BankID jest emitowany przez Stø AS, który należy do banków w Norwegii.

Umowa dotycząca Personal BankID

Wersja 1.0, kwiecień 2026

1. O Stø AS jako emitentowi BankID

Stø AS ("Stø"), org. nr 927 611 929, jest emitentem BankID dla osób fizycznych (Personal BankID) oraz podmiotów prawnych (Merchant BankID). Stø jest własnością banków działających w Norwegii.

Jako emitent BankID, Stø jest regulowany przez Ustawę o Elektronicznych Usługach Powierniczych (Ustawa o elektronicznych usługach powierniczych) oraz powiązane regulacje wdrażające rozporządzenie UE 910/2014 (eIDAS) do prawa norweskiego.

2. O BankID

BankID to elektroniczne rozwiązanie do identyfikacji i podpisu wydawane Ci jako konsumentowi. Możesz używać BankID do logowania się do bankowości online i mobilnej, uwierzytelniania płatności, identyfikacji na stronach publicznych i prywatnych oraz cyfrowego podpisywania umów.

BankID jest używane z aplikacją BankID lub urządzeniem kodowym, Twoim numerem tożsamości narodowej oraz hasłem osobistym i/lub danymi biometrycznymi, takimi jak rozpoznawanie linii palców czy twarzy.

Tylko Ty jako osoba fizyczna możesz używać swojego BankID.

3. O umowie BankID

Umowa ta reguluje prawa, zobowiązania i obowiązki między Tobą jako posiadaczem BankID a Stø jako formalnym emitentem. Prosimy o uważne przeczytanie umowy i zapoznanie się z wymaganiami dotyczącymi bezpieczeństwa i ochrony Twojego sprzętu oraz hasła osobistego.

4. Uzyskanie bankowego identyfikatora

Stø wybrał banki w Norwegii jako agentów do wydawania i zarządzania BankID, a także do obsługi klienta.

Aby uzyskać bankowy identyfikator, musisz skontaktować się ze swoim bankiem. Zamówienie składa się poprzez osobistą wizytę w banku lub innej organizacji wskazanej przez bank. Należy przedstawić paszport lub dowód tożsamości w celu weryfikacji wieku i tożsamości. Więcej informacji znajdziesz na stronie Stø: How to get BankID.

Jeśli masz pytania lub napotkasz problemy po aktywacji swojego BankID, skontaktuj się ze swoim bankiem.

Jeśli podejrzewasz, że Twój smartfon z aplikacją BankID, kodem lub hasłem osobistym został zgubiony lub przejęty przez kogoś innego, musisz natychmiast skontaktować się z bankiem po wsparcie. Musisz również niezwłocznie powiadomić swój bank po odkryciu naruszenia bezpieczeństwa lub jeśli podejrzewasz, że Twój BankID jest lub może być nadużywany przez innych, por. przepisy dotyczące blokowania BankID w sekcji 7.

5. Ochrona. Kontrola nad BankID

Aby BankID było dla Ciebie bezpiecznym rozwiązaniem, ważne jest, abyś kontrolował swoje BankID, chroniąc swoje osobiste hasło oraz urządzenia cyfrowe, których używasz do BankID. Natychmiast powiadom swój bank, jeśli podejrzewasz lub nie jesteś pewien, czy inni mogli uzyskać dostęp do Twojego BankID.

Aby chronić swoje bankID przed nadużyciem, musisz podjąć wszelkie rozsądne środki ostrożności, aby chronić swoje osobiste hasło, kody, urządzenie kodowe, smartfon oraz inne urządzenia cyfrowe, których używasz do BankID. Oznacza to na przykład, że:

- Nie ujawniaj nikomu hasła do BankID ani jednorazowych kodów, nawet członkom rodziny, opiekunom prawnym, bankowi, wydawcy BankID ani policji. Musisz podjąć wszelkie rozsądne środki ostrożności, aby nikt nie zobaczył twojego hasła lub kodów po ich wpisaniu.
- Bezpiecznie przechowuj swoje urządzenie kodowe, zapewniając, że nie jest ono dostępne otwarcie. Jeśli zabierzesz ją poza dom, upewnij się, że nie jest dostępna dla innych.
- Wybierz silne hasło, którego nie używasz nigdzie indziej. Wskazówki, jak tworzyć silne hasła, znajdziesz na nettvett.no. Zmień hasło, jeśli podejrzewasz, że inni mogli je znać.
- Zapamiętaj hasło do swojego BankID. Jeśli nadal musisz zapisać hasło, musi to zrobić w taki sposób, by nikt inny nie zrozumiał, do czego ono służy. Hasło nie może być przechowywane razem z kodem BankID, urządzeniem ani innym sprzętem czy urządzeniami.
- Kieruj się zdrowym rozsądkiem i bądź ostrożny przy używaniu hasła do BankID i jednorazowego kodu, zwłaszcza jeśli otrzymujesz linki e-mailem, SMS-ami lub mediami społecznościowymi, które wymagają wpisania hasła lub kodów BankID. Nie wpisuj swojego BankID, hasła ani jednorazowego kodu, jeśli nie jesteś pewien strony internetowej lub czy nadawca linku to osoba, za którą się podaje.

Pamiętaj, że nigdy, ustnie ani na piśmie, na przykład przez telefon, e-mail, linki czy SMS, nie wolno ujawniać swojego kodu BankID ani jednorazowego kodu. Dotyczy to również sytuacji, gdy ktoś podszywa się pod Twój bank lub policję.

6. Powiadomienie w przypadku podejrzenia naruszenia bezpieczeństwa itp.

Musisz niezwłocznie powiadomić agenta emitenta wymienionego w sekcji 4, jeśli wiesz lub podejrzewasz, że:

- inni, w tym Twój małżonek/partner lub członkowie rodziny, znają Twoje hasło do BankID,
- Zgubiłeś swoje urządzenie kodowe,
- Twoje urządzenie kodowe zostało skradzione,
- zgubiłeś telefon komórkowy zawierający aplikację BankID lub inne urządzenia używane z BankID, albo został skradziony, i/lub
- Ktoś nadużywał twojego BankID.

Nie poniesiesz kosztów wydania nowego bankID po zgłoszeniu naruszeń bezpieczeństwa lub utraty kodu urządzenia/smartfona, chyba że wystąpią szczególne okoliczności, takie jak powtarzające się powiadomienia o podobnym charakterze.

7. Blokowanie BankID

Po powiadomieniu zgodnie z artykułem 6, emitent będzie:

- zablokować swoje BankID, oraz
- Potwierdź na piśmie, że Twoje powiadomienie zostało otrzymane i że Twój Bank ID został zablokowany.

Twój bankowy identyfikator może również zostać zablokowany przez wydawcę, jeśli istnieje uzasadnione podejrzenie, że:

- Ktoś inny niż ty może użyć twojego BankID,
- Twój BankID jest używany przez robota lub podobne oprogramowanie, które wykonuje zadania automatycznie lub półautomatycznie na podstawie twojego BankID,
- Nie przestrzegałeś tej umowy, albo
- Nie będziesz w stanie spełnić tej umowy.

W przypadku zablokowania zostaniesz powiadomiony. Możesz poprosić o informacje, dlaczego Twój bankID został zablokowany oraz jak możesz kontynuować jego zniesienie, kontaktując się z wybranymi agentami Stø wymienionymi w sekcji 4.

8. Odpowiedzialność

Jeśli niedbale lub celowo naruszysz warunki tej umowy, możesz ponieść odpowiedzialność za straty poniesione przez Stø lub innych, w tym banki i innych sprzedawców z BankID.

Jeśli Stø lub jego agenci niedbale lub celowo naruszą warunki tej umowy, Stø jako emitent BankID może ponosić odpowiedzialność za poniesione straty, chyba że popełniłeś oszukańcze działania. Stø nie ponosi odpowiedzialności za straty finansowe wynikające z używania BankID w związku z zamawianiem lub nabywaniem towarów i usług lub jakiejkolwiek innej formy komunikacji cyfrowej (uwierzytelnianie/podpisywanie) z podmiotami trzecimi, takimi jak dostawcy usług finansowych czy inni publiczni i prywatni sprzedawcy BankID.

9. Okres trwania i rozwiązanie umowy

Relacja z klientem trwa do momentu, gdy jedna ze stron zakończy umowę.

Możesz zakończyć umowę BankID w dowolnym momencie bez podania konkretnego powodu. Takie rozwiązanie można dokonać, informując swój bank. Stø wtedy zablokuje Twój Bank ID.

Stø może rozwiązać umowę, gdy nie spełniasz już wymagań posiadania BankID.

Stø może również rozwiązać umowę, jeśli ją naruszysz, w tym jeśli nie podejmiesz wszelkich rozsądnych środków ostrożności w celu ochrony swoich osobistych haseł do BankID, kodów, sprzętu, smartfona i innych urządzeń cyfrowych używanych do BankID, a istnieją powody sądzić, że podobne naruszenia mogą się powtórzyć.

Zwolnienie przez Stø musi być wypowiedziane z czterotygodniowym (4) tygodniowym wypowiedzeniem i należy podać powód zwolnienia. Stø może natychmiast rozwiązać umowę w przypadku istotnego naruszenia przez Ciebie lub jeśli postąpiłeś nieuczciwie lub w złej wierze wobec Stø, Twojego banku lub sprzedawców BankID. Będzie to również stanowić istotne naruszenie, jeśli Twój BankID zostanie użyty przez robota lub podobne oprogramowanie do automatycznego lub półautomatycznego wykonywania zadań na podstawie Twojego BankID. Należy podać powód zwolnienia.

Po zakończeniu i anulowaniu umowy Twój BankID zostanie natychmiast zablokowany, zgodnie z sekcją 7.

10. Ceny i informacje o cenach

Cena BankID jest podana w cenniku Stø lub podana w inny odpowiedni sposób.

11. Przetwarzanie danych osobowych

Stø jest kontrolerem danych osobowych przetwarzanych w związku z wydawaniem, odnawianiem, korzystaniem, powiadomieniami, blokowaniem i cofnięciem BankID, a także w zakresie kontroli ważności i innych działań kontrolnych, w tym monitorowania i wykrywania oszustw, naruszeń tożsamości oraz innych nadużyć BankID. Stø będzie przetwarzać Twoje dane zgodnie z ustawą o danych osobowych. Więcej informacji można znaleźć w www.bankid.no/privat/personvern-og-regler/.

Twój bank pełni rolę procesora danych dla administracji i obsługi klienta zgodnie z umową ze Stø.

12. Zmiany w umowie

Umowa ta może zostać zmieniona przez Stø z dwutygodniowym (2) wypowiedzeniem, jeśli Stø ma uzasadnione powody do takich zmian. Obejmuje to zmiany cen, zmiany wynikające ze zmiany funkcjonalności lub zmiany wynikające z ustawodawstwa. Jeśli zmiana przyniesie Ci szkodę, na przykład podwyżka ceny, Stø powiadomi o niej dwa (2) miesiące przed wejściem w życie.

Jeśli kwestie bezpieczeństwa będą tego konieczne, Stø może bez wcześniejszego powiadomienia ograniczyć użycie BankID oraz wprowadzić inne zmiany w procedurach bezpieczeństwa lub podobnych procedurach. Stø powiadomi Cię o tym jak najszybciej po zmianie.

13. Rozwiązywanie sporów

Jeśli pojawi się spór między Tobą a Stø jako emitentem BankID dotyczący porozumienia lub skutków prawnych tej umowy, strony najpierw będą dążyć do rozwiązania sporu poprzez dialog.

Jeśli spór nie zostanie rozwiązany poprzez dialog, a dotyczy on wydania/zawierania umowy, odnowienia lub blokowania/cofnięcia BankID, możesz zgłosić sprawę do Norweskiej Rady ds. Skarg na Usługi Finansowe (Finansklagenemnda) w celu złożenia oświadczenia lub decyzji.

Aby uzyskać więcej informacji o Financial Services Complaints Board, prosimy zobaczyć www.finkn.no.