Danske Bank

Terms and Conditions for District

1 February 2023

Introduction 2

Part 1 – District – general description 2
1 Modules and services 2
2 Transactions 2
3 Registered accounts 2
3.1 Registered accounts in the Danske Bank Group 2
3.2 Registered accounts managed via SWIFT 2
4 Unregistered accounts 2
5 Payment by cheque 2
6 Electronic orders 2
6.1 Cancelling orders 2
6.2 Binding orders 3
7 Automatic registration for receipt of documents from Danske Bank in eArchive 3
7.1 Documents received in electronic form 3
7.2 Access to documents in eArchive 3
7.3 Storing documents 3
7.4 Deregistering for eArchive 3
7.5 Expiry 3
8 District user authorisation 3
8.1 User rights 3
8.2 Access to accounts 4
8.3 Confidential payments 4
8.4 Administrator rights 4
8.4.1 Agreement administration 4
8.4.2 User administration 4
8.4.3 Agreement information 5
8.4.4 Access and blocking 5
8.4.5 Payment limit – account 5
8.5 Message system 5
8.6 Changing District user authorisation 5
8.7 Revoking District user authorisations 5
8.8 Access to third-party accounts in District 5
8.9 Mandate to buy/sell currencies and financial instruments 6
8.10 Trade Finance authorisation in District 6
8.11 Authorisation for Collection Service – SEPA Direct Debit in District 6
9 Mandate types 6
9.1 Separate mandate 6
9.2 Two persons jointly 6
9.3 Two persons jointly (A mandate) 6
9.4 Two persons jointly (B mandate) 6
9.5 Two persons jointly (C mandate) 6
10. Data for display from external service providers 6
10.1 Retrieval of data from external service providers 6
10.2 Integration 7
10.3 Warranty of the Company (the District agreement owner) 7
10.4 Data processing 7
10.5 Service Providers Application 7
10.6 Liability of the Company 7
11 Customer Support 7

Part 2 – District security system 8
12 Technical matters 8
12.1 Transmission and access 8
12.2 Distribution, control and storage of software 8
12.3 Data security 8
12.3.1 eSafeID 8
12.3.2 e-Safekey 8
12.3.3 EDIsec 8
12.3.4 OpenPGP 8
12.3.5 EDIsec codes and OpenPGP codes 9
13 Acquiring a user ID, temporary password and eSafeID device 9
13.1 Storing user IDs, temporary passwords and eSafeID devices 9
13.2 Deregistering or blocking the business's or a user's access to District 10
13.3 Danske Bank's right to block the business's or a user's access to District 10
14 Encryption bans 10

Part 3 – Contractual matters 10
15 Business use requirement 10
16 Use of data 10
16.1 Use of business data 10
16.2 Use of personal data 10
17 Changes to District 10
18 Responsibility and liability 11
18.1 Your business's responsibility and liability 11
18.2 Danske Bank's responsibility 11
19 Other terms and conditions 12
19.1 Structure of the District agreement 12
19.2 Prices and fees 12
19.3 Assignment, transfer and third parties 12
19.4 Special provisions concerning payment accounts and the Danish Act on Payments 12
20 Termination and breaches 13
21 Law and venue 13
22 Definitions and glossary 13

DB0208UK 2023.02

Introduction

District 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. District can provides access to account information, payments and many other banking services requested by your company.

These terms and conditions contain a description of District.

Part 1 – describes the options available in District and how to use the system.
Part 2 – describes the security requirements for use of District.
Part 3 – describes the contractual aspects associated with the use of District.

Part 1 – District – general description

1 Modules and services

District is made up of separate modules and services.

The module description describes the modules and services of the chosen District version and/or the separate modules and services.

2 Transactions

In District, you can set up payment collections, make payments, view balances and transactions on accounts registered under your District access agreement, open fixed-term deposit accounts, open payment accounts, carry out cash and liquidity management as well as apply for loans and use the funds once granted. Loan proceeds become available only when Danske Bank has received the loan documentation duly signed by authorised signatories. Payments, payment collections, other transactions and queries are collectively referred to as transactions.

3 Registered accounts

Accounts must be registered with District in order for a business to carry out transactions using District (see below).

3.1 Registered accounts in the Danske Bank Group

Accounts in the Danske Bank Group are accounts set up in Danske Bank or another entity or divisions in the Danske Bank Group under this agreement.

The following accounts in the Danske Bank Group can be registered in District:

- Accounts belonging to your business and opened in the name of your business
- Accounts belonging to third parties, including subsidiaries, provided that the third party or subsidiary has issued a third-party mandate to your business 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 clause 3.2).

3.2 Registered accounts managed via SWIFT

Accounts opened in banks outside the Danske Bank Group and accounts in the Group that you want to use for SWIFT MT101 or MT940/942 transactions can also be registered under your District access agreement. You can register both your own accounts and third-party accounts. You or the third party must enter into an agreement with the bank holding the accounts on Payment Instruction via MT101 or an agreement on Balance Reporting via MT940 (see clause 8.9).

4 Unregistered accounts

If accounts belonging to your business and/or a third party are not registered for District, you can make payments to these accounts only. It is not possible to inquire about balances in or make payments from accounts not registered in District.

5 Payment by cheque

Your business can make payments by printing a cheque drawn on a registered account in the Danske Bank Group.

If you and/or a third party have an agreement covering payment requests via MT101, cheques can also be drawn on registered accounts outside the Danske Bank Group if this option is included in the agreement between your business and/or the third party and the bank outside the Danske Bank Group.

Issued cheques are considered to be bank cheques, and the amounts are charged to the account on the date of issue.

Your business can have the amounts of non-cashed cheques credited to a registered account. If the sum of non-cashed cheques is to be credited to your account or a third-party account, you or the third party must declare that you will indemnify Danske Bank if a cheque is subsequently presented.

6 Electronic orders

When your business or your business's users request an order or transaction to be executed in District, such as a payment, this is called an electronic order.

An order or transaction is executed when one or two users with the right authorisation level (see clause 9 regarding mandate types) have digitally signed the order.

6.1 Cancelling orders

You can cancel payment requests up until and including the day before the business day on which the request was to be executed. Other deadlines apply to cancellation of other orders.

Regarding deadlines for changing or cancelling payment orders (cut-off deadlines), please see:

- Rules on payment authorisation
- Prices and cut-off times – Denmark
- Terms and conditions for transfers to and from Denmark and transfers in foreign currency in Denmark

6.2 Binding orders
Orders executed in accordance with the information in the electronic order are binding on your business. Danske 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 the order.
Once an order has been executed, we send you an electronic receipt.

7 Automatic registration for receipt of documents from Danske Bank in eArchive

When you enter into a District agreement, your business is automatically registered for receipt of electronic documents from Danske Bank. The documents are filed in your eArchive in District.

Your business receives the documents from Danske Bank in electronic form with the same legal effect as ordinary mail in hardcopy.

Third-party accounts linked to your District agreement are treated as your own accounts.

7.1 Documents received in electronic form
Your business receives all documents sent electronically by Danske Bank in eArchive. In special cases, Danske Bank may send such documents in hardcopy by ordinary mail.

If your business is a customer of one or more of the Danske Bank Group's other entities, and you receive documents electronically from these, you also receive those documents in District.

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 in District, and not by post.

7.2 Access to documents in eArchive
The authorisations granted to an individual user determine the documents that the user can view. For example, a user is always able to view the user's own user authorisation in District.

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

7.3 Storing documents
We file the electronic orders and documents in eArchive for the current year plus seven years as a minimum. You should be aware, however, that the documents will be deleted if you deregister an account or change customer number, or if your business changes bank or for some other reason no longer has access to District. 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 Danske Bank offers via District, you should copy the documents and store them yourself.

7.4 Deregistering for eArchive
Contact Danske 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.

7.5 Termination
If your District agreement terminates or you change your customer number or deregister accounts, you can no longer receive electronic documents in eArchive. See clause 7.3 on storing documents.

8 District user authorisation

Users must be duly authorised to perform transactions in District on behalf of your business or third parties. This authorisation can be set up via Danske Bank's District user authorisation form.

If a third party has signed a mandate for your business, you can delegate this mandate to your users. You can do this using the District user authorisation form.

If the user needs to execute transactions via the cashier's desk, your business must sign the MANDATE - CORPORATE CUSTOMER.

8.1 User rights
You must decide what user rights each user should have:
- Payments between registered accounts in the same country in the Danske Bank Group
- Payment requests via SWIFT MT101
- Payments to unregistered accounts in or outside the Danske Bank Group – including payments via payment forms and MobilePay Payout. Payments via MobilePay Payout require an agreement with Danske Bank on MobilePay Payout
- Cross-border payments to registered and unregistered accounts with Danske Bank Group or elsewhere
- Creation of custody accounts, adding and removing financial instruments to/from custody accounts
- Other products and services

You must also decide which authorisation that should be assigned to a user for each user right.

You can choose between the following types of authorisation/ rights:
- View balances etc.
- Create/deposit
- Approve – two persons jointly
- Approve alone

The selected mandate is used by default for all payments under the given transaction type. If you have chosen a more restrictive mandate at account level (account access is described in clause 8.2), this applies to payments made to unregistered accounts and cross-border payments. It will also be regarded as a limitation if you have chosen not to assign a mandate at account level, as this means that the user has view access to the accounts only.

8.2 Access to accounts
For a user to be authorised to make payments to unregistered accounts and cross-border payments, the user must have a mandate at account level.
For each account to which the user has access at account level, a decision must be made regarding the user's level of authority:

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

The account mandate types are described in clause 9.
The selected account level mandate applies to all the District agreements for which the account is registered.

8.3 Confidential payments
Your business must decide whether the user is to be authorised to make confidential payments. Confidential payments are payments such as salaries, which may be seen, created or approved only by users with this right.

Users will have authorisation to make confidential payments within the types of transaction to which you have given the user access.

No distinction is made between confidential and non-confidential payments in relation to viewing balances etc.

8.4 Administrator rights
If District Administration is included in your agreement, you must decide whether the user should be assigned administrator rights in the form of
- agreement administration
- user administration
- agreement information
- access and blocking
- payment limit – account

When granting agreement and/or user administration rights, you must decide which of the following mandates the user should be assigned:
- Create/deposit
- Separate mandate
- Two persons jointly

The 'agreement information' and 'access and blocking' rights may be granted as separate mandates only.

8.4.1 Agreement administration
If you assign a user the 'agreement administration' right, you authorise the user (under the chosen mandate, see above) to do the following on behalf of your business:
- request that the agreement administration right be assigned to or changed for users
- delete users' agreement administration rights
- create, change and delete users' user administration rights – see clause 8.4.2
- create and delete users' agreement administration rights – see clause 8.4.3
- create and delete users' access and blocking rights – see clause 8.4.4
- create, change and delete users' payment limit – account rights – see clause 8.4.5

A user with these rights 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 rights. Nor will the agreement administrator be able to create and approve payment orders. The setting also applies to the user's rights as a user administrator.

Where an agreement administration right is assigned, this must always be signed by your business's authorised signatories. When a user with the agreement administration right has requested that a user authorisation with agreement administration rights be created, a District user authorisation form with a signature field is generated and made available in the District eArchive.

The user authorisation form is available to users with the agreement information right. The user authorisation must be signed and sent to Danske Bank. In other cases, the user approves and signs using his or her digital signature.

Users with the agreement administration right must also be assigned the user administration right.

8.4.2 User administration
If you assign a user administration right 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 user's data, including master data

A user with these rights 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 rights. Nor will the user administrator be able to create and approve payment orders. The setting also applies to the user's rights as an agreement administrator.

8.4.3 Agreement information
If you grant a user the 'agreement Information' right, 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 rights, access to accounts and payment access).

The user has access to the user list and selected documents shown in District.

8.4.4 Access and blocking
If you assign the access and blocking right to a user, you authorise the user to do the following on behalf of your business:

- Order temporary passwords for users
- Order eSafeID devices and complete activation of a new eSafesID
- Block and unblock user access

8.4.5 Payment limit – account
If you assign the payment limit – account right to a user, you authorise him or her to do the following on behalf of your business:

- Create, change and delete payment limits for the accounts that the user can manage under the agree-ment at any time

When granting the payment limit – account right, you must decide which of the following mandates the user should be assigned:

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

See the description of our account mandate types in clause 9

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

8.6 Changing District user authorisation
If you wish to extend or restrict a user's access to District, a new District user authorisation must be signed to replace the existing authorisation. If the change relates to the user's account mandates, you must sign an account mandate and third parties must sign a new third-party mandate.
If the changes are made by an agreement and/or user administrator under the agreement via District Administration, the changes must be approved by digital signing.

If the change also covers agreement administration rights, a user authorisation must also be signed in accordance with the business's signatory rules (see clause 8.4.1).

A user's District authorisation may be affected if the business issues an AUTHORISATION FORM – BUSINESS.

8.7 Revoking District user authorisations
District user authorisations apply until you revoke them. You can do this in writing by contacting the branch, or using digital signing where this is possible. Authorisations may also be revoked by telephone, but such revocation must always be confirmed in writing immediately afterwards. The user's access to act on behalf of your business via District is blocked after the telephone call.

When Danske Bank has received notice of revocation, we confirm in writing that the user ID and the user's eSafeID device have been deleted in our systems.

If you terminate the full District access agreement, we see this as revocation of all user authorisations issued under the agreement.

If you and/or a third party have given the user an account mandate, this mandate must be revoked separately. Merely revoking the user authorisation for District is not sufficient.

8.8 Access to third-party accounts in District
If you need to perform transactions on third-party accounts or create/manage third-party financial instruments in custody accounts in the Danske Bank Group, the third party must sign Danske Bank's third-party mandate.

You must enter into a special agreement with Danske Bank if you need to be able to view third-party accounts outside the Danske Bank Group, as this must be done via SWIFT using MT940.
The third party must also enter into an agreement with the account-holding bank that the Danske Bank Group may receive information about the third party's accounts with the third-party bank(s).

You must enter into an agreement with Danske Bank if you need to be able to make payments from third-party accounts outside the Danske Bank Group. The third party must also enter into an agreement with the account-holding bank to the effect that the Danske Bank Group may send payment instructions to the third-party bank(s).

The third party must sign Danske Bank's third-party mandate in order for you to be able to open a custody account and/or deposit/withdraw financial instruments to/from the custody account on behalf of a third party.

Danske Bank registers third-party accounts for District via your access agreement.

8.9 Mandate to buy/sell currencies and financial instruments

In order to be able to view trade positions, buy and sell foreign currency spot and forward and trade Danish and foreign shares, bonds and investment certificates, the user must have access to one or more of the Markets Online modules. Access to foreign currency trading spot and forward and trading in shares, bonds and investment certificates also requires that you issue the Foreign Ex-change Transactions and/or Securities Transactions authorisation to the user in question.

Such authorisation authorises the user only to enter into transactions on your business's behalf via Markets Online.

All transactions related to the purchase of foreign currency spot and forward are subject to the conditions in the framework agreement on netting and final settlement for transactions entered into between your business and Danske Bank.

8.10 Trade Finance authorisation in District

If a user is to be able to issue documentary credits, collect debt and/or issue guarantees, you must register the user in the Trade Finance module and sign the Connection to/Modification of the Trade Finance Module agreement in District.

In so doing, you decide whether the user should have access to
- documentary credits (exports and/or imports)
- debt collection (exports and/or imports)
- guarantees

You must also decide whether the user should be able to
- create and view balances etc.
- create and approve jointly with another person, or
- create and approve separately

8.11 Authorisation for Collection Service – SEPA Direct Debit in District

If a user needs to be able to generate SEPA Direct Debit collection collections, your business must register the user for the Collection Service – SEPA Direct Debit module.
The user will then have access to
- collection
- reimbursements
- revocations

on euro accounts linked to District.

9 Mandate types

Danske Bank uses the following types of mandate:
- Separate mandate
- Two persons jointly (A mandate)
- Two persons jointly (B mandate)
- Two persons jointly (C mandate)

Using these mandates, you can decide which users, jointly or alone, who may approve payments or orders. The mandates are described below.

9.1 Separate mandate

Orders or payments created or changed by a holder of this mandate are automatically deemed to be approved by the user. Users with this mandate may also approve orders or payments entered by users with all other types of mandate.

9.2 Two persons jointly

When a payment order or payment is created by a user with a 'two persons jointly' mandate, another (second) approval is required from a user with the same type of mandate.

9.3 Two persons jointly (A mandate)

When an order or payment is created by a user with an A mandate, it is automatically approved by this user (first approval).

The order or payment requires another (second) approval from a user with either a separate or an A, B or C mandate. Users with an A mandate are pari passu, and the approval order is therefore not important.

9.4 Two persons jointly (B mandate)

When an order or payment is created by a user with a B mandate, it is automatically approved by this user (first approval).

The order or payment must then be approved (second approval) by a user with either a separate or an A or C mandate. Two users with a B mandate cannot approve a payment together.

9.5 Two persons jointly (C mandate)

When an order or payment is created by a user with a C mandate, it is automatically approved by this user (first approval).

The order or payment then requires another (second) approval from a user with either a separate or an A or B mandate. Two users with a C mandate cannot approve a payment together.

10 Data for display from external service providers

10.1 Retrieval of data from external service providers

Users 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 take priority.

10.2 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, who stores 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 be 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.

10.3 Warranty of the Company (the District agreement owner)

The Company understands and acknowledges that

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

The Company acknowledges and accepts responsibility for any data retrieved from an external service provider through the Integration Process and warrants that

- the Company has 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

10.4 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.

10.5 Service Providers Application

Danske Bank is not responsible for the content, accuracy or availability of the data retrieved from the service provider via the Integration Process and shall not 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.

10.6 Liability of the Company

The Company is liable for and agrees to reimburse Danske Bank for any and all liability, loss, damages, costs, legal costs, professional and other expenses whatsoever incurred or suffered by Danske Bank, regardless of whether direct, indirect, or consequential arising out of or in connection with any dispute, claim or proceedings brought against Danske Bank by a third party based on or in connection with the use by the Company 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 Danske Bank is responsible.

11 Customer Support

Danske Bank provides support and service for your business, in the form of

- user administration
- telephone support, including blocking service in District
- internet-based support
- on-site support

User administration includes establishing service agreements and authorisations, modifying the access of your business and its users to individual elements of support and service, deleting and blocking users, ordering temporary passwords 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 District.
Telephone support in connection with installation, setup, training and troubleshooting, etc. of District is provided in cooperation with your business's IT department and at your risk.

Internet-based support may include training, user instruction, troubleshooting assistance and guidance in relation to modifications. Internet-based support is provided in cooperation with your IT department and at your business's risk. On-site support may include configuring and providing training in the use of District and troubleshooting.

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 business's risk.

Part 2 – District security system

12 Technical matters

12.1 Transmission and access
In order to use District, you must establish a data communication link with Danske Bank. You must bear all related expenses and purchase, install, set up and maintain the IT equipment required. You must also arrange for any adaptations to your IT equipment that may be required – to use the connection as well as to 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 Danske Bank.

12.2 Distribution, control and storage of software
Danske Bank distributes the programs you need to run District, which may, for example, be relevant in connection with file exchanging. The programs can be downloaded from the internet.

When you download programs from the internet, you or a user must check that the program delivery is digitally signed by Danske Bank.

If the programs are not digitally signed by Danske Bank, it may be because they have been changed or do not come from Danske Bank. The signature can subsequently be verified by checking 'properties' for the downloaded program file(s). If you discover that the digital signature is not Danske Bank's, you may not install the downloaded program.

12.3 Data security
eSafeID, e-Safekey, OpenPGP and EDISec are the general security systems used in District.

e-Safekey, OpenPGP and EDISec are Danske Bank's security systems for customers who want to exchange information digitally with Danske Bank directly through their own business systems. e-Safekey, OpenPGP and EDISec are based on a password and use permanent code files 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.

12.3.1 eSafeID
eSafeID is Danske Bank's web-based security system for logging on to District. eSafeID is a two-factor authentication solution, based on something you know and something you have: a personal 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 District.

When a user is created in District using the eSafeID security system, the user receives a personal user ID, a temporary password and an eSafeID device. The user must activate the eSafeID device and create a personal password before the eSafeID security system can be used to access District.

Activation of the eSafeID device requires two-factor identification, of which the password/temporary password constitutes the first factor. If the user registered a mobile phone number when the user was created in District, an activation code can be sent as a text message and will constitute the second factor. If the user registered using his or her civil registration (CPR) number, activation is NemID supported. Alternatively, the agreement administrator may complete the activation of a user without the above options.

Users who have already been created and who receive a new eSafeID device must activate it before it can be used. The activation procedure is the same as that described above.

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

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

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

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

When a user is to be created using the OpenPGP security system, Danske Bank allocates a personal user ID and a temporary password to the user. The customer must generate the customer's own OpenPGP codes and send them to Danske Bank together with the temporary password in accordance with the instructions described in the OpenPGP Security Implementation Guide from Danske Bank.

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

The customer is 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.

12.3.5 EDIsec codes and OpenPGP codes

For EDIsec and OpenPGP, the customer is responsible for using valid codes and securing data communication with Danske Bank. The following applies specifically:

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

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

Danske Bank is responsible for ensuring at any given time that valid versions of Danske Bank's public EDIsec code and public OpenPGP certificate are available to the customer.

13 Acquiring a user ID, temporary password and eSafeID device

When a user is created in District using the eSafeID security system, the user receives a personal user ID, a temporary password and an eSafeID device. Together with the eSafeID device, the temporary password is used for first-time identification when the user is registered in the system.

When a user is created using the EDIsec or OpenPGP security system, the user receives a user ID from Danske Bank. In OpenPGP, the user also gets a temporary password, which is used for first-time identification of the user.

The temporary password is machine-created and printed without anybody seeing it. If the letter containing the temporary password and/or the letter containing the eSafeID device has been tampered with or is not intact, the user must contact Danske Bank to order a new eSafeID device or a new temporary password. For security reasons, the letters containing the eSafeID device and the temporary password are sent at different times.

If the user has not received the letter containing the temporary password within seven business days of ordering, the user must, for security reasons, contact Danske Bank to cancel it and order a new one.

If the user has registered a mobile phone number in District, the user has the option of receiving the temporary password via text message. If the user does not receive a text message containing the temporary password within 15 minutes of ordering it, the user must, for security reasons, contact Danske Bank to cancel it and order a new one. When registering in the security system, the user must select a personal password and delete the temporary password. Danske Bank is not liable for any errors or losses resulting from the user or administrator not being able to update the user's mobile phone details in District.

During registration, the user creates his or her own password. The password must be changed regularly, and it is your responsibility to ensure that this happens. The user must then destroy the temporary password.

13.1 Storing user IDs, temporary passwords and eSafeID devices

You must implement effective security procedures to prevent unauthorised use of District, including unauthorised access to user code files and eSafeID devices.

The following rules apply to the use of eSafeID, e-Safekey, OpenPGP and EDISec:

- Only the user may use the user ID, password and eSafeID device.
- The password, eSafeID device and codes are strictly personal and may not be disclosed to third parties.
- The password and codes may be used only for communication with Danske Bank (except for OpenPGP, which the customer may use in other contexts)
- You may not write down the password and store it with the eSafeID device.
- Danske Bank recommends that the customer store secret codes in crypto hardware to the extent possible.

Further information about security recommendations is available under the Security menu in District, on the websites of Danske Bank and in other guidelines.

13.2 Deregistering or blocking the business's or a user's access to District

You must notify Danske Bank if you want it to remove the business's or a user's access to District. You must immediately contact Danske Bank to block user access if

- unauthorised use of a user's personal password, your business's or a user's code file or an eSafeID device is suspected
- third parties have gained access to a personal password or code file or an eSafeID device

Blocking can be requested or cancelled via District, telephone or one of Danske Bank's branches. If the request is made by 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 Danske 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 Danske Bank has been notified that the transactions must be deleted and confirms that this is possible.

A user with administration rights may also delete and block a user's access to District, see sections 8.4.2 and 8.4.4.

13.3 Danske Bank's right to block the business's or a user's access to District

Danske Bank reserves the right to block your business's or a user's access to District if we detect an attempt at unauthorised use. Danske Bank also reserves the right to block your business's access to District if your business's equipment, software or interfaces damage, interfere with or in any other way cause inconvenience to Danske Bank or its IT infrastructure. If access is blocked, you will be notified of this as soon as possible.

14 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 3 – Contractual matters

15 Business use requirement

District may be used only for business purposes. The information you receive access to, including price information, is for your own use only and may not be passed on to third parties without our prior written consent.

16 Use of data

16.1 Use of business data

It is possible for your business to give Danske Bank access to certain financial data by agreement, with a view to being offered customised solutions for your business in District and Danske Bank's analyses of such data. If Danske Bank anonymises this data, it may also use it for other purposes.

16.2 Use of personal data

You consent to Danske Bank's use of personal data related to users when they are registered as users in District, in accordance with the Danish Act on Processing of Personal Data (Persondataloven). Danske Bank may via District collect data on a user's IP addresses, logon times, business communications between users and Danske Bank and other data that Danske Bank deems to be relevant to the operation of District.

Functions in District may be carried out for Danske Bank by third parties on their servers, in accordance with the requirements and regulations of the Danish Act on Processing of Personal Data.

We register and use data about you to offer you the best advice and solutions, and to comply with the legal requirements that apply to us as a financial institution. You can read more about which data we register, how we use it and your rights in our privacy notice on Danske Bank's website. The notice also provides contact information if you have questions.

17 Changes to District

District provides access to the services Danske Bank offers. Danske Bank may at any time extend or reduce the content of District.

Danske Bank may without notice modify own equipment, basic software and related procedures, to ensure the best possible operating conditions and service levels. Danske Bank will notify the business of any modifications requiring adaption of the business's equipment by giving 30 days' written notice. We will inform you of any changes in District, where relevant, by letter or the like.

Danske Bank may extend the scope of District without notice. When the bank adds new services to District this will not require new signatures form your business,
provided that the new services are advantageous to your business and do not imply any material cost increase. If Danske Bank reduces the scope and/or content of District, Danske Bank will provide a 30 days prior notice, unless the changes are required by law.

We may change these Terms and Conditions without notice. Information on the changes will be provided in District, where relevant, by letter or in the daily press.

The new Terms and Conditions will apply to your business, unless you have notified us that you do not wish to be bound by the new terms.

If you notify Danske Bank that you do not wish to be bound by the new rules, we may regard the contractual relationship as terminated as from the effective date of the new Terms and Conditions.

18 Responsibility and liability

18.1 Your business's responsibility and liability

Use of District is at your own responsibility and risk.

This includes – but is not limited to – the risk associated with

- transmission of data to Danske Bank, as well as the risk that transmitted data is destroyed, lost, damaged, delayed or affected by transmission errors or omissions, e.g. during third-party handling or processing of data content
- information being passed on to third parties as a result of errors or unauthorised intrusion on the data transmission line
- all operations and transactions made using your own code or that of a registered user
- ensuring that users keep their personal passwords secure so that no third party becomes aware of them
- ensuring data security in connection with storage of user codes in the business's IT environment to prevent unauthorised access to the codes
- any incorrect or unauthorised use of District by registered users
- unauthorised use of District
- that data transferred to District is correct and can be transferred for the intended use

You cannot hold Danske Bank liable for any consequences thereof. Nor can you raise any claims against Danske 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

- verify that the terms of the user authorisations are consistent with the authorisations and mandates that you and any third party have granted users
- ensure that the terms of a user authorisation are in accordance with the requirements of your business in all other respects
- open and check all electronic documents sent by Danske Bank just as if they had been sent in hardcopy by ordinary mail
- notify Danske Bank if you will not have access to District for a certain period and consequently wish to receive electronic documents in hardcopy by ordinary mail

It is also your responsibility to ensure that user(s) know the terms and conditions for District and the various modules, and that each user complies with them and follows the instructions in the help texts displayed on the screen.

When the customer, or anyone on behalf of the customer, provides Danske Bank with personal data (such as name and personal identification number), the customer warrants that it is entitled to disclose such personal data and that the data subject has consented to Danske Bank's processing of the personal data for the use of the product in accordance with these terms and conditions. In addition, the customer warrants that the data subject has in due time received the requisite information about Danske Bank's processing of personal data as set out in Danske Bank's Privacy Notice. Danske Bank's Privacy Notice, as amended from time to time, may be found on Danske Bank's website.

At Danske Bank's request, or where public authorities request relevant information, the customer shall provide Danske Bank with documentation enabling Danske Bank to demonstrate that there is an appropriate and valid legal basis under GDPR for Danske Bank's processing of personal data as mentioned above.

18.2 Danske Bank's responsibility

Danske Bank is liable for the tardy or defective performance of its contractual obligations resulting from error or negligence.

Danske Bank is not liable for errors or omissions resulting from

- users disclosing their temporary PIN and/or personal passwords
- modifications to the security system (not performed by Danske Bank)
- the security system's integration with other systems or software not supplied by Danske Bank
- services, information and data supplied by third parties

Even in areas of stricter liability, Danske Bank is not liable for losses arising from

- breakdown of or failure to provide access to IT systems or damage to data in such systems due to any of the factors listed below, regardless of whether or not Danske Bank or a third-party supplier is responsible for the operation of such systems
- power failure or a breakdown of Danske Bank's telecommunications, legislative or administrative intervention, acts of God, war, revolution, civil unrest, sabotage, terrorism or vandalism (including computer virus attacks or hacking)
- strikes, lockouts, boycotts or picketing, regardless of whether Danske Bank or its organisation is itself a party to or has started such conflict and regardless of its cause (this applies even if the conflict affects only part of Danske Bank)
- other circumstances beyond Danske Bank's control

Danske Bank is not exempt from liability if

- Danske Bank ought to have foreseen the cause of the loss when the agreement was concluded or ought to have avoided or overcome the cause of the loss
- under Danish law, Danske Bank is liable for the cause of the loss under any circumstances

Danske Bank is liable only for direct losses and thus not for indirect losses or more extensive adverse effects, even where such effects are the result of errors made by Danske Bank.

Danske Bank is liable for damages in accordance with the rules in clause 17.2 above. Section 104 of the Danish Payment Services Act (Lov om betalinger) therefore does not apply.

19 Other terms and conditions

19.1 Structure of the District agreement

A District agreement consists of the following documents:

- District – access agreement
- District – user authorisation(s)
- Module description for District
- Terms and conditions for District
- General conditions
- Rules on payment authorisation
- Prices and cut-off times – Denmark
- Danske Bank District – prices for companies in Denmark
- Prices, terms and conditions for transfers to and from Denmark and transfers in foreign currency in Denmark
- Help documents and programs

All the documents form an integral part of the District agreement when you sign the access agreement.

In case of discrepancies between the rules and conditions listed above, they take precedence in the order listed.

The conditions and rules linked to the various module agreements or the access agreement also apply.

When you sign the District access agreement, you acknowledge having read and accepted these terms and conditions and rules as 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 business's current use of the services.

Unless agreed otherwise, if your business begins using 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.

The terms and conditions for District and other business terms and conditions can be viewed on and downloaded from Danske Bank's website.

19.2 Prices and fees

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.

Danske Bank is entitled to group and debit fees more than one month after the transaction to which they relate has been processed.

Danske Bank is entitled to charge a fee for delivering supplementary details or information at more frequent intervals than agreed when the District agreement was concluded.

Danske Bank may charge a fee for payments that you make from an account and for providing you with details about payments made.

Changes to prices and fees are effected as described in Danske Bank's General conditions. Changes are announced in District, in the daily press or by letter.

19.3 Assignment, transfer and third parties

This agreement has been concluded by Danske 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 Danske Bank may assign or transfer its rights and obligations under the agreement to another entity of the Danske Bank Group at any time.

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

19.4 Special provisions concerning payment accounts and the Danish Act on Payments

Payment services are governed by the Danish Act on Payments.

Unless otherwise stipulated by these terms and conditions or agreed with us, Danske Bank has deviated from the provisions of section 6 of the Act to the extent permissible.

If you are entitled to operate a payment account by way of a special payment instrument, such as a debit card, such operation is governed by the provisions of the agreements covering the payment instruments concerned. See also Terms and Conditions for Payment Accounts.

You are obliged to check entries in your accounts and custody accounts regularly. If the list contains transactions that you do not believe you have authorised, you must contact Danske Bank as soon as possible, and no later than four months after the amount was debited to the account.

Danske Bank is entitled to charge a fee for assisting you with reversing amounts that have been transferred to the wrong person by mistake, because the wrong identification code was provided.

This also applies if you send a payment collection in District, which is later found to be unauthorised and the debtor demands repayment.

20 Termination and breaches

You may terminate the access agreement at any time by giving us written notification. Orders and agreements that have been concluded prior to termination will be executed. Subscription fees and any prepaid charges are not refunded.

Danske Bank may terminate the access agreement giving 30 day's written notice.

However, we may terminate the agreement without notice if you breach the agreement or the terms and conditions for District. Breaches include failing to pay as agreed in the access agreement, suspending payments, becoming subject to bankruptcy proceedings or other insolvency administration, initiating composition negotiations or becoming subject to distraint or arrest of property.

21 Law and venue

This agreement is governed by Danish law and jurisdiction. If you have registered for a module, which is to be partially or completely used abroad, you (in the same way as Danske Bank) accept that the foreign banks' business conditions and the local laws and practices apply to execution of the transaction.

22 Definitions and glossary

- **API** – An API (Application Programming Interface) provides the technological means to connect District with external service providers in an automated manner in order to display external data to a User. It differs from a file transfer in that a file transfer refers to an exchange of data for which the User must manually transfer a file by downloading or uploading it.
- **Business days** – Saturdays, Sundays and public holidays, including 5 June, 24 December, 31 December and the Friday after Ascension Day, are not business days in Denmark.
- **Basic products** are simple banking products such as accounts.
- **Payment accounts** are accounts used for the execution of payment transactions.
- **Payments between registered accounts** are payments between registered accounts in the same country, within the Danske Bank Group.
- **User** – a person (for example an employee) who has been authorised by the business to act on the business's behalf via District. Where there is direct integration between the business's and Danske Bank's IT systems, a user can also be a computer system or a system at the business.
- **User ID** is a 6-digit number assigned to a given District user. The user ID is shown in the user authorisation.
- **User authorisation** – the business's authorisation for users, specifying the services, accounts, mandates and rights of a given user.
- **District** is the general name for Danske Bank's Internet-based payment and information systems for businesses.
- **Data delivery** is the transfer of data between the customer and bank. A data delivery can contain payment instructions, for example.
- **Digital signature** – an electronic signature which is given during binding transactions, such as payments, and when connecting to Danske Bank.
- **Business Online** - is the former designation for Danske Bank's Internet-based payment and information systems for businesses. A reference to Business Online is therefore a reference to District.
- **Temporary PIN** – a code issued and sent by Danske Bank to the business's user(s). The code contains four or eight characters, and is used by the business's user(s) for security registration in District.
- **eSafeID** – a web-based security system used to log on to District. eSafeID is a two-factor security system which consists of something the user knows (personal password), and something the user has (an eSafeID device).
- **e-Safekey** is a security system in the programs mentioned.
- EDISec is a security system used for connections other than within the above programs.
- **Confidential payments** are payments (such as salaries) which may only be seen or processed by users with special rights.
  Payments marked as confidential are accessible for processing only by users who have this right.
- **User authorisation** – an authorisation to use District.
- **Mandate** – a business mandate, District account mandate or one of Danske Bank's other mandate forms for District.
- **Mandate holder** – one or more associated authorities and/or natural persons who have been granted a mandate.
- **Cross-border payments** are payments, which 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.
- **Instruction** – an electronic, written or oral order to Danske Bank to carry out changes, transactions, etc.
- **Temporary password** – a code issued and sent by Danske Bank to the business's user(s).
- **The code contains** four or eight characters, and is used by the business's user(s) for registration in District.
- **Module agreement** – an agreement containing provisions for the given module, e.g. Trade Finance, Collection Service, etc.
- **Module description** – an itemised description of the functions in the various modules registered under the agreement.
- **Codes** – used in connection with user IDs and personal passwords when logging on to District using the eSafeID security system. Codes can be used only once.

- **Code files** are electronic files used in the e-Safekey and EDISec security systems. Each user generates a code file (containing a code pair) – a private code that is used to create digital signatures, and a public code that is used to verify the digital signature and encrypt data from Danske Bank to the customer.
  Each user has their own secret code file, so that the user can generate unique, personal digital signatures. Access to the code file is protected by the user's personal password. The code file is stored in the business's IT system.
- **eSafeID** devices are personal and may take various forms. They are all capable of displaying a code to be used when logging on to the District system using the eSafeID security system.
- **Customer support** – a help function in Danske Bank, which provides technical or general support to District users via telephone.
- **On-site support** – training or technical or other assistance provided by Danske Bank at the business's premises.
- **Personal password** – a password, which protects the user's secret code that is used to generate digital signatures. The code is 8-16 characters long and should contain upper and lower case letters, numbers and symbols.
- **Security registration** – the registration procedure users go through before District may be taken into use.
- **Master data** – first name, middle name, last name, username, customer number, civil registration (CPR) number/assigned customer number and associated business address.
- **Access agreement** – an agreement between your business and Danske Bank on the use of District.
- **Transactions** – payments, payment collections, other movements of funds and queries in District.