



PRIVACY POLICY ON VIDEO SURVEILLANCE UNDER EU REGULATION 679/2016

This policy is provided under EU General Data Protection Regulation 2016/679 (hereafter the GDPR) and the General Video Surveillance Act issued by the Italian Data Protection Authority on 8 April 2010.

This supplements the abridged policy provided on the signs displayed near video cameras.

DATA CONTROLLER

The Data Controller is the Politecnico di Milano, in the person of the Director General delegated by the pro-tempore Rector (email: dirgen@polimi.it).

INTERNAL DATA PROCESSOR

Dr Raffaele Sorrentino, Head of Infrastructures, Estates and General Services, Piazza Leonardo da Vinci 32, Milan (MI) - tel. +39/02/2399.2260 – email: raffaele.sorrentino@polimi.it.

The personal data will be processed by other authorised parties who will receive instructions for that purpose under current legislation.

DATA PROTECTION OFFICER AND CONTACT PERSON

The Data Protection Officer (hereafter DPO) is Dr Vincenzo Del Core (email: privacy@polmi.it - tel. +39/02/23999378).

PROCESSING PURPOSES

Data collected by the video surveillance systems is processed, within the scope of the University's institutional purposes, to fulfil the following specific purposes:

Personal data processing purposes	Processing legal basis	Personal data categories	Personal data storage period
Purpose 1. Data will be processed exclusively for the purpose of protecting the University's assets against vandalism, damage and theft.	Public interest (Art. 6, para. 1, letter e) of the EU Regulation).	Images and video footage.	72 hours from recording (longer when the University is closed or at the request of the judicial authorities or the judicial police).
Purpose 2. Data will be processed to promote the safety of university staff, students and users of University premises.			Only if there is suspected or evident damage or crimes, images extrapolated at the express request of the subject filing the complaint may be stored for a maximum of 15 days pending request from the relevant authority.
Purpose 3. Data will be processed to prevent and detect any unlawful and unauthorised access to University premises (Once the retention period has expired, the images are

high risk places, IT infrastructures).			automatically and irreversibly deleted.
Purpose 4. Data may be processed to help judicial authorities or police investigations.	Legal obligation (art. 6, paragraph 1, letter c) of the EU Regulation).		

Please note that, under art. 4 of Italian Law 300/1970 (Workers' Statute), the systems employed are in no way used to monitor the work of professors, technical/administrative staff or anyone else working in the University in their various capacities.

MANDATORY AND NON-MANDATORY CONFERRAL OF PERSONAL DATA

The conferral of data is mandatory and is strictly instrumental to accessing University spaces subject to video surveillance. Non-conferral may result in the party being denied access to facilities.

CATEGORIES OF DATA RECIPIENTS AND POSSIBLE DATA TRANSFER

Under the above processing purposes, data collected through video surveillance systems may be accessed by purposely authorised Politecnico di Milano employees and partners who operate at the express request of the Data Controller or Data Processor according to their duties, using the assigned authentication credentials.

The data may also be communicated to external parties entitled to request it, such as the judicial or public security authorities.

TRANSFERRING DATA TO NON-EU COUNTRIES

The Data Controller will not transfer data acquired through its video surveillance systems outside the European Economic Area.

PROCESSING METHODS

Video surveillance (using fixed cameras) uses digital cameras connected to the University's data network, which allow real-time viewing of images in control rooms and porters' lodges, in addition to the 24/7 recording of images in "Motion Detection" mode.

Video surveillance is carried out primarily in external areas close to the University (e.g. access to campuses and buildings, car parks, loading/unloading bays, waste storage areas). No cameras have been installed inside lecture halls, laboratories and offices.

Images are normally recorded using long shots, but it is also possible to zoom in for demonstrable needs.

Processing is carried out electronically, for the purposes set out above and under the principles of lawfulness, fairness and transparency set forth by privacy regulations. Please note that:

- Footage is stored on electronic media and storage servers located at the Data Controller's premises and may only be processed by authorised personnel;
- Video footage and any personal data may be made available to the judicial authorities or the police (at their express request) to help detect the perpetrators of unlawful deeds carried out to the detriment of the Data Controller and other parties;

- Security measures have been adopted, under art. 32 of the GDPR, to prevent any loss of data and any unlawful or improper use and unauthorised access to data, in compliance with Circular no. 2/2017 issued by AgID (Agency for Digital Italy): “Minimum ICT security measures for public administrations”;
- The video surveillance system is not connected to private surveillance institutes or police forces.

DATA SUBJECT RIGHTS

Data subjects (clearly identifiable from any video footage recorded) may contact the University to exercise the rights laid down by the GDPR, and more precisely:

- Right of access to personal data and to information under art. 15 of the GDPR;
- Right to object to the processing of personal data concerning the data subject, without prejudice to the mandatory nature of data processing to benefit from the services offered;
- Right to restrict processing under art. 18 of the GDPR;
- Right to erase data (‘right to be forgotten’), except for data contained in deeds which must be stored by Politecnico di Milano unless there are overriding legitimate grounds for the processing.

Data subjects acknowledge that, given the intrinsic nature of the data processed (images collected in real time), it is not feasible to exercise the right to update, supplement or rectify data as set forth by art. 16 of the GDPR. It is equally unfeasible to obtain the data portability right, under art. 20 of the GDPR, since images acquired via the University’s video surveillance system cannot be transferred to other parties (except in the cases referred to in the above section “CATEGORIES OF DATA RECIPIENTS AND POSSIBLE DATA TRANSFER”).

Data subjects clearly identifiable from any video footage recorded may request access to the footage in which they allegedly appear (attaching a valid ID document to their request). However, in such cases, data subjects shall not be given access to the data of other parties, and in no case will it be possible to extract images or selectively mask parts of video frames.

To exercise the right to access video footage and for more information, data subjects may contact the Politecnico di Milano Contact Center (email: contactcenter@polimi.it - tel. +39/02/23999300). To exercise the above-mentioned right to object to data processing, the right to restriction of processing and the right to erasure of data, data subjects may contact the Politecnico di Milano DPO.

Data subjects may lodge a complaint with the Italian data protection authority, i.e. the Autorità Garante per la Protezione dei Dati Personali (www.garanteprivacy.it).