Policy for behandling av personopplysninger

Revidert 04.06.2026

Gjensidige

Innhold

Policy for behandling av personopplysninger

1. Formål

Formålet med denne policyen er å fastsette detaljerte krav for behandling av personopplysninger. Policyen skal dermed bidra til å sikre etterlevelse av gjeldende personvernregler og kunder og ansattes tillit til at personopplysninger behandles i henhold til personvernregelverket

2. Virkeområde

Denne policyen gjelder for behandling av personopplysninger i Gjensidige Forsikring ASA med datterselskaper (heretter omtalt som Gjensidige).

3. Definisjoner

- «Personopplysninger» er enhver opplysning om en identifisert eller identifiserbar levende fysisk person
- «Særlige kategorier personopplysninger» (sensitive personopplysninger) er:
  - opplysninger om rasemessig eller etnisk opprinnelse,
  - politisk oppfatning, religion og filosofisk overbevisning
  - fagforeningsmedlemskap
  - behandling av genetiske opplysninger og biometriske opplysninger med det formål å identifisere en fysisk person,
  - helseopplysninger og
  - opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.
- Opplysninger om straffedommer og lovovertredelser behandles på samme måte som særlige kategorier av personopplysninger.
- «Den registrerte» er den personopplysningene er knyttet til.
- «Behandling» er enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.

4. Roller og ansvar

Konserndirektører/filialleder i Sverige

- Skal sørge for at det er etablert rutiner for å oppfylle gjeldende personvernregler.
- Skal sørge for at risikovurderinger og konsekvensanalyser (DPIA) utføres når dette er påkrevet.
- Skal sørge for at det føres oversikt over hvilke behandlinger av personopplysninger som utføres innenfor eget ansvarsområde.
- Skal sørge for at informasjonsplikten for den registrerte overholdes.

Konserndirektør People & Communication

- Skal ha et overordnet ansvar for å påse at behandling av personopplysninger om ansatte i felles prosesser, systemer og verktøy (f.eks. i samhandlingsverktøy) gjøres iht. personvernregelverket.

Personvernombud

- Skal gi råd ved vurdering av personvernkonsekvenser (DPIA), være dokumentansvarlig for rutinen for DPIA, bistå i vurderingene og kontrollere gjennomføringen av vurderingene.
- Øvrige oppgaver følger av Funksjonsbeskrivelse for andrelinje.

Ledere

- Skal være ansvarlig for at personvernregelverket etterleves innenfor sitt ansvarsområde og at medarbeidere har nødvendig kompetanse, og kjennskap til gjeldende personvernregler og hvordan personvernbrudd skal rapporteres.

Konserninnkjøp

- Skal sørge for at det etableres databehandleravtaler i anskaffelsesprosesser med tjenesteleverandører som behandler personopplysninger på vegne av Gjensidige.
- Skal etablere rutiner for kontroll av databehandlers etterlevelse av databehandleravtalen.
- Er ansvarlig for Gjensidiges mal for databehandleravtale, ansvarlig for å registrere databehandleravtalen i innkjøpssystemet og for å vurdere om bestemmelser i avtalemalen kan fravikes etter en konkret vurdering.
- Skal koordinere arbeidet med å gjennomføre og dokumentere risiko- og sikkerhetsvurderinger knyttet til anskaffelser og utkontrakteringer der det behandles personopplysninger.

Konsernsikkerhet

- Skal vurdere databehandlers sikkerhetsnivå med utgangspunkt i databehandlerens svar på sikkerhetsbilaget som del av databehandleravtalen.
- Skal kontrollere databehandlers etterlevelse av sikkerhetskrav basert på en risikobasert tilnærming.
- Sikre dokumentasjon av kontrollene og fremlegge dette ved forespørsel fra datterselskap og filialer.

IT-sikkerhet

- Skal gjennomføre IT-sikkerhetsvurderinger, som inkluderer vurdering av personvernrisiko for å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i systemer og tjenester hvor det behandles personopplysninger, herunder ved anskaffelser, utkontraktering, og utvikling.
- Skal anbefale tiltak for å redusere risiko.

Øvrige ansatte

- Skal innenfor sitt ansvarsområde bidra til overholdelse av gjeldende personvernregler, gjennomføre pålagt opplæring og melde personvernbrudd iht. gjeldende rutine.

5. Krav og metoder

5.1 Behandlingsgrunnlag

Personopplysninger skal kun behandles når det foreligger lovlig behandlingsgrunnlag. Det vanligste behandlingsgrunnlaget er at dette er nødvendig for å oppfylle en avtale med kunden eller arbeidsavtale med den ansatte. Andre relevante behandlingsgrunnlag er at behandlingen er nødvendig for at Gjensidige skal kunne ivareta sine interesser ("berettiget interesse"), at behandlingen er nødvendig for å kunne oppfylle en rettslig forpliktelse, for å oppfylle lovpålagte krav eller samtykke fra den registrerte.

For å kunne behandle sensitive personopplysninger kreves det et særskilt grunnlag i tillegg til et behandlingsgrunnlag. De mest relevante grunnlagene er samtykke, at behandlingen er nødvendig for å kunne fastsette, gjøre gjeldende eller forsvare et rettskrav, at behandlingen er nødvendig for å ivareta den registrertes vitale interesser når samtykke er umulig eller at behandlingen er nødvendig for å kunne ivareta viktige allmenne interesser.

Hvis behandling av sensitive personopplysninger er nødvendig for å inngå avtalen med den registrerte, for eksempel helseopplysninger ved kjøp av personforsikring, skal det innhentes samtykke fra den registrerte.

For å ivareta krav til dokumentasjon skal et samtykke innhentes skriftlig. Dersom dette ikke lar seg gjøre, skal muntlig samtykke registreres og som hovedregel bekreftes skriftlig til den registrerte.

Ved behandling av fødselsnummer (cpr-nummer) i den danske virksomheten kan behandling kun skje, hvis den har hjemmel i lov eller det foreligger samtykke. Utlevering av fødselsnummer i den danske virksomheten kan skje, så lenge det er et naturlig ledd i den normale driften og utlevering er av avgjørende betydning for å sikre en entydig identifisering av den registrerte eller utlevering er påkrevd av en offentlig myndighet.

5.2 Behandling av personopplysninger

Ved ny eller endret behandling av personopplysninger skal Risiko-, Compliance-, og Sikkerhetskoordinator kontaktes for dokumentasjon av behandlingsaktiviteten i relevant systemstøtte, som skal sikre etterlevelse av vesentlige krav som følger av personvernregelverket. Compliance Konsern skal etablere en rutine for hvordan behandlingsaktiviteter skal dokumenteres.

Sensitive personopplysninger, fødselsnummer og opplysninger om straffbare forhold skal være underlagt særskilt betryggende behandling, som skal konkretiseres i rutiner.

5.3 Kvalitetssikring, registrering og dataminimering
Den som behandler personopplysninger, skal påse at disse:

- er lovlig innsamlet,
- er relevant for virksomheten og begrenset til det som er nødvendig ut fra ett eller flere definerte formål,
- er korrekte og oppdaterte,
- avgrenses til det som er strengt nødvendig for å oppnå formålet.

Personopplysninger som ikke samsvarer med nevnte krav, skal ikke behandles. I tvilstilfelle skal leder konsulteres.

Alle personopplysninger skal registreres slik at:

- det ikke nedtegnes vurderinger, karakteristikker ol. av subjektiv karakter. Den registrerte skal som hovedregel kunne motta registrerte opplysninger uavkortet,
- opplysninger omfattet av innsynsrett enkelt kan fremlegges,
- opplysninger som ikke er undergitt innsynsrett, enkelt kan unntas.

Ved eventuelle rettelser av opplysninger skal dette også kommuniseres til andre som har mottatt opplysningene.

Informasjon fra sosiale medier og tips kan ikke uten videre anses som pålitelig informasjon og eventuell bruk skal vurderes og dokumenteres. Slike opplysninger skal kun samles inn dersom de møter kravene som nevnt over. Dersom kilden er anonym, må vurderingen underlegges særlig aktsomhet. Den registrerte kan ikke klassifiseres på bakgrunn av anonyme tips. Kildens eventuelle ønske om anonymitet kan ikke garanteres.

5.4 Formålsbegrensning og gjenbruk
Gjenbruk av personopplysninger til andre formål enn de ble samlet inn for, er tillatt dersom den registrerte samtykker til behandlingen eller behandlingen er nødvendig for å oppfylle en rettslig forpliktelse i nasjonal rett. I øvrige tilfeller kan personopplysninger bare benyttes for andre formål dersom det nye formålet ikke er uforenlig med det opprinnelige. Dette kan fastslåes ved bl.a. å ta hensyn til:

- Enhver forbindelse mellom opprinnelig og nytt formål
- I hvilken sammenheng opplysningene er blitt samlet inn
- Kunders og øvrige registrertes rimelige forventninger med hensyn til gjenbruk av opplysningene
- Personopplysningenes art
- Konsekvensene av tiltenkt gjenbruk for kunder og øvrige registrerte
- Nødvendige garantier, som kan omfatte kryptering eller pseudonymisering.

Ovennevnte vurdering skal dokumenteres, og Compliance Konsern skal bistå med en mal som kan benyttes for dette formålet.

5.5 Bruk av personopplysninger til testformål
Personopplysninger skal som hovedregel ikke brukes i test. Testing skal, så langt det er mulig, gjøres med fiktive eller anonymiserte data. Når dette ikke er mulig, kan det benyttes pseudonymiserte personopplysninger. Det kan kun benyttes personopplysninger i test dersom det kan dokumenteres at det er nødvendig for å oppnå formålet med testen.

Konserndirektør Teknologi og Innsikt skal implementere rutine for bruk av personopplysninger til testformål, herunder hvordan nødvendighetsvurderinger skal gjennomføres.

5.6 Innebygd personvern
Egnede tekniske og organisatoriske tiltak skal utformes med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger. Det skal tas hensyn til personvern i alle utviklingsfaser av en tjeneste, et produkt, system eller løsning, og de mest personvernvennlige innstillinger skal velges slik at de bidrar til at prinsippene for behandlingen blir etterfulgt.

Konserndirektør Teknologi og Innsikt skal implementere rutiner som sikrer at krav til innebygd personvern og personvern som standardinnstilling blir gjennomført..

5.7 Lagring
Personopplysninger skal som hovedregel registreres og lagres i fagsystemer, og skal kunne gjenfinnes ved søk på den registrerte. Dersom dette ikke er mulig, skal personopplysninger lagres på dedikerte mapper på filområdet (R:). Personopplysninger kan oppbevares i e-postsystem, så lenge de er under behandling.

Lagring av personopplysninger på Teams eller Sharepoint skal følge Gjensidiges klassifiseringsregler. Informasjon som klassifiseres «Confidential Privacy» skal ikke lagres på Teams eller Sharepoint, men i dedikert mappe på filområdet (R:).

Fysiske dokumenter skal håndteres forsvarlig og i henhold til rutiner

5.8 Utlevering
For utlevering av personopplysninger til andre selskap i konsernet kreves som hovedregel samtykke, med mindre annet fremgår av nasjonal lovgivning.

Ulike offentlige instanser kan kreve utlevering av personopplysninger. Det vises til vedlegg 1-3.

Forsikringsselskap kan utveksle personopplysninger når det foreligger konkret svikmistanke med mindre annet fremgår av nasjonal lovgivning. I dette tilfellet skal Utredning kontaktes før det utleveres personopplysninger til annet selskap.

5.9 Sletting
Personopplysninger som ikke lenger er nødvendige for å oppfylle formålet med behandlingen, skal slettes, med mindre annet følger av annen lovgivning. Sletting betyr at personopplysningene fjernes på en måte som gjør at de ikke kan gjenopprettes. Det skal etableres automatiske sletterutiner i systemer som lagrer personopplysninger. For all annen lagring skal manuelle rutiner for sletting etableres.

For kunder med avsluttet kundeforhold på grunn av svik, og med registrering om uønsket fremtidig kundeforhold, skal kundeopplysninger beholdes i den perioden kunden er uønsket med mindre annet følger av nasjonal lovgivning. Sletting utover uønsket periode følger deretter regelverk for foreldelsesfrister..

5.10 Anonymisering og pseudonymisering
Opplysninger som benyttes for analyse og statistikk skal som hovedregel anonymiseres. Anonymisering innebærer at opplysningene ikke lenger kan knyttes til enkeltpersoner. Dersom formålet ikke kan oppnås ved anonymisering, skal opplysningene pseudonymiseres. Pseudonymisering innebærer at opplysningene ikke lenger kan knyttes til enkeltpersoner uten tilleggsopplysninger som lagres atskilt fra opplysningene.

5.11 Informasjonsplikt ved innsamling og utlevering av personopplysninger
Ved innsamling av personopplysninger skal den registrerte informeres om innsamlingen og behandlingen av personopplysninger. Informasjonen skal som hovedregel gis gjennom personvernerklæringen på Gjensidiges nettsider eller i standardinformasjon som er inntatt i søknad, skademelding eller forsikringsvilkår. Informasjonen skal som utgangspunkt gis på det tidspunktet personopplysningene samles inn. Konserndirektør Privat skal sikre tilgjengeliggjøring og oppdatering av personvernerklæringen og cookie-erklæring for Gjensidige Forsikring ASA Norge og dansk filial. For svensk filial har Compliance koodinator tilsvarende ansvar.

Informasjon om at personopplysninger er samlet inn fra andre enn den registrerte skal gjøres tilgjengelig for den registrerte senest innen én måned etter at opplysningen er samlet inn. Dersom personopplysningene skal utleveres til en annen mottaker, skal den registrerte informeres senest når personopplysningene første gang utleveres.

Konserndirektør People & Communication skal sikre at informasjonsplikten knyttet til ansatte ivaretas i standardinformasjon som gis i rekrutteringsprosessen, og som vedlegg til arbeidsavtalen. Det skal tilgjengeliggjøres en personvernerklæring som beskriver Gjensidiges behandling av personopplysninger om ansatte og deres rettigheter.

Det kan unnlates å gi informasjon dersom innsamlingen eller utleveringen av opplysningene er fastsatt i lov, umulig eller uforholdsmessig vanskelig å gi, eller at den registrerte allerede kjenner til informasjonen. Det kan unnlates å gi informasjon dersom denne utelukkende er utarbeidet for intern saksforberedelse, ikke er utlevert til andre og det er nødvendig for å sikre forsvarlig intern saksbehandling.

Ved utredning kan informasjonsplikten utsettes til det ikke lenger er påkrevd med hemmelighold av hensyn til forebygging, etterforskning, avsløring og forfølging av straffbare handlinger. Det må vurderes konkret i den enkelte sak om varsling vil føre til at avklaring blir vanskeliggjort. Har politiet innledet etterforskning, må deres behov avklares innen Gjensidige varsler den registrerte. Tidspunktet for og innholdet i varslingen skal følge av interne rutiner.

Dersom personopplysninger skal brukes til andre formål enn de var innhentet for, inntrer opplysningsplikten på nytt.

5. 12 Den registrertes rettigheter
Selskapet skal legge til rette for at den registrerte kan utøve sine rettigheter, herunder retten til informasjon, innsyn, retting, sletting, begrensning, og retten til å protestere mot behandlingen.

Konserndirektør Privat, Commercial, Skade og filialleder i Sverige skal implementere rutiner for hvordan forespørsler fra den registrerte skal håndteres i de respektive områdene.

For Gjensidige Forsikring i Norge og Danmark skal Konserndirektør Privat ha ansvar for den tekniske innsynsløsningen, og for å koordinere svar på innsynsforespørsler fra de registrerte. For svensk filial har Chef Privatmarknad tilsvarende ansvar.

Konserndirektør People & Communication skal implementere rutiner for hvordan ansatte kan utøve sine rettigheter.

Enhver som lider skade som følge av en overtredelse av personvernforordningen, kan ha rett til å motta erstatning fra Gjensidige for den forvoldte skaden. Compliance Konsern skal utarbeide rutine for hvordan erstatningskrav skal håndteres.

5.13 Hendelser
Brudd på personopplysningssikkerheten er definert som sikkerhetsbrudd som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet. Internt i Gjensidige skal alle overtredelser av personvernregelverk- og rutiner registreres som personvernbrudd. Det vises til styrende dokument om registrering og rapportering av operasjonelle hendelser for nærmere fremgangsmåte for håndtering av personvernbrudd.

5. 14 Databehandleravtale
Dersom andre behandler personopplysninger på vegne av selskapet, eller selskapet behandler personopplysninger på vegne av andre, skal det i forkant inngås egen databehandleravtale (i tillegg til tjenesteutsettingsavtalen) som så langt mulig er i henhold til Gjensidiges mal for databehandleravtale. Avtaleeier er ansvarlig for at det inngås databehandleravtale.

5. 15 Risikovurdering
5.15.1 Vurdering av personopplysningssikkerheten
Som del av risikovurdering knyttet til sikkerhet, skal det gjennomføres en vurdering av personopplysningssikkerhet. IT-sikkerhet skal påse at dette gjøres i samarbeid med leder for det aktuelle området. Risikovurderingen skal ta utgangspunkt i risiko for den registrerte og identifisere potensielle hendelser som kan medføre utilsiktet eller uautorisert (ulovlig) tilgang, endring, sletting, tap eller utlevering av personopplysninger.

5.15.2 Vurdering av personvernkonsekvenser (DPIA
Dersom det er sannsynlig at en type behandling vil medføre høy risiko for den registrertes personvern, rettigheter og friheter, skal nærmeste leder sikre at det gjennomføres en DPIA konsekvensvurdering for sitt område. Compliance konsern skal utarbeide rutine for gjennomføring av DPIA.

5.15.3 Overføring utenfor EØS
Leder er ansvarlig for at det gjennomføres en risikovurdering (TIA – transfer impact assessment) ved overføring av personopplysninger utenfor EØS. Vurderingen skal gjøres i samarbeid med Konserninnkjøp som involverer personvernombud ved behov..

6. Rapportering
Konserndirektører og filialleder i Sverige skal rapportere personvernrisiko på eget område som del av årlig risikovurderingsprosess til konsernsjef.

Personvernombud skal kvartalsvis rapportere til styret og ledelsen om etterlevelse av personvernreglene gjennom Risiko- og kapitalrapporten.

Konserndirektører og filialleder i Sverige er forpliktet til å underrette relevante andre- og tredjelinjefunksjoner om forhold som er relevant for utførelsen av deres oppgaver, herunder skal avvik på bestemmelsene i dette dokumentet rapporteres i henhold til styrende dokument for registrering og rapportering av operasjonelle hendelser. Andre- og tredjelinjefunksjoner har rett til å få den informasjonen og de tilgangene som de ber om for å kunne utføre sine arbeidsoppgaver.

7. Kontroll
Konserndirektører og filialleder i Sverige skal etablere forsvarlig kontroll for å sikre etterlevelse av denne policyen som minst inneholder:
- Oppdatert behandlingsoversikt
- Manuelle sletterutiner

- Oppdatering av personvernerklæring ved ny behandling av personopplysninger
- Tilgangsstyring