Extended Video Surveillance Privacy Policy pursuant to art.13 GDPR

Pursuant to the current legislation on the protection of personal data (the "**Privacy Regulations**") including the EU Regulation 2016/679 (the "**GDPR**"), Italian Legislative Decree 196/2003 as amended by Italian Legislative Decree 101/2018, as well as the provisions of the Italian Data Protection Authority ("*Garante*") for data collected during video surveillance ("**Data Protection Authority**"), **Geico S.p.A.**, in its capacity as data controller (the "**Company**" or the "**Data Controller**"), informs those transiting within the range of the cameras and the employees of the Company (the "**Data Subjects**" or, in the singular, the "**Data Subject**") regarding the processing of their personal data, collected and processed through the video surveillance systems operating at the Company's premises. Processing will take place in strict compliance with the Privacy Regulations, for the purposes and in the manner described in this policy (the "**Privacy Policy**").

This Privacy Policy, pursuant to Article 13 of the GDPR, supplements the content of the simplified version of the Privacy Policy provided in the area covered by the cameras.

1. WHO IS THE DATA CONTROLLER?

The Data Controller is Geico S.p.A., with registered office at Via Pelizza da Volpedo 109/111, Cinisello Balsamo (MI), 20092, Italy, VAT No. 00688580968, which can be contacted via the phone number +39 02 660221 or at the following e-mail address infoprivacy@geico-spa.com.

2. WHAT TYPE OF PERSONAL DATA WILL BE COLLECTED?

The Data Controller processes the following personal data, collected through the video surveillance systems:

- images of the Data Subjects recorded by the video surveillance system.

3. FOR WHAT PURPOSES WILL PERSONAL DATA BE PROCESSED AND ON WHAT LEGAL BASIS WILL SUCH PROCESSING TAKE PLACE?

The Data Controller informs the Data Subjects that the personal data acquired by the Company through the video surveillance systems will be processed in compliance with what stated in art. 4 of Italian Act 300/1970 for the following purposes (the "**Purposes**"):

Purpose of the processing	Legal basis of data processing	Nature of personal data provision
a) Guarantee the safety of people who access company facilities for various reasons. b) Protect company assets against theft, robbery, damage and vandalism.	**Art. 6(1)(f) of the GDPR:** legitimate interest of the Data Controller to ensure the safety of the people who access the company's facilities for various reasons, and to protect the company's assets against theft, robbery, damage and vandalism. **NOTE** The images are displayed only when necessary (e.g. following unauthorised access, or theft, to identify the offender) and may, in this context, be transmitted to police and public authorities to prosecute offenders and ensure the protection, including judicial protection, of rights.	The provision of personal data is necessary as it is strictly instrumental to accessing the company premises of the Data Controller. Therefore, any refusal by the Data Subject to provide personal data, in whole or in part, will result in the impossibility to access the premises or the surrounding spaces and areas. In relation to the Provision of the Italian Data Protection Authority ("*Garante*") for the processing of personal data through video surveillance systems of 8 April 2010, the data subjects' consent is not required for the protection of corporate assets and the protection and safety of persons.

Considering that the legal basis of the aforementioned processing is the legitimate interest of the Data Controller, the latter guarantees to have previously carried out an assessment aimed at ensuring the **proportionality of the processing** so that the rights and freedoms of the Data Subjects are not prejudiced, taking into account the reasonable expectations of the same in relation to the specific processing activity.

Data Subjects may request **additional information about the above assessment** by sending an email to the following address: [infoprivacy@geico-spa.com].

The Data Controller also informs the Data Subject that s/he has the right to object to the processing of his/her Personal Data carried out on the basis of legitimate interest of the Company.

If the Company intends to use the personal data for any other purpose that is incompatible with the Purposes for which they were originally collected or authorised, the Company will inform the Data Subject in advance and, when required, will request consent for further processing of the data.

4. HOW WILL PERSONAL DATA BE PROCESSED?

Video surveillance activities shall be carried out in accordance with the **principles of fairness, lawfulness and transparency**, respecting the **privacy** and rights of the Data Subject, through automated means, according to a logic strictly related to the purposes and, however, in such a way as to ensure the security and confidentiality of data, in addition to compliance with the specific obligations under the regulations in force and applicable from time to time.

In relation to the aforementioned Purposes, the images taken by the cameras placed inside the Company premises are **viewed in real time, through dedicated monitors, by the personnel in charge, expressly authorised by the Data Controller, and are subject to recording and/or storage**.

Cameras are not pointed at any employee workstations, but only and exclusively at access areas to the Company premises, in corridors and common areas (particularly at lift landings) and along the perimeter of the building.

As far as **external cameras** are concerned, the processing of personal data is carried out in such a way as to **limit the viewing angle to the actual area to be monitored**, avoiding, as far as possible, the filming of surrounding places and details that are not relevant.

Without prejudice to the security profiles pursued through the installation of these systems, as far as technically feasible, **the orientation of the cameras is carried out in such a way as to ensure the minimisation of the data being processed**.

The **personal data thus acquired will not be subject to any automated decision-making process, including profiling**.

5. TO WHOM WILL PERSONAL DATA BE DISCLOSED?

The personal data of the Data Subjects will be processed by the Company's employees, who will be specifically designated as **authorised subjects**, where processing is required for the fulfilment of the Purposes set out in point 3 of this Privacy Policy.

The Data Controller has given them adequate operating instructions with particular reference to the security measures adopted, assigning them authentication credentials that allow them to perform, depending on the specific tasks assigned, only the operations for which they are responsible.

The Data Controller informs the Data Subjects that, for the fulfilment of the Purposes, their personal data may be disclosed to further recipients **or categories of recipients**, in their capacity as autonomous data controllers or, where necessary, as specially appointed data processors, including, by way of example but not limited to:

a) companies appointed by the Data Controller to carry out the maintenance of the video surveillance system;
b) public authorities and supervisory bodies, where necessary to fulfil legal obligations;
c) Judicial Authorities and Public Security Authorities.

The complete list of the recipients of the personal data of the Data Subjects, including further details on the location of the recipients, is kept at the Data Controller's head office and can be consulted upon request to be sent to the addresses indicated in point 8 of this Privacy Policy.

In particular, with reference to the companies referred to in point a) above, it should be noted that the specifically appointed personnel may view (when necessary and in any case not on a continuous basis) the images recorded by the video surveillance system both in real time or in playback, as well as delete or duplicate images, in order to assist the Data Controller in cases of requests and investigations by Judicial Authorities and Public Security Authorities.

Finally, the Data Controller informs the Data Subjects that their **personal data will not be disclosed to third parties and will not be disseminated**.

6. ARE PERSONAL DATA TRANSFERRED TO COUNTRIES OUTSIDE THE EU?

The personal data of the Data Subject will not be transferred to third countries outside the EU and will not be transferred to recipients other than those indicated in paragraph 5 of this Privacy Policy.

7. HOW LONG WILL PERSONAL DATA BE RETAINED?

The video surveillance system operates uninterrupted 24/7.

Taking into account the principles of minimisation of personal data and the principles of limitation of their retention, the recorded images are kept for a period of 72 hours following their recording, except in case of public holidays and office closing days.

The aforementioned images are kept for a longer period of time only when the Company has to comply with an explicit request of investigation by the Judicial Authority and the Judicial Police.

At the end of the retention period, the recorded images will be deleted automatically (by recording over them), thus making the deleted data non-reusable.

8. WHAT ARE YOUR RIGHTS IN RELATION TO THE PROCESSING OF YOUR PERSONAL DATA, HOW CAN YOU EXERCISE THEM AND HOW CAN YOU CONTACT US?

The Data Controller informs the Data Subject that s/he will always have, in accordance with the law, the right to revoke at any time his/her consent, where given, as well as to exercise, at any time, the following rights (collectively, the "**Rights**"):

a) the "**right of access**" and specifically to obtain confirmation of the existence or otherwise of personal data concerning him or her and their communication in intelligible form;
b) the "**right to rectification**", i.e. the right to request the rectification or, if interested, the integration of personal data;
c) the "**right to erasure**", i.e. the right to request the erasure, transformation into anonymous form of data processed in violation of the law, including data whose storage is not necessary in relation to the purposes for which the personal data were collected or subsequently processed;
d) the "**right to restriction of processing**", i.e. the right to obtain from the Data Controller the restriction of data processing in certain cases provided for under the Privacy Regulations;
e) the right to request from the Data Controller the list of the recipients to whom any rectification or erasure or restriction of processing was notified (in accordance with Articles 16, 17 and 18 GDPR, in fulfilment of the notification obligation except where this proves impossible or involves a disproportionate effort);
f) the "**right to data portability**", i.e. the right to receive (or to transmit directly to another data controller) personal data in a structured, commonly used and machine-readable format;
g) the "**right to object**" i.e. the right to object, in whole or in part:

- to the processing of personal data carried out by the Data Controller for its own legitimate interest;
- to the processing of personal data carried out by the Data Controller for marketing or profiling purposes.

In the above cases, where necessary, the Data Controller will inform the third parties to whom the Data Subject's personal data are communicated of the possible exercise of rights, except in specific cases where this is not possible or is too costly and, in any case, in accordance with the provisions of the Privacy Regulations.

The Data Subject may at any time exercise his/her Rights in the following ways:

- by email sent to: infoprivacy@geico-spa.com;

- by ordinary mail, to the address of the registered office of Geico S.p.A.: Cinisello Balsamo (MI), Via Pelizza da Volpedo 109/111, 20092, Italy.

9. HOW CAN YOU LODGE A COMPLAINT WITH THE ITALIAN AUTHORITY ("*GARANTE*")?

The Data Controller informs the Data Subject that, pursuant to the Privacy Regulations, he or she has the right to lodge a complaint with the competent supervisory Authority (in particular in the Member State of his or her usual residence, place of work or place of the alleged breach), if he or she deems that his or her Personal Data are being processed in a manner that would result in a breach of the GDPR.

In order to facilitate the exercise of the right to lodge a complaint, the name and contact details of the European Union Supervisory Authorities are available at the following link https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm.

Finally, if the Data Subject intends to lodge a complaint with the Supervisory Authority competent for the Italian territory (i.e. Italian Data Protection Authority ("*Garante*")), the complaint form is available at the following link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/4535524.