POLICY FOR BEHANDLING AV PERSONOPPLYSNINGER

Opprettet dato:	*01.06.2018*
Behandlet i styret:	*18.06.2018*
Filnavn:	*NF - Policy for behandling av personopplysninger v1.1*
Version:	*1.1*

NORSK FORSIKRING AS

INNHOLDSFORTEGNELSE

1 Definisjoner

GDPR: General Data Protection Regulation – EU forordning nr. 2016/679 (generell personvernforordning).

Personopplysninger: Personopplysninger er en opplysning eller vurdering som kan knyttes til deg som enkeltperson, slik som for eksempel navn, adresse, telefonnummer, e-postadresse, IP-adresse, bilnummer, bilder, fingeravtrykk, irismønster, hodeform (for ansiktsgjenkjenning) og fødselsnummer (både fødselsdato og personnummer). Jmf. artikkel 4 i forordningen.

Sensitive personopplysninger: Sensitive personopplysninger er opplysninger om helse, tilhørighet til fagforening, rasemessig eller etnisk bakgrunn, seksuell legning, politisk, filosofisk eller religiøs oppfatning, eller at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling. Opplysninger om atferdsmønstre er også regnet som personopplysninger. Jmf. artikkel 9 i forordningen.

Den Registrerte: Den som en personopplysning kan knyttes til (forsikrede, medforsikrede, begunstiget, skadelidt, ansatt). Jmf. artikkel 4 i forordningen.

Behandlingsansvarlig: Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Jmf. artikkel 4 i forordningen.

Databehandler : Den som behandler personopplysninger på vegne av den behandlingsansvarlige. Jmf. artikkel 4 og 28 i forordningen.

Helseopplysninger: Personopplysninger om en fysisk persons fysiske eller psykiske helse, medregnet informasjon om ytelse av helsetjenester, som gir informasjon om vedkommendes helsetilstand. Jmf. artikkel 4 og 9 i forordningen.

2 Formålet med denne policy

Policy for behandling av personopplysninger er utformet etter følgende formål:

- Å sikre at personopplysninger behandles på en forsvarlig, effektiv og hensiktsmessig måte som oppfyller krav i lov og tilhørende forskrifter.
- At behandlingen av personopplysninger verner om kunder, ansatte og andre, og at disse har tillit til hvordan forvaltningen av personlig informasjon utføres.
- At behandling av personopplysninger er en del av overordnet internkontrollregime.
- At det gjennomføres tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen (jmf. artikkel 24) og personopplysningsloven.
- At behandling ses i sammenheng med styring av IT-risiko.
- At man reduserer og håndterer sentrale risikoer knyttet til personvern, slik at den Registrerte i minst mulig grad blir skadelidende hvis persondata blir gjort tilgjengelig for uvedkommende eller blir skadelidende ved at persondata er feil.

3 Prinsipper for personvern

Prinsippene for personvern finnes i veileder fra Datatilsynet (lenke)

- Behandling av sensitive personopplysninger er ikke tillatt, unntatt i de særskilte tilfellene som er beskrevet i dette dokumentet og i tråd med de aktuelle prosedyrene.
- Behandling av personopplysninger skal utføres på en lovlig, rettferdig og åpen måte. Personopplysningene skal kun innhentes for spesifiserte, eksplisitte og legitime formål.
- Personopplysninger som samles inn skal være tilstrekkelig relevante og begrenset til det som er nødvendig i forhold til formålene som dataene innhentes for.
- Personopplysninger skal være korrekte, og må oppdateres ved endring eller behov.
- Ukorrekte personopplysninger skal slettes eller korrigeres.
- Personopplysninger skal ikke oppbevares lenger enn det som er nødvendig for de formålene de er hentet inn for, og skal slettes i henhold til program for sletting.

4 Relevante lovverk og forskrifter

Følgende liste er en ikke-uttømmende oversikt over relevante lover og forskrifter:

- Ot.prop. 56 LS med artikler
- Forslag til lov om behandling av personopplysninger i samme proposisjon
- Personopplysningsloven (nåværende)
- Forsikringsavtaleloven
- Markedsføringsloven
- Arbeidsmiljøloven

5 Brudd på personopplysningssikkerheten og varsling

I tilfellet det skjer brudd på personopplysningssikkerheten skal NF uten opphold undersøke hvor stor sannsynlighet og risiko bruddet har på den Registrertes rettigheter og frihet, f.eks. tap av kontroll over egne personopplysninger eller skade på omdømme.

Dersom det er sannsynlig at bruddet medfører risiko for den Registrertes rettigheter og frihet skal bruddet uten opphold og senest innen 72 timer rapporteres til Datatilsynet.

I de tilfeller der NF ikke selv er behandlingsansvarlig, og dersom det er høy sannsynlighet for at bruddet medfører risiko for den Registrertes rettigheter og frihet skal bruddet uten opphold og senest innen avtalt frist, rapporteres til den behandlingsansvarlige om de registrerte som er involvert. Det skal informeres om strakstiltak for skadebegrensning.

Varslingen skal utføres i tråd med dokumentert prosedyre og i henhold til databehandler avtale med den behandlingsansvarlige. Det skal dokumenteres relevante beredskapsplaner for brudd på informasjonssikkerheten og personopplysningssikkerheten.

6 Ansvar og organisering av personvern

Denne policy gjelder for Norsk Forsikring AS (NF). Selskapet kan være både behandlingsansvarlig og databehandler – dette varierer avhengig av hvilke avtaleparter som er involvert. NF er ansvarlig for at behandling av personopplysninger er i tråd med lover og krav. Roller, ansvar og oppgaver ifm. personvern følger organisasjonsstrukturen.

Alle ansatte som har tilgang til og som behandler personopplysninger skal ha nødvendig kunnskap og opplæring for å kunne etterleve lover og forskrifter.

7 Styret og administrerende direktør

Styret er overordnet ansvarlig for behandlingen av personopplysninger. Administrerende direktør er fra administrasjonen ansvarlig for NFs behandling av personopplysninger.

Krav til rapportering er beskrevet under pkt 16.

8 Personvernombud

NF behandler store mengder sensitive personopplysninger, og er derfor pålagt å utpeke eget personvernombud. Ombudet har et uavhengig kontrollansvar for at lover og regler som gjelder for behandling av personopplysninger blir fulgt.

Det skal settes av tilstrekkelige ressurser for at personvernombudet kan utføre sine oppgaver. Det er utarbeidet en egen instruks for personvernombud i tråd med personopplysningsloven.

Personvernombudet skal være ansvarlig for kontakten med Datatilsynet.

9 Behandlingsansvarlig og databehandler

Norsk Forsikring AS opptrer som databehandler på vegne av de forsikringsgivere som er leverandører til de enkelte forsikringsprodukter. Forsikringsgivere og andre distributører er behandlingsansvarlig eller delbehandlingsansvarlig etter Lov om Personopplysninger.

Behandlingsansvarlig ivaretar personvernet til egne ansatte, medlemmer, de forsikrede og andre personer tilknyttet forsikringene(samlet benevnt som den "Registrerte"). Alle personopplysninger om den Registrerte vil bli behandlet i samsvar med risikovurdering og bransjestandard for informasjonssikkerhet, og i full overensstemmelse med alle gjeldende lover og regler vedrørende behandling av personopplysninger.

Det samles ikke inn personopplysninger om ut over informasjon den Registrerte frivillig gir fra seg, eller der den Registrerte gir fullmakt til NF slik at selskapet kan samle inn slik informasjon.

Samtlige personopplysninger den Registrerte gir fra seg på denne måten, vil utelukkende bli brukt av NF og deres samarbeidspartnere i samsvar med formålet med innsamlingen.

Dersom opplysninger/dokumenter som sendes til NF inneholder informasjon som er unødvendig for saksbehandlingen, skal det etter retningslinjer gitt av Datatilsynet slettes eller sendes tilbake.

Personopplysninger skal behandles på sikker måte, slik som beskrevet under pkt 21.

Når det benyttes underleverandør for databehandlingen skal databehandleravtalen beskrive behandlingsansvarliges krav, kreve samsvar med disse, kreve sikringstiltak i tråd med risikovurdering og bransjestandard, og pålegge leverandørens leverandører tilsvarende krav.

10 Innhenting av personopplysninger

Norsk Forsikring AS innhenter personopplysninger fra kunder i kraft av avgitt samtykkeerklæring og fullmakt i kjøpsportal for forsikring, og senere med hjemmel i forsikringsavtalen og vilkårenes bestemmelser, samt etter reguleringer gitt av norsk lov oppgitt under pkt.4 i dette dokumentet. Personopplysninger innhentes fra ansatte i kraft av ansettelsesavtale og samtykke, samt etter reguleringer gitt av norsk lov oppgitt under pkt.4.

Den registrerte skal informeres om hvilke opplysninger som registreres, hvem som får tilgang til dem, den registrertes rettigheter, og hvor den registrerte skal henvende seg for spørsmål om databehandlingen, innsyn, retting eller sletting. Når behandlingsgrunnlaget er samtykke skal det informeres om hvordan samtykket kan trekkes tilbake.

Personvern skal være innebygget i alle løsninger som behandler personopplysninger, og standardvalget skal alltid gi best mulig beskyttelse av den registrertes personvern.

11 Behandling av personopplysninger

Behandling av personopplysninger er regulert av Lov om behandling av personopplysninger med tilhørende forskrift. Den 1. august 2018 innføres nye og enda strengere regler for behandling av personopplysninger (GDPR: https://www.datatilsynet.no/regelverk-og-skjema/nye-personvernregler/)

De personopplysninger som innhentes dersom en kunde bestiller forsikring er nødvendige for at NF skal kunne gi tilbud, administrere forsikringer, oppfylle NFs avtaleforpliktelser og forøvrig kundenes ønsker. Opplysningene vil kunne bli benyttet for å vurdere og fatte beslutninger om forsikringers innhold og vilkårsutforming. Den Registrerte kan reservere seg mot automatisk behandling.

Anonymiserte personopplysninger kan benyttes for å utarbeide rapporter og markedsanalyser. Anonymiseringen skal foretas i tråd med dokumenterte prosedyrer.

Dersom NF har opplysningsplikt overfor offentlig myndighet gjennom lovverket, vil opplysninger bli overlevert i henhold til myndighetenes krav. NF har bl.a plikt til å gjennomføre visse kontrolltiltak regulert av Lov om tiltak mot hvitvasking og terrorfinansiering mv. (hvitvaskingsloven).

NF skal informere den Registrerte når overlevering av opplysninger kan finne sted.

Personopplysninger som NF behandler skal beskrives i en egen protokoll. Protokollen angir behandlingsgrunnlag, opplysningenes opphav, hvordan de behandles, behandling utenfor EU/EØS, grunnlaget for risikovurderingen og hvilket program for sletting som er anvendt.

Ved endringer i behandlingen av personopplysninger skal det alltid foretas en risikovurdering.

12 Helseopplysninger

For kjøp av forsikringsprodukter som bl.a dødsfallsforsikring og uføreforsikring forutsettes det i enkelte tilfeller at det gjennomføres helseprøving. For kjøp av visse personprodukter i portal kreves det at det gjennomføres en individuell elektronisk helseprøving.

Dersom den Registrerte ikke ønsker å gjennomføre elektronisk helseprøving vil den Registrerte i stedet kunne fylle ut en egenerklæring om helse på et vanlig papirskjema.

13 Lovlig behandlingsgrunnlag

Behandlingsgrunnlag er det rettslige grunnlaget som gir selskapet rett til å behandle personopplysninger. Behandling av personopplysninger skal alltid være basert på et av følgende behandlingsgrunnlag:

1. **Samtykke:** den Registrerte har gitt klart og tydelig aksept for behandling av deres personopplysninger. Det skal informeres om at samtykke fritt kan trekkes tilbake. Samtykke skal dokumenteres. Samtykket skal tilfredsstille samtlige av følgende krav:
    - **Informert**: Det vil si at det tydelig skal fremgå hva det samtykkes til
    - **Frivillig:** Det vil si at det ikke foreligger fordeler eller ulemper knyttet til samtykke
    - **Spesifikt**: Det vil si at samtykke må være konkret for behandlingen det samtykkes til
    - **Utvetydig:** Det vil si at samtykke aktivt må avgis
2. **Kontrakt:** behandlingen er nødvendig for å kunne effektuere en kontrakt med den Registrerte, eller fordi den Registrerte har bedt selskapet om å gjøre handlinger før kontrakten inngås.
2. **Juridisk krav:** behandlingen er nødvendig for å etterleve lover og reguleringer. Dette gjelder for eksempel lønnsinnberetning.
3. **Legitime interesser:** behandlingen er nødvendig for at selskapet skal kunne utøve sine legitime interesser. Legitime interesser skal i forbindelse med personvern kunne begrunnes med rettsregler. Vår interesse for behandling av personopplysninger avveies mot den Registrertes rett til personvern.
4. **Vitale interesser:** behandlingen er nødvendig for å beskytte noens liv.
5. **Offentlig oppgave:** behandlingen er nødvendig for å utføre oppgaver på vegne av offentlige interesser og dette har klar forankring i loven.

14 Innsyn og retting

I henhold til personopplysningsloven har man krav på innsyn i de opplysninger som er registrert. Den Registrerte kan benytte seg av sin rett til å få tilgang til, korrigere, komme med innvendinger mot eller slette personopplysninger ved å skrive til Norsk Forsikring AS eller direkte til forsikringsgiverne. Opplysningene skal overleveres til den Registrerte på en sikker måte.

NF skal informere om konsekvensene av forespørselen på et entydig og lettfattet språk.

Identiteten på den Registrerte skal alltid kontrolleres før forespørselen utføres. Henvendelsen må inneholde polisenummer eller personnummer, samt den Registrertes underskrift.

Dersom de registrerte opplysninger ikke er riktige eller de er ufullstendige kan man kreve disse rettet i henhold til personopplysningsloven.

Håndtering av forespørsler fra den Registrerte om informasjon, innsyn, retting og sletting av personopplysninger skal utføres i tråd med dokumenterte prosedyrer.

15 Oppbevaring og sletting

I henhold til personopplysningsloven skal opplysninger som ikke lenger er nødvendig ut fra det formål de er lagret for slettes. NF har etablert et program for sletting av personopplysninger, databehandleravtaler forplikter leverandører og underleverandører til å følge dette.

Når NF opptrer som databehandler på vegne av en behandlingsansvarlig skal lagring og sletting av personopplysninger utføres i henhold til krav i databehandleravtalen.

16 Rapportering

Forhold knyttet til personvern skal rapporteres styret i NF halvårlig. Ved mistanke om alvorlige hendelser skal styret informeres umiddelbart. Personvernombudet har selvstendig rett til å informere styret om forhold som kan påvirke personvern, internkontroll, informasjonssikkerhet.

Policy skal fremlegges for styret to ganger i året og rapport fra virksomhetens behandling av personopplysninger, avvik, internkontrollrapport.

17 Reservasjon (markedsføring)

I henhold til markedsføringsloven § 12 kan de registrerte reservere seg mot å motta markedsføring fra Norsk Forsikring As og våre samarbeidspartnere.

18 Dataportabilitet

Hvis behandlingen baserer seg på samtykke eller kontrakt, og behandlingen utføres automatisk, har den Registrerte rett til å motta opplysninger om seg selv som han eller hun selv har gitt til den behandlingsansvarlige samt å overføre disse til andre.

Opplysningene skal være i et strukturert, alminnelig anvendt og maskinlesbart format.

Den Registrerte har rett til å få overført personopplysningene direkte fra en behandlingsansvarlig til en annen i den utstrekning det er teknisk mulig. Databehandleravtalen bør bestemme vilkårene og prosedyrene for overføring av personopplysninger.

19 Elektronisk kommunikasjon

Det må innhentes samtykke til elektronisk kommunikasjon fra kunder, og disse må lagres på en hensiktsmessig måte. Kunder har rett til å reservere seg mot elektronisk kommunikasjon, herunder å avlevere helseopplysninger og andre sensitive personopplysninger.

20 Sletting av personopplysninger – «retten til å bli glemt»

Den registrerte har «rett til å bli glemt».

Sletting skal skje når:

- opplysningene ikke lenger er nødvendig for å oppnå formålet med behandlingen
- samtykket til behandlingen er trukket tilbake og det ikke finnes et annet rettslig grunnlag for behandlingen
- den registrerte har fremsatt en berettiget innsigelse, for eksempel at vedkommende ikke ønsker direkte markedsføring
- personopplysninger er blitt behandlet på en måte som ikke er lovlig

Sletteplikten gjelder ikke dersom videre behandling er nødvendig for:

- at den behandlingsansvarlige skal oppfylle en rettslig forpliktelse

Dersom den registrerte har, eller har hatt, forsikringsdekning må den registrerte skriftlig bekrefte at alle fremtidige krav under denne dekningen frafalles.

21 Datasikkerhet

Data avgitt til NFs fagsystem skal overføres, lagres og behandles på en sikker måte. Sikringstiltakene skal ta utgangspunkt i bransjestandard, kundekrav og risikovurderinger.

Beskyttelse av personvern og informasjonssikkerheten er underlagt NFs retningslinjer for internkontroll. Viktige internkontrollaktiviteter er angitt på virksomhetens årshjul.

NFs retningslinjer for informasjonssikkerhet bestemmer rammene for sikringstiltak.

Overordnet plan for IT-beredskap og mål for informasjonssikkerhet er angitt i NFs IT-strategi.

Sensitive personopplysninger om skadesaker og helseopplysninger skal krypteres, tilgangen til sensitive personopplysninger skal være svært begrenset og kun for medarbeidere med eksplisitt fullmakt. Tilganger til sensitive personopplysninger skal loggføres.