BankID is issued by Stø AS which is owned by banks in Norway.

Agreement on Personal BankID

Version 1.1, May 2026

1. About Stø AS as Issuer of BankID

Stø AS ("Stø"), org. no. 927 611 929, is the issuer of BankID to natural persons (Personal BankID) and legal entities (Merchant BankID). Stø is owned by banks operating in Norway.

As issuer of BankID, Stø is regulated under the Act on Electronic Trust Services (lov om elektroniske tillitstjenester) and related regulations implementing EU Regulation 910/2014 (eIDAS) into Norwegian law.

2. About BankID

BankID is an electronic identification and signing solution issued to you as a consumer. You can use BankID for logging into online and mobile banking, authenticating payments, identifying yourself on public and private websites, and to digitally sign agreements.

BankID is used with the BankID App or a code device, your national ID number, and your personal password and/or biometrics such as fingerprint or facial recognition.

Only you as a physical person is allowed to use your BankID.

3. About the BankID agreement

This agreement governs the rights, obligations, and responsibilities between you as the holder of BankID and Stø as the formal issuer. Please read the agreement carefully and familiarize yourself with the requirements for security and protection of your equipment and personal password.

4. Obtaining BankID

Stø has chosen banks in Norway as agents for the issuance and management of BankID, as well as for customer support.

To obtain BankID, you must contact one bank. The order is placed by physically visiting the bank or another organization referred to by the bank. You must present a passport or national ID card for age and identity verification. For more information, see Stø's website: How to get BankID.

If you have questions or encounter problems after activating your BankID, please contact the bank. You must also notify the bank immediately upon discovering a security breach or if you suspect that your BankID is, or may be, misused by others, cf. the provisions on blocking of BankID in section 7.

If you suspect that your smartphone with the BankID App, code device, or personal password is lost or has been compromised, or if someone else has taken control of your BankID, you must contact the bank immediately for support.

5. Security. Control over BankID

For BankID to be a secure solution for you, it is important that you maintain control over your BankID by protecting your personal password and the digital devices you use for BankID. Notify the bank immediately if you suspect or are unsure whether others may have gained access to your BankID.

To protect your BankID from misuse, you must take all reasonable precautions to safeguard your personal password, codes, code device, smartphone, and other digital devices you use for BankID. This means, for example, that:

- Do not disclose your BankID password or one-time codes to anyone, not even to family members, legal guardians, the bank, the BankID-issuer or the police. You must take all reasonable precautions to ensure that no one can see your password or codes when you enter them.
- Store your code device securely, ensuring that it is not openly accessible. If you take it outside your home, ensure it is not accessible to others.
- Choose a strong 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 others may 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 onetime 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 code if you are unsure of the website or that the sender of the link is who it claims to be.

6. Notification in case of suspected security breaches etc.

You must immediately notify the issuer's agent referenced in section 4 if you know or suspect that:

- others, including your spouse/partner or family members, know your BankID password,
- you have lost your code device,
- your code device has been stolen,
- you lost your mobile phone containing BankID app or other equipment you use with BankID, or this has been stolen, and/or
- someone has misused you BankID.

You will not be charged the costs for issuing a new BankID after notification of security breaches or loss of code device/smart phone, unless there are special circumstances on your part, such as repeated notifications of similar nature.

7. Blocking of BankID

Upon notification as set out in section 6, the issuer will:

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

Your BankID may also be blocked by issuer if there is reasonable cause to believe that:

- someone other than you can use your BankID,
- your BankID is used by a robot or similar software that performs tasks automatically or semi-automatically based on your BankID,
- you have not complied with this agreement, or
- you will not be able to comply with this agreement.

You will be notified in the event of blocking. You can request information on why your BankID has been blocked and on how you can move forward to have the block lifted, by contacting Stø's selected agents referenced in section 4.

8. Liability

If you negligently or intentionally breach the terms of this agreement, you may be held liable for losses incurred by Stø or others, including banks and other BankID merchants.

If Stø or Stø's agents negligently or intentionally breaches the terms of this agreement, Stø may as issuer of BankID be held liable for losses you incur, unless you have acted fraudulently. Stø is not liable for financial losses arising from the use of BankID in connection with ordering or acquiring goods and services or any other form of digital communication (authentication/signing) with third parties, such as providers of financial services or other public and private BankID merchants.

9. Term and termination of the agreement

The customer relationship lasts until one of the parties terminates the agreement.

You may terminate the BankID agreement at any time without providing any specific reason. Such termination can be made by notifying your bank. Stø will then block your BankID.

Stø may terminate the agreement when you no longer fulfil the requirements to have a BankID.

Stø may also terminate the agreement if you breach this agreement, including if you fail to take all reasonable precautions to protect your personal BankID passwords, codes, equipment, smartphone, and other digital devices you use for BankID, and there is reason to believe that similar breaches will occur again.

Termination by Stø shall have four (4) weeks' notice and the reason for termination must be stated. Stø may terminate the agreement with immediate effect in the event of a material breach by you or if you have acted dishonestly or in bad faith towards Stø, your bank, or BankID merchants. It shall also constitute a material breach if your BankID is used by a robot or similar software to perform tasks automatically or semi-automatically based on your BankID. The reason for termination must be stated.

Upon termination and cancellation of the agreement, your BankID will be blocked immediately, as described in section 7.

10. Prices and price information

In order to ensure sustainable and responsible operation, management and further development of the BankID service, Stø may introduce pricing for BankID. The introduction of pricing for BankID will be notified in advance as mentioned in section 12. All prices are stated in Stø's price list or provided in another suitable manner.

11. Processing of personal data

Stø is the data controller for personal data processed in connection with issuance, renewal, use, notifications, blocking, and revocation of BankID, as well as for validity checks and other control actions, including monitoring and detection of fraud, identity violations, and other misuse of BankID. Stø will process your data in accordance with the Personal Data Act. For more information, see www.bankid.no/privat/personvern-og-regler/.

Your bank acts as a data processor for administration and customer support according to agreement with Stø.

12. Changes to the agreement

This agreement may be amended by Stø with two (2) weeks' notice when Stø has legitimate reasons for such changes. This includes changes in prices, changes due to altered functionality, or changes resulting from legislation. If the change is to your detriment, such as introduction of BankID prices or a subsequent price increase, Stø will notify the change and the background to it two (2) months before the change takes effect.

If security considerations make it necessary, Stø may, without prior notice, restrict the use of BankID and make other changes to security procedures or similar. Stø will notify you of this as soon as possible after the change.

13. Dispute resolution

If a dispute arises between you and Stø as issuer of BankID, about the understanding or legal effects of this agreement, the parties shall first seek to resolve the dispute through dialogue.

If the dispute is not resolved through dialogue, and the dispute concerns the issuance/contracting, renewal or blocking/revocation of BankID, you can bring the matter before the Norwegian Financial Services Complaints Board (Finansklagenemnda) for a statement or decision.

For further information about the Financial Services Complaints Board, please see www.finkn.no.

_____	_____	_____
Date	Place	Signature