Terms and conditions for Agreement on Danske Mobile Banking 15-17

Applicable from 17 April 2023

Danske Mobile Banking 15-17 is Danske Bank's digital banking solution for personal customers aged 15-17 for mobile devices such as mobile phones. To be able to use Danske Mobile Banking 15-17, you must have a Danske eBanking 15-17 agreement.

The Terms and conditions for Access agreement - Danske eBanking 15-17 apply to Danske Mobile Banking 15-17 to the extent that the terms and conditions of this agreement do not state otherwise.

1 What can you use Danske Mobile Banking 15-17 for?

Danske Mobile Banking 15-17 offers virtually the same features as Danske eBanking 15-17. Depending on your mobile device and the system you use, Danske Mobile Banking 15-17 allows you to

- view information about Danske Ung and Ung Opsparing accounts and information about executed and future transactions
- transfer funds to and from Danske Ung and Ung Opsparing accounts
- transfer funds to other accounts you may have with Danske Bank, to accounts held by others with Danske Bank and to accounts with other banks in Denmark
- pay payment forms (bills)
- send and receive messages, including attachments, to/from Danske Bank

2 How to get and use Danske Mobile Banking 15-17

2.1 Use of Danske Mobile Banking 15-17

You can use Danske Mobile Banking 15-17 if you have a mobile phone (or a tablet). The app is available in App Store and Google Play.

To use Danske Mobile Banking, you need a security solution that consists of

1. a mobile device (mobile phone or tablet)
2. a service code, which you find in Danske 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 phone to Danske Mobile Banking. Once you have done this, you need only your service code for future logons.

If your mobile phone allows this, you can use your fingerprint (Touch ID) or Face ID instead of the service code to log on. Activate the feature under Settings – choose Log on using Touch ID/Face ID. Remember that all fingerprints registered for your mobile phone can then be used to log on to Danske 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. Do not disclose your service code and password and/or codes to anyone else, including members of your household, do not write down the service code or password and keep it with your other authenticators, and do not write down the service code on your other authenticators.

If you suspect that somebody may know your service code, you must contact us immediately (see clause 14.3 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.

Even though you use a lock for your mobile phone, either to open it or as a substitute for your service code, you will still be liable under these terms and conditions.

3 Accounts

3.1 Access to accounts

Danske Mobile Banking 15-17 enables you to view balances in and operate Danske Ung and Ung Opsparing accounts (see clause 1).

The operation of your accounts is governed by the terms applicable to the individual account.

When transferring funds to another account, you are asked to enter the registration number and account number of the payee's account and, where relevant, the date of the transfer. If there are insufficient funds in the account or the payment cannot be made due to insufficient information, we are not under any obligation to execute the transaction.

You must enter data for funds transfers under the appropriate functions in the system. We will execute transactions only if they have been issued under the functions in your Danske Mobile Banking intended for that purpose.

When you have entered an order into Danske Mobile Banking, you approve the payment using an authenticator (typically your service code (see clause 2.1)). The time of approval is also the transmission time. When we have received your order, you receive a confirmation of execution of the payment.

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 Danske eBanking 15-17 under the Pay and transfer menu item.

3.3 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 Danske eBanking 15-17 under the Pay and transfer menu item. Your branch can also inform you about amount limits.

4 Checking of account entries

When you have transferred or received funds, the amounts will appear in the list of account entries in Danske Mobile Banking. They will also appear in the list of account entries in Danske eBanking, where you can see all transactions executed during a period of up to 13 months.

Each month, you can see the amount of fees paid over the past month. In addition, you regularly receive account statements as prescribed by the terms and conditions governing the individual accounts.

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

You are under an obligation to check your accounts on an ongoing basis to see if there are any deposits or payments that you do not believe you have made. If this is the case, you must contact us immediately.

If, by mistake, a withdrawal has been made from your account and you cannot accept it, we will of course credit the amount to your account. If it turns out later that the withdrawal was not a mistake, we debit the amount again and notify you accordingly.

If another person (a third party) has made unauthorised use of your Danske Mobile Banking service, your liability will be determined as stated under clause 6 Liability on unauthorised use of Danske Mobile Banking 15-17.

If it turns out that another person has not made unauthorised use of Danske Mobile Banking, or that it is not

due to a mistake on our part, we may charge interest from the time when the amount was credited to your account until we debit it again. You may have to pay a fee for ordering copies of relevant advices.

5 Revocation of approved payments/orders

You may revoke orders for account transfers and payment of payment forms via Danske Mobile Banking until the last business day prior to the business day on which the payment or transfer is to be made.

You cannot revoke an order in Danske Mobile Banking. You must do it in Danske eBanking or by contacting us.

6 Your liability on unauthorised use of Danske Mobile Banking 15-17

Clause 2.2 provides additional information about your duty to protect your security solution and to safely store your code card/token and service code.

In case of unauthorised use of your Danske Mobile Banking service, your liability will be determined according to the rules of the Danish Guardianship Act (Værgemålsloven), the rules on minors' and legally incompetent persons' liability and the Danish Act on Payments (Lov om betalinger). You are not liable for losses up to DKK 375 under the liability rule in section 100(2) of the Danish Act on Payments.

You are, however, liable for losses up to DKK 8,000 if we can prove that you have made unauthorised use possible through gross negligence.

You are liable for the full loss if we can prove that you disclosed your password or other codes to the unauthorised user or used another authenticator on behalf of 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 meet your obligations under the terms and conditions applying to Danske Mobile Banking.

You are not liable for losses arising after we have been asked to block your Danske Mobile Banking agreement.

We may contact your guardian in case of questions about liability or the like, for example in connection with your use of Danske Mobile Banking 15-17.

At the end of this document, you can read sections 97, 98 and 100 of the Danish Act on Payments and an excerpt from the Danish Guardianship Act.

7 Danske Bank's liability

Unless otherwise stipulated in clause 6, Danske Bank is liable for losses resulting from unauthorised use of Danske Mobile Banking when you use your security solution.

According to Danske Bank's General conditions – consumers (which also apply to your Danske Mobile Banking 15-17 agreement), Danske Bank cannot be held liable in certain extraordinary situations, unless Danske Bank ought to have foreseen, avoided or overcome the cause of the loss or if, under Danish law, Danske Bank is liable for the cause of the loss under any circumstances.

8 Your use of information in Danske Mobile Banking 15-17

Danske Mobile Banking 15-17 is for your use exclusively. This means that you are not allowed to disclose information from it to others, whether against payment or not, unless we have consented to such disclosure in writing.

9 Changes to terms and conditions and system features

We may change these terms and conditions and adjust the features of Danske Mobile Banking without prior notice if the changes are to your advantage. Changes to your disadvantage are subject to two months' notice. We notify you of any changes either by letter or digitally, for example by email or a digital message in Danske eBanking or Danske Netpost.

Under Danish legislation, when we change the terms and conditions of an agreement, our customers must be able to terminate their agreement with us free of charge before the changes take effect. Accordingly, 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 terminate when the new terms and conditions take effect.

We continually develop new digital services, which, in some cases, require a separate agreement. You will be informed accordingly.

10 Termination

You may terminate your Danske Mobile Banking 15-17 agreement without notice at any time by giving us written notification by letter or through Danske 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.

If your Danske eBanking 15-17 agreement is terminated with or without notice, Danske Mobile Banking 15-17 will no longer be available to you.

11 List of charges for access to and use of Danske Mobile Banking 15-17

An updated list of charges for Danske Mobile Banking 15-17 services is available in Danske 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 data traffic charges.

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

When you use Danske Mobile Banking 15-17, we register your account number and that of the payee, if any, the amount and date of the payment or transfer.

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.

The information is kept on file in the year of registration and for the following five years.

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

If you use VoiceOver on your mobile phone (a service to read text aloud), your personal data may be handled by a third party (the provider of that service). Danske Bank has no control over such processing.

Danske Bank processes all data in accordance with our privacy notice.

If you would like to know how the VoiceOver service provider processes your data, please refer to the provider's terms and conditions for the protection of personal data.

If you use a service on your mobile phone to read text aloud (such as VoiceOver on iPhones or the Talk Back function on Android phones), your personal data may be processed by the provider of that service. Danske Bank has no control over such processing. If you would like to know how the service provider processes your data, please refer to the provider's terms and conditions for the protection of personal data.

13 New copies of these terms and conditions

You can get a new copy of these terms and conditions at http://www.danskebank.dk/terms-and-conditions. You are also welcome to contact your branch.

14 Customer Service, business hours, and blocking

14.1Customer Service

If you need support, please call on +45 70 123 456. 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.

14.2 Danske Mobile Banking business hours

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

14.3 Blocking and notification incase of irregularities and unauthorised use

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

You can block access to your Danske Mobile Banking service by calling us on +45 70 123 456. We are open 24 hours a day.

When you have spoken with us, we send you written confirmation of the blocking, specifying the time when your request for blocking was made. The blocking also applies to your access to Danske eBanking.

If you block your service code, you also block your access to Danske Mobile Banking 15-17.

We reserve the right to block your access to Danske Mobile Banking 15-17 without notice if we discover or suspect irregularities or unauthorised use of the agreement.

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

You must call us on +45 70 123 456 to cancel the blocking.

14.4 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 secure way, for example by sending a notice in Danske 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.

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.

Excerpts from the Danish Guardianship Act

1.-(1) Children and young people under the age of 18 who have not married are minors and therefore legally incompetent.

(2) Minors cannot commit themselves in legal transactions or dispose of their assets unless otherwise stipulated.

(3)Unless otherwise stipulated, the guardians act on behalf of the minor in financial affairs.

42.-(1) Legally incompetent persons may dispose of the following assets: 1) assets acquired through own work after they have attained the age of 15 or have been deprived of their legal capacity; 2) assets given to them as a gift for their sole use and benefit or as an optional inheritance; and 3) assets that the guardian may have left to them pursuant to section 25(3).

(2) Legally incompetent persons' right to dispose of assets also covers income from the acquired assets and anything that replaces them.

It does not entail a right to assume debt obligations.