

PRIVACY POLICY FOR KROGERUS' CLIENT ENGAGEMENT WORK**1 GENERAL**

In this privacy policy we provide information required by the General Data Protection Regulation 2016/679 of the European Union ("**GDPR**") to data subjects, i.e. clients of the law firm and all individuals whose information may qualify as personal data processed in the course of client engagement work. In particular, we explain how we collect, retain and otherwise process personal data in connection with client engagement work.

Separate privacy policies have been prepared for participants in Krogerus' events and recipients of marketing communications, employees and job applicants, website and cookie practices, and access control and camera surveillance. These are available at <https://www.krogerus.com/privacy-notice> or upon request from the contact person named in section 2 below.

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 Oskar Palva.

Address: Fabianinkatu 9, 00130 Helsinki

E-mail: oskar.palva@krogerus.com

3 PURPOSES AND LEGAL BASES FOR THE PROCESSING OF PERSONAL DATA

The main purpose of processing personal data is the management of client engagements, i.e. the provision of legal services. We can only process personal data on legal bases derived from data protection legislation. The main legal bases for processing personal data are the legitimate interest of the data controller, a legal obligation and the performance of a contract. The processing activities and the applicable legal bases are described in more detail below.

Information provided in connection with the conclusion of an engagement agreement with an individual client is processed on the basis of the contractual relationship. In respect of corporate clients, the legal basis for processing in connection with the conclusion of an engagement agreement is Krogerus' legal obligation or legitimate interest.

Krogerus is subject to a number of statutory obligations applicable to legal practice in the context of client engagement work, and personal data must be processed in order to comply with these obligations. Such statutory obligations arise, among other things, from the Act on Attorneys (496/1958), the Act on Preventing Money Laundering and Terrorist Financing (444/2017; the "**Anti-Money Laundering Act**"), the Act on Criminal Procedure (689/1997), and the Code of Judicial Procedure (4/1734). Krogerus' activities are also governed by the Finnish Bar Association's guidelines on good professional conduct (the "**Conduct Rules**") and other instructions issued by the Finnish Bar Association.

Krogerus processes personal data on the basis of legitimate interest where personal data is processed for the purposes of managing client engagements, except where the rights and interests of the data subject override Krogerus' legitimate interest. Krogerus' legitimate interest is the conduct of its business, i.e. the provision of legal services to its clients. Since the significance of legal services is not limited to the benefits accruing to the law firm but extends to the clients who make use of those services, the interest is also that of a third party, namely the client. In practice, this means that the purpose of the processing is in particular to protect the client's interests and to safeguard the right of individuals and entities to obtain legal advice and assistance. Krogerus has assessed the applicability of this legal basis by means of a balancing test.

To the extent that Krogerus processes special categories of personal data in the course of managing client engagements, an exception under Article 9(2) of the GDPR applies where Krogerus processes such data for the establishment, exercise, or defence of legal claims.

The table below lists, by category, the purpose of the processing, the legal basis and the categories of personal data processed. For a more detailed description of the categories of personal data to be stored, see section 4.

Purpose of processing	Legal basis	Categories of personal data
Conclusion of an engagement agreement, management of client engagement work	Legitimate interest of the controller, contract (individual clients)	Identity data of clients and other information related to engagements.
Client due diligence and prevention of money laundering	Legal obligation	Information required to be retained under the Anti-Money Laundering Act, other information required for identification purposes, such as passport number, employer, family relationships, and political affiliations.
Conflict-of-interest checks	Legal obligation	Identity data of clients or other parties necessary for conflict-of-interest checks as required under the Conduct Rules, such as name, date of birth, contact details (address, email address, telephone number), and background information relevant to the engagement.

Purpose of processing	Legal basis	Categories of personal data
Management of client engagement work	Legitimate interest of the controller or a third party	Identity data of the counterparties of clients and other information necessary for the management of engagements.
Management of client engagement work	Legitimate interest of the controller or a third party, legal obligation In respect of special categories of personal data, the exception applies on the basis of the establishment, exercise, or defence of legal claims	Identity data and other information necessary for the management of engagements concerning current and former employees, business partners, suppliers, and other individuals connected with engagements involving clients and their counterparties which may depending on the engagement include health data or other data falling within special categories of personal data.
Management of client engagement work	Legitimate interest of the controller or a third party, legal obligation In respect of special categories of personal data, the exception applies on the basis of the establishment, exercise, or defence of legal claims	Identity data and other information necessary for the management of engagements concerning witnesses and experts in litigation, criminal proceedings, or other proceeding involving clients, which may depending on the engagement include health data or other data falling within special categories of data.
Management of client engagement work	Legitimate interest of the controller or a third party In respect of special categories of personal data, the exception applies on the basis of the establishment, exercise, or defence of legal claims	Identity data of parties to corporate transactions and individuals associated with them, such as employees, clients, business partners, and board members, information stored in data rooms, and other information necessary for the

Purpose of processing	Legal basis	Categories of personal data
		management of engagements, which may depending on the engagement include health data or other data falling within special categories of personal data.
Management of client engagement work	Legitimate interest of the controller or a third party	Identity data of employees of public authorities, courts, and other bodies, and of contact persons necessary for the resolution of legal claims, such as representatives of insurance companies.
Billing	Contract, legitimate interest of the controller, legal obligation	Billing information such as identity data defined in client agreements, name, email address, employer, and title.

4

CATEGORIES OF PERSONAL DATA

This table specifies in more detail the categories of personal data referred to in section 3 insofar as they are not otherwise unambiguously specified in the previous section.

Category of personal data	Content of the category
Identity data	The natural person's (data subject's) name, email address, telephone number, nationality, employer, position in a company, home address, and date of birth / personal identity code.
Client due diligence information	Information required to be retained under the Anti-Money Laundering Act, other information required for identification purposes, such as passport number, employer, family relationships, and political affiliations.

Information contained in communications and documents relating to the management of the engagement	Information necessary on a case-by-case basis for the management of the engagement, such as messages sent or received by clients and their counterparties' current and former employees, business partners, suppliers, and other individuals connected with engagements, and information appearing in documents and other materials such as signatures, employment-related information, contractual information, health data, financial information, ownership information, and any other personal data necessary for the management of the engagement.
Information stored in data rooms	The information may include a wide range of data relating to the parties to corporate transactions, such as identity data, salary data, employment-related information, lease agreement information, copies of identity documents, health data, and other data relating to the parties.

5 SOURCES OF PERSONAL DATA

Personal data is collected primarily directly from the data subject at the time of concluding the engagement agreement and during the course of the engagement. In the course of managing an engagement, the client or individuals connected with the engagement may provide personal data relating to other individuals connected with the engagement, in which case those data subjects may not be aware of the processing carried out for the purposes of managing the engagement.

Personal data may also be collected from third parties, such as public authorities or public or private registers, where this is necessary for the management of client engagement work.

6 RECIPIENTS OF PERSONAL DATA AND CATEGORIES OF RECIPIENTS

Krogerus may disclose personal data to third parties who act as service providers and processors for Krogerus, including providers of cloud services, office systems and tools, and artificial intelligence functionalities. Service providers may, for example, store, transfer or access data in accordance with Krogerus' instructions for the purpose of managing client engagements. 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.

Data may also be transferred or disclosed to third parties, such as other agents, advisers and other parties involved in an engagement.

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.

7 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 of 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 adequacy decision made by the European Commission, the European Commission's Standard Contractual Clauses or other transfer mechanism designated in the GDPR.

8 DATA RETENTION PERIOD OR CRITERIA FOR DETERMINING THE RETENTION PERIOD

Krogerus retains personal data for at least as long as is necessary for the proper management of client engagement work. In addition, Krogerus has statutory obligations to retain data after the conclusion of an engagement or the end of a client relationship.

Krogerus complies with the requirements and guidelines of the Finnish Bar Association, according to which materials relating to an engagement are as a rule retained for a minimum of 10 years from the conclusion of the engagement. Thereafter, data is retained to the extent necessary for resolving conflicts of interest and for the protection of the legal rights of the attorney, or where required by the nature of the engagement or the client relationship.

Krogerus is also required to retain data collected under the Anti-Money Laundering Act for a minimum of 5 years from the end of the client relationship, and materials required under the Accounting Act (1336/1997) for 10 years from the end of the financial year.

Upon expiry of the retention period, personal data will be securely destroyed or anonymised.

9 SECURITY OF THE 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. Krogerus also operates an ISO 27001-certified information security management system (ISMS).

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

10

RIGHTS OF THE DATA SUBJECT

As a data subject, you shall have the following rights, unless Krogerus' obligations under applicable law, such as attorney's professional secrecy obligations, provide otherwise.

Rights of the data subject	
Right of access to your data	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. Krogerus may charge a reasonable administrative fee based on administrative costs for additional copies requested. 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.
Right to rectify your data	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.
Right to have your data erased	You have the right to have your data deleted in certain cases where the processing is based on Krogerus' legitimate interest. In this context, this refers in particular to situations where your personal data is no longer needed for the purposes for which it was originally collected, or where personal data has been processed unlawfully. However, a request to delete personal data cannot be implemented if the personal data is stored, for example, to comply with a legal obligation or for the establishment, exercise, or defence of legal claims.
Right to restrict the processing of your data	In certain cases, you have the right to request restriction of the processing of your data where the processing is based on Krogerus' legitimate interest. You may request restriction of the processing of your data where you contest the accuracy of your personal data, where the processing has been unlawful and you request restriction rather than erasure, or where you require the data for the establishment, exercise, or defence of legal claims. Notwithstanding your request, we may process your data where you have given your consent to such processing, where it is necessary for the establishment, exercise, or defence of legal claims, for the protection of the rights of another natural or legal person, or for reasons of substantial public or EU interest.
Right to object to the processing of your data	In certain cases, you have the right to object to the processing of your data where the processing is based on Krogerus' legitimate interest, on grounds relating to your particular situation. If you object to the processing of your data, we must cease the processing unless there is com-

	elling legitimate ground for the processing which overrides the interests, rights, and freedoms of the data subject, or the processing is necessary for the establishment, exercise, or defence of legal claims.
Right to transfer data from one system to another	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.
Right to lodge a complaint with a supervisory authority	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 named in section 2. You can make a free-form request. We may ask you specific questions if necessary to fulfil your request.

More 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>.