General Terms and Conditions
Corporate Web Bank

Valid 25.5.2018

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

Table of contents

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

Danske Bank

Introduction

Business Online is the Bank's Internet-based office-banking system, which allows the Customer and the User of the service access to view account information, make payments and give other orders to the Bank.

The Terms and Conditions for Business Online include a service description.

Part 1 – Business Online – general description on the service and the use of Business Online.
Part 2 – Business Online – system and security.
Part 3 – Contractual entity of Business Online.

Part 1 – Business Online – general description

1. Modules and services

In Business Online, the following services can be provided:

- Business Online Basic (comprises different modules and services) or
- Business Online Global (comprises different modules and services)and/or
- Additional modules and services
- Agreement Administrator and/or User Administrator.

The Module Description contains a description of the selected modules and services. An individual module and service cannot be used until Customer has granted one or several Users access to the module or service. For some modules separate agreements must be signed.

2. Transactions

With Business Online, the Customer can perform actions in accordance with this User Rights, such as making

- queries about registered accounts within the Danske Bank Group,
- queries about registered accounts managed via SWIFT message type MT940,
- payment orders between registered accounts within the Danske Bank Group,
- payment orders via SWIFT message type MT101,
- payments to unregistered accounts within the Danske Bank Group or other financial institution, including cheque payments,
- cross-border payments to registered and unregistered accounts within the Danske Bank Group or other financial institution,
- collection, e-Invoice and related documents,
- view and update card- or card agreement administration information.
- Create and change Cash Pool Single Legal Account or Cash Pool Zero Balancing intra group limits and interest rates

In this text, payments, payment order, collections, and queries are jointly referred to as transactions.

3. Registered accounts

In the Access Agreement the Customer determines the accounts it will register in Business Online. These accounts are referred to as registered accounts. This applies to the Customer's own accounts as well as third-party accounts within the Danske Bank Group and other financial institutions. Accounts which are not registered in Business Online are called unregistered accounts.

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. If such an account is registered in Business Online it becomes a registered account within the Danske Bank Group.

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

- accounts held by the Customer,
- accounts held by third parties, including subsidiaries, provided that the third party or subsidiary has, issued a third-party mandate to the Customer authorizing to act on behalf of the third party or subsidiary.

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

3.2 Accounts managed via SWIFT messages

Accounts opened with banks within the Danske Bank Group or other banks which the Customer wishes to use for transactions via SWIFT message types MT101 or MT940/942 can be registered in Business Online via the Access Agreement. The Customer may register both its own accounts and third-party accounts. The Customer or third party must conclude an agreement with the account-holding bank concerning payment orders via message type MT101 or an agreement on Balance Reporting via message type MT940.

Third-party accounts can only be registered if the third party has issued an authorization to the company.

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

Danske Bank

4 Unregistered accounts

Accounts which have not been registered in Business Online are referred to as unregistered accounts. It is only possible to make payments into these accounts. It is not possible to make enquiries or payment orders from unregistered accounts.

5 Cheques

In countries where one can make payments using a cheque, payments can be made by issuing a cheque drawn on the issuer's own account in Danske Bank Group, or a third party account.

Issued cheques are regarded as banker's cheques, and the amounts are debited to the registered own or third-party account on the date of issue.

The Customer may have the proceeds from uncashed cheques deposited in registered accounts. Before crediting the account with the proceeds, the Bank is allowed to assess the financial status of the Customer.

If the proceeds from uncashed cheques are to be credited to the Customer's or a third-party's account, the Customer or third party must accept to indemnify the Danske Bank If a cheque is subsequently cashed.

If the customer and/or a third party has an agreement concerning payment orders via MT101, cheques can also be drawn on own or third party accounts in other financial institutions than the Danske Bank Group, provided that this option is included in the agreement between the Customer and/or third party and another financial institution than Danske Bank Group.

6 Payment orders

In this text, an order by the Customer or its User for a payment transaction in Business Online, is called a payment order.

The Customer is entitled to use the service in the Bank's website (at address www.danskebank.fi) during the notified service hours.

6.1 Submission of payment requests

When a User submits a payment order on behalf of the Customer and/or a third party, the Bank sends the User an electronic receipt. The moment the Bank has confirmed receipt of the payment order, the risk in relation to its being carried out in accordance with the instructions passes to the Bank.

The User can cancel a payment order one day prior to the due date of the payment.

6.2 Binding orders

Payment orders carried out in accordance with the instructions, are binding on the Customer. Consequently, the Bank cannot reverse payments, trades in foreign exchange or securities or other transactions, including cheque issuance, finalized in accordance with the payment order to the Bank.

6.3 Retention of payment orders

The Bank retains payment orders for at least the time which has been prescribed by law. During this period, the Customer and/or third party whose account is debited may obtain a hardcopy of the order against payment. The fee is that for extraordinary assistance printed in the Bank's List of service charges.

7 Automatic registration for documents from The Archive

The archive is activated in connection with the implementation of Business Online. The documents are file in Archive in Business Online

The Customer receives documents from the Bank to the archive in electronic format with the same legal effect as ordinary documents in paperformat.
Third party accounts comprised by the same agreement are treated as own accounts.

7.1 Documents in electronic format

The Customer will receive all documents from the Bank in electronic format to the Business Online Archive. In special cases Danske Bank may send such documents in hardcopy by ordinary mail.

Such documents are documents in electronic format sent to the Customer by the Bank, for ex. Balance statements and different kinds of service agreements.

If the company is a customer of one or more of the Danske Bank Group's other subsidiaries and branches, and they send documents to the company electronically, the company will also receive such documents in Business Online Archive

The Bank will send the Customer information via Business Online of new electronic documents.

7.2 Who has access to the documents

A User may be authorized to view the documents in the Archive in Business Online. The User Rights granted to a User will define the type of documents he or she has access to view. A User is always allowed to view his or her own User Right Agreement.

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

7.3 Filing in the archive

The Bank files the electronic documents in the Archive for the current year plus the following five years, as a minimum. The filed documents will be deleted when the Customer deregisters an account from Business Online, cancels the use of Business Online, or if the customer relationship with the Bank terminates. It is recommendable that the Customer prints the documents on paper or in some other lasting manner prior to deleting the documents.

If the Customer must keep the documents for a longer period than is possible in Business Online, it should save the documents in its own systems.

7.4 Deregistering the Archive

If the Customer does not wish to receive documents to the Archive, it shall notify the Bank when concluding the Agreement. The Bank will send the Customer the documents in paper format against a separate service fee.

7.5 Termination

Filed documents will be deleted when the Customer deregisters an account. The Customer will terminate the use of Business Online, or the customer relationship with the Bank terminates. See section 7.3.

8. User Authorizations for Business Online

All Users using Business Online on behalf of the Customer or a third party must have a valid User Right issued by the Customer. This User Right is created by using the User Authorization in Business Online.

If a third party, a company or other legal entity, has signed a Third party authorization, it can delegate this authorization to a designated and authorized User of Business Online. This shall be done by using the User Authorization in Business Online.

When the Customer creates a User Authorization for Business Online, the Customer shall have the consent of the User to pass on the personal data and CRP to the Bank.

For the withdrawal of cash in a branch of the Bank, or for making payment orders Customer shall authorize the User to represent the Customer by using a separate Authorization on Use of Account drawn up for this purpose.

8.1.1 Digital channel access

Users can access Business Online via various browsers and Business Apps. You can deny a user access to Business Online via Business Apps. Regardless of the choice of channel, users have only the rights set out in the User Authorization for Business Online.

8.1.2 Types of payment orders

The Customer must state which types of payment orders a single User is to have access to:

- payment orders created on registered accounts in the same country within Danske Bank Group, and which are registered in the Access Agreement;
- payment orders via SWIFT message type MT101,
- payment orders, including cheque payments, created on unregistered accounts within Danske Bank Group or other financial institutions, and which are registered in the Access Agreement;
- cross-border payments to registered or unregistered accounts in Danske Bank Group or accounts in other financial institutions
- euro payments into accounts in SEPA countries not registered on Business Online within or outside the Danske Bank Group - including payment of drafts.

Acceptance of the received e-Invoice is a payment order.

Furthermore, the Customer must state the scale of the User Rights, or the authorization of the User to

- create and approve payments
- or only to create the selected payments.
  If the User is empowered to both create and approve payments, the relevant authorization within each transaction type must also be stated. The following authorizations are available:
- separate authorization,
- two persons jointly (A authorization).

The various levels of user authorization are described in section 10.

The selected authorization is used for each payment types. If the Customer has selected a more restrictive authorization at account level, this authorization will apply for payments to unregistered accounts and cross-border payments. If the User has been granted no authorization at account level, this is also regarded as a restricted user authorization.

8.2 Access to use accounts

The Customer must define on which accounts each individual User may make inquiries and/or payments, including approving any Finnish e-Invoices. If the Customer empowers a User to make payments from a certain account, the User is granted access to the transaction types he or she the Customer has empowered him or her to have access to.

The User's authorization must be stated for each account that the User is granted access to. The following authorizations are available at account level:

- use of account, separate authorization ,

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

- two persons jointly (A authorization),
- two persons jointly (B authorization),
- two persons jointly (C authorization).

The various levels of User authorizations can be read in section 10.

An authorization granted at account level is valid in all Business Online agreements under which the account is registered.

8.3 Confidential payments
The Customer can authorize some of designated his Users to make confidential payments. Confidential payments include payments such as wages and salaries, which may be viewed, created or approved only by designated and authorized Users.

A User is empowered to make confidential payments only within the transaction types to which they have been granted access to in section 8.5.

In addition, Users may inquire about confidential payments within the limits they have been granted query access.

8.4 Administrator privileges
A Customer who has access to use the Administrator module gives the Users the right to manage the Agreement as follows:
- Agreement Administrator, principal user,
- User Administrator,
- viewing Agreement information,
- ordering and blocking passwords,
- viewing and updating cardinformation,
- viewing and updating cardadministration,
- viewing and updatting cardagreement administration

Users will be granted rights to manage the Agreement and User Rights as follows:
- separate authorization,
- two persons jointly (A authorization),
- to create.

The various authorization levels granted by the Bank are described in section 10.

8.4.1 Agreement Administrator
The Principal User who has been granted rights to manage the Agreement can, in the name of the Customer:
- add or change Agreement Administrator user rights to others or own User Rights,
- delete Agreement Administrator rights,
- create, change or delete User Rights – see section 8.2.1,
- create or delete rights to view agreement information – see section 8.2.2,
- create, change or delete user or account limitations for payments,
- Viewing and updating cardinformation,
- Viewing and updating cardadministration.

Agreement Administrator can give these user rights to oneself or other users.

Requests for Agreement Administrator privileges must always be signed by persons legally authorized to sign for the company. When a user with Agreement Administrator privileges has requested the creation or modification of a User Authorization with Agreement Administrator privileges, a User Authorization Business Online with a signature field is generated in Business Online. The User Authorization is accessible to users with Agreement Information privileges. The User Authorization must be signed as above and sent to the Bank.

In other cases, the user accepts and signs using his or her digital signature.

8.4.2 User Administrator
A user who is granted User Administrator privileges is authorized to perform the following on behalf of the company:
- create and change users, including giving users access to the required modules, accounts, authorizations and transactions types,
- create and delete users access to ordering basic products – see action 8.2.3
- create and change user master data,
- delete all user details, including master data.

User Administrators can grant these privileges to themselves and others.

8.4.3 Agreement Data
A User who has access to Agreement Data can view or retrieve user data, User Rights (data on users, modules, management rights, rights to use the account, and rights to make payments) of the Agreement. The User has access to the user interface and the selected documents through Business Online.

8.4.4 Payment Limit – Account
A user whom you grant Payment Limit – Account privileges is authorized 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.

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

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

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

Our account authorization types are described in section 10.

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 authorize the user to make binding agreements – on behalf of the company - about the basic products available from time to time 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 Rights
If the Customer wishes to extend or limit a User's access to Business Online, a new User Authorization for Business Online must be signed, replacing the previous one.

If the change relates to the User's User Rights at account level, the Customer and/or third party must sign an account mandate in addition to the User Authorization.

If the customer issues an Account Authorization to access other services than Business Line, the Customer should note that this may affect the authorizations given earlier by the Customer to the User.

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 Authorization, must be signed in compliance with your company's signing regulations.

8.7 Revoking Business Online User Rights
User Rights for Business Online remain in force until revoked by the Customer in writing. User Rights may also be revoked by telephone, but this must always be followed up by written confirmation. The User's access to act on behalf on the Customer via Business Online is blocked after the telephone call.

When the Bank has received notice of revocation, it sends written confirmation that the Users right to use bank identifiers has been deleted from the Customer's Business Online.

If the validity of a Business Online Access Agreement terminates, all User Rights granted under the agreement are also terminated.

If the Customer and/or a third party has granted the User Rights other than User Rights to Business Online – e.g. for cash withdrawals at a specified branch of the Bank – such authorizations must be revoked separately.

9. Other User Rights in Business Online

9.1 Third-party authorizations granted to The Customer
A third party may authorize the Customer in writing to make payments from his account. With this User Right the third party authorizes the Customer to register its accounts under the Customer's Business Online agreement and to delegate these User Rights to one or more Users of the Customer. The Customer delegates the powers via the Business Online User Right Agreement.

If the Customer is to make payments from a third party's accounts are held in another financial institution than Danske Bank Group, an agreement must be sent to the Bank stating that the Customer may send payment orders to the third party´s bank(s) via Danske Bank Group.

The Bank registers the third-party accounts in Business Online via the Customer's Access Agreement.

9.2 Authorization to use Business Online Markets Online
If a User is to have access to information, be able to view trade positions and buy and sell foreign exchange (spot and forward), as well as Finnish and foreign shares and securities, the User must be granted access to one or more Markets Online modules. Access to buy and sell foreign exchange (spot and forward) and to buy and sell shares and securities also requires that the Customer has authorized the User to use Markets Online. These authorizations empower the User to perform transactions which are binding to the Customer and on behalf of the Customer via Markets Online.

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

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 the Customer and the Bank.

The User Right must state the accounts and custody accounts that the User is authorized to receive information about or trade in.

9.3 Trade Finance Authorization in Business Online
If a User is to be able to issue letters of credit, collect debt and/or issue guarantees, the Customer must sign an agreement to this effect, a Trade Finance Module Agreement. In this connection, the Customer must state whether the User is to have access to:

- letters of credit (exports and/or imports),
- debt collectin (exporta and/or imports),
- guarantees.

Furthermore, the Customer must state whether the User is to be authorized to:

- make inquiries,
- create and approve orders and amendments separately (Separate authorization),
- create and approve orders and amendments two persons jointly (A authorization).

The User shall have access to the Trade Finance module.

9.4 Collection Service SEPA Direct Debit Authorization in Business Online
If a user is to be able to create SEPA Direct Debit collections, the company must register the user for the Collection Service – SEPA Direct Debit module. In this connection, the company must state whether the user is to have access to

- collections,
- reimbursements,
- revocations.

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

- creating and inquiring on all transactions, including transactions which cannot be created by the user.

9.5 Collection Service Finnish e-Invoice Authorization in Business Online
The Customer must agree on the functions of the Collection Service with the Bank and name the users who will be granted access rights to the Collection Service. Assignment of the module to a user gives the user access to all functions under this module, including creating and/or changing accounts connection to Collection Service.

10. Authorization levels

The Bank operates with the following authorization levels:

- separate authorization,
- two persons jointly (A authorization),
- two persons jointly (B authorization),
- two persons jointly (C authorization).

These authorizations allow the Customer to specify which Users may, separately or jointly, approve a payment or an order. The authorizations are described below.

10.1 Separate authorization
When requests or payments are created or changed by a User with this authorization, they are automatically deemed to have been approved by the User. Users with this authorization can also approve inquiries or payments entered by Users with all other authorization types.

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

10.3 Two persons jointly (B authorization)
When inquiries or payments are created by a User with a B authorization, they are automatically approved by this User (1st approval). Further approval (2nd approval) is required by a User with a separate, A or C authorization. Two users with B authorization cannot jointly approve a payment.

10.4 Two persons jointly (C authorization)
When inquiries or payments are created by a User with a C authorization, they are automatically approved by this User (1st approval). Further approval (2nd approval) is required by a user with a separate, A or B authorization. Two users with C authorizations cannot jointly approve a payment.

10.5 Cancellation of authorizations
An authorization is valid until it is cancelled by the Company, in writing.

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

10.6 Create authorization
When inquiries, authorization or payments are created by a User with to create authorizations, these must be verified by either a user with a separate authority or two users with the 'two persons jointly' authority.

11. Customer support

11.1 General
The Bank provides the Customer service and relevant Customer support including among other the following:

- Management of User Rights,
- Telephone support , also including freezing of Business Online Agreements,
- Instructions on www-pages and in Business Online service.

Management of User Rights includes e.g. establishment of an Access Agreement and a User Right Agreement, for the Customer and its Users to amend various support and service features, delete and block users, and to transmit Bank identifiers.

Telephone support may include training, User instructions, troubleshooting assistance and guidance in relation to modification, as well as freezing Business Online Agreements. Telephone support is provided in connection with installation, training and troubleshooting, etc. of Business Online.

Internet-based support may include training, troubleshooting assistance and guidance in relation to modification.

Customer support is provided in cooperation with the Customer's authorized IT department and at the risk of the Customer.

Part 2 – Business Online – system and security

12. Technical issues

12.1 Equipment, software, systems, interfaces and their use
In order to use Business Online, the Customer must establish a data communication link with the Bank. The minimum technical requirements for the use of Business Online can be read on the Bank's Internet pages. The Customer and the User are responsible for ensuring the access of the necessary equipment, software and systems, e.g. hardware, browser and interface, including IT connections. However, the Bank does not guarantee that the service can be used with the Customer's or User's equipment, software, systems or interfaces.

The Customer and User must be responsible for the purchase, use and service of their own equipment, software and interfaces, and the charges and costs related to it. The Customer and User ensure that the equipment, software, systems or interfaces they use cause no damage, disturbance or other inconvenience to the Bank or outsiders.

The Bank may at any time and without notice modify its own equipment, basic software and related procedures in order to be able to optimize their operations and service levels. The Bank shall notify of any modifications requiring adaptation of the customer's systems in order to use the services of the Bank, at least one month in advance. The notice shall be given in writing via Business Online or another channel.

Logging on to Business Online and using it is allowed by and intended for a natural person on behalf of a juridical person acting as Customer and authorized by it. Business Online may be used only through versions of operating systems, browsers and software defined by the Bank.

An exception from the rule above is data communication to and from Danske Bank. Data communication may be carried out using various kinds of commodity software like for instance FTP. In such cases instructions about configuration and usage must be acquired from Danske Bank

12.2 Security and Data protection
Banks ID, eSafeID, e-Safekey, EDISec, and OpenPGP Security are the general security systems used in Business Online.

Using these security systems ensures that data is encrypted and/or electronically signed before being transmitted to and from 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.

The Bank's Internet pages carry information about safe use of Business Online. Information about necessary requirements concerning equipments and software on threats against data protection at any time can be read on the Internet pages of the Finnish Communications Regulatory Authority.

The Customer and the User must ensure that they have the necessary equipment and software required for the use of Business Online and that they are also sufficient and necessary for data protection. The Customer and the User are responsible for updating software and data protection and for the expenses and costs relating to it.

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

In order to ensure safe use the Bank recommends that the Customer and the User read regularly the security regulations on the Internet pages of the Bank and the Finnish Communications Regulatory Authority. They shall also ensure in all reasonable ways that the equipment, software, systems and necessary data links are sufficiently safe and also that they and the necessary data protection programs are updated regularly.

The customer and the user are responsible for always ensuring that the necessary software, equipment and the Bank identifiers for using Business Online have been given by the Bank and that only relevant and authorized persons get access to them.

The bank will either inform the Customer or the User of any threats regarding fraudulent activities or security using the contact details provided by the Customer or the User, or announce them generally in the bank's electronic channels.

12.3. Business Online – security system of corporate web banking
When a User is to be created in Business Online, the Bank gives the User the Bank identifiers which consist of the personal user ID, a personal password and a security card. The Bank identifies the Customer and the User based on the Bank identifiers. The use of the Bank identifiers is equivalent to a person's signature.

The User must ensure that no outsiders get access to his/her Bank identifiers which must be stored in a secure way.

The Customer must ensure that the Users know and understand the terms and conditions of the security system and Bank identifiers.

The Customer must notify the Bank of changes in user accesses. The Customer or the User must notify the Bank immediately for invalidation of Bank identifiers if it is suspected that they have been misused or have been known to outsiders. The Customer is responsible for all payment orders and service requests made with the use of the Bank identifiers until the Bank has been notified of the invalidation of the Bank identifiers according to valid terms and conditions.

Further information about security recommendations can be found in the security menu for Business Online. They contain the vital responsibilities concerning Bank identifiers. The Bank's Terms and Conditions for electronic business valid at any time shall apply to the use of Bank identifiers.

12.4 eSafeID security system
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).

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.

In addition, eSafeID can be used as a one-factor authentication system based on the user's personal eSafeID password when logging on via a Business App. The one-factor authentication system provides access to a limited number of services/information only, such as:

- access to view all data accessible via the Business Apps
- payments to registered accounts
- creation of payments to non-registered accounts and cross-border payments

This means that the two-factor authentication system must be used for other kinds of transactions.
You may deny use of the one-factor authentication system. This means that the two-factor authentication system must be used when logging on to the Business Apps.

You may choose to permit the easy 1 factor logon to the users' access by Business Apps. When using 1 factor logon the user may log-on using only with his/hers personal code in order to see among others data and create electronic orders. For approval of electronic orders, i.e. transactions to external accounts, the user must additionally key in the security code from the eSafeID device.

12.5 Other security systems
e-Safekey, EDISec, and OpenPGP Security are Danske Bank supported security systems for the customers who want to exchange information with Danske Bank electronically directly through their own business systems. e-Safekey, EDISec, and OpenPGP Security use permanent digital signing and encryption keys stored in the company's IT environment.

12.6 e-Safekey
e-Safekey is the security component in Danske Bank's Business API solution.

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

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

12.7 EDISec

Is a security system used for integrated solutions to connect to Danske Bank's systems via data communication channels.

When a user is to be created for data communication with the EDISec security system, Danske Bank gives the user an individual user ID but no temporary password. Validity of the customer public key is ensured by generating a fingerprint of the key and exchange it with Danske Bank according to the EDISec implementation guide.

12.8 OpenPGP Security

Is a security system used for integrated solutions to connect to Danske Bank's systems via data communication channels.

When a user is to be created for data communication with the OpenPGP Security system, Danske Bank gives the user an individual user ID and a temporary password. Initially, an OpenPGP Security certificate is generated containing the security keys. The certificate is sent to Danske Bank together with the temporary password according to the OpenPGP Security implementation guide.

If an OpenPGP Security public certificate is issued by a third party issuer on behalf of a customer, Danske Bank will hold the customer as owner of the key and thus responsible for the validity and maintenance of the certificate.

It is the responsibility of the customer to acquire and maintain its own or third party OpenPGP Security software to handle the OpenPGP Security concept. Among other things the system must be able to handle certificates and have encryption and signing features.

12.9 EDISec keys and OpenPGP certificates

For EDISec and OpenPGP Security, it is the responsibility of the customer to ensure usage of valid keys at any time for securing Data communication. To be more specific, the customer must make sure that:

- Danske Bank has got a valid set of the customer's public keys. When the bank's public keys are about to expire then the customer must update the customer system with new public keys (provided by the bank)
- The customer is using a valid set of Danske Bank's public keys for securing the data communications. When the customer's public keys are about to expire then the customer must renew the customer's public key's and exchange them with Danske Bank
- If customer keys are compromised or damaged, then they should be revoked by contacting the bank

When Danske Bank receives the customer's public EDISec key or public OpenPGP Security certificates the keys/certificates will be stored in Danske Bank's systems in a secure way and will not be shared with anyone outside Danske Bank.

It is the responsibility of Danske Bank to make sure that a valid set of the bank's public EDISec key or OpenPGP Security certificates are always available to the customer.

13 Letters with temporary passwords and eSafeID device

A temporary password is used when starting up on the eSafeID, e-Safekey and OpenPGP Security solutions. 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.

13.1 Storing the user ID, personal password and eSafeID device

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

- 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

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

13.2 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.

13.3 Deregistration of 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.

13.4 Misuse or risk of misuse
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 unauthorized use of Business Online and unauthorized 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.
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 keys or the eSafeID device has been compromised
- others have had access to the personal password, the personal encryption keys or have gained possession of the eSafeID device

14. Limitation on encryption

National legislation in the country where Business Online is used may include a ban or limitation on encryption of data communication. Therefore, it is the responsibility of the Customer and the User to know and conform with the national legislation.

Part 3 – Contractual entity of Business Online

15. Business Online – Corporate Web Bank

Business Online is intended for and is to be used for companies and corporations only. The information made available to the Customer, including price information, is solely for its own use. The Customer may not pass on the information to others, except by written permission from the Bank.

16. Changes to service and support

The Bank is allowed to change the Terms of Agreement and its Business Online service. The Bank shall notify the Customer in writing or electronically of any changes to the Agreement or its Business Online service which considerably increase the liabilities of the Customer or considerably decrease the Customer's rights, and which are not prescribed by law, a decree by authorities or changes to the Banks' payment transmission system. The change will be in force as from the date notified by the Bank, however, no earlier than one (1) month from the date the notice of information was sent to the Customer. The Bank is entitled to notify of the change also by publishing it on the Bank's Internet pages at the address www.danskebank.fi. In these cases the said date starts from the time of publication of the change.

If the changes do not considerably increases the liabilities of the Customer or decrease the Customer's rights, or if the change is prescribed by law, a decree by authorities or changes to the Banks' payment transmission system, the Bank is entitled to notify of the change by publishing it in the branches of the Bank or on the Bank's Internet pages at the address www.danskebank.fi. The change will become valid on the date notified by the Bank.

The Agreement will stay valid as changed as from the date notified by the Bank unless the Customer terminates the Agreement before the change becomes valid.

17. Intellectual property rights

The owner right, copyright, brand and any other intellectual property right to the Business Online service material are held by the Bank, unless notified otherwise. Quoting, copying, saving, changing, amending, transferring, and otherwise utilizing the material or even part of it without the Bank's prior written consent is strictly forbidden.

18. Responsibilities and liabilities in respect of use of the service

18.1 The Customer's responsibilities
The Customer uses Business Online at its own responsibility and risk and is responsible for the use of it of its authorized Users.

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

The Customer bears the risk in relation to sending information to the Bank and in relation to any transmission being destroyed, lost, damaged, delayed or affected by transmission errors or omissions, e.g. during intermediate handling or processing of data content. The Customer also bears the risk in relation to information becoming accessible to third parties as a result of errors or unauthorized intrusion on the data transmission line.

The Bank is not liable for any consequences of omitting to fulfill the above responsibilities of the Customer.

It is the responsibility of the Customer to

- get the consent by the User before submitting his personal ID and other personal data to the Bank and to adhere to the valid jurisdiction in Finland relating to the protection of personal data,
- check that the User Rights created in the service always adhere to the authorizations given to the User by the Customer or third party,
- ensure that the contents of User Rights comply with the information which the Customer has notified the Bank.

Furthermore, it is the responsibility of the Customer to ensure that the Users are aware of the Terms and Conditions in the Agreement on Business Online, and that all Users observe them, including that they comply with the on-screen Help function.
A Customer is responsible for

- all orders and other measures made using the Customer's own or its Users' Bank identifiers. No economic limit is placed on the Customer's responsibility for the use of Bank identifiers.
- ensuring that the Users keep their Bank identifiers in a safe place and in a way which disallows them to be known to third parties
- errors or misuse of any user of the Business Online service.

The customer cannot make any claims on the Bank in respect of errors and omissions resulting from neglect to carry out actions which are the responsibility of the Customer, including non-observance of safety and control procedures. No economic limit is placed on the Customer's responsibility for the use of Bank identifiers.

Complaints about Business Online service shall be submitted to the Bank immediately, no later than one (1) month after the Customer or the User has noticed or should have noticed the reason for the complaint.

18.2 The Bank's responsibilities

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

18.2.1 Indirect damage

The Bank is under no circumstances liable for indirect damages such as loss of income or revenue, interest rate loss, non-receipt of revenue, decrease or intermission of business activities, agreement between the Customer and a User or a third party, or for non-adherence to same, or for any other claims on the Customer by a third party.

18.2.2 Force majeure

The Bank is not responsible for any damage resulting from unusual or unforeseeable reason beyond the Bank's control and which the consequences of which it could not have avoided by careful action. Such reasons may be:

- decree by law or authority,
- war, threat of war, rebellion or riot,
- disturbance inn mailing services, automatic data processing, data transmission, other electronic communication or availability of electricity beyond the Bank's control,
- industrial action like strike, lockout, boycott or blockade, even if only part of the Bank's staff is involved in it or the staff of a subcontractor to the Bank, irrespective of whether the Bank is a part of it or not, or
- any other comparable reason acting excessively hampering the activities of the Bank.

The Bank is liable to inform the Customer of Force Majeure as soon as it is reasonably possible. Force Majeure entitles the Bank to discontinue its activities until further notice.

19. Other terms and conditions

19.1 Structure of the Business Online Agreement

These Terms and Conditions are part of the complete Business Online Agreement comprising also the following documents:

- Business Online - Access Agreement,
- Business online – User Authorization,
- Business Online – Instructions,
- Business Online - Module Description,
- Business Online – Service prices and cut off times,
- Terms and conditions for Electronic Communication,
- General terms and conditions for Corporate cards.

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

In addition, terms and conditions valid at any time shall be applied on the service. Such terms and conditions can be read in agreements applying to individual modules and service agreements. If there is contradiction between the different language version of these terms and conditions, the terms and conditions of the version in the Finnish language will apply in the first place.

The above terms and conditions of Business Online will apply when the Customer and the Bank agree on Business Online service or other electronic banking services. To those parts that the above terms and conditions contain no instructions in respect of electronic services, Bank's Terms and Conditions for Material Transmission Service and Terms and Conditions for Electronic Communication valid at any time will apply. By signing the Business Online Access Agreement the Customer confirms having read, understood and approved the above mentioned terms and conditions of Agreement as binding unto itself and as part of the agreed service.

The General Terms and Conditions for Business Online service, Terms and Conditions for Material Transmission Service and the Bank's Terms and Conditions for Electronic Communication are accessible to the Customer at the address www.danskebank.fi/terms or select following www.danskebank.fi / business / Terms and conditions / Read More

Furthermore, the Customer approves that the Bank may change its General Terms and Conditions of Agreement within the time frame of notice stated in these Terms and Conditions.

19.2 Service charges and fees
The Customer is liable to pay the Bank the service charges and fees notified in the List of service charges or agreed separately. The Bank is entitled to debit the service charges from the Customer's account.

The Bank may change its List of service charges. The Bank publishes the change of service charges or fees in its List of service charges. The change will become valid on the day notified by the Bank, however, no earlier than one (1) month after the publication of the change. If the change is based on a change in the decrees by law or authorities, the change shall become valid on the date notified by the Bank. The List of service charges is available in the branches of the Bank.

19.3 Transfer of the Agreement
The parties are not entitled to transfer any parts of the Agreement to a third party without the written consent of the other party. However, the Bank has the right to transfer the Agreement to a party in the same group as itself without prior notice to the Customer to this effect.

Rights and obligations based on this Agreement are valid to the recipient of the business activities if the Bank merges or splits or concedes its business wholly or in part.

19.4 Act on Payment Service and Advance information
If conflicts arise between the decrees in paragraph 7 of the Act on Payment Services (290/1.5. 2010) which are compulsory only to those in capacity of consumer, and these Terms and conditions, the Terms and conditions of this Agreement shall apply. The Bank digresses from the act on Payment Service to the effect it is possible based on the decree, unless otherwise agreed in this Agreement.

The Customer confirms having received sufficient advance information regarding the Agreement by signing this Agreement and by receiving its own copy of the Agreement, of these Terms and Conditions, and of other Terms and Conditions mentioned in these Terms and Conditions.

The above also applies if the company sends a collection request through Business Online, and the request turns out to be unauthorized and the debtor subsequently seeks restitution.

19.5 Information about data protection
When dealing with the Bank in the capacity of being an individual, e.g. employee, director, beneficial owner and other individual associated to the Customer, the Bank registers and uses the personal data of the individuals to offer the Customer the best advice and solutions, and to comply with the legal requirements that apply to the Bank as a financial institution. More information about what such personal data the Bank registers, how the Bank uses it and the Customer's rights is written in the Bank's privacy notice www.danskebank.fi/tietosuoja , which can also be provided in hard-copy for the Customer. The notice also provides contact information if any questions arise.

When the Customer, or anyone on behalf of the Customer, provides the Bank with personal data, the Customer warrants that the Customer is entitled to disclose such personal data. The Customer also ensures that the person has been informed where to find the Bank's privacy notice.

20. Termination and breach of agreement

The Customer may terminate the Business Online Access Agreement without notice by notifying the Bank

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

hereof in writing. Fees, expenses and service charges debited in advance shall not be reimbursed although they when the service or Agreement is terminated apply to the time after the time of termination.

The Bank may terminate the Agreement with one (1) month's written notice either in Business Online service, by mail or in a branch office.

Service requests and orders made during the validity of this Agreement will be carried out by the Bank. The Customer is responsible for all obligations and responsibilities with regard to service requests made under this Agreement and in the name of the customer during the time of termination. The Customer's or User's right to use Business Online will cease when the time of termination has elapsed.

The Bank may terminate this Agreement without notice if the use of Business Online service or a module comprised in Business Online has been discontinued due to misuse or essential breach of the Agreement by the Customer or a User. Essential breach of Agreement are e.g. situations where the Customer omits to pay service charges as agreed in the Access Agreement, is subject to bankruptcy proceedings or other insolvent administration of its estate, negotiates for a composition or is subject to an execution or attachment order. Discontinuation shall be notified in Business Online or by mail. The Agreement will cease when discontinuation has been notified.

21. Governing law

This Agreement is governed by Finnish law and the legal venue is Finland irrespective of in which country Business Online is used. If any disputes arising from this agreement cannot be settled through negotiation, such disputes shall be settled in the District Court of Helsinki, in Finnish.

If the Customer is registered as a User of a module that is solely intended to be used abroad, the Customer accepts – to the same extent as the Bank – which it is subject to the Acts and usage applying in the country where the Customer operates as well as any particular terms and conditions relating to the specific country and the use of the module in that country.

22 Definitions and glossary

Authorization: Authorization by the customer to a physical person or a registered authority to represent itself in a legally binding way in Business Online. The authorization can be e.g. access authorization to Business Online, the bank's general authorization form or any other authorization form by the bank for Business Online.

Authorization holder: One or several registered (legal entity or natural) person who have been granted authorization are registered in Business Online.

Bank: Danske Bank A/S, Finland Branch, company registration No. 1078693-2.
Postal address: Televisiokatu 1, PL 1561, 00075 DANSKE BANK. Tel +358 (0) 10 515 15. Web page www.danskebank.fi. BIC code (SWIFT address) DABAFIHH. The bank is the Finland branch of Danske Bank A/S which is registered in Denmark, and thus part of Danske Bank Group. Business ID code number of Danske Bank A/S is 61126228.

Bank identifiers: A code consisting of a personal customer number, secret password and security card.

Banking days: Saturdays, Sundays, public holidays in Finland, 1 May, Midsummer Eve, 6 and 24 December and days not otherwise considered as banking days are not banking days in Finland.

Basic products are simple products, available from time to time in Busines Online.

Business Online: is the collective term for Danske Bank's Internet-based payment and information systems for companies. It covers both the Business Online webbased interface where customers can create payments, administrate users, see account information etc. – as well as the system enabling customers to exchange information (files) with Danske Bank via a data communication channel secured by either EDIsec or OpenPGP Security.

Certificate: An electronically exchangeable document used for holding at least one security key and associated identification and verification information.
Confidential payments: Confidential payments are payments (e.g. wages and salaries) that may only be viewed or processed by users with special privileges. Payments classified as confidential can only be processed by users with these privileges.

Cross-border payment: A payment is classified as a cross-border payment if it is paid between Finland and an ETA country in another currency than that of an ETA country, or in any currency between Finland and a non-ETA country. This applies to payments between registered accounts as well as to payments to unregistered accounts.

Customer: A legal company or other corporate customer having a Business Online Access Agreement based customer relationship with the

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

Bank in respect of a product or a service. The customer may also be a physical person if he is performing business activities and uses the service offered by the Bank in his business activities.

Danske Bank Group: Danske Bank A/S, its subsidiaries and branches in Finland and other countries.

Data transmission: Transfer of data between customer and bank. For example, a data transmission may contain payment instructions by the customer to the bank.

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 when connecting to Danske Bank's systems via data communication channels.

Encryption keys are used for the e-Safekey, EDISec, and OpenPGP 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.

Module agreement: An agreement containing provisions about the individual module and the services contained in it, as well as rights, obligations and liabilities connected to it, e.g. Trade Finance.

Module description: Bulleted short description of the functionality of the individual modules.

OpenPGP Security is a security system used for integrated solutions to connect to Danske Bank's systems via data communication channels.
Password is a code to protect a user's private key that is used to create digital (electronic) signatures.

Payments between registered accounts: Payments between registered accounts within the Danske Bank Group, which are registered in the same country.

Party: In this agreement, the customer, the bank or the user separately or together.

Role ID: A six-charcter aplhanumeric ID assigned to the individual Business Online user. The Role ID is stated in the User Authorization.

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.

Support Direct is a function at Danske Bank offering technical support or support for Business Online users by telephone.

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: A user is a person who has been authorized by the customer to act on its behalf via Business Online. Any actions by the user are binding for the customer. 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 Authorization: The customer's authorization of a user, specifying the services, accounts, authorizations and duties to which the individual user has right and access.

23. Customer service and regulating authorities

In matters regarding Business Online, the Bank should always be contacted primarily by sending the Bank a request for contact via Business Online, using a form on the Bank's web page or by phoning the telephone service for corporate customers, tel. +358 (0) 100 2580 (lnc/mnc).

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

The Customer may also contact the following regulating authorities:
The Bank's operations are supervised by the Finanstilsynet, Århusgade 110, DK-2100 Copenhagen Ø, Denmark, telephone +45 33 55 82 82, www.finanstilsynet.dk.

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

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

Danske Bank A/S, Finland Branch
Registered domicile and address Helsinki,
Televisiokatu 1, FI-00075 DANSKE BANK
Business ID 1078693-2

Danske Bank A/S, Copenhagen
Danish Business Authority
CVR-no 61 12 62 28

LETTER OF CONSENT

I hereby consent to

Name of company (hereinafter called the Customer)

Business ID:

Address

Passing on my name and identity number to Danske Bank. The information is passed on so that I can be created as a User under the Customer's Business Online agreement. The Bank has the right to register the User Right issued by the Customer under my identity number.

The information may be used within the Bank and Danske Bank Group for administration transactions agreed between the Customer and the undersigned in connection with my creation as a User under the Customer's Business Online service agreement.

Date

Full name

Signature

Identity number
