INFORMATION ON THE PROCESSING OF PERSONAL DATA ACQUIRED THROUGH VIDEO SURVEILLANCE SYSTEM pursuant to art. 13 and 14 of Regulation (EU) n. 2016/679

The following provisions for the processing of personal data are drawn up in compliance with current European and Italian legislation and, in particular, with the provisions of Regulation (EU) no. 2016/679 of April 27th, 2016, General Data Protection Regulation ("**Regulation**"), as well as, if and as applicable, Legislative Decree no. 196 of June 30th, 2003, and subsequent amendments, Code regarding the protection of personal data ("**Privacy Code**").

The user ("**User**") is strongly advised to consult this document frequently, in order to find out about the possible changes or amendments that could be made to it mainly as a result of regulatory changes.

1. Data controller

The provisions of this Privacy Policy ("**Video Surveillance Policy**") regulate the processing of personal data by **Digital Bros S.p.A. with registered office in Via Tortona, 37 20144 Milan (Italy)** as data controller ("**Data Controller**").

2. Data Protection Officer

The Data Controller has appointed a Data Protection Officer ("**DPO**"), Veronica Devetag Chalaupka, pursuant to Section 4 and art. 37 of the GDPR. The DPO can be contacted for all matters relating to the processing of data and the exercise of the rights of data subjects, at the following address dpo@digitalbros.com or by sending a written communication to Via Tortona n.37/3B – 20144, Milan.

3. Type of personal data and methods of collection

With reference to the processing of the data referred to in this Video Surveillance Policy, it should be noted that, pursuant to the Regulation and the Code, any information that allows the identification of the Data Subjects also through sounds and images is considered "personal data", and even if indirectly, through the link with other information. The law is also applicable to the processing of sounds and images carried out through video surveillance systems, regardless of the circumstance that such information, after its monitoring in a control circuit, is possibly recorded in an electronic archive or communicated to third parties.

The personal data being processed consist of images that are collected through the recording by the video surveillance systems installed at the Data Controller's premises.

4. Purpose and legal basis of the processing

The personal data collected will be processed for the purposes indicated below:

- to protect people, property and company assets against possible assaults, thefts, robberies or acts of vandalism;
- for the possible defense of the Company's rights in court.

The cameras are installed _____es outside the premises and film the access gates and areas considered at risk.

Furthermore, in compliance with art. 4 of the Workers' Statute, (Law 300/70), as last amended by Legislative Decree 151/2015 ("**Workers' Statute**"), as well as the provisions contained in Circular 5/2018 of INAIL, the equipment installed is not intended for remote control of work activity, i.e. it is not installed to verify the employees due diligence during working hours and their correctness in carrying out their work within the environments in which the systems are installed.

The processing of data for the aforementioned purposes is compliant with art. 6, letter (f) of the Regulation, according to which the processing is necessary for the pursuit of the legitimate interest of the Data Controller or of third parties, provided that the processing of the data collected does not prevail the interests or fundamental rights and freedoms of the User, in particular they are a minor.

Without prejudice to the foregoing and also regardless of the context in which the personal data are collected, the same will be processed by the Data Controller for the fulfillment of obligations established by laws, regulations and by EU and/or national legislation, as well as by provisions issued by authorities legitimized by the law or by supervisory and control bodies, also by way of prevention and detection of computer crimes.

5. Processing methods, mandatory or optional nature of providing data

In relation to the purposes indicated above, the data processing takes place using IT and telematic systems, through specifically identified natural or legal persons, pursuant to the Regulation and the Privacy Code, as "data processors" – i.e. the supervisory body that provides the video surveillance service - and as "in charge" of the processing. In any case, the data processing is carried out in compliance with the law, strictly related to the purposes in question and for the time strictly necessary to achieve them, as well as, in any case, to protect, as far as is reasonable and in the state of the art, the security and confidentiality of the same through suitable procedures that avoid the risk of loss, unauthorized access, illicit use and dissemination.

The provision of data is mandatory for the purposes of access or passage of the Data Subjects at the aforementioned entrances, premises and pertinent spaces, thus necessarily involving the shooting of images that may concern the User. Failure to provide data will make it impossible to access areas under video surveillance.

6. Subjects - data communication

For the pursuit of the purposes referred to in article 3 above, the User's personal data may be made known and/or communicated to other subjects, as data controllers, including in particular:

- individuals, natural and/or legal persons, appointed by the Data Controller to carry out technical repairs, ordinary and extraordinary maintenance, restoration and updating of IT systems;
- third-party companies appointed by the Data Controller to provide video surveillance services;
- public and/or private institutions, such as entities, competent authorities, control and supervisory bodies, when required by law.

Without prejudice to the foregoing, the Data Controller does not transfer or otherwise make available to third parties, unless expressly authorized by the User, any personal data collected through video surveillance systems, with the exception of its legal advisors or in the cases provided by the law or when required by a judicial or other competent authority decision.

The data are and will not be disseminated (meaning by this, the dissemination of personal data to indeterminate subjects, in any form, including by making them available or consulting them), except in those case where the dissemination is mandatory by law or regulation or is requested, in accordance with the law, by police forces, judicial authorities, information and security bodies or other public entities for purposes of defense or state security or prevention, detection or prosecution of crimes.

A list of appointed data processors is available for consultation at the headquarters of the Data Controller.

7. Security of personal data

In any case, the personal data provided by the User will be treated in full compliance with the provisions of the Regulation and the Privacy Code. Suitable and preventive security measures will be adopted to safeguard the confidentiality, integrity, completeness and availability of the User's personal data. Pursuant to the provisions of art. 32 of the Regulation, "Security of processing", Part I, Title V, "Security of data and systems", Privacy Code and the related technical specification, adequate technical and organizational measures are developed to guarantee a level of security appropriate to the risk, through technical, logical and organizational measures to prevent any damage, loss, even accidental, alterations, improper and unauthorized use of the personal data processed.

8. User rights

The User may request access to their data and have them integrated, updated or corrected and/or to exercise the other rights provided for by art. 15, 16, 17, 18, 19, 20 of the Regulation. Specifically:

Right of access	The User may request to obtain confirmation regarding the existence of a personal data processing and, if so, to access said data and specific information on the processing, such as, by way of example, the purposes, categories of data being processed, the existence of the other rights indicated below. User may also ask for a copy of your data.
Right to rectification	The User have the right to request and obtain rectification of personal data concerning them and/or the integration of incomplete personal data.
Right of cancellation	The User can obtain the cancellation of data, without unjustified delay, if (i) such data are no longer necessary for the purposes for which they were collected, (ii) the User opposes the processing of their data (as indicated below) and no other overriding legitimate reason for the processing subsist, (iii) the data are being processed unlawfully, (iv) the data must be canceled by virtue of a legal obligation, (v) the data belongs to a minor under 16 years of age.

Please note that this right does not apply if the data processing is necessary, *inter alia*:

- for the fulfillment of a legal obligation;
- for the assessment, exercise or defense of a right in court.

Right of limitation

The User has the right to obtain the limitation of the data processing in case of:

- dispute of the accuracy of personal data concerning them within the period necessary to verify the accuracy of these data;
- unlawful processing and request by the User to limit use instead of the relative cancellation;
- User necessity of the data for the assessment, exercise or defense of a right in court;
- opposition by the User to the processing, as indicated below, pending verification of the prevalence of legitimate reasons by the Data Controller.

Right to portability

The User has the right to receive the personal data concerning them in a structured, commonly used and automatically readable format and to transmit them to another data controller in relation to the cases in which the data processing is based on consent or concerns particular categories of personal data processed on the basis of consent, or the treatment is based on the execution of a contract and this treatment is carried out with automated means. The User also has the right to obtain direct transmission of data from one Data Controller to another, where technically feasible. The possibility of obtaining the deletion of data, as indicated above, remains unaffected.

Right to object

The User has the right to object at any time to the processing based on a legitimate interest of the Data Controller, subject to the demonstration by the latter of compelling legitimate reasons for proceeding with the processing which prevail over the interests, fundamental rights and freedoms of the User or for the assessment, exercise or defense of a right in court.

The rights referred to in art. 15, 16, 17, 18, 19, 20, 21 of the Regulation, as well as in art. 7 of the Privacy Code, can be exercised by the User at any time by writing to Digital Bros S.p.A. privacy@digitalbros.com or to the DPO at dpo@digitalbros.com.

The User can also lodge a complaint with the Data Protection Authority (www.garanteprivacy.it) should they n believes that their rights have been violated pursuant to the legislation on the protection of personal data.

9. Non-EU transfers

The personal data of the User are processed by the Data Controller within the territory of the European Union and are not disclosed.

If necessary, for technical or operational reasons, the Data Controller reserves the right to transfer the data of the User to countries outside the European Union. In this regard, the Data Controller ensures from now on that the transfer of data outside the EU will be regulated in compliance with the provisions of chapter V of the Regulation and authorized on the basis of specific decisions of the European Union. All the necessary precautions will therefore be taken in order to guarantee the total protection of personal data, basing this transfer: a) on adequacy decisions of the recipient third countries expressed by the European Commission; b) on adequate guarantees expressed by the recipient third party pursuant to art. 46 of the Regulation; c) on the adoption of binding corporate rules.

10. Conservation

The detected images are recorded and stored for the period of time strictly necessary to achieve the aforementioned purposes, normally consisting of 48 (forty-eight) hours, extendable, in the event of holidays or non-working days, until the resumption of activities and without prejudice to further conservation for any specific needs for the defense of rights in court and requests from the judicial or judicial police authorities in relation to investigative activities in progress. At the end of the retention period, the recorded images are deleted from the relevant electronic, computer or magnetic media.