PRIVACY STATEMENT CAMERA SURVEILLANCE EY NEDERLAND

This Privacy Statement informs you about the way in which EY processes personal data about you when applying camera surveillance at our locations in the Netherlands. Below you will find the most important points from our Privacy Statement. For more information, click on the headings with subjects under the summary.

PRIVACY STATEMENT CAMERA SURVEILLANCE EY NEDERLAND

This Privacy Statement will inform you about the processing of your personal data when using camera surveillance on our locations, for which the entities of the EY network of Ernst & Young Global Limited (jointly referred to as "EY", "We", "Us" or "Our") situated in the Netherlands are responsible. You can find a list of the entities it concerns via this link (no 380-392).

We process your personal data for, e.g.:

- the protection of the health and safety of persons;
- (supporting) the security of (access to) the buildings and premises of EY and the prevention of burglary, theft and vandalism;
- the monitoring of materials and information located in the buildings or on the premises of EY; and
- the recording of incidents.

For further information about the purposes for which your data is used in this context, please refer to the section "What do we use which personal data for?" below.

You have various privacy rights with regard to our processing of your private details. You can have the right:

(i) to insight into your personal data (right to insight);
(ii) to deletion of personal data when we (no longer) may process this data (right to have data deleted);
(iii) that we will keep your personal data even if we will (no longer) process it or when this is open for discussion (right to restrict the processing);
(iv) to **object to** the processing of your personal data in certain circumstances (right of objection)
(v) to submit a complaint with an authorised supervisor when you find out that there is a privacy infringement.

Please refer to the paragraph "What are your privacy rights" for more information about your privacy rights. Find our contact details in the paragraph "How to contact us?".

1. What is the relation between this Privacy Statement and other documents?

1.1 Other Privacy Statements of EY

This Privacy Statement specifically describes how we process your personal data when applying camera surveillance at our locations in the Netherlands. However, we may also process your personal data in another context, for example when you have an appointment at one of our offices or make use of our services. Please refer to the EY General Privacy Statement NL for the Netherlands (available via this link), and the EY General Privacy Statement on a global level (available via this link). This Privacy Statement forms an additional / detailed explanation of the general Privacy Statements, and how it prevails.

If EY also processes your personal data for other purposes, another specific Privacy Statement may apply to this processing. In that case you will be separately informed about this.

1.2 Privacy Statements of other parties

This Privacy Statement is not applicable to service provisions of third parties for which these third parties are themselves responsible. Think for example of cameras of third parties (such as building owners) that are placed in such way that they also record buildings and sites of EY. For information about how these third parties process your personal data, we refer you to the privacy statements and/or other information supplied by these parties.

2. Which personal data is used for what?

2.1 Purposes of processing personal data during camera surveillance

We place cameras and process your personal data for the following purposes:
- the protection of the health and safety of persons;
- (supporting) the security of (access to) the buildings and premises of EY and the prevention of burglary, theft and vandalism;
- the monitoring of materials and information located in the buildings or on the premises of EY; and
- the recording of incidents.

Recorded camera images and related personal data can then also be used for:
- investigating and handling (possible) incidents; and
- internal control operational management (including audits);
- processing any requests, complaints and disputes;
- accepting, exercising and defending our rights; and
- complying with legal obligations and professional regulations, and requests of authorised government institutions.

In a separate document, for each camera installed, a brief description is given about how the applicable privacy requirements are met. If needed, the person concerned may inspect the aforementioned document.

2.2 The persons involved in camera surveillance

As part of our camera surveillance, we process personal data about the following categories of persons:

- **Persons being filmed**. This concerns all persons who come within the visual range of one of our cameras. As far as persons are concerned, this depends on where the camera is installed. For example, a camera in an arrival hall can capture images of all kinds of visitors to one of our offices, while a camera in a certain department will in principle only capture images of people with access to that department.
- **Persons with request in relation to camera images**. This concerns persons who have submitted a request in relation to certain camera images, without necessarily being shown on these images themselves. Think, for example, of a request to find out how someone's car was damaged, or someone's request to erase certain camera images when someone doesn't even appear to be on them.
- **Persons who have/can have access to camera images**. This concerns persons who have or can have access to the camera images on the basis of their access rights. Think for example of security staff, but also IT or helpdesk staff in case of connection problems. Please refer to the section "Who has or will have access to your personal data" below.
- **Persons who have access to camera images**. This concerns persons who, on the basis of our logging and other records, have been given actual access to certain camera images. In addition to the above examples, think here also of persons involved from, for example, the police or an insurance company.

For each camera installed, a brief description is given in a separate document, of how the applicable privacy requirements are met. If needed, the person concerned may inspect the aforementioned document.

2.3 The types of personal data we process at camera surveillance

The kind of personal data we process with camera surveillance will depend on the type of camera and how it is set up. Below is an overview of personal data that in a general sense can be processed during camera surveillance. In a separate document, for each camera installed, a brief description is given of how the applicable privacy requirements are met. If needed, the person concerned may inspect the aforementioned document.

2.3.1 Personal data in general

With our camera surveillance, we process the following categories of personal data:

- **Personal data relating to persons being filmed**.
    - The camera images themselves;
    - Time of an image capture;
    - Location of an image capture;
    - Written report of an image capture;
    - Data regarding who has/can have access to the camera images;
    - (Log) data regarding who actually had access to the camera images; and
    - Data relating to a related request or communication (e.g. when reporting an incident such as theft or vandalism).
- **Personal data relating to persons who have/can have access to camera images**.
    - Name, job title and contact information;

- The type of camera images to which the person has/can have access and possibly the conditions for it.

- **Personal data relating to persons who have/can have access to camera images**.
  - Name, job title and contact information;
  - The type of camera images to which the person has been given access and possibly the reason why and the conditions for it.
- **Personal data regarding persons related to the camera images by request or communication**.
  - Name, job title and contact information;
  - Information about the link between this person and the request or communication regarding certain camera images.

2.3.2 Sensitive personal data

In principle, all camera surveillance applied within EY is not used for the purpose of processing sensitive personal data, including special categories of personal data as referred to in the General Data Protection Regulation ((EU) 2016/679). The images are not processed for the purpose of deducing special categories of personal data.

With the camera surveillance within EY, no biometric data are processed. Insofar as this is different for a specific camera, a separate document specifies on which exception to the processing ban/specific basis EY the processing is based. If needed, the person concerned may inspect the aforementioned document.

2.4 The legal basis on which we base the processing of personal data in case of camera surveillance

We base the processing of your personal data at our camera surveillance on the legal basis 'legitimate interests'. This means that a balance of interests is performed between the interests that are served by the processing on the one hand and your privacy interests on the other hand, and that the interests of the processing weigh more. Our interests in the processing of personal data within the framework of camera surveillance consist of the realisation of the purposes mentioned in the subsection "Purposes of processing personal data within the framework of camera surveillance" above.

Aspects taken into account when balancing interests
When weighing up the interests, the following aspects were taken into account, where relevant:

- If other solutions that have less privacy impact can be applied instead of camera surveillance (e.g. improved physical security or access control);
- The number of people filmed (e.g. purely the number or in relation to a certain group);
- The way the camera images are used (e.g. only consulted in case of an incident, versus always being analysed);
- The reasonable expectations of the persons being filmed (e.g. no camera surveillance in toilet, shower and prayer rooms); and
- Factors specific to the situation or the category of persons filmed (e.g. at an event organized for students).

As privacy friendly as possible
When using a camera, we investigate how this can be done in a way that minimizes invasion of the privacy of the persons being filmed. For example, we take into account as far as relevant:

- The kind of camera used (infrared, colour, black and white and the quality/detail of the images);
- The range of the camera and how it is adjusted;
- The functions of the camera (e.g. facial recognition or analysis capabilities);
- At what times camera surveillance takes place;
- Whether the camera images are recorded or not and - if so - for how long; and
- Who has access to the camera images under which conditions.

In a separate document, for each camera installed, a brief description is given of how the applicable privacy requirements are met. For each camera, EY registers why it was placed at a certain location, along with a motivation: why creating images is necessary to achieve that purpose and which of the above safety precautions EY has taken to prevent or limit undesirable consequences for the privacy of the persons being filmed. If needed, the person concerned may inspect the aforementioned document. In addition, if you want more information about balancing of interests, you can contact us directly (we refer to the paragraph "How to contact us?").

2.5 Minors and other persons with a legal representative

We do not focus our camera surveillance on persons under the age of 16. We also do not focus on people who are under liquidation or who are supervised or administered by someone else. If, in exceptional cases, we do focus on such persons with a legal representative, EY will take into account the vulnerable position of these persons and take specific measures where necessary.

3. How do we obtain your personal data?

3.1 Manner of obtaining personal data

We obtain your personal data in different ways:

- **Observed and/or recorded by us**. When applying our camera surveillance, we process data about the persons shown on the camera images. When these images are only viewed live, it concerns observed images. When these images are (also) recorded, it concerns captured images.
- **Supplied by you.** Some personal data we receive straight from you. Think for example of data you provide us when you request access to certain camera images.
- **Internally received.** It is possible that we could receive your personal data from other EY systems. Think for example of research in internal systems that is carried out following an incident - such as vandalism - that is shown on certain camera images.
- **Received from third parties.** We could also receive your personal data from other persons or external parties. Think, for example, of information obtained from colleagues or the police when investigating an incident - such as vandalism - that is shown on certain camera images.

- **Automatically obtained.** We obtain some personal data automatically. Think for example of the date and time to which camera images relate, which can be tracked automatically.
- **Derived.** Certain personal data we do not receive directly, but we can derive it from the information already in our possession. Think of data about your presumed involvement in an incident, for example based on license plate data that are visible on certain camera images, combined with the data known to us about this (regarding to whom the car with the relevant license plate belongs).

3.2 Compulsory provision of personal data

In principle, you are not obliged to provide any information about yourself to us as part of our camera surveillance. However, it may be the case that not providing certain data has a negative impact. For example, not answering questions following an incident can lead to further investigation.

If the provision of certain personal data is a legal or contractual obligation or an essential requirement for concluding an agreement with us, we will separately provide additional information about this if that is not clear in advance. We will then also inform you about the possible consequences of not supplying this data.

4. Who has or obtains access to your personal date?

4.1 Parties who have or may have access to your personal information

Camera images and related personal data may be shared on a need-to-know basis with authorized persons within one of the parties listed below. Within EY these are the designated employees of AWS Facilities and Risk Management NI-Security as well as the relevant office chairman. "Need-to-know" means that a party only gets access to personal data if and insofar as this is necessary to perform the activities performed by this party.

- The relevant EY entity involved in the relevant processing activity. Think, among other things, of the EY entity responsible for placing the camera.
- Affiliated entities within the EY network, who are involved with the relevant processing activity. Examples include the EY entity that owns/manages the location to which the camera surveillance relates.
- Service providers/subcontractors engaged by EY, who are involved in relevant processing activities. Think, among other things, of the possible external supplier and manager of a camera.
- A party that is also involved in the processing of personal data. Think here about any external owner of the building/plot on which the camera surveillance is focussing, involved insurers, professional advisors such as lawyers who have been called in as part of an incident, external investigators/research agencies who have been called in as part of an incident, and the victims of an incident.
- Authorised government institutions. For example, the police or other competent government agency if it is involved in following up an incident or otherwise requests footage to which EY must respond.

4.2 Requirements for sharing your personal data

Third parties may not use your personal data which we share with them for their own direct marketing purposes. In doing so, we will only share your personal data with a third party without your consent when:

- This is necessary for the service provision or involvement of the third party. Subcontractors will for example in principle only gain access to the personal details that they require for their part of the service provision.
- The persons within this third party who have access to the personal data are obliged to treat the personal data confidentially. Where necessary this is also contractually agreed on.
- This third party is obliged to comply with the applicable regulations in the area of protection of personal information, for example because we have concluded an agreement with this party or because our General Conditions apply. This means for example that this person has to take suitable technical and organisational security measures, and that any communication of personal data to countries outside the European Economic Area is adequately legitimized.

5. How do we secure your personal data?

5.1 Security measures

We deem the security of your privacy and personal data very important. EY has thus implemented suitable technical and organisational measures to protect and secure personal data, to prevent violations of the confidentiality, integrity and availability of the data. This also applies to the processing of personal data within the framework of our camera surveillance. All EY employees and other persons engaged by EY for processing the personal data are obliged to respect the confidentiality of the personal data.

5.2 Policy

EY has an internal policy and procedures that describe how we guarantee a suitable level of technical and organisational protection, including in the area of camera surveillance. Furthermore, a data breach procedure is applicable within EY, which carefully explains how to deal with (possible) data breaches. For example, we will inform the authorised supervisor and parties involved when this is required under the applicable law.
More information on how we protect your personal data can be found in the General Privacy Statement (see this link) and in the brochure "Protecting your data", see this link.

6. To which countries will we transfer your personal data?

It may happen that camera images are transferred to countries outside the European Economic Area (EEA) (including that the images are accessible from there). In that case, the transfer will be appropriately legitimized, as specified in the General Privacy Statement EY Netherlands, available via this link. This applies to transfer to countries outside the EEA for both within and outside the EY network.

7. How do we determine how long we will keep your personal data?

7.1 Main principle

In principle we do not keep your personal data for longer than what is necessary for the purpose that we process the personal data. In general terms, we have laid down our data retention rules in the EY retention policy. In this context, a general retention period of 72 hours applies within EY for camera images. There could however be exceptions to this general retention term.

7.2 Exception: shorter retention terms

If you exercise certain privacy rights it is possible that EY will remove your personal data earlier than usual based on the retention policy. For more information about this, go to the "What are your privacy rights?" paragraph below

7.3 Exception: longer retention terms

In certain situations, we will process your personal data for longer than the general rule based on the retention policy. This is the case, for example, when we have to process your personal data for longer:

- **Legitimate reason.** If EY can properly argue the legitimacy of the purpose and the need to keep the camera images longer, the argumentation is included per camera in Annex 1 of the Protocol Camera Surveillance.
- **Retention obligation.** To comply with a minimum retention term or other legal obligations resting on us based on EU law or the law of an EU member state;
- **Procedure.** Your personal data is necessary in the framework of a legal procedure; or
- **Freedom of expression.** When further processing of your personal data is necessary in order to exercise the right to freedom of expression and information.

8. What are your privacy rights?

8.1 A description of your privacy rights

In the context of the camera surveillance that we apply, the privacy rights detailed below are particularly relevant. For more information about other privacy rights to the extent they also apply, see our General Privacy Statement, available via this link.

8.1.1 Right of access

You have the right to obtain insight into the way in which we process your personal data. In the first place, you are entitled to a copy of the personal data, although in principle not to a copy of the documents where this personal data is included. In the context of camera surveillance, this means that, in principle, you are entitled to a copy of the camera images, but not to related documents such as copies of internal correspondence about an incident on which the camera images are seen. In addition, we may make other people unrecognisable when providing the camera images. Incidentally, it may also be the case that we have already deleted the camera images at the time of processing your request within the applicable retention period. In that case, we will inform you and cannot provide you with a copy.

In the second place you are entitled to detailed information about the way in which we process your personal data. For example, the purposes for which we process your personal data, where we got this from, and with whom we share it.

8.1.2 Right to erasure

Under certain circumstances you have the right to ask us to delete personal data we processed about you. You could have this right in the following cases, for instance:

- **Successful appeal.** You have successfully objected to the processing of these camera images and/or related personal data by EY (see below about the right of objection).
- **Data is no longer required.** EY no longer needs the camera images and/or related personal data for the purposes for which EY processes them.
- **Unlawful processing.** EY processes the camera images and/or related personal data unlawfully, for example because EY does not (or no longer) have a valid basis for this.
- **Compulsory erasure.** The camera images and/or related personal data must be deleted by EY in order to comply with a legal obligation.

8.1.3 Right to restriction of processing

The right to restrict the processing means that EY will continue to save information at your request but may in principle not do anything further with it. In short, you have this right when EY does not have (or no longer has) any legal grounds for the processing of your personal data or if this is open for discussion. This right is specifically applicable in the following situations:

- **Unlawful processing.** EY is not (or no longer) allowed to process certain camera images and/or related personal data about you, but you do not want EY to delete the data. For example, because you want to request the data later.
- **Personal data no longer required.** EY no longer needs the camera images and/or related personal data about you for the purpose for which EY processes them, but you still need the personal data for a legal claim. For example, in the context of a labour law dispute.
- **Pending an appeal.** You have submitted an objection EY's processing of the camera images and/or related personal data about you (see below about the right of objection). During the period we assess your appeal we will not further process this personal data at your request.

8.1.4 Right to object

You can object to EY's processing of camera images and/or related personal data about you. EY must respond to this objection in certain circumstances. EY will then no longer process these camera images and/or related personal data for the purpose to which you have objected. However, it is possible that EY continues to process the camera images and/or related personal data for another purpose, such as for the execution of an agreement with you or to meet a minimum retention period. In that case you will be informed about this.

8.1.5 Right to complain

You always have the right to submit a complaint with an authorised supervisory authority if you believe there has been a privacy infringement. It then specifically concerns the supervisory authorities in the field of privacy in the country within the European Economic Area:

- where you normally live;
- where you work; or
- where the alleged privacy infringement occurred.

The contact details of these supervisors can be found on this web page.

The right of complaint is applicable without prejudice to other options for administrative appeal or a legal provision. Furthermore, the supervising authority where the complaint was submitted must inform you about the progress and the result of your complaint, and about a possible legal provision.

8.2 The use of your privacy rights

You could also use your privacy rights to contact us via the contact details below. We request that you supply the following information with this:

- Your full first and last name.
- A description of your request. Do you want us to delete your personal data, or do you want us to keep the information, but also give you a copy? When describing your request, you may refer to the privacy rights we described above, but that is not compulsory. However, we do ask you to specify at which location and period of camera surveillance the request will be seen.

8.3 After you have submitted a request

After you have submitted a request with us where you indicate that you want to exercise a privacy right, you will first receive a confirmation of receipt from us. Next, we could ask you for additional information, for example to verify your identity. Another possibility is that we immediately respond to your request substantively. We indicate whether we will comply with your request, or when this is not possible, why not.

We respond to all privacy requests immediately and in principle always within one month after receipt. However, we could possibly need more time, for example in the view of the complexity and the number of requests we receive. In that case we will inform you that we need up to a maximum of two months extra time. We will inform you about this as soon as possible and at least within a month after receipt of your request and will then substantively respond within at least three months after receipt of your request.

9. Who is responsible for the processing of your personal data?

9.1 Responsible EY entity

This Privacy Statement informs you about the processing of your personal data in the context of camera surveillance at our locations in the Netherlands, for which the entities of the EY network of Ernst & Young Global Limited established in the Netherlands are (jointly) responsible. You can find a list of the entities it concerns via this link (no 380-392). The entity

(jointly/mainly) responsible for the processing of your personal data depends on the situation.

The following is normally applicable:

Party involved	(Main) EY entity responsible
Persons being filmed	The EY entity responsible for installing the camera.
Persons with request in relation to camera images.	EY entity responsible for camera installation, possibly together with other EY entity responsible for any related information (e.g. contact details of an EY employee visible on camera images)
Persons who have or will have access to camera images	EY entity responsible for installing the camera, and - if different - the EY entity which is the employer of the persons with access

When submitting questions or requests, you do not need to first find out which EY entity is responsible for the processing your personal data. If you submit your request via the contact form below, we will ensure that it is sent to the correct contact person.

10. How to contact us?

If you have questions or remarks about our processing of your personal data, you may contact our Data Protection Officer (DPO) via email at privacy.nl@nl.ey.com or by telephone via 088-4078895. The DPO is our "internal supervisor" in the field of data protection. See this web page of the Personal Data Authority for further explanation about the role and function of the DPO.

11. Changes

We may change this Privacy Statement from time to time. The latest version can always be consulted at https://www.ey.com/en_nl/privacy-statement-camera-surveillance. Important changes will always be communicated.