



BankID видається компанією Stø AS, яка належить банкам Норвегії.

## Угода про персональний банківський ідентифікатор

Версія 1.0, квітень 2026

### А. Про Stø AS як емітента BankID

Stø AS ("Stø"), організовальний номер 927 611 929, є емітентом BankID для фізичних осіб (Personal BankID) та юридичних осіб (Merchant BankID). Stø належить банкам, що працюють у Норвегії.

Як емітент BankID, Stø регулюється Законом про електронні довірчі послуги ([Закон про електронні довірчі послуги](#)) та пов'язаних нормативних актів, що впроваджують Регламент ЄС 910/2014 (eIDAS) у норвезьке законодавство.

### Б. Про BankID

BankID — це рішення для електронної ідентифікації та підписання, яке видається вам як споживачу. Ви можете використовувати BankID для входу в онлайн- та мобільний банкінг, автентифікації платежів, ідентифікації себе на публічних і приватних сайтах, а також для цифрового підписання угод.

BankID використовується разом із додатком BankID або кодовим пристроєм, вашим національним ідентифікаційним номером та вашим особистим паролем і/або біометрією, такою як відбиток пальців або розпізнавання обличчя.

Лише ви, як фізична особа, можете використовувати свій BankID.

### В. Про угоду BankID

Ця угода регулює права, зобов'язання та обов'язки між вами як власником BankID та Stø як офіційним емітентом. Будь ласка, уважно прочитайте угоду та ознайомтеся з вимогами щодо безпеки та захисту вашого обладнання та особистого пароля.

### Г. Отримання BankID

Stø обрав банки Норвегії як агентів для випуску та управління BankID, а також для підтримки клієнтів.

Щоб отримати BankID, потрібно звернутися до свого банку. Замовлення здійснюється шляхом фізичного візиту до банку або іншої організації, яку банк рекомендує. Ви повинні пред'явити паспорт або національне посвідчення особи для підтвердження віку та особи. Детальніше дивіться на сайті Stø: [How to get BankID](#).



Якщо у вас виникли питання або виникли проблеми після активації BankID, зверніться до свого банку.

Якщо ви підозрюєте, що ваш смартфон із додатком BankID, кодовим пристроєм або особистим паролем втрачено або скомпрометовано, або якщо хтось інший взяв під контроль ваш BankID, ви повинні негайно звернутися до банку за підтримкою. Ви також повинні негайно повідомити свій банк у разі виявлення порушення безпеки або якщо підозрюєте, що ваш BankID неправомірно використовується або може бути використаний іншими людьми, див. положення про блокування BankID у розділі 7.

## Д. Охорона. Контроль над BankID

**Щоб BankID був для вас безпечним рішенням, важливо контролювати свій BankID, захищаючи особистий пароль і цифрові пристрої, які ви використовуєте для BankID. Негайно повідомте свій банк, якщо підозрюєте або не впевнені, чи інші могли отримати доступ до вашого BankID.**

Щоб захистити свій BankID від неправильного використання, ви повинні вжити всіх розумних заходів для захисту свого особистого пароля, коду, пристрою для кодування, смартфона та інших цифрових пристроїв, які ви використовуєте для BankID. Це означає, наприклад, що:

- Не розкривайте пароль або одноразові коди від BankID нікому, навіть членам родини, законним опікунам, банку, емітенту BankID чи поліції. Ви повинні вжити всіх розумних заходів безпеки, щоб ніхто не міг побачити ваш пароль чи коди під час їх введення.
- Зберігайте свій кодовий пристрій безпечно, щоб він не був відкрито доступним. Якщо ви носите його поза домом, переконайтеся, що він недоступний для інших.
- Виберіть надійний пароль, який ви більше ніде не використовуєте. Інструкції щодо створення надійних паролів можна знайти на [nettvett.no](http://nettvett.no). Змініть пароль, якщо підозрюєте, що інші могли дізнатися про нього.
- Запам'ятайте свій пароль від BankID. Якщо вам все одно потрібно записати пароль, це потрібно робити так, щоб ніхто інший не міг зрозуміти, для чого він. Пароль не слід зберігати разом із кодом BankID або іншим обладнанням чи пристроями.
- Використовуйте здоровий глузд і будьте обережні, використовуючи пароль BankID та одноразовий код, особливо якщо ви отримуєте посилання електронною поштою, текстовими повідомленнями/SMS або соціальними мережами, які вимагають введення пароля або кодів BankID. Не вводьте пароль або одноразовий код BankID, якщо ви не впевнені в сайті або що відправник посилання — той, за кого воно видає.

**Майте на увазі, що ви ніколи, усно чи письмово, наприклад телефоном, електронною поштою, посиланнями чи SMS, не повинні розкривати свій пароль або одноразовий код від BankID. Це також стосується випадків, коли хтось прикидається, наприклад, вашим банком або поліцією.**



## Е. Повідомлення у разі підозри на порушення безпеки тощо.

Ви повинні негайно повідомити агента емітента, згаданого в розділі 4, якщо знаєте або підозрюєте, що:

- інші, включаючи вашого подружжя/партнера чи членів родини, знають ваш пароль від BankID,
- Ви втратили свій кодовий пристрій,
- Ваш кодовий пристрій було викрадено,
- Ви втратили свій мобільний телефон із додатком BankID або іншим обладнанням, яке ви використовуєте з BankID, або його вкрали, і/або
- хтось зловживав вашим банківським ID.

Ви не будете стягувати витрати на видачу нового BankID після повідомлення про порушення безпеки або втрату кодового пристрою/смартфона, якщо у вас немає особливих обставин, наприклад, повторних сповіщень подібного характеру.

## Ж. Блокування BankID

Після повідомлення, як зазначено в розділі 6, емітент:

- заблокуйте свій банківський ID, і
- Підтвердіть письмово, що ваше повідомлення отримано і що ваш банківський ID заблоковано.

Ваш BankID також може бути заблокований емітентом, якщо є обґрунтовані підстави вважати, що:

- хтось, окрім вас, може скористатися вашим банківським ID,
- ваш BankID використовується роботом або подібним програмним забезпеченням, яке виконує завдання автоматично або напівавтоматично на основі вашого BankID,
- ви не виконали цю угоду, або
- Ви не зможете дотримуватися цієї угоди.

Ви будете повідомлені у разі блокування. Ви можете запросити інформацію про причини блокування BankID і як діяти для зняття блокування, зв'язавшись із обраними агентами Stø, згаданими в розділі 4.



### З. Відповідальність

Якщо ви недбало або навмисно порушите умови цієї угоди, ви можете нести відповідальність за збитки, завдані Stø або іншим особам, включно з банками та іншими торговцями BankID.

Якщо агенти Stø або Stø недбало або навмисно порушують умови цієї угоди, Stø як емітент BankID може нести відповідальність за ваші збитки, якщо ви не діяли шахрайським шляхом. Stø не несе відповідальності за фінансові збитки, що виникли внаслідок використання BankID у зв'язку з замовленням або придбанням товарів і послуг або будь-якою іншою формою цифрового спілкування (автентифікації/підписання) з третіми сторонами, такими як постачальники фінансових послуг або інші публічні та приватні торговці BankID.

### И. Термін дії та припинення угоди

Відносини з клієнтом тривають до того часу, поки одна зі сторін не розірве угоду.

Ви можете розірвати угоду BankID у будь-який час без конкретної причини. Таке припинення можна здійснити, повідомивши ваш банк. Stø тоді заблокує ваш банківський ID.

Stø може розірвати угоду, якщо ви більше не відповідаєте вимогам для наявності BankID.

Stø також може розірвати угоду, якщо ви порушите цю угоду, зокрема якщо ви не вживете всіх розумних заходів для захисту ваших особистих паролів, кодів, обладнання, смартфона та інших цифрових пристроїв BankID, і є підстави вважати, що подібні витоки повторяться.

Припинення через Stø має бути попереджено за чотири (4) тижні, а причина припинення має бути вказана. Stø може негайно розірвати угоду у разі суттєвого порушення з вашого боку або якщо ви діяли нечесно чи недобросовісно щодо Stø, вашого банку чи продавців BankID. Також буде суттєвим порушенням, якщо ваш BankID використовується роботом або подібним програмним забезпеченням для автоматичного або напівавтоматичного виконання завдань на основі вашого BankID. Причину звільнення потрібно вказати.

Після розірвання та анулювання угоди ваш банківський ID буде негайно заблоковано, як описано в розділі 7.

### К. Ціни та інформація про ціни

Ціна на BankID вказана у прайс-листі Stø або надана іншим відповідним способом.

### Л. Обробка персональних даних

Stø є контролером персональних даних, оброблених у зв'язку з видачею, поновленням, використанням, повідомленнями, блокуванням і анулюванням BankID, а також для перевірки



дійсності та інших контрольних дій, включаючи моніторинг і виявлення шахрайства, порушень особистості та інше зловживання BankID. Stø оброблятиме ваші дані відповідно до [Закону про персональні дані](#). Детальніше див. [www.bankid.no/privat/personvern-og-regler/](http://www.bankid.no/privat/personvern-og-regler/).

Ваш банк виконує функції обробника даних для адміністрування та підтримки клієнтів відповідно до угоди зі Stø.

## М. Зміни до угоди

Ця угода може бути змінена Stø за два (2) тижні, якщо Stø матиме законні причини для таких змін. Це включає зміни цін, зміни через зміну функціональності або зміни, що виникають через законодавство. Якщо зміна зашкодить вам, наприклад, підвищить ціну, Stø повідомить про зміну за два (2) місяці до набуття чинності.

Якщо з міркувань безпеки це необхідно, Stø може без попереднього повідомлення обмежити використання BankID та внести інші зміни до процедур безпеки чи подібне. Stø повідомить вас про це якомога швидше після зміни.

## Н. Вирішення спорів

Якщо між вами та Stø як емітентом BankID виникне спір щодо розуміння або юридичних наслідків цієї угоди, сторони спочатку повинні намагатися вирішити спор шляхом діалогу.

Якщо спір не вирішується шляхом діалогу, і він стосується видачі/укладання контракту, поновлення або блокування/анулювання BankID, ви можете звернутися до Норвезької ради зі скарг на фінансові послуги (Finansklagenemnda) для отримання заяви або рішення.

Для отримання додаткової інформації про Раду зі скарг на фінансові послуги, будь ласка, див. [www.finkn.no](http://www.finkn.no).