

## **Information notice concerning the processing of the personal data through the video cameras located at the premises of Alu Menziken**

### **1. Preamble**

The protection of personal data is a priority for Alu Menziken SRL, therefore the processing of your personal data is carried out in accordance with the principles applicable throughout Europe, more specifically in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR), but also in accordance with the applicable national legislation in the field of data protection (Law 190/2018 implementing Regulation (EU) 2016/679).

Alu Menziken SRL provides all people entering the video surveillance area with the information required by the Regulation on video surveillance in an effectively and detailed form. For this, we follow a multi-layered approach consisting of a combination of the following two methods:

- a primary information, presented in a clear and permanent manner, represented of an appropriate sign (an icon), with sufficient visibility and located in the area under surveillance, to signal the existence of surveillance cameras, but also to communicate essential information regarding the processing of personal data.
- a detailed information, represented by this information note.

### **2. Purpose of video processing**

Alu Menziken SRL (hereinafter referred to as "AME") with registered office in Medieșu Aurit, no. 793, RO-447185, Satu Mare County, installs and uses the equipment and components of the video surveillance system only in accordance with the legal regulations in force, with the following main purposes:

- ensuring the safety of persons in the production area and monitoring the optimal operation of production equipment;
- preventing, preventing and , if required, investigating any unauthorized entering into secured areas or areas considered to pose a danger to an unauthorized person;
- ensuring the integrity of the goods and values that AME owns in its assets, as well as of the persons with whom AME comes into contact as employees, employees of subcontractors and partners, clients, potential clients, third party visitors;
- compliance with legal obligations in terms of occupational health and safety;
- ensuring the continuity of essential production services.

Alu Menziken SRL uses the video surveillance subsystem in addition to the detection, and fire alarm or equipment failure alarm subsystems, thus forming an integrated physical security system. All these subsystems ensure real-time surveillance and the possibility of post-event review in case of security or safety incidents.

### **3. Conditions of legitimacy**

The processing of personal data through the use of video surveillance means, the installation and technical use of equipment and components of the video surveillance system shall be carried out in accordance with the relevant legal provisions in the field:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

- Law No 190/2018 on measures implementing the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

- Methodological rules for the implementation of Law No 333/2003 on the security of objectives, goods, values and protection of persons, approved by Govern Decision no 301/2012, with subsequent amendments;

### **3. Areas under video surveillance**

Video surveillance is carried out within the office area, the AME production spaces as well as in places and spaces open or intended for the public, including access roads and parking areas on the company's premises, under the conditions laid down by law, as follows:

- Office building: the video cameras in the company premises are positioned to view the corridors and access routes into the company: front office area with clients, accounting, entrances to private offices (the aim of the surveillance is ensuring the integrity of the objectives, assets, values that AME holds in its assets, as well as of persons with whom AME comes into contact as employees, employees of subcontractors and partners, clients, potential clients, third party visitors);
- production area: the cameras are positioned so that they can view the access and work paths in the production departments (extrusion, cast house, maintenance, packing), but also on production equipment to monitor their optimal and continuous operation;
- outside the building: access routes into the company and the car parking are monitored to ensure the integrity and safety of the company's assets and the property of employees and visitors.

There is NO surveillance of areas with high privacy expectations (offices, toilets, changing rooms and other similar locations). Exceptionally, in case of well-justified security needs, cameras may be installed in offices where employees work, but only after an impact assessment and a legitimate interest analysis has been carried out and the Data Protection Officer has been consulted.

### **4. Protecting privacy and information security**

In order to protect the security of the video system and to enhance the protection of personal data, the following technical and organizational measures have been introduced:

- limiting the storage time of the footage in accordance with security requirements;
- storage media (digital video recorders) are located in secure premises protected by physical security measures;
  - the right of access shall be granted to users only for those resources which are strictly necessary for the performance of their duties;
  - the person who has the right to grant, modify or cancel users' access rights, in accordance with the procedure for access to databases, is the system administrator, designated for this purpose by the controller, with prior notification of the data protection officer;
  - the administrator/physical security system manager designated for this purpose shall keep an up-to-date list of all persons with access rights to the video-surveillance system at all times, specifying the type of access;
  - the Data Protection Officer will be consulted prior to the installation of any new video system.

At the same time, the prevention of unlawful processing of personal data or non-authorized access to such data is a permanent concern.

### **5. Access to personal data collected through the video surveillance system**

Access to live and recorded video footage is limited to a small number of people (IT manager - system administrator, HSE department manager, Company Administrator, Cast house

manager, Maintenance department manager) and is determined by the duties specified in the job description.

AME sets limits on who can copy, download, delete or modify any footage.

All staff with access rights to video recordings receive initial training in data protection. Training is provided to each new staff member and regular workshops on data protection issues are organized at least once every two years for all staff members with data access rights.

Any breach of security in relation to the video-surveillance subsystem shall be indicated in the **Security Incident Log** and the Data Protection Officer shall be informed thereof without undue delay within a maximum of 12 hours.

The video surveillance system is not used to verify attendance or evaluate job performance.

In exceptional cases, but subject to the safeguards described above, the Disciplinary Investigation Committee may be granted access in a disciplinary investigation, provided that the information assists in the investigation of a criminal offence or disciplinary offence likely to prejudice the rights and freedoms of a person.

## **6. Disclosure of personal data collected through the video surveillance system**

The information recorded by video surveillance systems is intended to be used by AME for the purpose of *monitoring people's access in the institution, ensuring the security of the institution's premises and property and the safety of people on the institution's premises* and shall be made available to judicial bodies and other institutions empowered by the law to request such information, upon their express request.

Any transfer and disclosure of personal data to third parties will be documented and subject to a rigorous assessment of the necessity of the disclosure and the compatibility between the purpose for which the disclosure is made and the purpose for which such data was originally collected for processing (security and access control). In these cases the Data Protection Officer designated at the level of the data controller will also be consulted.

## **7. Storage of information**

The duration of storage of data obtained through the video surveillance system is proportionate to the purpose for which the data is processed, so that images are stored for a period not exceeding 30 days (according to ANSPDCP Decision no 52/31.05.2012), except in situations expressly regulated by law or in duly justified cases.

When the storage period expires, the data is automatically deleted in the order in which it was recorded.

If a security incident happens and in duly justified cases, the retention period of the relevant footage may exceed normal limits depending on the time required for further investigation of the security incident. The record-keeping is rigorously documented and the need for retention is reviewed periodically (every two months).

## **8. Data subject's rights**

AME ensures that the rights of data subjects are respected in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

All persons involved in the video surveillance activity and those responsible for the management of the filmed images will respect the procedure for access to personal data.

Information to data subjects shall be provided clearly and permanently by means of an appropriate sign with sufficient visibility and located in the area under surveillance so as to signal the existence of the surveillance cameras and to communicate essential information on the processing of personal data.

Under the provisions of Regulation 679/2016 the data subject has the following rights:

- *access right* - is the right to receive confirmation from AME that your personal data are being processed, as well as access to a range of information such as, but not limited to, the categories of personal data concerned, the purpose of the processing, the period for which the personal data are expected to be stored or the criteria used to determine the period.

- *right to rectification* - is the right to request the correction, without undue delay, of inaccuracies or data which are no longer up to date, and the right to obtain the completion of incomplete personal data.

- *the right to have data erased* - you have the right to ask us to delete personal data we hold about you in certain circumstances. This right is also known as the "right to be forgotten" and usually only applies under certain conditions, such as if the personal data are no longer needed for the purpose for which they were originally collected.

- *the right to restrict processing* applies only if (i) the data subject disputes the accuracy of the personal data, (ii) the processing is unlawful and the data subject objects to the erasure of the personal data by requesting instead the restriction of the processing, (iii) we no longer need your personal data, but the data subject requests them for the establishment, exercising or defending a legal right in court, (iv) the data subject has objected to the processing for the period of time during which it is verified whether the legitimate interests of the company in the processing of personal data outweigh the rights of the data subject;

- *the right to data portability* - the data subject shall have the right to receive personal data relating to him or her which he or she has provided to the controller in a structured, commonly used, and machine-readable format and shall have the right to transmit such data to another controller without hindrance from the controller to whom the personal data were provided;

- *the right to object*. The right to object allows you to object at any time, on compelling legitimate grounds relating to your particular situation, to the processing of your personal data, except where there are compelling legitimate grounds for the processing which override your interests, rights, and freedoms or where the purpose is to establish, exercise or defend a legal right.

- *the right not to be subject to a decision based solely on automated processing, including profiling* - is your right not to be subject to a decision or measure taken solely based on automated processing that produces legal effects concerning your person.

In order to exercise the above-mentioned rights, the data subject must send a written, dated and signed request to: Alu Menziken SRL, nr. 793, Medieșu Aurit, Satu Mare or by e-mail: [office.ro@alu-menziken.com](mailto:office.ro@alu-menziken.com), or contact the Data Protection Officer on 0741 119 963 or at the same e-mail address.

Also, according to the General Data Protection Regulation, the data subject has the right to lodge a complaint (Article 77) with the National Supervisory Authority for Personal Data Processing at its headquarters in General Gheorghe Magheru Boulevard, no. 28-30, District 1, Bucharest, postal code 0103336, e-mail: [anspdcp@dataprotection.ro](mailto:anspdcp@dataprotection.ro) or to apply to the courts (Article 79).