Terms and conditions for using Integration Services

November 2023

1 Integration Services

These terms and conditions apply to the use of Integration Services by a customer of Danske Bank (the Bank) and an external data provider (the Utilizer or You).

The Utilizer must provide the equipment, software, and interfaces necessary for using Integration Services. Further, the Utilizer must ensure that such equipment, software, and interfaces cause no damage, disturbance, or other inconvenience to the Bank. In addition, the Utilizer must ensure that the necessary adaptations of the IT equipment are made to ensure the continuity of operations.

2 Setting up Integration Services

Integration Services include the following tools:

- Communication channels
- Technical user
- Security solutions

The tools to be used depend on the types of files to be sent. Information about the tools to be used in connection with the various file types can be found on the Bank's Integration Services website: www.danskebank.com/INTS. In addition, a description of the tools is included in this document.

The Utilizer is registered as an EDI partner in the Bank. In this connection, Danske Bank creates a technical user for the purpose of identification of messages received from the Utilizer on behalf of customers having an agreement with the Utilizer.

The Bank registers the assigned technical user number internally on all the District Access Agreements under which a Danske Bank customer uses the Utilizer as data provider and under which the individual customer has signed an Agreement on utilisation of Integration Services.

2.1 Communication channels supported

The Utilizer must set up a communication channel between the Utilizer and the Bank in accordance with the Bank's requirements from time to time.

You can find more information about the various channels on the Integration Services website: www.danskebank.com/INTS.

2.2 Technical user

When needed, a technical user is created in order to identify the Utilizer when the Utilizer sends data via Integration Services.

2.3 Security solutions provided by the Bank

The security solution to be used depends on the choice of communication channel as not all security solutions can be combined with all communication channels. The security solution is assigned to the technical user. Use of a security solution ensures that the data are transmitted securely, encrypted, and protected from alteration. In addition, the authenticity of the sender's digital signature is checked, and a financially binding transaction is signed digitally (using a digital signature) by the technical user. The Utilizer is responsible for the implementation and use of the chosen security solution in its own systems.

The technical user and thus the Utilizer is identified digitally, for example by a password, temporary password, security code, user ID, certificate, key, or other security credentials delivered by the Bank as required by the chosen solution. The Bank identifies the Utilizer or a party acting on behalf of the Utilizer only in accordance with these identification measures.

The Utilizer is liable for maintaining and storing the security credentials with due care and according to good practices for the area in question so that they are not disclosed to any third party and so that no third party is able to use them.

If the Utilizer uses security solutions that require public keys or certificates, it is the responsibility of the Utilizer to ensure that (i) the Bank at all times has a valid set of the User's public keys or certificates; (ii) the User at all-time uses a valid set of the Bank's keys or certificates; and (iii) the Utilizer at all times uses a valid set of its own certificates. The Bank makes sure that a valid set of the Bank's public keys or certificates is always available to the Utilizer.

Danske Bank A/S, Bernstorffsgade 40, 1577 København V
CVR no. 61126228, SWIFT: DABADKK
Tel.: +45 33 44 00 00, Fax: +45 33 44 28 85

More information about the various security solutions can be found on Danske Bank's Integration Service website: www.danskebank.com/INTS.

If the data is to be secured, the Utilizer must use a security solution provided by the Bank.

3 Formats

The data sent to the Bank by using Integration Services must be in a format supported by the Bank. Information about the various formats supported by the Bank can be found on the Integration Services website: www.danskebank.com/INTS.

4 Testing

When Integration Services has been set up in accordance with the Bank's requirements, the Utilizer must test the setup before starting to use the services.

5 The Bank's services

When data are received by the Bank, the Bank will determine only whether or not the file has been sent in accordance with the Bank's requirements. The Bank thus checks

- whether the technical user is known to the Bank
- whether the data are secured correctly
- whether the Utilizer is allowed to send the data to the Bank according to an agreement with the Bank
- whether the data are sent in a valid format

If these requirements are met, the data is delivered and processed in compliance with the terms and conditions for the service in question. It is a precondition that the customer has an agreement with the Bank on the service in question. If not, the service cannot be executed.

If the service requires that data be returned to the Utilizer, the data will in some cases be returned via Integration Services. The Integration Services website, www.danskebank.com/INTS, offers more information on data sent from the Bank via Integration Services.

If the data contain format or transaction errors when received by the Bank, the Bank may reject the data or part of the data. The Utilizer can request notification of whether the data format received is valid. The service is available only for certain formats. Read more on the Integration Services website: www.danskebank.com/INTS.

If an error occurs in the communication channel, the security solution or the data format, the service request is rejected. The same applies if the Utilizer's setup does not comply with the Bank's applicable requirements.

6 Areas of use

Integration Services can currently be used for payments, invoices, direct debits, e-invoices, and account information, among other things.

A list of the types of files that can be exchanged with the Bank via Integration Services and the tools to be used for each type of file can be found on the Integration Services website: www.danskebank.com/INTS.

The Bank continually expands the range of file types that can be exchanged via Integration Services. There may also be changes to existing file types. The Bank recommends that the Utilizer keep up to date about such changes.

7 Internal procedures

The Utilizer is aware and accepts that by enabling the use of Integration Services, the Utilizer is responsible for establishing internal procedures regarding (i) the types of transactions to be carried out; (ii) the persons who can initiate an order or transaction; (iii) the ways in which an order or transaction can be initiated in the Utilizer's own system; (iv) the process that facilitates digital signing by the technical user and the subsequent transmission of the data to the Bank; and (v) the approval of transactions in the Utilizer's own systems.

The Utilizer must implement security procedures that prevent unauthorised access to Integration Services from the Utilizer's systems as well as access to security credentials, if any.

If the Utilizer suspects or ascertains that unauthorised persons have had access to Integration Services or security credentials, the Utilizer must immediately notify the Bank so that the Bank can block the access.

When making a payment through Integration Services from a Norwegian account between the Utilizer and the Bank, where the social security number of the

Danske Bank A/S, Bernstorffsgade 40, 1577 København V
CVR no. 61126228, SWIFT: DABADKK
Tel.: +45 33 44 00 00, Fax: +45 33 44 28 85

person who approved the payment in the customer's ERP system is a part of the payment file, the Bank may require access to the Utilizer's logs of who has authorised payments in connection with Integration Services. When, in the Bank's opinion, this is necessary to fulfil the Bank's public obligations, the Utilizer must provide such information to the Bank without undue delay and no later than 14 days after the Bank's request.

8 Blocking of Integration Services

The Bank is entitled to block the Utilizer's access to Integration Services if the Bank registers or suspects unauthorised access to Integration Services.

Further, the Bank reserves the right to block the Utilizer's access to Integration Services if conditions in the Utilizer's equipment, software or interfaces cause damage, disturbance or other inconvenience to the Bank or the Bank's IT infrastructure.

9 Files sent via an external data provider

If a file is sent on behalf of a Danske Bank customer via an external data provider, the data provider must include proof of identity of the customer.

Please find more information about the various types of proof of identity to be included on the Integration Services website: www.danskebank.com/INTS.

10 Use of Integration Services

Integration Services are for business use only and may not be used for illegal activities or purposes.

11 Changes

Integration Services gives access to specific services provided by the Bank. The Bank may at any time extend or reduce the Terms and conditions for the use of Integration Services and the services and functionality in Integration Services, including modifications to the Bank's own equipment, basic software, and related procedures, in order to optimise operations and service levels. Changes that benefit the Utilizer may be implemented without notice. Changes that considerably increase the obligations of the Utilizer or considerably decrease the Utilizer's rights are subject to one month's notice unless the changes are prescribed by law or a decree by public authorities.

The Bank must be notified if the Utilizer does not wish to be bound by a change or a new set of Terms and conditions for the use of Integration Services. The Bank may consider the contractual relationship to be terminated as of the date on which the notification becomes effective or the time of notification from the Utilizer, whichever comes first.

A change comes into force on the date stated by the Bank, although no earlier than one month from the date on which the notice was sent to the Utilizer.

12 Notices

All notices or other communications under or regarding this agreement must be in writing (for example by email) or be made through another channel as agreed between the Bank and the Utilizer, and all communications and notices are deemed to have been delivered when they are delivered to the most recent address given by the Utilizer to the Bank or to its registered address. The Bank must always be informed of the Utilizer's current address.

13 Assignment

This agreement has been concluded by Danske Bank on behalf of the Danske Bank Group. This means that any unit of the Danske Bank Group is entitled to fulfil and enforce this agreement. It also means that the Bank may at any time transfer its rights and obligations to another unit of the Danske Bank Group.

In addition, the Bank is entitled to transfer performance under this agreement to subcontractors. Such transfer will not affect the responsibilities of the Bank under this agreement.

14 Treatment of confidential information

The Bank is subject to and will comply with general rules on confidentiality set out in relevant legislation and regulations.

15 Trade name and trademarks

The Utilizer acknowledges and agrees that the Bank's company name, trade names and trademarks are the exclusive property of the Bank and can be used only in accordance with the Bank's instructions and acceptance.

16 Termination

16.1 The Utilizer's right of termination

The Utilizer may terminate this agreement with immediate effect by giving written notice to the Bank.

Danske Bank A/S, Bernstorffsgade 40, 1577 København V
CVR no. 61126228, SWIFT: DABADKK
Tel.: +45 33 44 00 00, Fax: +45 33 44 28 85

16.2 Danske Bank's right of termination

The Bank may terminate this agreement by giving three months' written notice to the Utilizer. The Bank may terminate the agreement without notice, however, if the Utilizer is in breach of the agreement.

16.3 Events of default

Each of the following events constitutes an event of default that entitles the Bank to terminate the agreement with immediate effect:

- the Utilizer does not comply with the terms and conditions of this agreement
- the Utilizer is unable to pay or declares to be unable to pay its debt as and when it falls due
- the Utilizer becomes subject to debt restructuring, bankruptcy or insolvency proceedings or other similar proceedings

17 Effect of termination

The Utilizer is responsible for all files sent via Integration Services in accordance with this agreement until the Bank is requested to change or terminate the agreement in accordance with its terms or until the Utilizer's access to Integration Services is blocked in accordance with this agreement. The change comes into effect when the Bank has confirmed in writing to the Utilizer that the change, the blocking, or the termination has been registered. Files sent before such change, blocking or termination will generally be executed.

18 Governing law

This agreement is governed by and must be construed in accordance with the law and jurisdiction stated in the Agreement on utilisation of Integration Services or the Agreement on utilisation of Integration Services – External Data Provider.

Any service included in Integration Services is subject to the law governing the service in question.

19 Liability

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

The Bank is not liable for (i) customer losses arising as a result of other parties' unauthorised use of/errors in the external data provider's access and implementation of Integration Services; (ii) indirect losses, consequential losses, loss of profit or interest; as well as (iii) other losses caused by circumstances that are beyond the Bank's control, including technical disruption in the data transmission or operation of networks.

Even in areas where stricter liability applies, the Bank is not liable for losses arising from

- breakdown of or lack of access to IT systems or damage to data in these systems due to any of the factors listed below and regardless of whether the Bank or a third-party supplier is responsible for the operation of these systems
- power failure or breakdown of the 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 the 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 the Bank
- other circumstances beyond the Bank's control

The Bank is not exempt from liability if

- the 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 Swedish law, the Bank is liable for the cause of the loss under any circumstances

20 Contact

Please contact Integration Services support for more information. Contact information can be found at www.danskebank.com/INTS.

Danske Bank A/S, Bernstorffsgade 40, 1577 København V
CVR no. 61126228, SWIFT: DABADKK
Tel.: +45 33 44 00 00, Fax: +45 33 44 28 85