

Privacy policy

04.04.2025

Introduction

Kravia is a debt collection company operating in Norway, Finland and Sweden. We are committed to protecting the privacy and personal data of individuals in accordance with the General Data Protection Regulation (GDPR) and other applicable data protection laws. This Privacy Policy outlines how we collect, use, disclose, and protect personal information in the course of our debt collection activities. The data controller for the processing of your personal data is the Kravia entity in your jurisdiction.

Collection of Personal Data

We may collect and process the following categories of personal data:

- **Contact Information:** Name, address, telephone number, email address, and other contact details.
- **Financial Information:** Debt details, payment history, and related financial information necessary for debt collection.
- **Identification Information:** National identification number, passport number, driver's license details, or other identification documents as required by law.



- **Employment Information:** Employment history, employer details, and income information.
- **Legal and Court Proceedings Information:** Information related to legal claims, court proceedings, and judgments.
- **Communication Information:** Correspondence, communications, and other information exchanged with individuals.

We collect personal data directly from individuals or from third parties, such as creditors, credit bureaus, public registers, or other lawful sources.

Use of Personal Data

We use personal data for the following purposes:

- **Invoicing and Debt Collection:** To send invoices and perform debt collection services, including contacting debtors, negotiating payment arrangements, and recovering outstanding debts.
- **Compliance with Legal Obligations:** To comply with our legal and regulatory obligations, including anti-money laundering, fraud prevention, and reporting requirements.
- **Communication and Support:** To communicate with individuals, respond to inquiries, and provide customer support.
- **Business Operations:** To manage and administer our business activities,

including record keeping, accounting, and internal analysis.

- **Legal Defense:** To exercise or defend our legal rights in the event of disputes, claims, or legal proceedings.

Legal Basis for Processing Personal Data

We process personal data on the following legal bases:

- **Performance of Contract:** Processing is necessary for the performance of a contract or agreement with the data subject, such as the debt collection agreement.
- **Legal Obligations:** Processing is necessary to comply with our legal obligations, such as those imposed by financial, bookkeeping, tax, and anti-money laundering laws.
- **Legitimate Interests:** Processing is necessary for our legitimate interests or the legitimate interests of third parties, such as debt recovery, fraud prevention, and business management. We carefully balance our interests against the rights and freedoms of the data subjects.
- **Consent:** Processing is based on the individual's explicit consent, which may be obtained in certain situations. If we process your personal data based on your consent, you may withdraw this at any time.

Disclosure of Personal Data

We may disclose personal data to the following recipients or categories of

recipients, as permitted by law:

- **Creditors and Business Partners:** To communicate debt-related information and collaborate with creditors and business partners involved in the debt collection process.
- **Service Providers:** To engage third-party service providers who assist us in providing debt collection services, such as IT service providers, legal advisors, and professional consultants.
- **Legal and Regulatory Authorities:** To comply with legal and regulatory requirements, we may disclose personal data to courts, law enforcement agencies, regulatory authorities, and government bodies.
- **Debtors' Representatives:** In certain circumstances, we may disclose personal data to debtors' legal representatives, agents, or advisors involved in debt negotiation or dispute resolution.
- **Successors and Acquirers:** In the event of a merger, acquisition, or transfer of assets, personal data may be disclosed to potential or actual successors, acquirers, or assignees.

Data Retention and Anonymization

We prioritize data privacy and take steps to handle your personal information responsibly. We retain your data for as long as necessary to perform our service and comply with legal authorities for auditing purposes. Once this period ends, we anonymize or delete the data to protect your privacy.

For invoicing and debt collection carried out by Kravia, the data will be kept for at least until the outstanding amounts have been settled with the addition of retention thereafter in accordance with mandatory bookkeeping and record keeping obligations. In most cases this will mean that the data is kept for up to five years after the year in which the final outstanding amounts are settled, unless a longer retention period is mandated by law or special circumstances.

Data Security Measures

Securing and maintaining the confidentiality of the data stored within our systems is a paramount concern at Kravia. We have implemented robust measures to protect your data, ensuring that only authorized personnel with job-related responsibilities can access and process it. The following security measures are in place:

- **Access Control:** Data stored in our system can only be accessed by individuals whose job duties require data management. User authorizations are assigned based on specific job descriptions, ensuring that access is limited to relevant data.
- **System Protection:** Kravias systems is safeguarded from external threats, with servers protected by firewalls. Communication within the system is conducted using encrypted connections, adding an extra layer of security.
- **Personal Authorization Control:** Data is protected through personal authorization controls, which are closely monitored. Staff members/users are

bound by non-disclosure agreements to maintain the confidentiality of the information they handle during their duties.

- **Training and Guidance:** We place great importance on training and guidance regarding confidentiality and data protection. Our staff receives continuous training to ensure they are up to date with best practices and regulatory requirements.
- **Physical Security:** Our company premises are secure, with restricted access. Manual materials are stored in locked cabinets, and obsoleted materials are securely stored in locked data security containers. The premises are equipped with an alarm system to further enhance security.
- **Data Backup and Storage:** Application data is backed up at least once daily, and database data and backups are stored in multiple physically separate locations. Backup copies are always encrypted and protected using various technical measures to prevent unauthorized access.

These security measures are in place to provide a high level of protection for your data. We are committed to maintaining the confidentiality and integrity of your information and continuously improving our security practices to meet evolving threats and industry standards.

User Rights

At Kravia, we respect your rights concerning your personal information. As an individual, you have the following rights:

- **Right to Access:** You can request to know what personal information we have stored about you in our systems.
- **Right to Correction:** If any of your personal information is inaccurate, incomplete, or outdated, you have the right to request corrections.
- **Right to Erasure:** You may ask us to erase your personal data, which request we will respect and comply with.
- **Right to Restriction:** If we are processing your personal information without a legal basis or if you believe we shouldn't use it for specific purposes, you can request restrictions on its processing.
- **Right to Object:** You are entitled to object to certain processing activities. You are furthermore, on grounds relating to your particular situation (for example, a specific need for protection of your identity), entitled to object to processing of personal data based on legitimate interests, which we will comply with, unless there exists compelling legitimate grounds for our processing which override your interest, or if our processing is necessary for the establishment, exercise or defence of legal claims.
- **Data Portability:** You may ask us to provide you or others with your personal data in a structured, commonly used and machine-readable format.

Please note that the above rights may be subject to further exceptions and limitations in accordance with the data protection legislation. To exercise these rights or for further information, please contact us as set out below in this Privacy Policy. Please note that we may request additional information from you if such information is necessary to confirm your identity.

International Data Transfers

We do not transfer personal data to foreign countries outside the European Economic Area, unless it is necessary for the purposes of providing our services, such as utilizing cloud services. We want to assure you that any data transfers made for these purposes will be conducted in full compliance with applicable data protection laws and regulations. Such measures include the use of Standard Contractual Clauses to safeguard the transfer of data outside of the EEA or reliance on adequacy decisions as adopted by the European Commission. Our commitment is to uphold the highest standards of security and confidentiality to safeguard your information.

Contact Information

If you have any questions about this Privacy Policy, including how we process personal data, or would like to submit a request to exercise your rights, please contact us at: compliance@kravia.ai.

You may also lodge a complaint with the relevant supervisory authority if you believe that Kravia's processing of your personal data is not in accordance with the applicable data protection laws. The contact details for all EEA Supervisory Authorities can be found [here](#).

Changes

We may update the Privacy Policy from time to time. The Privacy Policy will, for example, be updated to comply with any legislative amendments or if we make changes to our processing of personal data.

The most recently updated version of the
Privacy Policy will always be available at
[https://kravia.ai /legal/privacy-policy](https://kravia.ai/legal/privacy-policy)