Terms and Conditions District

Applicable from 6 June 2024

Contents

Part 1 - District – General description
1. Modules and services
2. Logging on to District
3. Transactions
4. Registered accounts
5. Unregistered accounts
6. Foreign cheques
7. Digital Orders
8. Automatic registration for receipt of documents in eArchive
9. Module selection
10. User authorisations
11. Exchange rates
12. Mandate types
13. Other mandates in District
14. District Mobile
15. Data for display from external Service Providers
16. Customer Support

Part 2 - Third Party Providers' access rights
17. Third-Party Providers (TPPs)

Part 3 - District Security System
18. Technical issues

Part 4 - Contractual Matters
19. For business purposes only
20. Changes to District
21. Changes to service and support
22. Changes to these Terms and Conditions
23. Responsibilities and liability
24. Use of data
25. Other terms and conditions

Part 5 - Definitions and Glossary

Introduction

These Terms and Conditions are incorporated into each Access Agreement agreed with a Customer, and together with the terms and conditions that apply to each Registered Account (in the following referred to as the "General Terms and Conditions"), they form the agreement between Danske Bank and the Customer (further referred to as the "Agreement"). Unless otherwise stated, where there is any inconsistency between these Terms and Conditions and the General Terms and Conditions in relation to District, these Terms and Conditions will prevail.

District is a multichannel platform with a full customer interface, which aims to combine various Danske Bank services with selected third-party services to create a complete and user-friendly digital system of linked financial services. District can provide access to account information, payments and many other banking services requested by You.

These Terms and Conditions are divided into the following parts:

- Part 1 – describes the options available in District and how to use the system
- Part 2 – describes third-party access rights
- Part 3 – describes the security requirements for use of District
- Part 4 – describes the contractual aspects associated with the use of District
- Part 5 – contains a list of defined terms

In these Terms and Conditions:
Where these Terms and Conditions refer to "us", "we", "Danske Bank", "the Bank" or "the Danske Bank Group", the reference is to Danske Bank A/S and all of its subsidiaries, branches and entities.

"You", "Your" or "the Customer" means the customer that has entered into an Agreement with the Bank by signing an Access Agreement.

Part 1 – District – General description

1. Modules and services

District comprises separate Modules and services. Your Access Agreement specifies the Modules You have selected.

Each time You select a new Module, it is added to Your Access Agreement and You must sign an updated Access Agreement. Please see section 9 below for further information on the selection of Modules.

District is available in both a web and an app version. The app version, called District Mobile, gives You access to core District functionality.

You accept that by using a digital device (such as a smartphone, tablet or mobile phone capable of accessing the internet or downloading the app) to access District Mobile, You will have access only to a limited range of services.

When a User downloads District Mobile, You accept that these Terms and Conditions apply in relation to the use of District by You or the User.

2. Logging on to District

Solutions for logging on to District include Danske Bank's eSafeID security solution using either an eSafeID device (physical token) or the Danske ID mobile authentication app. Sector IDs such as MitID and BankID in Norway and Sweden are supported for various authentication purposes. However, where eSafeID and Danske ID are the standard options in all markets, sector solutions may vary depending on the Access Agreement Country.

Please find more details on the security solutions available in District in section 18.3 below.

A User is required to enter all elements of the chosen security solution when using District. For the District Mobile application, biometric logon can be enabled after activation of the device/application.

A User who does not use District for a period of five minutes may be prompted to re-enter certain elements of the chosen security solution to continue to use District.

3. Transactions

District allows You to make payments, collect payments and view balances and transactions on Registered Accounts.

Use of the chosen security solution is required to authorise and consent to payments through District. When making a payment via District, a User may be prompted to re-enter one or more of the elements of the chosen security solution. For further information on payments, authorisations and mandates, please see sections 12 and 13 below.

Use of the chosen security solution constitutes Your authorisation of and consent to all services and activities available via District.

4. Registered Accounts

Accounts must be registered in District before You can carry out Transactions.

4.1. Registered Accounts in the Danske Bank Group

The following accounts can be registered in District:

- Accounts held by You and opened in Your name with the Danske Bank Group
- Accounts held by Third Parties, provided that the Third Party 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, subject to availability in Your country (see the description in section 4.2).

4.2. Registered Accounts managed via SWIFT

Accounts held with banks outside the Danske Bank Group with whom we collaborate through the SWIFT network and accounts held with the Danske Bank Group that You wish to use for Transactions via SWIFT MT101 or SWIFT MT940 can also be registered in District as part of an Access Agreement. You can register both Your own accounts and third-party accounts. You and/or the Third Party must conclude an agreement with the account-holding bank concerning payment requests made 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 District, You can make payments into those accounts only. It is not possible to view entries for or make payments from accounts that are not registered in District.

6. Foreign cheques

You can make payments by issuing a cheque. If You and/or a Third Party has an agreement on payment requests via SWIFT MT101, cheques can also be executed outside the Danske Bank Group, provided that this option is included in the agreement between You and/or the Third Party and the external bank. Issued cheques are regarded as banker's cheques, and the amounts are debited from the relevant accounts on the date of issue. You may have the amounts of uncashed cheques deposited in Registered Accounts. If the amounts of uncashed cheques are to be credited Your or a Third Party's account, You or the Third Party must covenant to indemnify the Danske Bank Group if a cheque is subsequently presented.

7. Digital Orders

When the User requests an order or Transaction to be executed in District, such as a payment, this is called a Digital Order. A Digital Order or Transaction is executed when one or two Users with the right mandate type (see section 12) have digitally signed the Digital Order. When a User submits a Digital Order and the order has been executed, we send a digital receipt.

As soon as we have confirmed receipt of the Digital Order, the risk in relation to execution in accordance with the instruction passes to us.

If a payment is authorised on Your behalf but states an incorrect unique identifier for the payee, we are not 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 a fee for this. We store Digital Orders for a minimum of seven years and up to 10 years (depending on the General Terms and Conditions that apply to You). During this period, You and/or the Third Party whose account has been debited may obtain a hardcopy of the request against payment of such fee as may be charged by us for administrative assistance. For further information on fees, please see section 25.2.

7.1. Refusing to execute orders

If we refuse to execute a Digital Order authorised on Your behalf via District, we will notify You of such refusal as soon as possible via District, by telephone, in writing, by secure email, by fax or other reasonable means.

7.2. Orders binding on You

Orders executed in accordance with the information in the Digital Order 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 a Digital Order.

7.3. Cancelling orders

You can change or cancel Digital Orders in accordance with the rules and deadlines provided in the General Terms and Conditions that apply to You.

8. Automatic registration for receipt of documents in eArchive

When You enter into an Agreement, You are automatically registered for digital receipt of documents. The documents are filed in eArchive. You receive the documents in digital form with the same legal effect as physical documents received by post. Third-party accounts linked to Your Agreement are treated as Your own accounts.

8.1. Documents received in digital form

You receive all documents sent digitally by the Bank in eArchive. In special cases, we may send such documents in physical form by post.

If You are a customer of one or more of the Danske Bank Group's entities and You receive documents digitally from such entities, You also receive those documents in eArchive.

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

You can choose to receive the documents in physical form, subject to a fee.

8.2. Access to documents in eArchive

The authorisations granted to an individual User determine the documents that the User can view in eArchive.

For example, a User can always view their own User Authorisation.

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

Users can be granted a specific authorisation to access confidential documents and summaries in eArchive.

8.3. Storing documents

We file the Digital Orders and documents in eArchive for the current year at a minimum plus additional retention time according to the document type. You should be aware, however, that the documents are 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 District. In such case, 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 District, You should copy the documents and store them yourself.

8.4. Termination

If Your Agreement terminates or You change Your customer number or deregister accounts, You can no longer receive documents digitally in eArchive. See section 8.3 on the storing of documents.

9. Module selection

The Access Agreement specifies the Modules that You have selected to form part of Your Agreement with the Bank. The details of each Module are provided in the Module Descriptions that form part of Your Access Agreement.

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 District.

Where You have assigned the Administration Module to a User, You are also required to specify the Administrator Privileges that You wish to assign to the User in question. The User Authorisation specifies what those Administrator Privileges are. Section 10.1 describes the various 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 actively select the Administrator Privileges that the User appointed as an administrator is to have. None of the Administrator Privileges are granted by default. 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
- Logon and blocking
- Payment limit – account
- Card administration

The Bank may from time-to-time update and expand the types of Administrator Privileges available. Any new or additional types of Administrator Privileges will be governed by these Terms and Conditions. You will receive separate notification of any such changes via District or in another suitable manner. Where a User has been granted Administrator Privileges, references to You in these Terms and Conditions are to be construed accordingly, so that anything that an Agreement Administrator does under the terms of the User Authorisation is treated as if it was done by You. If a Third Party has signed a mandate in Your favour, You may delegate this mandate to a User. This is done via the User Authorisation in District.

10.1.1. User Authorisation

For Users granted Agreement Administrator and/or User Administrator Privileges, You must also decide the level of authority that the Users are to have, i.e., whether the User is to be granted

- A 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 individual Users

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 their own User ID, they cannot assign themselves the above Administrator Privileges, nor will the Agreement Administrator be able to create and approve Digital Orders. The setting also applies to the User's Privileges as a User Administrator.

Where an agreement administration and a User 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 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. If circumstances so warrant, the Bank can choose to accept a 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 Administrator 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 their own User ID, they will not be able to assign themselves the above Privileges, nor will the User Administrator be able to create and approve Digital Orders. The setting also applies to the User's Privileges as an Agreement Administrator.

If tbe Bank creates a User with these Admiinistrator Privileges, the User Authorisation form must be printed, signed, and sent to the Bank. If circumstances so warrant, the Bank can choose to accept a Digital Signature.

10.1.4. Agreement information

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

10.1.5. Logon and blocking

If You assign the logon 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 new eSafeID Devices
- Block and unblock User access

10.1.6. Payment limit – account

If You assign the payment limit – account Privilege to a User, You authorise them 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 authorisation
- Two persons jointly (A) authorisation

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

10.1.7. Card administration

If You assign the Card administration Privilege to a User, You authorise them 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, in some cases, the Cardholder will need to enter into separate documentation with the Bank. In such case, You warrant that You will arrange for the Cardholder to sign the required document(s) prior to the issuing of the Card and agree that You will forward such document(s) to the Bank on demand.

10.1.8. Markets Online – Danske FX
A User who is assigned the Markets Online - Dnaske FX Privilege is authorised on Your behalf to create, edit and delete orders related to trading in securities or foreign exchange via District or via the OneTrader Module. For a User to be able to trade securities or enter into foreign exchange contracts on Your behalf, You must execute the applicable mandate for that User in writing.

10.1.9. Notification Centre
The Notification Centre Privilege allows a User to perform the following on Your behalf:

- Create notification subscriptions for Users
- Read notifications received
- Manage User information
- Delete subscriptions for notifications created by Users

The Bank may charge a fee for notifications submitted by the User.

10.1.10. Trade Finance
A User who is assigned Trade Finance Privileges is authorised on Your behalf to create, edit, or delete cases relating to trade finance instructions provided to the Bank using the Guarantees and Trade Finance Module. The various types of authorisations are described in section 12 below.

10.2. Deletion of inactive Users
Notwithstanding the terms in section 10.1, the Bank deletes a User's access to District if the User has not logged on to District for a period of 15 months. Deletion of a User does not affect any other mandates granted to that User.

10.3. Message system
All Users can send messages digitally to the Bank via a secure encrypted line. Users can view only messages that they themselves send and receive in District. Digital Orders cannot be placed via the message system.

10.4. Cancellation of the Administration Module
If You wish to cancel the Administration Module, please contact the Bank. You may be charged a yearly fee for further administration of Your Agreement by the Bank. If the Administration Module is cancelled, then the payment limits that have been authorised will continue to apply to this Agreement. In respect of any accounts opened after the date of cancellation of the Administration Module, payment limits will not apply but payment limits for individual Users will continue to apply. You must contact the Bank in writing if You wish to amend or cancel authorised payment limits 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.

10.5. Changing User Authorisation
If You wish to extend a User's access to District, You must sign a new User Authorisation for District physically or, where possible, using Your Digital Signature in District. This new User Authorisation replaces the previous one. If the change relates to the User's authorisations at account level, You and/or the relevant Third Party may need to sign an account mandate. Note that a User's authorisation in District may be affected if You issue an account mandate.

10.6. Revoking User Authorisations
User Authorisations remain in force until revoked by You in writing - physically or digitally using the chosen security solution where applicable. If You terminate the Agreement, we will construe this as revocation of all User Authorisations granted under the 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.

10.7. Access to accounts
For each User, You must state which accounts the User may view balances and entries for 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.

10.8. Payment limits
Where You have included the Administration Module in Your Agreement, You may manage the limits of Digital Orders created and/or approved through District either at an account level that applies to all Users (known as Payment Limit - account) or at individual Users level (known as Payment Limit - User). It is Your responsibility to create payment limits

suitable for Your requirements. If a Payment Limit – account or a Payment Limit - User is exceeded, payments may not be processed until appropriate action is taken by You. In exceptional circumstances, the Bank may, at its discretion, agree to create a Payment Limit on Your behalf on receipt of written instructions.

10.9. 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 Registered Accounts and unregistered accounts in the same country, within the Danske Bank Group 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 to both 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 mandates 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, that 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 in the relevant jurisdiction within or outside the Danske Bank Group may be processed

- without currency exchange – where no exchange is required (for example when the payment is made in the same currency as the one in which the beneficiary account is denominated)
- at the relevant Fixing Rate
- at the spot rate – a currency exchange rate based on the prevailing market rate at the time and at or within the spreads on our rates (available in District)
- at the agreed rate – a rate agreed in advance with the Bank for the specific payment (You must have an agreement number to use this rate)
- at the forward rate – a rate agreed in respect of a forward contract agreed between us (You must have a forward contract number to use this rate)

Domestic Payments from one currency to another between Registered Accounts processed as an Account Transfer Internal in District are processed at the relevant Fixing Rate.

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.

The mandates are described below.

12.1. Separate mandate

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 holding all other types of mandates.

12.2. Two persons jointly (A mandate)

When requests or payments are created by a User holding an A mandate, they are automatically approved by that User (1st approval). Further approval (2nd approval) by a separate User holding an A, B or C mandate or by a User holding a separate authorisation according to 12.1 is also required. Users holding 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 holding a B mandate, they are automatically approved by that User (1st

approval). Further approval (2nd approval) by a separate User holding an A or C mandate or by a User holding a separate mandate according to 12.1 is also required. Two Users holding B mandates cannot jointly approve a payment.

12.4. Two persons jointly (C mandate)

When requests or payments are created by a User holding a C mandate, they are automatically approved by that User (1st approval). Further approval (2nd approval) by a separate User holding an A or B mandate or by a User holding a separate mandate according to 12.1 is required. Two Users holding C mandates cannot jointly approve a payment.

13. Other mandates in District

13.1. Third-party mandates granted to You

If You wish to make transactions on third-party accounts held with the Danske Bank Group, the Third Party must sign our Third-party Mandate form. If account queries are to be possible using SWIFT MT940 regarding 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) must first be submitted to us.

If You are to 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 must first be submitted to us. The Bank registers the third-party accounts in District via Your Access Agreement. The availability of SWIFT MT101 will depend on third-party banks.

14. District Mobile

14.1. Access and use

To access District through District Mobile You must have completed and signed an Access Agreement and the User must be assigned to the Access Agreement. When a User downloads District Mobile, You accept that these Terms and Conditions apply in relation to the use of District by You or that User via District Mobile In addition, the use of District Mobile is subject to the terms and conditions of the licence under which it may be downloaded from the Apple App Store, Google Play Store.

District Mobile gives access, for instance, to the following content and services:

- View balances
- View transactions
- View transaction history
- Create and approve payments
- Administration

The Bank may from time to time update, extend or reduce the services offered via District Mobile.

14.2. Security

In addition to any other obligations or responsibilities that You may have under these Terms and Conditions, You and each User must take all reasonable steps to maintain the confidentiality of any information shown or stored on the mobile device in connection with the use of District Mobile. You alone are responsible for the safety and security of the mobile device.

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

- Set a PIN on the mobile device, change it regularly and keep Your keypad locked.
- Ensure that You and each User logs off from any District Mobile session as soon as You have finished using the relevant service(s)
- Keep the mobile device in Your possession at all times and do not leave Your mobile device unattended where it may be accessed by unauthorised persons.

15. Data for display from external Service Providers

15.1. Retrieval of data from external Service Providers

A User can retrieve data from a selected range of financial and non-financial Service Providers for display in some of the products and services in District if the User has access to the data via a personalised security solution with the selected Service Provider (the "Integration Process"). The data is retrieved to District using the Service Provider API. Data availability depends on the User's access rights with the Service Provider and in District.

In some cases, access to data from a Service Provider requires additional agreements to be signed, for example the District Access Agreement when a Module is a precondition for obtaining access to data in a product or service in District via the Integration Process. In the event of discrepancy between these terms and conditions and an additional agreement/module providing access to data via the Integration Process in District, the terms of the additional agreement/module will prevail.

15.2. Integration
When a User wants to retrieve data from an external Service Provider for the first time, District redirects the User to the chosen Service Provider. The Service Provider prompts the User to authenticate themselves with relevant personalised security credentials. This is necessary to establish the connection between the Service Provider and District. Danske Bank does not have access to such personalised security credentials.

However, the Service Provider generates a token that uniquely identifies the User and sends it to Danske Bank, which will store the token. When the User uses the product or service in question, Danske Bank sends the token to the Service Provider's API and the Service Provider returns the data.

If a User no longer has valid personalised security credentials with the Service Provider in question, the token is deleted and it is no longer possible for the User to access the data through District. The same applies if the User no longer has access to District or the relevant product or service in District. The User can also remove a connection in the connection overview dashboard in District.

15.3. Warranty of the Customer
You understand and acknowledge that

- any retrieval of data (including personal data) through the Integration Process is done on Your behalf
- through the Integration Process, it is possible to retrieve and display data that does not belong to You and thus may belong to another legal entity or a natural person

You acknowledge and accept the responsibility for any data retrieved from an external Service Provider through the Integration Process and warrant that

- You have all legal rights to use data accessed by a User through the Integration Process and retrieved for display in a product or service in District
- data is not retrieved if any applicable third-party agreement prohibits data from being accessed in this way
- any User using the Integration Process has all legal rights to do so and has been informed of and will comply with these Terms and Conditions when retrieving data via the external Service Providers.

15.4. Data processing
Data retrieved is stored temporarily in the User's browser memory and Danske Bank does not store or share the data or process it in any way other than for the purposes of displaying it in real time to the User.

Danske Bank processes the data only when the User is using the products or services in District displaying the data from the Service Provider.

15.5. Service Provider's Application
Danske Bank is not responsible for the content, accuracy or availability of data retrieved from the Service Provider via the Integration Process and cannot be held liable for any loss or damage (including any indirect or consequential loss) arising under or in connection with the use of the Service Provider APIs and the Integration Process.

15.6. Liability of the Customer
You are liable for and agree to reimburse the Bank for any and all liability, loss, damages, costs, legal costs, professional and other expenses whatsoever incurred or suffered by the Bank, regardless of whether direct, indirect, or consequential, arising out of or in connection with any dispute, claim or proceedings brought against the Bank by a Third Party based on or in connection with Your use of the products and services retrieving data from Service Providers, except if such claim arises out of material breach in respect of the Integration Process, wilful default or fraud for which the Bank is responsible.

16. 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 Your and Users' access to individual elements of support and service, deleting and blocking Users, ordering Temporary PINs and registering changes to authorisations and mandates.

Telephone support may include training, User instruction, troubleshooting assistance, guidance in relation to modifications, and an option to block District. Telephone support in connection with training in and the installation, setup, and troubleshooting, etc. of District 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 District.

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 are provided in cooperation with Your IT department and at Your risk.

Part 2 – Third-Party Providers' Access Rights

17. Third- Party Providers (TPPs)

Through District You can use TPPs' services to access Your account to provide You with account information services, initiate payments from Your account and to make confirmation of funds requests

The use of TPP services does not affect the fees that the Bank charges You for the respective services.

TPPs are independent Service Providers. If we enable a TPP service for You, we will make that clear to You at the time. TPP services can be used to access any of Your accounts that are accessible online. Your account is accessible online unless the General Terms and Conditions or other terms applicable to the relevant account state otherwise.

Through District You can access the following types of services offered by TPPs:

Account Information Services
These services allow account holders to consolidate information about various payment accounts that 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.

Payment Initiation Services
These services help account holders make a range of credit transfers from their account(s).

Card-Based Payment Instrument Issuers
Some TPPs may issue instruments for making Card-Based Payments from an account. Such TPPs may ask us to confirm whether the amount needed for a payment using a card they have issued is available on Your account.

If You use a TPP to make a payment from Your account, You must confirm the details of the payment, including the sort code and account number, or, where applicable, the BIC and IBAN of the Payee and the amount of the payment. When You confirm these details, we process the payment as set out in the relevant General Terms and Conditions or other terms applicable to the relevant account. You should note that payments initiated by a TPP that require authorisation by more than one User (for example, where a User holds a joint mandate to approve payments) are deemed to have been received by us only when we receive final authorisation from an appropriate User. Any payment from Your account using the services of a TPP is made from the account as a credit transfer even if the account is one for which we have issued a Card.

TPPs may provide their services in different ways. Some TPPs use an API to access Your account while others use a technique known as Screen Scraping. The way in which a TPP accesses Your account is important because this affects how these Terms and Conditions apply to You when using TPP services.

If a User consents to a TPP accessing an account using an API, we ask the User to authenticate any TPP requests that we receive by entering the User's personalised security credentials on a secure Bank page – which is not the District logon page. By entering their personalised security credentials, the User gives us the consent to providing information to the TPP, making a payment that they have initiated or responding to a confirmation of funds request, whichever applies. The TPP can view only the information that Your User specifically authorises it to view or to debit the specific payment that Your User authorises.

If the User consents to a TPP accessing the account using Screen Scraping, the User gives us consent to providing information or making payments using that TPP by providing them with the User's personalised security credentials. A TPP accessing the account using Screen Scraping can access all Your accounts (both payment and non-payment accounts), and all the information that Your Users can access in District and can make payments from Your account in the same way that Your Users can. The TPP may ask the User for their personalised security credentials on its own website,

or it may redirect the User to the District logon page via 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 such circumstances, You must provide us with the details of the TPP on request.

The User will be able to revoke TPP access to Your account either

- directly with the TPP by following its procedures
- in District under 'Contact and help' or
- by contacting the Bank directly

You can also obtain a full list of the TPPs to whom Your Users have granted authorisation to access Your account(s) by contacting the Bank. We can only provide this service where the TPP uses an API to access Your account. The User can revoke TPP access to Your account directly with the TPP using its own procedures, if the TPP is using screen-scraping techniques to access Your account.

Where You tell us that You want to revoke a TPP's ability to access Your account, we will comply with such request, but this will not constitute revocation of consent to a payment that has already been debited from Your account or information that has already been provided to a TPP in response to a confirmation of funds request or for Account Information Services.

We will otherwise only 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.

We recommend that You check that the TPP is authorised and regulated by the local regulator or, for accessing accounts held with a branch of the Bank in the EEA, another European regulator before using its services. If the TPP is appropriately authorised and regulated in the jurisdiction where the account is held, 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.

Part 3 – District security system

18. Technical issues

18.1. Transmission and access

To use District, 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 that the necessary adaptations to Your IT equipment are made 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 District.

Users must operate the system directly via the User interface and the software provided by the Bank.

18.2. Distribution, control and storage of software

The Bank distributes the programs You need to use District, which may, for example, be relevant in connection with file exchanging.

18.3. Data security

18.3.1. Logon solutions

Sector IDs (MitID in Denmark and BankID solutions in Norway and Sweden), eSafeID and Danske ID are the authentication solutions supported in District. The logon solutions may be subject to a fee.

18.3.2. Sector IDs

To use sector IDs for logon to District, the following applies:

- It is a condition that the User is registered in Danske Bank's systems with a national registration number or a personal ID number
- It is a condition that the User follows the instructions provided by the issuing authority to order and activate the security solution
- The sector IDs enable the User to log on to District and sign in District without obtaining any other security solution/device from the Bank

18.3.3. eSafeID

eSafeID is the Bank's web-based security system for logging on to District available in all countries where District is offered. eSafeID is a two-factor authentication solution consisting of the following elements:

- a Unique User ID
- a Password
- the Danske ID mobile authentication app

As an alternative to Danske ID, the User can get an eSafeID Device that generates security codes, which can only be used once. When a User is created in District using the eSafeID security solution, the User will receive the above-mentioned credentials. The Bank may charge a fee for issuing eSafeID devices.

The Temporary PIN is system-generated and printed digitally 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 the Bank to cancel it and order a new one.

For security reasons, all credentials require activation before the first use. During activation, the User must set a Password and subsequently destroy the Temporary PIN. The Password must be changed regularly by the User.

If the User has registered a mobile phone number in District, the User has the option of receiving the Temporary PIN via 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 District, 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 District.

18.4. Other security solutions

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.

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.

18.4.1. 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 public EDIsec Encryption Key is confirmed by the fingerprint which the User must make of the Encryption Key and which is exchanged with the Bank in accordance with the guidelines described in the "EDIsec Implementation Guide".

18.4.2. 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 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.

18.4.3. 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 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 Encryption Keys are compromised, You must contact the Bank to have them blocked.

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

The Bank is responsible for ensuring that valid versions of our public EDIsec code and public OpenPGP certificate are always available to You.

18.5. Storing the User ID, Password, eSafeID Device and activated Danske ID app
You must implement effective security procedures to prevent unauthorised use of District, including unauthorised access to Encryption Keys and eSafeID Devices.

The following rules apply to the use of eSafeID and Danske ID:

- Only the User may use the User ID, Password, eSafeID Device and the activated instance of the Danske ID app
- The User ID, Password, eSafeID Device and activated Danske ID app are strictly personal and must not be shared with any Third Party
- The User ID, Password, eSafeID Device and activated Danske ID app may be used only when communicating with the Bank
- The Password must not be written down and stored together with the eSafeID Device or the phone with an active Danske ID app installed
- The Bank recommends that the User store secret codes in crypto hardware to the extent possible
- The User must always use the most recent version of the Danske ID application

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 District and on the Danske Bank Group websites.

18.6. District Mobile Security
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 District Mobile. You and each User are alone responsible for the safety and security of the Device.

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

- Set a PIN on the Device and change it regularly, or use an alternative security function, such as touch ID.
- Keep Your keypad locked, when the Device is not in use;
- Ensure that the User logs off from a District Mobile session as soon as the User has finished using the relevant service(s); and
- Keep the device in the User's possession at all times and do not leave the Device unattended where persons, who are not authorised to use it may access it.

18.7. Deregistering or blocking access
You must notify the Bank if You want it to remove a User's access to District. You must immediately contact the Bank to block User access if

- unauthorised use of a Password, Encryption Key or an eSafeID Device is suspected
- a Third Party has gained access to a Password, Encryption Key, an eSafeID Device or a device with an active instance of Danske ID

Blocking can be requested or cancelled via District or by contacting the Bank. 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.

18.8. The Bank's right to block Your 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 District for objectively justified reasons relating to the security of District 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 as we may choose, and we will lift the blocking of the access to District if the reasons for blocking cease to exist.

The Bank also reserves the right to block Your access to District 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 of this as soon as possible.

If You wish to apply for blocking of Your access to District to be lifted, please contact the Bank. Once the blocking has been lifted, a Temporary PIN may be issued by text message to a User if the User has registered a mobile telephone number.

You must take all reasonable steps to prevent unauthorised use of the District service and unauthorised access to User Encryption Keys, Passwords, eSafeID Devices or devices with active instances of Danske ID.

18.9. Encryption Bans

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

Part 4 – Contractual matters

19. For business purposes only

District is to be used for business purposes only. The information made available to You, including price information, is solely for Your own use.

20. Changes to District

We may at any time extend the scope of District without advance notice, whereas not less than one month's notice is required prior to any reduction in its scope and/or content. We provide written information about changes via District or in another suitable manner.

21. 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 one month's prior written notice via District or in another suitable manner.

We will provide notification of any modifications requiring adaptation of Your equipment to retain the link and access by giving not less than one month's prior written notice via District or in another suitable manner.

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.

Users must operate the system directly via the user interface and the software provided by the Bank.

22. Changes to these Terms and Conditions

We may change these Terms and Conditions upon notice to You. We will notify You one month in advance or otherwise as set out in the General Terms and Conditions that apply to You. Provision of notice and information about the changes is provided via District or in another suitable manner.

The new Terms and Conditions will apply to You unless You have notified us that You do not wish to be bound by the new terms. We then consider the Agreement to be terminated at the time when the new conditions take effect. In some cases, when the changes are in Your favour, the new Terms and Conditions come into force immediately

23. Responsibilities and liability

23.1. Your responsibilities

You use District 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, for example during intermediate handling or processing of data content
- information becoming accessible to Third Parties because of errors or unauthorised intrusion on the data transmission line
- incorrect use or misuse of District 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 District
- that data transferred to District being correct and transferable 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 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
- ensure that You are familiar with the content in eArchive and have set up the relevant notifications in eArchive
- 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 and the requirements of Your business in all other respects
- ensure that the content of the User Authorisation is in accordance with the User's wishes
- where any Password, Digital Signature or Encryption Key relating to Your access to District has been misappropriated or used in an unauthorised manner, notify us by telephoning the Bank or Your Account Manager. You should confirm Your notification by writing to the Bank or Your Account Manager within seven days. Subject to applicable laws, You cannot make any claims against us in respect of errors and omissions resulting from Your circumstances, including non-observance of Your safety and control procedures.

23.2. Our responsibilities
We will be liable if, through error 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 that is part of the security system in District
- 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
- changes in services, information and data supplied by Third Parties in Your security system (that have not been implemented by the Bank),
- Your security system integration with other systems or software that the Bank has not supplied

In areas that are subject to stricter liability, we will not be liable for losses resulting from

- legislation or governmental decisions,
- 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 ourselves or have outsourced the operations
- telecommunication or power failures at our offices
- statutory intervention
- 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. Use of data

24.1. Use of the Customer's data
It is necessary for Danske Bank to process Your data to be able to provide You with the financial solutions and products You have chosen in District and to be able to develop new products and services for our customers in District and as required by law.

Danske Bank and You are each separate data controllers as defined in the GDPR. It follows that If You share or ask the Bank to share data with Third Parties, such data sharing is Your responsibility.

24.2. Use of a User's Data
Any User must share some personal data with us to be able to access and use our services securely. For security reasons, we log Users' access and use of District. Knowing more about Users also means that we may be able to provide products and services in the best possible way.

Please be advised that the name and other identifiers of Users may be shown to other Users.

24.3. Use of Third Party data
If a Third Party has authorised You to operate the Third Party's accounts and use other services on behalf of the Third Party in District, we will be sharing data with the Users on the basis of a signed Third-party Mandate.

Please be advised that the name and other identifiers of the Third Party may be shown to all Users with access to the District Agreement.

24.4. Warranty
When You provide us with personal data, including national personal IDs for a User, You warrant that You are entitled to disclose such personal data to us.

In addition, You confirm that You have previously ensured that the User has been informed where to find information about our processing of personal data.

At the Bank's request, or where public authorities request relevant information, You must 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.

24.5. More information
You can read more about the personal data we register, how we use it and the rights of data subjects in the applicable privacy notice available on the local website. The notice also provides contact information if You have questions.

25. Other terms and conditions

25.1. Structure of the Agreement
The Agreement comprises the following:

- the Access Agreement
- Module Description
- User Authorisation(s)
- these Terms and Conditions
- the General Terms and Conditions and/or other terms and conditions that may apply to the banking services used via District

By signing the Access Agreement, You acknowledge having read and accepted all parts of the Agreement, including these Terms and Conditions, which form an integral part of the Agreement.

New terms of use for services offered in District, including terms of use for services offered by selected Third Parties, may be regularly added, depending on Your current use of the services.

Unless otherwise agreed, if You start to use a service offered in District, 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 Terms and Conditions and other terms and conditions can be viewed on and downloaded from the Bank's website.

25.2. Prices
You must pay subscription and other fees for District in accordance with the at any time applicable list of charges of the Danske Bank entity in the Access Agreement Country, or as otherwise agreed between You and the Bank.

The Bank can change fees and charges for District at one month's notice. Changes to fees and charges are communicated in writing via eArchive in District or in another suitable manner.

The Bank is entitled to

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

25.3. Assignment, transfer and Third Parties
The 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 assignment will not exempt the Bank from liability under the Agreement.

25.4. Termination and breach
You may terminate the 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 and any prepaid charges will not be refunded.

We may terminate the Agreement in writing at any time with an advance notice as set out in the Access Agreement.

We may terminate the Agreement without notice if You breach the Agreement. Breaches include failing to pay amounts due to us, suspending payments generally or becoming subject to insolvency proceedings.

25.5. Law and venue
These Terms and Conditions as well as the Agreement are governed by and must be interpreted in accordance with the laws of the country of the Danske Bank Group entity, with which the Agreement has been concluded.

If You have registered for a Module that is solely intended for use abroad, You accept – to the same extent as the Bank – that it is subject to the legal rules and regulation applying in the country where You operate as well as any specific terms and conditions relating to the specific country and the use of the Module in that country.

25.6. Notices and communication
Notices and other communication between You and the Bank in relation to the Agreement should be given in writing unless

- otherwise agreed between You and the Bank
- the Bank determines otherwise. This may apply, for example, where the Bank needs to contact You urgently.

Notice and other communication from the Bank are delivered in eArchive in District.

The Bank does not deliver notices or other communication on a durable medium and notices and other communication will be provided in another suitable manner.

Part 5 – Definitions and glossary

All definitions used in these Terms and Conditions have the same meanings as defined below.

In these Terms and Conditions,

Access Agreement:
means the agreement between You and us concerning the use of District and the Modules that will be available to You.

Access Agreement Country:
means the country where You have entered into the Access Agreement.

Account Information Services:
means services of the type described in section 17.

Administrator Privileges (or Privileges):
means the rights and privileges granted to a User as described in section 10.1, a full list of which is available in District.

Agreement:
means the complete agreement in relation to District as further described in the introduction to these Terms and Conditions.

Agreement Administrator:
means a User as- signed the Agreement Administrator Privileges as described in section 10.1.1.

API:
means an Application Programme Interface.

Authorisation/Mandate:
means any User Authorisation, account mandate or one of our other mandate forms for District.

Business Days:
means as described in the General Terms and Conditions.

Card:
means the business debit and/or corporate credit card issued by the Bank available in the relevant country.

Card-based Payments:
means payments from Your account made using a card 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 a Card has been issued.

Cross-border Payments:
means payments that cross national borders – even if made in the same currency (such as euros). Local regulations may apply to payments made abroad. This applies to payments both between Registered Accounts and to unregistered accounts.
Payments do not cross borders if made between two accounts in the same country in one of the countries where the Danske Bank Group is represented. Payments handled via SWIFT also do not fall into this category.

Customer:
means the customer of the Bank that has entered into an Agreement with the Bank by signing an Access Agreement.

Danske Bank A/S and the Bank :
means Danske Bank A/S, Bernstorffsgade 40, DK-1577 København V, Denmark, CVR no. 61126228.

Danske Bank Group:
means Danske Bank A/S, all its subsidiaries, branches and entities.

Danske ID:
means the mobile authentication application developed by Danske Bank, which can be downloaded from both Apple App Store and Google Play Store.

Digital Order:
means a request by You or any User for a Transaction.

Digital Signature:
means a Digital Signature generated by a Customer or User using their User ID, Password and Sector ID/eSafeID Code.

District:
means 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 system of linked financial services.

District Mobile:
means the Bank's business mobile banking app available from the Apple App Store or Google Play Store (or such other software application distributor as may from time to time offer a bank business mobile banking application), which enables the digital receipt and transmission of information (including information in relation to a Registered Account).

Domestic Payments:
means a payment to a beneficiary domiciled in a market in which the Danske Bank Group operates and where the sending account is registered.

eArchive:
means the digital archive facility accessed via District.

Encryption Key:
means digital files used in the e-Safekey, OpenPGP and EDIsec security systems as a pair of keys: a private key to create a Digital Signature and a public key to confirm the Digital Signature and encrypt data from the Bank to the Customer or User.

eSafeID:
means a web-based security solution further described in section 18.3.3.

eSafeID Code:
means a one-time code created using the eSafeID Device together with the User ID and the Password for logging on to and operating District.

eSafeID Device:
means a device that comes in various formats. A common feature is that they display a security code to be used when logging on to District with the eSafeID security system.

Fee Account:
means the account(s) specified by You as the account(s) where the Bank are entitled to debit District fees (modules and service fees), transaction fees and other charges under the Access Agreement.

Fixing Rate:
means as set out in the terms and conditions governing the individual accounts.

Module:
means a subset or subset of functions in District.

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

Notice period:
means the notice period set out in the General Terms and Conditions and may vary.

Password:
means, when registering for District, the password that You or a User create to replace the Temporary PIN.

Payment Account:
means an account used for the execution of payment transactions.

Payment Initiation Services:
means services of the type described in section 17.

Registered Account:
means any account registered in District in accordance with the Agreement.

Screen Scraping:
means a computer-based program that copies data from the User's computer, such as the information in District, and translates it so that the information can be displayed to the User in a different format.

Sector ID:
means the different logon solutions as described in section 18.

Service Provider:
means a Third-Party provider as described in section 17 or another entity in the service provider's role.

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

SWIFT MT940:
means a digital 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 District.

Transactions:
means the collective term for the services and functions of District described in section 3.

Third Party:
means a person other than the Customer, including a subsidiary of a Customer, which has signed a Third-party Mandate.

Third-party Mandate:
means a document signed by the Third Party, authorising the mandate holder to operate the Third Party's accounts and use other services on behalf of the Third Party in District.

You:
means you as the Customer.

User:
means a person who has been authorised by You to act on Your behalf via District.

User Administrator:
means a User assigned 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 an individual User has access.

User ID:
means a combination of six characters that is assigned to a User to identify the User and is stated in the User Authorisation

DENMARK
Danske Bank A/S has been licensed by and operates under the supervision of
Finanstilsynet (the Danish Financial Supervisory Authority)
Strandgade 29
DK-1401 København K
Tel. +45 3355 8282
www.finanstilsynet.dk.
The Danish Financial Supervisory Authority has registered Danske Bank's licence under FSA No. 3000.

IRELAND
Danske Bank A/S (trading as Danske Bank), is authorised by the Danish FSA in Denmark and is regulated by the Central Bank of Ireland for conduct of business rules.
www.danskebank.ie

FINLAND
Within the scope of the authority, the operations of the Bank are also supervised by the
Financial Supervisory Authority,
Snellmaninkatu 6,
P.O. Box 103,
FI-00101 Helsinki,
Finland.

The Bank's activities are supervised in respect of consumer issues also by the
Consumer Ombudsman (www.kkv.fi),
Finnish Competition and Consumer Authority,
P.O. Box 5,
FI-00531 Helsinki
Finland,
tel. +358 (0)29 505 3000 (switchboard).

NORWAY
Within the scope of its authority, the operations of Danske Bank, Norwegian branch, are supervised by the
Norwegian Financial Supervisory Authority,
Revierstredet 3,
0151 OSLO
P.O Box 1187 Sentrum
0107 OSLO
Norway

SWEDEN
Danske Bank A/S, Danmark, Sverige Filial Is authorised by the Danish FSA in Denmark and is also supervised by the Swedish Financial Supervisory Authority.

UNITED KINGDOM
Authorised and regulated by the Danish Financial Supervisory Authority (Finanstilsynet). Authorised by the Prudential Regulation Authority. Subject to regulation by the Financial Conduct Authority and limited regulation by the Prudential Regulation Authority. Details about the extent of our regulation by the Prudential Regulation Authority are available from us on request.
Registered Branch in England and Wales, Company No. FC011846, Branch No. BR000080. Danske Bank A/S, a public limited company incorporated in Denmark, CVR No. 61 12 62 28 København.

POLAND
The Bank's operations are supervised by:
Komisja Nadzoru Finansowego (Polish Financial Supervision Authority) whose registered office is situated at the address 20, Piękna str.,
00-549 Warszawa,
in respect of any matters mentioned in the relevant provisions of the Banking Law; and the Danish Financial Supervisory Authority whose registered office is situated at the address Strandgade 29,
DK-1401 København K.