

### BankID agreement

Version 1.0

#### 1. Contact details to the Bank

Name: **Nordea Bank Abp, filial i Norge**  
Address: **P.O.Box 1166 Sentrum, N-0107 Oslo, Norway**

URL: **www.nordea.no**

For blocking your BankID or other questions relating to BankID, please call **(+47) 23 20 60 01**

When these terms ask you to notify your bank, you can use the telephone number listed here, or in another way as instructed by your bank.

Notices from your bank will be made to you directly by means of electronic communication such as e-mail, SMS, or the mailbox in your digital bank.

#### 2. About the agreement

This agreement contains the terms and conditions for BankID between you and your bank. These terms and conditions explain what BankID is and specify your obligations as a user of BankID. Read the agreement carefully and contact your bank if you have any questions.

BankID is a common solution operated by the banking sector in Norway. A BankID issued by one bank can be used for other banks and websites, as it is based on a common set of rules. **To make sure BankID is a secure solution, it is important that you keep your BankID private, protect your equipment and password for using BankID, and inform the bank if you suspect others may have gained access to your BankID. See section 4 for details.**

A bank may require you to enter into a customer relationship before issuing you with a BankID.

#### 3. Brief description of the service

BankID is an electronic identification and signing solution issued to you by your bank.

You may use your BankID to log in to Norwegian banks, to verify your identity on public and private websites, and to sign agreements digitally on the internet.

BankID may be used with an app, a code device or code card, a fixed password and your Norwegian national identity number. If you have enabled BankID Mobile, the security elements will include communication between the solution or website relying on BankID and your phone, as well as a PIN-code. BankID may also be used as an app on your smartphone, in which you use the phone's passcode or biometrics, in addition to your password where this is required, to confirm a login or signature.

#### 4. Storing, securing and blocking your BankID

##### 4.1. Your obligation to protect your BankID

To protect your BankID against fraud and unauthorised use, you must take all reasonable precautions to protect your password, codes, equipment, mobile phone and other digital devices you have for using BankID. This means, for example, that you:

- Do not disclose your BankID password or one-time codes to anyone, not even to family members, legal guardians, the Bank, BankID or the police. You must take all reasonable precautions to ensure that no one can see your BankID password or one-time password when you enter it.
- Store your BankID code device in a suitable place, ensuring that it is not openly accessible. If you bring your BankID code device with you outside your home, ensure it is not accessible to others.
- Must choose a strong BankID password that you do not use anywhere else. You can find guidelines on how to create strong passwords at nettvett.no. Change your password if you suspect that others have come to know it.
- Memorise your BankID password. If you still need to write down your password, it must be done in a manner that ensures nobody else can understand what the password is for. The password must not be kept together with the BankID code device or other equipment or devices.
- Use common sense and be cautious when you use your BankID password and one-time code, especially if you receive links by e-mail, text message/SMS or social media which require you to enter your BankID password or codes. Do not enter your BankID password or one-time codes if you are unsure of the website or that the sender of the link is the one it claims to be.

Keep in mind that you must never, orally or in writing, for example by phone, email or SMS, state your BankID passwords or one-time codes. This also applies where someone pretends to be for example your Bank, BankID or the police.

##### 4.2. Notifying the bank off loss or suspicion of loss of BankID

You must immediately notify the bank if you know or suspect that:

- others, including your spouse/partner or family members, know your BankID password
- you have lost your BankID code device
- your BankID code device is stolen
- you lost your mobile phone or other equipment you use with BankID, or this has been stolen, so that the bank can investigate any unauthorised use of your BankID.
- Someone has misused your BankID

You will not be charged for the bank's costs of issuing a new BankID after notification of loss, unless there are special circumstances on your part, such as repeated notifications of loss.

### 5. The bank's security measures and blocking of BankID

#### 5.1. Blocking BankID due to loss or suspected loss

After receiving a notification of loss from you, the bank must:

- immediately block your BankID, and
- confirm in writing to you that the notification has been received and that the BankID has been blocked.

#### 5.2. Blocking BankID on the bank's initiative

The bank may on its own initiative block your BankID when your bank has reasonable grounds to believe that:

- someone other than you are able to use your BankID;
- you have not complied with this agreement;
- you will not be able to comply with this agreement.

In the event that the bank blocks your BankID, the bank shall notify you and provide information on why your BankID has been blocked and on how you can move forward to have the block lifted.

### 6. Liability

#### 6.1 General liability

If you negligently or intentionally breach the terms and conditions of this agreement, you may be responsible for any loss incurred by your bank or others, including financial institutions and other solutions or websites relying on BankID, caused by your breach of this agreement.

If the bank negligently or intentionally breaches the terms and conditions of this agreement, the bank may be liable for any loss incurred by you, unless you have acted fraudulently.

#### 6.2 Responsibilities under the Financial Contracts Act

When your BankID is used to confirm payments or sign agreements on financial services, the Financial Contracts Act will regulate your and the bank's respective liability. Breaches of the obligations in this agreement may also be invoked by other providers of financial services when determining whether you are liable for a payment that has not been authorised or for the misuse of an electronic signature, as set out in the Financial Contracts Act.

### 7. Termination of the agreement

You are free to terminate the BankID agreement without prior notice, by notifying your bank of the termination in the agreed way. The bank will then block your BankID.

The bank may terminate the agreement if you breach this agreement, e.g. if you breach the obligation to take all reasonable precautions to protect your BankID-password, one-time codes, equipment, mobile phone and other digital devices you have to use BankID, and there is reasonable grounds to believe that breach of the obligation will occur again.

The bank must notify you of the termination four weeks in advance and include the reason for the termination. The bank can terminate the agreement with immediate effect if you have materially breached the terms and conditions or if you acted contrary to the requirement

of honesty or good faith towards your bank or towards other solutions or websites relying on BankID. The reason for the termination must be stated.

When terminating the agreement, the bank may block your BankID immediately, as described in section 5.2.

The bank may also terminate the agreement without specific notice if the customer relationship is terminated.

### 8. Price and price information

The price of BankID is to be shown in the bank's price list or published in another suitable way.

### 9. Processing personal data

Your bank is the data controller for your personal data and will process your personal data in accordance with the data protection rules and legislation (GDPR). For further information, see here:

[www.bankid.no/en/private/protection-of-privacy-and-status/](http://www.bankid.no/en/private/protection-of-privacy-and-status/)

### 10. Changes to agreement

The bank may, with two weeks' notice, make changes to the agreement when it has legitimate reasons for doing so. This includes price changes, changes caused by altered functionality or changes due to legislation. If the change is to your disadvantage, such as a price increase, the bank will notify you 2 months before the change comes into effect.

If security-related factors so require, the bank may without prior notice limit the area of application of your BankID or make other changes in security procedures or similar. The bank must notify you as soon as possible after such a change has been made.

### 11. Dispute resolution

If a dispute arises between you and the bank you have entered into an agreement on the use of BankID with, you can bring the case before the Norwegian Financial Services Complaints Board (FinKN) for consideration, provided the case is within the board's authority, and you have an objective interest in obtaining the board's consideration. The bank may bring a dispute about the use of BankID before the FinKN when your BankID has been used to confirm payment transactions.

If BankID is used to authorise a payment transaction that you deny having consented to, there are provisions in the Financial Contracts Act on what you must do, and on your bank's obligations. Further information on that what you should do can also be found in the account agreement between you and your bank.

Enquiries to FinKN are to be sent to Finansklagenemnda, Post box 53, Skøyen, N-0212 Oslo. Telephone no. (+47) 23 13 19 60. For further information, see [www.finkn.no](http://www.finkn.no).