

How we process your personal data

For Handelsbanken, your confidence in how we process your personal data is critical, and we want you to feel assured that we protect your personal integrity. Here we describe the personal data that Handelsbanken processes, and why. The information also includes our sources of personal data, with whom we share data, and how long it is saved. We also describe how you can exercise your rights under the General Data Protection Regulation, make your views known and contact us.

The company within Handelsbanken with which you have a relationship generally act as the controller for the processing of your personal data. In the description below, any references to 'Handelsbanken', 'the Bank', 'we', or 'us' refer to all companies in the Handelsbanken Group in Sweden. Further information on how to contact us can be found on the 'Contact us' page of our website.

For whom the information is intended

The information is intended for you, where relevant, based on the various relationships you have with the Bank, such as when you are:

- An existing or prospective customer of the Bank
- A trustee, administrator, holder of power of attorney or other agent
- A payer, pledgee or guarantor
- A beneficial owner, authorised signatory or representative for one of our corporate customers
- In contact with the Bank in your professional role, such as employee of another bank, consultancy firm, broker, supplier or public authority
- A private individual without an existing agreement with the Bank, whom the Bank contacts as part of marketing activities
- Shareholders in the Bank and its representatives
- A visitor on the Bank's premises, for example visits related to your professional role, as a customer or in connection with a job interview

What personal data the Bank processes

The personal data we collect and process is divided into different categories:

- **Basic personal data**, for example civic registration number or equivalent, name, contact details and information about ID documents and associated details
- **Personal choices** for example relating to direct marketing, language or acceptance of cookies
- **Assessments and classifications** according to rules regulating money laundering, securities trading or, for example, liability for taxation in the USA
- **Agreements** including all types of information linked to such agreements, such as account numbers, loan numbers, card details, property designations and powers of attorney
- **Financial transactions**, such as deposits, withdrawals, loan payments, card purchases and securities transactions
- **Communication** between you and the Bank, for example by mail (electronic or physical), sms, chat or telephone
- **Review logs**, for example IP or MAC address, logins to Online Banking or the Bank's app
- **Special categories of personal data** referring to particularly sensitive personal data, such as information about your health. We only process this type personal data when it is relevant for a specific product or service, such as our life insurance products, or when required to do so by law.

For what purposes and legal grounds do we process your personal data

The basic purpose for which Handelsbanken collects, processes and stores personal data is to enable us to prepare, provide and administer the Bank's products and services to you – whether digitally, at a branch, by mail or telephone. The legal grounds for this is to fulfil the terms and conditions of our agreements.

Fulfilling the terms and conditions of our agreements

The basic purpose for which Handelsbanken collects, processes and stores personal data is to enable us to prepare, provide and administer the Bank's products and services to you – whether digitally, at a branch, by mail or telephone. The legal grounds for this is to fulfil the terms and conditions of our agreements.

Complying with laws and decisions from public authorities

The Bank is required to comply with numerous laws and decisions from public authorities, and in this context, we process your personal data in order to, for example:

- To check and verify your identity
- Monitor and analyse how you use your accounts, enabling us to prevent or identify fraud, money laundering and other crimes, and to meet the Bank's obligations under the Swedish Act (2017:630) on Money Laundering and Terrorist Financing (Prevention)
- Document and save personal data linked to credit testing and advice on securities
- Manage the security requirements for online payments and account access
- Report to public authorities, such as the Swedish Tax Agency or the Swedish Financial Supervisory Authority
- Follow the Swedish Book-keeping Act, and rules on risk management and statistics
- Managing, analyse and follow up complaints
- Inform our customers, for example at a branch, by mail (electronic or physical), sms, push notifications or telephone

The Bank's legitimate interest

Handelsbanken offers financial services with the objective of creating good, long-term relationships with our customers. To this end, we process your personal data for the following purposes for example:

- Market research and customer research to develop our products, services, offerings and meeting places
- Marketing activities through which we identify and suggest products or services that may be relevant to you, unless you have informed us that you would not like to take part in such activities or receive such offerings. You may receive offers about these activities, for example, by mail (electronic or physical), sms, push notifications or telephone.
- Quality surveys in collaboration with customer survey companies
- Developing, improving and managing our products, services, applications, technical systems and IT infrastructure, and testing associated with these activities
- Developing, maintaining and validating our models and methods for risk analyses, for example capital adequacy, and preventing and identifying fraud, money laundering and terrorist financing
- Risk analyses, and developing statistics to improve our credit risk models, for example
- For security reasons, to have the necessary information about visitors on the Bank's premises

With your consent

For certain products, we require your consent to process your personal data, and in such cases, we request this separately from the agreement for the product or other documentation. We also describe how you can revoke your consent and how this affects you with regards to that specific product or service.

One example where we use consent is when you use our website. A cookie with a unique ID is saved by your browser and allows us to analyse and understand how the website is used. You provide your consent for this when you accept cookies the first time you visit our website. However, we do not analyse how individual users use the website, and thus no names, e-mail addresses, IP addresses or similar are stored in our cookies. Further information on how we use cookies can be found on the 'Cookies' page of our website.

Profiling and automated decision-making

In some cases, the Bank uses profiling. This refers to the automatic processing of personal data to conduct analyses of our customer's financial situation, personal choices or behavior in different meeting places. Profiling is used, for example, to analyse our advisory documentation, in conjunction with marketing, in the development of our systems or in connection with preventive measures against money laundering and terrorist financing.

The bank also uses automated decision-making, including profiling, in some cases. An automated decision is made technically without human intervention. The bank uses these kind of decisions to increase speed, objectivity and correctness in our offering of services. Examples when this is used are:

- Granting/refusal of an application for a committed loan offer or a credit application via the internet or app. Decisions regarding committed loan offers and credits are based on, among other things, the information provided in connection with the application, together with other external credit scoring information such as income and records of non-payment. An overall assessment is made as to whether the credit application can be granted or not.
- Granting/refusal of an application of debit card via Online Banking or the Bank's app. The automated decision is based, among other things, on how your affairs in the bank are handled, for example, if overdrawn accounts or payment reminders occur. It also requires that an up-to-date customer due diligence is available as the bank is obliged to understand the purpose of the business relationship and the transactions occurring.
- Transaction monitoring, in order to identify and prevent fraud.

When applying for a service where automated decision-making, including profiling, you are always entitled to contact your branch to object to the decision and request re-assessment.

From where we obtain your personal data

We collect personal data directly from you, for example when you apply for a service or a product, when you sign an agreement with the bank or when you use various services and products. Data is also collected in connection with interactions you have with us, for example meetings, telephone conversations, mails (electronic or physical), quality surveys or via our digital channels.

We also use the contact information we collect directly from you, in our continued contact with you. This means that information you provide in connection with a certain service, can be used in subsequent contacts for other services as well. Examples when you give us your contact details are when you send us a loan application or when you connect your mobile phone number to Swish.

You can change your settings as regards direct marketing in the 'My Profile' section of Online Banking. You can also contact us to update the settings.

We also obtain information from public registers and other databases, such as Swedish Personal Address Register (SPAR), the Swedish Tax Agency, UC ((Swedish credit agency) and the Swedish National Land Survey.

If you are not a customer of the Bank and are contacted by us as part of our marketing activities, we have obtained your personal data from a public database such as SPAR, unless another specific source is disclosed for the activity in question.

Video surveillance

The Bank uses video surveillance as part of our security work for the Bank's employees and customers. It is used, for example, to prevent and investigate crimes, counter fraud, money laundering and other

criminal activities, and to ensure your and your employees' physical security. Video surveillance takes place in or immediately outside the Bank's premises. Areas in which video surveillance is in operation are clearly signposted. Video surveillance may also be in operation on ATMs close to the Bank's branches. If the Bank suspects a crime, audio may also be recorded.

Surveillance is permitted under the Swedish Video Surveillance Act (2018:1200), and it is deemed necessary to protect the Bank's legitimate interest in appropriate security work. In assessing whether surveillance is to be used, we have taken personal privacy into account and determined that video recordings, and in certain cases sound recordings, entail a limited infringement of your right to privacy which is outweighed by the increased security provided by surveillance cameras in or immediately outside the Bank's premises.

Where a crime is suspected, personal data is processed to establish, support or defend a legal claim. We share video and audio recordings with authorities where required by law, such as when the recordings are needed as part of a criminal investigation.

Video and any audio recordings are saved for up to 30 days.

Recording of telephone conversations

We record, save and potentially review telephone conversations for various purposes. This is done for the following reasons, for example:

- Documentary evidence, whereby we are required by law to document that we have reached an agreement during a telephone conversation, in conjunction with securities transactions, for example
- Educational purposes, for which we invoke the legal grounds of the Bank's legitimate interest
- Suspicions of fraud or other criminal activity
- Threats against the Bank's employees
- Other purposes, including documentary evidence not required by law, recording invokes the legal grounds of the Bank's legitimate interest. This includes, for example, when we collect, process and store personal data in order to enable ourselves to prepare, provide and administer the Bank's products and services to you. We also make recordings to enable the verification of agreements or conversations between you and the Bank.

Information we receive from you about other private individuals

If you, with regard to a product or service at the Bank, provide us with information about another person, you must show this document 'Processing of personal data' to these individuals, and gain assurance that the person in question is aware of, and does not object to, the sharing of their personal data, to the extent required for the purposes of the processing. This may be applicable, for example, when you, as a private individual, make a joint credit application with another person or provide a power of attorney enabling another person to handle your affairs at the Bank.

It may also be applicable when you, as a representative of a company or organisation that is a customer of the Bank, provide us with information about other individuals as a part of our business relationship or in conjunction with other corporate actions. Such individuals may refer to our own customers, tenants, employees, business partners, board members, shareholders or holders of power of attorney, from whom the Bank assumes you have authorisation to disclose their personal data.

With whom we share your personal data

By law, The Bank may not share information relating to you unless there is clear support for this, either as required for us to fulfil the terms and conditions of an agreement with you, or for legal purposes that require or permit sharing, such as reporting to the public authorities.

In order to fulfil the terms and conditions of our product and service agreements, we need to share information regarding you with other companies in the Handelsbanken Group, and at times also with external companies that provide the Bank and our customers with agreed services. This may refer to, for example, other banks,

Handelsbanken

payment intermediaries and other financial infrastructure parties, suppliers, parties that act on behalf of customers, or other parties in the product agreement.

Examples of when we share your personal data outside the Group are:

- When we obtain credit scoring information in conjunction with an application for a loan, e.g. to UC (Swedish credit agency)
- To parties that constitute part of payment flow linked to a product of service, such as a card issuer or acquirer of card transactions
- When we make a payment on your behalf, e.g. Mastercard, Bankgirocentralen (BGC), Finansiell ID-teknik (BankID) or Getswish AB (Swish)
- To other banks in or outside the EU/EEA (the European Economic Area), when we transfer funds or other assets on your behalf
- To other public authorities in order to comply with laws and other regulations relating to, for example, taxes, money laundering or terrorist financing
- To companies in which you, as a private individual, are a shareholder, in order to comply with laws relating to information that must be disclosed about shareholders
- We work with Citibank on the custody of financial instruments. In order to allow the Bank to offer custody service for financial instruments, the Bank shares personal data with Citibank. Information on how Citibank processes personal data can be found via 'Citibank Privacy Policy' linked in our 'How we process your personal data' on our website.
- We also share information about customers of the Bank with other companies in the Handelsbanken Group for marketing purposes
- In addition, we work with customer survey companies that perform quality surveys on behalf of the Bank
- In the event that we sell parts of our business, Handelsbanken may share your personal data with acquiring companies

Transfers to a third country

On occasion, we may transfer personal data to recipients in a country outside the EU and EEA. This is then called a 'third country'. This mainly occurs when we transfer funds or other assets to a recipient in a third country as assigned by you, in order to fulfil an agreement between you and the Bank.

Another reason for such transfers may be that the Bank is obliged to submit personal data to a public authority in a third country.

If we do not perform an assignment to fulfil an agreement with you, one of the following conditions must be met for us to execute a transfer to a third country:

- That the European Commission has determined there is an appropriate level of protection in the country in question
- That there are other protective measures, such as standard contractual clauses or binding corporate rules
- That the transfer is a specifically permitted by a supervisory authority, or
- That the transfer is permitted under applicable data protection legislation

For how long we save your personal data

We save your personal data for as long as it is necessary to provide the products and services for which you have an agreement with us. We also save personal data to be able to fulfil requirements in laws and decisions by public authorities, such as those for accounting records or tax reporting.

If you close your account or discontinue another service at the Bank, we need to save the parts of your personal data that are related to that product or service for a given time period. For example, we need to retain some personal data for seven years to be able to report to the Swedish Tax Agency, and for a maximum of 10 years to comply with rules relating to money laundering.

If you apply for one of the Bank's services but do not subsequently enter into any agreement with the Bank, your personal data may need to be saved to comply with rules relating to money laundering. As a general rule, your personal data is not saved for longer than a maximum of five years.

If you are not a customer of the Bank and have been contacted by us as part of a marketing activity, your personal data is saved for the duration of the marketing activity up to a maximum of three months.

On social media

The Bank is active on several social media networks, such as Facebook, Instagram and LinkedIn. If you contact us via our social media accounts, your personal data will be collected and processed by both us and the social media network in question, in accordance with their data protection policies.

The Bank and the individual social media networks have a shared responsibility for personal data, meaning that you as a registered user have the right to know what information is held by both parties. The Bank is responsible only for the processing linked to the Bank's accounts.

You as a social media user can take part of the processing of personal data linked to your account via their Data Policies, which can be found on respective networks' websites. Information on how you can take part of the division of responsibilities' in the joint controllership for example for Facebook and Instagram, can be found via the link 'Controller Addendum' in the document 'How we process your personal data' on our website.

We may also analyse your activities and send targeted messaging to different target groups on social media for marketing purposes. The purpose of such analyses is to ensure that you, as a customer, receive relevant information. You can find more information about how we work with social media under 'Handelsbanken on social media' on our website.

Our apps

If you have downloaded one of the Bank's apps, we may send information to the device on which the app is installed in the form of push notifications. Such messages may, for example, include information that a card purchase has been made, or that the terms and conditions of a product have been updated. You can choose whether the information is sent or not via the settings for the Bank's apps. You can also decide how the information is displayed on the device's screen when locked, via the device's system settings. The information sent to your device is encrypted.

Your rights regarding processing of personal data

You have several rights regarding your personal data that is processed by the Bank. In order to exercise these rights, you need to fill in the request 'Registerutdrag för personuppgifter via Online Banking, our website, at your local branch or when you call 0771-77 88 99 for personal service. You can request a copy of your personal data that is being processed by the Bank, request specific information by indicating precisely the information to which you are referring or exercise any of the other rights at the same request.

We will respond to your query as soon as possible and as a general rule within a month. In most cases, the administration of your query is free of charge. Before sending the requested information, the Bank must ensure that the right person will receive it, for which reason you will need to securely identify yourself, such as when the request is made via Online Banking.

If you have more questions about how to exercise your rights, further information on how to contact us can be found on the 'Contact us' page of our website and under 'Further information' below.

Requesting access to your personal data

You have a right to request a copy of your personal data being processed by the Bank. The extract includes information that you, in many cases, will find in the online services we offer you. You can also request specific information by indicating precisely the information to which you are referring.

In some cases, the right of access may be restricted, due to for example legislative requirements, confidential information or information linked to business secrets. Internal information that constitutes part of the preparatory work for ensuring correct administration, or information kept secret in order to prevent, investigate or uncover criminal activity are other examples of when access to information is restricted.

Requesting the correction of erroneous or incomplete data

If you discover that the Bank has erroneous or incomplete data about you, you are entitled to request correction. The Bank corrects the data it holds as soon as we are made aware of the matter, unless restrictions are in place due to legislative requirements. If the Bank has shared information with a third party, we also ensure that this information is corrected.

Requesting deletion

You can request the deletion of your personal data processed by the Bank under some circumstances. This is possible when, for example, the data is no longer needed for the purposes for which it was collected, when you revoke your consent and the Bank has no legal grounds for continued processing, when the processing is illegal, or when the processing is related to direct marketing and you object to this. You can change your settings as regards direct marketing in the 'My Profile' section of Online Banking. You can also contact us to update the settings.

The right to deletion of the data may sometimes be restricted, such as when the Bank needs the information to administer your agreements, or when the Bank is legally required to store certain information for the duration of your relationship with the Bank. Following the conclusion of such a relationship, we may also be required to retain some of your personal data for up to 10 years and sometimes - for certain specific purposes - for even longer, due to stipulations in the Swedish Anti-Money Laundering Act, rules about accounting information in the Swedish Book-keeping Act, and rules in the Act of Limitations regarding the limitation of claims.

Object to the Bank's processing

You have the right to object to the Bank processing your personal data when this takes place on the legal grounds of the Bank's legitimate interest. Objections to the Bank's processing of your personal data for direct marketing can be made at any time, and will result in the Bank discontinuing this type of processing.

Request restriction of processing

You have the right to request restrictions to the processing of personal data in the event that you object to the accuracy of the information relating to you that the Bank has registered, or if you object to the legality of the processing. Restrictions can also be requested when you have objected to the processing and, for example, requested the deletion of personal data. In such cases, the processing is restricted to specific limited purposes, such as retention until the data is corrected, or until it is established that the Bank is entitled to process the personal data on the legal grounds of the Bank's legitimate interest.

Data portability

You can obtain a digital copy of most of the personal data that you have submitted to the Bank, for which the processing is based on the legal grounds 'consent' or 'agreements' and is automated. We can, on your behalf and where technically possible, transfer this data directly to another company or public authority for processing of your personal data.

Further information

If you have any questions or comments on how we process your personal data, you are welcome to contact your branch, write to the Bank's Data Protection Officer at dpo@handelsbanken.se or write to the following postal address:

Handelsbanken
Data protection officer
106 70 Stockholm

This contact information is also applicable for the Bank's Swedish subsidiaries:

Ecster AB
Handelsbanken Finans AB
Handelsbanken Fonder AB
Handelsbanken Liv Försäkrings AB

Stadshypotek AB and the pension Fund:

Pensionskassan SHB Försäkringsförening

In addition, any complaints concerning the processing of your personal data may be lodged with the Bank's complaints team or the supervisory authority, the Swedish Authority for Privacy Protection. The contact details for the Bank's complaints team can be found under 'Contact us' on Handelsbanken's website, and for the supervisory authority on IMY's website.

Changes and latest version

'How we process your personal data' is updated on an ongoing basis, in conjunction, for example, the addition of new purposes for processing or when additional categories of personal data are processed.

Last updated as of January 2023.