Oma Savings Bank's privacy policy
Personal customers

1. General

OmaSp takes the compliance with the EU's General Data Protection Regulation and other legislation concerning the processing of personal data seriously. We ensure that the processing of personal data is secure and that our privacy policies enable the full realisation of the rights of data subjects.

With this privacy policy, we provide OmaSp's personal customers with the information required by the EU's General Data Protection Regulation and other applicable data protection legislation on how we process their personal data when providing banking services.

In addition to providing its own banking services, OmaSp offers fund and insurance products in the role of an agent, in which case the fund or insurance company in question acts as a controller and the processing of personal data is described in the company's own privacy policy.

OmaSp may make changes to this privacy policy. You can always find the up-to-date privacy policy on our website: omasp.fi. This privacy policy was last updated on 10 November 2026.

2. Data Controller

Oma Savings Bank Plc
Postal address: P.O. Box 77, 53101 Lappeenranta
Phone: +358 207 640 600
Visiting address: Valtakatu 32, 53100 Lappeenranta
Website: omasp.fi

("OmaSp" or "we")

3. Contact details of the Data Protection Officer

OmaSp's Data Protection Officer
Postal address: P.O. Box 77, 53101 Lappeenranta
Email: tietosuoja@omasp.fi

4. Who does this privacy policy apply to?

This privacy policy applies to the following data subjects:

- OmaSp's current personal customers;
- OmaSp's potential personal customers; and
- Private persons related to OmaSp's personal customers, such as guardians, holders of power of attorney and other authorised representatives, guarantors and pledgers, with whom OmaSp is in contact in connection with the customer relationship

("Data Subject" or "You")

5. What personal data do we process?

We process data belonging to the categories of personal data described below. The list of examples presented in the table is not exhaustive and the data collected may vary depending on the group of data subjects and the purpose for which they are used.

Category of personal data	Group data content	Examples
Basic	Basic identifying information about a person	Name, social security number and contact information, such as phone number, email address and postal address
Knowing Your Customer (KYC)	Information related to knowing a person as defined by legislation	Passport or identity card information, such as expiry date, issuer and number, nationality, politically exposed person (PEP information), tax information
Customer information	Information related to customer relationship management and monitoring	Start date of the customer relationship, nature of the customer relationship
Consents	Consents, withdrawals and prohibitions given by the data subject regarding the processing of personal data	Marketing consent, consent for electronic direct marketing
Contract and product information	**Information on agreements between the data controller and the data subject; Information about the products and services purchased by the data subject**	**Account agreement, promissory note, online banking agreement, insurance-based investment products**
Customer transaction information	Transaction information related to the data subject's banking transactions	Credit transfers, payment transactions, cash transactions
Background information	Background information provided by the customer or obtained from other sources	Life situation, financial status
Interests	Information about the interests of the data subject	Interest in a certain OmaSp product or service, such as interest in investing
Technical management and identification data and behavioural data	Technical identification data related to devices or systems; data collected about the data subject's behaviour in different channels with the help of cookies	IP address, device or application identifier, electronic service usage and browsing data
Recordings and message content	Recordings related to conversations and communication with the data subject and visits to our branches	Call and video recordings, chat conversations, web conferences and messages

6. For what purposes and on what legal basis do we process personal data?

OmaSp processes personal data for pre-defined purposes, ensuring that we have a legal basis for processing the data in accordance with the General Data Protection Regulation.

We process personal data of data subjects for the purpose of providing services and operations to our personal customers and to fulfil our legal and contractual obligations.

Purpose of processing	Legal basis	Categories of personal data
Customer verification and knowledge	Legal obligation under the Money Laundering Act	Basic information, knowledge, customer information, contract and product information
Customer relationship management and implementation of customer channels	Our legitimate interests in delivering customer service	Basic information, customer relationship information, contract and product information, customer transaction information, recordings and message content
Implementation of payment transactions and payment services	An account agreement with you and/or a card agreement	Basic information, contract and product information, customer transaction information
Sanctions monitoring of payment services and prevention of money laundering and terrorist financing	Statutory obligations under the Anti-Money Laundering Act, the Sanctions Act and the Act on the freezing of assets to combat terrorism	Basic information, knowledge, contract and product information, customer transaction information, technical management and identification information, and behavioral information
The granting of a loan and the execution of loan services	A loan, guarantee and/or pledge agreement with you and pre-contractual measures	Basic information, customer information, contract and product information, customer event information, background information
Recovery of claims and management of legal claims	Our legitimate interests in the establishment, exercise and defence of claims	Basic information, contract and product information, customer event information, background information
Mapping the investor profile related to saving and investing	Legal obligations under the Investment Services Act, an investment contract with you or a private bank agreement, your consent	Basic information, contract and product information, customer relationship information, background information, interests
Collecting customer feedback and analysing and developing services and functionalities	Our legitimate interests in developing our business	Basic information, customer relationship information, contract and product information, customer event information, interests, technical management and identification information and behavioral information, recordings and message content
Marketing of customer-related products and communication with our customers and their potential representatives	Our Legitimate Interests in Member Communications	Basic information, customer information, consents, contract and

		product information, customer event information, interests
Marketing communication and implementation of sweepstakes and competitions	Your consent	Basic information, customer information, consents, interests
Reporting to the authorities and responding to enquiries from the authorities	Statutory obligations imposed by the Act on the Financial Supervisory Authority, the Police Act, the Enforcement Code and the Tax Procedures Act	Basic information, identification information, customer relationship information, contract and product information, customer event information, background information, technical management and identification information and behavioral information, recordings and message content
Implementation of OmaSp's accounting	Legal obligation under the Accounting Act	Basic information, customer information, contract and product information, customer transaction information

In addition to the purposes described herein, the processing of personal data carried out by OmaSp is also described in our other privacy statements. In addition, we may process your personal data for purposes compatible with the original purpose of collection, to comply with legal requirements, or we may ask for your consent for a later purpose.

7. Profiling and automated decision-making

OmaSp may utilise the profiling of personal data, for example, to assess credit risk, prevent and detect money laundering and fraud, assess the likelihood of insolvency risk or the value of assets.

In automated decision-making, our systems make decisions based on information about you, without human intervention. This may include not only the information we already have, but also information obtained from public registers and other public sources, depending on the type of decision in question. When we make use of automated decision-making, this is necessary for the conclusion or performance of a contract, or the decision is based on the data subject's explicit consent or a provision of law.

We evaluate and monitor the methods used in automated decision-making on a regular basis to ensure their reliability.

You have the right to express your opinion on a decision based solely on automated processing, such as profiling, if that decision has legal effects concerning you or if the decision otherwise significantly affects you in a similar way. You also have the right to demand human participation in decision-making.

Automated decision-making in the context of payment monitoring

As a bank, we have legal obligations to prevent money laundering and terrorist financing. The purpose and grounds for the processing of personal data related to this is described above in the section describing the purposes of the processing and the applicable legal grounds. We make use of automated decision-making to fulfil these obligations, which means that, for example, the payment you make may be automatically rejected. If your payment is rejected, you will immediately be notified in the online banking view and instructed on the possibility of contacting our customer service.

Automated decision-making in the context of student loans

We utilize automated decision-making in the processing of student loan applications. In this case, automated decision-making supports the homogeneity of our credit decisions and strengthens our operations as a responsible lender.

In automated decision-making, we use the following information to describe the borrower's ability to pay:

- Information you provide in connection with your application
- Customer information that may already be on OmaSp (e.g. information describing payment behaviour)
- Suomen Asiakastieto Oy's credit information register and the Tax Administration's Information to be retrieved from the positive credit information register maintained by the Incomes Register Unit

In automated decision making, the application can be either approved or rejected automatically. Information leading to automatic rejection may include a lack of ability to pay or a failure to pay entry.

The system can also transfer the application directly to manual processing if the system does not have sufficient information at its disposal to make a decision. In this case, the application is processed and the decision is made by a natural person.

As a credit applicant, you have the opportunity to ask an OmaSp staff member to verify the accuracy of an automatically rejected credit decision. In this case, your loan application will be reprocessed by a natural person. You can request a review of the student loan application by contacting OmaSp customer service.

8. Where do we get personal data about you?

We collect personal data mainly from the data subject or their representative. Data is collected when the data subject visits OmaSp's branches or otherwise contacts OmaSp, for example, by phone, through feedback surveys or digital channels. Personal data may also be collected when you use OmaSp products and services, such as accounts, payment cards or online services.

We also receive information from third parties, such as registers maintained by the authorities (e.g. the Population Information System, the Positive Credit Information Register and other Tax Administration registers, the title and mortgages register) and credit information registers. We receive information related to payment orders from money transfer service providers, shops, other banks, payment service providers and other similar parties.

We also use national and international registers to determine whether the data subject is a politically exposed person (PEP data) and to ensure that the data subject is not subject to sanctions regulations or freezing decisions.

9. Disclosure of data

Bank secrecy restricts the disclosure of information held by OmaSp: OmaSp may disclose personal data only with the permission of the person in question or when the disclosure of information has been separately provided for in applicable legislation. OmaSp only discloses personal data when there is a justified need for it and always in accordance with the requirements of legislation.

Personal data is regularly disclosed:

- to companies belonging to the same group as OmaSp in accordance with applicable law;
- to authorities, such as the police, enforcement authorities, the Finnish Financial Supervisory Authority FIN-FSA and the Tax Administration to the extent required by law;
- to external business partners and operators, such as card companies or recipients of card transactions and payment service intermediaries.

As a rule, OmaSp discloses personal data only within the European Economic Area (EU Member States, Iceland, Liechtenstein and Norway). If, exceptionally, we disclose your personal data within the European Economic Area outside, we will notify you on a case-by-case basis and ensure the protection of your personal data adequate level as required by law and we use the approved personal data from time to time transfer mechanisms.

10. Transfer of personal data to processors

We have outsourced data processing tasks and use subcontractors and partners to produce and provide services. We may transfer your personal data to such parties for processing on our behalf. Even after the transfer, we are responsible for the personal data we transfer to the processors as a data controller. Subcontractors and partners may only process the personal data we provide to them in accordance with our instructions and are not entitled to use the personal data they receive from us for their own purposes. Through contractual and other arrangements, we ensure that our subcontractors and partners always process personal data carefully, in compliance with the requirements of legislation and good data processing practices.

OmaSp mainly processes personal data within the EEA (EU member states, Iceland, Liechtenstein and Norway). If, exceptionally, we transfer your personal data outside the European Economic Area in situations other than those listed above, we will notify you of the transfer on a case-by-case basis and ensure an adequate level of protection of your personal data as required by law and use the approved data transfer mechanisms from time to time.

Personal data processing tasks have been outsourced to the following entities located in the areas listed below:

External Service Provider	Region
Customer information system administrator	EU
Service provider of online conferencing tools	EU
Mobile application administrator	EU
Customer mailing service provider	EU
Service providers of sanctions monitoring	EU
Provider of demographic data forwarding services	EU
Electronic signature service provider	EU
Supplier of event invitations and feedback questionnaires	EU
Supplier of the payment cards service portal	EU, UK (based on adequacy decision)
Customer service chat and telephone service provider	EU, India (based on standard data protection clauses issued by the European Commission)

11. How do we protect your personal data?

OmaSp has appropriate technical and organisational security measures in place to ensure the processing of personal data in a secure manner that meets the requirements of legislation. The security measures we use include:

- Access management of systems and facilities
- Encryption methods
- Maintenance of change logs
- Regular training of staff

We also require our subcontractors to provide appropriate protection for the personal data being processed.

In security measures, OmaSp has paid special attention to the fact that certain purposes of processing personal data in accordance with this privacy policy are of such a nature that it is not possible to publish all data concerning the processing without compromising the purpose of the processing. OmaSp has limited such unpublished information to what is strictly necessary and documented the necessity and other processing information internally. OmaSp's Data Protection Officer monitors such processing independently. The data subject has the right to contact the Data Protection Ombudsman (see section 15), who can, at the request of the data subject, check the lawfulness of the processing of personal data.

12. What rights do you have as a data subject?

As a data subject, you have the rights described below under data protection legislation. You can submit a request for your rights described here at one of our branches or online banking.

Data Subject Rights	Description
The right to access your personal data	You have the right to access your personal data held by OmaSp. However, this right may be restricted by law, the protection of the privacy of other people and the protection of OmaSp's trade secrets.
The right to demand the rectification of incorrect or outdated information	You have the right to demand that incorrect information about you in the register be corrected, erased or supplemented, unless this is restricted by legislation.
The right to object to data processing	To the extent that we process your personal data on the basis of a legitimate interest, you have the right to object to the processing of your data on grounds relating to your particular personal situation. You also always have the right to object to the use of your personal data for direct marketing purposes.
The right to request restriction of processing	If you have reported that your data is incorrect, you have the right to request restriction of the processing of your data, for example, while any requests concerning your data have been clarified or resolved.
The right to request erasure	You have the right to demand the erasure of your data, for example, if you object to the processing of the data and there is no justified reason for continuing the processing or if the processing of the data is unlawful. However, due to regulations in the financial sector, OmaSp is in many cases obliged to store your personal data for the duration of the customer relationship and even after it, if the processing of the data is necessary, for example, to comply with legal obligations or to process legal claims.
The right to transfer data to a system maintained by another party	You have the right to receive the data you have provided yourself with in a machine-readable format and to transfer it to a system maintained by another party when the processing of the data is based on a contract or consent, the processing of the data is carried out automatically and the transfer is technically possible.
The right to withdraw consent	To the extent that we process your personal data on the basis of consent, you always have the right to withdraw your consent. The withdrawal of consent does not affect the lawfulness of the processing of personal data carried out before the withdrawal.

13. How long do we retain your personal data?

We will only store your data for as long as it is needed for the purposes specified in this privacy policy or we have a legal obligation to keep the data. After this, the personal data will be deleted or anonymised.

The applicable retention periods vary depending on the purpose of use of the personal data in question and the legal basis for the processing. Below are examples of the retention periods we observe:

- As a rule, the information concerning the customer relationship and the contract is stored for ten years after the end of the customer relationship in order for OmaSp to prepare, present and defend any legal claims and to demonstrate that it complies with the obligations set by law and regulations.
- Customer due diligence data (Knowing your customer KYC) is stored for five years from the end of the said contractual relationship as required by legislation on the prevention of money laundering and terrorist financing.
- Call and chat recordings are stored for 12 months from their recording to verify customer transactions, to improve customer service and security, and to ensure regulatory compliance.
- Web conferencing records are stored for seven years to verify customer transactions, to improve customer service and security, and to comply with the statutory retention period for any investment advice included in the web conferencing.

14. Cookies

The Omasp.fi website uses cookies to implement the website's functions, develop user experience and for marketing activities. A cookie is a small text file that is stored on the user's computer when visiting a website. You will be asked for your consent to the use of cookies when you visit our website for the first time and you can later modify your cookie preferences on our website under "Cookie settings".

15. Notification to the Data Protection Ombudsman

If you consider that the processing of your personal data is not lawful, you have the right to lodge a complaint with the Data Protection Ombudsman. Contact information can be found on the website www.tietosuoja.fi.