POLICY FOR PERSONVERN I SMN

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	Åpen
Versjon	3.1
Opprettet	23.11.2017
Dato sist oppdatert	02.12.2021
Styrebehandlet	04.12.2021 04.02.2021 05.03.2019 18.12.2017

Revisjonshistorikk

Dato	Versjon	Endring	Godkjent av	Forfatter
22.11.17	**1.0**	**Etablering av Retningslinjer for personvern**	**Styret**	**Nina Marie Grinde**
23.01.19	**2.0**	**Tilpasset ny personopplysninglov, herunder GDPR, og endret tittel til Policy**	**Styret**	**Åshild Margrethe Revhaug**
27.01.2021	**3.0**	**Tilføyelse av formelle roller i SBb1-Alliansesamarbeidet i 4.9.**	**Styret**	**Åshild Margrethe Revhaug**
15.11.2021	**3.1**	**Delegert behandlingsansvarlig har ansvar for oppdatering og revidering av policy**	**Styret**	**Åshild Margrethe Revhaug**

Innholdsfortegnelse

1. Innledning

1.1. Bakgrunn

Personopplysningsloven gjennomfører EUs personvernforordning 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger (Heretter forkortet GDPR). Loven og forordningen trådte i kraft 20. juli 2018. Formålet med forordningen er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger og sikre vern av den enkeltes grunnleggende rettigheter og friheter.

SpareBank 1 SMN («SMN» eller «banken» i det følgende) behandler personopplysninger knyttet til kunder og ansatte. Det samme gjelder konsernselskap.

1.2. 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.

Banken er avhengig av tillit fra kunder, eiere, samarbeidspartnere og tilsynsmyndigheter og andre interessenter for å kunne opprettholde og øke egen markedsposisjon. Banken må derfor sikre at personopplysninger håndteres på en tillitvekkende og sikker måte, i tråd med regelverket. Overordnet formål med arbeidet med personvern i SMN er gjennom en systematisk og risikobasert tilnærming å:

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

1.3. Policyer, standarder og rutiner

Policyen må ses i sammenheng med andre policyer, retningslinjer, standarder og rutiner i banken og for øvrig i SpareBank1-alliansen. Se vedlegg 2 i denne policyen.

1.4. Relevante lover på personvernområdet

Behandling av personopplysninger i SMN er regulert av en rekke lover og regler. Dette er noen av de mest sentrale:
- Personopplysningsloven av 15. juni 2018 nr. 38 med personvernforordningen (GDPR) som vedlegg av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning)
- Forskrift om bruk av e-postkasse og annet elektronisk lagret materiale
- Forskrift om kameraovervåkning i virksomhet
- Finanstilsynsloven

- Finansforetaksloven
- Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT-forskriften)
- Finansavtaleloven
- Forskrift om risikostyring og internkontroll
- Hvitvaskingsloven med forskrifter
- Markedsføringsloven

2. Sentrale krav ved behandling av personopplysninger

For å nå bankens målsetninger må banken 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

SMN skal:

- ha oversikt over de opplysninger som blir behandlet
- ha oversikt over ansvars- og myndighetsfordelingen i banken ved behandling av personopplysninger
- ha oversikt og kunnskap om regelverkskrav ved behandling av personopplysninger, herunder krav til behandlingsgrunnlag, oppfyllelse av kvalitetskrav, ivaretakelse av informasjonsplikt, innsynsrett, retting og sletting
- ha etablert hensiktsmessige og praktiske rutiner som beskriver hvordan den daglige håndtering av personopplysninger skal foregå samt sikres for å ivareta konfidensialitet, integritet og tilgjengelighet
- ha etablert kontrollrutiner som gir informasjon om hvorvidt etablerte tiltak og rutiner blir fulgt
- ha prosesser som sikrer jevnlig vurdering av behovet for nye tiltak eller endring i eksisterende tiltak og rutiner
- til enhver tid ha personvernombud som del av bankens interne kontroll.
- sikre at personvernombudet blir involvert på riktig måte og til rett tid i alle spørsmål som gjelder vern av personopplysninger. Påse i slike saker, at personvernombudets råd og vurdering blir hørt og tatt i betraktning.
- støtte personvernombudet i utførelsen av rollen og oppgaver ved å stille til rådighet de ressurser og tilganger som er nødvendig for å utføre dette.

3. Sikkerhetsmål

SMNs behandling av personinformasjon skal være i samsvar med regulatoriske, interne og avtalerettslige krav til informasjonssikkerhet.

Personopplysninger og annen beskyttelsesverdig informasjon skal vurderes, klassifiseres og håndtereres og sikres på en betryggende måte gjennom fysiske, tekniske og organisatoriske tiltak, slik at personvernet ikke krenkes.

Konfidensialitet
Personopplysninger og annen beskyttelsesverdig informasjon som behandles i SMN skal være beskyttet mot uautorisert tilgang.
Personopplysninger behandles konfidensielt og kan bare deles med andre medarbeidere i den grad det er tjenstlige behov.
Personopplysninger om egne arbeidstakere kan kun behandles av den som har tjenstlig behov.

Integritet
Informasjon som SMN har ansvaret for blir bare produsert og endret av ansatte, eller av eksterne som har fullmakt til dette. Informasjon skal ikke endres utilsiktet.

Tilgjengelighet
Behandlingssystemene - og tjenestene skal være tilgjengelige for autoriserte brukere ved behov.

Robusthet
Informasjonssystem hvor det behandles personopplysninger, skal være motstandsdyktige og robuste, slik at normaltilstand raskt kan opprettes.

4. Organisering og ansvarsforhold

Banken behandler personopplysninger i hovedsak som behandlingsansvarlig, men i enkelte tilfeller også som databehandler, blant annet for datterselskaper. Behandlingsansvarlig skal sørge for at personvernregelverket etterleves, og at nødvendige avtaler er på plass, se nærmere pkt. 5.7.

4.1. Styret

Styret har det overordnede ansvar for at banken etterlever personopplysningsregelverket.

Styret skal:

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

4.2. Konsernsjef

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

Konsernsjef skal:

- Operasjonalisere mål og strategi for personvern og informasjonssikkerhet
- Avklare ansvar og myndighetsforhold innad i banken, herunder daglig behandlingsansvar og delegere nødvendige oppgaver
- Påse at det er tilstrekkelige ressurser til å ivareta de rettslige rammebetingelser på området
- Lede den årlige gjennomgang av status på området (ledelsens gjennomgang) som oppsummerer status og gir føringer for prioriteringer fremover.
- Bidra til å skape en felles forståelse for risikobildet og behovet for sikringstiltak slik at arbeidet med personvern og informasjonssikkerhet gis nødvendig tyngde og legitimitet i hele organisasjonen.
- Konsernsjef kan delegere sine oppgaver til en av sine direktører i rollen som delegert behandlingsansvarlig

4.3. Delegert behandlingsansvarlig

KL-direktør for Teknologi og Utvikling, utøver rollen som delegert behandlingsansvarlig. Dette innebærer at direktøren opptrer som behandlingsansvarlig i det daglige.

Delegert behandlingsansvarlig skal:

- Ha et overordnet ansvar for at selskapet har skriftlige rutiner og retningslinjer for å sikre daglig behandling av persondata i henhold til gjeldende regelverk, og at disse holdes oppdatert
- Ta avgjørelser i saker om personvern på konsernsjefens vegne. Dette gjelder spesielt godkjennelse av personvernkonsekvensvurderinger (DPIAer), og om avvik skal meldes til Datatilsynet i større avvikssaker, og i avvikssaker som gjelder flere/alle bankene i SB1 Alliansen.
- I SMN vil delegert behandlingsansvarlig ta beslutninger om personvern formelle organer i SB1, herunder i Kunderåd Marked (KRM) og Kunderåd IT (KRIT)

4.4. Alle KL-direktører

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

KL direktør skal:

- Delegere oppgaver for å ivareta personvern og informasjonssikkerhet til ledere i avdelingen og påse at det avsettes tilstrekkelige ressurser for å sikre etterlevelsen.
- Påse at respektive avdeling er organisert og gjennomfører sine oppgaver slik at rettslige rammebetingelser og interne retningslinjer mv. blir etterlevd.
- Sørge for at det gjennomføres nødvendige risikovurderinger ved behandling av personopplysninger innen enheten, og at det iverksettes adekvate tiltak for å overholde kravene til behandling av personopplysninger og informasjonssikkerhet.

- Sikre at alle ledere og ansatte innen egen enhet har nødvendig opplæring for å kunne overholde kravene til behandling av personopplysninger i utførelsen av sine oppgaver.
- Sikre at identifiserte avvik følges opp og lukkes innen egne områder i samarbeid med personvernombud og teknologi, drift og sikkerhet.
- Sørge for at innehavere av roller som «systemeier», «systemansvarlig», «produkteier» og «prosesseier» og tilsvarende roller er kjent med sin rolle og tilhørende oppgaver for å ivareta kravene til personvern og informasjonssikkerhet.
- Sørge for at personvernombudet, teknologi, drift og sikkerhet, og juridisk konsulteres ved behov for bistand knyttet til bruk av personopplysninger, gjennomføringer av risikovurderinger og inngåelse av avtaler med databehandlere (leverandører), mv.
- Påse ved innføring av nye produkter eller prosesser, eller betydelige endringer i slike, at det vurderes om det foreligger behov for å inkludere personvernombudet for gjennomføring av personvernkonsekvensvurdering (DPIA) eller innhente generell råd og veiledning.

4.5. Personvernombud

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

Personvernombudet skal:

- Bidra til at SMN ivaretar personvernet til kunder, ansatte og samarbeidspartnere og andre, i samsvar med bestemmelsene i personvernforordningen, personopplysningsloven og annet relevant regelverk med personvernbestemmelser
- Informere og gi råd om forpliktelsene SMN har i henhold til personvernforordningen
- Gi SMN råd og veiledning om behandling av personopplysninger, jf. personvernforordningen art. 38 nr. 1 og 39
- På anmodning fra SMN, gi råd om vurderingen av personvernkonsekvenser (Data Protection Impact Assessment – DPIA) og kontrollere gjennomføringen av personvernkonsekvensvurderingen
- Være kontaktpunkt for de registrerte ved spørsmål om behandlingen av deres personopplysninger og om utøvelsen av de rettigheter de har etter personvernforordningen
- Være kontaktpunkt overfor og samarbeide med tilsynsmyndighetene, herunder foreta undersøkelser på forespørsel fra Datatilsynet, samt koordinere kommunikasjon om brudd på regelverk og andre avvik mellom tilsynet og SMN.
- Kontrollere etterlevelse av personvernforordningen og interne personvernretningslinjer

4.6. Juridisk

Juridisk avdeling har det overordnede juridiske fagansvaret i SMN.

Juridisk avdeling skal:

- Bistå med avklaringer knyttet til personvern, herunder regelverkskrav til risikovurderinger og utkontrakteringer

- Kvalitetssikre avtaler, herunder databehandleravtaler

4.7. Etterlevelse

Personvernombudet er organisatorisk plassert i Etterlevelsesfunksjonen, og har faglig ansvar for kontroll og rådgivning knyttet til etterlevelse av personopplysningsloven.
Etterlevelsesfunksjonen kan ellers også gjennomføre kontroller innenfor området.

Etterlevelsesfunksjonen skal også:

- Bidra til å identifisere nye og endrede lovkrav knyttet til personvern,
- Vurdere og utrede konsekvenser av endringer slik at det blir foretatt nødvendige endringer i prosesser og rutiner.

4.8. Risikostyring

Risikostyring har ansvaret for den overordnede risikostyringen og skal bistå de ulike områdene i deres risikostyring på området.

Risikostyring skal:

- Sørge for å videreutvikle bankens rammeverk for helhetlig risikostyring
- Sørge for at det er etablert metodikk og verktøy for risikovurderinger,
- Sørge for overordnede rapporteringsstrukturer til konsernsjef og styret ift. risikorapportering (f.eks. lederbekreftelse)
- Sørge for en effektiv rutine for godkjenning av nye produkter og prosesser som alle inneholder spørsmål knyttet til etterlevelse av personopplysningsloven.

4.9. Alle ansatte

Alle ansatte har plikt til å sette seg inn i de rutiner og instrukser som gjelder og spørre nærmeste leder eller personvernombudet om noe er uklart.

Ansatte som blir kjent med brudd på personopplysningssikkerheten skal melde ifra til om dette i bankens kanaler og eventuelt direkte til personvernombudet uten ugrunnet opphold, slik at banken ved personvernombudet kan overholde fristen for å melde avviket til Datatilsynet innen 72 timer der slik melding skal sendes.

4.10. Samarbeidsfora i SpareBank1-Alliansen

4.10.1. Felles Bestiller

Felles Bestiller består av representanter fra regionbankene i SB1-alliansen og representant for Samspar-bankene. Felles Bestiller innstiller og forvalter de økonomiske rammene for drifts- og investeringsbudsjettet på vegne av styret for SB1 Utvikling, og opptrer som avtalepart fra bankene med SB1U som leverandør og databehandler ved Fellestjenester.
Representant fra SMN er Konserndirektør Finans.

4.10.2. Kunderåd Marked (KRM)

Kunderåd Marked -har ansvaret for samlet kundetilbud for Felles tjenester for SB1-bankene, herunder utvikling av felles produkter og tjenester, felles retning og innhold i samarbeidsområder på forretnings- og markedssiden, og innstiller sammen med Kunderåd IT på Masterplan.
Konserndirektør for PM representerer SMN i dette organet.

4.10.3. Kunderåd -IT (KRIT)

Kunderåd IT har ansvaret for utvikling av felles kapabiliteter, herunder arkitektur, infrastruktur og løsninger, som er nødvendig for å understøtte de forretningsmessige behovene. Videre får KRIT ansvar for innhold i felles samarbeidsområder på IT-siden og innstiller sammen med Kunderåd Marked på Masterplan.
Kunderåd IT har ansvaret for å følge opp at løpende utviklingsaktiviteter følger vedtatte arkitekturprinsipper.
Konserndirektør for Teknologi og Utvikling representerer SMN i Kunderåd- IT.

5. Strategier for å sikre etterlevelse

5.1. Oversikt over behandlinger (behandlingsprotokoll)

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

Protokollen er dokumentasjon over bankens behandlinger av personopplysninger, og at slik behandling skjer i tråd med regelverkskravene.

Bankens ledere har et ansvar for at alle nye behandlinger eller endringer i behandling av personopplysninger innen sitt ansvarsområde, legges inn og dokumenteres i protokollen/behandlingsoversikten.
Behandlinger som driftes av SB1 Utvikling, skal i tillegg dokumenteres i egen protokoll som SMN har tilgang til.

5.2. 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.

5.3. Risikovurderinger

All behandling av personopplysninger i SMN skal gjennomføres basert på en risikobasert tilnærming. Risikostyring og aksept av risiko er et lederansvar.

Ved all informasjonsbehandling og bruk av personopplysninger foreligger det en risiko for brudd på konfidensialitet, integritet og tilgjengelighet. Risikoaksept og tiltak skal stå i forhold til

sannsynligheten for og konsekvensen av sikkerhetsbrudd. Restrisiko (risiko etter tiltak) skal være akseptert av ledelsen.

Det skal gjennomføres jevnlige risikovurderinger av personopplysningssikkerheten ved endringer som har betydning for ivaretakelse av den enkeltes personvern, og rettigheter og friheter, og ved enhver ny behandling av personopplysninger.

Risikovurderinger er en metode for å fastsette tilstrekkelige sikringstiltak (tekniske eller organisatoriske) og skal ta utgangspunkt i personopplysningenes beskyttelsesbehov og fastsatte klassifisering.

Risikovurderingene skal vurdere risiko for tap av liv og helse, økonomisk tap for den enkelte eller tap av anseelse og personlig integritet ved at personopplysninger kommer uvedkommende i hende, endres utilsiktet, ikke er tilgjengelig ved behov eller at personvernhensyn på andre måter blir krenket. Der slik fare er til stede skal de planlagte og systematiske tiltakene som treffes i samsvar med personopplysningsloven, stå i forhold til sannsynligheten for og konsekvensen av sikkerhetsbrudd. Slike tiltak kan enten være av organisatorisk, teknisk eller fysisk karakter.

Negative funn gjennom en risikovurdering som er utenfor det som i forkant er definert som akseptabel risiko, skal rapporteres videre oppover i linjen slik at tiltak enten kan besluttes iverksatt eller det treffes beslutning om at den aktuelle risikoen aksepteres.

Risikovurderingene gjennomføres i henhold til metodeverk og rammer utarbeidet for bruk i SMN. Resultatet av risikovurderingen og aksept av eventuell restrisiko, skal dokumenteres.

Risikovurderingene skal vurderes på ny årlig eller ved behov.

5.3.1. 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. Egen mal for DPIA skal benyttes.

Ansvar for utarbeidelse av DPIA, tilhører ansvarlig KL-direktør innenfor respektivt område. Delegert behandlingsansvarlig godkjenner endelig DPIA.

Personvernombudet skal bistå ved gjennomgangen og gi sin vurdering i saken, sammen med leder for informasjonssikkerhet.
Dersom risikovurderingen viser at det kan være høy risiko for personvernet også etter eventuelle tiltak, skal Datatilsynet konsulteres.

Delegert behandlingsansvarlig skal påse at vurderingen fremlegges tilsynet for vurdering innen behandling kan skje.
.
Ansvarlig KL-direktør skal sørge for at en ansvarlig innen direktørens respektive ansvarsområde, forvalter og følger opp DPIAer som er utarbeidet på jevnlig basis.

5.4. God og rettidig ivaretakelse av kundenes rettigheter

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.

5.5. 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. Både kontroller utført av avdelingene selv, Personvernombudet og Etterlevelsesfunksjonen skal inngå i slik plan.

5.6. 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.

Alle ledere har et særlig ansvar for å være oppmerksomme på avvik og brudd på personopplysningssikkerheten innen sine ansvarsområder, og sørge for forsvarlig håndtering i samarbeid med personvernombudet, og at avvik meldes til Datatilsynet ved brudd som kan medføre risiko for personvernet.

Banken ved Etterlevelse, skal melde inn brudd på personopplysningssikkerheten til Datatilsynet innen 72 timer dersom det kan foreligge en middels til høy risiko for den registrerte.

5.7. 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.

I de tilfeller databehandlingen innebærer en overføring av personopplysninger utenfor EØS-området, skal det vurderes om det foreligger et særskilt overføringsgrunnlag. Juridisk eller/og personvernombudet skal alltid konsulteres i slike saker.

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.

SMN skal forsikre seg om at databehandleren holder et tilstrekkelig sikkerhetsnivå. Dette gjøres ved å gjennomføre en risiko- og sårbarhetsanalyse. Databehandler må også kunne dokumentere hvordan de arbeider med informasjonssikkerhet.

SMN skal minimum annen hvert år gjennomføre sikkerhetsrevisjoner av sine viktigste databehandlere, og for øvrig etter en risikobasert tilnærming.

I de tilfeller banken har felles behandlingsansvar med en annen behandlingsansvarlig, skal det skriftlig avtales en ordning mellom partene for å sikre personvernet, og hvordan de registrertes rettigheter og friheter, kan ivaretas.

Der banken opptrer som databehandler, har banken et ansvar for å gi råd til behandlingsansvarlig om regelverket, slik at behandlingen av personopplysninger skjer i overenstemmelse med grunnleggende regulatoriske krav.

Se for øvrig «Policy for utkontraktering av virksomhet i SpareBank 1 SMN» som stiller krav i forbindelse med inngåelse av utkontrakteringsavtaler.

5.8. Rapportering

Personvernombudet skal rapportere direkte til det høyeste ledelsesnivået hos SMN.

Rapporteringen skal omfatte:

- Kvartalsvise rapporter i forbindelse med Etterlevelsesrapport
- Minst halvårlig rapportering til konsernsjef om generell status for SMNs behandling av personopplysninger.
- Årlig rapportering til styret

Personvernombudets råd og vurderinger i saker som omhandler vern av personopplysninger skal dokumenteres og følge saken frem til beslutningstaker.

Dersom det ved SMN blir tatt avgjørelser som kan være i strid med personvernlovgivningen eller det ikke i tilstrekkelig grad blir tatt hensyn til personvernombudets råd, skal personvernombudet gis mulighet til å legge frem sine vurderinger til de som skal ta avgjørelsen, og om nødvendig virksomhetens øverste ledelse ved konsernsjefen. Dersom forholdet ikke blir avklart, kan personvernombudet rapportere forholdet til styret.

5.9. Tilgjengelig dokumentasjon

Dokumentasjonen av internkontroll herunder aktuelle rutiner mv., skal være lett tilgjengelig for ansatte og andre som utfører oppgaver for banken, eventuelle databehandlere og for Datatilsynet.

6. Vedlegg 1

Policyer:

- Policy for informasjonssikkerhet
- Policy for utkontraktering av virksomhet i SpareBank1 SMN

Rutiner og retningslinjer:

- Rutine for avvikshåndtering av personopplysninger
- Rutine ved forespørsel om innsyn
- Rutine for databehandleravtaler
- Rutine for DPIA – vurdering av personvernkonsekvenser
- Retningslinje for sletting