Policy for personvern

1. Formål

Denne policyen inngår i den styrende delen av internkontrollen, og skal bidra til å identifisere overordnede krav og plikter til behandling av personopplysninger, samt beskrive intern organisering, ansvars- og myndighetsforhold.

For å kunne bevare og styrke egen markedsposisjon, er det avgjørende at SpareBank 1 SMN (SMN) har tillit fra kunder, eiere, samarbeidspartnere og tilsynsmyndigheter og andre interessenter. Derfor må SMN sørge for at personopplysninger behandles på en trygg og sikker måte, i samsvar med regelverket.

Overordnet formål med arbeidet med personvern i SMN er gjennom en systematisk og risikobasert tilnærming å:

- ivareta de registrertes (kunder, ansatte og andre) personvern
- understøtte forretningsdriften ved å til enhver tid ha kontroll på sine behandlinger av personopplysninger
- sikre omdømme til SMN, gjennom en korrekt håndtering av personopplysninger
- sikre etterlevelse av personopplysningsloven og GDPR

2. Målgruppe

Alle ansatte og innleide som har tilgang til og/eller bearbeider og forvalter personopplysninger gjennom SMNs IKT-infrastruktur, samt datterselskap så langt det passer.

3. Definisjoner

Behandlingsansvarlig er en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.

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

Konfidensialitet betyr å sikre at informasjonen ikke blir kjent for uvedkommende, men at informasjon og informasjonssystemer bare er tilgjengelig for de som har et tjenstlig behov og at det eksisterer et gyldig behandlingsgrunnlag.

Integritet betyr å sikre at informasjon er korrekt, gyldig og fullstendig og ikke kan endres utilsiktet eller av uvedkommende.

Tilgjengelighet betyr å sikre at informasjon og informasjonssystemer er tilgjengelig ved behov innenfor de tilgjengelighetskrav som er satt.

Robusthet betyr at organisasjonen, informasjonssystemer og tjenester som behandler personopplysninger skal kunne tåle endringer og ytre påvirkninger.

4. Styrende prinsipper og krav

SpareBank 1 SMN skal sørge for at alle som behandler personopplysninger i eller på vegne av SMN bidrar til at personopplysninger:

- 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
- er adekvate, relevante og begrenset til det som er nødvendig (dataminimering) for behandlingen
- er korrekte og oppdaterte
- lagres slik at det ikke er mulig å identifisere de registrerte lengre enn nødvendig
- behandles på en måte som ivaretar krav til informasjonssikkerhet og personopplysningssikkerhet

4.1 Oversikt over behandlinger

SMN skal ha en samlet oversikt over alle behandlinger av personopplysninger i form av en behandlingsprotokoll. Oversikten skal oppfylle minimumskravene som angitt i GDPR artikkel 30.

4.2 Opplæring

Alle medarbeidere skal ha grunnleggende kjennskap til regelverket rundt personopplysninger og taushetsplikt. Opplæring skal for øvrig tilpasses i hvor stor grad og på hvilken måte medarbeiderne håndterer personopplysninger.

4.3 Risikovurderinger

I SMN skal alle personopplysninger behandles ut fra en risikobasert tilnærming og følge en fastsatt prosess for å vurdere risiko. Riktig beslutningstaker skal stå for risikostyring og aksept av risiko.

4.4 Vurdering av personvernkonsekvenser (DPIA)

Ved behandling av personopplysninger som kan innebære en høy risiko for personvernet, og kundenes og andre registrertes rettigheter og friheter, skal det gjennomføres en vurdering av personvernkonsekvensene av behandlingen.

4.5 God og rettidig ivaretakelse av kundenes rettigheter (innsyn)

Det skal legges til rette for å ivareta rettigheter som kundens rett til informasjon, innsyn, retting av feilaktige opplysninger mv på en enkel, helhetlig og lik måte på tvers av organisasjonen.

4.6 Kontroller

Det skal etableres rutiner for hensiktsmessig kontroll av etterlevelsen av krav til ivaretakelse av personvernhensyn. En plan for løpende kontroller skal utarbeides og revideres årlig.

4.7 Systematisk oppfølging av uønskede hendelser og avvik

Det skal legges til rette for enkel innrapportering av uønskede hendelser og avvik, som deretter følges opp og systematiseres for å sikre kontinuerlig læring og forbedring.

Brudd på personopplysningssikkerheten skal meldes til Datatilsynet innen 72 timer dersom det kan foreligge en middels til høy risiko for den registrerte.

4.8 Databehandlere og utkontraktering av virksomhet

Behandling av personopplysninger kan innenfor forsvarlige rammer utkontrakteres. Det vil si at SMN overlater til andre virksomheter (databehandler) å utføre behandlingsoppgaver herunder behandling av personopplysninger, som SMN kunne utført selv.

SMN skal i slike tilfeller ha databehandleravtaler som minst samsvarer med kravene som er gitt i personvernforordningen artikkel 28 og 29, og som sikrer tydeliggjøring av ansvarsforhold og kontroll med alle slike eksterne leverandører.

4.9 Rapportering

Personvernombudet for banken skal jevnlig rapportere direkte til det høyeste ledelsesnivået hos SMN og ellers ved behov.

4.10 Tilgjengelig dokumentasjon

Styrende dokumenter herunder aktuelle rutiner mv., skal være lett tilgjengelig for ansatte og andre som utfører oppgaver for SMN, eventuelle databehandlere og for Datatilsynet.

5. Organisering og ansvar

5.1 Styret

Styret har det overordnede ansvar for at SMN etterlever personopplysningsregleverket.

Styret skal:

- Fastsette målene og overordnet strategi for arbeidet med personvern i SMN
- Påse at SMN har god internkontroll og hensiktsmessige systemer
- Påse at SMN har tilfredsstillende organisering som understøtter etterlevelsen
- Sørge for å holde seg orientert om SMNs viktigste risikoområder og beslutte om overordnet risiko er akseptabel for personvernhåndteringen i SMN.
- Vedta policy for personvern

5.2 Konsernsjef

Behandlingsansvarlig i SMN er konsernsjefen. Konsernsjefen har det øverste ansvaret for at regelverket rundt personopplysninger etterleves og operasjonaliseres i virksomheten.

Konsernsjef har delegert sine oppgaver for banken til Konserndirektør Teknologi og Utvikling i rollen som delegert behandlingsansvarlig.

5.3 Alle KL-direktører

KL-direktører har det operative behandlingsansvaret innenfor sitt område, og for at personvernet til kunder og ansatte og andre registrerte ivaretas ved de behandlinger som skjer innen ansvarsområdet.

5.4 Personvernombud

Banken skal ha ett personvernombud. Personvernombudet har en sentral, uavhengig, rådgivende, kontrollerende, koordinerende og rapporterende rolle i organisasjonen knyttet til etterlevelse av personopplysningsloven og internt regelverk. Personvernombudet skal bistå den behandlingsansvarlige i arbeidet med å ivareta kravene i personvernregelverket.

Personvernombudet skal jevnlig rapportere til styret og ellers ved behov.

5.5 Alle ansatte

Alle ansatte og innleide i SMN har ansvar for å sette seg inn i og etterleve retningslinjer og krav rundt informasjonssikkerhet og personvern, melde fra om hendelser eller dersom sikring av personopplysninger og forretningsinformasjon ikke fungerer som tiltenkt, samt gjennomføre de opplæringsaktiviteter som SMN iverksetter på området.

6. Forvaltning og revisjon av policy

Policy for personvern skal revideres årlig og godkjennes av styret ved vesentlige endringer. Policyen skal uansett styregodkjennes hvert tredje år.

7. Håndtering av avvik

Avvik fra policyen skal registreres i etablert system for avvikshåndtering og behandles av ansvarlig.

8. Referanser og relevante koblinger (kan oppdateres uten ny godkjenning)

«Policy for utkontraktering av virksomhet i Sparebank 1 SMN», stiller krav i forbindelse med inngåelse av utkontrakteringsavtaler.

Gjelder for	SpareBank 1 SMN - alle ansatte, og tillitsvalgte og alle som har tilgang til og/eller bearbeider og forvalter personopplysninger gjennom SMNs IKT-infrastruktur, samt konsernselskap så langt det passer
Hjemmel	Personopplysningsloven og GDPR art. 5 og art. 24
Ansvarlig for etterlevelse	Konsernsjef ved KL-direktører
Ansvar for oppdatering/revidering	Delegert behandlingsansvarlig
Beskyttelsesgrad	Intern
Versjon	5.0
Opprettet	23.11.2017
Dato sist oppdatert	06.08.2025