Policy for personvern SpareBank 1 Østlandet med datterselskaper

Eier	Konserndirektør HR og juridisk
Besluttet av	Styret i SpareBank 1 Østlandet
Status	Vedtatt 28.10.2022
Opprettet	11.06.2018
Sist endret	1.7.2022
Antall sider	5

Innholdsfortegnelse

1. BAKGRUNN OG FORMÅL

1.1 INNLEDNING

Policy for personvern beskriver overordnede prinsipper og krav til personvern i konsernet SpareBank 1 Østlandet. Policyen gjelder for datterselskaper så langt det passer, og gir et grunnlag for virksomhetenes egne rutiner for personvern. Policyen gjennomgås årlig og revideres ved behov.

SpareBank 1 Østlandet (SB1Ø) håndterer personopplysninger som en del av daglig drift. SB1Ø skal ivareta de registrertes rettigheter og friheter innen personvern i relevante prosesser og oppgaver.

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 beskriver overordnede krav og plikter til behandling av personopplysninger, samt intern organisering, ansvars- og myndighetsforhold. Policyen støttes av 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

I SB1Ø skal personopplysninger behandles slik at grunnleggende prinsipper for behandling av personopplysninger etterleves. SB1Ø skal vise og dokumentere at kravene i personvernregelverket etterleves.

Personopplysninger skal

- behandles på en lovlig, rettferdig og åpen måte
- kun samles inn for spesifikke, uttrykkelig angitte og berettige 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 rutiner 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 gjennom systemers levetid (innebygd personvern).
- Risikovurderinger skal gjennomføres og oppdateres ved behov.
- Personvernkonsekvenser (DPIA) skal gjennomføres og oppdateres ved behov.
- Databehandleravtaler med tredjeparter som behandler SB1Øs personopplysninger skal inngås.
- Brudd på personopplysningssikkerheten (avvik) skal håndteres. Det skal gis rettidig melding til tilsynsmyndigheter og informasjon til de registrerte.
- SB1Ø skal ha intern kontroll for å overvåke den løpende håndteringen av personopplysninger for å sikre at etablerte tiltak og rutiner blir fulgt.

4. ORGANISERING, ROLLER OG ANSVAR

4.1 BEHANDLINGSANSVARLIG OG DATABEHANDLER

SB1Ø behandler personopplysninger som behandlingsansvarlig og som databehandler. SB1Ø er behandlingsansvarlig når SB1Ø 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 enkelte selskap i SB1Ø er behandlingsansvarlig og databehandler, og styret har det overordnede ansvaret etter personvernregelverket. Styret vedtar policy for personvern.

4.3 ADMINISTRERENDE DIREKTØR

Administrerende direktør i selskapet har ansvaret for at oppgavene for å ivareta at behandlingsansvaret og databehandleransvaret etterleves 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.

4.4 PERSONVERNOMBUD

I de selskapene som har oppnevnt personvernombud har personen 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 PERSONVERNPOLICY OG OPPFØLGING

Brudd på policy for personvern og tilhørende standarder og rutiner kan være brudd på personopplysningsloven, og skal meldes som et mulig avvik etter gjeldende rutiner.

6. DEFINISJONER

Begrep	Beskrivelse
Personopplysninger	Opplysninger om en 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.