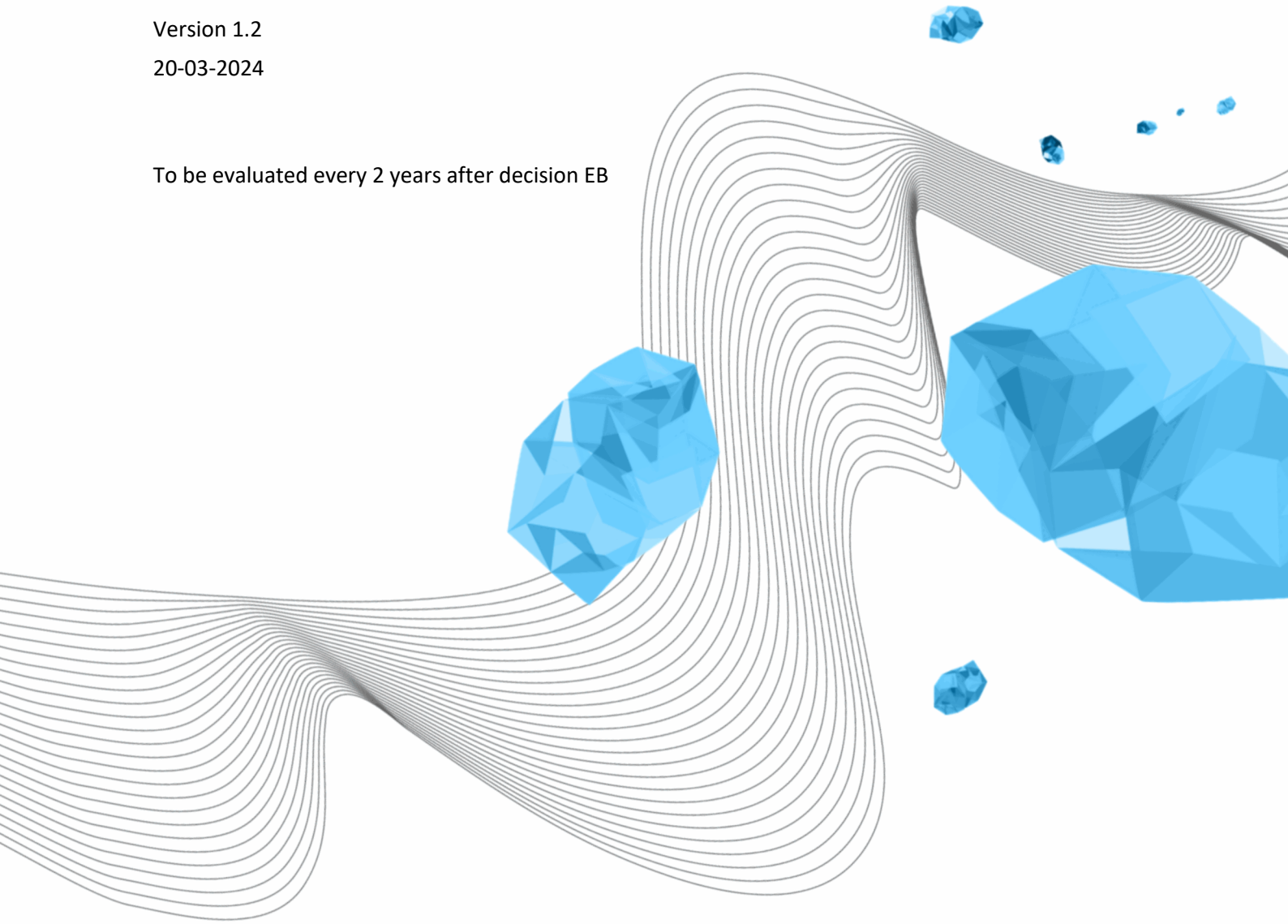
READING GUIDE CAMERA SURVEILLANCE REGULATIONS

Version 1.2

20-03-2024

To be evaluated every 2 years after decision EB



UNIVERSITY OF TWENTE.

PUBLISHING DETAILS

ORGANISATION
General affairs

TITLE
Reading guide camera surveillance regulations

VERSION
1.1

DATE

20-03-2024

AUTHOR
Erwin Medendorp

DOCUMENT HISTORY

VERSION	DATE	AUTHOR	COMMENTS
1.0	24-02-2023	M. van de Ven-Davids	First draft
1.1	06-03-2023	M. van de Ven-Davids	A number of amendments
1.2	20-03-2023	Erwin Medendorp	Small amendments based on discussion UCM

CONTENTS

READING GUIDE FOR CAMERA SURVEILLANCE REGULATIONS

This reading guide accompanies the Camera Surveillance Regulations version 2.4 (hereinafter referred to as 'the Regulations'). This reading guide aims to provide further explanation and background to the various provisions of the Regulations.

GENERAL

The Regulations apply to Camera Surveillance on the University of Twente (UT) campus.

By means of the Regulations, Data Subjects are informed about the processing of their personal data in accordance with Article 14 of the General Data Protection Regulation (GDPR).

Terms in this reading guide have the same meaning as in the Regulations (see Article 1 of the Regulations).

Where possible, further explanation and background on each of the articles of the Regulations will be provided below.

Cameras have been set up on UT's campus and buildings to protect the safety of people and buildings and to record Incidents. These Regulations apply to the camera system used for this purpose. These Regulations do not apply to cameras installed for any other purpose (e.g. to monitor a laboratory test or the cameras installed by third parties in rented rooms on the UT campus). Or the cameras installed by third parties in rented premises on UT premises. For use of other cameras, please refer to the rules for use of cameras not intended for camera surveillance.[1]

EXPLANATORY NOTES TO ARTICLE 1 TERMS AND DEFINITIONS

Various terms are explained in this article. It has been decided not to mention names for various positions and roles, as this would result in the Regulations no longer being up to date if the relevant position or role were to be filled by someone else. These include the Administrator (in the present case the CFM Director) and the Functional Administrator. The CFM website shows who fills the role of CFM Director[2]. The CFM Director may specify who is the Functional Administrator. Contact details can be found[3] on UT's People Pages.

[1] See https://www.utwente.nl/nl/cyber-safety/cybersafety/wetgeving/regels-voor-cameragebruik.pdf
[2] See https://www.utwente.nl/en/service-portal/services/cfm/about-us-contact/#organisation-cfm
[3] See https://people.utwente.nl/

EXPLANATORY NOTES TO ARTICLE 4 RECORDING AND USE OF DATA

The 2016[4] policy regulations on the application of provisions of the Personal Data Protection Act and the Police Data Act of the Data Protection Authority (DPA) state with regard to indicating where cameras are placed:

> *'This means that placing a single sign at a central location within the camera area is not sufficient. In any event, those affected should be made aware at the edges of the camera area that they are entering a camera area. The cameras themselves, however, need not be visible. Nor does it have to be visible whether the cameras are in operation.*
>
> *Furthermore, the requirement of recognisability must be met not only when images are captured, but also when monitoring is involved and therefore no recordings are made.'*

UT has placed signs on the various roads and bicycle paths that provide access to the campus. Camera Surveillance has also been made known at building entrances.

EXPLANATORY NOTES TO ARTICLE 5 INCIDENTS

A strict test generally applies when deploying covert Camera Surveillance. The general principle is that it is not permitted, as it represents a major invasion of personal privacy.

It follows from the Data Protection Authority's 2016 policy regulations on the application of provisions of the Personal Data Protection Act and the Police Data Act:

> *p. 21-22*
>
> ***Covert Camera Surveillance***
>
> *Covert Camera Surveillance is generally not permitted, as it represents a major invasion of privacy. The principles of proportionality and subsidiarity will only be met in exceptional circumstances. This may occur in case of theft or fraud, or a reasonable suspicion thereof, and other measures taken have not been able to put an end to this. In addition, covert Camera Surveillance may only be used temporarily.*
>
> *If there are no exceptional circumstances, it is a criminal offence and the person filmed by a covert camera can report the offence to the police under Articles 139f(1) and 441b of the Dutch Penal Code.*
>
> ***Example: necessary***
>
> *In a car park, cars are often vandalised at night. The car park owner has already erected a fence around the car park, installed extra lighting and arranged for a security guard to patrol more frequently. However, these measures did not prove to be sufficiently effective, leading the car park operator to decide to deploy Camera Surveillance. The cameras are only switched*

[4] See https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_cameratoezicht-.pdf The policy regulations are still based on the Personal Data Protection Act (PDPA), the predecessor of the General Data Protection Regulation (GDPR). These policy regulations are also applicable to the General Data Protection Regulation.

on during the night-time hours. The car park operator has therefore demonstrated the necessity (proportionality and subsidiarity) of Camera Surveillance.

Example: not necessary

A company has deployed Mystery Shopping with hidden cameras. The cameras film the staff as part of a training exercise. The company opted for the deployment of covert cameras due to unsatisfactory results from previous training. The learning effect following concrete examples from one's own work situation would be greater after general educational insights, according to the company, than after only a general talk on sales technique. However, in doing so, the company does not sufficiently argue why the deployment of covert Camera Surveillance is the ultimate remedy to achieve the training objective. A greater learning effect can also be achieved otherwise and by less intrusive means, for example through role-play, mystery shoppers without a covert camera and customer orientation courses. It follows that the use of covert camera observation is not necessary.

p. 29-30

Covert Camera Surveillance

Similarly, the provision of information to Data Subjects may be omitted insofar as this is necessary in the interests of preventing, investigating and prosecuting criminal offences (Article 43(b) of the Personal Data Protection Act). This ground for exemption may apply to an employer who institutes covert Camera Surveillance because of theft or fraud (or a reasonable suspicion thereof). In that situation, however, the following conditions apply:

- *The employer must inform all employees in general terms in advance about the possible use of covert Camera Surveillance in the future.*
- *If there is an employee council or staff association, this employee council or staff association must have agreed to an arrangement regarding such processing.*
- *The employer must always inform employees afterwards about the covert Camera Surveillance if it has actually deployed this. In fact, the duty to inform of Article 34 in conjunction with °Article 33 of the Personal Data Protection Act resumes as soon as covert Camera Surveillance is no longer necessary in the interests of preventing, investigating and prosecuting criminal offences. The employer must personally inform those affected (e.g. the offender).*

Example: failure to comply with duty to inform

A camera is hanging immediately after the entrance to a shop. Behind the shop's counter is a sign saying 'For your and our safety, camera surveillance is used here'. This practice is not permissible, as the provision of information must take place before the visitors to the shop are filmed. The sign should therefore have been visible from the entrance to the shop.

Example: compliance with duty to inform

Camera Surveillance is used in a shop. There is a clear sign with a symbol of a camera at the entrance to the shop, before visitors are filmed. It is clear from the context that the cameras

serve to secure the goods in the shop, and that the shop owner is the responsible party. The duty to inform is complied with in this case.

Example: failure to comply with duty to inform

Camera Surveillance is used at a business park. There is a clear sign with a symbol of a camera at the entrance to the business park. This sign with only a symbol is not sufficient in this case, as it is not clear to visitors to the business park who is the responsible party. The sign should therefore have included the name of the responsible party.

Example: informing after covert Camera Surveillance ends

A transport company has a reasonable suspicion that an employee regularly commits a theft of cargo from a truck when transporting the cargo. The company sets up covert Camera Surveillance of the truck in which, and the times when, the employee in question transports the cargo. This films other employees helping to load and unload the cargo, as well as random passers-by. At the end of the surveillance, the company must inform all employees who were filmed about the deployment of the covert cameras. However, the company cannot find out who the random passers-by are. It would be impossible, or at least take a disproportionate effort, to inform these passers-by as well. The company therefore does not have to inform the passers-by in this case. However, the company must establish the origin of the Camera Images. Incidentally, Camera Images should not be kept for longer than is necessary for their purpose. Therefore, when the images are not or are no longer necessary to deal with the issue related to the theft, the company should immediately destroy the images.

It follows from the Data Protection Authority[5]'s decree on the list of Personal Data processing operations for which a Data Protection Impact Assessment (DPIA) is mandatory that a DPIA is mandatory for the deployment of covert Camera Surveillance:

Covert investigation
Large-scale processing of Personal Data and/or systematic monitoring involving the collection of information by means of research without informing the Data Subject in advance (e.g. covert investigations by private investigation agencies, anti-fraud investigations and internet investigations in the context of, for example, online copyright enforcement). A Data Protection Impact Assessment (DPIA) is also mandatory in the event of covert Camera Surveillance by employers in the context of theft or fraud prevention by employees. In the latter type of processing, a Data Protection Impact Assessment (DPIA) should also be carried out in incidental cases due to the unequal power relationship between the Data Subject (employee) and the data controller (employer).

EXPLANATORY NOTES TO ARTICLE 6 SHARING CAMERA IMAGES WITH THIRD PARTIES

When there is an Incident or the sharing of the Camera Images is deemed necessary to contribute to safety (or the feeling of safety) on UT campus grounds and in UT buildings, UT may decide to share Camera Images with this third party at the request of third parties, including the housing association

[5] See https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf

(which owns, amongst other things, student residences on the UT campus grounds). Guarding property is an example of contributing to security on UT's campus and buildings.

Providing Camera Images to third parties is a type of processing of Personal Data, for which UT needs a purpose and basis. These should be determined on a case-by-case basis.

Disclosure to housing association

UT sees it as its duty to create a safe environment on campus. Some buildings, such as student residences, are owned by the housing association. In case of Incidents at the relevant student residences, UT can share the Camera Images with the housing association so that possible suspects can be identified and, for instance, damage done to the buildings can be recovered from the perpetrators, the buildings can be secured and the Incidents recorded. The provision of Camera Images to the housing association can therefore contribute to the overall feeling of safety on campus.

Providing Camera Images to third parties is a type of processing of Personal Data, for which UT needs a purpose and basis. The housing association may have a legitimate interest (Article 6(1)(f) of the General Data Protection Regulation) in the provision of the Camera Images, for example the interest to protect property and to recover any damage. These are not the interests of UT, but under the General Data Protection Regulation recourse to legitimate interest is also open if it serves the interests of a third party (the housing association). In his opinion to the European Court of Justice the Advocate General considered:

> *"The Court has already ruled that transparency (16) and the protection of property, health and family life (17) are legitimate interests. The concept of legitimate interest is sufficiently flexible to take into account other considerations. I have no doubt that a third party's interest in obtaining Personal Data from the person who has caused damage to his property, in order to recover the damage from that person in court, can be considered a legitimate interest."*[6]

UT may also have its own legitimate interest in sharing the Camera Images with the housing association. This is because UT's aim is, among other things, to ensure safety on campus, recording Incidents and, as part of this, being able to share Camera Images with third parties if necessary. UT must weigh up whether it can invoke this principle on a case-by-case basis using the three criteria:

1) is there a legitimate interest (of the housing association and/or UT),
2) is the provision necessary and
3) does the balancing of interests between the interests of UT/the Housing Association, on the one hand, and the interests of Data Subjects (impact on privacy), on the other, fall in favour of UT and the housing association?

This should be assessed on a case-by-case basis. This will include whether the Camera Images is shared with the housing association only after an Incident, with only the images relevant to that Incident, or whether, for example, all images are handed over. The privacy impact on Data Subjects should be minimised as much as possible.

[6] Conclusion of AG M. Bobek of 26 January 2017, ECLI:EU:C:2017:43 (State Police Riga Regional Directorate, Criminal Police Board), Spatial Planning 65.

It is also important who is visible on the Camera Images. In the event of an Incident, is only the perpetrator/suspect visible in the images, or also third parties? If third parties are also visible, their privacy interests also play a role in the overall consideration.

EXPLANATORY NOTES TO ARTICLE 7 RIGHTS OF DATA SUBJECTS

The rights of Data Subjects are discussed in Articles 12 to 23 of the General Data Protection Regulation. UT cannot or need not always honour requests from Data Subjects, see Article 23 of the General Data Protection Regulation, Article 41 of the GDPR Implementation Act and, for the right to deletion, Article 17(3) of the General Data Protection Regulation. This will be assessed on a request-by-request basis.

Regarding a request on the right to deletion: UT does not have to honour such a request, if UT would have to bring a civil claim for damages against a Data Subject due to deletion.

Also, such a request need not be met if the Personal Data in question is necessary for the prevention, investigation, detection and prosecution of criminal offences.

EXPLANATORY NOTES TO ARTICLE 8 COMPLAINTS

The complaints procedure can be found here.