Privacy Notice for Private card holders

This Privacy Notice provides information as to how, when, and why SEB Kort Bank AB 556574-6624 ("SEB Kort" or "we" or "us") will collect, process, store and share personal data for you as a private customer, cardholder or prospective customer or cardholder.

We will process your personal data in a careful and responsible manner. By personal data, we mean any information that can be directly or indirectly traced back to you.

Sources of personal data

Personal data is normally collected directly from you, for instance when you apply for our services or products or generated in connection with your use of our services and products. Sometimes additional information is required to keep the information up to date or to check that the information we have collected is correct.

<u>Personal data from you</u>
We collect the following personal data categories directly from you:

- Identification details such as name, national ID/passport or both in some circumstances, citizenship, contact details e.g., postal address, email address, telephone number, mobile number.
- Information regarding affiliations, status as a politically exposed person and close family members.
- Authentication information in all situations where we need to identify you as a customer or when a signature is necessary, for example when signing an agreement or when visiting My pages.
- Information about your financial situation e.g., income, employer, source of wealth, debt, housing conditions will be collected when applying for a credit card or loan. This information shall be updated by you on a regular basis.
- Information about how you expect to use your credit card e.g., amount, type of purchases and in which region must be collected according to the regulations for anti-money laundering ("AML").
- Transactional information regarding your purchases, such as which merchant and amount. We also collect information about your use of cash withdrawals.
- Your communication with us such as emails, telephone calls or via our app and website.
- Visual media such as photos or video surveillance if you visit our SEB premises.
- We record the call when you call our customer service. We do that i.a. to document and/or clarify circumstances when concluding agreements as well as to detect and avoid fraud, to improve our services and educate our employees.
- Special categories of personal data e.g., health declaration is collected on special occasions e.g., when the reason for an unpaid dept is because of illness. In case you have a special agreement because of a membership in a union, we ask for information about union membership.
- We may store information from your use of our mobile app or other online services. For example, your IP address or your geographical location for the purpose of improving our service to you.

Personal data from other sources

In addition to the information that you provide us with yourself, we may collect information about you elsewhere. This applies, for example, when we:

- Regularly update information about name and address via population registers.
- Carry out checks that we are required to perform in order to prevent our products and services being used for money laundering, by retrieving information from sanction lists with international organizations such as the European Union ("EU") and United Nations ("UN") or Criminal offense data.
- Retrieve information from Credit information bureaus.
- Receive payments, we collect information from senders, stores, banks, and payment service providers.

In some cases, we also collect information from other entities in the SEB Group pursuant to Group internal service arrangements and appropriate data transfer mechanisms.

Please note that our websites use cookies. A cookie is a piece of information that a website transfers to the cookie file on your computer or device. Read more about the use of cookies here

- Eurocard: https://eurocard.com/cookies/

Why we process your personal data and on which lawful ground.

We are often required by law or as a consequence of our contractual relationship with our clients to collect certain personal data. Failure to provide this information may prevent or delay the fulfilment of these obligations.

The performance of a contract that you are a party of

The main purpose of our processing of personal data is to collect, control and process personal data before and when signing agreements with you, as well as to document, administer and perform what is required to fulfil the agreements. We process your personal data when:

- You are applying for a credit card, loan, or service.
- You are contacting our customer service.
- The processing is performed to establish, assert, or defend legal claims and debt.

Comply with laws & regulations.

We must be able to comply with the various laws and regulations in the jurisdictions that we operate in:

- Anti-money laundering and terrorist financing laws ("AML/TF") – we are required to perform due diligence activities, including identity checks and transaction monitoring.
- Activities relating to financial crime and market abuse prevention and detection, fraud, tax evasion and corruption.
- We store your transaction information to comply with regulatory, accounting and tax reporting requirements.
- When we are asked to co-operate with regulatory-, judicial and other authorities.
- We process your financial information to comply with regulatory requirements to measure and manage risks regarding credit development, risk quality and capital adequacy.

- We process your data received from the credit application, credit bureaus and from transactions- and payment history to assess your credit rating by using models and business rules.
- To be able to assess your credit rating and build and improve our credit models. The models make it possible to assess how to act as a responsible lender and our models ensure that we fulfil our legal obligations and conduct a proper creditworthiness assessment.
- We ensure that our credit decisions are adapted to the SEB credit policy. This includes profiling of existing customers to ensure correct credit decisions.

Legitimate interest

We have, in certain circumstances, a legitimate interest in processing your personal data. When vi process personal data with reference to "legitimate interest" we shall demonstrate that we have justified compelling reasons for the processing and that these reasons take precedence over your interests and rights.

The following are examples of situations where we process personal data using legitimate interest as the legal ground for processing:

- To perform customer and product analyses to improve our business relationship with you and to provide relevant offers.
- To improve our business processes in order to provide a better service to you, e.g., when you contact our Customer Service.
- For fraud monitoring purposes, to unveil fraud situations as early as possible so that you as a customer can feel safe using our products.
- When we process personal data related to customer surveys.
- We record the call when you call our customer service. We do that i.a. to document and/or clarify circumstances when concluding agreements as well as to detect and avoid fraud, to improve our services and educate our employees.

Consent

We usually do not base the processing of your personal data on a consent.

If you provide us with your consent to process and store your personal data, you can at any time withdraw such consent. Withdrawal of consent will however not affect any processing of personal data based on the consent prior to the withdrawal.

There might however be other reasons for obtaining a consent from you than for processing of your personal data, e.g., when it is necessary in accordance with local marketing legislation.

Profiling

Profiling is when your personal data is automatically processed, primarily your financial circumstances or personal preferences such as transaction data on your credit card or financial information from you or credit bureaus.

We use profiling for:

- combating money laundering and terrorist financing, to fulfil our legal obligations
- fraud prevention, to find and act on fraud behaviors

- segmenting for marketing research. We use profiling to give you better and relevant offers.
- the purpose of approving or declining a credit card- or loan application, to secure a proper and correct credit worthiness assessment

Automatic decisions

We use automatic decisions, for instance when you apply for a credit card using our online application form. Such application can be approved or declined by using automatic decisions.

Our automated decisions may sometimes be based on profiling. Where such a decision has legal consequences for you, e.g., a decline of an application or otherwise significantly affects you, you have a right to object to the automatic decision.

Personal data sharing and data transfers

SEB Group

We will share personal data about you with other legal entities and affiliates within the SEB Group in order to meet our legal and regulatory obligations such as:

- For internal approval processes
- For risk measurement, control, and reporting
- For regulatory and financial transaction reporting
- Financial crime and external fraud prevention, for instance to be able to comply with our obligations pursuant to AML/TF regulation
- To be able to provide as good service to you as possible and act as one bank

External recipients

We will share personal data about you to external recipients for the following purposes:

- To authorities and institutions where required or requested and where we are permitted to do so by law, regulation, supervisory or similar authority or court order.
- We will pass on your personal data to our debt collector Intrum in the event of non-payment.
- Our suppliers. We share your personal data with service providers. This is relevant where e.g., we authenticate you in different digital channels for example when logging in to My Pages (Signicat AS) or when we produce cards (Tieto Evry Card Services AS), hosting or support services from vendors (e.g., Depona AB or Mastercard) and when we share personal data with credit bureaus or similar (such as Experian A/S, UC AB, Dun & Bradstreet AS and Suomen Asiakastieto Oy etc). In all such instances and where applicable, we take steps to ensure that there are Data Processing Agreements in place to protect your data and to limit access and use of that data strictly for the purposes and to the extent needed for those services to be performed. When a service is terminated, we impose requirements that any data stored outside of SEB is returned to us or destroyed.
- If you apply for or already use a digital wallet such as Apple Pay or Samsung Pay, etc., we will be transferring data including e.g. your card information to the digital wallet provider, to enable use of the digital wallet.

Third countries

We do not share your data with suppliers outside the EU/EEA ("European Union/European Economic Area") also known as third countries unless it is required by law or necessary for fulfilling our service to you as a customer. One example of the latter is our cooperation with Mastercard where some of your data may be transferred to the United States of America ("USA").

Another example is when we use Adobe Campaign for IT support services which are performed in EU/EEA as well as in India.

We only make such transfers after having performed a Transfer Impact Assessment ("TIA") to ensure that GDPR has been followed and if any of the following conditions are met:

- The European Commission has determined that there is an adequate level of protection in the country in question.
- We have taken other appropriate protective measures, e.g., Standard Contractual Clauses (SCCs) or Binding Company Rules (BCRs). You can obtain a copy of such standard contract by contacting us, see contact details below.
- Special authorisation from a supervisory authority has been obtained.
- Such transfers are permitted in special cases by applicable data protection legislation.

Data Retention

We will store your personal data for as long as it is necessary for fulfilling the purposes for which they were collected. The required retention period differs between the Nordic countries. Below we list some examples on relevant retention periods.

- If you have a contract with us, we typically store your personal data for 10 years after our business relationship has ended to be able to exercise our legal claim to defend ourselves. Some data will be deleted after 5 years according to the Money Laundry Act or after up until 10 years according to the Bookkeeping Act (depending on national legislation) e.g., copy of invoices.
- Marketing activities, such as send-outs, are saved for a maximum of two years
- If you are a prospective cardholder and do not have an agreement with us but have provided personal data to us in an application e.g., when your application has been declined, we will store your information for a maximum of two years.

Using our websites and our apps

If you have downloaded one of our apps, we can send information to the device where the app is installed, for example in the form of push notifications. The message may, among other things, contain information that a purchase has been made, an incorrect PIN code has been used or if a purchase has been denied.
In your device's system settings, you can control whether the information is sent or not and how the information is displayed on the device's screen in locked mode.

When the information is sent outside the SEB Group, it is done with uninterrupted encryption until the information arrives at your app.

To be able to do aggregated analysis of user interactions we gather information about what services you use on our website, in our in-logged environment and apps and how you use them.

The information that we collect are:

- Identification Data, such as IP address, device type and operation system, and
- Digital Tracking information, such as geographic location.

Your rights

We respect your rights to request access, modification, deletion, and portability of your personal data.

According to the GDPR, you are entitled to control your own personal data and to know how we process information about you. You can contact us if you want to exercise any of your rights.

Sometimes your rights are subject to limitations e.g., when we are unable to delete your personal data due to regulatory requirements and when the retention period has not been reached.

Requesting a personal data extract

You have the right to obtain information about what personal data we process about you. You can obtain this by requesting an extract from us.

Correcting incorrect or incomplete data

Should it turn out that we are processing personal data about you that is incorrect, you are entitled to request the personal data to be corrected. You may also request that an incomplete piece of personal data about you be supplemented.

Deletion of your personal data

You have the right to have any or all your personal data deleted. This is sometimes referred to as “the right to be forgotten”. In some cases, we may be unable to delete all the personal data because this is still necessary for its original purpose, and we still have a legal basis for processing it.

Restricting how we process your data

In some situations, you are entitled to ask for our processing of your data to be restricted for a certain period. This could be, for example, if you believe that some personal data about you is incorrect and we need to verify this. This may also be if you have objected to processing that is based on legitimate interest. In this case, we will assess whether our interests take precedence over yours.

Objecting to how we process your data

If we process personal data about you based on legitimate interest, you may object to this processing. For instance, if we process your personal data for the purpose of direct marketing.

Transferring your data to another party ("Data portability")
If we process your personal data based on an agreement or based on your consent, you have the right to access the personal data you have provided to us. If it is technically possible, you also have the right to have the data transferred to another party. This is known as data portability.

Automated decision making
When a decision is based on automatic processing (including profiling), you have the right to contact us to object to being subject to an automatic processing of your personal data.

Contact information and complaints

You are always welcome to contact us if you have any questions about your rights or about how we process your personal data.

Contact details to Data Protection Officer (DPO):

Office	**Contact Details**
Head Office **SEB Kort Bank AB**	SEB, Data Dataskydd 106 40 Stockholm Sweden 08-14 70 00
SEB Kort Bank AB, Denmark branch	Postbox 100 0900 København C. Denmark persondata@seb.dk
SEB Kort Bank AB, Norway branch	Personvernsombudet Postboks 1843, Vika 0123 Oslo personvernsombud@seb.no
SEB Kort Bank AB, Finland branch	Data Protection Officer Eteläesplanadi 18 00130 Helsinki Finland 09 6162 8000

Where applicable, you have the right to make a complaint to the competent supervisory authority.

Sweden	Denmark
Swedish Authority for Privacy Protection ("Integritetsskyddsmyndigheten (IMY)") Box 8114 104 20 Stockholm imy@imy.se	Danish Data Protection Agency ("Datatilsynet") Carl Jacobsens Vej 35 2500 Valby dt@datatilsynet.dk

Norway Data Protection Authority (“Datatilsynet”) Postboks 458 Sentrum 0105 Oslo	Finland Office of the Data Protection Ombudsman Lintulahdenkuja 4 00530 Helsinki tietosuoja@om.fi

If you are not satisfied with how we process your personal data and if your contact to our DPO, listed under “Contact details” did not provide you with a satisfying answer, please contact our responsible for complaints.

Sweden Att.: Klagomålsansvarig 106 40 Stockholm kundrelationerkort@seb.se	Denmark Att.: Klageansvarlig Postboks 351 0900 København C. kundeklager@sebkort.dk
Norway Att.: Klageansvarlig Postboks 1373 Vika 0114 Oslo kundeklage@sebkort.no	Finland Att.: Asiakasvalitusvastaava P.Box 1085 00101 Helsinki asiakaspalaute@seb.fi