

# Oma Savings Bank's privacy policy – Private persons related to corporate 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 complete implementation of the rights of data subjects.

With this privacy policy, we provide private persons involved in customer relationships between OmaSp and its corporate 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.

OmaSp may make changes to this privacy policy. You can always find the up-to-date privacy policy on our website: [omasp.fi](https://omasp.fi). This privacy policy was last updated on 18 February 2025.

## 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](https://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](mailto:tietosuoja@omasp.fi)

## 4. Who does this privacy policy apply to?

This privacy policy applies to OmaSp's:

- representatives and contact persons of corporate customers;
- representatives and contacts of potential corporate customers;
- corporate online banking users authorised by corporate customers and other account authorisations for OmaSp's corporate customers;
- main users of the OmaYritys portal and users who manage the corporate cards issued by OmaSp;
- cardholders of cards issued to corporate customers (Visa Business Debit, OmaSp Visa Business Credit and K-Business Credit); both
- beneficial owners of corporate customers

("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 information	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 ID card details, such as expiry date, issuer and number, nationality, politically exposed person (PEP information);  In the case of beneficial owners, also the country of taxation, tax number, country of issuance of the tax number
Customer information	Information related to corporate 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 or prohibition of electronic direct marketing
Contract and product information	Information on agreements between OmaSp and the data subject and information on the services used by the data subject	Account agreement, card agreement, corporate online banking agreement, terms of use of the OmaYritys portal
Customer transaction information	Transaction information related to the bank transfer of the data subject	Credit transfers, payment transactions, cash transactions
Background information	Background information reported by the data subject and obtained from other sources	Financial status
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 browsing data, log data
Recordings and message content	Recordings related to conversations and communication with the data subject and visits to our offices	Call and video recordings, chat conversations, online messages

## 6. For what purposes do we process personal data?

OmaSp processes personal data only for predetermined purposes or for purposes compatible with them.

We process personal data on data subjects for the purposes of managing the services and operations provided to our corporate customers and to fulfil our legal and contractual obligations.

This includes among others:

- communication with representatives and contact persons of OmaSp's corporate customers;

- management and service of the customer relationship related to the use and management of the cardholders' corporate card;
- distinguishing and identifying data subjects and their roles;
- risk management and ensuring safety;
- fulfilling retention, reporting and inquiry obligations arising from the law and in accordance with the regulations and instructions of the authorities;
- developing the quality and functionalities of services; and
- marketing of OmaSp's products and services.

## 7. On what legal bases do we process personal data?

We always ensure that we have a basis for processing your personal data in accordance with the EU General Data Protection Regulation. The processing criteria used by OmaSp and their examples are described in the table below.

Legal basis	Description	Examples
<b>Performance of the contract</b>	We collect and process personal data in order to perform the contract between us and the data subject and to take measures prior to entering into a contract.	Examples of agreements on the basis of which we process personal data: <ul style="list-style-type: none"> <li>• a card agreement with the cardholder;</li> <li>• business online banking agreement; and</li> <li>• agreement on the use of the OmaYritys portal.</li> </ul>
<b>Compliance with legal obligations</b>	We need to process personal data due to legal obligations and decisions of the authorities.	Examples of our legal obligations: <ul style="list-style-type: none"> <li>• the obligation to verify identity and know the customer;</li> <li>• prevention of money laundering and terrorist financing, compliance with sanctions regulations and freezing orders;</li> <li>• requirements related to payment services;</li> <li>• accounting and risk management obligations, such as credit and collateral risks, as well as capital adequacy requirements;</li> <li>• the obligation to report to authorities such as customs, tax, police, enforcement and supervisory authorities; and</li> <li>• other obligations related to service- or product-specific legislation, such as obligations related to loans, funds and collateral.</li> </ul>
<b>Legitimate interest</b>	The processing of personal data may be justified due to OmaSp's legitimate interest. We will always ensure that such processing is proportionate to the rights and interests of the data subject.	Examples of processing based on our legitimate interest: <ul style="list-style-type: none"> <li>• managing the customer relationship and communicating with a representative or other contact person of our corporate customer with whom OmaSp does not have a direct contractual relationship;</li> <li>• marketing our products and services;</li> </ul>

		<ul style="list-style-type: none"> <li>• conducting customer satisfaction and marketing surveys to develop services or products;</li> <li>• developing and managing systems and processes, including testing;</li> <li>• developing statistics and analyses, for example to improve credit risk models;</li> <li>• implementing camera surveillance at our offices to prevent and investigate situations that endanger safety; and</li> <li>• establishing, exercising or defending legal claims.</li> </ul>
<b>Consent</b>	We may also process your personal data on the basis of your separate consent.	<p>Examples of processing for which we may ask for your consent:</p> <ul style="list-style-type: none"> <li>• electronic direct marketing;</li> <li>• use of cookies on the OmaSp website.</li> </ul>

## 8. 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.

We will always clearly inform you if we use your personal data for automated decision-making. You have the right to express your opinion on a decision based solely on automated processing, such as profiling, whether the decision in question produces legal effects concerning you or if the decision otherwise has a similarly significant effect on you. You also have the right to demand human participation in decision-making.

## 9. Where do we get personal data about you?

We collect personal data mainly from the data subject and the company they represent. 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, such as the OmaYritys portal.

When we receive information about business card payments, we collect information from senders, shops, banks, and payment service providers whose services the card has been used for.

We also receive information from third parties, such as registers maintained by the authorities (e.g. the Population Information System and business registers), credit information registers and other registers that provide information on, for example, beneficial owners. 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.

## 10. 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 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; and
- K-Business Credit cards to Kesko Corporation for the implementation of the K-Business entity.

## 11. Transfer of personal data to processors

We have outsourced data processing tasks and use subcontractors and partners, such as IT suppliers, 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.

## 12. Transfer of personal data outside the European Union or the European Economic Area

OmaSp mainly processes personal data within the EEA (EU member states, Iceland, Liechtenstein and Norway). If we transfer your personal data outside the EEA, we will ensure an adequate level of protection of your personal data as required by law and use the data transfer mechanisms approved at the time, such as the European Commission's Standard Contractual Clauses.

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

## 14. 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
<b>The right to access your personal data</b>	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.  If you are a user of the OmaYrityys portal, the personal data we process is largely visible in the portal in question.
<b>The right to demand the rectification of incorrect or outdated information</b>	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.
<b>The right to object to data processing</b>	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.

<b>The right to request restriction of processing</b>	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.
<b>The right to request erasure</b>	<p>You have the right to demand the erasure of your data, for example, if you object to the processing of your data and there is no justified reason for continuing the processing or if the processing of the data is unlawful.</p> <p>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.</p>
<b>The right to transfer data to a system maintained by another party</b>	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 if the processing of the data is based on a contract, the processing of the data is carried out automatically and the transfer is technically possible.
<b>Right to withdraw consent</b>	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.

## 15. 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.
- The application logs of the OmaYritys portal are stored for two years, after which the log data is anonymised.

## 16. 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".

The OmaYritys portal uses only technically necessary cookies to maintain the portal user's session. If you want to avoid the use of cookies, you can configure your browser settings so that cookies are not downloaded to your computer. However, this may affect the functionality of the portal.

**17. 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](http://www.tietosuoja.fi).