Terms for Merchants' Access to and Use of the BankID Service

(«Merchant Terms»)

bankAxept bankID

Besøksadresse
Biskop Gunnerus gate 14 A
0185 Oslo

Postadresse
Postboks 9236 Grønland
0134 Oslo

Org.nr.:
NO 927 611 929 MVA

Content

PART I INTRODUCTORY PROVISIONS

1. ABOUT THE MERCHANT TERMS

The Merchant Terms are structured as follows: Part I sets out introductory provisions, Part II contains general conditions for general terms for legal entities' access to and use of BankID and the BankID Service. Part III contains special terms applicable to financial entities subject to the Act of May 27, 2025 on digital operational resilience in the financial sector (DORA-loven). A glossary is included in Part IV.

The Merchant Terms are established by Stø AS in its role as Issuer of BankID and provider of related services and products included in the BankID Service.

The Merchant Terms govern the Issuer's and legal entities' rights, obligations, and responsibilities towards each other in relation to the access and use of Merchant BankID and the BankID Service. The Merchant Terms in force at any given time are mandatory for legal entities that enter into an agreement with the Issuer regarding BankID and other services and products covered by the BankID Service.

2. ABOUT THE ISSUER OF BANKID

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

For the issuance of electronic identification (eID) and qualified trust services, Stø AS is regulated under Act of 15 June 2018 No. 44 on electronic trust services (lov om elektroniske tillitstjenester) and associated regulations implementing EU Regulation No. 910/2014 (eIDAS).

3. SERVICE DESCRIPTION AND DOCUTMENTATION

Below are web addresses/links to supplementary descriptions and other Documentation as part of the Merchant Terms:

- Issuer's website: BankID
- Service and product descriptions: Våre tjenester
- Technical and functional description (Documentation): BankID documentation

4. ABOUT BANKID

BankID is an electronic ID and a qualified trust service that a Merchant may use for authentication and identification of natural persons, as well as signing of documents.

A Personal BankID meets the requirements for qualified certificates for natural persons and advanced/qualified electronic signatures under eIDAS, as implemented in Norwegian law. Terms for issuing Personal BankID to natural persons (End Users) are not covered by these Merchant Terms.

PART II GENERAL CONDITIONS

5. ORDERING, VERIFICATION AND CONCLUSION OF AGREEMENT

5.1 Ordering of the BankID Service

To order and purchase Merchant BankID and other services and products included in the BankID Service, the Ordering Party must normally contact an authorized Reseller as described on the Issuer's website.

During the ordering process, the Reseller acts under power of attorney and on behalf of the Ordering Party. The Merchant Agreement, including these Merchant Terms and the accompanying Documentation, shall be deemed accepted by the Ordering Party upon signing the Merchant Agreement and confirmation by the Reseller.

5.2 Eligibility requirements - Rejection

A Merchant must at all times be registered in Norway or another state within the EU/EEA.

The Merchant's business must comply with applicable laws and regulations and must not be of a nature that could undermine the trust in the Trademark, the BankID Service, the Issuer, or the Issuer's reputation or goodwill.

The Issuer, or the Reseller acting on behalf of the Issuer, may refuse to issue a Merchant BankID to an Ordering Party that does not meet the eligibility requirements, where there is reasonable suspicion that the Ordering Party's actual business does not comply with applicable laws or regulations, or if the business could otherwise undermine the trust in the Trademark, the BankID Service, the Issuer, or the Issuer's reputation or goodwill.

If the Issuer or the Reseller rejects an order for the BankID Service on behalf of the Issuer for legitimate and reasonable grounds, the Issuer or the Reseller shall provide the Ordering Party with the reason for such rejection.

5.3 Identification and identity control of the Ordering Party

When ordering and accepting the Merchant Terms, the Ordering Party shall be represented by a person with signing authority, or natural person with written authorization from a person with signing authority, having the right to bind the Ordering Party to the BankID Service Agreement.

The Reseller shall, on behalf of the Issuer, carry out verification of identity and credentials for the Ordering Party as a legal entity (company) and for the natural person acting as the authorized signatory on behalf of the Ordering Party.

To ensure that the order is complete and legitimate, the Reseller shall, on behalf of the Issuer:

a) Ensure that the Ordering Party and the Ordering Party's business are correctly identified, and that the identified authorized signatory has the necessary legal capacity and authority to bind the Ordering Party when entering into the Merchant Agreement; and

b) Verify that the order does not contain errors or omissions of significance for the issuance of Merchant BankID and the provision of other ordered services and products in the BankID Service

The Issuer may, in addition to the Reseller, engage one or more agents to perform identification and identity verification of the Ordering Party.

5.4 Conclusion of the Agreement

If the order and the accompanying verified documentation are found to be in good order, and the Ordering Party's authorized signatory has signed the Merchant Agreement, the Ordering Party will obtain status as Merchant and be granted access to the BankID Service.

5.5 Notification of errors and deficiencies

Before activating the BankID Service, the Merchant shall immediately verify that the company details and contact information provided match the information submitted in the order for the BankID Service, in order to identify any errors or deficiencies.

As the BankID Service may only be used by the Merchant itself (see Section 7.1), the Merchant must ensure that organization number to which the Merchant BankID has been issued is correct.

If any errors or deficiencies are discovered, the Merchant shall promptly notify the Reseller, acting on behalf of the Issuer, of any matters that need to be corrected or amended prior to using the BankID Service, including organization number, address, company name, ownership, contact persons, and similar details.

6. INTEGRATION

The Merchant shall integrate with the BankID OpenID Connect (OIDC) interface in accordance with the Documentation and applicable security standards.

The Merchant undertakes to test and maintain its integration to ensure compatibility with the interface at all times.

7. USE OF THE BANKID SERVICE

7.1 Scope of Merchant BankID

Permitted use cases for Merchant BankID and the products included in the BankID Service are specified in the Service Description for the BankID Service.

The Merchant may only use the BankID Service within the organization number to which the Merchant BankID has been issued. In the event of a business transfer or other corporate changes, including mergers or demergers, that results in the Merchant no longer holding the organization number associated with its Merchant BankID, continued use of the BankID Service requires issuance of a new Merchant BankID linked to the new organization number.

See also Section 13 regarding intellectual property rights and usage rights.

7.2 Usage Restrictions – ID Exchange with Personal BankID

ID exchange with Personal BankID is not permitted unless the Merchant has entered into an agreement with the Issuer for the purchase of ID exchange as an add-on product under the BankID Service or has entered into a separate agreement with the Issuer for ID exchange.

Optional features, pricing, and typical scenarios for ID exchange are described in detail on the Issuer's website.

8. VALIDITY CONTROL AND VALIDATION

The Issuer has established systems for validity checks of Personal BankID, including a register of valid, suspended, and revoked BankID Certificates (the Validation Register). Information recorded in the Validation Register will be retained for up to ten (10) years after the validity period of the BankID has expired or been revoked.

The Merchant shall always perform validity checks and submit validity requests to the Issuer in accordance with the requirements set out in the Documentation.

The Issuer shall confirm or deny the validity of a Personal BankID. The response to a validity request from the Merchant shall at a minimum include:

- Information on whether the Personal BankID has been revoked or suspended;
- Information on whether the Personal BankID is unknown.

The register data will be used by the Issuer to ensure that Personal BankID remains valid at all times and that its use complies with the applicable agreement terms.

9. EXPIRY, RENEWAL, AND BLOCKING OF BANKID

9.1 Expiry and renewal

Before the expiry of its validity period, the Merchant BankID will be renewed automatically.

9.2 Duty to notify in case of loss

The Merchant must notify the Issuer in writing as soon as possible after becoming aware of or suspecting that the Merchant BankID has been misused or compromised.

9.3 Blocking of Merchant BankID

If there is suspicion of misuse or compromise, the Merchant shall refrain from using the Merchant BankID or the BankID Service as a whole and/or from accepting the use of Personal BankID. The Merchant shall assist the Reseller and the Issuer to ensure that the Merchant BankID is blocked as quickly as possible. The Issuer will carry out the blocking.

The Issuer may, on its own initiative, block a Merchant BankID if the certificate no longer contains correct information or if, in the Issuer's reasonable opinion, there are other legitimate reasons for blocking, including situations where the BankID Service is or may be misused or used for unlawful activities. Legitimate reasons for blocking also include if the Merchant's use of the BankID Service could undermine confidence in the Trademark, the BankID Service, or the Issuer's reputation or goodwill.

The Issuer may block a Merchant BankID that has not been used for a period of six (6) months.

10. PROCESSING OF INFORMATION IN THE BANKID SERVICE

10.1 Information about the Merchant

The Merchant BankID contains, among other things, the following information:

- Identification of the Issuer;

- Details of the Merchant's company name and Norwegian organization number or other unique identifier;
- The certificate's validity period;
- Data necessary to verify the Merchant's digital signature;
- The Issuer's digital signature;
- Data uniquely identifying each BankID (serial number).

The above information will be available to the Issuer, the Merchant, and the Merchant's chosen Reseller.

10.2 Exchange and Use of Transaction Data
When performing BankID Transactions, transaction data will be included in the message exchange between the Merchant and the End User. Both the Merchant and the Issuer may make transaction data available to the relevant End User.

The Issuer will use this transaction data to establish and maintain a register of Merchants and their transactions for billing purposes. Furthermore, transaction data will be used as a basis for notifications, messages, and transaction information to End Users, for monitoring and detecting identity fraud, criminal activity, and other misuse of BankID, as well as for further development of the BankID Service.

10.3 Responsibility for Processing Personal Data
Processing of personal data shall comply with applicable data protection legislation and other relevant regulatory requirements.

The Merchant is the data controller for personal data processed by the Merchant when using Merchant BankID.

The Issuer is the data controller for personal data processed by the Issuer in connection with issuance, renewal, use, message exchange, blocking, and revocation of BankID, as well as when performing validity checks and other control actions, including providing information to End Users and monitoring and detecting fraud and other misuse of BankID.

10.4 Disclosure of End User's national ID number or D-number
Issuer's disclosure of an End User's national ID number or D-number under the BankID Service requires that the Merchant is legally obligated under law, regulations, or decisions issued pursuant to law to collect and process the End User's national ID number or D-number in connection with establishing a customer relationship or providing services to the End User.

The Merchant's collection and use of national ID numbers or D-numbers presupposes that the Merchant has applied for access to such data, based on the Merchant's declaration in the Merchant Agreement of its statutory obligation to collect such information, and has received approval from the Issuer. The Issuer may reject applications for disclosure of national ID numbers or D-numbers.

10.5 Use of Data for Detection and Prevention of Identity Violations
The Issuer operates an anti-fraud system for monitoring and tracking BankID transactions to prevent, detect, and stop identity violations and other criminal acts against Merchants, End Users, the Issuer, and/or affected third parties.

The Parties shall at all times cooperate to prevent or limit the scope of criminal activity, identity violations, and other misuse of BankID, stop any attempts, and identify incidents and causes. To fulfill the purpose of the anti-fraud system, the Merchant shall share relevant data with the Issuer, recorded by the Merchant in connection with logins, service purchases, and/or signing of agreements or other dispositions. Such data shall be shared with the Issuer in real time, near real time, or after the transaction, as specified in the section on BankID Anti-Fraud below.

The data to be shared by the Merchant is specified in the Service Description for the BankID Service, while interfaces, formats, and operational requirements for technical integration and information exchange between the Merchant and the Issuer are described in the Documentation.

10.6 Statistical Data

The Issuer may use data that is not subject to confidentiality or that, after anonymization, is no longer considered personal data, for statistical purposes. This includes anonymized data, volume data, frequency measurements, or other information collected during the provision of the Service (service data).

11. BANKID ANTI-FRAUD

11.1 Mandatory connection

The Merchant will, as part of the BankID Service, be functionally connected to the BankID anti-fraud system.

The functionality of the anti-fraud system is described in detail in the Service Description for the BankID Service and in the Documentation.

11.2 Purpose of the Anti-Fraud system

The anti-fraud system encompasses the development, management, and operation of software, databases, hardware, and interfaces for collecting data on BankID Transactions, and, as an optional add-on service, relevant alert services aimed at detecting identity violations, fraud, and other criminal acts against Merchants, End Users, the Issuer, and other actors in the BankID value chain.

Under an optional add-on service, the Merchant may receive alerts regarding BankID Transactions that the Issuer assumes have an increased risk of criminal activity, based on the Issuer's own data and data submitted by the Merchant. Alerts ordered separately by the Merchant may include various alarms, signals, analyses, and reports delivered through defined interfaces.

Different types of alarms or analyses for individual transactions may, under an add-on service, be provided in real time, near real time, or after the BankID Transactions, depending on the data submitted by the Merchant, the detection capabilities of the anti-fraud system, and available system capacity.

11.3 Submission of Data

The Merchant shall submit defined data to the Issuer via the specified API for transaction analysis and, where applicable as an add-on service, receive signals, alerts, etc., in return, in accordance with the Service Description for the BankID Service and the Documentation.

Data formats, frequency, and other criteria for such information exchange shall be determined by the Issuer.

12. CONFIDENTIALITY

The Parties undertake to comply with statutory and contractual confidentiality obligations and not to disclose to unauthorized persons any confidential information received from the other Party during the contractual relationship, regardless of the form or means by which the information is received, or whether it is communicated in writing or orally.

Confidential information means information that a Party has expressly designated as confidential, as well as all other information about a Party's business, information of a business, financial, commercial and technical nature, information about products and development, trade secrets, expertise, information about the respective Party's personnel, consultants, subcontractors and customers, or information otherwise reasonably considered confidential by the Party providing the information.

A Party undertakes not to use the other Party's confidential information in any way other than to fulfill its obligations under the agreement.

Confidential information shall only be disclosed to the Party's employees, advisors, or consultants who need the information in the course of their duties to enable the Party to fulfill its obligations under the agreement. Each Party shall ensure that all its employees, advisors, or consultants who gain access to the other Party's confidential information are obliged to comply with the confidentiality provisions in the legislation, Merchant Terms, special confidentiality agreements, or equivalent provisions and obligations.

A Party's obligation to comply with confidentiality under this section does not apply to information that

- was already known to the receiving Party at the time of receipt,
- is or becomes publicly available or known without the receiving Party having breached confidentiality,
- is lawfully received from a third party, provided that the third party is not bound by confidentiality,
- is required to be made publicly available by final court judgment, government decision, or otherwise under applicable law, or
- is developed independently by a Party without the other Party's confidential information.

Confidentiality obligations are waived in the case of disclosure orders under the Criminal Procedure Act, other statutory disclosure obligations, government orders pursuant to law, or if required by court judgments.

Disclosure of necessary information during security audits or inspections by public authorities is not considered a breach of confidentiality.

The confidentiality obligation applies for a period of two (2) years after termination of the Agreement.

13. INTELECTUAL PROPOERTY RIGHTS AND LICENSING

BankID is protected by copyright and is also a registered trademark owned and managed by the Issuer.

All intellectual property rights, including patents, copyrights, trademarks, and design rights related to the Trademark, the BankID Service, and associated Documentation and certificate policies belong to the Issuer and/or the Issuer's licensors, subcontractors, or partners.

The Merchant is granted a limited, non-exclusive, non-transferable, revocable right to use the Trademark, the BankID Service, and the Documentation solely for the purposes of preparing, installing, integrating, and using the BankID Service as specified in the Documentation. The Merchant does not acquire any intellectual property rights, in whole or in part, to the Trademark, the BankID Service, or the associated Documentation.

The Merchant shall not make any changes (including further development or otherwise) to the BankID Service or the Documentation.

The BankID Service may only be used in connection with the Merchant's own business and may not be sublicensed.

The Issuer, or any party authorized by the Issuer, has the right to verify compliance with the license terms, and the Merchant is obliged to provide the Issuer or its authorized representative with necessary access to the Merchant's systems and use of the BankID Service and software for such verification.

14. USE OF THE TRADEMARK

The Merchant is both authorized and required to use the "BankID" trademark when utilizing the BankID Service and must clearly indicate that the Merchant uses the BankID Service in its business operations.

The presentation of the Trademark must comply with the form, logo, design, format, color, and quality standards specified in the Issuer's brand guidelines and may only be used in accordance with the instructions published on the Issuer's website at any given time.

The Issuer reserves the right to publicly disclose that the Merchant uses the BankID Service in its business, including on the Issuer's website and in other relevant marketing materials.

15. DELIVERY AND SUPPORT

Unless otherwise specifically agreed, the BankID Service shall be delivered in accordance with the Service Description for the BankID Service and the Documentation. No guarantee is provided that the BankID Service will function with the Merchant's or Reseller's designated products or other third-party products, unless explicitly stated in the Documentation.

The Reseller shall provide the Merchant with necessary product guidance, technical assistance, and first-line support for services and products included in the BankID Service.

16. CHANGES TO THE AGREEMENT AND THE BANKID SERVICE

The Issuer may make changes to the Merchant Terms and the BankID Service, provided such changes do not materially disadvantage the Merchant's use of the BankID Service.

The Merchant will be informed in advance, within a reasonable timeframe, via the Issuer's website about any new version of Merchant BankID and the BankID Service, including:

- when the new version of the BankID Service is made available to the Merchant,
- what changes must be made by the Merchant,
- when the Merchant will have access to the test environment,
- which versions are supported after the change, and
- the deadline for implementing the change.

The Merchant is obliged to adopt new versions of the BankID Service within the deadline specified by the Issuer.

Changes that are significantly detrimental to the Merchant shall be announced at least six (6) months in advance on the Issuer's website. This includes, for example, prolonged downtime of the BankID Service or situations where Merchants must make substantial changes to their own systems to continue using the BankID Service.

If circumstances related to the Reseller and/or the Merchant, security considerations, or regulatory decisions or orders from public authorities make it necessary, the Issuer may unilaterally and without prior notice amend the Merchant Terms and the BankID Service in accordance with the situation. The Issuer shall notify the Merchant of such changes as soon as possible via its website.

17. TRANSFER OF RIGHTS AND OBLIGATIONS

The Merchant is not entitled to transfer any rights or obligations under the Merchant Agreement to any other party, including companies within the same corporate group, whether through business transfers or other forms of corporate restructuring such as mergers or demergers.

18. BREACH - TERMINATION

Either Party may terminate the Agreement with immediate effect by written notice if:

- A Party fails to comply with the Merchant Terms and does not remedy the breach within sixty (60) calendar days after receiving written notice from the other Party requesting correction;
- A Party commits a material breach of the Merchant Terms and does not remedy the breach within thirty (30) calendar days after receiving written notice from the other Party requesting correction;
- A Party files for bankruptcy, or another party petitions for bankruptcy or public administration, and such petition is not dismissed within thirty (30) calendar days; or
- A Party is declared bankrupt, placed under public administration, liquidated, or initiates debt negotiations, liquidation, or similar proceedings.

Material breach also includes situations where the Merchant or its Reseller is in material breach of payment to the Issuer, or where the Merchant uses BankID unlawfully, for illegal activities, or in a manner that may damage the reputation, goodwill, or trust in the Trademark, the BankID Service, or the Issuer.

The Merchant's right to hold a Merchant BankID and use the BankID Service may be revoked if the Merchant acts with gross negligence or willful misconduct in violation of the provisions of the Merchant Agreement.

19. LIABILITY AND LIMITATION OF LIABILITY

19.1 Merchants liability

The Merchant is, in accordance with general rules of liability for damages, responsible for direct financial losses suffered by the Issuer as a result of the Merchant, or any party for whom the Merchant is responsible (such as a chosen subcontractor), acting in violation of the Merchant Agreement.

19.2 Issuer's liability

The Issuer is, in accordance with general rules of liability for damages, responsible for direct financial losses suffered by the Merchant as a result of the Issuer, or any party for whom the Issuer is responsible (such as a chosen subcontractor), acting in violation of the Merchant Agreement.

19.3 Limitation of liability

Compensation for indirect losses cannot be claimed. Indirect losses include, but are not limited to, lost profits of any kind, lost savings, and claims from third parties. Loss of data is considered an indirect loss except for costs related to the reconstruction of data and other direct costs incurred by the injured Party as a result of the loss of data.

The Issuer is not liable for damage or financial loss resulting from the BankID Service being used outside the specified scope of application disclosed to the party relying on a Personal BankID. The Issuer is also not liable for losses caused by fraud, deception, or other criminal acts committed by the End User or unauthorized third parties against the Merchant following misuse of Personal BankID.

The Issuer's liability for losses suffered by the Merchant is in any case limited to NOK 100,000 per transaction. The total compensation per calendar year for losses arising after acceptance of the Merchant Terms is limited to an amount equal to the total annual fee paid by the Merchant for the BankID Service, including VAT.

If the liable Party or any party for whom it is responsible has acted with gross negligence or intent, these liability limitations do not apply.

The Parties' liability for damages may be reduced or eliminated if the injured Party has contributed to the loss through negligent failure in its own routines or other negligence.

A Party's liability lapses to the extent that the injured Party is compensated for its loss by others.

20. FORCE MAJEURE

Neither Party can be held liable for breach of contract resulting from an extraordinary situation beyond the control of one of the Parties that makes fulfillment of the Merchant Agreement difficult and which, according to general rules of liability for damages, is considered force majeure.

The exemption from the obligation to fulfill the Merchant Agreement lasts only as long as the extraordinary situation persists. The Parties are obliged to mitigate the effects of the extraordinary situation as far as possible.

A Party invoking force majeure must notify the other Party without undue delay and keep the other Party continuously informed of the situation. If the force majeure situation lasts for more than thirty (30) calendar days, either Party may terminate the Merchant Agreement with immediate effect.

21. TERMINATION OF THE AGREEMENT

21.1 Termination by Notice

The Agreement shall remain in effect until terminated by either Party with three (3) months' written notice to the other Party.

21.2 Termination for cause

The Agreement may otherwise be terminated with immediate effect in the event of material breach by the other Party or under other circumstances as specified in Section 18 (Breach – Termination).

21.3 Effect of Termination

Upon termination of the Agreement, the Merchant shall cease all use of the Trademark. The Issuer will block and invalidate the Merchant BankID to prevent further use.

22. GOVERNING LAW, DISPUTE RESOLUTION AND VENUE

The Parties rights and obligations under the Reseller Agreement are determined in full by Norwegian law. Any dispute between the Parties shall first be sought resolved through negotiations.

If negotiations do not succeed, either Party may bring the matter before the ordinary courts.

Venue is Oslo.

PART III SPECIAL CONDITIONS

23. ADDITIONAL TERMS FOR FINANCIAL INSTITUTIONS SUBJECT TO DORA

23.1 Regulatory Requirements under DORA

When delivering the BankID Service to financial entities (hereinafter referred to as "Financial Institutions") acting as Merchants, the Parties shall comply with the Act of May 27, 2025 No. 18 on Digital Operational Resilience in the Financial Sector ("DORA Act") and related regulations, or equivalent rules in the Financial Institution's home country. The DORA Act implements Regulation (EU) 2022/2554 of December 14, 2022 on digital operational resilience for the financial sector ("DORA Regulation").

The special terms below ("DORA Terms") supplement the Merchant Agreement, including the Merchant Terms (Part I and Part II), with specific requirements under the DORA Act that Financial Institutions are obligated to include in agreements with ICT service providers. The Merchant Terms partially cover these requirements; the DORA Terms are added to highlight elements not clearly specified in the general terms (Part I and Part II), the Service Description, and the Documentation.

In the event of any conflict between the DORA Terms below and the Merchant Agreement, including the Merchant Terms (Part I and Part II), the DORA Terms shall prevail.

23.2 Obligation to Assist and Continuity Plan

The Issuer shall provide assistance to the Financial Institution and relevant supervisory authorities, as well as persons or entities appointed by them, to ensure that the Financial Institution's operations comply with the DORA Act and regulatory decisions issued under the DORA Act. This duty to assist also applies during crisis management and other adverse events, as well as upon termination of the Agreement.

Upon written request from the Financial Institution, the Issuer shall provide its Business Continuity Plan for the BankID Service. The Issuer shall regularly conduct training and testing of its continuity plan. Test results shall be shared with the Financial Institution upon request.

23.3 ICT Security and Threat Assessments

If deemed relevant and necessary for ICT security related to the BankID Service, the Issuer shall, upon reasonable written notice, participate in the Financial Institution's ICT security and digital operational resilience training programs.

Upon reasonable written notice to the Issuer, the Financial Institution may conduct threat-led penetration tests (TLPT) and other forms of security testing of all or parts of the BankID Service. Such tests shall be planned and carried out in cooperation with the Issuer. The Financial Institution shall promptly provide the Issuer with access to documentation showing test results and any remediation plans following the Financial Institution's security tests of the BankID Service.

23.4 Risk Analyses

The Issuer shall maintain procedures for conducting annual risk analyses and additional risk analyses in connection with changes or events affecting ICT security related to the BankID Service. Risk analysis shall be documented and comply with industry standards.

The Issuer shall inform the Financial Institution of any new risk factors affecting ICT security under the Merchant Agreement and the use of the BankID Service. Such information shall include the cause, consequences, and an action plan to address the new risk factors.

23.5 Reporting of Serious ICT-Related Incidents
The Issuer shall notify the Financial Institution as soon as possible of any deviations from agreed delivery conditions and, in accordance with the DORA Act, report serious ICT-related incidents that negatively impact the BankID Service and are significant for the Financial Institution. The report shall include the cause, consequences, and an action plan to address such deviations and incidents.

The Parties shall also notify each other of serious cyber threats.

23.6 Access to and Processing of Data and Personal Data
Upon written request from the Financial Institution, the Issuer shall promptly provide access to the Financial Institution's data in a standardized format, unless the Financial Institution already has access or possession of the data. If necessary, the Financial Institution shall be granted access to premises and the right to copy relevant documentation on-site if critical for operations.

The Parties shall ensure that all relevant personal data processed under the Merchant Agreement meets requirements for availability, integrity, authenticity, and confidentiality, and is protected against unauthorized access.

The Issuer shall have written agreements with its subcontractors ensuring compliance with the Issuer's obligations under the BankID Service and establishing adequate procedures for monitoring and verifying that subcontractors meet agreed requirements for security, service levels, reporting, processing locations, etc.

Upon termination of the Merchant Agreement, regardless of reason, the Issuer shall ensure access, recovery, and return of all data belonging to the Financial Institution in an easily accessible format, unless the Financial Institution already possesses the data.

23.7 Assistance in Case of Adverse Incidents – Compensation
The Issuer shall provide assistance to the Financial Institution free of charge in handling adverse incident under the BankID Service caused by the Issuer or its subcontractors.

For assistance related to adverse incidents under the BankID Service caused by the Financial Institution or its other suppliers, the Issuer shall be entitled to reasonable compensation for its work, based on actual time spent and documented costs necessary to manage the incident.

23.8 Assistance upon Termination of the Agreement – Exit Plan

Upon termination of the Agreement, regardless of reason, the Issuer shall keep the BankID Service available to the Financial Institution and provide reasonable related assistance until the Financial Institution has established an alternative solution to the BankID Service. Such access and assistance are conditional upon the Financial Institution confirming in writing its compliance with its obligations under the Merchant Agreement and shall in any case not exceed eighteen (18) months after the termination date.

The Issuer shall also assist the Financial Institution in developing and maintaining an exit plan to ensure that termination of the Merchant Agreement and any transition to a new third-party provider or internal solution within the Financial Institution can be carried out with minimal risk of disruption.

Assistance provided by the Issuer under the first and second paragraphs shall be compensated by the Financial Institution in accordance with the Issuer's standard prices for authentication and signing services plus a 10% surcharge, as well as hourly rates for consulting services as listed on https://bankid.no/bedrift/priser. This does not apply if termination of the Agreement is due to material breach by the Issuer.

23.9 Relationship with Relevant Supervisory Authorities
Relevant supervisory authorities, including people appointed by such authorities, shall have the right to obtain information from the Issuer and to conduct inspections at the Issuer and/or its subcontractors where deemed necessary as part of the supervision of the Financial Institution.

General information about the Issuer's subcontractors and data processing locations is available on https://stoe.no/om-selskapet/baerekraft. Further details may be provided upon written request from the Financial Institution.

23.10 Extended Right of Termination under DORA Regulation Article 28(7)
The Parties' right to terminate the Merchant Agreement due to breach, etc., follows from the Merchant Terms Part II, Section 18 (Breach – Termination).

In addition to these provisions, the Financial Institution has the right to terminate the Merchant Agreement in situations specified in Article 28(7) of the DORA Regulation.

PART IV GLOSSARY

Explanations of terms and expressions used in the Reseller Agreement, the Merchant Terms and other Documentation on relevant websites:

a) **BankID OIDC:** OpenID Connect; technical interface and integration point between Issuer and Merchants for delivery of the BankID Service.

b) **BankID Certificate**: A sequence of data containing an End User public key and other information signed with the Issuer's private key. BankID is used for electronic message exchange with other End Users and Merchants by confirming the correct identity of the parties (authentication) and securing the content against alteration (integrity).

c) **BankID Service**: Collective term for Merchant BankID and other services and products included in the service delivery at any given time.

d) **BankID Transaction**: Message exchange between End User, Merchant and Issuer secured with BankID.

e) **Ordering Party:** A legal entity that contacts a Reseller intending to purchase and enter into agreement for the BankID Service with the Issuer directly or via a Reseller.

f) **Merchant**: A company or other type of legal entity, registered in the Register of Business Enterprises or a corresponding public register, that has entered into an agreement for the BankID Service with the Issuer either directly or through a Reseller

g) **Merchant BankID:** BankID issued to a Merchant.

h) **Merchant Agreement:** The Merchant's agreement with the Issuer for the BankID Service including the order form, Merchant Terms, service description and other Documentation.

i) **Merchant Terms**: The standardized general and specific terms for Merchants' access to and use of the BankID Service.

j) **Documentation**: The Issuer's current documentation for the description, testing, integration, implementation, use and modification of the BankID Service, as amended from time to time.

k) **Reseller:** Authorized entity that, on behalf of the Issuer, enters into agreement with Merchants for access to and use of the BankID Service.

l) **ID Exchange**: Authentication with and any other use of Personal BankID to activate, restore or increase trust in the Merchant's identification or authentication mechanism in its own app, establishment of derived identities of End Users for use in merchant's own business or within the same group as the Merchant, and/or to establish and forward derived identities of End Users to the Merchant counterparties.

m) **Qualified Electronic Signing**: A qualified trust service for digital signing of documents online (QES), offered by Stø as a separate trust service or in combination with Qualified Timestamping, pursuant to the Act of 15 June 2018 No. 44 on electronic trust services.

n) **Qualified Timestamping**: A qualified trust service for digital timestamping online (QTimestamp), offered by Stø as a separate trust service or in combination with Qualified Electronic Signing (QES), pursuant to the Act of 15 June 2018 No. 44 on electronic trust services.

o) **Party/Parties:** The Issuer and the Merchant are each referred to individually as a "Party" and collectively as the "Parties."

p) **Personal BankID:** BankID issued to a natural person as End User.

q) **End User**: Natural person who has entered into an agreement with Issuer for Personal BankID.

r) **Issuer**: Stø AS, org.no. 927 611 929.

s) **Validation Register:** A central register at the Issuer of valid, suspended, and revoked BankID Certificates.

t) **Trademark**: Norwegian trademark registrations no. 257727, 258031, 290364 and 290365.