Camera surveillance protocol

Content

Intro

This protocol applies to the Roompot Groep (hereinafter also referred to as 'Roompot'). Roompot Recreatie Beheer B.V., having its registered office at Schuverweg 2 in 4462 HKGoes, is the data controller.

Aim of this protocol

The aim of this protocol is to lay down the manner in which Roompot records, collects, uses and stores camera images on cameras that Roompot has or will install in and and around the grounds and/or buildings owned by Roompot.

Aim of camera surveillance

Roompot uses camera surveillance for the following purposes:

- Access control of Roompot buildings and grounds.
- Surveillance of the property present of Roompot, its guests, its employees and other visitors, to protect against theft.
- Security of the grounds and buildings of Roompot, its guests and its employees to prevent unauthorised access and other undesirable activities (particularly at unmanned areas).
- To be able to register and identify unauthorised persons and persons who commit other undesirable activities.
- And everything directly related thereto.

Camera images will not be used in a manner that is incompatible with the purposes set out above, unless this is necessary in the interests of the prevention, investigation and prosecution of criminal offences.

The camera images may not be used to assess the performance of employees.

Controller

The Management Board of Roompot has appointed the Technical Services and Property Management manager as the Controller. The Controller monitors the correct use of the camera images.

Location of the cameras

Roompot takes the following into account when installing the cameras:

- The cameras will be placed at locations where they can seen by the data subjects and only at locations where camera surveillance has proved to be necessary.
- Roompot does not use hidden cameras.
- The cameras will not focus on public spaces, unless this is inevitable for the security of goods monitored and persons supervised by Roompot.
- Cameras will not be installed at locations which are private, such as toilets, changing rooms and homes, or at locations where primarily Roompot employees are present, such as offices and canteens.
- Only fixed cameras will be installed. No use will be made of camera surveillance by means of drones, for example.

Information provision

It is Roompot's policy to inform the data subjects in advance of the processing of personal data. Camera surveillance will be communicated by means of signs near the entrance to the grounds or the building where the cameras have been installed, the Camera Surveillance Protocol and the Privacy Statement.

All employees will be informed of the protocol prior its entry into force. In addition, the protocol will be published on the Roompot website.

Legal basis for camera surveillance

The necessity to protect the legitimate interest of Roompot, namely the protection of visitors, employees and property, constitutes the legal basis for camera surveillance.

It has been established that Roompot has no less invasive options other than camera surveillance to protect its grounds and/or buildings appropriately and that camera surveillance forms part of a total package of measures.

Access to and protection of the images

Roompot has put adequate measures in place to protect the camera images. Roompot will ensure that the camera images are protected in the appropriate manner against loss or any form of unlawful use. The camera images are protected with login codes so that only persons authorised thereto have access to the system in order to prevent the misuse or the unlawful inspection of recordings. Access control and logging can be used to verify who has had access to the camera images and when.

Camera images may only be inspected after an incident has occurred or if an incident is suspected. In this case, incidents are understood to mean: theft, burglary, vandalism, fraud, damage to property, sabotage, (other) crimes, serious violations (of the House Rules), and events endangering persons or otherwise injuring them.

Access to the camera images in the event of a suspected or actual incident is limited to the following persons:

- The Technical Services and Property Management manager.
- Employees of the security company responsible for ensuring safety at the parks – this company and its employees have a duty of confidentiality in respect of the camera images.
- The members of the Roompot Management Board.

In principle, no copies of camera images will be made. This may be derogated from if a copy is required to be provided to third parties pursuant to a statutory obligation or if necessitated by a failure or maintenance of the camera recording equipment. After use by the third party, the Controller must ensure that the copy made is destroyed immediately.

Provision to the police or judicial authorities

In the event of an alleged crime, Roompot may be authorised to provide the camera images to the police and/or judicial authorities. Whether it actually is necessary to provide the camera images will be assessed by the Controller and the Management Board in joint consultation.

Retention period of the images

After recording, the camera images will be retained for a maximum period of seven days, unless an incident has occurred and the camera images serve as evidence. A longer retention period may also be necessary if further investigation is required. The camera images will be retained for as long as necessary in connection with incidents that have occurred, or for as long as necessary for the further investigation.

Rights of data subjects

Data subjects are entitled to inspect the images on which they are identifiable and to submit a request to delete the data, provided that this does not violate the rights and liberties of others. A request to that end should be addressed to Roompot, PO Box 6, 4460 AA Goes, or digitally to the email address: privacy@roompot.nl. A request to inspect or to obtain a copy must contain a clear indication of the time period in which the data subject presumes he or she has been filmed. Roompot will respond to the data subject's request within four weeks.

Complaints

Any complaints regarding the manner in which Roompot handles personal data should be reported to Roompot (PO Box 6, 4460 AA Goes). In addition, complaints may also be submitted to the RECRON Disputes Committee or to the Dutch Data Protection Authority (Dutch DPA).

Amendments

Any amendments to this protocol can only be made with the prior consent of the Works Council.

Substantial changes in camera surveillance and/or expansion of camera surveillance which are incompatible with the purposes stated in this protocol must be notified in advance to the Works Council. The Works Council will assess together with the Management Board whether the changes and/or expansion affects the protection of personal data and/or the privacy of an individual. Should this prove to be the case, an application for consent is required.