Handelsbanken

Terms and condition
Applying from 1 January 2020

Terms and conditions for Handelsbanken's security solutions

1. Scope of application

These terms and conditions apply to Handelsbanken's security solutions. "Security solutions" refers, among other things, to BankID, Mobile BankID, log-in cards, security applications, log-in devices, PINs, single-use passwords and other procedures specified by the Bank for the identification or creation of electronic signatures under this agreement.

A security solution can be used for identification vis-à-vis the Bank and, in certain cases, a third party. With the aid of a security solution, the customer can also create electronic signatures to authorise orders, e.g. in Online Banking, Mobile Banking, and other telephone services. An electronic signature of this type is the equivalent of signing a document. In certain cases, the customer can also create electronic signatures in order to enter into agreements with a third party.

Personalised security credentials can be linked to a security solution. "Personalised security credential" refers to a personalised function which the Bank provides or approves for the purpose of authentication, such as a personal code and biometric readers such as a fingerprint reader (e.g. Touch ID for Mobile BankID).

Handelsbanken's security solutions are hereinafter referred to as "payment instruments", and this term shall have the same meaning as specified in applicable legislation regarding payment services, i.e. they are a personalised instrument or a personalised procedure that is, or can be, used by agreement to initiate a payment order.

The holder of a payment instrument is normally a customer of the Bank, but may also be a representative of the customer without themselves being a customer of the Bank. That which is stated in these terms and conditions concerning "the customer" shall therefore apply where applicable to the person who is a representative of the customer without themselves being a customer of the Bank.

Payment orders are also regarded as "electronically initiated" when the customer has identified himself/herself using their payment instrument, but authorises the transaction in a different way.

BankID is an example of a payment instrument which is stored in the chip on the log-in card or can be stored and used with other methods. BankID can be used by customers as proof of identity with companies, public authorities and other parties that are linked to Bankernas ID-tjänst (the Swedish bank ID service).

Further information on and more detailed instructions for the various procedures for identification and authorisation of orders are available from branches of the Bank and the Bank's website.

2. Responsibility for payment instruments and personalised security credentials

The payment instrument is personal and can only be used by the person to whom it is issued. The payment instrument must not be given to any other person, regardless of whether this will entail increased risk of unauthorised use. The same applies to personal codes and other personalised security credentials (see section 1 above). Payment instruments and personalised security credentials must be kept safe in the same way as money and other valuables, so that no other person is given the opportunity to use them. In environments with a high risk of theft, special vigilance must be observed, and a strict watch must be kept on the payment instrument. In the event of a burglary in the home, it is necessary to check that the payment instrument has not been stolen. All other instructions provided by the Bank together with the payment instrument must be followed.

Customers must exercise caution when using their payment instrument, and must not use the payment instrument in a manner which gives any other person access to the customer's accounts or services with the Bank. The customer is required, when the payment instrument's functionality so allows, to carefully examine that which is to be signed, and to decide whether he/she wishes to submit their signature.

The payment instrument must not be used in breach of prevailing legislation.

In order to protect the customer's electronic identity, it is of the utmost importance that the customer keeps the personal code for the payment instrument secret. The customer therefore undertakes:

a not to disclose a personal code to another person,
b only to use the personal code directly in the Bank's services and not to use the personal code when logging in to the Bank's services indirectly via another company's services,
c if there is an option of choosing a personal code, not to choose a personal code which has any connection with the customer's civic registration number, account number or phone number,
d not to write a personal code down in such a way that another person may gain knowledge of it,
e if a personal code is written down, not to state that it is a personal code or its connection with the customer's payment instrument and
f not to store the payment instrument or written notes about the personal code in such a way that another person can gain access to them.

That which is specified in a) - f) above also pertains, where applicable, to single-use passwords, other passwords, etc. `Single-use passwords' refers, for example, to the codes generated by the card reader and displayed on the card reader after the customer has entered their PIN code on the card reader.

The customer is aware that the payment instrument may be on a mobile device. A "mobile device" refers to a mobile phone, laptop computer, tablet, watch, wristband or similar device which can access the internet or some other network for phone and data traffic. If the payment instrument is on a mobile device, the customer must use the applicable security arrangements such as a passcode for locking the mobile device. The customer is also obliged to protect a mobile device or other technical equipment used by the customer against unauthorised access, for example, by installing virus protection or the equivalent and keeping this up-to-date.

If the customer chooses to verify their identity using biometric information, such as a fingerprint stored on a mobile device, the customer is obliged to ensure that only the customer's own biometric information can be used. The customer must,
for example, ensure that no other person's biometric information is registered on the mobile device.

It is the responsibility of the customer, where applicable, to update software and/or replace devices and/or use other methods or procedures which the Bank provides the customer with or gives instructions about and which, according to notification from the Bank, are required in order for the Bank's services to function.

When the customer has requested the blocking of his/her payment instrument, or the payment instrument has been blocked for any other reason (see sections 7 and 9 below), the customer is only liable for use of the payment instrument if the customer has acted fraudulently.

ID 2019-12-30 09:27:27

A457-1 2.9 2020-01-01

With the limitations that may exist according to laws or agreements, the customer also undertakes to accept liability for any damage that may arise as a result of the customer's handling of the payment instrument and/or the personalised security credentials.

Nothing expressed in this section 2 shall be regarded as preventing the customer from utilising payment initiation services or account information services provided by a third-party provider which the customer has retained.

“Third-party provider” refers to a payment service provider other than the Bank which has the required permits or is registered to provide payment initiation services and/or account information services.

“Payment initiation service” refers to an online service to initiate a payment order from a payment account with another payment service provider at the request of the customer.

“Account information service” refers to an online service to provide a compilation of information regarding one or more payment accounts which the customer has with one or more other payment service providers.

3. Legal implication of an electronic signature with a payment instrument

Before the customer submits an electronic signature using the payment instrument, the customer must carefully examine that which is to be signed, and decide whether the customer wishes to submit the signature. Signing electronically means that the customer wishes their electronic signature to have the same effect as if they had signed a paper document.

Unless expressly stated otherwise in the terms and conditions for the service in which a payment instrument is used, the customer gives the Bank and other parties that accept the payment instrument issued by the Bank, the right to execute the orders that are requested through the use of the customer's payment instrument and/or personal code. Submitted orders and documents that have been signed electronically with the customer's payment instrument are - apart from any exceptions stipulated in laws or agreements - binding upon the customer and may only be revoked or amended if this is expressly stated by the Bank or by the party providing the service in which the payment instrument is used.

4. Fees and charges

Fees for the payment instrument are payable in accordance with the terms applied by the Bank at any time for payment instruments. Upon request, the Bank's branches will provide information concerning applicable fees and payment terms and conditions.

5. Investigations

It is the customer's responsibility to request rectification from the Bank about any faults in the payment instrument within a reasonable period after the customer noticed or should have noticed the fault.

6. Restrictions in the use of the payment instrument

The Bank reserves the right to temporarily restrict the use of the payment instrument or to terminate the services with immediate effect due to maintenance activities, disruptions to operations, or if, in the view of the Bank, this is necessary to prevent damage to the Bank or other parties.

The Bank does not guarantee that it will be possible to use the payment instrument at all times at companies, public authorities and other parties that accept payment instruments issued by the Bank.

7. Validity period and blocking of payment instruments

a) Validity period and ordering of a new payment instrument

An issued payment instrument may be used for the purposes of identification and signing for a limited period of validity. When the validity period expires, the customer may order a new payment instrument from his/her bank branch. The expiry of the validity period does not affect the validity of the authorisations and attestations that the customer has already submitted to a counterparty.

The customer can request blocking of the payment instrument at any time, and order a new one.

b) The customer's obligation to block the payment instrument

The customer must immediately report to the Bank if a payment instrument has been lost, or if there is a suspicion that a payment instrument or a personalised security credential has been used in an unauthorised manner and, if the Bank so requests, also to report the incident to the police. Reporting that a payment instrument must be blocked is free of charge, and is done by calling Handelsbanken, in Sweden at 020 41 12 12, and from outside Sweden at +46 8 41 12 122. Customers connected to Handelsbanken Online Banking can also make a report via Online Banking in accordance with the instructions given there.

c) The Bank's blocking of the payment instrument

The Bank reserves the right to block the customer's payment instrument at any time and without prior notice to the customer or a holder of the customer's right if:

a the customer does not comply with these terms and conditions or other instructions issued by the Bank, or if the Bank has reasonable cause to assume that the customer's payment instrument may be used in contravention of the law or these terms and conditions,

b the customer dies, is declared bankrupt, or if an administrator is appointed for him/her pursuant to the Swedish Children and Parents Code,

c the Bank becomes aware that certain information in the customer's payment instrument is incorrect, or the Bank has reason to assume that this is the case,

d the Bank becomes aware or has reason to suspect that the customer's payment instrument and/or personal code have been disclosed, stolen, copied or used in any other authorised manner, or

e if there is a risk that the payment instrument cannot be used in a secure manner, such as for technical reasons.

If there is any suspicion of ID theft or other misuse of a Bank ID, it may be blocked by a party other than the Bank pursuant to the rules applying for *Bankernas ID-tjänst* (the Swedish bank ID service).

The Bank must cancel the block or replace the payment instrument as soon as there is no reason to let the block remain in place.

After notifying the customer separately, the Bank has the right to block the customer's payment instrument if legislation, decisions by public authorities, regulations, general guidelines or similar circumstances mean that the Bank is not able to fulfil this agreement, despite reasonable efforts.

8. Ownership and copyright

Software and other copyrighted information that is provided by the Bank or its suppliers in conjunction with payment instruments is the property of the Bank or its suppliers.

ID 2019-12-30 09:27:27

A457-1 2.9 2020-01-01

9. Special provisions for BankID and Mobile BankID

a) General information

This section, section 9, contains special provisions for BankID (BankID - card) and Mobile BankID which have been issued by the Bank. BankID and Mobile BankID are hereafter referred to collectively as "BankID". The provisions of this section apply in addition to the other provisions in these terms and conditions.

Information regarding the function of BankID and the information it contains is set out on www.bankid.com.

b) Processing of data, etc.

A BankID contains information on the customer's name, civic registration number, and the bank that issued the BankID.

The customer consents to this data being shown to the party within whose services the customer is using their BankID.

In addition, the customer consents to the Bank:

- registering and compiling the data that the customer has approved when ordering, in a directory that can be kept available for the party that has accepted BankID as an identification document,
- processing the personal data in the Bank's customer and issuer database, within the framework of *Bankernas ID-tjänst* (the Swedish bank ID service),
- using log data to compile information on the use of BankID, and
- disclosing information to any other party in *Bankernas ID-tjänst* (the Swedish bank ID service) which is necessary for them to protect their rights in the event of a claim made upon that party.

c) The customer's obligation to block their BankID

If the customer's BankID contains incorrect information, the customer must immediately block their BankID and inform the Bank of this.

10. Amendments to these terms and conditions

The Bank is entitled to amend these terms and conditions without notice of termination. The new terms and conditions come into force sixty (60) days after the customer has been informed of the amendment. If new legislation or other regulations come into force immediately, and this leads to a change in the conditions for payment instruments, the Bank may apply the new regulations immediately.

11. Notices

a) General information

Notices from the Bank to the customer arising from this agreement, etc. are sent by post to the address registered at the Bank. If the customer has access to Handelsbanken Online Banking, notices can be provided via this service. Notices sent by the Bank to the customer with regard to the customer's payment instrument shall be deemed to have reached the customer no later than on the seventh day after despatch if the notice is sent by registered post to the address that is registered in the Bank's customer database, or is otherwise known to the Bank.

Notices from the Bank that are of a general nature may be published electronically on the Bank's website. Such notices shall be deemed to have been received by the customer no later than 30 days after publication.

The Bank must be immediately informed of any change of name, address, e-mail address or phone number.

b) Notices regarding amendments to terms and conditions

When terms and conditions are changed, a notice to this effect, which is transmitted via an electronic communication service such as Online Banking or Mobile Banking, is deemed to have reached the customer as soon as the notice has been made available and the Bank has notified the customer of this in the form of an electronic message such as an SMS text message or other form of electronic notification.

c) Notification in the case of unauthorised use and security risks

In the event of unauthorised use or security risks, the Bank will notify the customer by telephone, SMS text message, Online Banking, Mobile Banking or via www.handelsbanken.se. In any such contact, the Bank will never request sensitive information or codes related to the customer's payment instrument (such as card details, log-in codes or signature information). If the customer is contacted by the Bank, by phone or SMS text message, the account holder/customer must always check by phoning the Bank at +46 (0)8 701 1000 or another publicly available switchboard number.

12. Limitation of the Bank's liability

The Bank shall not be liable for any damage that may arise as a result of payment instruments containing incorrect information that the customer has affirmed to be correct when the payment instrument was ordered.

The Bank shall not be held liable for any loss resulting from a Swedish or foreign legal enactment, the intervention of a Swedish or foreign public authority, an act of war, a strike, a blockade, a boycott, a lockout or any other similar circumstance. The reservation in respect of strikes, blockades, boycotts and lockouts applies even if the Bank itself is subjected to such measures or takes such measures. Nor shall the Bank be held liable for damage or inconvenience due to operational breakdowns or other disruptions to computer systems or telecommunications used by any party that accepts the payment instrument issued by the Bank.

The Bank is not liable to pay compensation for damage which arises as a result of other causes if the Bank has acted with normal care. The Bank is liable to the consumer for indirect damage only if the damage was caused by gross negligence on the part of the Bank. Otherwise, the Bank shall in no case be liable for indirect damage.

13. Jurisdiction and disputes

The application of the agreement regarding the payment instrument, including these terms and conditions, shall be in accordance with Swedish law.

If action is brought by the Bank, the dispute shall be resolved in a Swedish court of law. The Bank is entitled, however, to pursue a claim outside Sweden if the customer is domiciled there or has assets in that country. The customer may also, in order to find a resolution to the dispute out of court, submit a request for rectification directly to the Bank or report the dispute to be considered by the Swedish National Board for Consumer Complaints (see below under "Resolution of complaints and disputes out of court"). The Bank may respond to the customer's complaint verbally, for example by phone, or in a personal meeting. The Bank may also reply to the customer by letter, in Online Banking, Mobile Banking or as agreed by the customer and the Bank.

ID 2019-12-30 09:27:27

Handelsbanken

Terms and condition
Applying from 1 January 2020

Information

Processing of personal data

Controller, etc.

The Bank is responsible (the controller) for the processing of the personal data that you provide in conjunction with entering into this service, or that is otherwise registered in conjunction with this service.

The information below that relates to you also applies to your guarantor, pledger, representative, trustee, or guardian.

Purpose and legal basis

Performance of contract

The basic purpose of the Bank's processing of personal data in conjunction with this service, and the legal basis for it, is to collect and check the personal data prior to making a decision on providing a service for you, and to fulfil the terms and conditions of our agreement.

Legal obligations

The data is also processed so that the Bank can fulfil its legal obligations or decisions by authorities. An example of such processing is the Bank's processing of personal data to be compliant with the Swedish Accounting Act and the Anti-Money Laundering Act, as well as the reporting requirements of authorities such as the Swedish Tax Agency, the Swedish Police and the Swedish Enforcement Authority.

Basis for analysis and marketing, etc.

The personal data is processed for marketing and customer research, which comprises background material for marketing, methods and business development, and risk management. Risk management also involves processing information about borrowers and credits to assess the quality of credits for capital adequacy purposes. Personal data may also be processed for use as background material for financial advisory services.

Personal data may be used for direct marketing, unless you have requested that this should be blocked.

Insofar as the Bank's actions are not conducted with the aim of fulfilling contractual terms and conditions, or required by law or the authorities, the legal basis for processing is generally that it is a legitimate interest for the Bank pursuant to the prevailing legislation.

How long do we save personal data?

We save personal data as long as it is necessary in order to fulfil our contractual terms and conditions for the service, and otherwise as required by law or decisions by authorities.

Your rights

You are entitled to receive information about the personal data about yourself that is being processed by the Bank, and to request the correction of erroneous or incomplete information.

More information

Comprehensive information about the Bank's processing of personal data and your rights in conjunction with this processing is available at www.handelsbanken.se.

If you have any questions

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

Handelsbanken
Data Protection Officer
SE-106 70 Stockholm, Sweden

You are also always entitled to contact the Bank's Complaints Manager or the Swedish Data Protection Authority with any complaints concerning the processing of personal data.

Resolution of complaints and disputes out of court

Complaints regarding the services in the agreement should primarily be addressed to the customer's branch office. If the customer is not satisfied, the customer may contact the Bank's complaints officer at Handelsbanken, Central Customer Complaints, SE-106 70 Stockholm, Sweden, or by phone +46 8 701 1000. The Bank may respond to the customer's complaint verbally, for example by phone, or in a personal meeting. The Bank may also reply to the customer by letter, in Online Banking, Mobile Banking or as agreed by the customer and the Bank.

The customer may also obtain answers to questions and information on banking services and complaints from the Swedish Consumers' Banking and Finance Bureau (*Konsumenternas Bank- och Finansbyrå*), the Swedish Consumers' Insurance Bureau (*Konsumenternas Försäkringsbyrå*) or, where applicable, the consumer affairs service in the customer's municipality.

As regards disputes with the Bank, the customer has the option of contacting the Swedish National Board for Consumer Disputes (ARN), which is a board for alternative resolution of disputes. Address: ARN, Box 174, SE-101 23 Stockholm, www.arn.se. A submission to the Board must be made in writing. Certain value and time limits must be met for the Board to try the case. The Bank undertakes to participate in ARN's processing of the dispute.

A customer who has entered into an agreement via Handelsbanken Online Banking or Mobile banking, and where a dispute has arisen, is entitled to use the EU online platform for resolution of disputes: https://ec.europa.eu/consumers/odr. Even if the customer uses the online platform regarding complaints/disputes with the Bank, the case will be sent to ARN for a decision. More information about online dispute resolution can be found at www.konsumenternas.se

A457-1 2.9 2020-01-01