SpareBank 1 Forsikring AS

Retningslinjer for personvern

Vedtatt av Ledergruppen i SpareBank 1 Forsikring AS
01.06.23

1. Innhold

Revisjonshistorikk:

Versjon	Dato	Kommentar	Vedtatt av
1.0	01.06.23	Første versjon av retningslinjene.	Ledergruppen

1. Bakgrunn og formål

Selskapet skal ivareta de registrertes personvern og håndtere personopplysninger på en god og sikker måte i tråd med personvernregelverket, i både prosesser og oppgaver som selskapet utfører. Selskapets behandlinger av personopplysninger skal skje på en etisk forsvarlig måte.

Disse retningslinjene beskriver de overordnede krav og plikter som er knyttet til prinsippene for personvern.

Det nærmere innholdet i kravene og pliktene knyttet til personvern er utdypet i egne retningslinjer, se særlig Retningslinjer for etterlevelse av personvernregleverket.

SpareBank 1 Forsikring (heretter kalt selskapet) håndterer personopplysninger som en del av den daglige driften. Dette gjelder både personopplysninger på vegne av kunder og om egne medarbeidere.

Disse retningslinjene er en del av styringsdokumentene i internkontrollen til personvern.

I tillegg til de grunnleggende krav og plikter som er knyttet til prinsippene for personvern, beskriver disse retningslinjene roller og ansvar, organisering og myndighetsforhold.

2. Omfang

Arbeidet med personvern er knyttet til mange fagområder og må derfor sees i sammenheng med andre retningslinjer som gjelder for selskapet. Følgende retningslinjer er spesielt relevante:

- Etterlevelse av personvernregelverket
- Behandling av registrertes rettigheter
- Informasjonssikkerhet
- Utkontraktering
- Oppbevaring og sletting av personopplysninger
- Informasjonsklassifisering
- Tilgangshåndtering
- Håndtering av loggdata
- Risikostyring og internkontroll
- Registrering og oppfølging av hendelse (selskapets rutine)
- Utveksling av informasjon mellom SpareBank 1 Forsikring og andre finansforetak

3. Prinsipper

3.1 Innledning- oversikt regelverk

Behandlingen av personopplysninger i selskapet er regulert av personopplysningsloven og EUs personvernforordning (GDPR), men det er også en rekke andre lover og forskrifter som legger føringer for selskapets behandling av personopplysninger:

- Personopplysningsloven med EUs personvernforordning (GDPR)
- Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale
- Forskrift om kameraovervåkning i virksomhet
- Finansforetaksloven med forskrifter

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

3.2 Personvernprinsippene

For å etterleve selskapets prinsipper for personvern må alle som behandler personopplysninger i eller på vegne av selskapet, bidra til at personopplysningene behandles i tråd med de grunnleggende prinsippene for behandling av personopplysninger. Personopplysninger skal derfor:

- behandles på en lovlig, rettferdig og åpen måte
- kun samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles på en måte som er uforenelig med behandlingens formål
- være adekvate, relevante og begrenset til det som er nødvendig (dataminimering)
- være korrekte og oppdaterte
- lagres slik at det ikke er mulig å identifisere de registrerte lenger enn nødvendig
- behandles på en måte som ivaretar krav til informasjonssikkerhet

3.3 Krav til behandling av personopplysninger

Selskapet skal ha prosesser, retningslinjer og rutiner som sikrer at:

- personvernregelverket og aktuelle veiledere følges i det daglige
- internkontrollsystemet for behandling av personopplysninger er oppdatert, dokumentert og kjent i selskapet
- det gjennomføres kontroller for å overvåke den løpende håndteringen av personopplysninger og at etablerte tiltak og rutiner blir fulgt
- de registrertes rett til innsyn, sletting og retting er ivaretatt.
- det finnes en oppdatert oversikt over behandlinger av personopplysninger (behandlingsprotokoll) i rollene som behandlingsansvarlig og eventuelt databehandler hvis selskapet har slik rolle
- personopplysningssikkerheten skal være tilfredsstillende
- personvern ivaretas i utviklingsløp og systemers levetid (innebygd personvern)
- det jevnlig gjennomføres og oppdateres risikovurderinger i henhold til regelverk, samt personvernkonsekvensvurderinger (PKV/DPIA) ved behov
- det inngås databehandleravtaler med tredjeparter som behandler personopplysninger på selskapets vegne
- brudd på personopplysningssikkerheten (avvik) skal håndteres og det føres oversikt over brudd på personopplysningssikkerheten.

Hvordan selskapet skal etterleve kravene finnes blant annet i Retningslinjer for etterlevelse av personvernregelverket, samt øvrige nevnte retningslinjer under punkt 2.

4. Organisering, roller og ansvar

4.1 Behandlingsansvarlig

SpareBank 1 Forsikring er behandlingsansvarlig når selskapet bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal brukes. Personopplysningen til pensjons- og

forsikringskundene samt egne medarbeidere i SpareBank 1 Forsikring behandles i egenskap av å være behandlingsansvarlig. Dette er hovedsakelig rollen til selskapet i dag.

SpareBank 1 Forsikring er databehandler dersom det behandles personopplysninger på vegne av et annet foretak (behandlingsansvarlig).

4.2 Styret

Styret i SpareBank 1 Forsikring er behandlingsansvarlig og har det overordnede ansvaret etter personopplysningsregelverket. Styret vedtar prinsipper for personvern.

4.3 Administrerende direktør

Administrerende direktør har det overordnede ansvaret for å iverksette styrets føringer og beslutninger for å sikre etterlevelse av personvernregelverket. Administrerende direktør delegerer utførelse av oppgavene knyttet til behandlingsansvaret og eventuelt databehandlerrollen, til avdelingslederne i selskapet.

4.4 Avdelingsleder

Avdelingsledere er ansvarlig for å sikre etterlevelse av personvernregelverket innenfor sine respektive avdelingers ansvarsområder.

4.5 Informasjonssikkerhetsansvarlig

Informasjonssikkerhetsansvarlig er premissgiver for informasjonssikkerhetsarbeidet i virksomheten og ansvarlig for å sikre selskapets etterlevelse innenfor området. Personopplysningssikkerheten ivaretas som en del av informasjonssikkerheten i virksomheten.

4.6 Personvernombud

Selskapet har et personvernombud. Personvernombudet har et særlig ansvar for at de registrertes rettigheter og friheter blir ivaretatt.

Personvernombudet har en rådgivende og kontrollerende rolle i internkontrollen for personvern.

4.7 Data Governance-ansvarlig

Data Governance-ansvarlig har ansvaret for å sikre at rammeverk for Data Governance er kjent i selskapet og at dets prinsipper benyttes.

5. Rapportering

Personvernombudet rapporterer til styret på følgende måte:

- I selskapets Compliancerapport
- I årlig rapportering på personvernområdet

Brudd på retningslinjene vil innebære brudd på personopplysningsregelverket. Det kan medføre sanksjoner fra Datatilsynet.

6. Revidering

Denne retningslinjen revideres ved behov, og minimum hvert år.

7. Definisjoner

Begrep	Beskrivelse
Personopplysninger	Opplysninger om en identifisert eller identifiserbar fysisk person.
Behandling	Enhver håndtering av personopplysninger, for eksempel innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering, spredning, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.
Behandlingsansvarlig	Virksomheten som bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes
Databehandler	Virksomheten som behandler personopplysninger på vegne av den behandlingsansvarlige
Den registrerte	Personen som personopplysningene kan knyttes til.
Brudd på personopplysningssikkerheten	Brudd på konfidensialitet, integritet og tilgjengelighet for personopplysningene
Internkontroll personvern	Består i består i hovedsak av følgende tre elementer: - Styringsdokumenter, det vil si retningslinjer som gjelder for selskapet og som angir hvilke krav selskapet skal følge. - Gjennomføringsdokumenter, er den enkeltes avdeling sine rutiner. Det er rutiner for gjennomføring av kravene som følger av styringsdokumentene, basert på den enkelte avdelingens oppgaver og ansvar. - Kontrollerende aktiviteter er type aktiviteter som bidrar til å fange opp avvik eller hendelser samt gjennomføring av ulike type kontrollerende aktiviteter