POLICY FOR PERSONVERN

Innhold

1.0 FORMÅL

SpareBank 1 Nord-Norge (SNN) håndterer store mengder personopplysninger som en del av daglig drift som et finanskonsern. Dette gjelder både personopplysninger på vegne av kunder og om egne medarbeidere.

I de prosesser og oppgaver SNN utfører er det viktig å ivareta den registrertes personvern og håndtere personopplysninger på en god og sikker måte, i tråd med personvernregelverket. Dette vil skape tillit hos kunder, medarbeidere, samarbeidspartnere, eiere og tilsynsmyndigheter, og kunne skape nye forretningsmuligheter.

Den overordnede målsettingen for alt arbeid med personvern i SNN er derfor gjennom en systematisk og risikobasert tilnærming å

- ivareta de registrertes personvern
- understøtte forretningsdriften ved at konsernet til enhver tid har kontroll på sine behandlinger av personopplysninger
- sikre omdømme til SNN gjennom korrekt håndtering av personopplysninger
- sikre etterlevelse av personopplysningsloven og EUs personvernforordning (GDPR), øvrig personvernregelverk relevante bransjenormer og tilhørende interne standarder og rutiner
- dokumentere etterlevelsen.

SNN skal ta hensyn til personvern i alle utviklingsfaser av et system eller en løsning. Videre skal SNN som standard bare samle inn personopplysninger som er nødvendige for det spesifikke formålet med behandlingen. Den operasjonelt ansvarlige vil normalt være produkteier, systemeier eller prosesseier avhengig av ansvarsfordelingen for det enkelte system/prosess.

Denne policyen inngår i den styrende delen av internkontrollen. Den skal bidra til at SNN etterlever det til enhver tid gjeldende regelverk innen personvern.

2.0 PRINSIPPER

2.1 Relevante lover og forskrifter på personvernområdet

Behandling en av personopplysninger i SNN er primært regulert av personopplysningsloven og EUs personvernforordning (GDPR). I tillegg er det også en rekke andre lover og forskrifter som legger føringer for selskapets behandling av personopplysninger.

Dette er noen av de mest sentrale:

- Personopplysningsloven med EUs personvernforordning (GDPR)
- Forskrift om bruk av e-postkasse og annet elektronisk lagret materiale
- Forskrift om kameraovervåkning i virksomhet
- Finansforetaksloven
- Finansavtaleloven

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

2.2 Sentrale krav ved behandling av personopplysninger

Alle som behandler personopplysninger, skal bidra til at personopplysningene behandles i tråd med de grunnleggende prinsippene for behandling av personopplysninger:

Lovlighet, rettferdighet og åpenhet: SNN skal kun behandle personopplysninger når det er tillatt etter personvernregelverket, og hvor dette anses rettferdig i det konkrete tilfellet. Behandlingen må forankres i et rettslig grunnlag, og den skal gjøres i respekt for de registrertes rettigheter og i samsvar med deres rimelige forventninger. I tillegg skal SNN sin behandling av personopplysninger som et utgangspunkt være åpen, det vil blant annet si at opplysninger skal registreres slik at de 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 entydig forståelse av hva personopplysningene skal brukes til. Personopplysninger skal ikke videre behandles for formål som er uforenlige med de opprinnelige formålene.

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

Riktighet: SNN skal ha korrekte og oppdaterte personopplysninger. Medarbeidere, kunder og andre vi behandler personopplysninger om, kan be om at uriktige opplysninger rettes.

Lagringsbegrensning: SNN skal bare lagre personopplysninger når selskapet 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 konfidensialitet: SNN skal behandle personopplysninger fortrolig og med integritet, slik at medarbeidere, kunder 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 som kan påvise at vi etterlever personvernregelverket.

2.3 Utarbeidelse av standarder og rutiner

SNN skal utarbeide standarder og rutiner for å sikre etterlevelse av regelverket på personvernområdet og prinsippene i denne policyen.

3.0 ROLLER OG ANSVAR

SNN behandler personopplysninger som behandlingsansvarlig og som databehandler.

3.1 Styret i SNN

Styret i SNN har det overordnede ansvaret for å sikre at selskapet etterlever personvernregelverket.

3.2 Konsernsjef

Konsernsjef har det øverste ansvaret for at grunnkravene for behandling av personopplysninger er oppfylt, at informasjonssikkerheten ivaretas og at skriftlige rutiner som beskriver den daglige håndteringen av personopplysninger utarbeides og etterleves.

Vedkommende kan delegere utførelse av oppgavene knyttet til behandlingsansvaret og databehandlerrollen til en eller flere definerte roller.

Konserndirektør som får delegert beskrevet ansvar, skal sørge for at alle ansatte, vikarer og innleide konsulenter gis opplæring i personvernreglementet til SNN. I tillegg omfatter ansvaret også at disse setter seg inn i og etterlever de rutiner og retningslinjer som gjelder behandling av personopplysninger i SNN.

3.3 Konserndirektører og andre ledere i SNN

Konserndirektører har for sitt ansvarsområde plikt til å dokumentere at kravene for behandling av personopplysninger er oppfylt i henhold til gjeldende rett for virksomheten, herunder utarbeidelse av skriftlige rutiner om den daglige håndteringen av personopplysninger.

Dette ansvaret kan delegeres til andre ledere.

3.4 Styret i datterselskap

Styret i datterselskapene har det overordnede ansvaret for å sikre at selskapet etterlever personvernregelverket.

3.5 Administrerende direktører i datterselskap

Som for pkt 3.2 tredje avsnitt og 3.3

3.6 Systemeiere og prosesseiere

Systemeiere og prosesseiere har ansvaret for at behandlingen av personopplysninger i deres produkter/systemer/prosesser skjer i henhold til kravene i personopplysningsloven, og at kravene til informasjonssikkerhet etterleves.

Det nærmere innholdet i disse rollenes ansvar skal følge av egne stillingsbeskrivelser.

3.7 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 behandlingsansvarlige i arbeidet med å ivareta kravene i personvernregelverket.

3.8 Compliancefunksjonen

Compliancefunksjonen utøver en rådgivende og kontrollerende rolle for å påse etterlevelse av alle regulatoriske krav og interne retningslinjer i hele konsernet.

3.9 Risk Management

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

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

3.10 Juridisk

Juridisk avdeling har det overordnede juridiske fagansvaret i SNN. Juridisk avdeling skal blant annet bistå med avklaringer knyttet til personvern, herunder regelverkskrav til risikovurderinger og utkontrakteringer, samt kvalitetssikre avtaler, herunder databehandleravtaler.

3.11 Fagansvarlig personvern og personvernkoordinatorer

Det operative behandlingsansvaret kan ivaretas gjennom roller som fagansvarlig personvern og personvernkoordinatorer. Deres oppgaver fastsettes i standard for personvern.

4.0 RAPPORTERING

De ansvarlige etter denne policyen skal rapportere til styret hva angår SNN sin etterlevelse av gjeldende personvernreglement. Det gjøres gjennom kvartalsvis førstelinjerapport til styret, samt at personvernombud rapporterer til styret per kalenderår.

Personvern berøres også i risikorapport og compliancerapport som jevnlig framlegges til styret.

Det skal i den daglige virksomhet legges til rette for enkel innrapportering av brudd på personopplysningssikkerheten, som deretter følges opp og systematiseres for å sikre kontinuerlig læring og forbedring.

Alle medarbeidere i SNN skal ha et bevisst forhold til hvilke krav som stilles til behandling av personopplysninger og så snart som mulig varsle ved mistanke eller kunnskap om et brudd på personopplysningssikkerheten iht SNNs rutine for håndtering av avvik på personopplysningssikkerheten.

5.0 REGULATORISKE KRAV SOM LEGGER FØRINGER FOR POLICYEN

L15.06.2018 Nr. 38 Lov om behandling av personopplysninger.

Policy for personvern besluttes av styret og forvaltes av delegert behandlingsansvarlig. Mindre endringer og presiseringer av innholdet i denne policyen, kan besluttes av delegert behandlingsansvarlig.