



Thematic Privacy & Personal Data Protection Policy

Camera Surveillance



Table of Contents

1. Introduction	3
2. Scope of this Policy	3
3. Principles	3
4. Camera Surveillance	4
4.1. Lawfulness and Efficiency	4
4.2. Information Presence Cameras	5
4.3. Camera Placement	5
4.4. Security and Storage of Camera Images	5
4.5. Viewing and Transmission of Camera Images	6
4.6. Right of Access by the Data Subject	6

Readers' Guide

This Thematic Policy is part of the Privacy & Personal Data Protection Policy and describes, for camera surveillance purposes, the way in which Tilburg University implements the General Data Protection Regulation (GDPR) with regard to the protection of Personal Data.

All information regarding European legislation (GDPR) and the protection of Personal Data is included on the **Tilburg University website**¹ including the Frequently Asked Questions.

Each School/Division within Tilburg University has appointed so-called Data Representatives, who are the first point of contact for employees in case of questions about the protection of Personal Data.

The Policy includes references to other policy documents, which are marked as “**referrals**”, and the applicable guidelines are set out in blocks to make them easy to find:

Subject

Guideline

When *he* is referred to in this Policy, it is understood to mean he/she or gender-neutral.

For the filming, photography, and sound recording on the Tilburg University campus, the rules of conduct as included in the **Tilburg University House Rules**² and the **Student Charter** apply³. For the filming of lectures we also refer to the **Thematic Policy Education and Students**.

¹<https://www.tilburguniversity.edu/intranet/support-facilities/legal/legalprotection/privacy/>

²<https://www.tilburguniversity.edu/about/tilburg-university/conduct-integrity/house-rules/>

³<https://www.tilburguniversity.edu/students/studying/regulations/charter/rules-of-conduct/>

1. Introduction

General policy	The Tilburg University Privacy & Personal Data Protection Policy is applicable. If there are any details that apply to camera surveillance, these are included in this Policy.
Other guidelines Camera Surveillance	<ul style="list-style-type: none">- Policy Rules for Camera Surveillance of the Authority for Personal Data;- Policy Memorandum on Security Systems of December 7, 2006 (Adopted by the Executive Board on January 9, 2007 and University Council of February 1, 2007), supplemented by the decision to extend the storage period for visual material (Adopted by the Executive Board on January 13, 2009 and University Council of February 6, 2009).

2. Scope of this Policy

The Thematic Policy Camera Surveillance applies to **all Processing of Personal Data** that takes place in relation to camera surveillance on the Tilburg University campus.

This Policy applies to those who are charged with activities relating to camera surveillance and concerns all those who are located in the buildings or on the premises of Tilburg University (Data Subjects).

Responsible for policy compliance	The Managing Director of Facility Services is ultimately responsible for compliance with the legislation and regulations regarding the privacy & protection of Personal Data. The responsibility for compliance with these guidelines lies with the person making the recordings.
--	---

3. Principles

The principles with regard to Privacy & Processing of Personal Data are the same as the principles in the **Privacy & Personal Data Protection Policy**.

4. Camera Surveillance

4.1. Lawfulness and Efficiency

The processing basis for camera surveillance is:

Basis for processing (Article 6 GDPR)	Explanation
Necessity for legitimate interest	<ul style="list-style-type: none">• The Processing must be necessary for the representation of the legitimate interests of Tilburg University or a Third Party;• A balancing of interests also applies: Processing may not take place if the interests or fundamental rights and freedoms of the Data Subject outweigh the aforementioned interests of Tilburg University or a Third Party;• The Data Subject may object to the Processing at any time, after which Tilburg University discontinues the Processing or puts forward compelling justified grounds for exceeding the objection.

Tilburg University uses camera surveillance on campus and in buildings for security purposes; according to the legislation, camera surveillance must be proportional and subsidiary. Each time a camera is installed, it must be considered whether the intended purpose can be achieved in a different, less intrusive way. Compared to the application of human monitoring on the same scale, camera monitoring has the advantage that continuous monitoring is possible at a lower cost.

Tilburg University uses the following security measures, among other things:

- human monitoring or the surveillance monitoring system;
- Access Control System

Because these measures have proven to be insufficiently effective (and in relation to cost benefits), Tilburg University also uses video camera surveillance for the following purposes:

- a higher degree of security and safety of persons, goods, buildings, and sites entrusted to the care of Tilburg University;
- preventative effect regarding theft, burglary, and violence;
- increasing the possibilities of detection in the event of theft, burglary, or violence.

Tilburg University takes the following into consideration with regard to the processing of Special Personal Data:

- The purpose of processing camera images is not to process Special Personal Data or to make a distinction on the basis of Special Personal Data,
- it is not reasonably foreseeable for Tilburg University that the Processing will lead to a distinction being made on the basis of a Special Personal Data, and
- the processing of special personal data is, however, unavoidable when processing camera images for the abovementioned purposes.

Permitted reasons for camera surveillance	<p>The collection of Personal Data obtained by the camera is only permitted for the purpose of:</p> <ol style="list-style-type: none"> 1. the protection of the safety of one or more natural persons entrusted to the care of Tilburg University, 2. the security of the buildings and sites, 3. the security of items located in the buildings or on the premises of Tilburg University, and 4. the recording of incidents with a view to the investigative proceedings after identified incidents.
--	--

4.2. Information Presence Cameras

Information on camera surveillance presence	<p>Camera surveillance is in place at the premises of Tilburg University, which is indicated by signs and/or stickers at the entrance to the premises and at the entrance doors to buildings.</p>
--	---

4.3. Camera Placement

Cameras requirements	<p>Tilburg University applies the following requirements to the placement of the cameras.</p> <ul style="list-style-type: none"> • The cameras are <u>static cameras</u> and are set up in such a way that they always capture the same area, whereby the proportionality of this area is checked beforehand; • cameras may <u>never</u> be placed in sensitive areas, such as changing rooms, toilets, or treatment rooms; and • the video cameras do <u>not record sound</u> but only video.
-----------------------------	---

It may be necessary to use covertly placed cameras in some cases.

Concealed camera	<p>In the event of reasonable suspicion or suspicion of an unlawful act, concealed cameras may be used without the Data Subjects being informed.</p> <p>This is only permitted with the approval of the Executive Board.</p>
-------------------------	--

4.4. Security and Storage of Camera Images

Camera Image Security	<p>The camera images shall be adequately protected (both physically and technically) and stored to ensure that the data are accurate and to prevent the loss or unlawful processing of Personal Data. The measures shall ensure an appropriate level of security for the category HIGH, taking into account the technical state of the art and the cost of their implementation. For further information, please refer to the Information Security Policy.</p>
Camera image storage period	<p>The recorded video images are <u>stored for 24 hours on a working day, for 72 hours at weekends, and for longer periods up to and including</u></p>

	<p>the first working day until 4 p.m. in the event of consecutive public holidays and/or collective holidays of Tilburg University, in order to be able to support the investigation into incidents in these specific periods.</p> <ul style="list-style-type: none"> • The images may only be stored for more than 72 hours if an incident is detected, in which case they will be safeguarded and stored by order of the Executive Board until the incident has been dealt with.
--	---

4.5. Viewing and Transmission of Camera Images

It is important that only authorized persons have access to the camera images.

Access to camera images	<p>Review is only allowed for:</p> <ul style="list-style-type: none"> • employees of the Safety and Security team of the Safety and Document Services unit and the relevant supervisor; • Director Facility Services; • (functional) application manager of the systems. • in the context of incidents: <ul style="list-style-type: none"> ○ the Secretary General of the University ○ Legal Affairs ○ the Governance, Risk & Compliance Officer.
Motivation to view camera images	<p>The data recorded through camera surveillance can be analyzed for the purpose of detecting unlawful behavior or further investigating unlawful behavior if there is a reasonable suspicion or a presumption of an unlawful act by one or more Data subjects.</p>
Viewing the location	<p>Camera images should only be viewed in the area designated for this purpose.</p>
Disclosure to third parties	<p>The camera images are only disclosed to the judicial authorities (in a technically secure manner) in the context of a claim, in compliance with the procedure for securing and delivering camera images to the judicial authorities.</p>

4.6. Right of Access by the Data Subject

Right of access	<p>The Data Subject will have the right to inspect the personal data recorded about him if these are stored for more than 72 hours and if this is in the interests of further investigation.</p>
------------------------	--