Terms and Conditions for Business Online

1 October 2018

Introduction ................................................................. 2

Part 1 – Business Online – 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 Business Online 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
8.4.6 Ordering basic products .................................. 5
8.5 Message system .................................................... 5
8.6 Changing Business Online user authorisation ........ 5
8.7 Revoking Business Online user authorisations ...... 5
8.8 Access to third-party accounts in Business Online .... 6
8.9 Mandate to buy/sell currencies and financial instruments .................................................. 6
8.10 Trade Finance authorisation in Business Online .... 6
8.11 Authorisation for Collection Service – SEPA Direct Debit in Business Online ................... 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] ......................... 7
10 Customer Support .................................................. 7

Part 2 – Business Online security system ....................... 7
11 Technical matters .................................................... 7
11.1 Transmission and access ................................... 7
11.2 Distribution, control and storage of software .......... 7
11.3 Data security ..................................................... 7
12 Acquiring a user ID, temporary password and eSafeID device .............................................. 7
12.1 Storing user IDs, temporary passwords and eSafeID devices .............................................. 8
12.2 Deregistering or blocking the business’s or a user’s access to Business Online ................ 8
12.3 Danske Bank’s right to block the business’s or a user’s access to Business Online ........... 8
13 Encryption bans ....................................................... 8

Part 3 – Contractual matters ............................................. 8
14 Business use requirement ........................................ 8
15 Use of data .......................................................... 9
16 Changes to Business Online .................................... 9
17 Responsibility and liability ..................................... 9
17.1 Your business’s responsibility and liability ........... 9
17.2 Danske Bank’s responsibility ............................... 10
18 Other terms and conditions .................................... 10
18.1 Structure of the Business Online agreement ......... 10
18.2 Prices and fees .................................................. 10
18.3 Assignment, transfer and third parties ................. 11
18.4 Special provisions concerning payment accounts and the Danish Act on Payments .......... 11
19 Termination and breaches ...................................... 11
20 Law and venue ...................................................... 11
21 Definitions and glossary ........................................ 11
Introduction

Business Online is Danske Bank’s internet-based office banking system, which provides access to account information, payments and other banking services requested by your business.

These Terms and Conditions for Business Online contain a description of Business Online.

Part 1 – describes the options available in Business Online and how to use the system.

Part 2 – describes the security requirements for use of Business Online.

Part 3 – describes the contractual aspects associated with the use of Business Online.

Part 1 – Business Online – general description

1 Modules and services

Business Online is made up of separate modules and services. The module description describes the modules and services of the chosen Business Online version and/or the separate modules and services.

2 Transactions

In Business Online, you can set up payment collections, make payments, view balances and transactions on accounts registered under your Business Online 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 Business Online in order for a business to carry out transactions using Business Online (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 for Business Online:
- 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 Business Online 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 (see clause 8.9).

4 Unregistered accounts

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

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 Business Online, 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 Business Online agreement, your business is automatically registered for receipt of electronic documents from Danske Bank. The documents are filed in your eArchive in Business Online.

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 Business Online agreement are treated as your own accounts.

7.1 Documents received in electronic form
Your company 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 Business Online.

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 Business Online, 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 Business Online.

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 Business Online. 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 Business Online, 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 Expiry
If your Business Online agreement expires 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 Business Online user authorisation
Users must be duly authorised to perform transactions in Business Online on behalf of your business or third parties. This authorisation can be set up via Danske Bank’s Business Online 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 Business Online user authorisation form.

Before you create a user authorisation for Business Online, you must have the user’s consent to disclose the user’s civil registration (CPR) number to Danske Bank. A template for the consent declaration is available in Business Online.

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 Business Online 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 Business Online 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

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 Business Online user authorisation form with a signature field is generated and made available in the Business Online 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’ 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

Users with this right are called user administrators.
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 agreement 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.

8.4.6 Ordering basic products
Business Online Administration gives you access to ordering basic products, which allows you to enter into agreements covering basic products in Business Online. If you assign the ordering basic products right to a user, you authorise him or her to enter into binding agreements on your business’s behalf regarding the products available under ordering basic products in Business Online. The user is authorised to create and approve agreements alone.

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 Business Online. Orders cannot be placed via the message system.

8.6 Changing Business Online user authorisation
If you wish to extend or restrict a user’s access to Business Online, a new Business Online 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 Business Online 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 Business Online authorisation may be affected if the business issues an AUTHORISATION FORM – BUSINESS.

8.7 Revoking Business Online user authorisations
Business Online 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 Business Online 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 Business Online 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 Business Online is not sufficient.
8.8 Access to third-party accounts in Business Online
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 Business Online 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 Business Online
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 Business Online.

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 Business Online
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 Business Online.

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 'two persons jointly' mandate, another [second] approval is required 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 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.
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 Customer Support
Danske Bank provides support and service for your business, in the form of
- user administration
- telephone support, including blocking service in Business Online
- 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 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 Business Online 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 – Business Online security system

11 Technical matters

11.1 Transmission and access
In order to use Business Online, 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 and ensure continuity of operations. You may not use special software, such as ‘overlay services’ or similar types of software, when you use Business Online. 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 you need to install Business Online. You can download the programs from the internet.

When you download programs from the internet, you or a user must ensure that the program 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 must 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 for logging on to Business Online. 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. The security code generated by the eSafeID device can be used only once and is saved temporarily in the browser session while the user remains logged on to Business Online.

e-Safekey and EDISec are Danske Bank’s security systems for customers who want to exchange information electronically with Danske Bank directly through their own business systems. e-Safekey 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 is encrypted before transmission to Danske Bank and is not changed during transmission. The identity of the sender is also always verified, and all financially binding transactions are signed digitally.

12 Acquiring a user ID, temporary password and eSafeID device

When a user is created in Business Online 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 in Business Online using the e-Safekey or EDISec 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.

The temporary password is machine-created and printed without anybody seeing it. If the letter containing the eSafeID device or the temporary password 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 three 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 Business Online, 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 Business Online.

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.

12.1 Storing user IDs, temporary passwords and eSafeID devices

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

The following rules apply to the use of eSafeID, e-Safekey 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
• Passwords and codes may be used only when communicating with Danske Bank
• You must not write down the password and store it with the eSafeID device

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

12.2 Deregistering or blocking the business’s or a user’s access to Business Online

You must notify Danske Bank if you want it to remove the business’s or a user’s access to Business Online. 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

Blocks can be requested or cancelled via Business Online, telephone or one of Danske Bank’s branches. If the request is made via telephone, the message must subsequently be confirmed in writing. However, the user will be blocked in the interim period.

You are responsible for all transactions executed by a user until 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.

12.3 Danske Bank’s right to block the business’s or a user’s access to Business Online

Danske Bank reserves the right to block your business’s or a user’s access to Business Online if we detect attempted unauthorised use.

Danske Bank also reserves the right to block your business’s access to Business Online 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 are notified as soon as possible.

13 Encryption bans

National legislation in the country where Business Online is being used may contain a general ban or restrictions on encryption.

It is therefore important to be familiar with the country’s legislation.

Part 3 – Contractual matters

14 Business use requirement

Business Online 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.
15 Use of data

You consent to Danske Bank's use of personal data related to users when they are registered as users in Business Online, in accordance with the Danish Act on Processing of Personal Data [Persondataloven]. Danske Bank may via Business Online 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 Business Online.

Functions in Business Online 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.

16 Changes to Business Online

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

Danske 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 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 Business Online, 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 Business Online, 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.

17 Responsibility and liability

17.1 Your business's responsibility and liability

Use of Business Online 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

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 Business Online 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 Business Online 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.

17.2 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.

18 Other terms and conditions

18.1 Structure of the Business Online agreement
A Business Online agreement consists of the following documents:
• Business Online – access agreement
• Business Online – user authorisation[s]
• Module description for Business Online
• Terms and conditions for Business Online
• General conditions
• Rules on payment authorisation
• Prices and cut-off times – Denmark
• Danske Bank Business Online – 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 Business Online 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 Business Online access agreement, you acknowledge having read and accepted these terms and conditions and rules as an integral part of the agreement.

The terms and conditions for Business Online and other business terms and conditions can be viewed on and downloaded from Danske Bank’s website.

18.2 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 Business Online 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 Business Online, in the daily press or by letter.
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 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.

18.4 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 Business Online, which is later found to be unauthorised and the debtor demands repayment.

19 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 Business Online. 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.

20 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.

21 Definitions and glossary

- **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 Business Online. 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 Business Online user. The user ID is shown in the user authorisation.
- **User authorisation** - the company’s authorisation for users, specifying the services, accounts, mandates and rights of a given user.
- **Business Online** 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.
- **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 Business Online.
- **eSafeID** - a web-based security system used to log on to Business Online. 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 Business Online.

Mandate – a business mandate, Business Online account mandate or one of Danske Bank’s other mandate forms for Business Online.

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 Business Online.

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 Business Online 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 Business Online system using the eSafeID security system.

Customer support – a help function in Danske Bank, which provides technical or general support to Business Online 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 Business Online may be taken into use.

Master data – first name, middle name, last name, username, customer number, civil registration number/assigned customer number and associated business address.

Access agreement – an agreement between your business and Danske Bank on the use of Business Online.

Transactions – payments, payment collections, other movements of funds and queries in Business Online.