KRASSKY PRIVACY POLICY

The purpose of this Privacy Policy shall be to provide the natural person – the customer of Krassky SIA (hereinafter – Company) – with information on the purpose, scope, protection, duration of processing and the rights of the data subject at the time of obtaining the data, as well as when processing the personal data of the customer.

CONTROLLER AND ITS CONTACT DETAILS

The data controller responsible for the processing of your data shall be Krassky SIA, reg. No. 40003774722. The company shall be responsible for the secure storage, processing and erasure of your data. If you have any questions about the processing of your personal data, please contact the Company by sending an e-mail to krassky@krassky.lv or by calling 67781400.

SCOPE OF APPLICATION

Personal data shall mean any information concerning an identified or identifiable natural person. Categories and examples of personal data are set out below:

Data Category	Examples
Customer and Business Partner Data	Name, surname, place of work and position, personal identity number, bank account number, address, telephone number, mobile phone number, e-mail, Facebook profile, date of the name day, date of birth, and preferred language of communication.
Details of the job candidate (natural person applying for a job vacancy at the Company)	Name, surname, telephone number, e-mail, LinkedIn profile address, CV received.

The Privacy Policy shall apply to ensure the privacy and protection of personal data of the data subjects listed below (hereinafter – Customers):

- Natural persons – customers and other users of the services of the Company (including potential, former and existing users), as well as third parties who, in connection with the provision of services to a natural person (customer, partner), receive or provide the Company with any information (including contact persons, payers, etc.);
- Visitors to the showrooms, offices, warehouse, and other premises of the Company, including those subject to video surveillance;
- Visitors to the websites maintained by the Company and callers to telephones registered in the name of the Company;
- Natural persons – candidates for the vacancies of the Company.

The Company cares about the privacy and protection of personal data of the Customers and respects the rights of the Customers to the lawful processing of personal data in accordance with the applicable legislation – Regulation 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 (hereinafter – Regulation) and other applicable legislation in the area of privacy and data processing.

The Privacy Policy shall apply to the processing of data regardless of the form and/or medium in which the Customer provides personal data (website, mobile app, self-service portal, paper or telephone) and in which Company systems or paper form it is processed.

With regard to specific types of data processing (e.g., cookie processing, etc.), environment, purposes, additional, specific rules may be established, of which the Customer shall be informed at the time of providing the relevant data to the Company.

PURPOSES OF PROCESSING OF PERSONAL DATA

Krassky shall process data for the following purposes:

- For the provision of services and the sale of goods:

    - For the identification of the customer;
    - For the drafting, conclusion and proof of conclusion of the contract;
    - For the supply of goods and services (performance of contractual obligations);
    - For the provision of services;
    - For the performance of guarantee obligations;
    - For the improvement of goods and services, and the development of new goods and services;
    - For the promotion, advertising and distribution of the service;
    - For customer service;
    - For the examination and processing of applications and objections;
    - For the retention of customers, building loyalty, measuring satisfaction;
    - For the administration of payments;
    - For the recovery and enforcement of debts;
    - For the maintenance and improvement of websites and mobile apps.
- For business planning and analytics:
    - For statistics and business analysis;
    - For planning and accounting;
    - For the measurement of effectiveness;
    - For the assurance of data quality;
    - For market and public opinion research;
    - For the preparation of reports;
    - For conducting customer surveys;
    - For risk management activities.
- For information, information systems and enterprise security.
- For the provision of information to state administration authorities and subjects of operational activity in the cases and to the extent prescribed by state and local government laws and regulations.
- For the assessment of the suitability of candidates for job vacancies.
- For other specific purposes, which are notified to the Customer at the time of providing the relevant data to the Company.

LEGAL BASIS FOR THE PROCESSING OF PERSONAL DATA

The Company shall process personal data of natural persons in accordance with the following legal basis:

- Consent of the Customer – the Customer, as the subject of the personal data, gives his or her own consent to the collection and processing of personal data for certain purposes. The consent of the Customer is his or her free will and independent decision, which may be given at any time, thereby authorising the Company to process the personal data for the specified purposes. The consent of the Customer shall be binding upon him or her if it is given orally (during a telephone conversation after identification of the Customer) or in writing (by filling in a form in the showroom of the Company, by sending an electronic request after identification of the Customer). The Customer shall have the right to withdraw his or her prior consent at any time through the designated channels of communication with the Company. The withdrawal of consent shall not affect the lawfulness of the processing based on the consent prior to withdrawal.
- Consent of the job candidate – a candidate for a vacant position in the Company, as a personal data subject, gives his or her consent to the collection and processing of personal data to enable the Company to assess the suitability of the candidate for the vacant position as accurately as possible. The consent of the job candidate is his or her free will and independent decision, which may be given at any time, thereby authorising the Company to process the personal data for the specified purposes. The consent of the Customer shall be binding upon him or her if it is given orally (during a telephone conversation after identification of the candidate) or in writing (by filling in a form in the showroom of the Company, by sending an electronic request). The job candidate shall have the right to withdraw his or her prior consent at any time through the designated channels of communication with the Company. The withdrawal of consent shall not affect the lawfulness of the processing based on the consent prior to withdrawal.
- Conclusion and performance of the contract – for the Company to conclude and perform the contract with the Customer, to provide quality services and to serve the Customer, the Company must collect and process certain personal data that is collected before or during the conclusion of the contract with the Company.
- Compliance with legal obligations – the Company shall be entitled to process personal data to comply with the requirements of laws and regulations, as well as to respond to lawful requests of the state and local government.
- Protection of vital interests – the Company shall be entitled to process personal data to protect the vital interests of the Customer or another natural person, e.g., where processing is necessary for humanitarian purposes, for monitoring natural and man-made disasters, in particular epidemics and their spread, or in humanitarian emergencies (acts of terrorism, technogenic disasters, etc.).
- Performance of legal authorisation or public interest – the Company shall be entitled to process data for the performance of a task carried out in the public interest or in the exercise of legal authorisations vested in the

Company. In such cases, the basis for the processing of personal data shall be included in the laws and regulations.

- Legitimate (lawful) interests of the Company or a third party – in accordance with the interests of the Company, which are based on the provision of quality services and timely support to the Customer, the Company shall have the right to process the personal data of a natural person to the extent objectively necessary and sufficient for the purposes set out in this Policy. The Company shall have the following legitimate interests:
    - To perform commercial activities;
    - To provide the services of the Company;
    - To verify the identity of the Customer before entering into a contract;
    - To ensure the performance of contractual obligations;
    - To avoid undue financial risks to their commercial activities (including credit risk assessment before and during the sale of goods and services);
    - To retain Customer applications and submissions regarding the purchase of goods and the provision of services, other applications and submissions, and notes thereon, including those made in writing or orally, by calling the telephone numbers of the Company and on the websites of the Company;
    - To record the negotiations with the Customer regarding the operation, maintenance and payment of services to control the quality of customer service;
    - To record negotiations with the Customer to organise the performance of the contractual obligations of the service;
    - To record negotiations with the Customer, during which a verbal contract is concluded, to prove that a contract has been concluded;
    - To analyse, develop and implement improvements to the operation of the websites, web pages and mobile apps of the Company;
    - To take actions to retain Customers;
    - To segment the customer database for more efficient service delivery;
    - To design and develop goods and services;
    - To advertise the goods and services of the Company;
    - To send other reports on the progress of the performance of the contract and events relevant to the performance of the contract, as well as to conduct surveys of Customers about the goods and services and their user experience;
    - To prevent fraud;
    - To provide corporate governance, financial and business accounting and analytics;
    - To ensure effective corporate governance processes;
    - To ensure efficiency in the provision of services and the sale and delivery of goods;
    - To ensure and improve the quality of services;
    - To administer payments;
    - To administer missed payments;
    - To select the best candidate to work for the Company;
    - To apply to public administration and law enforcement authorities and to the courts to protect your legal interests;
    - To inform the public about the activities of the Company.

PROCESSING OF PERSONAL DATA

The Company shall process the data of the Customer using modern technologies, taking into account the existing privacy risks and the organisational, financial and technical resources reasonably available to the Company.

To ensure the quality and prompt performance of its obligations under the contract with the Customer, the Company may authorise its business partners to perform certain activities, such as the delivery of goods or the provision of services, the sending of invoices and similar. If, in the performance of these tasks, the business partners process the personal data of the Customer held by Krassky, the respective business partners shall be deemed to be data processing operators (processors) of Krassky and the Company shall have the right to transfer the personal data of the Customer necessary for the performance of these activities to the business partners to the extent necessary for the performance of these activities.

The business partners of the Company (as data processors) shall ensure compliance with the requirements of the processing and protection of personal data in accordance with the requirements of the Company and the legislation and shall not use personal data for any other purpose than for the performance of the obligations under the contract/agreement entered into with the Customer on behalf of Krassky.

PROTECTION OF PERSONAL DATA

The Company shall protect the data of the Customer by using modern technological capabilities, taking into account the privacy risks and the organisational, financial and technical resources reasonably available to the Company, including the

following security measures:

- Encryption of data during transmission (SSL encryption);
- Data encryption on servers;
- Firewalls;
- Break-in protection and detection programmes;
- Other protection measures in accordance with the current technological solutions.

CATEGORIES OF RECIPIENTS OF PERSONAL DATA

The Company shall not disclose to third parties the personal data of the Customer or any information obtained during the provision of the services and the term of the contract, including information about the services received, except:

- If the data shall be provided to the relevant third party within the framework of a concluded contract to perform a function necessary for the performance of the contract or delegated by law (e.g., to a bank for payment purposes or to provide a service, such as the delivery of goods, of which the Customer shall be informed);
- Subject to the explicit and unambiguous consent of the Customer;
- To persons provided for in external laws and regulations, upon their reasoned request, in the manner and to the extent provided for in external laws and regulations;
- In cases provided for in external laws and regulations for the protection of the legitimate interests of Krassky, for example, by taking legal action against a person who has infringed the legitimate interests of the Company in court or before other public authorities.

DURATION OF STORAGE OF PERSONAL DATA

The Company shall store and process the personal data of the Customer for as long as at least one of the following criteria applies:

- Only for as long as the contract with the Customer is in force (including recordings of negotiations where an oral contract is concluded/a service request is made);
- The data are necessary for the purpose for which they were received;
- Until Krassky or the Customer is able to exercise its legitimate interests (e.g., to file objections or to bring or pursue legal action) in accordance with the procedures set out in the external laws and regulations;
- As long as one of the parties is legally obliged to keep the data (e.g., according to the laws and regulations of the Republic of Latvia, the company must keep invoices for 5 years, etc.);
- As long as the consent of the Customer to the processing of personal data is valid, unless there is another lawful basis for the processing;
- After the conditions referred to in this Paragraph cease to apply, the personal data of the Customer shall be erased. Audit trails shall be kept for at least one year from the date of their execution in accordance with the laws and regulations.

ACCESS TO PERSONAL DATA AND OTHER RIGHTS OF THE CUSTOMER

The Customer shall have the right, in accordance with the laws and regulations, to request Krassky to have access to his or her personal data, to request the Company to supplement, rectify or erase such data, or to restrict processing in respect of the Customer, or to object to processing (including processing based on the legitimate interests of the Company), as well as the right to data portability. These rights shall be exercised to the extent that the processing of the data does not result from obligations imposed on Krassky by applicable laws and regulations, and which are carried out in the public interest.

The Customer shall be entitled to submit a request for the exercise of its rights:

- In writing in person at the showroom of the Company at Duntes iela 3, Riga, upon the presentation of an identity document;
- By electronic mail, by sending the request to krassky@krassky.lv and signing it with a secure electronic signature.

Upon the receipt of a request of the Customer to exercise its rights, Krassky shall verify the identity of the Customer, evaluate the request and execute it in accordance with the laws and regulations.

The Company shall send the response to the Customer by registered mail to the contact address provided by the Customer or in accordance with the method of receipt indicated by the Customer.

Krassky shall ensure compliance with the data processing and data protection requirements in accordance with the laws and regulations and, in the event of an objection by the Customer, shall take reasonable steps to resolve the objection. However, if this shall fail, the Customer shall have the right to apply to the supervisory authority – Data State Inspectorate.

CONSENT OF THE CUSTOMER TO THE PROCESSING OF DATA AND RIGHT TO WITHDRAWAL

The Customer may give his or her consent to the processing of personal data, for which consent is the legal basis, on the websites of the Company (e.g., newsletter subscription forms), by telephone or in person at the showrooms of the Company.

The Customer shall have the right to withdraw the consent to data processing at any time in the same way as it was given, i.e., by calling, sending an e-mail or in person at the Krassky showrooms, in which case no further data processing based on the consent previously given for the specific purpose will be carried out.

Withdrawal of consent shall not affect the processing of data carried out at the time when the consent of the Customer was valid.

Withdrawal of consent cannot interrupt the processing of data carried out on the basis of other legal grounds.

COMMUNICATION WITH THE CUSTOMER

The Company shall communicate with the Customer using the contact details (telephone number, e-mail address, postal address) provided by the Customer.

The Company shall communicate with regard to the performance of service contractual obligations on the basis of the concluded contract (e.g., delivery of goods or services, information on invoices, changes in services, etc.).

COMMERCIAL COMMUNICATIONS

Communication regarding commercial communications about the services of the Company and/or third parties and other communications not directly related to the provision of the agreed services (e.g., customer surveys) shall be carried out by Krassky in accordance with external laws and regulations or with the consent of the Customer.

The Customer may give consent to receive commercial communications from the Company and/or its business partners on the websites of the Company (e.g., newsletter sign-up forms), by telephone or in person at the showrooms of the Company.

The consent given by the Customer to receive commercial communications shall be valid until revoked (including after termination of the service contract). The Customer may withdraw from receiving further commercial communications at any time in any of the following ways:

- By sending an e-mail to krassky@krassky.lv;
- By calling 67781400;
- In person at the showrooms of the Company;
- By using the automated withdrawal option provided in the commercial communication to stop receiving further communications by clicking on the unsubscribe link at the end of the commercial communication (e-mail).

The Company shall stop sending commercial communications as soon as the request of the Customer has been processed. The processing of the request shall depend on the technological possibilities, which may take up to seven days.

By expressing his or her opinion in the surveys and leaving his or her contact details (e-mail, telephone), the Customer shall agree that Krassky may contact him or her in connection with the evaluation provided by the Customer, using the contact details left by the Customer.

USE OF COOKIES ON KRASSKY WEBSITES

The websites of the Company shall use cookies. Cookies are small text files that are stored by a browser (e.g., Chrome, Mozilla Firefox, Safari, etc.) on the end device (computer, mobile phone, tablet) used (at the time the user visits a website) to identify the browser or the information or settings stored in the browser. Thus, with the help of cookies, the website gains the ability to store the individual settings of the user, and recognise him or her and react accordingly, with the aim of improving the experience of using the website. The user can disable or limit the use of cookies, but without cookies, it will not be possible to make full use of all the site's features.

Depending on the functions to be performed and the purpose of use, the Company shall use the following cookies:

- Mandatory cookies
  These cookies are necessary to allow the user to freely visit and translate the website and use the facilities offered by the website, including information on news and products. These cookies shall identify the device of the user, but shall not reveal the identity of the user, nor shall they collect or gather information. Without these cookies, the website will not be able to function fully, for example, to provide users with the necessary information. These cookies remain stored on the device used until the time when the browser is closed.
- Functional cookies
  With functional cookies, the website remembers the settings and preferences chosen by the user to enable the user to navigate the website more easily. These cookies are stored permanently on the device of the user.
- Analytical cookies
  Analytical cookies collect information about how the user uses the website, detecting the most frequently visited sections, including the content that the user selects when browsing the website. The information shall be used for

analytical purposes to find out what is of interest to users of the website and to improve the functionality of the website to make it more user-friendly. Analytical cookies only identify the device of the user and do not reveal the identity of the user. In some cases, some of the analytical cookies are managed by third-party data processors (operators), such as Google Analytics, on behalf of the website owner, in accordance with the instructions of the owner of the website and only for the purposes indicated.

- Target (advertising) cookies
  Target (advertising) cookies are used to collect information about the websites visited by the user and to offer the products of the Company or its business partners that are of direct interest to a specific user or to target offers that are relevant to the interest expressed by a specific user. Generally, these cookies are placed by third parties, such as Google Ads, with the permission of the website owner, for the purposes indicated. Target cookies are stored permanently on the device of the user.

Krassky shall use cookies for the following purposes:

- To improve the user experience on websites and webpages;
- To ensure the functionality of the website;
- To adapt the functionality of the website to the usage habits of the user – including language, search queries, and previously viewed content;
- To get statistics on the traffic of visitors to the site – number of visitors, time spent on the site, geography, device used, etc.;
- To promote content and offers created or distributed by the Company.

Cookie retention period

Unless otherwise stated, cookies shall be stored until the action for which they were collected is performed, after which they shall be erased.

Cookie information shall not be transferred for processing outside the European Union and EEA countries.

Confirmation and disabling of cookies

When visiting the websites and webpages of the Company, the user is presented with a window containing a message stating that cookies are used on the website. By closing this message window, the user shall confirm that he or she has read the information on cookies, the purposes of their use, the cases in which their information is passed on to a third party, and agrees to them. Accordingly, the legal basis for the use of cookies is the consent of the user. The security settings of each web browser allow the restriction and erasure of cookies. However, it should be noted that the use of mandatory and functional cookies cannot be refused, as without them, the full use of the website cannot be ensured.

Krassky websites may contain links to third-party websites, which have their own terms of use and personal data protection policies for which the Company is not responsible.

OTHER PROVISIONS

The Company shall have the right to update the Privacy Policy by making the current version available to the Customer on the website of the Company – www.krassky.lv.

KRASSKY VIDEO SURVEILLANCE SYSTEM SECURITY RULES

1. **Used Terms:**
   Controller – Krassky SIA, unified registration No. 540003774722, legal address Duntes iela 3, Riga, hereinafter – Company.
   Object – Krassky showroom on the 1st and 6th floors at 3 Duntes Street, Riga, and office premises on the 2nd and 4th floors at 3 Duntes Street, Riga.
   General Data Protection Regulation – 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).
   Video surveillance system – video recording by means of video surveillance cameras and viewing in an online system, resulting in images of person or other information relating to identifiable natural persons.
   Responsible Person – an employee authorised by Krassky SIA.

2. **General Provisions:**
   2.1. The Video Surveillance System Security Rules (hereinafter – Rules) of the Company determine the procedure for processing personal data – image and sound in the Video Surveillance System, and its general technical and organisational requirements in accordance with the requirements of laws and regulations governing the protection of data of natural persons.
   2.2. The Rules shall determine:
      2.2.1. The technical resources for the processing and security of personal data;
      2.2.2. The duration of storage of video surveillance recordings;
      2.2.3. In which cases and under what procedures access to the online video surveillance and to the archive of video surveillance camera recordings shall be permitted;
      2.2.4. The daily compliance with the security requirements of video surveillance;
      2.2.5. The person responsible for technical issues;
      2.2.6. The placement of warning signs on the conduct of video surveillance.
   2.3. The Company, when carrying out video surveillance:
      2.3.1. Shall be guided by a common understanding and protection requirements regarding video surveillance as a form of processing the data of natural persons;
      2.3.2. Shall avoid risks and possible breaches related to the processing of data of natural persons, which may have legally and/or materially adverse consequences for the Company.
   2.4. The Rules are based on the General Data Protection Regulation and other laws and regulations governing the protection of data of natural persons, as well as the recommendations and guidelines of the Data State Inspectorate for the processing of data in the field of video surveillance and the protection of personal data in the workplace.
   2.5. The Rules shall be binding on all users of the Video Surveillance System – the Board of the Company, the Responsible Person, employees who perform direct viewing and monitoring of the video surveillance image or other persons who have been granted appropriate access by the Company to work with the Video Surveillance System in certain cases, as well as they undertake to comply with the requirements specified in the instructions for use of the equipment software.
   2.6. Video surveillance equipment and cameras shall be installed in such a way as to ensure image and audio quality appropriate to the technical specification and the location or environment in which they are placed.
   2.7. If the video surveillance does not produce an image from which the data subject can be identified (low resolution image), the requirements of these Rules relating to the protection of data of natural persons shall not apply.
   2.8. Video surveillance cameras shall not be used to record conversations between people. The equipment must not have audio recording, or it must be switched off. The Responsible Person shall ensure that no audio recording is made when video surveillance is being carried out.

3. **Purpose of Video Surveillance:**
   3.1. The purpose of video surveillance shall be the prevention and detection of crime, the protection of life, health and property of persons, the interests of other members of the public, and the maintenance of public order.
   3.2. The Company, taking into account the fact that the Object shall be a public place attended by a wide range of

persons and that the Object shall host events with heightened security requirements, shall be satisfied that the benefits of video surveillance outweigh the risks to the privacy of the natural person and that it will achieve the objective set out in Paragraph 3.1 of the Rules in a manner that least intrudes on the right to privacy of the natural person.

3.3. When carrying out video surveillance, the regulation of video surveillance as a form of data processing, as laid down in external laws and regulations and in the Rules, shall be respected.

4. Technical Resources for the Processing and Security of Personal Data:

4.1. Personal data shall be collected by means of video surveillance cameras operating continuously.

4.2. For the processing of personal data at the Object, 26 (number) indoor cameras shall be used.

4.3. When using technical resources, the Company shall use them in accordance with the requirements set by the manufacturer, and their proper use shall ensure the security and operation of the Video Surveillance System.

4.4. The operation of the system shall be ensured by a video recording device with the storage of information on a hard disk for up to 15 (fifteen) days.

4.5. Live monitoring of the video surveillance shall be carried out by the administrators on weekdays from 7.00 to 21.00, and from 21.00 to 07.00, and on weekends in 24 h mode by connecting the video surveillance to the technical security alarm system. The recorded information shall only be accessible to the Responsible Person and a Board Member of the Company.

4.6. Access to technical resources shall only be granted to the Responsible Person. The Responsible Person shall, in the cases provided for by the laws and regulations, be entitled to show the recorded information to another person by filling in the information referred to in Paragraph 6.5 of these Rules, provided that prior authorisation is obtained from a Board Member of the Company, stating the reason for the disclosure of such data.

4.7. The Responsible Person shall, upon the receipt of a written request from law enforcement authorities for the release of a video recording, prepare a recording of the requested excerpt of the video recording and complete the information referred to in Paragraph 6.5 of these Rules.

4.8. The Company shall use the software in accordance with the requirements specified in the licence for the software.

4.9. On the premises where the processing of personal data is carried out (location of the server or computer):

4.9.1. The temperature shall be not less than +10 °C and not more than +30 °C;

4.9.2. The physical conditions for the data storage device shall be maintained by providing heating and ventilation in the room;

4.9.3. Portable fire extinguishers shall be installed;

4.9.4. Uninterruptible Power Supply (UPS) shall ensure the continuity of operation of the technical resources.

4.10. Backup of system records shall be optional. The decision on the need to provide backup copies shall be taken by the responsible person for the security of the information system.

4.11. The responsible person shall ensure that an information notice on video surveillance is posted at all entrances of the object (Annex 1).

5. Place and duration of storage of video surveillance recordings:

5.1. The information shall be considered to be of medium-high value.

5.2. On the basis of confidentiality, the information shall be considered as restricted information.

5.3. The video surveillance recordings shall be classified as restricted information to which only the Responsible Person may have access.

5.4. The duration of the storage of video surveillance recordings shall be up to 15 (fifteen) days. After the expiry of this period, the recordings shall be erased automatically in chronological order from the moment of recording.

5.5. Video recordings of video surveillance on the Object shall be stored on the on-site video recording equipment at the Object. In the case of maintenance or repair of the Video Surveillance System, the Responsible Person shall ensure that the archive of the video recording is transferred to an external storage medium.

6. Security Measures for Access to the Video Surveillance System:

6.1. The following requirements shall be observed to ensure the security of the data contained in the Video Surveillance System and the video recording equipment installed by the Company, and to record all instances of inspection and copying of data:

6.1.1. Video surveillance recordings shall be made electronically and shall be kept for a maximum period of 15 (fifteen) days from the time of recording. Recordings shall be deleted automatically in chronological order from the time of recording. Where illegal offences have been detected and the video recordings shall be necessary for their detection, the data shall be kept for as long as necessary;

6.1.2. The Company shall designate a Responsible Person for access to the Video Surveillance System and the personal data (recordings) contained therein;

6.1.3. Any manual erasure, copying or transmission to the data subject or law enforcement authorities of personal data (recordings) contained in a Video Surveillance System recording device shall only take

place upon the written request of a competent public authority. The erasure, copying or transfer of the recording to third parties shall only be carried out with the written authorisation of a Board Member of the Company, completing the information referred to in Paragraph 6.5 of these Rules.

6.2. Access to video recordings from video surveillance cameras shall be restricted and shall be divided into two types:
  6.2.1. online viewing mode;
  6.2.2. archive viewing mode.

6.3. Access to all Video Surveillance Systems installed by the Company in online viewing mode shall be restricted to the Administrators and the Responsible Person.

6.4. The archive viewing mode shall be accessible to the Responsible Person and a Board Member of the Company. Only the Responsible Person shall have the rights of an administrator of a Video Surveillance System

6.5. The following shall be recorded on the relevant record sheets where data transfer is required:

  6.5.1. Inspection of the data (recordings) on the video recorder (Annex 2);
  6.5.2. Copying of data (recordings) on the video recorder to other storage media (Annex 3);
  6.5.3. Transfer of data (recordings) contained in the video recording equipment, to the data subject, to third parties and to law enforcement authorities (Annex 2);
  6.5.4. Deletion of the video recording (Annex 4).

6.6. The video surveillance camera recordings held by the Company shall, in accordance with external laws and regulations, be subject to the right to request and receive them by the designated authorities for the performance of their legal and regulatory duties.

6.7. The data subject shall be entitled to request video surveillance recordings, but only those relating to the data subject. If another natural person is visible and identifiable in the video recording, the Company shall ensure that his or her data (image) is not disclosed, for example, by making the image indistinguishable. If the video recording is several hours long but the data subject is only visible for a few minutes, only part of the recording shall be provided to the data subject.

7. Exceptional Circumstances:

7.1. In the event of an exceptional circumstance, the operation of the Video Surveillance System shall be protected in accordance with the fire safety rules of the premises. Where possible, the technical resources storing personal data shall be removed to a secure location.

7.2. The Company shall provide sufficient documentation to allow for changes to the system or full system restoration in the event of a compromise.

7.3. In the event of an exceptional circumstance, similar technical resources shall be used to restore the operation of the Video Surveillance System.

8. Means of Securing Technical Resources Against Intentional Damage and Unauthorised Acquisition:

8.1. Security of the premises shall be provided by the Company. The premises shall have technical security with 24-hour access to a monitoring station, including fire alarm systems and alarm buttons and a physical security post (24 hours a day).

8.2. The technical resources of the system shall be maintained by locking the premises after working hours.

8.3. The premises where personal data are processed (server or computer on which the record is stored) shall be inaccessible to unauthorised persons.

8.4. The password for access to personal data (records) shall only be known to the Responsible Person.

8.5. The logical security of the processing of personal data shall be ensured by the content management system installed, which shall not allow personal data to be rectified or erased without authorised access. Access for editing data shall be restricted to the data subject.

9. Rights of the Data Subject to Receive Video Surveillance Data:

9.1. The data subject shall have the right to access information relating to video surveillance held by the Controller (including where it is technically accessible), but which cannot be rectified or supplemented; otherwise, it will be considered as falsification or distortion of information.

9.2. The Responsible Person shall ensure the reservation of a copy of the video material by extracting the video material from the local video archive:

  9.2.1. Upon the receipt of a request, the Company shall register it and hand it over to the Responsible Person for execution. The law enforcement authority shall acknowledge the receipt of the requested information by certifying it with the name, position of the person concerned, and date on the data carrier. The request with the said acknowledgement shall be kept in the nomenclature file of the Company;

  9.2.2. In the event of the receipt of a personal complaint, including an anonymous complaint, which the Responsible Person, in the context of the purposes of the video surveillance, has assessed as sufficient to process the request for data reservation (e.g., where the subject is not identified in person but an anonymous report is received that an employee is observed to have taken unlawful advantage);

9.2.3. If an event has occurred which automatically informs of the signs of a security incident, or if the Responsible Person has made a reservation request in accordance with the internal control requirements;

9.2.4. where a written request is received from the data subject containing information to identify the data requested and the data subject is identified in person in accordance with the requirements set out in Paragraph 9.5.

9.3 The Responsible Person shall provide the data subject with the still image(s) from the video without disclosing the still image data of other persons and the description of the video and/or the outline of the audio recording without disclosing the audio recording data of other persons. The data subject shall be provided with the still image that is most relevant to the justification for the request for the video surveillance data.

9.4. If the data subject has not been identified prior to the receipt of the reservation request, the video surveillance data shall only be provided to the data subject if the data subject has submitted a written request and the data subject has been identified in person.

9.5. To obtain the video surveillance data, the data subject shall visit the Responsible Person at the object or the Company at its legal address:

9.5.1. The data subject shall present an identity document to the Responsible Person or an employee of the Company, and submit a written application stating:

9.5.1.1. The grounds for requesting the video surveillance data;

9.5.1.2. The date, time and place (including the location of the video camera, if known) where the video footage was taken;

9.5.1.3. A description of the situation or event (in which the video surveillance data of the data subject was recorded);

9.5.1.4. A detailed description of the visual appearance of the data subject, which shall include information about the clothing and belongings that were on the data subject and the specific location where the data subject was located;

9.5.1.5. Other information relevant to the identification of the requested data;

9.5.1.6. The desired date of receipt of the video surveillance data;

9.5.1.7. If the video surveillance data cannot be provided immediately, submit one colour photograph showing the data subject in full height and from which the data subject can be visually identified according to the photograph in the identity document.

9.6. The data subject shall only be entitled to receive those video surveillance data in which the data subject concerned can be seen or heard and whose visual appearance matches the photograph and the description of the visual appearance provided. Video surveillance data shall not be released unless there is reasonable assurance that the request for the video surveillance data is justified and that the data subject is identifiable in the video material.

9.7. The data subject shall not be entitled to receive video surveillance data in which other data subjects can be seen or heard. Therefore, the data subject shall only be provided with information relating to the video surveillance in the prescribed form and shall not be provided with copies of the video footage in redacted form, in particular, because of the scope, context and purposes of the video surveillance carried out by the Responsible Person and the Company:

9.7.1. There may be other data subjects at the video surveillance site whose data shall not be disclosed (whether identified or not);

9.7.2. The edited footage may give a false impression of what really happened.

9.8. The data subject shall not be provided with information relating to video surveillance where the request of the data subject is clearly unfounded (including irrelevant to the purposes of the video surveillance or insufficient to justify the request for video surveillance data) or requires excessive effort, in particular, due to regular repetition.

9.9. Any written application by a data subject, including the exercise of their rights, shall be answered by the Company within one month, except for data subjects provided for in the laws and regulations, who shall be answered within a shorter period of time.

9.10. Where the exercise of the rights of the data subject is the receipt of information relating to video surveillance, the Responsible Person shall, as far as possible, take into account the period of time specified by the data subject for the receipt of the desired video surveillance data. If it is not possible to answer within one month or within any other time limit set out in the laws and regulations, the data subject shall be provided with an interim reply informing of the time limit for the provision of the information.

9.11. If the data subject considers that an infringement of the rights of the data subject has occurred in the video surveillance area and that the urgent provision of evidence is necessary, the data subject shall have the right to apply to a law enforcement authority. Accordingly, the Company shall prepare and provide information to such a data reservation request in this case.

9.12. The Company shall cooperate with law enforcement authorities with respect to any requests for information that threaten personal or public safety and the data exchange process, and to ensure the availability of the information required by law enforcement authorities.

10. Procedures for the Investigation of Security Incidents:

10.1. In the event that System equipment is damaged or unauthorised access to information is attempted, or information or a piece of equipment is lost, this shall constitute a security incident.

10.2. In the event of a personal data breach or a System Security Incident, or a breach of these Rules or the consequences thereof, the Responsible Person shall take the following actions:

10.2.1 Verify the manual and electronic audit trails and their integrity for access to the System and suspend the System until the risks and causes of the incident have been determined;

10.2.2. Request a written explanation from the person involved in the personal data breach or security incident;

10.2.3. Make an entry in the Breach Register (Annex 5) about the occurrence of a personal data breach or the possible existence of a security incident;

10.2.4. Establish the causes of a personal data breach or security incident and, if necessary, amend the rules to introduce additional protection requirements;

10.2.5. Make a decision on the impact of the risk on the rights of the data subject;

10.2.6. If a personal data breach or security incident may pose a risk to the rights and freedoms of the data subject, the Responsible Person shall notify the Company, which shall immediately notify the Data State Inspectorate and CERT.lv of the data breach, but no later than within 72 hours from the time the security incident became known;

10.2.7. If it is established that a personal data breach or security incident may result in a high risk to the rights and freedoms of the data subject, the Company shall immediately notify the data subject thereof;

10.2.8. Where necessary, the guilty employee shall be held liable.

10.3. If a criminal offence (theft of personal data) is suspected, the Company shall immediately notify law enforcement authorities.

10.4. In the event of a System Security Incident, the System shall be checked and, if necessary, other security measures shall be implemented.

10.5. The form for the notification of a security incident in relation to the protection of personal data to the State Data Inspectorate is available at: http://www.dvi.gov.lv/lv/personas-datu-apstrades-aizsardzibas-parkapuma-pazinojuma-iesniegsana/.

11. Final Provision:

The safety requirements set out in the Rules shall be reviewed once a year, as well as in the event of changes to laws and regulations.

VIDEO SURVEILLANCE

Purpose: prevention and detection of criminal offences, protection of the life, health and property of persons, as well as the interests of other members of the public, and ensuring public order at Duntes street 3, Riga.

Controller: Krassky SIA, unified registration No. 540003774722, legal address Duntes street 3, Riga.

More information about the rights of the data subject shall be available on the website of the Data Controller krassky.lv or may be obtained by writing to krassky@krassky.lv.

Annex 2
Video Surveillance System Security Rules

Registration Sheet No. 1 for Viewing/Transfer to Third Parties of Video Recordings (Personal Data). Made by the Video Surveillance System of the Immovable Property at Duntes street 3, Riga.

No.	Date and time	Third party, name, surname, position, who participated in the data inspection	Signature or forwarding address of the third party	Signature of the Responsible Person	Reason for inspection/transfer of record	Date and time of the period for which the record was viewed/transferred
1.						
2.						
3.						
4.						
5.						
6.						
7.						

Annex 3
Video Surveillance System Security Rules

Registration Sheet No. 2 for the Copying of Video Recordings (Personal Data) to Other. Media by the Video Surveillance System of the Immovable Property at Duntes street 3, Riga.

No.	Date and time	Name, surname, position of the person who participated in the data copying	Signature of the Responsible Person	Reason for copying the record	Date and time of the period for which the record was copied
1.					
2.					
3.					
4.					
5.					
6.					
7.					

Annex 4
Video Surveillance System Security Rules

Registration Sheet No. 3 for the Erasure of Video Recordings (Personal Data). Made by the Video Surveillance System of the Immovable Property at Duntes street 3, Riga

No.	Date and time	Name, surname, position of the person who participated in the data erasure	Signature of the Responsible Person	Reason for erasure of the record	Date and time of the period for which the record was erased
1.					
2.					
3.					
4.					
5.					
6.					
7.					

Breach (Incident) Register

No.	Controller	Processor involved	Incident (description)	Date	Impact	Governance	Significance of the incident