

PERSONVERNPOLICY 2024



ENKELT
ANNERLEDES
SAMMEN

BN Bank

Innhold

1.	Innledning	3
1.1.	Formål og virkeområde	
1.2.	Klassifisering	
2.	Definisjoner	4
3.	Organisering og ansvar	5
3.1.	Behandlingsansvarlig og databehandler	
3.2.	Styret	
3.3.	Administrerende direktør	
3.4.	Personvernombud	
3.5.	Den enkelte ansatte	
4.	Overordnede føringer og prinsipper	6
5.	Rapportering	7
6.	Endringer	7

1. Innledning

1.1. Formål og virkeområde

BN Bank ASA («banken») håndterer personopplysninger som en del av daglig drift. Banken skal ivareta de registrertes rettigheter og friheter innen personvern i relevante prosesser og oppgaver.

Det er viktig at banken ivaretar personvernet, og håndterer personopplysninger på en sikker og god måte, for å skape tillit hos kunder og ansatte, og samtidig skape nye forretningsmuligheter. Målet med personvernarbeidet er gjennom systematisk og risikobasert tilnærming å

- Ivareta de registrertes personvern, rettigheter og friheter
- Ha kontroll på bankens behandlinger av personopplysninger
- Sikre bankens omdømme gjennom korrekt håndtering av personopplysninger
- Etterleve personopplysningsloven med tilhørende forskrifter, personvernforordningen (GDPR), relevante bransjeveiledere, interne policyer og rutiner («personvernregelverket»)

Formålet med policy for personvern er å fastsette prinsipper, krav, roller og ansvar for håndtering av personopplysninger. Policyen inngår i den styrende delen av internkontrollen, og beskriver krav og plikter ved behandling av personopplysninger, samt intern organisering, ansvars- og myndighetsforhold.

Policyen gjelder for alle ansatte i banken, inkludert midlertidig ansatte, innleide konsulenter og styremedlemmer («ansatte»).

1.2. Klassifisering

Denne policy har klassifisering åpen. Det innebærer at dokumentet kan deles utenfor banken og kan legges ut på bnbank.no.

2. Definisjoner

Behandling	Enhver håndtering av personopplysninger, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering, spredning, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.
Behandlingsansvar	Virksomheten som bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.
Databehandler	Virksomheten som behandler personopplysninger på vegne av den behandlingsansvarlige.
Den registrerte	Personen som personopplysningene kan knyttes til.
Brudd på personopplysningsikkerheten	Brudd på konfidensialitet, integritet og/eller tilgjengelighet for personopplysningene.
Personopplysninger	Opplysninger om en identifisert eller identifiserbar fysisk person.

3. Organisering og ansvar

3.1. Behandlingsansvarlig og databehandler

BN Bank behandler personopplysninger i rollen som behandlingsansvarlig og som databehandler.

3.2. Styret

Styret har det overordnede ansvaret for at banken etterlever personopplysningsregleverket, og vedtar denne policy.

3.3. Administrerende direktør

Administrerende direktør har det øverste ansvaret for at oppgavene med å ivareta behandlingsansvaret og databehandleransvaret etterleveres i henhold til personvernregelverket.

Administrerende direktør kan delegerer utførelse av oppgaver knyttet til behandlingsansvaret til definerte roller i henhold til gjeldende prosesser og stillingsinstrukser.

3.4. Personvernombud

BN Bank skal ha et personvernombud. Personvernombudet har et særlig ansvar for at de registrertes rettigheter og friheter blir ivaretatt. Personvernombudet har en sentral, uavhengig, rådgivende og kontrollerende rolle i internkontrollen for personvern, og rapporterer direkte til styret ved behov. Personvernombudet skal gi Datatilsynet opplysninger når tilsynet ber om det, herunder foreta undersøkelser i konkrete saker.

3.5. Den enkelte ansatte

Alle ansatte, vikarer og innleide konsulenter har plikt til å følge bankens rutiner og retningslinjer for personvern.

4. Overordnede føringer og prinsipper

I BN Bank skal personopplysninger behandles i tråd med grunnleggende prinsipper for behandling av personopplysninger. Banken skal dokumentere at kravene i personvernregelverket etterleves.

Personopplysninger skal

- Behandles lovlig, rettferdig og åpent
- Samles inn for spesifikke uttrykkelig angitte og legitime formål, og skal ikke brukes til andre formål (formålsbegrensning)
- Være adekvate, relevante og begrenset til det som er nødvendig (dataminimering)
- Være korrekte og oppdaterte
- Lagres kun så lenge det er nødvendig (lagringsbegrensning)
- Behandles på en måte som ivaretar kravet til informasjonssikkerhet

BN Bank skal ha prosesser og rutiner for å sikre etterlevelse av personvernregelverket, herunder ha etablert kontroller for å sikre at aktuelle rutiner følges i det daglige. («Internkontroll»)

- Internkontrolldokumentasjon, herunder rutiner og retningslinjer, for behandling av personopplysninger skal være oppdatert, dokumentert, tilgjengelig og kjent.
- Oversikt over behandlinger av personopplysninger (behandlingsoversikt) i rollen som behandlingsansvarlig og databehandler skal være oppdatert.
- Det skal være etablert rutiner som ivaretar de registrertes rett til innsyn, retting og sletting.
- Personvernerklæringen skal ivareta de registrertes rett til informasjon.
- Behandling av personopplysninger skal være i samsvar krav til informasjonssikkerhet, herunder skal det iverksettes nødvendige fysiske, tekniske og organisatoriske tiltak for å sikre personopplysningene på en betryggende måte.
- Personvern skal ivaretas i utviklingsløp og gjennom systemers levetid (innebygd personvern).
- Risikovurderinger og personvernkonsekvensvurderinger (DPIA) skal gjennomføres og oppdateres ved behov.
- Databehandleravtaler med tredjeparter som behandler personopplysninger på vegne av BN Bank skal inngås og følges opp i tråd med gjeldende rutiner for avtaleoppfølging.
- Brudd på denne policy og tilhørende rutiner kan være brudd på personopplysningssikkerheten. Brudd på personvern og personopplysningssikkerheten skal håndteres i tråd med rutiner for hendelseshåndtering.
- Sikre at personvernombudet blir involvert på riktig måte og til rett tid i spørsmål som gjelder personvern, herunder påse at personvernombudets råd og vurdering blir hørt og tatt i betraktning.
- Alle ansatte skal gjennom bankens opplæringsprogram få nødvendig kjennskap til personvernregelverket.
- BN Bank skal ha intern kontroll for å overvåke løpende håndtering av personopplysninger for å sikre at etablerte tiltak og rutiner følges.

5. Rapportering

Personvernombudet skal rapportere til det høyeste ledernivået i BN Bank, herunder til bankens styre.

Rapporteringen skal minst omfatte

- Rapportering om status på bankens håndtering av personopplysninger i kvartalsvis risikoreport
- Rapportering i forbindelse med årlig compliancerapport

6. Endringer

Dette dokumentet eies av avdeling for Risikostyring og Compliance, og skal være gjenstand for årlig revisjon.