Retningslinjer for behandling av personopplysninger

Vedtatt av Ledergruppen i SpareBank 1 Forsikring AS
Juni 2021

Innhold

Revisjonshistorikk:

Versjon	Dato	Kommentar	Vedtatt av
1.2	19.9.2016	Ny retningslinje	Ledergruppa SpareBank 1 Forsikring
1.3	28.11.2017	Revidert versjon	Ledergruppa SpareBank 1 Forsikring
1.4	19.09.2019	Revidert etter omorganisering av SB1F	
1.5	10.06.2021	Oppdatert retningslinje: inntatt registrertes rettigheter, endret rollerbeskrivelser samt redaksjonelle endringer	Ledergruppa SpareBank 1 Forsikring AS

1 Bakgrunn og formål

Dette dokumentet er et juridisk dokument tilhørende policy for compliancerisiko . Dokumentet skal bidra til at SpareBank 1 Forsikring AS (heretter kalt Selskapet) etterlever reglene i personvernregelverket, det vil si personvernforordningen, personopplysningsloven, interne retningslinjer og policyer.

Dokumentet identifiserer overordnede krav til behandling av personopplysninger og beskriver intern organisering, ansvars- og myndighetsforhold. Kravene er videre operasjonalisert i skriftlige rutiner.

2 Omfang

Dette dokumentet gjelder all behandling av personopplysninger i Selskapet. En personopplysning er enhver opplysning om en identifisert eller identifiserbar fysisk person.

Dette dokumentet gjelder for alle ansatte i Selskapet (inkl. vikarer og konsulenter), samt Selskapets styre. Retningslinjene omfatter Selskapets behandling av personopplysninger knyttet til potensielle og etablerte kundeforhold, opplysninger om ansatte og innleide, opplysninger som behandles i forbindelse med sikkerhetstiltak og opplysninger fra logging av nettrafikk.

3 Mål

Selskapet skal innrette og organisere sin virksomhet på en slik måte at Selskapets behandlinger av personopplysninger skjer i tråd med lovgivning og interne rutiner. Selskapets behandlinger av personopplysninger skal skje på en etisk forsvarlig måte.

4 Lovkrav

Selskapets behandling av personopplysninger er regulert av personopplysningsloven, personvernforordningen og personopplysningsforskriften. I tillegg reguleres behandlingen av særlovgivning, og da spesielt forsikringsavtaleloven, finansforetaksloven og forsikringsvirksomhetsloven. Selskapet skal også se hen til relevant selvregulering i bransjen i sitt arbeid med behandling av personopplysninger.

I henhold til personvernforordningen artikkel 24, nummer 2, skal den behandlingsansvarlige virksomheten (Selskapet) iverksette egnede retningslinjer for vern av personopplysninger.

5 Prinsipper

5.1 Behandlingsgrunnlag

Enhver behandling av en opplysning som kan knyttes opp mot en enkeltperson defineres som behandling i lovens forstand. Dette tilsier at blant annet registrering, utsending, analysering, tilgjengeliggjøring, sending, lagring og sletting, er å anse som behandling i lovens forstand. Alle behandlinger av personopplysninger skal oppfylle ett av vilkårene i GDPR artikkel 6, dvs. at behandlingen skal ha et behandlingsgrunnlag.

For særlige kategorier kreves i tillegg et behandlingsgrunnlag fra GDPR artikkel 9. I Selskapet behandles personopplysninger primært for å oppfylle en avtale med den registrerte, etter samtykke, for å etterleve en rettslig forpliktelse eller for å ivareta en berettiget interesse. Særlige kategorier av personopplysninger behandles primært på bakgrunn av samtykke, for å fastsette, gjøre gjeldende eller forsvare et rettskrav eller for statistiske formål.

5.1.1 Nærmere om samtykke

Dersom Selskapet ikke har annet behandlingsgrunnlag, kreves det at kunden har avgitt et samtykke til behandlingen. Samtykket skal være frivillig, spesifikt, informert og utvetydig. Samtykket skal også være dokumentert.

For de fleste situasjoner hvor samtykke er påkrevd har Selskapet utformet standardiserte skjemaer. Disse vil også være i samsvar med bransjestandarder på dette området. I tillegg henter Selskapet inn samtykker fra kunder gjennom nettbank eller Selskapets egne, digital kundeløsninger. Samtykkene som innhentes elektronisk av banker gjelder for forsikring og visa versa. Enheter og avdelinger som behandler personopplysninger basert på samtykke må sikre at behandlingen er i henhold til samtykkene.

Dybdeopplysninger og særlige kategorier av personopplysninger kan ikke deles på tvers av juridiske selskapsgrenser uten kundens samtykke.

5.2 Formålet med behandling av personopplysninger

Enhver behandling av personopplysninger skal ha et på forhånd fastsatt og skriftlig dokumentert formål. De overordnede formålene med Selskapets behandling av personopplysninger om Selskapets kunder er administrasjon og gjennomføring av forsikringsavtaler, fakturering, analyse og rapportering.

Selskapet vil også behandle personopplysninger om egne medarbeidere. Formålet med dette vil være knyttet til HR, lønnsutbetaling og rekruttering. Selskapet behandler videre personopplysninger om kunders aktivitet på Selskapets digitale flater, som Selskapets nettsider eller på sosiale medier. Formålet med dette er optimalisering av tjenester på nett og analyse av personenes aktiviteter på Selskapets nettsider. I tillegg vil Selskapet kunne være behandlingsansvarlig for behandling av personopplysninger som skjer ved kameraovervåkning av bygninger.

Detaljert beskrivelse av Selskapets ulike behandlinger av personopplysninger fremgår av Selskapets behandlingsprotokoll.

Formålet med behandling av personopplysninger vil være sammenfallende med medarbeidernes og avdelingens normale aktiviteter. Behandling av personopplysninger som ligger utenfor det overordnede formålet vil kreve særskilte vurderinger. Personvernombudet skal i så fall konsulteres.

5.3 Innhenting av personopplysninger

Innsamling av personopplysninger kan skje både fra den personen behandlingen gjelder for eller fra andre kilder. Innsamling av personopplysninger anses som en behandling, og skal alltid ha et behandlingsgrunnlag.

Ved innsamling av helseopplysninger og andre særlige kategorier opplysninger er hovedregelen at behandlingsgrunnlaget skal være samtykke. Det skal foreligge skriftlige rutiner i de enhetene som behandler slike opplysninger. Rutinene skal følge bransjens standarder for bruk av fullmakter. Helseopplysninger kan ikke brukes til andre formål enn det som etter en forsvarlig fortolkning er hjemlet i den aktuelle samtykketekst og den situasjon og kontekst samtykket er avgitt i.

5.4 Utlevering av personopplysninger

Taushetsplikten innebærer at personopplysninger som hovedregel ikke kan utleveres til utenforstående uten samtykke fra den registrerte. Utlevering av personopplysninger kan likevel skje hvis det foreligger et behandlingsgrunnlag og et grunnlag for unntak fra eventuell taushetsplikt. Kundene skal få kortfattet og forståelig informasjon om den utlevering av personopplysninger som gjøres.

5.5 Overskuddsinformasjon

Personopplysninger Selskapet får utover det som er forespurt eller som viser seg å være nødvendig for å kunne utføre oppgaven, skal returneres til avsender eller slettes uten ugrunnet opphold. Dette kan for eksempel være legejournaler som inneholder informasjon utover det Selskapet har forespurt eller som viser seg irrelevant for aktiviteten som utføres. De avdelinger som berøres av dette skal ha rutiner for håndtering av overskuddsinformasjon.

5.6 Analyse for markedsføringsformål

Det vil ofte være nødvendig eller ønskelig å analysere kundeopplysninger fra ulike kundedatabaser for å gjøre tilpassede markedsføringstiltak eller skape økt kundeinnsikt. Hovedregelen skal alltid være at analyser primært bør gjøres med anonyme personopplysninger. Likevel fins det analyser som krever reelle personopplysninger.

Det vil ofte være ønskelig å kunne gjøre slike uttrekk på tvers av selskapsskillelinjer. Slike uttrekk skal som utgangspunkt benytte nøytrale kundeopplysninger. Sammenstilling av dybdeopplysninger på tvers av selskapsskillelinjer forutsetter at den aktuelle kunden har samtykket til deling av dybdeopplysninger. Slike uttrekk kan også skje dersom de foregår på aggregert eller på annen anonymisert måte.

Avdelingene som gjennomfører analyser skal ha rutiner for fastsettelse av formål med analysen og for kontroll av samtykker.

5.7 Kategorier av personopplysninger

Etter personopplysningsloven er personopplysninger definert som enhver opplysning og vurdering som kan knyttes til en enkeltperson. Dette gjelder uavhengig av om vedkommende er kunde, ansatt, annen interessent eller har en løsere tilknytning til Selskapet. I SpareBank 1 er personopplysninger delt inn i tre hovedkategorier: nøytrale, dybde- og særlige kategorier personopplysninger.

5.7.1 Nøytrale kundeopplysninger

Med nøytrale kundeopplysninger menes navn, fødselsnummer, adresser, fødselsdato, i hvilke av selskapene kunden har sitt avtaleforhold og hvilke produkter som er en del av kundeforholdet. Selv om fødselsnummer er en nøytral opplysning gjelder særlige regler for behandling av fødselsnummer. Spesielt skal ikke fødselsnummer sendes på ukryptert e-post.

Nøytrale kundeopplysninger kan utveksles mellom selskaper i samarbeidende gruppe, og vil kunne registreres i et sentralt kunderegister for finanskonsernet, uten at det må innhentes aktivt skriftlig samtykke fra kundene.

5.7.2 Dybdeopplysninger

Mer detaljerte opplysninger utover nøytrale kundeopplysninger, regnes som dybdeopplysninger. Opplysninger om premiestørrelser, forsikringssummer, betalingsvilje og –evne, kundekontakt, informasjonskapsler og informasjon om aktivitet på nett, samt inntekt er eksempler på dybdeopplysninger. Dybdeopplysninger kan ikke utveksles mellom selskaper i samme konsern uten samtykke den registrerte.

5.7.3 Særlige kategorier av personopplysninger

Personvernforordningen definerer særlige kategorier av personopplysninger til å omfatte:

- rasemessig eller etnisk opprinnelse,

- politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap,
- genetiske opplysninger
- biometriske opplysninger,
- helseopplysninger og
- opplysninger om en persons seksuelle forhold eller seksuelle orientering

Særlige kategorier av personopplysninger behandles i hovedsak innenfor risikovurdering, ved avdelingene som behandler erstatningskrav og hos utrederne. I tillegg behandles informasjon om medlemskap i fagforening ved tegning av pensjonsforsikringsavtaler i LOfavør-programmet. Behandling av særlige kategorier av personopplysninger skal være særlig behandlet i behandlingsrutinene i disse avdelingene. Opplysninger om straffedommer og lovovertredelser har også en særskilt beskyttelse etter personvernlovgivningen, men kan i hovedsak behandles som særlige kategorier av personopplysninger.

5.8 Behandlingsprotokoll

En oversikt over de behandlinger av personopplysninger som skjer i Selskapet, herunder formål, behandlingsaktiviteter og behandlingsgrunnlag, fremgår av Selskapets behandlingsprotokoll.

5.9 Opplæring

Operativ behandlingsansvarlig (avdelingslederne) har ansvaret for at medarbeidere som behandler personopplysninger får nødvendig opplæring i regelverket for behandling av personopplysninger. Opplæringen skal tilpasses i hvor stor grad og på hvilken måte medarbeiderne håndterer personopplysninger.

Alle ansatte skal ha grunnleggende kjennskap til personvernregelverket og taushetsplikt. Denne opplæringen ivaretas blant annet av gjennomføring av Alliansens og Selskapets e-læringsaktiviteter.

Personvernombudet kan bistå avdelingsleder i utforming og gjennomføring av opplæring av avdelingens medarbeidere.

5.10 Registrertes rettigheter

5.10.1 Innsyn

Alle kunder har rett til å få innsyn i personopplysninger om seg selv som Selskapet lagrer. Innsynsretten inkluderer eventuelle lagrede taleopptak av kundesamtaler.

Det skal foreligge rutiner for behandling av krav om innsyn i personopplysninger om seg selv.

5.10.2 Retting og sletting

Kunder kan kreve retting av personopplysninger om seg selv som de mener er uriktige. Kunden kan også kreve at personopplysningene som behandles i Selskapet suppleres av tilleggsopplysninger.

Kunden må sannsynliggjøre hvilke opplysningene er uriktige og hva som er korrekt.

Det skal foreligge rutiner for behandling av krav om retting og sletting av personopplysninger om seg selv

5.10.3 Begrenset behandling

I påvente av at Selskapet vurderer krav fra kunde om retting og sletting av personopplysninger, kan behandlingen begrenses i en periode. Det samme gjelder om kunde har protestert på selskapet behandling av vedkommendes personopplysninger.

Når behandlingen av personopplysninger er begrenset, skal Selskapet lagre opplysningene, men som hovedregel ikke bruke dem til noe uten kundens samtykke.

Det skal foreligge rutiner for behandling av krav om begrenset behandling.

5.10.4 Dataportabilitet

Kunde har rett til å få utlevert egne personopplysninger for videre og personlig bruk. Kunden har rett til å flytte, kopiere eller overføre personopplysningene sine fra en virksomhet til en annen.

Retten til dataportabilitet gjelder kun hvis opplysningene som ønskes utlevert er samlet inn på bakgrunn av kundens samtykke eller avtale.

Personopplysninger som er samlet inn fra andre eller ikke direkte fra kunde, men basert på analyser omfattes ikke av retten til dataportabilitet.

Det skal foreligge rutiner for behandling av krav om dataportabilitet.

5.11 Databehandlere

Behandling av personopplysninger kan utkontrakteres. Det vil si at Selskapet overlater til andre virksomheter (en databehandler) å utføre behandling av personopplysninger. Selskapet skal ha databehandleravtaler med alle eksterne leverandører. Databehandlere kan utføre en rekke oppgaver, som vedlikehold, drift og support av datasystemer, helsevurdering, utredning, oppgjørsfunksjoner eller lignende. Bankenes arbeid med forsikringstjenester skal også reguleres av databehandleravtaler. De operative behandlingsansvarlige er ansvarlig for å gjøre nødvendig undersøkelser og om nødvendig inngå databehandleravtaler med motpart der det kjøpes tjenester fra eksterne. Databehandleravtaler må oppdateres hvis det skjer faktiske endringer i de hovedelementer avtalen skal inneholde.

Bruk av eksterne leverandører til enkeltstående oppdrag vil normalt falle utenfor utkontrakteringsbegrepet, og det vil i slike tilfeller være tilstrekkelig å be oppdragstakeren om å signere Selskapets standard taushetserklæring.

Se for øvrig Selskapets Policy for utkontraktering, som stiller krav i forbindelse med inngåelse av utkontrakteringsavtaler.

5.11.1 Lagring/ arkivering av databehandleravtaler

Den operative behandlingsansvarlige er ansvarlig for å sørge for lagring av undertegnede databehandleravtaler i konsernets sentrale avtalearkiv som administreres av innkjøpsavdelingen. Avtaler som inneholder databehandleravtaler skal merkes med merkelapp «Databehandler innenfor EU/ EØS» eller «Databehandler utenfor EU/ EØS».

5.11.2 Bruk av taushetserklæringer

Det er utarbeidet standardiserte formularer for taushetserklæringer, som skal benyttes ved nyansettelser, herunder også ved midlertidige ansettelser. Taushetserklæringer skal også signeres av innleievikarer og av selvstendige oppdragstakere, konsulenter og lignende.

6 Beskrivelse av metodikk og prosesser

Selskapets system for internkontroll av etterlevelse av personvernregelverket består av Selskapets retningslinjer, relevante rutiner, opplæringsopplegg, samt informasjon på intranett og Confluence.

6.1 Vurdering av personvernkonsekvenser

I Selskapet gjøres det rutinemessig vurdering av personvernkonsekvenser (Data Protection Impact Assessment, DPIA). Som minimum skal det gjennomføres en vurdering av personvernkonsekvenser i forkant av etablering produkter og systemer som behandler personopplysninger på nye måter, med stor risiko eller i spesielt stort omfang.

6.2 Løpende kontroller

Det skal rutinemessig gjennomføres kontroller og revisjoner av etterlevelsen av personvernregelverket.

Operativ behandlingsansvarlig (avdelingsleder) er ansvarlig for å gjennomføre en vurdering av risiko for manglende etterlevelse av personverregelverket innenfor eget ansvarsområde. På grunnlag av vurderingen må det gjennomføres sjekker / kontroller for faktisk å vurdere etterlevelsen av regelverket. Kontrollene må også omfatte databehandlere.

Personvernombudet skal kontrollere at operativt behandlingsansvarlig gjennomfører kontroller av eget ansvarsområde.

Kontrollene kan både skje i form av egenerklæringer, som lederbekreftelsen, og stikkprøver.

Forbedringstiltak identifisert gjennom risikovurderinger, internkontrollbekreftelsen, internrevisjoner eller andre kilder skal følges opp i Selskapets oversikt for forbedringstiltak. Gjennomføringen av forbedringstiltakene skal eies av delegert behandlingsansvarlig. Oppfølging av at forbedringstiltakene virker, gjøres i forbindelse med internkontrollgjennomgangen.

6.3 Sletting av personopplysninger

Selskapet skal ikke lagre personopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. For inngåtte forsikringsavtaler skal opplysninger lagres i tråd med oppbevaringsplikten i forsikringsavtaleloven. Når opplysningene ikke lenger er nødvendig å oppbevare skal de slettes. Med sletting menes også anonymisering når anonymiseringen i tilfredsstillende grad fjerner koblingen mellom data og den registrerte.

Alle systemer som lagrer personopplysninger skal ha funksjonalitet for sletting og rutiner for å gjennomføre slettingen. Slettefunksjonaliteten må følge enkle og implementerbare kriterier og utformes slik at en ivaretar øvrige personvernrettslige krav til systemene, som integritet og kvalitet. I de tilfellene der det ikke er mulig å etablere automatiserte sletterutiner, så skal det utformes manuelle rutiner for håndtering av sletting.

6.4 Avvikshåndtering

Hendelser som innebærer brudd på rutiner knyttet til personvernregelverket skal håndteres i tråd med Selskapets avviksrutine. Ved avvik skal medarbeideren som får kjennskap til bruddet rapportere om avviket gjennom Selskapets avvikssystem. Selskapet skal legge til rette for at alle medarbeidere effektivt kan rapportere avvik.

Personvernombudet er ansvarlig for at det gjennomføres lovpålagt avviksrapportering til Datatilsynet.

Alvorlige avvik skal legges fram for styret ved compliancerapporteringen. Det er personvernombudet som avgjør hvilke saker som skal være gjenstand for en gjennomgang i ledelsen. Avviksrapporten bør omfatte årsaker til hendelser og avvik i vid forstand og hvordan hendelser og avvik er håndtert.

6.5 Informasjonssikkerhet

Behandling av personopplysninger skal skje i henhold til fastlagte retningslinjer for informasjonssikkerhet. Personopplysninger skal behandles på en måte som sikrer tilfredsstillende nivå av integritet, konfidensialitet og tilgjengelighet.

6.5.1 Risikovurderinger

Det skal gjennomføres risikovurderinger av informasjonssikkerheten i Selskapets behandling av personopplysninger for å identifisere uønskede hendelser og risikoen for at disse kan inntreffe. Før man iverksetter en behandling og før man tar i bruk et informasjonssystem, skal det alltid gjennomføres risikovurdering. Risikovurderingene gjennomføres i henhold til SpareBank 1s metodikk.

Risikovurderingen må ses i sammenheng med etablerte akseptkriterier for risiko og den behandlingsansvarlige skal iverksette nødvendige tiltak for å oppnå tilfredsstillende informasjonssikkerhet

7 Organisering, roller og ansvarsforhold

SpareBank 1 Forsikring AS er behandlingsansvarlig for personopplysningene som behandles i Selskapet. Det vil si opplysninger om kunder og personer tilknyttet kunder, samt om medarbeidere. I tillegg vil Selskapet kunne være behandlingsansvarlig for personopplysninger innhentet fra logging av nettrafikk, bruk av sosiale medier, kameraovervåkning av bygninger og andre sikkerhetstiltak. Styret har det overordnede ansvar for å sikre at Selskapet etterlever personvernforordningen og personopplysningsloven, samt andre myndighetskrav på området. Det er administrerende direktør som er øverste ansvarlig for at Selskapet ivaretar rollen som behandlingsansvarlig.

Selskapet har et personvernombud som skal bistå i arbeidet med å ivareta personvernet etter lov og forskrift. Selskapets Data Governance, personvern og informasjonssikkerhetsutvalg eies av Data Governance-ansvarlig.

Selskapets avdelingslederne vil ha rollen som operativt behandlingsansvarlige. Dette innebærer at den enkelte avdelingsleder har ansvaret for å sikre at de behandlinger av personopplysninger som skjer i egen avdeling er i tråd med Selskapets rutiner.

7.1 Styret

Styret har det overordnede ansvaret for å sikre at Selskapet etterlever personvernregelverket.

7.2 Administrerende direktør

Administrerende direktør har det overordnede ansvaret for å implementere styrets føringer og beslutninger for å sikre etterlevelse av personvernregelverket.

7.3 Operativt behandlingsansvarlig

Den operative behandlingsansvarlige er alle avdelingsledere som leder avdelinger hvor personopplysninger behandles. Operativ behandlingsansvarlig er ansvarlig for etterlevelsen av personvernregelverket innenfor sitt ansvarsområde. De er ansvarlige for at det foreligger skriftlige rutiner for all behandling av personopplysninger, og at rutinene jevnlig oppdateres. De er også ansvarlige for at det gjennomføres kontroller av at personvernregleverket etterleves.

7.4 Compliancefunksjonen

Compliancefunksjonen rapporterer eventuelle brudd på personvernregelverket i Selskapets compliancerapport og i månedlige orienteringer i Selskapets ledermøte.

7.5 Data Governance-ansvarlig

Det er fremgår av personvern- og solvensregelverket at selskapet skal benytte korrekte data i grunnlaget for sin tjenesteyting/forsikringsvirksomhet. Riktige og korrekte data gir også grunnlag for at Selskapet kan foreta viktige vurderinger og stategiske beslutninger.

Selskapet behandler data i alle systemer og i alle prosesser. Riktige data er altså et grunnvilkår for å kunne drive forsikringsvirksomhet.

I arbeidet med å styre data må selskapet ha kontroll på hvor og hvordan dataene behandles og at de behandles konsistent gjennom ulike deler av selskapets virksomhet.

Data Governanceansvarlig har ansvaret for å sikre at rammeverk for Data Governance er kjent i selskapet og at dets prinsipper benyttes. Dette gjøres gjennom samhandling med alle avdelinger i selskapet samt spesielt samarbeid med Personvernombudet og ansvarlig for informasjonssikkerhet.

7.6 Personvernombud

Personvernombudet har en rådgivende, koordinerende og kontrollerende rolle for Selskapets etterlevelse av personvernregelverket. Personvernombudets rolle og oppgaver er beskrevet i egen rollebeskrivelse. Personvernombudet vil være kontaktperson mot Datatilsynet, og har spesielt ansvar for å oversende avviksmeldinger. Personvernombudet vil også kunne bistå den registrerte ved behov.

Ved stedlig tilsyn av Datatilsynet eller Finanstilsynet (når temaet for tilsynet er behandling av personopplysninger) skal personvernombudet være tilsynets ledsager og har ansvaret for å legge til rette for at det kan gjennomføres et effektivt tilsyn.

Personvernombudet skal følge opp:

- at personvernregelverket og aktuelle bransjenormer følges i det daglige
- at det gjennomføres og oppdateres risikovurderinger av informasjonssikkerhet og vurderinger av personvernkonsekvenser (DPIA)
- at internkontrollsystemet for behandling av personopplysninger er oppdatert, dokumentert og kjent i Selskapet
- at Selskapet har rutiner som sikrer
    - at personopplysninger har et gyldig behandlingsgrunnlag og et saklig formål
    - at det er etablert tilgangsstyring til personopplysninger i tråd med fastlagte krav til tilgangsstyring
    - at personopplysninger slettes i tråd med fastlagte slettekrav

7.7 Personvernressurs og Data Governance-, personvern-, og informasjonssikkerhetsutvalget (DPIU)

Avdelinger som behandler personopplysninger i en viss grad skal ha en ressursperson som skal avlaste og bistå avdelingslederne i oppgaver knyttet til personvern. Personvernressursen skal identifisere behov for rutiner, og bistå under utarbeidelse og oppdatering av rutiner som omhandler personvern. Personvernressursene vil sammen med Data Governanceansvarlig, og Informasjonssikkerhetsansvarlig og personvernombudet utgjøre Data Governance-, personvern- og informasjonssikkerhetsutvalget (DPIU).

8 Rapportering

Avvik fra etablerte rutiner for behandling av personopplysninger skal rapporteres gjennom Selskapets system for hendelsesrapportering

9 Revidering

Personvernombudet er ansvarlig for å utarbeide og vedlikeholde dette dokumentet. Dokumentet skal behandles av Data governance-, personvern-, og informasjonssikkerhetsutvalg, men dokumentet besluttes formelt av Selskapets ledergruppe.