Terms and conditions for Access agreement – Danske Mobile Banking – consumers

Applicable from 26 November 2024

Danske Mobile Banking – consumers (hereinafter 'Mobile Banking') is Danske Bank's digital banking solution for mobile devices such as smartphones and tablets.

To be able to use Mobile Banking, you must have an agreement on Danske eBanking – consumers (hereinafter 'eBanking').

The Terms and conditions for Access agreement – Danske eBanking – consumers apply to the extent that these terms and conditions do not stipulate otherwise.

1 Features of Mobile Banking

Depending on the mobile device and system you use, Mobile Banking allows you to

- view balances in all your present and future accounts and custody accounts that you have been or will be given a mandate to operate
- operate all your present and future accounts and custody accounts as well as accounts that you have been or will be given a mandate to operate
- view information about share and bond prices and exchange rates
- transfer funds to third-party accounts with Danske Bank or other banks in Denmark
- pay electronic payment forms
- view information about your accounts with other banks
- receive an account summary
- receive a custody account summary
- sign certain agreements with Danske Bank using your digital signature
- send and receive messages and include attachments

Note that specific amount limits apply to transfers, securities trades and electronic payment forms. The limits are available in eBanking and Mobile Banking.

1.1 Possibility of using apps linked to Mobile Banking

When you have Mobile Banking, you can link and use apps that we offer for Mobile Banking.

If you download an app requiring Mobile Banking, your use is subject to the same terms and conditions as those applying to Mobile Banking, and the security solution is the same.

When you download such an app, you also accept that these Terms and conditions for Access agreement – Danske Mobile Banking – consumers apply in full to the app in question.

2 Access and use

2.1 Use of Mobile Banking

The stipulations below apply to you if you are currently using the existing security solution with a service code. The security solution in Mobile Banking will automatically be updated, but in the period until the update, the sections below apply to you.

You can use Mobile Banking if you have a mobile device with internet access. You register in eBanking under the Mobile services menu item. You then get an access code (service code) for Mobile Banking.

The app is available in App Store and Google Play – search for the 'Mobilbank DK – Danske Bank' app.

To use Mobile Banking, you need a security solution that consists of
1. a mobile device
2. a service code, which you will find in eBanking under the Mobile services menu item
3. your MitID

The first time you log on, you need your MitID and you link your mobile device to Mobile Banking. Once you have done this, you need only your service code for future logons.

Some types of transactions and the signing of some types of agreement require both a service code and your MitID.

If your mobile device allows this, you can use your fingerprint (Touch ID) or facial recognition (Face ID) instead of the service code to log on, for example. All you need to do is activate the feature in Mobile Banking. You can do so under Settings. Choose Log on using fingerprint (Touch ID) or facial recognition (Face ID).

Remember that all fingerprints and facial recognition registered for your mobile device can then be used to log on to Mobile Banking.

The stipulations below apply to you if you use the updated security solution with the option of a 6-digit PIN.

You can use Mobile Banking if you have a smartphone or a tablet (mobile device) with internet access.

The app is available in App Store and Google Play – search for the 'Mobilbank DK – Danske Bank' app.

To use Mobile Banking, you need a security solution that consists of
1. a mobile device
2. a PIN that you create when you log on for the first time
3. your MitID

The first time you log on, you need your MitID. In connection with the first logon, you have the option of creating a PIN to be used for future logons.

The PIN can also be used to authenticate transfers and other actions in Mobile Banking.

If you want to transfer funds to someone other than yourself, sign agreements or the like, additional security is required, and you need to use your MitID for authentication.

If your mobile device supports it, you can also choose to use your fingerprint (Touch ID) or facial recognition (Face ID) instead of the PIN. You activate this feature via 'Settings'. Choose Log on using fingerprint (Touch ID) or facial recognition (Face ID).

Remember that all fingerprints/facial recognition registered for your device can be used to log on to Mobile Banking.

2.2 Duty to protect your authenticators

The rules applicable to MitID, including your MitID password, code display, audio code reader, chip and app, are available at www.MitID.dk.

Generally, your authenticators may be used only by you. Therefore, you must not

- disclose your service code or PIN and password and/or codes to anyone else, including members of your household
- write down the service code or PIN or password and keep it with your other authenticators
- write down the service code or PIN or password on your other authenticators

If you suspect that somebody may know your service code or PIN, you must contact us immediately (see clause 16.3, Blocking and notification in case of irregularities and unauthorised use).

If you become aware that somebody knows your MitID, you must contact us or MitID immediately (see the 'Terms and conditions for MitID' document at www.MitID.dk).

You must also take care to store your mobile device so as to prevent others from gaining unimpeded access to it. Always use a code to lock your mobile device, for example a keypad or biometric lock (fingerprint or facial recognition).

Even though you use a biometric lock or password to open your mobile device, you will still be liable under these terms.

3 Accounts and custody accounts

3.1 Access to accounts and custody accounts with Danske Bank

Mobile Banking allows you to view balances in all your present and future accounts and custody accounts as well as accounts and custody accounts that you have been or will be given authorisation to view (read more below). In addition, you can operate all your present and future accounts and custody accounts.

To operate accounts of other Danske Bank customers via Mobile Banking, you must have a separate account mandate for each account.

To operate custody accounts of other Danske Bank customers, you must have a separate account mandate for each custody account.

The operation of accounts and custody accounts is governed by the terms applying to the individual accounts and custody accounts.

When you initiate an account transfer, you are asked to enter the registration number and account number of the payee's account. If applicable, you should also enter the date of the transfer. For more details, see the help section in Mobile Banking.

We are not obliged to execute orders for which cover is insufficient or which cannot be executed because of incomplete information.

Similarly, we are not obliged to execute orders if you or your mandator dies. We are also not obliged to execute orders if you or your mandator is subject to bankruptcy, reconstruction or other insolvency proceedings; or opens negotiations for a rescheduling of debt, debt relief or a composition with creditors, including a request for a voluntary composition with Danske Bank or any other creditor.

You must enter data for funds transfers and securities trades under the appropriate functions in Mobile Banking. We execute orders only if they are submitted under the appropriate functions in Mobile Banking.

When you have entered a payment or order, you approve it using an authenticator (see clause 2.1). The order is then binding. The time of approval is also the transmission time.

When we have received your order, you receive confirmation of execution, provided that you are still logged on.

3.2 Cut-off times, booking date and value date

A number of cut-off times apply to the receipt of your orders if we are to execute them on time. You can find information about cut-off times, booking dates and value dates in eBanking under the About Danske eBanking menu item.

3.3 Securities trading

Securities trades with us are subject to our Terms and conditions for trading in financial instruments. Mobile Banking offers trading in Danish and foreign securities.

The Mobile Banking solution does not, however, offer the same features as eBanking. For example, the help texts and warnings are not the same.

We consider a trading order binding when you have submitted the order to us using an authenticator (see clause 2.1). When a securities trade has been executed, you receive confirmation on your mobile device, provided that you are still logged on. If you do not receive confirmation, you can contact us to find out whether the order has been executed.

3.3.1 Execution only – no advisory services

Mobile Banking does not offer advisory services, only execution of orders. For securities such as shares, bonds and certificates of mutual funds/UCITS funds, the trades are executed as execution-only trades.

This means that we do not check whether you have any knowledge of and experience with the specific type of security, and thus, we do not assess whether the security in question is an appropriate investment for you.

3.4 Amount limits

Limits apply to the total daily amount of payments and cash transfers.

In addition, a special limit applies to the total amount you can transfer on a daily basis to third-party accounts, including payment of electronic payment forms.

Information about applicable limits is available in Mobile Banking, eBanking or from one of our advisory centres.

3.5 Account mandates

If you want another person to be authorised to view information about and/or operate your accounts and/or view information about your custody accounts through Mobile Banking, you must issue an account mandate to that person. The mandate holder can then operate your accounts through their own access to Mobile Banking. When you no longer want a mandate to be in force, you must revoke it in writing.

3.6. Your accounts with other banks

Mobile Banking can give you a complete overview of your payment accounts with other banks in Denmark. All you need to do is to give your consent to our retrieving information about your payment accounts.

You can also transfer funds from your payment accounts with other banks via Mobile Banking. When you do so, you approve and execute the transfer using the security solution of the account servicing bank.

Once you have approved a transfer via the account servicing bank, you cannot cancel it.

If you are not sure whether a transfer has been executed, you can check it by updating the account entries for the relevant account in Mobile Banking. You can also check the account using the other bank's mobile banking solution.

Please note that the information about your payment accounts with other banks is only a snapshot of the accounts. As we retrieve the account information from other banks, we cannot guarantee the accuracy of the information retrieved.

We do not assume any responsibility or liability for decisions and transactions that you make on the basis of the information. Similarly, Danske Bank cannot be held liable if the feature is temporarily unavailable or not fully functional.

4 Access to multiple Mobile Banking agreements

If you are a user under multiple Mobile Banking agreements (such as Danske Mobile Banking Business and Danske Mobile Banking – consumers), you can log on and operate accounts under all of them using your personal security solution.

Every time you log on to Mobile Banking, you must choose which agreement to access. You can also choose a default agreement for direct access every time you log on. You can switch to another agreement without having to log on again.

When you use your security solution to operate accounts under other Mobile Banking agreements to which you have access, you are bound by the terms applying to the agreements in question, including the terms on liability in the event of unauthorised use by a third party. The terms on liability may thus differ for the individual Mobile Banking agreements.

5 Checking of account entries

When a transaction has been executed, it appears on the list of account entries in Mobile Banking (and eBanking).

Each month, you can see the amount of fees paid over the past month. In addition, you regularly receive account and custody account statements either in eBanking or e- Boks or by letter.

When you check accounts and entries, you should note that there may be transactions that have not yet been finally registered in your account or custody account.

You are obliged to check entries in your accounts and custody accounts regularly. If you come across transactions that you do not believe you have made, you must contact us as soon as possible – with due consideration to the time limits listed in clause 7.

6 Revocation of approved payments/orders

You cannot revoke orders for transfers or securities trades through Mobile Banking. If you want to revoke an order, you must do so either in eBanking or by contacting us.

7 Unauthorised payments/orders

If you believe that one or more payments/orders have been executed without your authorisation, you must contact us as soon as possible. When we assess whether you have contacted us in due time, we attach importance to your duty

to regularly check entries in your account and custody account (see clause 5).

We must always receive your objection within 13 months of the individual amount having been debited to your account.

7.1 Processing of objections against unauthorised payments

When you have contacted us, we examine your objection. While we do so, the amount in question will normally be deposited in your account.

If your objection is subsequently found to be unjustified, we will withdraw the amount from the account. If our investigation shows that another person has used your access to Mobile Banking fraudulently, you are liable according to the terms of clause 8, Liability for unauthorised use.

If we find your objection unjustified, we are entitled to charge interest from the date the amount was credited to your account to the date it was withdrawn. We may also charge a fee for producing copies of relevant advices (see the list of charges).

8 Liability for unauthorised use

You are liable for losses up to DKK 375 if your access to Mobile Banking has been subject to unauthorised use.

You are liable for losses up to DKK 8,000 if we can prove that your authenticators were used and you did not contact us to block your agreement as soon as possible after you discovered that you had lost one or more of your authenticators or that another person had obtained your service code, PIN or codes.

The same applies if you informed the unauthorised user of your service code, PIN or one or more of your codes but are not fully liable for the loss under Danish law, or if, through gross negligence, you made unauthorised use possible.

You are liable for the full loss if your authenticators were used and we can prove that you disclosed your service code, PIN or one or more of your codes to the unauthorised user and that you realised, or ought to have realised, that there was a risk of unauthorised use.

You are also liable for the full loss if you have committed fraud or have deliberately omitted to protect your security solution (see clause 2.2) or block the agreement (see clause 16.3).

You are not liable for losses arising after we have been asked to block your agreement. At the end of this document, you can read sections 97, 98 and 100 of the Danish Act on Payments.

9 Danske Bank's liability

The rules concerning Danske Bank's liability are set out in clause 5 of the Terms and conditions for agreement on digital signature – consumers and in General conditions – consumers.

10 Your use of information in Mobile Banking

The services you receive through Mobile Banking, including price information, are for your use exclusively. You are not allowed to pass them on to others, with or without payment, unless we have authorised your doing so in writing.

11 Changes to terms and conditions and system features

We may change these terms and conditions and adjust the features of Mobile Banking without prior notice if the changes are not to your disadvantage. Notice of changes that are to your disadvantage must be given two months in advance of the changes taking effect.

We notify you of changes by message in Mobile Banking or eBanking, or by email or letter (see also clause 13 of Danske Bank's General conditions – consumers about communications).

When we change the terms and conditions, you must inform us – before the changes take effect – if you do not want to be bound by the new terms and conditions. If we do not hear from you, you will be bound by the new terms and conditions.

If you inform us that you do not want to be bound by the new conditions, the agreement will be terminated when the new conditions take effect.

We continually develop and adjust our digital services, and additional services may be offered in the future.

In some cases, new digital services require a separate agreement. You will be informed accordingly.

12 Termination

You may terminate your Mobile Banking agreement without notice at any time by giving us written notification by letter or through eBanking.

We may terminate the agreement at two months' written notice. If you fail to fulfil your obligations under the agreement, we will be entitled to terminate it without notice, however.

Orders and agreements entered into prior to termination will be executed (see, however, clause 3.1).

If your eBanking agreement is terminated, your Mobile Banking agreement will also be terminated.

13 Costs associated with access and use

An updated list of charges for Mobile Banking services is available in eBanking.

Transaction fees are charged to the accounts used for the transactions.

We may charge a fee for help to recover funds transferred to an account by mistake because you stated a wrong identification code.

Your telephone service provider can provide information about telephone subscriptions and call charges.

14 Use, storage and disclosure of personal data and information about purchases etc.

When you use Mobile Banking, we register account numbers, amounts and transaction dates as well as any messages.

When you transfer funds, we send information about amounts and transaction dates as well as any messages from you to the payee. Data are transmitted through the payee's bank and its data and settlement centre.

The information is stored with the payee's bank and Danske Bank. The information is used by the banks for bookkeeping purposes, account statements and subsequent correction of errors, if any.

The information is disclosed to others only if so required by Danish law or if it is needed for legal actions arising out of the use of the system.

We keep your personal data only for as long as it is needed for the specified purposes for which your personal data was registered and used or as required by law for the purpose. More information is available in our privacy notice.

When you send messages to us, we register the contents of the message and any attached documents. We use the information for advisory purposes and for our agreement with you.

The information is processed in accordance with our privacy notice.

If you use a service on your mobile device to read text aloud (such as VoiceOver on iPhones or Talk Back on Android phones), your personal data may be processed by the provider of that service.

Danske Bank does not have any control over such processing. If you would like to know how the provider processes your data, please refer to the terms and conditions on the protection of personal data of the provider.

15 New copies of these terms and conditions

Should you lose these terms and conditions or need an additional copy for other reasons, you can find them at www.danskebank.dk/terms-and-conditions. You are also welcome to contact us.

16 Customer service

16.1 Customer service

If you need support, please call on +45 70 12 34 56. You can see our opening hours at https://danskebank.dk/contact.

You can find answers to the most frequently asked questions concerning Mobile Banking and eBanking at www.danskebank.dk/help.

16.2 Mobile Banking business hours

Mobile Banking is open 24 hours a day, 365 days a year.

16.3 Blocking and notification in case of irregularities and unauthorised use

You must inform us immediately if you discover or suspect irregularities or unauthorised use of your Mobile Banking app.

You can block access to your Mobile Banking app by calling us on +45 70 12 34 56. We are open 24 hours a day.

You can also block your access to Mobile Banking by blocking your service code or PIN.

We reserve the right to block your access to Mobile Banking without notice if we discover or suspect irregularities or unauthorised use of the app.

We also reserve the right to block your access to Mobile Banking without notice if we believe that external factors threaten the security of the system.

16.4 Danske Bank's notification of unauthorised use and security threats

We contact you if we suspect or discover unauthorised use. We also contact you if we become aware of any potential security threats.

We contact you in a safe way, for example by sending a message in eBanking, Danske Netpost or e-Boks, or by email or telephone.

Excerpts from the Danish Act on Payments

Liability rules

97. Objections to unauthorised or incorrectly executed payment transactions must be received by the provider as soon as possible and not later than 13 months after the debit date of the relevant payment transaction. The deadline is calculated from the time at which the provider has communicated this information or made it available, if it has not been communicated in advance.

(2) Objections against unauthorised or erroneous payment transactions initiated via a provider of payment initiation services must be addressed to the account-holding provider in accordance with subsection (1), see, however, section 99(2) and (3) and section 104 and 104 a.

98. If a payer denies having authorised or initiated a payment transaction, the provider of the payment service must prove that the payment transaction was correctly registered and booked and not affected by technical failure or other errors, see, however, subsection (3). In connection with the use of a payment instrument, the provider furthermore has to prove that the payment instrument's personalised security feature was used in connection with the payment transaction.

(2) If a payer denies having authorised or initiated a payment transaction, the recorded use of a payment instrument is not in itself proof that the payer authorised the transaction, that the payer acted fraudulently or failed to fulfil his obligations.

(3) If a payer denies having authorised or initiated a payment transaction which was initiated via a provider of payment initiation services, the provider of the payment initiation service must prove that the payment transaction was correctly registered and booked and not affected by technical failure or other errors.

100. The payer's provider of payment services is liable to the payer for any loss incurred due to the unauthorised use by a third party of a payment service unless otherwise provided in subsections (2) to (5) hereof. The payer is only liable under subsections (3) to (5) hereof if the transaction was accurately recorded and entered in the accounts, see, however, subsection (2).

(2) However, the payer is liable without limitation with respect to any loss incurred due to the payer acting fraudulently or wilfully failing to fulfil his obligations under section 93.

(3) Except where subsection (4) or (5) hereof provides for more extensive liability, the payer is liable for an amount up to DKK 375 for any loss incurred due to the unauthorised use by a third party of the payment service where the personalised security feature linked to the payment service has been used.

(4) Except where subsection (5) provides for more extensive liability, the payer is liable for an amount up to DKK 8,000.00 for any loss incurred as a result of the unauthorised use by a third party of the payment instrument if the payer's provider is able to establish that the personalised security feature linked to the payment instrument was used; and

1) that the payer failed to notify the payer's provider as soon as possible after having become aware that the payment service's payment instrument was missing or that the personalised security feature linked to the payment instrument had come to the knowledge of an unauthorised user;

2) that the payer intentionally made the personalised security feature of the payment instrument available to the person making such unauthorised use without this falling within the scope of subsection (5); or

3) that, through grossly inappropriate conduct, the payer made such unauthorised use possible.

(5) The payer is liable without limitation with respect to any loss incurred due to the unauthorised use by a third party of the payment service where the personalised security feature linked to the payment instrument was used and the payer's provider proves that the payer disclosed the personalised security feature to the person making the unauthorised use, and that the circumstances were such that the payer knew or ought to have known that there was a risk of abuse.

(6) Notwithstanding the provisions of subsections (3) to (5) hereof, the payer's provider is liable for any unauthorised use;

1) after the provider was notified that the payment instrument linked to the payment service had been lost, that the personalised security feature had come to the knowledge of an unauthorised person, or that the payer required the payment instrument to be blocked for any other reason;

2) when it is caused by actions taken by a service provider's employees, agents or branch or an entity to whom the service provider's activities have been outsourced, or their passivity; or

3) because the provider has not taken appropriate measures, see section 94(1)(2).

(7) Notwithstanding subsections (3) to (5) hereof, the payer's provider is also liable, unless the payer has acted fraudulently. The payment recipient or his/her provider must compensate the loss suffered by the payer's provider if the payee or its service provider has failed to use strong customer authentication. Subsections (1) and (2) do not apply to the services comprised by section 1(5) and section 5(14)-(16).

(8) Notwithstanding the provisions of subsections (3) to (5) hereof, the payer's provider is also liable if the loss, theft or unauthorised acquisition of the payment instrument linked to the payment service or the personalised security feature linked to the payment service could not be detected by the payer prior to the unauthorised use.

(9) Moreover, notwithstanding the provisions of subsections (3) to (5) hereof, the payer's provider is liable if the payee knew or ought to have known that the use of the payment service was unauthorised.

(10) The provisions of subsections (1) to (9) hereof also apply to electronic money except where the payer's provider of electronic money is unable to block the payment account or the payment instrument.