Terms and Conditions for Business Online

15 June 2014

Danske Bank A/S
CVR-nr.: DK-61 12 62 28 - København

Introduction

Business Online is Danske Bank's Internet-based office-banking system, which provides access to account information, payments and other banking transactions requested by your company.

In the Terms and Conditions for Business Online,you will find a description of the system.

Part 1 – describes the options available in Business Online and how to use the system.
Part 2 – describes the security requirements for Business Online users.
Part 3 – describes the contractual aspects of connecting to Business Online.

Part 1 – Business Online – general description

1. Modules and services

Business Online comprises separate modules and services.

The module description outlines the modules and services contained in the chosen version of Business Online and/or the separate modules and services.

2. Transactions

Business Online allows you to, for example, create collections, make payments and view balances and movements in accounts registered in Business Online via the Access Agreement, to open term deposits, to do cash and liquidity management or apply for and draw on loans granted. Loans cannot be drawn until Danske Bank has received loan documentation, duly signed by authorised signatories of your company. Payments, collections, other drawings and the checking of account balances and movements are jointly referred to as transactions.

3. Registered accounts

Accounts must be registered in Business Online before a company can make transactions via Business Online, see below.

3.1. Registered accounts within the Danske Bank Group

Accounts within the Danske Bank Group are opened with Danske Bank and affiliates and divisions of Danske Bank under this agreement.

The following accounts within the Danske Bank Group can be registered in Business Online:

- Accounts held by your company and opened in the name of your company
- Accounts held by third parties, including subsidiaries, provided that the third party or subsidiary has issued a third-party mandate to your company authorising you to act on behalf of the third party or subsidiary.

Registered accounts within the Danske Bank Group can also be managed via SWIFT MT101 or MT940/942, see section 3.2.

3.2. Registered accounts managed via SWIFT

Accounts opened with banks other than the Danske Bank Group, and accounts within the Group which you wish to use for transactions via SWIFT MT101 or MT940/942, can also be registered in Business Online via the Access Agreement. You may register both your own accounts and third-party accounts. You or the third party must conclude an agreement with the account-holding bank concerning Payment Requests via MT101 or an agreement on Balance Reporting via MT940. See section 8.9.

4. Unregistered accounts

If accounts held by your company and/or a third party are not registered in Business Online, it is only possible to

make payments into these accounts. It is not possible to inquire about or make payments from unregistered accounts.

5. Cheque payments

Your company may make payments by issuing a cheque drawn on a registered account within the Danske Bank Group.

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

Issued cheques are regarded as banker's cheques, and the amounts are debited to the accounts on the date of issue.

Your company may have the proceeds from uncashed cheques deposited in registered accounts. If the proceeds from uncashed cheques are to be credited to your account or a third-party's account, you or the third party must accept to indemnify Danske Bank if a cheque is subsequently cashed.

6. Electronic requests

A request by your company or its users for a transaction in Business Online, for example a payment, is called an electronic request.

6.1. Submitting and revoking requests

When a user submits an electronic request on behalf of your company and/or a third party, we send an electronic receipt.

You can revoke payment requests up until and including the day before the business day on which the request is to be executed. Other deadlines apply to revocation of other requests.

With regard to deadlines for change or revocation of payment requests, please see:

- Rules on payment authorisation
- Prices and deadlines - Denmark
- Prices and terms and conditions for cross-border payments and payments in foreign currencies in Denmark

6.2. Binding requests

Requests carried out in accordance with the instructions in the electronic request are binding on your company. Consequently, Danske Bank cannot reverse payments, trades in foreign exchange or securities or other transactions, including cheque issuance, finalised in accordance with the request.

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

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

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

Third-party accounts comprised by the Business Online agreement are treated as own accounts.

7.1. Documents received in electronic form

Your company will receive 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 company is a customer of one or more of the Danske Bank Group's other companies, and you receive documents electronically from these companies, you will also receive such documents in Business Online.

Account statements, lists of deposits and withdrawals and various other lists

are examples of documents that you will receive in electronic form.

We currently increase the types and number of electronic documents that you will receive in eArchive. Every time a new type of document becomes available in electronic form, you will be notified in Business Online and not by ordinary mail.

7.2. Who has access to the documents in eArchive

The rights and authorisations granted to the individual user determine which documents the user can view. A user will, for instance, always be able to view his or her individual User Authorisation in Business Online. Users with query access/access to operate an account are granted access to view the documents relating to the account in question in eArchive.

7.3. Archiving

We file the electronic requests and documents in eArchive for the current year plus five 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 company changes bank or for some other reason no longer has access to Business Online. In such cases we recommend that you copy the documents yourself.

If you need to keep the documents for a longer period than possible via Business Online, you should copy the documents for your own files for storage.

7.4. Deregistering eArchive

If you do not wish to receive documents in eArchive, you must notify Danske Bank. Subject to agreement, we may forward documents in hardcopy against payment of a fee.

7.5. Termination

If your Business Online agreement terminates, or if your customer number changes, or you deregister an account, you will no longer be able to receive documents in electronic form in eArchive. See section 7.3 on filing, etc.

8. User Authorisations for Business Online

All users performing transactions in Business Online on behalf of your company or a third party must be duly authorised to do so by your company. You can create this authorisation via Danske Bank's User Authorisation in Business Online.

If a third party has signed a mandate to your company, you may delegate this mandate to your users. You can do so via the User Authorisation in Business Online.

Before you create a User Authorisation for Business Online, you must obtain the user's consent to pass on his or her CPR number to Danske Bank. A sample consent form can be found in Business Online.

If a user needs to carry out transactions via the cashier's desk, your company must sign the MANDATE – CORPORATE CUSTOMERS form.

8.1. User rights

For each user, you must state which user rights the user is to have access to:

- Payments between registered accounts in the same country within the Danske Bank Group
- Payment requests via SWIFT MT101
- Payments to unregistered accounts within or outside the Danske Bank Group, including payments via payment forms and MobilePay Payout. The use of MobilePay Payout requires an agreement with Danske Bank about MobilePay Payout.
- Cross-border payments to registered and unregistered accounts within or outside the Danske Bank Group
- Creation of custody accounts and depositing and withdrawal of securities from such accounts
- Other products and services

Furthermore, you must state which authorisations a user is to be granted for each user right. You can choose from the following authorisations:

- View
- Create/set-up
- Approve two persons jointly
- Approve singly

In general, the selected authorisation is used for all payments within each transaction type. If you have selected a more restrictive authorisation at account level (access to accounts is described in section 8.2), this authorisation is used for payments to unregistered accounts and cross-border payments. If you have chosen not to grant any authorisation to the user at account level, this is also regarded as a restriction and means that the user has query access only.

8.2. Access to accounts

If you authorise a user to make payments to unregistered accounts and cross-border payments, the user must have an authorisation at account level.

For each account to which the user is granted access at account level, your company must state the authorisation the user is to be granted.

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

Our account authorisation types are described in section 9.

The authorisation chosen at account level will apply to all Business Online agreements under which the account is registered.

8.3. Confidential payments

Your company must state whether the user is authorised to make confidential payments. Confidential payments include payments such as wages and salaries, which may only be viewed, created or approved by users with these privileges.

Users are authorised to make confidential payments within the transaction types to which you have granted them access.

No distinction is made between confidential and non-confidential payments in connection with account queries.

8.4. Administrator privileges

If Business Online Administrator forms part of your agreement, you must consider whether the user is to be granted administrator privileges in the form of:

- Agreement Administrator
- User Administrator
- Agreement Information
- Log-on and Blocking
- Payment Limit - Account

For users granted Agreement and/or User Administrator privileges, you must state which of the following authorisations should be granted to the user:

- Create/set-up
- Separate authorisation
- Two persons jointly authorisation

The privileges Agreement Information and Log-on and Blocking may be granted only as separate authorisations.

8.4.1. Agreement authorisation

A user who is granted Agreement Administrator privileges is authorised to perform the following on behalf of your company:

- request that users be granted Agreement Administrator privileges or that such privileges be modified
- delete Agreement Administrator privileges
- create, modify and delete User Administrator privileges – see section 8.4.2..

- create and delete Agreement Information privileges – see section 8.4.3
- create and delete user privileges in relation to Log-on and blocking – see section 8.4.4
- Create, edit and delete Payment Limit – Account privileges – see section 8.4.5.

A user holding these authorisations is called an Agreement Administrator.

You must state whether the Agreement Administrator is to be authorised to make modifications under his or her own user ID.

If an Agreement Administrator is subject to restricted use under his or her own user ID, the Agreement Administrator will not be able to grant himself or herself the authorisations stated above. Nor will the Agreement Administrator be able to create and approve payment requests. Your choice also applies to the user's privileges as User Administrator.

Requests for Agreement Administrator privileges must always be signed by persons legally authorised to sign for your company. When a user with Agreement Administrator privileges has requested the creation or modification of a User Authorisation with Agreement Administrator privileges, a User Authorisation Business Online with a signature field is generated in the Business Online eArchive. The User Authorisation is accessible to users with Agreement Information privileges. The User Authorisation must be signed as stated above and sent to Danske Bank. In other cases, the user accepts and signs using his or her digital signature.

Users with Agreement Administrator privileges must also have User Administrator privileges.

8.4.2. User Administrator

If you grant User Administrator privileges to a user, you authorise the user to perform the following on your behalf:

- create and modify your users, including giving users access to the required authorisations and transaction types, modules and accounts registered under the Agreement at any time
- create and delete users' access to ordering basic products – see section 8.4.6
- create and modify user master data
- delete all user details, including master data

A user holding these authorisations is called a User Administrator.
You must consider whether the User Administrator is to be authorised to make modifications under his or her own user ID.

If a User Administrator is subject to restricted use under his or her own user ID, he or she will not be able to grant the above privileges to himself or herself. Nor will the User Administrator be able to create and approve payment requests.

Your choice also applies to the user's privileges as Agreement Administrator.

8.4.3. Agreement Information

Via a user overview, users whom you provide with Agreement Information privileges can search by agreement users and view their individual privileges (including master data, modules, administrator privileges, access to accounts and payment access).

Users have access to the user overview and selected documents shown in Business Online.

8.4.4. Log-on and Blocking

A user whom you grant Log-on and Blocking privileges is authorised to

perform the following on behalf of your company:

- order temporary PINs for users
- order eSafeID device
- block and unblock users

8.4.5. Payment Limit - Account

A user whom you grant Payment Limit – Account privileges is authorised to perform the following on behalf of your company:

- Create, edit and delete payment limits on the accounts which the user can at any time dispose of under the agreement.

For users granted Payment Limit – Account privileges, you must state which of the following authorisations should be granted to the user:

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

Our account authorisation types are described in section 9.

8.4.6. Ordering of Basic Products

With Business Online Administration, you have access to Ordering of Basic Products, enabling you to make agreements about basic products in Business Online. If you grant a user the Ordering of Basic Products privilege, you authorise the user to make binding agreements – on behalf of the company – about the products available from time to time in Ordering of Basic Products in Business Online.

8.5. Message system

All users can send messages electronically to Danske Bank through a secure communication line. Users can view only messages that they themselves send and receive in Business Online. The message system cannot be used for transmitting orders to Danske Bank.

8.6. Changing Business Online User Authorisations

If you wish to extend or limit a user's access to Business Online, a new User Authorisation for Business Online must be signed, replacing the previous one. If the change relates to the user's authorisations at account level, you must also sign an account mandate, and the third party must sign a new third party authorisation.

If the changes are made via Business Online Administration by the Agreement and/or User Administrator of the agreement, the changes are approved by using digital signature. If the change also comprises Agreement Administrator privileges, User Authorisation, cf. 8.4, must be signed in compliance with your company's signing regulations.

A user's authorisation in Business Online may be affected if your company issues a MANDATE – CORPORATE CUSTOMERS.

8.7. Revoking Business Online User Authorisations

User Authorisations for Business Online remain in force until revoked by you, either in writing, by contacting the branch or using an electronic signature where applicable. Authorisations may also be revoked by telephone, but this must always be followed up by immediate written confirmation. The user's access to act on behalf on your company via Business Online is blocked after the telephone call.

When Danske Bank has received notice of revocation, we will send written confirmation that the user ID and key have been deleted in our systems.

If you terminate the entire Business Online Access Agreement, Danske Bank construes 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 Business Online user authorisation.

8.8. Transactions involving third party accounts in Business Online

If you wish to make transactions on third-party accounts or to create/operate third party securities in custody accounts with the Danske Bank Group, the third party must sign Danske Bank's third-party mandate form.

If account queries are to be possible on third-party accounts outside the Danske Bank Group, you must conclude a special agreement with Danske Bank, since such queries must be made through SWIFT and by using MT940. Furthermore, the third party must conclude an agreement with the account-holding bank, stating that the Danske Bank Group may receive data about the third party's external account(s).

If you are to be able to make payments from the third party's accounts outside the Danske Bank Group, you must conclude an agreement with Danske Bank to this effect. Furthermore, the third party must conclude an agreement with the account-holding bank, stating that the Danske Bank Group may send payment instructions to the third party's bank(s).

If you are to be able to create custody accounts and/or deposit/withdraw securities from the the third party's accounts, the third party must sign Danske Bank's third-party mandate form.

Danske Bank registers third-party accounts in Business Online via your Access Agreement.

8.9. Authorisation to buy/sell foreign exchange and securities

To be able to view trade positions and buy and sell foreign exchange spot and forward, as well as to buy and sell Danish and foreign shares, bonds and investment certificates, the user must have access to one or more Markets Online modules. Access to buy and sell foreign exchange spot and forward and to buy and sell shares, bonds and investment certificates also requires that you grant the user Currency trading and/or Securities trading authorisations. These authorisations only authorise the user to perform transactions on behalf of your company via Markets Online.

All transactions relating to purchase and sale of foreign exchange spot and forward are subject to the provisions of the framework agreement on netting and final settlement of trades concluded between your company and Danske Bank.

8.10. Trade Finance Authorisation in Business Online

If a user is to be able to issue letters of credit, collect debt and/or issue guarantees, you must register the user for the Trade Finance module and sign the Connection to/Modification of the Trade Finance Module in the Business Online agreement. In this connection, you must state whether the user is to have access to

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

Furthermore, you must state whether the user is to have access to

- create and inquire
- create and approve – two persons jointly or
- create and approve – separately.

8.11. Collection Service SEPA Direct Debit Authorisation in Business Online

To be able to create SEPA Direct Debit collections, the user must be registered for the Collection Service - SEPA Direct Debit module. This will give the user access to

- collections
- reimbursements
- revocations

in euro accounts attached to Business Online.

9. Authorisation types

Danske Bank operates with the following authorisation types:

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

These authorisations allow you to specify which users may, separately or jointly, approve a payment or request. The authorisations are described in the following.

9.1. Separate authorisation

When requests or payments are created or changed by a user with this authorisation, they are automatically deemed to have been approved by the user. Users with this authorisation can also approve requests or payments entered by users with all other authorisation types.

9.2. Two persons jointly

When a user with a two persons-jointly-authorisation creates a payment request or a payment, authorisation (2nd authorisation) from a user holding the same type of authorisation is required.

9.3. Two persons jointly (A authorisation)

When requests or payments are created by a user with an A authorisation, they are automatically approved by this user (1st approval). Further approval (2nd approval) by a user with Separate, A, B or C authorisation is required.
Users with A authorisations rank equally, and the order of approval is therefore of no consequence.

9.4. Two persons jointly (B authorisation)

When requests or payments are created by a user with a B authorisation, they are automatically approved by this user (1st approval). Further approval (2nd approval) by a user with Separate, A or C authorisation is required. Two users with B authorisations cannot jointly approve a payment.

9.5. Two persons jointly (C authorisation)

When requests or payments are created by a user with a C authorisation, they are automatically approved by this user (1st approval). Further approval (2nd approval) by a user with Separate, A or B authorisation is required. Two users with C authorisations cannot jointly approve a payment.

10. Customer support

Danske Bank provides support and service to your company in the form of

- user administration
- telephone support, including blocking service in Business Online
- Internet-based support
- on-site support.

User administration often includes establishment of Access Agreements and authorisations, adjustment of your company's and its users' access to the various support and service features, deletion and blocking of users, ordering of temporary PINs and registration of modifications to authorisations, etc.

Telephone support may include training, user instruction, troubleshooting assistance, guidance in relation to modifications, and an option to block Business Online. Telephone support in connection with installation, set-up, training and troubleshooting, etc. of Business Online is provided in cooperation with your company's IT department and at the risk of your company.

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 the risk of your company.

On-site support may include installation of and training in Danske Bank's officebanking system, as well as troubleshooting. Troubleshooting may result in adaptation and/or modification of the computer set-up and your IT systems, modification of registration databases, installation of routers, firewalls and proxy servers, internal security systems and other software and hardware modifications. Installation and troubleshooting take place in cooperation with your IT department and at the risk of your company.

Part 2 – Business Online – security system

11. Technical issues

11.1. Transmission and access

You must establish a data communication link with Danske Bank to be able to use Business Online. You bear the costs related to the link and must purchase, install, set up and maintain the required IT equipment.
Likewise, you must ensure the necessary adaptations to your IT equipment – in order to be able use the link and ensure continuity of operations.
Danske Bank may at any time and without notice modify its own equipment, basic software and related procedures in order to optimise operations and service levels. Danske Bank will notify the company of any modifications requiring adaptation of the company's equipment in order to retain the link and access by giving 30 days' written notice via Business Online or otherwise.
The company may not use special software such as "overlay services" or similar types of software when accessing the Business Online system. Users must operate the system directly via the user interface and the software provided by Danske Bank.

11.2. Distribution, control and storage of software

Danske Bank distributes the programs required to install Business Online. You can download the programs from the Internet.

When programs are downloaded from the Internet, you or a user must check that the program delivery has been electronically (digitally) signed by Danske Bank.

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

11.3. Data security

eSafeID, e-Safekey and EDISec are the general security systems used in Business Online.
eSafeID is Danske Bank's web-based security system to log on to Business Online. The eSafeID is a two-factor authentication system, which means that it is based on something you know (your personal password) and something you have (your eSafeID device that generates security codes). The security code generated by the eSafeID device is saved temporarily in the browser session while the user is logged on to Business Online.

e-Safekey and EDISec are Danske Bank's security systems for the customers who want to exchange information with Danske Bank electronically directly through their own business systems. e-Safekey and EDISec are built on a password (digital signature) and use permanent encryption keys stored in the company's IT environment.

Using these security systems ensures that data is encrypted before being transmitted to Danske Bank and is not tampered with during transmission. In

addition, the authenticity of the sender's digital signature is always checked, and all financially binding transactions are provided with a digital signature.
Danske Bank is entitled to block a company's or user's access to Business Online if it registers attempts at misuse. If access is blocked, you will be notified as soon as possible.

You must implement effective security procedures to prevent unauthorised use of Business Online and unauthorised access to user keys and the eSafeID device.

Further information about security recommendations is available under the *Security* menu item in Business Online on Danske Bank's website and in other guidelines.

12. Acquiring a user ID, temporary password and eSafeID device

When a user is to be created in Business Online with the eSafeID security system, Danske Bank gives the user an individual 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 security system.

When a user is to be created in Business Online with the e-Safekey or EDISec security systems, Danske Bank gives the user an individual user ID and a temporary password. The temporary password is used for first-time identification when the used is registered in the security system.

The temporary password is system-generated and printed electronically without anybody seeing the combination. If the letter containing the temporary password and/or the letter containing the eSafeID device has been opened or is not intact, the user must contact Danske Bank to order a new temporary password and/or a new eSafeID device. For security reasons, the letters containing the temporary password and the eSafeID device are not sent at the same time.
If the user has not received the letter containing the temporary password within three workdays of ordering, the user must, for security reasons, contact Danske Bank to cancel it and order a new one. On registering in the security system, the user chooses a personal password and must subsequently destroy the temporary one.

12.1. Storing the user ID, personal password and eSafeID device

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

- Only the user may use the user ID, personal password and eSafeID device
- The password, eSafeID device and security codes are strictly personal and must not be shared with any third parties
- The password and security codes may be used only when communicating with Danske Bank
- The password must not be written down and stored together with the eSafeID device

12.2. Changing the password

The user must change his or her password regularly, and it is your responsibility to ensure that this is done.

For further information, read the security recommendations under the Security menu section in Business Online on Danske Bank's website and in other guidelines.

12.3. Deregistering users

You must inform Danske Bank if users are to be deleted. You are responsible for all transactions performed by a user until Danske Bank is requested to delete

or block the user. You are also responsible for all future transactions previously requested by a deleted/blocked user until Danske Bank is notified that the transactions are to be deleted.

12.4. Misuse or risk of misuse

You or the user must immediately contact Danske Bank in order to block user access if

- either of them suspects that the personal password, the company's or user's encryption key or the eSafeID device has been misused
- others have had access to the personal password, the personal encryption key or have gained possession of the eSafeID device

13. Ban on encryption

Local, national legislation in the country where Business Online is used may include a general ban or limitations on encryption. Therefore, it is important to be familiar with national legislation.

Part 3 – Contractual aspects

14. For business purposes only

Business Online is to be used for business purposes only. The information made available to you, including price information, is solely for your own use. Your company may not pass on the information to others, except by written permission from Danske Bank.

15. Changing Business Online

Business Online gives access to the services offered by Danske Bank.

Danske Bank may at any time extend or reduce the scope of Business Online. The bank may extend the scope of Business Online without notice. When the bank adds new services to Business Online this will not require new signatures from you, provided that the new services are advantageous to you and do not imply any material cost increase. If the bank reduces the scope and/or content we may only do so upon 30 days' prior notice.
We may change these Terms and Conditions without notice, and information on changes will be provided in Business Online, by letter or by announcement in the daily press.

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.

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.

16. Changes to service and support

Danske Bank may change the scope and content of its service and support at any time by giving 30 days' notice. The price list shows the prices charged for the various services and support functions.

17. Responsibilities and liability

17.1. Your company's responsibilities

Use of Business Online is at your own responsibility and risk.

The risk borne by you includes, but is not limited to, the risk in relation to

- sending information to Danske Bank, as well as the risk that a transmission is destroyed, lost, damaged, delayed or affected by transmission errors or omissions, e.g. during intermediate handling or processing of data content
- information becoming accessible to third parties as a result of errors or unauthorised intrusion on the data transmission line

- all operations and transactions made using your own key or that of a registered 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 user keys in your company's IT-environment to prevent unauthorised access to the keys
- any incorrect use or misuse of Business Online by registered users
- misuse of Business Online

You cannot hold Danske Bank liable for any consequences thereof. Nor can you make any claims on Danske Bank in respect of errors and omissions resulting from circumstances pertaining to you, including non-observance of safety and control procedures.
In addition, it is your responsibility to

- obtain the consent of the user before passing on his or her CPR number to Danske Bank
- 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 company's wishes
- open and check the electronic documents sent by Danske Bank to the same extent as if the electronic documents had been sent in hardcopy by ordinary mail
- notify Danske Bank if for a period you have no access to Business Online and consequently wish to receive electronic documents in hardcopy by ordinary mail.

Furthermore, it is your responsibility to ensure that users are aware of the Terms and Conditions for Business Online and the various modules, and that all users observe them and comply with the on-screen Help instructions.

17.2. Danske Bank's responsibilities

Danske Bank will be liable for damages if, through errors or neglect, it is late in performing its obligations under the Agreement or performs its obligations inadequately.

However, Danske Bank is not liable for errors and omissions resulting from

- third-party software which is part of the Business Online security system
- a user's disclosure of the temporary PIN and/or the password
- 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
- information and data provided by a third party.

Norin areas that are subject to stricter liability, will Danske Bank be liable for losses resulting from

- IT-system failure/downtime or corruption of data in these systems as a result of the events listed below, irrespective of whether Danske Bank operates the systems itself or has outsourced operations
- telecommunication or power failures at Danske Bank, statutory intervention or administrative acts, natural disasters, wars, rebellions, 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 Danske Bank or its organisation and irrespective of the cause of the conflict. This also applies if the conflict affects only parts of Danske Bank
- any other circumstances beyond Danske Bank's control.

Danske Bank's exemption from liability does not apply if

- Danske Bank 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 Danske Bank liable for the cause of the loss.

Danske Bank is only liable for direct losses and is therefore not liable for any indirect or consequential damage, regardless of whether such damage is due to errors or omissions on the part of Danske Bank.

Danske Bank is liable in damages according to section 17.2 above. Section 68 of the Danish Act on payment services does therefore not apply.

18. Other terms and conditions

18.1. Structure of the Business Online Agreement

A Business Online Agreement is comprised by the following documents:

- Business Online – Access Agreement
- User Authorisation(s) for Business Online
- Module Description for Business Online
- Terms and Conditions for Business Online
- General Terms and Conditions - Corporate
- Rules on payment authorisation
- Prices and deadlines - Denmark
- Danske Bank Business Online - Prices for companies in Denmark
- Prices and terms and conditions for cross-border payments and payments in foreign currencies in Denmark
- Help documents and programs.

All documents become integral parts of Business Online when you sign the Access Agreement.

In case of a discrepancy between the terms and conditions and rules stated, the listed order of priority will apply.

Furthermore, the terms and conditions and sets of rules, related to the individual Module Agreements or the Access Agreement apply.

By signing the Business Online Access Agreement, you also acknowledge having read and accepted these terms and conditions and sets of rules as an integral part of the Agreement.

The Terms and Conditions for Business Online and other terms and conditions are accessible on Danske Bank's website.

18.2. Prices and fees

Danske Bank may at any time change its prices by giving 30 days' written notice via Business Online or otherwise. Danske Bank will debit fees and charges to the account(s) specified as fee account(s) unless otherwise agreed in the terms and conditions relating to each specific module.

Danske Bank is entitled to collect and debit fees later than one month after completion of the transaction for which a fee is charged.

Danske Bank is entitled to charge a fee for providing supplementary/more frequent information than agreed in the Business Online Agreement.

Danske Bank may charge fees for payments made by you from an account as well as for notifying you of any payments made.

18.3. Assignment, transfer and third parties

This Agreement has been concluded by Danske Bank on behalf of the Danske Bank Group. This means that any member of the Danske Bank Group is entitled to fulfil and enforce this Agreement. It also means that we may transfer our rights

and obligations to another member of the Danske Bank Group at any time.

We are entitled to transfer the performance under this Agreement to subcontractors. Such transfer will not affect our responsibilities under the Agreement.

18.4. Special provisions concerning payment accounts and the Danish Act on payment services

In relation to payment accounts, the Danish Act on payment services applies.

We have departed from that Act to the extent the Act makes this possible, unless otherwise stated in these Terms and Conditions or agreed with us.

If you have the disposal of a payment account by way of a special payment instrument such as a debit card, the terms and conditions thereof are regulated separately in the agreements on the payment instruments concerned.

For additional information, see the Terms and Conditions of payment accounts.

You are under an obligation to check the entries/transactions in relation to your accounts and custody accounts on an ongoing basis. If on such check you discover transactions that you believe have not been made by you, you must notify Danske Bank immediately of this and not later than four months after withdrawal of the amount from 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 collection request through Business Online, and the request turns out to be unauthorised and the debtor subsequently seeks restitution.

19. Termination and breach

You may terminate the Access Agreement in writing without notice. Requests and agreements made before the time of termination will be carried out. Paid subscription fees and any prepaid fees will not be refunded.
Danske Bank may terminate the Access Agreement in writing by giving 30 days' notice.
We may, however, terminate the Access Agreement without notice if you are in breach of the Agreement or the Terms and Conditions for Business Online. You are in breach if , for example, you omit to pay as agreed in the Access Agreement, suspend your payments, are subject to bankruptcy proceedings or other insolvent administration of your estate, negotiate for a composition or are subject to an execution or attachment order.

20. Governing law

This Agreement is governed by Danish law and the legal venue is Denmark.

If you are registered for a module that is wholly or partly intended to be used abroad, you accept – like Danske Bank – that the terms and conditions of the foreign banks and the legal rules and usage apply for the completion of the transaction.

21. Definitions and glossary

- **Access Agreement** is an agreement between your company and Danske Bank concerning the use of Business Online.
- **Authorisation/mandate** is either User Authorisation for Business Online, Mandate – Corporate customers, Business Online account mandate or one of Danske Bank's other mandate forms for Business Online.
- **Authorisation/mandate holder** is one or more registered mandates or authorisations and/or physical persons who have been granted authorisations/mandates.

- **Banking days** are all days except Saturdays, Sundays, Danish public holidays, 5 June, 24 December, 31 December and Friday after Ascension Day.
- **Basic products** are simple products, available from time to time in Busienss Online.
- **Business Online**:is the collective term for Danske Bank's Internet-based payment and information systems for companies.
- **Confidential payments**: are payments (such as wages and salaries) that may only be seen or processed by users with special privileges. Payments classified as confidential can only be processed by users with these privileges.
- **Cross-border payments** are payments crossing a national border – even if it involves only one transaction currency, e.g. the euro. This applies to payments between registered accounts as well as payments to unregistered accounts. In the countries where the Danske Bank Group is represented, payments between accounts in the same country are not cross-border payments. Payments managed via SWIFT are not included in this category either.
- **Customer support** is a function at Danske Bank offering technical support or support for Business Online users by telephone.
- **Data delivery** is transfer of data between customer and bank. For example, a data delivery may contain payment instructions.
- **Digital signature** is an electronic signature appended to binding transactions, e.g. payments, and used when linking to Danske Bank.
- **eSafeID device** is personal. The devices come in various formats. A common feature is that they show a security code to be used when logging on to Business Online with the eSafeID security system.
- **eSafeID** is a web-based security system to log on to Business Online. eSafeID is a two-factor authentication system consisting of something the user knows (the personal password) and something the user has (the eSafeID device that generates security codes).
- **EDISec** is a security system used for integrated solutions to connect to Business Online.
- **Encryption key**s are used for the e-Safekey and EDISec security systems. Each user generates an encryption key that comprises a pair of keys: a private key to create digital signatures and a public key to confirm the digital signature and encrypt data from Danske Bank to the customer. Each user has a secret encryption key in order to create unique, personal digital signatures. Access to use the encryption key is protected by the user's personal password. The encryption key is stored in the company's IT environment.
- **e-Safekey** is a security system used for integrated solutions to connect to Business Online.
- **Instruction** is an electronic, written or oral request to Danske Bank to carry out changes, transactions, etc.
- **Master data** is the first name, middle name (if any), surname, user name, customer number, CPR number/assigned customer number and related company's address.
- **Module agreement** is an agreement containing provisions about the individual module, e.g. Trade Finance or Collection Service.
- **Module description** is a bulleted description of the functionality of the individual modules registered under the agreement.
- **On-site support** is training, technical assistance or other assistance provided by Danske Bank at your company's premises.
- **Password** is a code to protect a user's private key that is used to

create digital (electronic) signatures.

- **Payment accounts** are accounts opened with a view to completing payment transactions.
- **Payments between registered accounts** are payments between registered accounts in the same country within the Danske Bank Group
- **Security code** is used together with the user ID and the personal password for logging on to Business Online with the eSafeID security system.
- **Security registration** is the registration process that a user must go through before using Business Online for the first time.
- **Temporary password** is generated by Danske Bank that sends it to the company's user(s). The password consists of four or eight characters and is used by the company's user(s) for registering in Business Online.
- **Transactions** are payments, collections, other operations and queries in Business Online.
- **User** is a person (for example an employee) who has been authorised by your company to act on its behalf via Business Online. If your company's and Danske Bank's IT systems are directly integrated, a user may also be a computer or system located within your company.
- **User Authorisation** is your company's authorisation of a user, specifying the services, accounts, authorisations and privileges to which the individual user has access.
- **User ID** is a six-digit number assigned to the individual Business Online user. The user ID is stated in the User Authorisation.