Policy for personvern

Eier	*Konserndirektør Organisasjon*
Sist revidert	27.03.2025

Innhold

1. INNLEDNING

Policy for personvern beskriver overordnede prinsipper og krav til personvern i konsernet Sparebank 1 Østlandet (SB1Ø). Policyen gjelder for datterselskaper så langt det passer, og gir et grunnlag for virksomhetenes egne rutiner for personvern.

SB1Ø skal ivareta de registrertes rettigheter og virksomhetens plikter innen personvern. SB1Ø skal behandle personopplysninger i henhold til personvernregelverket, arbeidsmiljøloven, finansavtaleloven og øvrige finansregulatoriske rammer, regelverk for kunstig intelligens (AI act) og relevant regelverk. Denne policyen beskriver hvordan SB1Ø skal sikre etterlevelse av personvernregelverket.

1.1 FORMÅL

Formålet med policy for personvern er å fastsette prinsipper og krav, roller og ansvar for behandling av personopplysninger i SB1Ø. Policyen inngår i den styrende delen av internkontrollen og støttes av konkrete rutiner som spesifiserer kravene.

1.2 MÅL

SB1Ø skal håndtere personopplysninger på en lovlig, rettferdig og sikker måte for å skape tillit fra kunder og ansatte. Målet med personvernarbeidet er gjennom en systematisk og risikobasert tilnærming å sørge for:

- å respektere de registrertes privatliv og 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 konfidensialitet, integritet og tilgjengelighet til personopplysninger
- å sikre omdømme til SB1Ø gjennom korrekt håndtering av personopplysninger

2. KRAV TIL BEHANDLING AV PERSONOPPLYSNINGER

SB1Ø skal ivareta og dokumentere ivaretakelse av følgende krav i personvernregelverket. Rutiner for de ulike kravene ligger som egne rutinebeskrivelser.

2.1 IVARETA PERSONVERNPRINSIPPENE

I SB1Ø skal vi behandle personopplysninger slik at grunnleggende prinsipper for behandling av personopplysninger etterleves. SB1Ø skal dokumentere at kravene i personvernregelverket etterleves.

2.1.1 LOVLIGHET, RETTFERDIGHET OG ÅPENHET

SB1Ø skal kun behandle personopplysninger når det er tillatt etter personvernregelverket. Hvert formål for behandling av personopplysninger krever et behandlingsgrunnlag, som skal dokumenteres og begrunnes. Behandlingsgrunnlaget kan være samtykke, avtale, rettslig forpliktelse eller berettiget interesse. Behandling av særlige kategorier av personopplysninger er som hovedregel forbudt, men kan gjennomføres med ekstra krav til behandlingsgrunnlag.

Behandlingen skal gjøres i respekt for de registrertes rettigheter, samt være nødvendig og proporsjonal. Behandling av personopplysninger skal på en kort og forståelig måte beskrives i personvernerklæringer, som skal være lett tilgjengelig for alle registrerte (kunder, ansatte, andre).

2.1.2 FORMÅLSBEGRENSNING

SB1Ø skal kun samle inn og behandle personopplysninger for spesifikke, uttrykkelig angitte og berettigede formål. Ethvert formål skal identifiseres og beskrives presist, og alle formål skal være forklart på en måte som gjør at alle berørte forstår hva personopplysningene skal brukes til. Personopplysninger skal ikke viderebehandles til formål som er uforenlige med de opprinnelige formålene.

2.1.3 DATAMINIMERING

All behandling av personopplysninger skal være relevant og begrenset til det som er nødvendig for formålet de ble samlet inn for. SB1Ø skal ikke bruke flere eller mer personopplysninger enn det som er nødvendig for formålet.

2.1.4 RIKTIGHET

SB1Ø skal ha korrekte og oppdaterte personopplysninger. Kunder, ansatte og andre vi behandler personopplysninger om, kan be om at uriktige opplysninger korrigeres.

2.1.5 LAGRINGSBEGRENSNING

SB1Ø skal bare lagre personopplysninger så lenge de er nødvendige for formålet de ble innhentet for. De skal deretter anonymiseres eller slettes. Egen rutine for sletting av personopplysninger beskriver prinsipper og slettefrister for behandling av personopplysninger. Slettefrister for hver behandling skal dokumenteres i Behandlingsoversikten og sletterutiner skal dokumenteres.

2.2 IVARETA DE REGISTRERTES RETTIGHETER

SB1Ø skal ivareta de registrertes rettigheter, herunder

- Rett til informasjon om behandling av egne personopplysninger, gjennom oppdaterte personvernerklæringer og annen informasjon.
- Rett til innsyn i behandlingen av egne personopplysninger.
- Rett til retting og sletting av egne personopplysninger.
- Rett til begrenset behandling av egne personopplysninger.
- Rett til dataportabilitet.

Rettighetene skal ivaretas på en enkel, helhetlig og lik måte på tvers av organisasjonen. Når SB1Ø er behandlingsansvarlig, er det SB1Ø som er ansvarlig for at den registrertes rettigheter ivaretas. Det skal være enkelt for de registrerte å ivareta sine rettigheter. Personvernombudet skal bistå de registrerte med å ivareta rettighetene. Når SB1Ø leverer tjenester til andre virksomheter, og er databehandler, skal SB1Ø bidra til at behandlingsansvarlig kan oppfylle den registrertes rettigheter.

2.3 BEHANDLINGSOVERSIKT

SB1Ø skal ha en dokumentert og oppdatert behandlingsoversikt over behandlingsaktiviteter som utføres, både i rollen som behandlingsansvarlig og som databehandler.

2.4 UTLEVERING AV PERSONOPPLYSNINGER

Personopplysninger kan bare utleveres til eksterne virksomheter som har et behandlingsgrunnlag, som rettslig forpliktelse eller samtykke fra den registrerte. Ved forespørsel fra offentlig myndighet om utlevering av opplysninger, skal SB1Ø sikre at nødvendig formål og behandlingsgrunnlag er ivaretatt. Daglig behandlingsansvarlig skal beslutte om personopplysninger kan utleveres. Der SB1Ø er databehandler, er det behandlingsansvarlig som må sørge for at det foreligger et behandlingsgrunnlag. SB1Ø utleverer da kun personopplysninger etter instruks fra den behandlingsansvarlige.

2.5 Opplæring

Alle medarbeidere skal ha nødvendig kjennskap til personvernregelverket.
Opplæring skal tilpasses ulike roller, ut fra ansvar og arbeidsoppgaver.

2.6 Nyanskaffelser og endringer i systemer mv.

Ved utvikling/anskaffelse og vesentlige endringer av produkter og systemer skal SB1Ø sikre at krav til personvern er ivaretatt, innebygd og dokumentert. SB1Ø skal ivareta og dokumentere personvern i utvikling og gjennom hele systemet levetid (innebygd personvern).

2.7 Informasjonssikkerhet og risikovurdering

Behandling av personopplysninger skal ha tilfredsstillende informasjonssikkerhet. Systemer og digitale tjenester skal tilfredsstille krav til tilgjengelighet, konfidensialitet og integritet. IT-systemer skal være motstandsdyktige og robuste, slik at normaltilstand raskt kan opprettes.

- Med tilgjengelighet menes at personopplysninger og systemer er tilgjengelig ved behov.
- Med konfidensialitet menes å ivareta taushetsplikten, og sikre at uvedkommende ikke får tilgang til personopplysningene.
- Med integritet menes at personopplysninger er korrekte og pålitelige.

SB1Ø skal gjennomføre og løpende oppdatere risikovurderinger for informasjonssikkerhet. Konsekvensvurdering skal gjennomføres både for SB1Ø og for den registrerte. Formålet med risikovurderingen er å sikre at den risikoen som avdekkes ved behandling av personopplysninger er innenfor akseptabelt nivå, for både SB1Ø og for den registrerte. Nødvendige tiltak skal iverksettes.

En leverandørs risikovurdering kan brukes som underlag, men kan ikke erstatte SB1Øs egen risikovurdering. Der SpareBank 1 Utvikling har gjort risikovurderinger med tilfredsstillende kvalitet kan SB1Ø dokumentere at dokumentasjonen er gjennomgått og vurdert, og sikre at den er tilgjengelig i vår dokumentasjon.

2.8 Personvernkonsekvensvurdering

En personvernkonsekvensvurdering skal utarbeides ved behandling av personopplysninger, som kan innebære en høy risiko for de registrertes personvern, rettigheter og friheter. Formålet med personvernkonsekvensvurdering er å sikre at personvernprinsippene og de registrertes rettigheter og friheter er på et akseptabelt nivå. Systemeier eller prosjektleder er ansvarlig for å vurdere behovet for og eventuelt gjennomføre en personvernkonsekvensvurdering, og skal alltid be personvernombudet om råd. Et system skal ikke settes i drift før personvernkonsekvensvurderingen er godkjent av behandlingsansvarlig.

En leverandørs personvernkonsekvensvurdering kan brukes som underlag, men kan ikke erstatte bankens egen vurdering. Der SpareBank 1 Utvikling har gjort personvernkonsekvensvurdering med tilfredsstillende kvalitet kan SB1Ø dokumentere at personvernkonsekvensvurderingen er gjennomgått og vurdert, og sikre at den er tilgjengelig i vår dokumentasjon.

2.9 Bruk av databehandler

2.9.1 Krav til databehandleravtale

Der SB1Ø bruker en annen virksomhet til å behandle personopplysninger på SB1Øs vegne vil denne virksomheten anses som en databehandler. SB1Ø skal da sikre at databehandleren etterlever personvernregelverket og holder et tilstrekkelig sikkerhetsnivå. SB1Ø skal inngå en skriftlig databehandleravtale som regulerer ansvarsforhold og setter krav til personvern og informasjonssikkerhet.

Dersom databehandler, eller underleverandør av denne, skal behandle personopplysninger utenfor EU/EØS, skal det foreligge et gyldig overføringsgrunnlag.

2.9.2 Oppfølging av Databehandlere

SB1Ø skal jevnlig gjennomgå og følge opp databehandlerens etterlevelse av databehandleravtalen, herunder om databehandleren har gjennomført tilstrekkelige tekniske og organisatoriske tiltak som sikrer etterlevelse av personvernregelverket. Gjennomgangen skal dokumenteres. Dersom databehandler bruker underdatabehandler, skal SB1Ø ha oversikt over hele leverandørkjeden. Det er imidlertid SB1Øs databehandler som skal sikre at sine underdatabehandlere etterlever SB1Øs krav i databehandleravtalen.

Ved avslutning av et databehandlerforhold skal SB1Ø sikre at løsningen og personopplysningene blir behandlet slik avtalen beskriver ved opphør av tjenesten.

2.10 Brudd på personopplysningssikkerheten (Avvik)

Brudd på personopplysningssikkerheten (avvik) er brudd på konfidensialitet, integritet og/ eller tilgjengelighet til personopplysningene. Avvikene skal håndteres, følges opp og systematiseres for å sikre kontinuerlig læring og forbedring. Tiltak for å hindre gjentakelse og for å redusere skadevirkninger skal gjennomføres.

Alle medarbeidere i SB1Ø skal ha kunnskap om hva som er brudd på personopplysningssikkerheten og så snart som mulig varsle om brudd eller mistanke om brudd på personopplysningssikkerheten.

Oversikt over alle brudd på personopplysningssikkerheten (avvik) skal være oppdatert. Brudd på personopplysningssikkerheten skal håndteres i tråd med interne rutiner.

Brudd på personopplysningssikkerheten skal meldes til Datatilsynet med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. De registrerte skal informeres ved brudd på personopplysningssikkerheten dersom det er sannsynlig at avviket fører til en høy risiko for deres rettigheter og friheter.

2.11 Kontroll og oppfølging

SB1Ø skal ha intern kontroll for å ivareta behandling av personopplysninger og sikre at etablerte tiltak og rutiner blir fulgt. De rollene som gjennomfører arbeidsoppgaver som sikrer at banken etterlever personvernregelverket skal kontrollere egne oppgaver.

Personvernombudet og øvrige internkontrollfunksjoner skal kontrollere utvalgte områder vurdert ut fra risikoene med behandlingsaktivitetene.

3. Organisering, roller og ansvar

3.1 Behandlingsansvarlig eller databehandler

SB1Ø er behandlingsansvarlig når SB1Ø bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal brukes. Behandlingsansvarlig må etterleve kravene i denne policyen og tilhørende rutiner.

SB1Ø er databehandler når SB1Ø behandler personopplysninger på vegne av en behandlingsansvarlig.

3.2 Styret

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

3.3 Administrerende direktør

Administrerende direktør har ansvaret for å ivareta at behandlingsansvaret og databehandleransvaret etterleves i henhold til personvernregelverket. Administrerende direktør delegerer oppgaver for å sikre etterlevelse av personvernregelverket i samsvar med de generelle prinsippene for risikostyring og internkontroll.

3.4 Personvernombud

Personvernforordningen bestemmer om virksomheten skal ha personvernombud, og fastsetter også personvernombudets lovpålagte oppgaver. Personvernombudet har et særlig ansvar for at de registrertes rettigheter og friheter blir ivaretatt. Personvernombudet rapporterer til styret. Personvernombudet skal informere og gi råd, og skal kontrollere etterlevelse av personvernkravene. Personvernombudet skal gi Datatilsynet opplysninger når tilsynet ber om det, herunder foreta undersøkelser i konkrete saker.

3.5 Medarbeidere

Alle medarbeidere skal sette seg inn i og etterleve rutiner for personvern. Alle medarbeidere skal gjennomføre opplæring for å sikre at de har grunnleggende kjennskap til personvernregelverket.

4. Rapportering av personvern

Personvernombudet og behandlingsansvarlig skal rapportere status for personvern til SB1Øs styre jevnlig. Som en del av denne rapporten skal brudd på personopplysningssikkerheten (avvik) rapporteres.

5. Avvik fra personvernpolicy og oppfølging

Brudd på policy for personvern og tilhørende rutiner kan være brudd på personvernregelverket, og skal meldes som et mulig avvik.

6. Revisjon

Denne policyen skal gjennomgås årlig og revideres ved behov.

7. Definisjoner

Avvik	Brudd på personopplysningssikkerheten 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.
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	Den virksomheten som bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.

Databehandler	Virksomhet som behandler personopplysninger på vegne av behandlingsansvarlig.
Den registrerte	Personen som personopplysningene kan knyttes til.
Personopplysninger	Opplysninger om en identifiserbar fysisk person.
Personvernregelverket	Personopplysningsloven, inkludert personvernforordningen (GDPR), interne policyer og rutiner for å ivareta krav til personvern.
Særlige kategorier personopplysninger	Med særlige kategorier personopplysninger menes personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning, fagforeningsmedlemskap, genetiske opplysninger, biometriske opplysninger for å identifisere noen, helseopplysninger, seksuelle forhold og seksuell legning