
Information on video surveillance activities at the USI Campuses

1. Introduction

The purpose of this information notice is to provide guidance on the processing of personal data collected by USI - Università della Svizzera italiana through the use of the video surveillance system installed on its Campuses. In particular, this notice is provided in accordance with the General Regulation on Video Surveillance at USI ("GRVS-USI") and the Provisions on the management of the video surveillance system ("PVS"), as amended from time to time, and in compliance with the applicable regulations to which the GRVS-USI refers.

2. Data Controller

This information notice is provided by USI - Università della Svizzera italiana, with registered office in Via Buffi 13, 6900 Lugano, Switzerland as Data Controller.

The Data Controller may be contacted by writing to the address of the registered office, by calling +41 58 666 40 00 or by sending an email to: info@usi.ch.

The Service of the Data Protection Consultant may be contacted directly at: privacy@usi.ch.

3. Purpose of the data processing, justification, categories of data and retention period

The provision of data is mandatory to access USI's internal and external premises and is essential to maintain and promote safety and public order on the campuses managed by USI, supporting the competent administrative or judicial authorities. The provision of data is therefore mandatory in the event of presence – subject to prior notice – within the areas subject to video surveillance. In any case, where possible, appropriate technical and organizational measures are implemented to limit the collection of and operational access to the processed data.

Purpose of the data processing	Justification	Categories of personal data	Retention period
To operate video surveillance in a deterrent manner in order to maintain and promote safety and public order on the Campuses, as well as to support the competent administrative or judicial authorities, and in particular to: - protect the life, physical integrity, and other legally protected interests of individuals using the facilities managed and monitored by USI;	Legal basis (Article 6(1) CAPDP i.c.w. art. 1 GRVS-USI).	Images of individuals present or transiting within the field of operation of the cameras. No audio recording takes place. In particular, the following uses are <u>prohibited</u> : the use of automatic facial recognition techniques, automated tracking functions of individuals, and automated behavioral analysis.	In accordance with Article 6(1) and (3) of the GRVS-USI, recorded images are retained for a maximum period of 30 days following their capture, after which they are deleted. A copy of the recordings may be retained for a period exceeding the established retention term, in the cases and under the conditions set out in Article 6(2) of the GRVS-USI.

- protect University assets and infrastructure;
- prevent and detect unlawful acts;
- manage any emergency situations involving legally protected interests safeguarded by the legal system.

In clearly defined cases, in particular at guard posts, video surveillance may be operated in a more intrusive manner (real-time monitoring with clear images) in order to manage access to administrative assets or facilities managed by USI, or to ensure their logistical operations.

Legal basis (Article 6(1) CAPDP i.c.w. art. 1 GRVS-USI).

Images of individuals present or transiting within the field of operation of the cameras.

No audio recording takes place.

In particular, the following uses are prohibited: the use of automatic facial recognition techniques, automated tracking functions of individuals, and automated behavioral analysis.

The images collected are retained solely for the deterrence purposes described in the aforementioned processing activity, under the applicable conditions.

In accordance with Article 4 of the GRVS-USI, video surveillance is managed in a manner proportionate to the purposes for which it is established. In particular, USI ensures that the installation and use of video surveillance equipment respect the private sphere, health, and freedom of movement of individuals in the areas under surveillance. In all cases, it is strictly prohibited to use or disclose recordings for purposes that, in good faith, would be incompatible with the aforementioned objectives.

In any event, it is strictly prohibited to use or configure the USI video surveillance system for the purpose of employing automatic facial recognition techniques, enabling automated tracking of individuals, conducting automated behavioral analysis, or viewing live footage and/or recordings without authorization and in the absence of a specific and legitimate purpose.

4. Categories of Data recipients

(1) Categories of Data Recipients:

In order to ensure the provision of the aforementioned services and in compliance with their respective purposes, the personal data referred to above shall, in principle, be processed and, where applicable, disclosed solely by the University's administrative staff, strictly to the extent necessary for the performance of their respective duties, in accordance with the roles, processes, and authorizations defined by the GRVS-USI and the PVS.

To the extent strictly necessary for the performance of the intended purposes, the personal data contained in the footage and recordings may, however, be transmitted to third parties, specifically:

- by way of viewing: to qualified persons and auxiliaries who, externally and on behalf of the Controller, provide services necessary to achieve the aforementioned purposes in support of its institutional activities; in particular, USI may allow viewing of the footage and recordings to external providers of surveillance and security services, as well as to their personnel, or to IT consultants of the video surveillance software provider for support in the management and configuration of the video surveillance system;
- in the event of civil, criminal, or administrative proceedings, video recordings may be transmitted to the competent authorities, to the extent necessary for evidentiary and/or investigative purposes. In such cases, the aforementioned parties shall act as independent data controllers and, accordingly, data subjects may contact such parties to exercise their rights, where applicable.

In all cases, the disclosure of personal data to third parties shall take place in the manner and under the conditions provided for in the GRVS-USI and the PVS, in applicable cantonal or federal regulations, and in accordance with the contractual safeguards established with any appointed parties.

(2) Cross-border disclosure of personal data:

As a general principle, data are managed and stored exclusively in Switzerland.

At the same time, if a transfer of data abroad for the processing of personal data as described above is deemed necessary, USI shall have the right to proceed accordingly. In this case, the Data Controller confirms that the transfer of data within or outside the EU will be carried out in compliance with the applicable regulations (in particular Art. 14a Cantonal Act on Personal Data Protection (CAPDP) and/or, if applicable, Arts. 16 et seq. Federal Act on Data Protection (FADP), undertaking in particular, where and to the extent necessary,

- to ensure that the recipient country guarantees adequate data protection;
- to guarantee an adequate level of protection by entering into specific agreements that include previously approved standard contractual clauses, or, exceptionally,
- to collect your specific consent for the transfer abroad.

5. Data Subject's rights

Where the conditions set out in the FADP, the CAPDP, and any applicable public-law provisions relating to video surveillance, as well as the Controller's internal regulations on data protection and video surveillance, are met, the Data Controller – taking into account the specific circumstances related to the operation of a video surveillance system – grants you, in particular, the following rights:

1. to request, through the competent civil, criminal, or administrative authorities, access to and, where applicable, a copy of the video recordings, under the conditions provided by law;
2. to request that any unlawful processing of your data be ceased, that personal data collected, stored, or otherwise processed unlawfully be destroyed, that the consequences of such unlawful processing be remedied, or that its unlawfulness be established;
3. to request that the disclosure of your personal data to third parties be blocked;

4. to lodge a complaint with the Cantonal Data Protection Commissioner should you disagree with the way USI processes your data (<https://www4.ti.ch/can/sgcds/pd/generalita>).

Please note that the above-mentioned rights may be partially or fully restricted by legal obligations to which USI is subject, or in the presence of overriding interests of USI or of a public nature.

To exercise the above rights, you are invited to contact the Data Protection Consultant Service at the following email address: privacy@usi.ch.

Last update: 01.07.2026 (v. 1.0.2-en).