

## Information provided to data subjects – CCTV system<sup>1</sup>

### Update 2024

Company **Barrandov Studio a. s.**, ID: 281 72 469, with its registered office at Prague 5 - Hlubočepy, Kříženeckého nám. 322/5, Postal Code 15200 (hereinafter referred to as the "**Controller**"), as a personal data controller within the meaning of Art. 4 paragraph 7 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Regulation on the protection of personal data (hereafter referred to as "**GDPR**"), in accordance with the Article 13 of the GDPR provides the concerned data subjects (also referred to as the "**DS**") with following information:

In accordance with current legislation, the Controller processes **image record** through the CCTV system, which is a personal data (hereinafter also referred to as "PD"). The image record is processed when the DS moves in the monitored area.

The monitored area is the entire premises of the Controller, i.e. the Barrandov premises at the address of the Controller's registered office and the Hostivař premises at the address of U Továren 261/27, 102 00 Praha 15 - Hostivař. The cameras are evenly distributed around the premises so that the video recording, taken only to the extent necessary, ensures the achievement of the purpose for which the camera system is installed on the premises of the Controller. Information on the exact number of cameras and their location is available from the Controller upon request. The cameras are static only and record continuously. The monitored area shall be properly and consistently marked with information signs (camera pictograms) so that the DS is informed of the possibility of capturing its video footage before entering the monitored area. The cameras are positioned in such a way as not to interfere with the privacy of the employees pursuant to the prov. § 316 par. 2) of the Labor Code.

If the DS does not want his/her image record to be captured in the CCTV system, he/she must not enter the monitored area.

The legal basis for the processing of the image recording **is the necessity for the protection of the legitimate interests of the Controller**, its contractual partner or another person on the Controller's premises.

The **purpose of processing** the image record is:

- **To increase the protection of the property** located on the Controller's premises (against theft, burglary, vandalism, etc.);;
- **To increase the security of persons** on the premises of the Controller (against assault, robbery, theft, other physical harm, etc.)
- **Prevention and early detection of security incidents;**
- **Obtaining evidence for the relevant public authorities or insurance companies.**

This purpose cannot be achieved to the extent necessary except through the camera system.

**Ensuring** the above purpose **only through physical security**, which is implemented on the basis of a contractual relationship that meets the requirements of the GDPR, **would not be sufficient to achieve the purpose**. For this reason, the Controller uses a combination of a camera system and physical security service to achieve the stated purpose, where the physical security service is not objectively capable of monitoring all parts of the Controller's premises that are captured by the camera system at one time and thus preventing damage to the Controller's property, threats to the safety of persons, emergencies/security incidents or providing evidence of an illegal act or a harmful event if it occurs on the Controller's premises.

In the case of an image record, it is not a processing of special categories of PD (sensitive data) within the meaning of Art. 9 paragraph 1 of the GDPR. Basically, it is the visual identification of a person in connection with a particular behavior. With help of the CCTV system, the Controller will be able to identify a record that would capture e.g. a criminal offense or other unlawful conduct, regardless of nationality, race, ethnic origin, religion or medical conditions of the person recorded on that record or regardless the biometric characteristics of that person. The processing of a special categories of PD would occur if the storage and/or comparing of some biometric

---

<sup>1</sup> Updated according to the Methodology of the Office for Personal Data Protection on the design and operation of camera systems in terms of processing and protection of personal data.

characteristics of the data subject (facial features/markers, biometric walking characteristics, facial recognition, etc.)<sup>2</sup> take place during the recording or processing of the image record, which does not occur through the Controller's camera system.

The PD are processed by the Controller and stored primarily in the image record **within a time loop for a period of 10 days**. This period of retention of the image record has been assessed by the Controller as the shortest possible to achieve the purpose, in particular because the potential damage to the Controller's or its contractual partner's property may not become known to the Controller immediately after it occurs<sup>3</sup>. The exception is a CCTV system which has the automatic parking pay machines in its viewing angle; i.e. PD are processed by the Controller and stored in the image record within a time loop for **a period of 30 days due to a contractual arrangement with a bank (contractual obligations of the Controller)** that processes payments through cashless payment terminals.

In addition to the actual storage of the video footage in a technically secured room, the actual image from the camera system is projected in two designated rooms within the Hlubočepy premises and in one room within the Hostivař premises. The rooms are properly secured technically and organizationally, and access to these rooms is granted to designated employees of the Controller and security personnel under the conditions defined in the contract with the Controller.

In the event that the image record does not capture such behavior so as to make it necessary for the purpose of the legitimate interest of the Controller, the DS, contractual partner or other third person or the public interest to have this record as evidence, the image record will be automatically deleted after the lapse of specified period of time in overwrite. In the event that the image record captures such behavior, the image record will be kept for the time necessary to protect the legitimate interest of the Controller, the DS, contractual partner or other third person, or the public interest.

**No automated decision making, including profiling, will take place** when processing the image record. The Controller does not transfer personal data to third countries or international organizations. The image record will be processed exclusively by the Controller's employees or by the person who process the personal data for the Controller on the grounds of the contract concluded with the Controller. On the part of the Controller, the camera records are properly and in accordance with the applicable legislation technically and organizationally secured against access by unauthorized persons. The image record may be provided **to other recipients only** if it will be necessary to use the CCTV record as an evidence to protect the legitimate interest of the Controller, DS, a contractual partner or other third person who demonstrates a legitimate interest in its provision, or the public interest. In such a case, it would be provided, for example, to the law enforcement authorities, a court, an insurance company or other public administration, or to another authorized entity under the conditions laid down by the legislation in force.

In connection with the PD protection under the GDPR, the DS has following rights:

#### **Right of access to PD**

According to Article 15 of the GDPR the DS has the right to obtain, upon request from the Controller, a confirmation of whether or not are PD processed. In case the PD are processed, the DS has the right to notification about: the purpose and extent of their processing, the possible recipients to whom the PD has been or will be made available, the period during which the PD will be stored by the Controller, the possibility of exercising the right to request correction from the Controller, erasure of his / her PD or restriction of their processing, the right to object to the processing of the PD and the right to lodge a complaint with the Office of Protection of the Personal Data. The DS has the right to receive all available information about the source from which the PD has been obtained and the information on whether the automatic decision-making, including profiling is made on the ground of PD processing.

In the case of the DS's image record processing, the exercising of this right will be possible only to a limited extent, as the individual image record is not usually associated with a particular DS.

---

<sup>2</sup> Operation of CCTV systems: Methodology for fulfilling the basic obligations imposed by the Personal Data Protection Act prepared by the Office for Personal Data Protection.

<sup>3</sup> Weekends, banking holidays, vacations, etc. on the part of the Controller's employees, contractors or physical security personnel.

### **Right to correct inaccurate PD**

According to article 16 of the GDPR the DS has the right to correct inaccurate personal data, as well as to complete the incomplete personal data, which concerns the DS. However, in the case of an image record, the exercising of this right is not objectively possible.

### **Right to erasure of PD**

According to article 17 of the GDPR the DS has the right to erase personal data if the PD are no longer needed for the purpose of fulfilling the lease agreement, if the DS objects to the processing of the PD due to a particular situation and there is no overriding justified reason for processing the PD. The DS has also the right to erasure of personal data if the PD are unlawfully processed or if PD has to be erased in order to fulfill the legal obligation that applies to the Controller.

With regard to the method of processing the image record and the length of time the image record is stored, the exercising of this right will be possible only to a limited extent.

### **Right to restrict the processing of PD**

According to article 18 of the GDPR the DS has the right to restrict the processing of the PD, i.e. in particular the right to transfer the data to another system and their non-accessibility to the public, and by the relevant data the right to indicate that they are subject to restrictions, provided that the DS denies the accuracy of the PD, for a period enabling the Controller to verify the accuracy of the personal data, the processing is unlawful and the DS opposes the erasure of the PD and requests the restriction of their use instead, the Controller no longer needs the PD for the purpose of the fulfillment of lease agreement, but the PD are required for the establishment, exercise or defense of legal claims or if DS has objected to processing due to particular situation and PD are processed for the purpose of their necessity for the legitimate interests of the Controller or third party, pending the verification whether the legitimate grounds of the Controller override those of the DS.

Where PD processing has been restricted in the above mentioned manner, the Controller is entitled to process PD, with the exception of storage, only with the DS's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the European Union or of a Member State.

With regard to the method of processing the image record and the length of time the image record is stored, the exercising of this right will be possible only to a limited extent.

### **Right to portability of PD**

According to article 20 of the GDPR the DS shall have the right to receive from the Controller his/her PD, , in a structured, commonly used and machine-readable format and to ask their transmission to another controller if the PD processing was carried out by automated means and this transmission was technically feasible.

This right does not apply to the processing of PD, but the DS may exercise the right of access to personal data in accordance with Article 15 of the GDPR against the Controller, where the DS may be provided with an image record of his or her person in a machine-readable format. **Right to object to the processing of PD**

According to article 21 of the GDPR the DS has the right to object to the processing of the PD on grounds relating to his or her particular situation, if the PD were processed for the purposes of the legitimate interests of the Controller or a third party. Submission of an objection will cause that the Controller shall no longer process the PD unless the Controller demonstrates that the Controller's interest (legitimate grounds for the processing) override the basic rights and freedoms of the DS.

With regard to the blanket monitoring of the premises with CCTV system, the exercising of this right will be possible only to a limited extent.

### **The right not to be subject to any decision based on automated processing, including profiling.**

According to article 22 of the GDPR the DS has the right not to be subject to a decision based on automated processing, including profiling. However, in the case of PD provided to the Controller, such decision-making will not occur.

**Right to lodge a complaint with a supervisory authority**

According to article 77 of the GDPR the DS has the right to lodge a complaint with the supervisory authority, i.e. with the Office of Protection of the Personal Data, if the DS considers that the GDPR has been violated in connection with the processing of his/her PD.

DS is entitled to exercise all the aforementioned rights by the Controller either by sending a letter to the address of its registered office to the attention of the statutory body or by e-mail to the address: [recepce@barrandov.cz](mailto:recepce@barrandov.cz).

The Controller is obliged to respond to the request of the DS in connection with aforementioned rights without undue delay after the request is received, however not later than 1 month after the receipt of the request.