2018

Policy for personvern

SpareBank 1 Nord-Norge konsern (SNN)

SpareBank 1 NORD-NORGE

Innhold

Eier	Complianceavdelingen
Skrevet av	
Gjelder for	SpareBank 1 Nord-Norge og datterselskaper i konsernet
Filnavn	Policy for personvern
Tilgjengelighet	Korsn
Status	Til godkjenning
Versjon	0.10
Opprettet	05.04.2018
Sist endret	
Antall sider	6

1. Innledning

SpareBank 1 Nord-Norge og dets datterselskaper (SNN) skal ha en policy for personvern for å ivareta at det til enhver tid gjeldende personvernregelverk er implementert og at det etterleves og kontrolleres.

Med personvernregelverk menes bl.a. den til enhver tid gjeldende personopplysningslov med evt. tilhørende forskrifter, policyer, strategier og standarder fra SpareBank 1-alliansen, samt styringsdokumenter, interne retningslinjer og rutiner for SNN.

Formålet med policyen er å sikre at enkeltpersoners personvern ikke blir krenket som følge av SNNs behandling av personopplysninger.

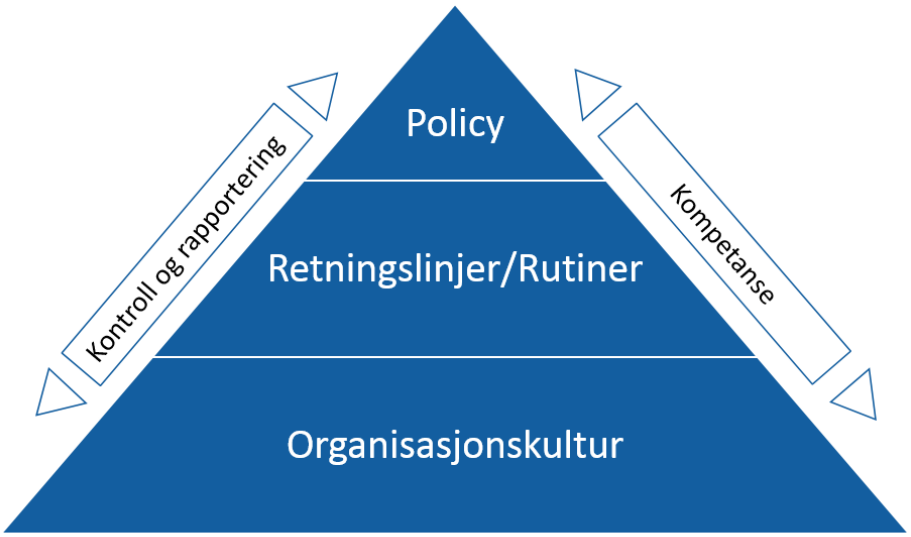
2. Definisjoner

Personopplysning	Opplysninger og vurderinger som kan knyttes til en enkeltperson
Behandling av personopplysninger	Enhver operasjon eller rekke av operasjoner som omfatter personopplysninger, både automatisert og ikke automatiserte operasjoner, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning, endring eller utlevering av personopplysninger, eller en kombinasjon av disse
Den registrerte	En identifisert eller identifiserbar fysisk person som en personopplysning kan knyttes til
Sensitive personopplysninger	Opplysninger om rase, etnisk bakgrunn, politisk, filosofisk eller religiøs oppfatning, opplysninger om en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, helseforhold, seksuelle forhold, medlemskap i fagforeninger
Behandlingsansvarlig	Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Formelt ligger ansvaret hos øverste ledelse i det aktuelle selskapet i konsernet, men i praksis vil det daglige operasjonelle ansvaret ligge hos systemeier i det aktuelle selskap.
Databehandler	Den som behandler personopplysninger på vegne av den behandlingsansvarlige, f.eks. underleverandører som behandler personopplysninger. F.eks. vil banken være databehandler for datterselskapene når den håndterer HR-rollen på vegne av døtrene.
Personvernombud	En person i konsernet som har som oppgave å rapportere til ledelsen og holde kontakten med Datatilsynet vedrørende personvernrelaterte spørsmål, samt rådgi i personvernrettslige spørsmål og kontrollere etterlevelse.

3. Formål og rammeverk for personvernarbeid

SNN skal ha effektive retningslinjer og rutiner for å sikre ivaretakelse av personvern og etterlevelse av personvernregelverket. Formålet med retningslinjene er å ivareta

privatpersoner og å sikre at SNN ikke bryter lovregler. Brudd på lovregler kan føre til betydelige økonomiske konsekvenser og omdømmerisiko for SNN.



Figur 1: Rammeverk for personvern

Formålet nås ved:

- aktiv og effektiv opplæring av nye medarbeidere (kompetanse)
- fokus på personvern i alle ledd i den daglige drift (policy)
- aktive tiltak for å opprettholde kompetanse på personvern, f.eks. gjennom tiltak som «Passopp» moduler og årlig gjennomgang av reglene på avdelingsmøter (kompetanse)
- oppdaterte og skriftlige, effektive retningslinjer og rutiner for personvern (retningslinjer/rutiner)
- å sikre ansatte enkel tilgang til gjeldende retningslinjer og rutiner i Korsn (organisasjonskultur)
- implementering av de til enhver tid gjeldende Sparebank 1-alliansens styrende dokumenter hva gjelder personvern (policy)
- årlig utarbeidelse av en risikoanalyse (kontroll og rapportering)
- gjennomføring av en effektiv internkontroll

4. Behandling av personopplysninger

All behandling av personopplysninger i SNN skal skje i samsvar med gjeldende personvernregelverk, herunder SpareBank 1-alliansens regler for personvern slik de fremkommer i policyer, standarder, og rutiner.

4.1 Prinsipper

Personvernopplysninger skal behandles i tråd med følgende grunnleggende prinsipper for behandling av personopplysninger:

- **Lovlighet og rettferdighet:** SNN skal kun behandle personopplysninger når det er tillatt etter loven, og hvor dette anses rettferdig i det konkrete tilfellet. I tillegg til at

behandlingen må forankres i et rettslig grunnlag, skal denne gjøres i respekt for de registrertes rettigheter og i samsvar med deres rimelige forventninger.

- **Gjennomsiktighet:** SNNs behandling av personopplysninger skal som utgangspunkt være åpen, hvilket bl.a. vil si at opplysninger skal registreres slik at den opplysningene gjelder skal kunne få innsyn i informasjon om seg selv, og behandlingen av denne.

- **Formålsbegrensning:** SNN skal kun samle inn 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 har en entydige forståelse av hva personopplysningene skal brukes til. Personopplysninger skal ikke behandles for andre formål som er uforenlige med de opprinnelige formålene. F.eks. hvis personopplysninger samles inn i forbindelse med en lånesøknad, kan banken i utgangspunktet ikke bruke disse til noe annet enn å vurdere lånesøknaden.

- **Dataminimering:** SNNs behandling av personopplysninger skal være adekvat, relevant og begrenset til det som er nødvendig for det konkrete formål de ble samlet inn for. Dette betyr f.eks. at opplysningene skal slettes når vi ikke lenger har et saklig behov for disse.

- **Riktighet:** SNN skal ha korrekte og oppdaterte personopplysninger. Kunder, ansatte osv. kan be om at uriktige opplysninger korrigeres.

- **Lagringsbegrensning:** SNN skal bare lagre personopplysninger når konsernet har et grunnlag for det. Når de lagrede personopplysningene ikke lenger er nødvendige for formålet de ble innhentet for, skal de lagres anonymisert eller slettes.

- **Integritet og fortrolighet:** SNN skal behandle personopplysninger fortrolig og med integritet, slik at kunder, ansatte og andre har tillit til oss. Dette betyr at vi skal behandle disse med tilstrekkelig sikkerhet, herunder vern mot uautorisert eller ulovlig behandling og lignende.

- **Ansvarlighet:** SNN skal være en ansvarlig aktør og alle l i konsernet skal opptre i samsvar med reglene for behandling av personopplysninger.

4.2 Informasjonssikkerhet

For å ivareta informasjonssikkerheten må SNN behandle alle personopplysninger konfidensielt, og sikre at tilgjengeligheten til opplysningene begrenses til de som har behov for informasjonen.

Informasjonssikkerheten er ivaretatt når personopplysninger som behandles av SNN håndteres på en trygg og sikker måte. Dette ivaretas gjennom adgangskontroll i systemene, slik at det kun er de som har berettiget interesse som har innsynsrett. Informasjon blir oppbevart og lagret i henhold til systemrutiner. Fysisk oppbevaring av personopplysninger

skal kun skje i avlåste arkivskap. For øvrig skal utlevering, sletting og makulering av opplysninger skje i henhold til beskrevne rutiner.

Det skal foreligge overordnede rutiner for oppbevaring, sletting og utlevering av informasjon, utarbeidet av leder for Compliance. Disse skal legge føringer for ivaretakelse av personvern ved utarbeidelse av nye rutiner for det enkelte system og prosess som behandler personopplysninger.

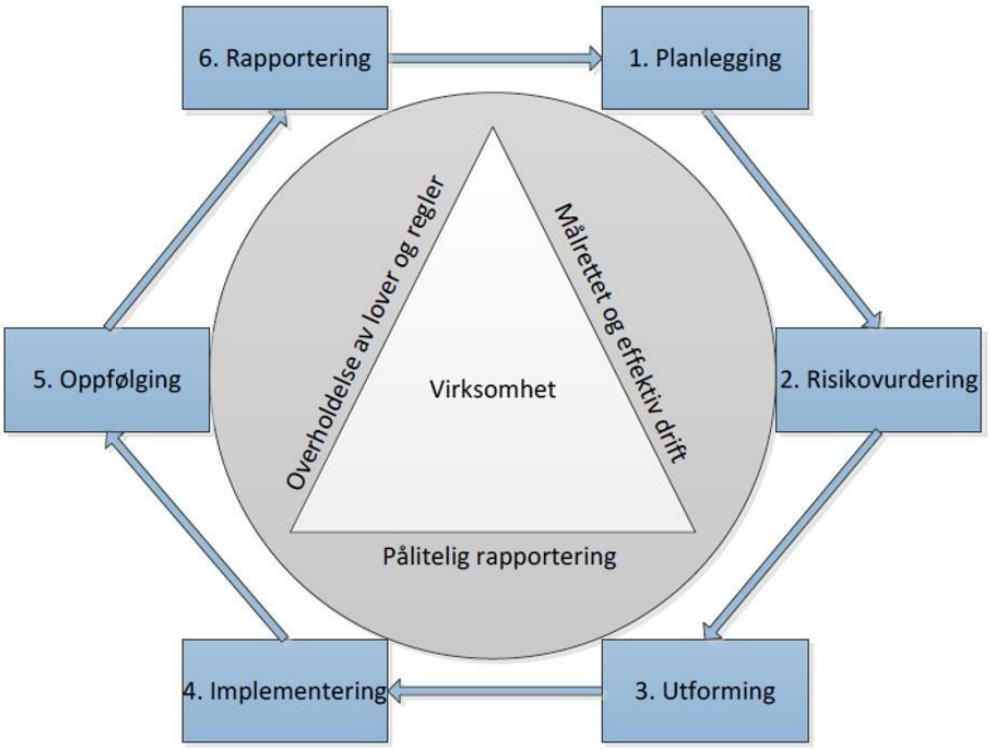
4.3 Internkontroll

Sikkerhetstiltak skal dokumenteres. Det er et krav etter personvernlovgivningen at SNN til enhver tid vurderer hvorvidt sikkerhetstiltakene er tilfredsstillende i forhold til risiko.

En effektiv internkontroll skal sikres gjennom å etablere og holde ved like egnede tekniske og organisatoriske tiltak.

Internkontrollsystemet består av et fundament som omfatter styrings- og kontrollmiljø, og informasjon- og kommunikasjon (triangel). Internkontrollprosessen består av planlegging, risikovurdering, utforming, implementering, oppfølging og rapportering.

Eventuelle brudd på gjeldende personvernregelverk skal straks meldes til personvernombudet.



Figur 2: Internkontrollsystem

5. Roller og ansvar

Behandlingsansvarlig (virksomhetens leder) har det overordnede ansvaret for at grunnkravene for behandling av personopplysninger er oppfylt, at informasjonssikkerheten ivaretas tilstrekkelig og at effektive retningslinjer og rutiner hva gjelder personvern utarbeides, implementeres og etterleves. Videre har behandlingsansvarlig i konsernet (Konsernsjef) ansvar for at det utpekes et personvernombud med nødvendig kompetanse. Behandlingsansvarlig har også ansvaret for at styret mottar nødvendig informasjon for å påse at virksomheten etterlever kravene på personvernområdet.

I SNN delegeres det daglige operasjonelle ansvaret for etterlevelse av personvernregelverket slik det fremgår av de til enhver tid gjeldende rutiner og stillingsinstrukser. Den operasjonelt ansvarlig vil normalt ha en systemeierrolle i konsernet.

Systemeiere har et selvstendig internt ansvar for at behandling av personopplysninger i personopplysningsloven er oppfylt, og at kravene til informasjonssikkerhet etterleves. I tillegg har de andre oppgaver som følger av egen instruks. Selv om det daglige operasjonelle ansvaret delegeres internt i organisasjonen, er det alltid øverste ledelse som har behandlingsansvaret utad.

Databehandleravtaler kan inngås i to forskjellige typer konstellasjoner; eksternt eller internt. For eksempel skal det foreligge en databehandleravtale med Visma når Regnskapshuset benytter seg av deres tjenester som behandler personopplysninger på deres vegne. Da er Visma databehandler og Regnskapshuset behandlingsansvarlig. Ved avtaler internt i konsernet får vi interne databehandleravtaler, for eksempel der bankens HR avdeling er databehandler overfor Regnskapshuset og behandler personopplysninger om de ansatte i Regnskapshuset, på vegne av Regnskapshuset som behandlingsansvarlig. Motsatt vil eksempelvis banken kunne være behandlingsansvarlig og Regnskapshuset databehandler dersom Regnskapshuset i fremtiden kjører lønn for bankens ansatte.

Databehandlere for SNN behandler personopplysninger på vegne av det enkelte selskaper som er part i avtalen. SNN skal bare bruke databehandlere som har inngått en databehandleravtale. En databehandler kan ikke behandle personopplysninger på annen måte enn det som følger av avtalen (databehandleravtalen).

Banken som databehandler behandler personopplysninger på vegne av sine datterselskaper (behandlingsansvarlige). Bankens datterselskaper skal bare bruke banken som databehandler når banken har inngått databehandleravtale. Banken som databehandler kan ikke behandle personopplysninger på annen måte enn det som følger av avtalen med bankens datterselskaper (databehandleravtalen).

Personvernombudet skal involveres i alle spørsmål som gjelder vern av personopplysninger. I tillegg har personvernombudet andre oppgaver som følger av egen instruks.

Complianceavdelingen skal sikre at endringer i personvernregelverket fanges opp, samt bistå med implementering i instrukser, rutiner og retningslinjer som gjelder personvern.

Complianceavdelingen skal involveres ved gjennomføring av risikovurdering og konsekvensanalyse når nye systemer og prosesser vurderes iverksatt, og skal godkjenne nye behandlinger av personopplysninger, samt vesentlige endringer i eksisterende behandling.

Complianceavdelingen skal også sørge for at det blir utført jevnlige kontroller for etterlevelse av personvernregelverket.

Ledere og medarbeidere har ansvar for å følge, og holde seg oppdatert på, gjeldende personvernregelverk og på SNNs retningslinjer og rutiner. Dette gjøres gjennom deltakelse i intern opplæring og ved selvstudie av retningslinjer, rutiner og annen informasjon som gjøres tilgjengelig i Korsn.

6. Rapportering

Rapportering av personvernstatusen i SNN inngår i compliancerapport som årlig oversendes til konsernledelse og styret. I tillegg behandles utvalgte personvernrettslige temaer i kvartalsvise risikorapporter og i lederbekreftelsen.

Datterselskaper skal årlig avgi rapport til complianceavdelingen på status i arbeidet med personvern, herunder resultatet av gjennomførte kontroller.