

Policy for personvern

Versjon	Dato	Dokumenteier	Godkjenning	Beslutning	Doknivå	Status
2022-01	30.03.2022	Silje Mjelle	Hanne Nordgaard	Styret	2	Besluttet

Innhold

1. Bakgrunn og formål	1
1.1 Innledning	1
1.2 Formål	1
1.3 Mål	1
2. Prinsipper for behandling av personopplysninger	2
3. Krav til behandling av personopplysninger	2
4. Organisering, roller og ansvar	2
4.1 Behandlingsansvarlig og databehandler	2
4.2 Styret	3
4.3 Administrerende direktør	3
4.4 Personvernombud	3
4.5 Alle medarbeidere	3
5. Avvik fra personvernpolicy og oppfølging	3

1. BAKGRUNN OG FORMÅL

1.1 Innledning

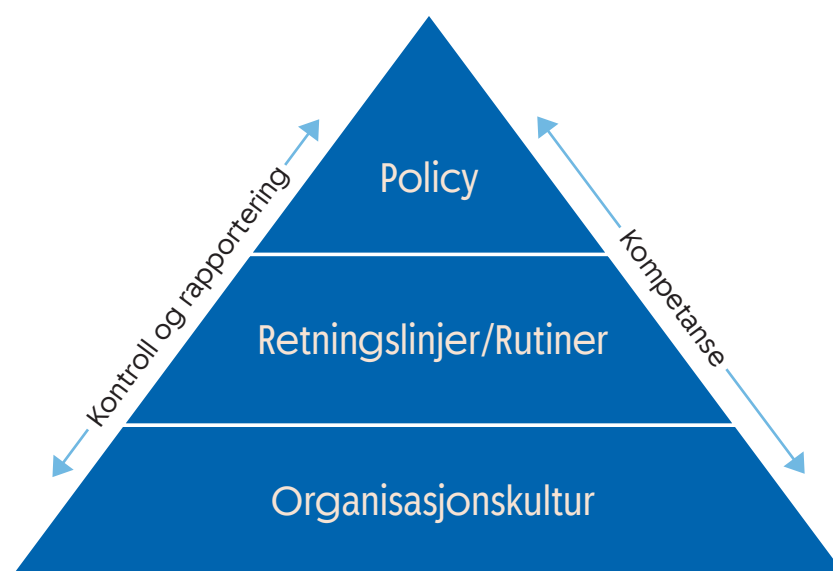
Policy for personvern beskriver overordnede prinsipper og krav knyttet til personvern. Policyen skal revideres årlig.

SpareBank 1 Helgeland (SBH) håndterer personopplysninger som en del av daglig drift. Banken skal ivareta de registrertes rettigheter og friheter innen personvern i prosesser og oppgaver banken utfører.

1.2 Formål

Formålet med policy for personvern er å fastsette prinsipper og krav, samt roller og ansvar, for bankens håndtering av personopplysninger.

Policyen er en del av rutineverket som skal følges som en del av internkontrollen. Den skal beskrive overordnede krav og plikter til behandling av personopplysninger, samt intern organisering, ansvars- og myndighetsforhold. Policyen underbygges av «Standard for personvern», i tillegg til andre øvrige rutiner som konkretiserer kravene i denne policyen.



Figur 1: Rammeverk for personvern

1.3 Mål

Det er viktig at SBH håndterer personopplysninger på en god og sikker måte for å skape tillit fra kunder og ansatte, og samtidig kunne skape nye forretningsmuligheter. Målet med personvernarbeidet er, gjennom en systematisk og risikobasert tilnærming, å sørge for:

- å respektere de registrertes privatliv og familieliv, deres hjem og korrespondanse, samt øvrige menneskerettigheter;
- å sikre etterlevelse av personopplysningsloven og EUs personvernforordning (GDPR), øvrig personvernregelverk og anerkjente veiledere;
- å understøtte forretningsdriften ved at SBH til enhver tid har kontroll på sine behandlinger av personopplysninger
- å sikre omdømme til SBH gjennom korrekt håndtering av personopplysninger

2. PRINSIPPER FOR BEHANDLING AV PERSONOPPLYSNINGER

For å nå bankens mål skal SBH behandle personopplysninger slik at de grunnleggende prinsippene for behandling av personopplysninger etterleveres.

Personopplysninger skal:

- behandles på en lovlig, rettferdig og åpen måte
- kun samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke viderebehandles på en måte som er uforenelig med behandlingens 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 (lagringsbegrensning)
- behandles på en måte som ivaretar krav til informasjonssikkerhet

3. KRAV TIL BEHANDLING AV PERSONOPPLYSNINGER

SBH skal ha prosesser og rutiner for å sikre personvern og personopplysningssikkerheten.

- Personvernregelverket og aktuelle veiledere skal følges i det daglige.
- I internkontrollsystemet skal kontroller knyttet til behandling av personopplysninger skal være oppdatert og dokumentert.
- Master behandlingsprotokoll skal være oppdatert.
- De registrertes rett til innsyn, sletting og retting skal ivaretas i rutiner. Personvernerklæringen skal ivareta de registrertes rett til informasjon.
- Informasjonssikkerheten ved behandling av personopplysninger skal være tilfredsstillende.
- Personvern skal ivaretas i utviklingsløp og systemers levetid (innebygd personvern).
- Risikovurderinger skal gjennomføres og oppdateres ved behov.
- Personvernkonskvenser (DPIA) skal gjennomføres og oppdateres ved behov.
- Databehandleravtaler med tredjeparter som behandler bankens personopplysninger skal inngås.
- Brudd på personopplysningssikkerheten (avvik) skal håndteres.
- SBH skal ha intern kontroll for å overvåke den løpende håndteringen av personopplysninger for å sikre at etablerte tiltak og rutiner blir fulgt.

Standard for personvern med tilhørende rutiner beskriver nærmere hvordan SBH skal sikre etterlevelse av de ovennevnte kravene.

4. ORGANISERING, ROLLER OG ANSVAR

4.1 Behandlingsansvarlig og databehandler

SBH behandler personopplysninger som behandlingsansvarlig og som databehandler. SBH er behandlingsansvarlig når banken bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal brukes. SBH er databehandler når SBH behandler personopplysninger på vegne av en behandlingsansvarlig.

4.2 Styret

Det er sparebank 1 Helgeland som er behandlingsansvarlig og databehandler, og styret i SBH har det overordnede ansvaret etter personvernregelverket. Styret vedtar policy for personvern.

4.3 Administrerende direktør

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

Administrerende direktør har delegert oppgaver for å sikre etterlevelse av personvernregelverket i samsvar med de generelle prinsippene for risikostyring og internkontroll i banken. Standard for personvern beskriver hvordan det daglige operasjonelle ansvaret for etterlevelse av personvernregelverket er delegert.

4.4 Personvernombud

SBH har utnevnt et personvernombud. Personvernombudet har et særlig ansvar for at de registrertes rettigheter og friheter blir ivaretatt. Personvernombudet skal gi Datatilsynet opplysninger når tilsynet ber om det, herunder foreta undersøkelser i konkrete saker. Det skal involveres i alle spørsmål som gjelder vern av personopplysninger. Personvernombudet rapporterer til styret som del i års rapportering for compliance, og har rett til å møte styret når dette anses som vurderes som nødvendig.

4.5 Alle medarbeidere

Alle ansatte, vikarer og innleide konsulenter har plikt til å sette seg inn i og etterleve de rutiner og retningslinjer som gjelder for personvern.

5. AVVIK FRA PERSONVERNPOLICY OG OPPFØLGING

Brudd på policy for personvern og tilhørende standarder og rutiner vil for banken innebære brudd på personopplysningsloven. Dette kan være alvorlig for SBH, og kan medføre sanksjoner fra Datatilsynet.

6. DEFINISJONER

Beskrivelse	
Personopplysninger	Opplysninger om en identifisert eller identifiserbar fysisk person.
Behandling	Enhver håndtering av personopplysninger, for eksempel innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering, spredning, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.
Behandlingsansvarlig	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 personopplysnings-sikkerheten	Brudd på konfidensialitet, integritet og tilgjengelighet for personopplysningene.
Master behandlingsprotokoll	Oversikt over alle plasser vi behandler personopplysninger med behandlingsgrunnlag. Samspår foretar løpende oppdatering av denne.