Policy for behandling av personopplysninger

20.10.2021

BN Bank

Innhold

1. Innledning

1.1. Formål og virkeområde

Formålet med policy for behandling av personopplysninger («policy») er å implementere kravene i personopplysningsloven med tilhørende forskrifter og relevante bransjeveiledere.

Policyen er en del av bankens styrende dokumenter og gjelder for alle ansatte i BN Bank ASA («banken»), inkludert midlertidig ansatte, innleide konsulenter og styremedlemmer («ansatte»), og skal bidra til å identifisere overordnede krav og plikter med hensyn til behandling av personopplysninger, samt beskrive intern organisering og ansvarsforhold.

1.2. Klassifisering

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

2. Definisjoner

Behandling

Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsulering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.

Behandlingsansvarlig

Behandlingsansvarlig er den enheten som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.

Databehandler

En fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.

Den registrerte

Fysisk person som personopplysningene kan knyttes til.

Brudd på personopplysningssikkerheten/avvik

Brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

Personopplysninger

Opplysninger om en identifisert eller identifiserbar fysisk person.

Personvernregelverket

Personopplysningsloven (inkl. GDPR), interne policyer og rutiner på personvern.

3. Organisering og ansvar

3.1. Behandlingsansvarlig

BN Bank behandler personopplysninger som behandlingsansvarlig.

3.2. Styret

Styret har det overordnede ansvar for at banken etterlever personopplysningsregleverket.

Styret skal:

- Fastsette målene og overordnet strategi for arbeidet med personvern i BN Bank ASA.
- Påse at banken har god internkontroll og hensiktsmessige systemer.
- Påse at banken har tilfredsstillende organisering som understøtter etterlevelsen.
- Sørge for å holde seg orientert om bankens viktigste risikoområder og beslutte om overordnet risiko er akseptabel for personvernhåndteringen i banken.
- Vedta policy for behandling av personopplysninger.

3.3. Administrerende direktør

Administrerende direktør er behandlingsansvarlig i BN Bank, og har det øverste ansvaret for at regelverket rundt personopplysninger etterleves og operasjonaliseres i virksomheten.

Administrerende direktør skal:

- Operasjonalisere mål og strategi for personvern og informasjonssikkerhet.
- Avklare ansvar og myndighetsforhold innad i banken, herunder delegere nødvendige oppgaver knyttet til operasjonelt behandlingsansvar.
- Påse at det er tilstrekkelige ressurser til å ivareta bankens forpliktelser på området.
- Sørge for å skape en felles forståelse for viktigheten av å ha et godt personvern.

3.4. Prosessansvarlig/delprosessansvarlig

Prosessansvarlig/delprosessansvarlig har det operasjonelle ansvaret for behandling av personopplysninger, og skal sørge for at det blir gjennomført personvernkonsekvensvurderinger ved behov, og at det foreligger skriftlige rutiner som beskriver behandlingen av personopplysninger. Rutinene skal dekke eksterne og interne krav til behandling av personopplysninger, og oppdateres ved behov. Prosessansvarlig/delprosessansvarlig skal ha kjennskap til reglene som regulerer behandlingen av personopplysninger.

3.5. Personvernombud

BN Bank skal utnevnte et personvernombud. Utnevnelsen er personlig og foretas av administrerende direktør.

Personvernombudet skal:

- Kontrollere etterlevelse av personvernregelverket, og ved behov rapportere direkte til styret.
- Gi råd i forbindelse med vurdering av personvernkonsekvenser.
- Være Datatilsynets og de registrertes kontaktpunkt.

Personvernombudets oppgaver og ansvar er nærmere beskrevet i ombudets stillingsinstruks.

3.6. Den enkelte ansatt

Alle ansatte, vikarer og innleide konsulenter har ansvar for og plikt til å sette seg inn i personvernregelverket.

4. Organisering og ansvar

BN Bank håndterer store mengder personopplysninger som en del av daglig drift, både om kunder, samarbeidspartnere, og om egne medarbeidere.

For å nå bankens målsetninger må alle som behandler personopplysninger i eller på vegne av banken bidra til at personopplysningene behandles i tråd med de grunnleggende prinsippene for behandling av personopplysninger.

Personopplysninger skal:

- Behandles på en lovlig, rettferdig og åpen måte.
- Kun samles inn for spesifikke uttrykkelig angitte og legitime formål, og ikke (senere) til uforenlige formål.
- Være adekvate, relevante og begrenset til det som er nødvendig (dataminimering).
- Være korrekte og oppdaterte.
- Lagres slik at det ikke er mulig å identifisere de registrerte lenger enn nødvendig.
- Behandles på en måte som ivaretar kravet til informasjonssikkerhet.

BN Bank skal ha prosesser og rutiner som sikrer at:

- Personvernregelverket og relevante bransjeveiledere følges i det daglige.
- Det gjennomføres kontroller for å overvåke at håndteringen av personopplysninger skjer i samsvar med personvernregelverket.
- Internkontrollsystemet for behandling av personopplysninger er oppdatert, dokumentert og kjent i banken.
- Det finnes en oppdatert og komplett oversikt over behandlinger av personopplysninger (behandlingsprotokoll).
- Informasjonssikkerheten ved behandlingen av personopplysninger ivaretas.
- Personvern ivaretas i utviklingsløp og systemers levetid (innebygd personvern).
- Det jevnlig gjennomføres og oppdateres risikovurderinger i henhold til regelverk, samt vurderinger av personvernkonsekvenser (DPIA) ved behov.
- Det inngås databehandleravtaler med leverandører, og at personopplysninger ikke blir behandlet på annen måte enn det som går frem av avtalen.
- Det føres et register over brudd på personopplysningssikkerheten.

5. Opplæring

Personvernombudet har ansvar for at det etableres og gjennomføres opplæring av bankens ansatte. Deler av opplæringen kan delegeres til prosessansvarlig/delprosessansvarlig innenfor sitt område.

Alle ansatte (både faste og midlertidige) skal gjennom bankens opplæringsprogram få grunnleggende kjennskap til regelverket rundt personopplysninger, informasjonssikkerhet og taushetsplikt. Ved behov skal de ansatte gjennomgå rollebasert opplæring.

6. Brudd på personopplysningssikkerheten

Det skal legges til rette for enkel rapportering av brudd på personopplysningssikkerheten, som deretter følges opp og systematiseres for å sikre kontinuerlig læring og forbedring.

Alle ansatte i BN Bank skal ha et bevisst forhold til hvilke krav som stilles til behandling av personopplysninger, og så snart som mulig varsle ved mistanke om eller kunnskap om et brudd på personopplysningssikkerheten.

Brudd på personopplysningssikkerhet skal håndteres i tråd med bankens rutine for håndtering av avvik, og registreres i bankens kvalitetsstyringssystem (EQS).

7. Rapportering

Personvernombudet skal rapportere på bankens håndtering av personopplysninger i kvartalsvis risikorapport, som oversendes styret.

8. Endringer

Dette dokumentet eies av avdeling for Risikostyring og Compliance, og skal være gjenstand for revisjon minimum hvert andre år. Revisjonen skal ta hensyn til endringer i både interne forhold og eksterne omgivelser.