

## PRIVACY POLICY FOR KROGERUS' CAMERA SURVEILLANCE AND ACCESS CONTROL

### 1 GENERAL INFORMATION

In this privacy policy, we provide the information required by the General Data Protection Regulation 2016/679 of the European Union (the "**GDPR**") to persons visiting at Krogerus' premises.

In particular, we explain how we collect, retain and otherwise process personal data of our employees, customers and other persons visiting at Krogerus' premises when we conduct camera surveillance and access control.

### 2 CONTROLLER AND CONTACT DETAILS OF THE CONTROLLER

Krogerus Attorneys Ltd ("**Krogerus**" or "**we**") acts as the data controller in accordance with this privacy policy.

The contact person of the controller is Piia Järvinen.

Address: Fabianinkatu 9, 00130 Helsinki

E-mail: [piia.jarvinen@krogerus.com](mailto:piia.jarvinen@krogerus.com)

### 3 PURPOSES AND LEGAL BASIS FOR THE PROCESSING OF PERSONAL DATA

The main purpose of processing personal data is to ensure the legal protection and safety of Krogerus' employees, customers and other visitors at the premises, to protect the data and property of the employer, employees and customers, and to prevent and investigate crime. Personal data are also processed to investigate cases of misuse and false alarms as well as to identify and recognise persons on the premises. The data may also be used for installation and maintenance work. We can only process personal data on legal bases derived from data protection legislation.

Krogerus processes personal data on the basis of legitimate interest of the data controller. Krogerus has carefully considered the interests and rights of data subjects on the basis of legitimate interest and assessed the use of the legal basis by conducting a so-called balancing test. Processing of personal data through camera surveillance and access control is necessary to protect the safety, security and property of Krogerus' employees and customers.

The table below lists, by category, the purpose of the processing, the legal basis and the personal data processed.

Purpose of processing	Legal basis	Personal data
Ensuring the legal protection and safety of employees, customers and other visitors at the premises, investigating cases of misuse and false alarms, identifying persons entering the premises, and carrying out installation and maintenance work.	Legitimate interest of the controller	Camera footage of persons visiting Krogerus' premises and the monitored area, personal identification data generated from access control (person's name, RFID tag number, time stamp, reader location)

#### 4 SOURCES OF PERSONAL DATA

The personal data we process is mainly obtained from the data subjects themselves in connection with camera surveillance and access control. Camera surveillance is installed at Krogerus' premises. The purpose of the camera surveillance is to monitor and record of entrances to and at the area subject to the camera surveillance. Signs are displayed to inform about the camera surveillance in the area.

Personal data generated from camera surveillance is stored on a separate storage device located on Krogerus' premises.

In order to carry out access control, access control devices with RFID readers have been installed in Krogerus' premises, which collect and store personal data on data subjects. The data is collected when the data subject logs on to the controlled area and/or moves within the area. When receiving an RFID tag, the data subject signs a form that allows the RFID tag with a unique identification number to be connected with that person.

#### 5 RECIPIENTS OF PERSONAL DATA AND CATEGORIES OF RECIPIENTS

In principle, we process personal data in the internal operations of Krogerus. In addition, Krogerus discloses personal data to third parties who act as service providers and processors for Krogerus. Camera surveillance and access control is operated by Securitas Oy.

Service providers process personal data only to the extent necessary to provide the service in question or in connection with system maintenance and troubleshooting. Krogerus concludes a contract to process personal data with all of its subcontractors who process personal data on behalf of Krogerus. In addition, contracts concerning the use of personal data are also concluded with service providers other than those acting as processors. Further information on the processing of data by such service providers can best be found on their own websites. Each service provider processes personal data only to the extent necessary for the provision of the service.

We may also transfer or disclose personal data to other authorities if required by applicable laws or if necessary, for example, in connection with a suspected crime.

## **6 TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES**

Krogerus does not as a rule transfer data outside the European Union or the European Economic Area ("EU/EEA"). However, data may be transferred outside the EU/EEA in situations where our service providers or their parent companies are located in such third countries. Where data is transferred outside the EU/EEA, such transfers will be subject to the conditions set out in data protection legislation, such as the European Commission's Standard Contractual Clauses or other transfer mechanism designated in the GDPR.

## **7 DATA RETENTION PERIOD OR CRITERIA FOR DETERMINING THE RETENTION PERIOD**

The person's name and RFID access key identification number are retained in the access control system until the end of the person's employment or access rights. Other access control data is retained for 30 days. Camera surveillance recordings are retained for 30 days.

Camera surveillance and access control data may be retained for the time necessary for the preparation, presentation or defence of a legal claim.

## **8 SECURITY OF PROCESSING**

Krogerus implements and maintains the following technical and organisational measures to ensure the protection of personal data:

- designated personnel responsible for developing, implementing and maintaining data security;
- internal guidelines and regulations on data security and data protection;
- non-disclosure agreements and undertakings;
- regular audit and risk assessment processes;
- processes for managing updates;
- control of access rights and use;
- data encryption;
- organised and regular staff training;
- business continuity and recovery plans; and
- physical and perimeter security of production facilities and other areas containing confidential client information

The adequacy of the measures is scaled on the basis of a risk assessment, taking into account, among other things, the nature, scope, context and purposes of the processing, as well as the risks to the rights and freedoms of data subjects. The measures are regularly assessed and reviewed and updated, as necessary.

Krogerus is committed to comply with the guidelines of the Finnish Bar Association.

The data will not be used for profiling. The processing does not include automated decision-making.

**RIGHTS OF THE DATA SUBJECT**

As a data subject, you shall have the following rights:

<b>Rights of the data subject</b>	
<b>Right of access to your personal data</b>	<p>You have the right to know whether Krogerus is processing your personal data and what personal data Krogerus is processing. You can also request a copy of your personal data. You have the right to inspect the personal data concerning you. Krogerus cannot, however, in order to protect the confidentiality of its clients, agree to requests for data that could jeopardise the processing of confidential client data.</p> <p>If you make your request electronically and have not requested another form of delivery, the data will be provided in the commonly used electronic format.</p>
<b>Right to rectify your data</b>	<p>You have the right to request that inaccurate or incorrect personal data concerning you be corrected or completed. However, due to the nature of the legal profession, Krogerus cannot always correct data, especially in the case of large requests.</p>
<b>Right to have your data erased</b>	<p>You have the right to have your data deleted in certain cases. However, a request to delete personal data cannot be implemented if the personal data is stored, for example, to comply with a legal obligation.</p>
<b>Right to restrict the processing of your data</b>	<p>In certain cases, you have the right to request restriction of the processing of your data.</p>
<b>Right to object to the processing of your data</b>	<p>You have the right to object to the processing of your data in certain cases. Krogerus may refuse a request if the</p>

	processing is necessary for the legitimate interests of Krogerus or a third party.
<b>Right to transfer data from one system to another</b>	To the extent that we process your data on a contractual basis and the processing is carried out automatically, you have the right to receive the personal data concerning you that you have provided to us in a structured, commonly used and machine-readable format and the right to transfer that data to another controller.
<b>Right to lodge a complaint with a supervisory authority</b>	You have the right to lodge a complaint with the competent supervisory authority if you consider that data protection legislation has not been respected in the processing of your personal data. In Finland, the supervisory authority is the Data Protection Ombudsman.

All requests mentioned here should be sent to the contact person of Krogerus mentioned in section 2. You can make a free-form request. We may ask you specific questions if necessary to fulfil your request.

More detailed information on the exercise of data subjects' rights is available on the website of the Data Protection Ombudsman (<https://tietosuoja.fi/en/what-rights-do-data-subjects-have-in-different-situations>).