

Policy for personvern

Eier	Konserndirektør HR og juridisk
Skrevet av	Fagsjef personvern
Besluttet av	Styret i SpareBank 1 Østlandet
Status	Besluttet
Versjon	2.0
Opprettet	11.06.2018
Sist endret	14.09.2021

Innholdsfortegnelse

1.	BAKGRUNN OG FORMÅL	3
1.1	INNLEDNING	3
1.2	FORMÅL.....	3
1.3	MÅL.....	3
2.	PRINSIPPER FOR BEHANDLING AV PERSONOPPLYSNINGER	3
3.	KRAV TIL BEHANDLING AV PERSONOPPLYSNINGER	3
4.	ORGANISERING, ROLLER OG ANSVAR	4
4.1	BEHANDLINGSANSVARLIG OG DATABEHANDLER	4
4.2	STYRET	4
4.3	ADMINISTRERENDE DIREKTØR	4
4.4	PERSONVERNOMBUD	4
4.5	ALLE MEDARBEIDERE	4
5.	AVVIK FRA PERSONVERNPOLICY OG OPPFØLGING	5
6.	DEFINISJONER	5

1. BAKGRUNN OG FORMÅL

1.1 INNLEDNING

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

SpareBank 1 Østlandet (SB1Ø) 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, roller og ansvar for håndtering av personopplysninger i SB1Ø.

Policyen inngår i den styrende delen av internkontrollen. Den skal beskrive overordnede krav og plikter til behandling av personopplysninger, samt intern organisering, ansvars- og myndighetsforhold. Policyen støttes av «Standard for personvern» samt andre konkrete rutiner som spesifiserer kravene i denne policyen.

1.3 MÅL

Det er viktig at SB1Ø 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, sitt hjem og sin korrespondanse samt øvrige menneskerettigheter
- å sikre etterlevelse av personopplysningsloven og EUs personvernforordning (GDPR), øvrig personvernregelverk og anerkjente veiledere
- å understøtte forretningsdriften ved at SB1Ø til enhver tid har kontroll på sine behandlinger av personopplysninger
- å sikre omdømme til SB1Ø gjennom korrekt håndtering av personopplysninger

2. PRINSIPPER FOR BEHANDLING AV PERSONOPPLYSNINGER

For å nå bankens mål skal SB1Ø behandle personopplysninger slik at de grunnleggende prinsippene for behandling av personopplysninger etterleveres. SB1Ø skal vise og dokumentere at banken etterlever kravene i personvernregelverket.

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

SB1Ø skal ha prosesser og rutiner for å sikre personvern og personopplysningssikkerheten.

- Personvernregelverket og aktuelle veiledere skal følges i det daglige.

- Internkontrollsystemet for behandling av personopplysninger skal være oppdatert, dokumentert og kjent.
- Oversikt over behandlinger av personopplysninger (behandlingsoversikt) for rollene som behandlingsansvarlig og databehandler 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.
- Personvernkonsekvenser (DPIA) skal gjennomføres og oppdateres ved behov.
- Databehandleravtaler med tredjeparter som behandler bankens personopplysninger skal inngås.
- Brudd på personopplysningssikkerheten (avvik) skal håndteres.
- SB1Ø 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 SB1Ø skal sikre etterlevelse av de ovennevnte kravene.

4. ORGANISERING, ROLLER OG ANSVAR

4.1 BEHANDLINGSANSVARLIG OG DATABEHANDLER

SB1Ø behandler personopplysninger som behandlingsansvarlig og som databehandler. SB1Ø er behandlingsansvarlig når banken bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal brukes. SB1Ø er databehandler når SB1Ø behandler personopplysninger på vegne av en behandlingsansvarlig.

4.2 STYRET

Det er SpareBank1 Østlandet som er behandlingsansvarlig og databehandler, og styret i SB1Ø 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

SB1Ø har utnevnt et personvernombud. Personvernombudet har et særlig ansvar for at de registrertes rettigheter og friheter blir ivaretatt. Personvernombudet rapporterer til styret. Personvernombudet har en rådgivende og kontrollerende rolle i internkontrollen for personvern. Personvernombudet skal gi Datatilsynet opplysninger når tilsynet ber om det, herunder foreta undersøkelser i konkrete saker.

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 PERSONVERN POLICY OG OPPFØLGING

Brudd på policy for personvern og tilhørende standarder og rutiner vil for banken innebære brudd på personopplysningsloven. Dette kan være alvorlig for SB1Ø, og kan medføre sanksjoner fra Datatilsynet.

6. DEFINISJONER

Begrep	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.