a Data Protection Impact Assessment (DPIA) pursuant to Article 35 of GDPR) in accordance with the Foundation's Data Protection Impact Assessment (DPIA) Procedure, which governs the preliminary assessment, risk analysis and identification of appropriate mitigation measures.

The video surveillance system is also subject to periodic review, particularly in the event of technological changes, the extension of monitored areas or the installation of additional cameras.

9. Updates

This Document is subject to periodic review. All future changes to this Document will be duly communicated to Users and made public on the FBK website.