APPROVED
closed joint-stock company „Hi-steel“
General Manager
Dainius Volskis
2022-02-04
No. 22-003-V

COMPANY „HI STEEL“
RULES FOR PROCESSING VIDEO DATA

CHAPTER I
GENERAL PROVISIONS

1. The purpose of the Video Data Processing Rules (hereinafter referred to as the "Rules") is to regulate video surveillance in order to ensure compliance with and implementation of 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 (the "General Data Protection Regulation" (GDPR), as amended by the Council of the European Parliament and of the Council of 27 April 2016, (OJ L 119, p. 1) (hereinafter referred to as the "EU Regulation (EU Regulation (2016/679) 2016/679"), the Law on the Legal Protection of Personal Data of the Republic of Lithuania, and the implementation of the other laws and legislation on processing and protecting personal data.

2. The terms used in the Rules are consistent with the terms used in the ADTAA. The provisions of the Rules shall not broaden or narrow the scope of application of the GDPR and shall not conflict with the requirements for the processing of personal data set out in the GDPR and other legal acts regulating the processing of personal data.

3. Data Controller - UAB "Hi steel", registered number 110604391, address Jonavos Str. 68A, Kaunas, Lithuania (hereinafter referred to as the Company).

4. The Data Controller engages a data processor to process the image data - UAB "APSAUGOS KOMANDA", Inc. 122668722, address Verkių Str. 29, Vilnius.

CHAPTER II
PURPOSE AND SCOPE OF VIDEO SURVEILLANCE

5. The purpose of video surveillance is to ensure the security of the Company's assets, the safety of the Company's employees and other persons who visit the Company and their property.

6. Video surveillance is carried out:

6.1. on the territory of Jonavos Str. 68A, Kaunas - entrance, driveway, main gate, courtyard, end of courtyard, car park;

6.2. premises located at 68A Jonavos St., Kaunas - warehouses, tool room, main production room, repair room, intermediate warehouse, warehouse for finished products, a warehouse for the production of finished products, a metal warehouse, a metal warehousing room (on two sides), a security office, a room for the main entrance of a security guard station, and a room for assembling.

7. Cameras shall be installed in such a way that the video surveillance does not extend beyond the territory or premises of the controller as specified in point 6 of the Rules.

8. It is forbidden to install and operate cameras in such a way that the field of view of the cameras extends into a dwelling and/or its private area or entrance, except as provided by law.

9. The installation and operation of cameras in such a way that the surveillance field of the cameras extends into the residence and/or its private area or entrance is prohibited, except as provided by law. Video surveillance shall be prohibited in premises where the data subject has a reasonable expectation of absolute privacy and where such surveillance would be degrading to human dignity (e.g. toilets etc.).

10. The company's indoor and outdoor areas are under continuous video surveillance.

CHAPTER III

RIGHTS, DUTIES AND FUNCTIONS OF THE CONTROLLER AND PROCESSOR

11. The data controller has the following rights:

11.1. drafting and adopting internal legislation governing video surveillance;

11.2. dealing with the provision of image data;

11.3. designate a person or unit responsible for the protection of image data;

11.4. authorise data processors to process image data;

12. The data controller has the following obligations:

12.1. to ensure compliance with the requirements for the processing of personal data set out in Regulation (EU) 2016/679, the Law on Legal Protection of Personal Data of the Republic of Lithuania, these Rules and other legal acts regulating the processing of personal data

12.2. to exercise the rights of the data subject in accordance with Regulation (EU) 2016/679, and in accordance with these Rules;

12.3. ensure the security of personal data by implementing appropriate organisational and technical measures for the security of personal data;

12.4. select only a processor that implements appropriate organisational and technical measures for the security of personal data and ensures that the processing complies with the requirements of Regulation (EU) 2016/679 and the protection of the data subject's rights, and enter into a contract with the processor governing the processing of the data by the processor, which complies with the requirements laid down in Article 28(3) of Regulation (EU) 2016/679. Give instructions to the processor regarding the processing of image data;

13. The Data Controller shall perform the following functions:

13.1. determine the purpose and scope of the video surveillance;

13.2. organise the installation of the video surveillance system;

13.3. establish procedures for granting, modifying and deleting access rights and powers to process image data;

13.4. analyse the technological, methodological and organisational challenges in the management of video data and take the necessary decisions to ensure the proper implementation of video surveillance;

13.5. provide methodological assistance to staff and data processors on the processing of image data;

13.6. perform other functions necessary for the exercise of the controller's rights and obligations referred to in paragraphs 10-11 of these Rules.

14. The Data Processor shall have the rights and obligations and perform the functions set out in the personal data contract between the Company and the Data Processor.

15. The person(s) authorised by the Company to carry out video surveillance (as well as the person(s) authorised by the Data Processor) shall be made aware of and shall comply with these Terms and Conditions by signature.

16. The person(s) authorised by the Company to carry out video surveillance (including a person authorised by the Data Processor) must:

16.1. Comply with the basic principles of image data processing and the confidentiality and security requirements set out in the Law on Legal Protection of Personal Data of the Republic of Lithuania, these Rules and other legal acts.

16.2. Ensure that cameras do not penetrate residences, entrances to residences, private areas belonging to residences, private areas belonging to residences, and areas where individuals have a reasonable expectation of absolute protection of privacy.

16.3. Take measures to prevent accidental or unlawful destruction, alteration, disclosure or any other unauthorised processing of video data, and to protect the data contained in video data recorders.

16.4. Ensuring that the CCTV system is in good working order and that technical malfunctions are dealt with promptly, using all available technical resources.

16.5. Not to disclose, transmit, or allow by any means the accidental or unlawful destruction, alteration, disclosure, or any other unauthorised processing of the video data, or the storage of the data contained in the video data recorders;

16.6. Immediately notify your line manager of any threat to data security.

CHAPTER IV
PROVISION OF IMAGE DATA AND DATA RECIPIENTS

17. Image data is provided to third parties in accordance with the procedures laid down by law, as well as at the request of the data recipients under at least one of the conditions for the lawful processing of personal data set out in Article 6 of Regulation (EU) 2016/679. The request must specify the purpose of the use of the image data, the legal basis for the provision and receipt of the image data and the scope of the image data requested.

18. Image data may be provided by the controller to a pre-trial investigation body, a public prosecutor or a court in connection with administrative, civil or criminal proceedings at their disposal, as evidence or in other cases established by law.

CHAPTER V
TECHNICAL AND ORGANISATIONAL MEASURES FOR THE SECURITY OF PERSONAL DATA

19. The following organisational and technical measures shall be implemented to ensure the security of image data: access to personal data shall be protected, managed and controlled; access to personal data shall be limited to the person who needs the personal data to perform his/her functions; personal data shall only be accessed in accordance with the rights granted to the user; and access shall be protected by means of passwords: granted, changed and stored confidentially; unique, consisting of at least 8 characters, without the use of information of a personal nature; personal data shall also be protected against unauthorised access to the internal computer network by means of electronic communications; the security of the premises where personal data are stored shall be ensured (restricting unauthorised persons from accessing the premises concerned, etc.); the security of the premises where personal data are stored shall be ensured.); protection of computer equipment against malicious software (installation and updating of anti-virus programs, etc.).

20.Procedures for granting, deleting and modifying access rights and authorisation to process image data:

20.1. access rights and authority to process image data shall be granted, deleted and modified by order of the Head of the Company;

20.2. access to the image data is requested by the controller's line manager;

20.3. the Head of the Company shall be responsible for the execution of the order to grant or delete access to image data;

20.4. access rights to image data shall be terminated upon termination of the employment relationship between the controller and the controller's employee, in the event of a change in the job functions for which access to the image data is not required, or in the event of the termination of the contract for the processing of personal data concluded with the processor, or in the event of expiry of the said contract.

21. No copying of image data.

21.1. 24-hour video data recording.

22.Video data is recorded and stored for 14 calendar days, after which it is destroyed. Where video data are used as evidence in civil, administrative or criminal proceedings or in other cases provided for by law, the video data may be retained for as long as necessary for those processing purposes and shall be destroyed as soon as they are no longer required.

CHAPTER VI
PROCEDURES FOR MANAGING AND RESPONDING TO VIDEO DATA BREACHES

23. Employees of the controller or processor who have access rights to the image data shall inform the Head of the Company if they notice any breaches of security of the image data (acts or omissions likely to cause or resulting in a threat to the security of the personal data).

24. After assessing the risk factors for an image data breach, the degree of impact of the breach, the damage and the consequences, the Head shall decide on a case-by-case basis on the measures necessary to remedy the image data breach and its consequences.

CHAPTER VII
PROCEDURES FOR EXERCISING THE RIGHTS OF THE DATA SUBJECT

25. The data subject has the following rights:

25.1. to receive information about the processing of data;

25.2. access to data;

25.3. to object to the processing of data;

25.4. to request deletion of the data ("right to be forgotten") if the image data is stored for longer than the retention period set out in these Rules;

26. Duomenų subjekto teisė žinoti apie savo asmens duomenų tvarkymą įgyvendinama šia tvarka:

26.1. persons who are not employees of the controller and whose image data are processed in the context of video surveillance are informed about the video surveillance

26.1.1. by displaying information boards and/or affixing stickers before entering the premises or area under video surveillance;

26.1.2. indicating on information boards/stickers that video surveillance is being carried out, the name and code number of the legal entity of the controller, contact information (address, e-mail address and/or telephone number), other additional information (e.g. purpose of the video surveillance); a model form of the information board/sticker shall be as set out in Annex 1 to these Rules;

26.2. the fact that video surveillance is being carried out shall be indicated in all cases, irrespective of the fact that video surveillance is not being carried out at the time at some designated locations (e.g. a CCTV camera is not working all the time, is working at a fixed periodicity, etc.).

26.3. the employees of data controllers shall be informed of the video surveillance by means of the information provided for in Article 13(1) and (2) of Regulation (EU) 2016/679, by means of a signed statement or any other form of proof of information, as well as by means of a briefing on these Rules, prior to the commencement of the video surveillance, or on the employee's first day of work, or on the first day after the employee's holiday, period of incapacity to work etc., in the case of a period of sickness, if the video surveillance is initiated in this period.

26.3.1. providing the following information under signature:

26.3.1.1. video surveillance is carried out and video data is processed by UAB Hi steel, registered number. 110604391, Jonavos Str.. 68A, Kaunas.

26.3.1.2. video surveillance is carried out for the following purposes: to ensure the security of the Company's assets, the safety of the Company's employees and their property.

26.3.1.3. video data is provided to UAB "APSAUGOS KOMANDA", which carries out security in the territory and premises of Jonavos Str. 68A, Kaunas.

27. The data subject's right of access to his or her image data shall be exercised as follows:

27.1. the data subject shall have the right to obtain, on production of a document proving his or her identity to the controller or processor, or on verification of his or her identity by means of a procedure established by law or by means of electronic communication which permits the person to be properly identified, information on the sources and the nature of his or her personal data concerning the collection of the personal data concerned, the purposes for which they are being processed, and the recipients to which

they are being provided and to whom they are being provided, and for which they have been provided for at least the last 1 year.

If the data subject sends the request by post or courier, a notarised copy of the data subject's identity document must be attached to the request. Where a representative of the data subject requests information on the data subject, he/she must provide a document certifying the representation and his/her identity document.

In the event that the data subject's right of access to his or her image data cannot be exercised through the data subject's representative without the provision of the data subject's identity document or a certified copy thereof, the data subject's representative shall be informed of this fact at the latest within 30 calendar days from the date of the request. If the data subject's representative's request is made in writing, the controller shall provide him/her with a written reply.

27.2. upon receipt of an enquiry from the data subject concerning the processing of his or her personal data and after verification of the identity of the data subject, the data subject shall be provided with information as to whether or not the personal data concerning him or her are being processed and shall be provided with the data requested by the data subject (by providing an opportunity to view the video recording on the controller's premises, or, at the request of the data subject, by making available a copy of the video recording on an external medium or a photograph);

27.3. the exercise of the data subject's right of access to his or her image data shall ensure the right to privacy of third parties, i.e. in the case of access by the data subject to a video, if the video shows other identifiable persons or other information which may violate the privacy of third parties (e.g., for example, the licence plate number of a vehicle), the images must be retouched or otherwise de-identified;

28. The right of the data subject to object to the processing of image data shall be exercised as follows

28.1. The right to have your personal data erased or to suspend, with the exception of storage, the processing of your personal data where processing is not carried out in accordance with the provisions of this and other laws shall be exercised in the following manner:

28.2. if the data subject establishes, after having access to his or her personal data, that his or her personal data are being processed unlawfully and fraudulently and contacts the controller, the controller shall without delay, and at the latest within 5 working days, verify the lawfulness and fairness of the processing of the data subject's personal data, free of charge, and shall without undue delay destroy the illegally and fraudulently stored personal data or suspend the processing of such personal data, except for the purposes of storage;

28.3. the controller who, at the request of the data subject or his/her authorised representative, has suspended the processing of the data subject's personal data, shall keep the personal data for which processing has been suspended until their destruction (at the request of the data subject or after the expiry of the data retention period). Further processing operations on such personal data may only be carried out:

28.3.1. for the purpose of demonstrating the circumstances which led to the suspension of processing operations;

28.3.2. if the data subject, directly or through an authorised representative, gives consent to the further processing of his or her personal data;

28.3.3. where it is necessary to protect the rights or legitimate interests of third parties.

28.4. the controller shall notify the data subject or his or her authorised representative without delay and at the latest within 5 working days of the destruction or suspension of the processing of personal data relating to the data subject at his or her request;

28.5. the erasure or suspension of the processing of personal data relating to the data subject on the basis of documents supporting the identity of the data subject and his or her personal data, at the request of the data subject or his or her authorised representative;

28.6. the controller shall inform the recipients of the data without delay, and at the latest within 5 working days, of the destruction of the data subject's personal data at the request of the data subject or of the data subject's authorised representative, or the suspension of the processing of the personal data, unless it would be impracticable or unreasonably burdensome to provide the information in question (for example due to a high number of data subjects, the length of the period of time covered by the data, or the undue expense).

CHAPTER VIII
FINAL PROVISIONS

29. Staff who are authorised to process image data or who become aware of it in the course of their duties shall comply with these Rules, the basic requirements for the processing of personal data, and the confidentiality and security requirements set out in these Rules. Staff members who infringe these Rules shall be liable to the procedure laid down by law.

30. Once approved, the Rules shall be communicated to staff members by signature. When a new staff member is recruited, he/she shall be familiarised with the Regulations on his/her first day of work. The person responsible for familiarisation with the Rules shall be a member of staff designated by order of the Company's Manager Executive Officer.

31. The Rules shall be reviewed at least once every 2 years and updated as necessary or in the event of changes in the legislation governing the processing of image data.

(Sample form for an information board (sticker))

(symbol for a CCTV camera)
VIDEO SURVEILLANCE OF THE GROUNDS AND PREMISES

(symbol for a CCTV camera)

UAB „HI STEEL“,
registered number 110604391

Jonavos Str. 68A, Kaunas,
tel. 8 683 11607