Special Terms and Conditions Online Banking

Effective from September 28th 2020

These General Terms and Conditions and any Special Terms and Conditions which apply to You, supersede any previous versions of the Terms and Conditions.

Danske Bank

Contents

Introduction

The General Terms and Conditions – Corporates & Institutions (the **"General Terms and Conditions"**) and these Special Terms and Conditions apply to the Online Banking Channel.

Unless otherwise stated, where there is any inconsistency between these Special Terms and Conditions and the General Terms and Conditions in relation to the Online Banking Channel, these Special Terms and Conditions will prevail.

The Online Banking Channel is a multichannel platform with a full customer interface, which aims to combine all Danske Bank services with selected third-party services to create a complete and user-friendly digital ecosystem of linked financial services. The Online Banking Channel can provides access to account information, payments and many other banking services requested by your company.

These Special Terms and Conditions are divided into the following parts:

Part 1 – describes the options available in our Online Banking Channel and how to use the system

Part 2 – describes third party access rights

Part 3 – describes the security requirements for use of the Online Banking Channel

Part 4 – describes the contractual aspects associated with the use of the Online Banking Channel

Part 5 – contains a list of defined terms

In these Special Terms and Conditions:

where the Customer comprises more than one person, these Special Terms and Conditions will apply to such persons jointly and severally so that all such persons are liable together and also individually for their obligations to us; and **"you"** shall mean "you" the Customer and/or "you" the User as the context shall require.

Part 1 – Online Banking Channel – General Description

1. Modules and services

The Online Banking Channel comprises separate Modules and services. Your Access Agreement will specify the Modules you have selected. Certain Modules are categorised as mandatory.

When you select certain Modules, we may require you to enter into a separate *Module Description* form. Where this applies, the Access Agreement will refer to the *Module Description* form. By way of example a separate *Module Description* form will be required where you select the *SEPA Direct Debit Collection Service IRL Module*. Please see section 9 below for further information on the selection of Modules.

Our Business Mobile Banking App allows you to avail of certain services and carry out certain activities, as further set out in section 13, below. By using a Device to access the Business Mobile Banking App, you will only have access to a reduced range of Online Banking Channel services.

2. Logging On to the Online Banking Channel

A User will be required to insert all 3 component parts of their Digital Signature when using the Online Banking Channel. The requirement to enter all 3 component parts of your Digital Signature may be reduced to 2 component parts when logging on to the Business Mobile Banking App if the User selects the *"Remember User on this Device"* function.

A User who allows an Online Banking Channel to sit idle for a period of 5 minutes may be prompted to reinsert certain elements of their Digital Signature in order to continue using the Online Banking Channel.

3. Transactions

The Online Banking Channel allows you to make payments, collect payments and query balances and transactions on Registered Accounts.

Use of your Digital Signature is required to authorise and consent to payments through the Online Banking Channel. When making a payment via the Online Banking Channel you may be prompted to re-enter one or more of the component parts of your Digital Signature. For further information on payment authorisations and mandates please see sections 12 and 13, below.

Use of the Digital Signature shall be your authorisation of, and consent to, all services and activities available via the Online Banking Channel.

4. Registered Accounts

Accounts must be registered in the Online Banking Channel before you can carry out Transactions.

4.1 Registered Accounts in the Danske Bank Group

The following accounts can be registered in the Online Banking Channel:

- Accounts held by you and opened in your name with the Bank and affiliates and divisions of the Danske Bank Group, and
- Accounts held by third parties, including subsidiaries, provided that the third party or subsidiary has issued a third-party mandate

to you authorising you to act on behalf of the third party or subsidiary.

Registered Accounts in the Danske Bank Group can also be managed via SWIFT MT101 or MT940/942 (see the description in section 4.2).

4.2 Registered Accounts managed via SWIFT
Accounts opened with banks outside the Danske Bank Group, and accounts within the Danske Bank Group which you wish to use for Transactions via SWIFT MT101 or SWIFT MT940, can also be registered in the Online Banking Channel via an Access Agreement. You may register both your own accounts and third-party accounts. You or the third party must conclude an agreement with the account-holding bank concerning payment requests via SWIFT MT101 or an agreement on balance reporting via SWIFT MT940.

5. Unregistered accounts

If accounts held by you and/or a third party are not registered in our Online Banking Channel, it is only possible to make payments into those accounts. It is not possible to enquire about or make payments from accounts not registered in the Online Banking Channel.

6. Foreign Drafts

You may make payments by issuing a draft drawn on a Registered Account. If you and/or a third party has an agreement concerning payment requests via SWIFT MT101, drafts can also be drawn on Registered Accounts outside the Danske Bank Group, provided that this option is included in the agreement between you and/or third party and the bank outside the Danske Bank Group. Issued drafts are regarded as banker's drafts, and the amounts are debited from the accounts on the date of issue. You may have the proceeds of uncashed drafts deposited in Registered Accounts. If the proceeds from uncashed drafts are to be credited to your or a third-party's account, you or the third party must covenant to indemnify the Bank if a draft is subsequently presented.

7. Electronic Request

When you or your Users request an order or Transaction to be executed in the Online Banking Channel, such as a payment, this is called an Electronic Request. An order or Transaction is executed when one or two Users with the right mandate type (see section 12) have digitally signed the order. When a User submits an Electronic Request and the order has been executed, we send an electronic receipt. The moment we have confirmed receipt of the Electronic Request, the risk in relation to it being carried out in accordance with the instruction passes to us.

If a payment is authorised on your behalf but provides an incorrect unique identifier to us to identify the payee, we will not be liable if we process the payment in accordance with that unique identifier, but we will make reasonable efforts to recover the funds involved. You agree that we may charge you for this.

We retain Electronic Requests for seven years. During this period, you and / or the third party whose account is debited may obtain a hardcopy of the request against payment of such fee as may be charged by us for administrative assistance (separate rules will apply where the information is requested by a Data Subject and is Personal Data – see our Data Privacy Notice on our website).

Details of our current fees and charges can be found in our Corporates & Institutions – Fees & Charges brochure, also available on our website.

7.1 Refusing orders
If we refuse to execute a payment authorised on your behalf via our Online Banking Channel, we shall notify you of this refusal as soon as possible via the Online Banking Channel, by telephone, in writing, by email, by fax or such other reasonable means as we may select.

7.2 Orders binding on you
Orders executed in accordance with the information in the Electronic Request are binding on you. The Bank therefore cannot reverse payments, foreign currency transactions or trades in financial instruments or other transactions, including issued cheques, which have been finalised in accordance with an Electronic Request.

8. Automatic registration for receipt of documents in eArchive

When you enter into an Agreement, you are automatically registered for receipt of electronic documents. The documents are filed in your eArchive. You receive the documents in electronic form with the same legal effect as ordinary mail in hardcopy. Third-party accounts linked to your Agreement are treated as your own accounts.

8.1 Documents received in electronic form
You receive all documents sent electronically by the Bank in eArchive. In special cases, we may send such documents in hardcopy by ordinary mail.

If you are a customer of one or more of the Danske Bank Group's other branches or entities, and you receive documents electronically from these, you also receive those documents in eArchive.

Account statements, lists of payments made and received and various other statements are examples of documents received in electronic form. We regularly add document types and increase the number of documents that you receive electronically in eArchive.

Each time a new type of document becomes electronically available, you will receive a message via the Online Banking Channel, and not by post.

8.2 Access to documents in eArchive
The authorisations granted to an individual User determine the documents that User can view. For example, a User is always able to view their own User Authorisation.

Users with permission to view or operate an account are also granted access to view the documents relating to that account in eArchive.

8.3 Storing documents
We file the Electronic Requests and documents in eArchive for the current year plus seven years at a minimum. You should be aware, however, that the documents will be deleted if you deregister an account or change customer number, or if you change bank or for some other reason no longer have access to the Online Banking Channel. In such cases, we recommend that you copy the documents and store them yourself.

If you need to keep the documents for a longer period than the Bank offers via the Online

Banking Channel, you should copy the documents and store them yourself.

8.4 Deregistering for eArchive

Contact the Bank if you no longer wish to receive documents in eArchive. We can send you the documents in hardcopy by agreement, subject to a fee.

8.5 Termination

If your Agreement terminates or you change your customer number or deregister accounts, you can no longer receive electronic documents in eArchive. See section 8.3 on storing documents.

9. Module Selection

The Access Agreement will specify the Modules that you have selected to form part of your Agreement with the Bank. The following is a non-exhaustive list and brief description of some of the Modules available to you (please contact your Account Manager for further information on the Modules available on District):

- *Administration*
- *Notifications*
- *Cash Management – Account Information*
- *Payments*
- *File Transfer*
- *Collection service – SEPA Direct Debit*
- *Markets Online*
- *Trade Finance*

9.1 Administration Module

This Module allows you to authorise Users to:

- view the list of Users
- create/delegate, edit and delete Users under the Access Agreement
- grant Users Administration Privileges (see section 10, below, for further information)

9.2 Notifications Module

This Module allows you / the User to:

- receive notifications when a certain action/event occurs
- manage notifications in the *Notifications Centre*, including:
  - creating, editing and deleting notifications
  - selecting the delivery channel for notifications (e.g. email and/or text message)
- view the history of notifications

9.3 Cash Management – Account Information

This Module allows you / the User to view:

- a list of Registered Accounts
- balance history
- interest-rate history
- terms on the accounts
- a list of fees
- account transactions with details
- Payment Limits set per Registered Account.

9.4 Cash Management – Payments

This Module allows you / the User to:

- effect local payments
- effect cross-border payments
- effect cross-border transfers to and from your Customer group's own accounts within the Danske Bank Group without loss of interest days
- save and re-use master data about your creditors
- update the status of payments
- cancel or edit payments that have been submitted but not yet processed

- effect confidential payments, e.g. wages/ salaries.

The User will be able to effect payments as outlined in the individual User Authorisation.

9.5 Cash Management – File Transfers
This module allows you/the User to:

- transfer files to and from the Bank
- use the file conversion service
- use files to integrate with most major ERP systems, thereby saving time and minimising the risk of input errors.

The User will get access to files regarding all accounts under the Access Agreement.

9.6 Collection Service – SEPA Direct Debit
To be able to create SEPA Direct Debit collections you must register the User for the *Collection Service – SEPA Direct Debit* Module. This will give the User access to:

- collections
- reimbursements
- refunds

On euro Registered Accounts.

9.7 Markets Online Modules
In order to be able to view trade positions, buy and sell foreign currency spot and forward and trade shares, bonds and investment certificates, a User must have access to one or more of the *Markets Online* Modules. Access to buy and sell foreign exchange spot and forward contracts also requires that you grant the User *currency trading* and/or *securities trading* authorisations. These authorisations authorise the User only to perform transactions on your behalf via the *Markets Online* Module.

All transactions relating to the purchase and sale of foreign exchange spot and forward contracts are subject to the provisions of the separate framework agreement on netting and final settlement of trades concluded between you and us.

The User Authorisation must state the accounts and custody accounts that the User is authorised to inquire about or trade in.

9.8 Trade Finance Module
If a User should be able to issue letters of credit, collect debt and/or issue guarantees, you must register the User for the *Trade Finance* Module and sign the "Connection to/Modification of the *Trade Finance* Module" in the Access Agreement or grant the User access to the *Trade Finance* Module using the *Administration* Module. In this regard, you must state whether the User shall have access to:

- letters of credit (exports and/or imports)
- debt collection (exports and/or imports)
- trade guarantees

Furthermore, you must state whether the User shall have access to:

- create and view balances etc.
- create and approve jointly with another person, or
- create and approve separately

10. User Authorisations

All Users performing Transactions on your behalf must be duly authorised to do so. These authorisations are created via the Bank's *User*

Authorisation form or via the *Administration* Module in the Online Banking Channel.

Where you have assigned the *Administration* Module to a User, you will also be required to specify the Administrator Privileges that you wish to assign to the User. The User Authorisation will specify what those Administrator Privileges are. Section 10.1 describes the different types of Administrator Privileges that may be specified on the User Authorisation.

10.1 Administrator Privileges
If the *Administration* Module is included in your Agreement, you must decide what Administrator Privileges the User appointed as an administrator should have. The following is a non-exhaustive list and brief description of the Administrator Privileges that may be granted (a comprehensive list is available in District):

- *agreement administration*
- *user administration*
- *agreement information*
- *log-on and blocking*
- *payment limit – account*
- *card administration*
- *markets online administration*
- *corporate notifications administration*
- *trade finance administration*

10.1.1 For Users granted Agreement Administrator and/or User Administrator Privileges, you must also decide the level of authority that the User will have i.e. whether the User shall be granted:

- *Separate authorisation*
- *Two persons jointly (A authorisation)*

The various authorisations granted by the Bank are described in section 12. A User granted Agreement Administrator and User Administrator Privileges must have the same approval rights for both Privileges.

10.1.2 Agreement administration
If you assign a User the *agreement administration* Privilege, you authorise the User to do the following on your behalf:

- create, modify or delete Users' *agreement administration* Privileges
- create, modify and delete other Privileges in respect of each User

A User with these Administrator Privileges is called an Agreement Administrator. You must decide whether an Agreement Administrator is to be authorised to make changes to their own User ID. If an Agreement Administrator is restricted in relation to his or her own User ID, he or she cannot assign themselves the above Administrator Privileges. Nor will the Agreement Administrator be able to create and approve payment orders. The setting also applies to the User's Privileges as a User Administrator.

Where an *agreement administration* Privilege is assigned, this must always be signed by your authorised signatories. When an Agreement Administrator requests that a User Authorisation with *agreement administration* Privileges be created, a *User Authorisation* form with a signature field is generated and made available in the eArchive.

The *User Authorisation* form is available to Users with the *agreement information* Privilege. The *User Authorisation* form must be printed,

signed and sent to the Bank. In other cases, the User approves and signs using his or her Digital Signature.

Users with the *agreement administration* Privilege must also be assigned the user *administration* Privilege.

10.1.3 User administration
If you assign a *user administration* Privilege to a User, you authorise the User to do the following on your behalf:

- create and change Users, including giving Users access to the mandate and Transaction types, Modules and accounts existing under the Agreement at any time
- create and change User master data
- delete all of a User's data, including master data

A User with these Privileges is called a User Administrator. You must decide whether a User Administrator is to be authorised to make changes to their own User ID. If a User Administrator is restricted in relation to his or her own User ID, he or she will not be able to assign themselves the above Privileges. Nor will the User Administrator be able to create and approve payment orders. The setting also applies to the User's Privileges as an Agreement Administrator.

10.1.4 Agreement information
If you grant a User the *agreement information* Privilege, the User has access – via a User list – to search for Users covered by the Agreement, and see each User's access rights (including master data, Modules, Administrator Privileges, access to accounts and payment access).

10.1.5 Log-on and blocking
If you assign the *log-on and blocking* Privilege to a User, you authorise the User to do the following on your behalf:

- Order Temporary PINs
- Order eSafeID Devices and complete activation of a new eSafeID Device
- Block and unblock User access

10.1.6 Payment limit – account
If you assign the *payment limit – account* Privilege to a User, you authorise him or her to create, change and delete payment limits for the accounts that the User can manage under the Agreement at any time.

When granting the payment *limit – account* Privilege, you must decide which of the following mandates the User should be assigned:

- Separate mandate
- Two persons jointly

For further information on our account mandate types, see section 12.

10.1.7 Card administration
If you assign the *card administration* Privilege to a User, you authorise him or her to perform the following on your behalf:

- block a Card
- re-order a Card
- order and re-order a PIN for a Card
- change a Card limit
- view Card information
- update Cardholder information

To view transactions on a Registered Account associated with a Card a User must hold viewing rights for the account in question.

You and each Cardholder will need to enter into separate documentation with the Bank. This documentation will confirm among other things that; (i) the Cardholder has read and accepted the terms and conditions for use of the relevant Card now published and up-dated from time to time on the Bank's website, and; (ii) that the Bank exchanges information with business partners for the establishment and administration of additional benefits of the Card and for the processing of any claims. The Customer warrants that it will have the cardholder sign this document prior to the issue of the card and agrees that it will also be required to forward such documentation to the Bank on demand.

10.1.8 Markets online
If you assign the *markets online* Privilege to a User, you authorise him or her to create, edit and delete User Authorisations relating to the trading in securities or foreign exchange via the Online Banking Channel or viewing trades via the Online Banking Channel.

In order for a User to be able to trade securities or enter into foreign exchange contracts on your behalf, you must execute the applicable mandate in writing for that User.

10.1.9 Corporate Notifications
If you assign the *corporate notifications* Privilege to a User, you authorise him or her to perform the following on your behalf:

- create notification subscriptions for Users
- read notifications received
- manage User information
- delete subscriptions for corporate notifications created by Users

The Bank may charge a fee for notifications sent to Users as notified to you in the Online Banking Channel. Where you grant a User *corporate notifications* Privileges you acknowledge and agree to pay to the Bank any fees associated with notifications created.

10.1.10 Trade Finance
A User who is assigned *trade finance* Privileges is authorised on your behalf to create, modify or delete User Authorisations relating to *trade finance* instructions provided to the Bank using the trade finance Module as set out in section 9.6, above. The various types of authorisations are described in section 12 below.

The Bank may from time to time update and increase the types of Administrator Privileges available. Any new or additional types of Administrator Privileges will be governed by these Special Terms and Conditions. You will receive separate notification of any such changes via the Online Banking Channel or otherwise. Where a User has been granted Administrator Privileges then references to you in these Special Terms and Conditions should be construed accordingly so that anything which an Agreement Administrator does under the terms of the User Authorisation shall be treated as if it was done by you. If a third party has signed a mandate in favour of you, you may delegate this mandate to a User. This is done via the User Authorisation in the Online Banking Channel.

10.2 Message system
All Users can send messages electronically to the Bank via a secure encrypted line. Users can view only messages that they themselves

send and receive in the Online Banking Channel. Orders cannot be placed via the message system.

10.3 Cancellation of the *Administration* Module

If you cancel the *Administration* Module, then the payment limits which have been authorised will continue to be applicable to this Agreement. In respect of any accounts which are opened after the date of cancellation of the *Administration* Module, payment limits on accounts will not apply but payment limits on Users will continue to apply. You must contact the Bank in writing if you wish to amend or cancel any payment limits which have been authorised. If you do not have access to the *Administration* Module.

After cancellation of the *Administration* Module any Users who have been granted automatic access to future accounts will not have automatic access to any future accounts opened.

10.4 Changing User Authorisation

If you wish to extend or limit a User's access to the Online Banking Channel, a new User Authorisation for the Online Banking Channel must be signed physically or using your Digital Signature on your Online Banking Channel where applicable, replacing the previous one. If the change relates to the User's authorisations at account level, you and/or the relevant third party must also sign an account mandate. Note that a User's authorisation in the Online Banking Channel may be affected if you issue an account mandate form.

10.5 Revoking User Authorisation

User Authorisations remain in force until revoked by you in writing – physically or using your Digital Signature where applicable. When we have received notice of revocation, we will send written confirmation that the User ID and Encryption Key(s) have been deleted in our systems. If you terminate this Agreement, we will construe this as revocation of all User Authorisations granted under this Agreement. If you and/or a third party have granted the User an account mandate, this mandate must be revoked separately. It is not sufficient for you merely to revoke the User Authorisation.

10.6 Access to Accounts

For each User, you must state which accounts the User may inquire about and/or make payments from. If you authorise a User to make payments from an account, the User is granted access to the transaction types determined by you. For each Account that the User is granted access to, the User's mandate type must be stated. Please see section 12 below for further information on mandate types.

10.7 Payment Limits

Where you have included the *Administration* Module in your Online Banking Channel Agreement, you may control the value of requests created and/or approved through the Online Banking Channel either at an account level which applies to all Users (known as Payment Limit – account) or on individual Users (known as payment limit – user). It is your responsibility to create payment limits suitable for your requirements. If a Payment Limit – account or Payment Limit - user is exceeded, payments may not be processed until appropriate action is taken by you. (Please refer to our "Getting Started Guide on Administration - Payment Limits" for more information). In exceptional circumstances the

Bank may, at its discretion, agree to create a Payment Limit on your behalf on receipt of written instructions.

10.8 Transaction Types
For each User, you must state which Transaction types the User is to have access to:

- Payments between accounts registered under this Agreement in the same country within the Danske Bank Group
- Payment requests via SWIFT MT101
- Euro payments to accounts in Ireland or within the Single Euro Payments Area (SEPA)
- Cross-border payments to Registered Accounts and unregistered accounts within or outside the Danske Bank Group.

Furthermore, you must state whether the User is to be authorised to create and approve, or only to create, the payments selected. If the User is authorised both to create and approve payments, the relevant mandates for each Transaction type must also be stated. The following mandates are available at Transaction level:

- Separate authorisation
- Two persons jointly

The various mandate granted by us are described in section 12, below, In general, the selected mandate is used for all payments within each payment type. If you have selected a more restrictive authorisation at account level, this authorisation will apply for payments to unregistered accounts and cross-border payments. Note that if the User has not been granted any authorisation at account level, this is also regarded as a restriction.

11. Exchange Rates

Payments to Registered Accounts and unregistered accounts within or outside the Danske Bank Group may be processed:

- without exchange – where no exchange is required (for example, the payment is being made in the same currency as the beneficiary account)
- at the relevant Fixing Rate
- at the spot rate – a currency exchange rate based off the prevailing market rate at that time and at or within the spreads on our rates (available on the Online Banking Channel)
- at the agreed rate – a rate agreed in advance with the Bank for the specific payment (an agreement number must be held by you to use this rate)
- at the forward rate – a rate agreed in respect of a forward contract agreed between us (a forward contract number must be held by you to use this rate)

Domestic Payments from one currency to another between Registered Accounts processed as *Account Transfer* Internal on the Online Banking Channel will be processed at the relevant Fixing Rate.

The relevant exchange rate may be subject to change, at the discretion of the Bank, in respect of foreign payments for an amount in excess of €50,000 (or its equivalent).

12. Mandate types

The Bank operates with the following mandate types:

- Separate authorisation
- Two persons jointly (A mandate)
- Two persons jointly (B mandate)
- Two persons jointly (C mandate)

These mandates allow you to specify which Users may, separately or jointly, approve a payment or request. These mandates are described below.

12.1 Separate authorisation
Requests or payments that are created or changed by a User with this mandate are automatically deemed to have been approved by the User. Users with this mandate can also approve requests or payments entered by Users with all other mandate types.

12.2 Two persons jointly (A mandate)
When requests or payments are created by a User with an A mandate, they are automatically approved by this User (1st approval). Further approval (2nd approval) by a separate User with an A, B or C mandate is also required. Users with A mandates rank equally, and the order of approval is therefore of no consequence.

12.3 Two persons jointly (B mandate)
When requests or payments are created by a User with a B mandate, they are automatically approved by this User (1st approval). Further approval (2nd approval) by a separate User with an A or C mandate is also required. Two Users with B mandates cannot jointly approve a payment.

12.4 Two persons jointly (C mandate)
When requests or payments are created by a User with a C mandate, they are automatically approved by this User (1st approval). Further approval (2nd approval) by a separate User with an A or B mandate is required. Two Users with C mandates cannot jointly approve a payment.

13. Other mandates in the Online Banking Channel

13.1 Third-party mandates granted to you
If you wish to make transactions on third-party accounts with the Danske Bank Group, the third party must sign our third-party mandate form. If account queries should be possible using SWIFT MT940 on third-party accounts outside the Danske Bank Group, an agreement stating that the Danske Bank Group may receive data about the third party's external account(s) shall first be submitted to us. If you should make payments from the third party's accounts outside the Danske Bank Group using SWIFT MT101, an agreement stating that you may send payment instructions to the third party's bank(s) via the Danske Bank Group shall first be submitted to us. The Bank registers the third-party accounts in the Online Banking Channel via your Access Agreement. The availability of SWIFT MT101 will be dependent on third party banks.

14. Business Mobile Banking App

14.1 Access and use
To be eligible to access the Online Banking Channel through the Business Mobile Banking App you must have completed and signed an Access Agreement and you, together with each User, must be registered for the Online Banking Channel, have a Device and otherwise comply with any requirements set down by the relevant software application distributor.

When a User downloads the Business Mobile Banking App to a Device you accept that these Special Terms and Conditions apply in relation to the use of the Online Banking Channel by you or

that User via the Business Mobile Banking App. In addition, the use of the Business Mobile Banking App is subject to the terms and conditions of the licence under which it may be downloaded from the App Store, Google Play and any other relevant software application distributor.

It is important that you and each User only downloads the Business Mobile Banking App in accordance with the terms and conditions agreed with Apple (for the App store) or Google (for Google Play).

The Business Mobile Banking App currently gives access to the following content and account services:

- View Balances
- View Transactions
- View history of transactions
- Create Domestic Payments and approve payments
- Administration

The Bank may from time to time update, extend or reduce the services offered via the Business Mobile Banking App. The Bank may extend the scope of the services offered via the Business Mobile Banking App without notice and add new services to the Business Mobile Banking App without advance notice and without obtaining new signatures from you, provided that the new services are advantageous to you. Whereas not less than two months' notice is required prior to any reduction in scope and/ or content. If you are a Corporate Customer, then the requirement as to notice will apply save that the period of notice can be less than two months.

14.2 Security

In addition to any other obligations or responsibilities which you may have under these Special Terms and Conditions, you and each User must take all reasonable steps to maintain the confidentiality of any information shown or stored on the Device in connection with your use of the Business Mobile Banking App. You are solely responsible for the safety and security of your Device.

You and each User should as a minimum take the following steps to protect your account information:

- Set a PIN on the Device, change it regularly and keep your keypad locked
- Ensure that you and each User logs-off from any Business Mobile Banking App session as soon as you have finished availing of the relevant service(s)
- Keep the Device in your possession at all times and do not leave your Device unattended where it may be accessed by unauthorised persons.

The Business Mobile Banking App is currently free of charge from the Bank, however you should refer to your network service provider for any additional charges that could be imposed by them. If you use Mobile Banking, certain services on the Business Mobile Banking App use location data sent from a Device which can be turned off by you or a User at any time if you wish. If you use these services you consent to collection and processing of this location data.

15. Customer support

The Bank provides support and service to you in the form of:

- user administration
- telephone support
- internet-based support functions
- on-site support

User administration includes establishing Access Agreements and authorisations and mandates, modifying the access of your business and its Users to individual elements of support and service, deleting and blocking Users, ordering Temporary PINs and registering modified authorisations and mandates.

Telephone support may include training, User instruction, troubleshooting assistance, guidance in relation to modifications, and an option to block the Online Banking Channel. Telephone support in connection with installation, setup, training and troubleshooting, etc. of the Online Banking Channel is provided in cooperation with your IT department and at your risk.

Online support may include training, User instruction, troubleshooting assistance and guidance in relation to modifications. Online support is provided in cooperation with your IT department and at your risk.

On-site support may include providing training in the use of the Online Banking Channel.

Troubleshooting may include adjusting and/or changing the configuration of your computers and IT systems, changes in registration databases, configuring routers, firewalls, proxy servers and internal security systems and general changes in software and hardware configuration.

Configuration and support is provided in cooperation with your IT department and at your risk.

Part 2 – Third Party Access Rights

16. TPPs – general

You can use TPP services to aggregate your account information, make payments out of your account and to make confirmation of funds requests, if you are registered for the Online Banking Channel and have a Digital Signature. All references to you in this section include any User with a Digital Signature authorised to access your account. You must have a Digital Signature that allows you to make payments out of your account to use Payment Initiation Services and Card Based Payment services.

TPPs are independent providers of services. If we provide you with a TPP service then we will make that clear to you at the time. TPP services can be used to access any of your accounts which are accessible online. Your account will be accessible online unless the terms and conditions for your account state otherwise. The following types of services are offered by TPPs:

- **Account Information Services** – these services allow Customers to consolidate information about different payment accounts which they have with one or more banks to review their overall aggregated financial position. Some TPPs may also offer a range of associated services such as budgeting and financial planning tools. Further information is set out below.
- **Payment Initiation Services** – these services help Customers to make a range of credit transfers out of their account.
- **Card Based Payment instrument issuers** – some TPPs may issue instruments for making Card Based Payments out of your account. These TPPs may ask us to confirm whether an amount needed for a payment using a card they have issued is available on your account. Further information about how we respond to such requests is set out below.

If you use a TPP to make a payment from your account, then you will need to confirm the details of the payment including the sort code and account number or, where applicable, the BIC and IBAN of the Payee and also the amount of the payment. When you confirm these details, we will process the payment as set out in our Corporates & Institutions – Fees & Charges brochure. In particular, you should note that payments initiated by a TPP which require authorization by more than one User (for example, where a User has a joint mandate to approve payments) will only be deemed to have been received by us when we receive the final authorisation from an appropriate User. Any payment from your account using the services of a Third Party Provider will be made from the account as a credit transfer even if the account is one on which one of our Cards has been issued. Further information on how this may impact on the protections that you have is set out below.

TPPs may provide their services in different ways. Some TPPs use the Open Banking APIs to access your account whilst others use a technique known as Screen-scraping. The way in which a TPP accesses your account is important because this will affect how these Special Terms and Conditions apply to you when using the TPP services.

If you consent to a TPP accessing your account using the Open Banking APIs, we will ask you to authenticate any TPP requests that we receive by entering your Digital Signature on a secure Bank page – this will not be the Online Banking Channel log on page. By entering your Digital Signature, you give us your consent to provide information to

that TPP, make a payment that they have initiated or to respond to a confirmation of funds request, whichever applies. The TPP will only be able to view the information that you specifically authorise it to view or to debit the specific payment that you authorise.

If you consent to a TPP accessing your account using Screen-scraping then you give us your consent to provide information or make payments using that TPP by providing them with your Digital Signature. A TPP accessing your account using Screen-scraping will be able to access all of your accounts, including being able to access all the information that you can access in the Online Banking Channel and make payments from your account in the same way that you can. The TPP may ask you for your Digital Signature on its own website or it may instead redirect you to the Online Banking Channel log on page with the Bank's website and ask for the information there.

Where the TPP uses Screen-scraping techniques it may not be clear to us that the services of a TPP are being used. In these circumstances, you must provide us with the details of the TPP on request.

You will be able to revoke TPP access to your account either:

(i) directly with the TPP by following its procedures,
(ii) in our Online Banking Channel under 'Contact and help' or
(iii) by contacting the Bank directly.

You can also obtain a full list of TPPs who you have authorised to access your account by contacting us. We can only provide this service where the TPP uses the Open Banking APIs to access your account. You can revoke TPP access to your account directly with the TPP using its own procedures, where the TPP is using Screen- scraping techniques to access your account.

Where you tell us that you want to withdraw a TPP's ability to access to your account we will comply with that request but it will not act as a revocation of consent to a payment that has already been debited from your account or to information that has already been provided to a TPP in response to a confirmation of funds request or for Account Information Services.

We will only otherwise revoke a TPP's access to your account if we believe its access is unauthorised or fraudulent or if we become aware that it is no longer authorised or regulated by an appropriate authority.

17. TPPs – Account Information Services

A TPP will only be able to get information about your account if it is accessible online. Your account is accessible online unless the terms and conditions for your account state otherwise. All references to you in this section include any User who has a Digital Signature and is authorised to access your account. All Users with a Digital Signature and are authorised to access your account can use Account Information Services.

The TPP will ask you to give your explicit consent before it can access your account. This means that the TPP should make available to you the information that you need to make an informed decision so that you understand what you are consenting to.

If the TPP accesses your account using the Open Banking APIs the TPP will only receive

the specific information that you have explicitly consented to be provided. When the TPP uses this method you will be redirected to a Bank webpage where you will be asked to provide your Digital Signature. By entering the Digital Signature you are giving us your consent to provide the information to the TPP for a specified period of time. Only certain accounts are accessible in this way (for example accounts which are not payment accounts are not accessible). Information about your accounts will be available as "data clusters" – this means that we will group certain information into a data set (a cluster). When you confirm your consent all of the information in the data cluster will be made available to the TPP.

If the TPP accesses your account using Screen-scraping the TPP will be able to access and download all of the information that is available within our Online Business Channel and we will not be able to limit or restrict this. By giving the TPP your Digital Signature you are giving us your consent to provide the information to the TPP. Unless the TPP has taken steps to identify itself to us we may think that the request is being made directly by you. A TPP which uses Screen-scraping techniques will be able to access both payment and non-payment accounts. A non-payment account would include any loan accounts that you have with us.

We recommend that you check that the TPP is authorised and regulated by the Central Bank of Ireland or another European Regulator before using its services. If the TPP is authorised and regulated by the Central Bank of Ireland then it will be subject to the Payment Services Regulations. This means that it is obliged to ensure that any personalised security credentials are not available to any unauthorised person and that it uses safe and efficient channels in providing its services to you.

A TPP should not request more information than is absolutely necessary to provide the specific service it is offering to you.

A TPP which provides an Account Information Service may use the User's personalised security credentials if it is necessary to provide the Account Information Service. We will treat a request from an Account Information Service TPP in the same way as we treat a request received from you. We will release information about all parties to any joint accounts. Any information that you have recorded on your account about any third party will not be released. We will not provide your Digital Signature to a TPP.

You will be able to revoke TPP access to your account either directly with the TPP by following its procedures, in our Online Business Channel under 'Contact and help' or by contacting the Bank directly. You can also obtain a full list of TPPs whom you have authorised to access your account by contacting us. We can only provide this service where the TPP uses the Open Banking APIs to access your account. You can revoke TPP access to your account directly with the TPP using its own procedures, where the TPP is using Screen-scraping techniques to access your account.

Where you tell us that you want to withdraw access to a TPP being able to access your account we will comply with that request but it will not act as a revocation of consent where information has already been provided to a TPP which provides Account Information Services.

We will only otherwise revoke a TPP's access to your account if we believe its access is unauthorised or fraudulent or if we become aware that it is no longer authorised or regulated by an appropriate authority.

If you experience detriment caused by your Account Information Service provider (AISP) other than in relation to an unauthorised payment you should contact the AISP in the first instance. If you believe that we have breached any of our obligations in relation to a TPP having accessed your account for the purposes of provision of Account Information Services then you should contact us. We will be liable for any loss that you have suffered as a result of us having breached any of our obligations. We are not responsible to you under this section where any failure on our part was due to (i) abnormal or unforeseeable circumstances beyond our control, the consequences of which would have been unavoidable despite all of our efforts to the contrary or (ii) our obligations to comply with any other provision of applicable laws.

18. TPPs – Card Based Payments

All references to you in this section include any User with a separate mandate to make payments out of your account.

We will confirm whether an amount needed for a Card Based Payment out of your account is available when this information is requested by the card issuer if:

- your account is accessible online at the time we receive the request or
- you have given us your consent to do so.

When we receive the first confirmation of funds request from a card issuer, we will ask you to authenticate the request. We will then show you all the information relating to the request, including who has made it, the account it relates to and the date on which consent for us to respond to such requests from the TPP expires, if any.

We will then ask you to confirm your consent before we respond to the request. We will only respond with a "yes/no" answer about the availability of funds in a particular account to cover the amount in the request. We will not provide details of your account balance or block funds on your account for payment. We will continue to respond to confirmation of funds requests made by that particular card issuer until either your consent expires or you revoke it, whichever is earlier.

You can view your confirmation of funds history and revoke your consent to us responding to further confirmation of funds requests in the Online Banking Channel or by otherwise contacting us to communicate this.

Part 3 – Online Banking Channel Security System

19. Technical issues

19.1 Transmission and access

In order to use our Online Banking Channel, you must establish a data communication link with us. You must bear the costs related to the link and must purchase, install, set up and maintain the required IT equipment. You must also ensure the necessary adaptations to your IT equipment in order to use the link and ensure continuity of operations.

You may not use special software, such as 'overlay services' or similar types of software, when you use the Online Banking Channel. Users must operate the system directly via the user interface and the software provided by the Bank.

19.2 Distribution, control and storage of software

The Bank distributes the programs you need to install and run the Online Banking Channel, which may, for example, be relevant in connection with file exchanging. You can download the programs from the internet.

When you download programs from the internet, you must check that the program delivery has been electronically (digitally) signed by us.

If the programs have not been electronically signed by us, the reason may be that they have been tampered with or do not come from us. The signature can subsequently be verified by checking the properties of the downloaded program file(s). If the electronic signature is not from us, the downloaded program must not be installed.

19.3 Data security

eSafeID, e-Safekey, EDISec and OpenPGP are the general security systems used in our Online Banking Channel.

e-Safekey, OpenPGP and EDISec are the Bank's security systems for customers who want to exchange information digitally with the Bank directly through their own business systems. e-Safekey, OpenPGP and EDISec are based on a password and use permanent Encryption Keys that are stored in the business's IT environment.

Use of the above security systems ensures that data can be encrypted before transmission to Danske Bank and that data is not altered during transmission.

The identity of the sender is also always verified, and all financially binding transactions are signed digitally.

19.3.1 eSafeID

eSafeID is the Bank's web-based security system for logging on to the Online Banking Channel. eSafeID is a two-factor authentication solution, based on something you know and something you have: a Password and an eSafeID Device that generates security codes, which can only be used once. These two factors are used to authenticate the person, after which sessions are generated as well as customer-specific codes saved temporarily in the browser session while the user remains logged on to the Online Banking Channel.

When a User is created using the eSafeID security system, the User receives a personal User ID, a Temporary PIN and an eSafeID Device. The User must activate the eSafeID Device and

create a Password before the eSafeID security system can be used to access the Online Banking Channel.

When a User is created in the Online Banking Channel using the eSafeID security system, we give the User an individual User ID, a Temporary PIN and an eSafeID Device. Together with the eSafeID Device, the Temporary PIN is used for first-time identification when the User is registered in the security system.

The Temporary PIN is system-generated and printed electronically without anybody seeing the combination. If the letter containing the Temporary PIN and/or the letter containing the eSafeID Device has been tampered with or is not intact, the User must contact us to order a new Temporary PIN and/or a new eSafeID Device. For security reasons, the letters containing the Temporary PIN and the eSafeID Device are sent at different times.

If the User has not received the letter containing the Temporary PIN within five Business Days of ordering it, the User must, for security reasons, contact us to cancel it and order a new one.

During registration in the Online Banking Channel, the User chooses a Password and must subsequently destroy the Temporary PIN. The Password must be changed regularly by the User.

If the User has registered a mobile phone number in the Online Banking Channel, the User has the option of receiving the Temporary PIN via SMS text message. If the User does not receive a text message containing the Temporary PIN within 15 minutes of ordering it, the User must, for security reasons, contact the Bank to cancel it and order a new one. When registering in the Online Banking Channel, the User must select a Password and delete the Temporary PIN. The Bank is not liable for any errors or losses resulting from the User or Agreement Administrator not being able to update the User's mobile phone details in the Online Banking Channel.

19.3.2 e-Safekey

e-Safekey is the security system in the Bank's Business API solution. When a User is to be created using the e-Safekey security system, the user receives a personal user ID and a temporary password. This temporary password is used for first-time identification when the User is registered in the system.

19.3.3 EDIsec

EDIsec is a security solution used to protect data in direct data transmission between you and the Bank via a communication channel established between you and the Bank.

When a User is to be created using the EDIsec security system, the Bank allocates a personal user ID to the User, but not a temporary password. The validity of the customer's public EDIsec Encryption Key is confirmed by the fingerprint which the customer must make of the Encryption Key and which is exchanged with the Bank in accordance with the guidelines described in the EDIsec implementation guide.

19.3.4 OpenPGP

OpenPGP is a security solution used to protect data in direct data transmission between you and the Bank via a communication channel established between you and the Bank.

When a User is to be created using the OpenPGP security system, the Bank allocates

a personal user ID and a temporary password to the User. You must generate your own OpenPGP Encryption Keys and send them to the Bank together with the temporary password in accordance with the instructions described in the *"OpenPGP Security Implementation Guide"* from the Bank.

If a certificate has been issued by a third party's issuer, the Bank regards the User as the certificate owner and thus as responsible for the validity of the certificate and maintenance thereof. The Bank uses only the public cryptographic code contained in the certificate.

You are responsible for acquiring and using suitable OpenPGP software (own or third-party software) that can handle OpenPGP security. This means that the software must be able, for example, to handle OpenPGP codes and file signing/encryption.

19.3.5 EDIsec codes and OpenPGP codes
For EDIsec and OpenPGP, you are responsible for using valid Encryption Keys and securing data communication with the Bank. The following applies specifically:

- the Bank must have valid versions of your Encryption Keys. When your Encryption Keys are about to expire, you must ensure that your public Encryption Keys are exchanged with the Bank
- you must use valid versions of the Bank's Encryption Keys to secure the data communication with the Bank. When the Bank's public Encryption Keys are about to expire, you must ensure that your system is updated with a new version of the Bank's Encryption Keys, which the Bank will make available
- if the your Encryption Keys are compromised, the customer must contact Danske Bank to have them blocked.

When Danske Bank receives your public EDISec code or public OpenPGP certificate, they will be stored in the Bank's IT infrastructure and will not be exchanged with parties outside the Bank.

The Bank is responsible for ensuring at any given time that valid versions of our public EDISec code and public OpenPGP certificate are available to you.

19.4 Storing the User ID, Password and eSafeID Device
You must implement effective security procedures to prevent unauthorised use of the Online Banking Channel, including unauthorised access to Encryption Keys and eSafeID Devices.

The following rules apply to the use of eSafeID:

- Only the User may use the User ID, Password and eSafeID Device
- The User ID, Password and eSafeID Device are strictly personal and must not be shared with any third parties
- The User ID, Password and eSafeID Device may be used only when communicating with the Bank
- The Password must not be written down and stored together with the eSafeID Device
- The Bank recommends that the customer store secret codes in crypto hardware to the extent possible.

The User should select a Password that is as difficult as possible to guess — for example using upper and lower-case letters, numbers and symbols. The User must ensure that other

Users do not know the Password and must store it in a suitable and safe manner. Further information about security recommendations is available under the Security menu in the Online Banking Channel and on the Danske Bank Group websites.

19.5 Deregistering or blocking access
You must notify the Bank if you want it to remove a User's access to the Online Banking Channel. You must immediately contact the Bank to block User access if:

- unauthorised use of a Password, Encryption Key or an eSafeID Device is suspected
- third parties have gained access to a Password or Encryption Key or an eSafeID Device

Blocks can be requested or cancelled via the Online Banking Channel or via telephone. If the request is made via telephone, the message must subsequently be confirmed in writing. However, the User will be blocked in the interim period.

You are responsible for all transactions executed by a User until the Bank has been requested to delete or block the User. You are also responsible for all future transactions previously ordered by a deleted/blocked User until the Bank has been notified that the transactions must be deleted and confirms that this is possible.

19.6 The Bank's right to block the business's or a User's access
Users can also be blocked by the Bank. We reserve the right to block your or a User's access to the Online Banking Channel for objectively justified reasons relating to the security of the Online Banking Channel service or if we register attempts at misuse. If access is blocked, you will be notified immediately by telephone, in writing, by email, by fax or other such reasonable means we may choose and we will unblock access to the Online Banking Channel if the reasons for blocking cease to exist.

The Bank also reserves the right to block your access to the Online Banking Channel if your equipment, software or interfaces damage, interfere with or in any other way cause inconvenience to the Bank or its IT infrastructure. If access is blocked, you will be notified as soon as possible.

If you wish to apply for unblocking of your access to Online Banking Channel please contact the Online Banking Channel helpdesk, your Account Manager or by phoning 1850 812 040. After unblocking, a Temporary PIN may be issued by SMS to a User where the User has registered a mobile telephone number.

You must take all reasonable steps to prevent unauthorised use of the Service and unauthorised access to User Encryption Keys, Passwords or eSafeID Devices.

19.7 Encryption Bans
National legislation in the country in which District is being used may contain a general ban or restrictions on encryption. It is therefore important to be aware of a given country's legislation.

Part 4 – Contractual Matters

20. For business purposes only

The Online Banking Channel is to be used for business purposes only. The information made available to you, including price information, is solely for your own use. You may not pass on the information to others, except with our prior written permission.

21. Changing the Online Banking Channel

We may at any time extend the scope of our Online Banking Channel without advance notice, whereas not less than two months' notice is required prior to any reduction in its scope and/or content. If you are a Corporate Customer, then the requirement as to notice will apply save that the period of notice can be less than two months. We shall provide written information of any changes via the Online Banking Channel or otherwise.

22. Changes to service and support

We may change the scope and content of our service and support at any time by giving not less than two months' written notice via our Online Banking Channel or otherwise. If you are a Corporate Customer, then the requirement as to notice will apply save that the period of notice can be less than two months.

We will provide notification of any modifications requiring adaptation of your equipment in order to retain the link and access by giving not less than two months' written notice via the Online Banking Channel or otherwise. If you are a Corporate Customer, then the requirement as to notice will apply save that the period of notice can be less than two months.

We may at any time and without notice modify our own equipment, basic software and related procedures in order to optimise operations and service levels.

You may not use special software, such as 'overlay services' or similar types of software, when you use the Online Banking Channel. Users must operate the system directly via the user interface and the software provided by the Bank.

23. Responsibilities and liability

4.1 Your responsibilities

You use our Online Banking Channel at your own responsibility and risk.

This includes, but is not limited to, the risk in relation to:

- sending information to us, as well as the risk that a transmission is destroyed, lost, damaged, delayed or affected by transmission errors or omissions, e.g. during intermediate handling or processing of data content
- information becoming accessible to third parties as a result of errors or unauthorised intrusion on the data transmission line
- incorrect use or misuse of the Online Banking Channel by Users
- all operations and transactions made using your Encryption Key or that of a User
- ensuring that Users keep their Passwords secure so that no third party becomes aware of them
- ensuring data security in connection with storage of Encryption Keys in your IT environment to prevent unauthorised access

- unauthorised use of the Online Banking Channel
- that data transferred to the Online Banking Channel is correct and can be transferred for the intended use

You cannot hold the Bank liable for any consequences thereof. Nor can you raise any claims against the Bank in respect of errors and omissions arising out of your own circumstances, including non-observance of security and control procedures.

It is also your responsibility to:

- ensure that User(s) are familiar with these Special Terms and Conditions and the various Modules, and that each User complies with them and follows the instructions in the help texts displayed on the screen
- check that the content of User Authorisations always matches the authorisations given to the User by you and any third party
- ensure that the content of the User Authorisation is in accordance with your wishes
- ensure that the content of the User Authorisation is in accordance with the User's wishes
- inform us as soon as possible if you find that the statement of any Registered Account includes any item authorised via the Online Banking Channel which seems to be incorrect. On becoming aware of an unauthorised amount having been debited to such an account, you should telephone the Bank or your Account Manager as soon as possible and, in any event, no later than thirteen months after the debit date in which case you will, subject to all applicable laws and a prompt investigation by us demonstrating that the transaction was, in fact, unauthorised, be able to obtain a refund from us. You should confirm such telephone call in writing to the Bank or your Account Manager within seven days
- where any Password, Digital Signature or Encryption Key relating to your access to our Online Banking Channel Service has been misappropriated or used in an unauthorised manner, notify us by telephoning the Bank or your Account Manager. You should confirm your notice by writing within seven days to the Bank or your Account Manager. Subject to any applicable laws, you cannot make any claims on us in respect of errors and omissions resulting from your circumstances, including non-observance of your safety and control procedures.

When you provide us with Personal Data for a User, you warrant that you are entitled to disclose such Personal Data to us. In addition, you confirm you will promptly ensure that the Data Subject has been informed where to find information about our processing of Personal Data. If a User needs to have manual access to accounts, e.g. to carry out transactions at An Post branches or sign cheques, you must sign an account mandate form (which you can obtain from us) authorising the User to do so.

At the Bank's request, or where public authorities request relevant information, you shall provide the Bank with such documentation as may be reasonably required to enable the Bank to demonstrate that there is an appropriate and valid legal basis for the Bank's processing of Personal Data as mentioned above.

23.2 Our responsibilities
We will be liable if, through errors or neglect, we fail to perform our contractual obligations.

We are not liable for errors and omissions resulting from:

- errors and omissions in third-party software which is part of the Online Banking Channel security system
- a User's disclosure of that User's Temporary PIN and/or Password
- modifications to the security system (not performed by us)
- the security system's integration with other systems or software not supplied by us
- services, information and data supplied by third parties
- In areas that are subject to stricter liability, we will not be liable for losses resulting from:
- IT system failure/downtime or corruption of data in these systems as a result of the events listed below, irrespective of whether we operate the system itself or have outsourced operations
- telecommunication or power failures at our offices, statutory intervention or administrative acts, natural disasters, wars, rebellions, pandemics, civil unrest, acts of sabotage, terrorism or vandalism (including computer viruses and hacking) strikes, lockouts, boycotts or blockades, irrespective of whether the conflict is targeted at or initiated by us or our organisation and irrespective of the cause of the conflict. This also applies if the conflict affects only parts of our organisation
- any other circumstances beyond our control
- Our exemption from liability does not apply if:
- we should have predicted the circumstances resulting in the loss at the time when the Agreement was concluded, or should have prevented or overcome the cause of the loss
- legislation under any circumstances renders us liable for the cause of the loss.

In accordance with general liability provisions in force we are liable only for direct losses attributable to errors made by us. Apart from that, our liability is limited to remedying the deficiencies. No further claims can be made against us, including for indirect or consequential damage.

24. Other terms and conditions

24.1 Structure of the Agreement
The Agreement is comprised of the following:

- the Access Agreement
- all User Authorisation forms
- all Module Descriptions forms
- these Special Terms and Conditions
- the General Terms and Conditions
- the Bank's Corporates & Institutions – Fees & Charges brochure
- help documents and programs

By signing the Access Agreement you also acknowledge having read and accepted all parts of the Agreement.

When you sign the Access Agreement, you acknowledge having read and accepted these Special Terms and Conditions as an integral part of the Agreement.

New terms of use for services offered in the Online Banking Channel, including terms of use for services offered by selected third parties, may be regularly added, depending on your business's current use of the services.

Unless agreed otherwise, if your business begins using a service offered in the Online Banking Channel, the related service conditions are deemed to have been accepted, and amendments to separate terms of use will be deemed to have been accepted by continued use.

These Special Terms and Conditions and other business terms and conditions can be viewed on and downloaded from the Bank's website.

24.2 Prices
We debit charges and fees to the account(s) designated by you for this, unless otherwise agreed in the special conditions attached to the given Module.

We are entitled to:

- group and debit fees more than one month after the transaction to which they relate has been processed
- charge a fee for delivering supplementary details or information at more frequent intervals than agreed when this Agreement was concluded
- charge a fee for payments that you make from an account and for providing you with details about payments made

We may at any time change our prices by giving not less than two months' written notice via the Online Banking Channel or otherwise. If you are a Corporate Customer, then the requirement as to notice will apply save that the period of notice can be less than two months. Details of our current fees and charges can be found in our Corporates & Institutions - Fees & Charges brochure.

24.3 Assignment, transfer and third parties
This Agreement has been concluded by the Bank on behalf of the Danske Bank Group. This means that any entity of the Danske Bank Group is entitled to fulfil and enforce the Agreement. It also means that the Bank may assign or transfer its rights and obligations under the Agreement to another entity of the Danske Bank Group at any time.

The Bank may assign its rights under the Agreement to subcontractors. Such an assignment will not exempt the Bank from liability under this Agreement.

25. Termination and breach
You may terminate the Access Agreement at any time by giving us written notification. Requests and agreements made before the time of termination will be carried out. Paid subscription fees will not be refunded.

We may terminate the Access Agreement in writing at any time by giving not less than two months' notice. If you are a Corporate Customer, then the requirement as to notice will apply save that the period of notice can be less than two months.

We may terminate the Access Agreement without notice if you breach this Agreement. Breaches include failing to pay as agreed in the Access Agreement, suspending payments or becoming subject to insolvency proceedings.

Part 5 – Definitions and Glossary

Defined terms used in these Special Terms and Conditions shall have the meanings given to them in the General Terms and Conditions, unless otherwise defined herein.

In these Special Terms and Conditions:

Access Agreement: means the agreement between you and us concerning the use of the Online Banking Channel and what Modules will be available to you

Account Information Services: means services of the type described in sections 16 and 17

Administrator Privileges (or Privileges): means the rights and privileges afforded to a User as described at section 10.1, a full list of which is available on the Online Banking Channel

Agreement: means the complete agreement in relation to the Online Banking Channel as further described in section 24.1

Agreement Administrator: means a User assigned the Agreement Administrator Privileges as described in section 10.1.1

Application Programme Interface: has the meaning given to such term in the Payment Service Regulations

Authorisation / mandate: means any User Authorisation, account mandate or one of our other mandate forms for the Online Banking Channel

Business Mobile Banking App: means the Bank's business mobile banking app available from the Apple or Android online stores (or such other software application distributor as may offer a Bank business mobile banking application from time to time) which enables the electronic receipt and transmission of information (including information in relation to a Registered Account)

Card: means the Mastercard Corporate Classic card, the Mastercard Corporate Classic Standard card, the Debit Mastercard Business card, the Mastercard Corporate Gold card or the Mastercard Corporate Platinum card as provided to the Cardholder by the Bank

Card Based Payments: mean payments out of your account made using a card that has been issued by a Third Party Provider – such payments do not include payments made using a Card that we have issued to you

Cardholder: means, for each Card, the person to whom we issue that Card

Customer: means you, the Customer, who has entered into an Agreement, and includes each and every person nominated by you on any Authorisation or mandate, through the Administration Module in the Online Banking Channel or other document provided by you in connection with your Agreement

Device: means an electronic device (such as a smartphone, tablet or mobile phone) which is capable of accessing the internet or downloading the Business Mobile Banking App

Digital Signature: means an electronic signature generated by a Customer or User using his or her User ID, Password and eSafeID Code

District: is a multichannel platform with a full customer interface, which aims to combine all Bank services with selected third-party services to create a complete and user-friendly digital ecosystem of linked financial services.

Domestic Payments: means a payment to a beneficiary domiciled in the country within the Danske Bank Group where the sending account is registered

eArchive: means the electronic mailbox facility accessed via the Online Banking Channel

Electronic Request: means a request by you or any User for a Transaction

Encryption Key: means electronic files used in the e-Safekey, OpenPGP and EDISec security systems being a pair of keys: a private key to create a digital signatures and a public key to confirm the digital signature and encrypt data from the Bank to the Customer or User

eSafeID: is a web-based security solution further described in section 19.3.1

eSafeID Code: means a one-time code created using the eSafeID Device used together with the User ID and the Password for logging on to, and operating, the Online Banking Channel

eSafeID Device: means the device that generates an eSafeID Code

Module: a subset or particular subset of functions within the Online Banking Channel

Module Description: means the bullet-listed description of the functionality of the individual Modules registered under the Access Agreement

Online Banking Channel: is the collective term used to describe our multichannel online platform with a full customer interface, which aims to combine all Bank services with selected third-party services to create a complete and user-friendly digital ecosystem of linked financial services and comprises both District and the Business Mobile Banking App

Password: means, when registering for the Online Banking Channel, the password that you or a User have created to replace the Temporary PIN

Payment Initiation Services: means services of the type described in section 16

Payment Services Regulations: means the European Union (Payment Services) Regulations 2018 (S.I. 6 of 2018) which implemented Directive 2015/2366/EU (PSD2) into Irish law, and any other implementing or supplementary legislation from time to time

Registered Account: means any account registered in the Online Banking Channel in accordance with the Agreement

Screen-scraping: means a computer based programme which copies data from your computer, such as the information on your Online Banking Channel, and translates it so that the information can be displayed to you in a different format

SWIFT MT101: means a request for a payment transfer sent via the SWIFT network

SWIFT MT940: means an electronic account statement received via the SWIFT network

Temporary PIN: means a personal identification number issued and sent by the Bank to a User that consists of four or eight characters and is used by the User to register in the Online Banking Channel

Third Party Provider (or TPP): means an independent provider of Account Information Services or Payment Initiation Services

Transactions: is the collective term for the services and functions of the Online Banking Channel described in section 3

User: means a person who has been authorised by you to act on your behalf via the Online Banking Channel

User Administrator: means a User assigned the User Administrator Privileges as described in section 10.1.2

User Authorisation: means your authorisation of a User, specifying the services, accounts, authorisations and/or rights to which the individual User has access

User ID: means a six-digit number assigned to a User which is stated in the User Authorisation