Retningslinjer vedrørende personvern for tillitsvalgte i STAFOs medlemsorganisasjoner

Hva er GDPR?

GDPR - Forkortelsen står for General Data Protection Regulation, og er ny lovgivning om personvern fra EU.

Gjennom Norges EØS-avtale er vi forpliktet til å følge det nye personvernregelverket til EU som trådte i kraft 20. juli 2018 i Norge. Den nye norske personopplysningsloven er tilpasset dette og erstatter personopplysningsloven som vi har hatt siden 2001.

Hva betyr GDPR for deg som tillitsvalgt?

EUs nye regler om personvern, kalt GDPR, innebærer en ny personopplysningslov i Norge. Dette betyr på endringer i kravene til hvordan vi håndterer personopplysninger.

Gjennom vår **personvernerklæring til våre medlemmer** har vi beskrevet hva og hvordan vi behandler deres personopplysninger. Du som tillitsvalgt er en viktig ressurs ovenfor våre medlemmer for å oppfylle de nye kravene i GDPR og vår personvernerklæringen.

Denne beskrivelsen av retningslinjene vedrørende personvern for tillitsvalgte i STAFOs medlemsorganisasjoner, skal bidra til å sikre at STAFO og medlemsorganisasjonene overholder den nye loven om personopplysninger, og sikre god og relevant kommunikasjon med våre medlemmer.

STAFO og du som tillitsvalgt kan ikke samle inn og bruke flere personopplysninger enn det som er nødvendig for det enkelte formål.

For å sikre at du ikke samler inn eller oppbevarer mer informasjon enn du har saklig behov for, kan du stille følgende kontrollspørsmål når du ser behov for å samle inn personopplysninger.

Hva er formålet med opplysningene?

Hvilke personopplysninger trenger jeg til det konkrete formålet?

Hvorfor trenger jeg disse personopplysningene til dette konkrete formålet?

Viktig å være kritisk til hva du trenger av informasjon når du svarer på spørsmålene, da du kun skal ha det minimum av personopplysninger som er nødvendig for å ivareta **medlemmets** interesse eller besvare en forespørsel i den konkrete saken.

PROSEDYRER OG RUTINER FOR TILLITSVALGTES HÅNDTERING AV PERSONOPPLYSNINGER

1. Formål

Personopplysningsloven stiller krav til internkontroll i form av etablering og vedlikehold av planlagte og systematiske tiltak. Tiltakene skal oppfylle kravene i eller i henhold av personopplysningsloven. Denne instruksen regulerer hvordan tillitsvalgte håndterer og sikrer personopplysninger på STAFO og på den enkelte medlemsorganisasjons vegne, og sørger for overholdelse av personopplysningslovens bestemmelser.

Når det gjelder tillitsvalgtes håndtering av personopplysninger i forbindelse med deres rolle i utvalg som AMU og medbestemmelse i tråd med avtaleverket, samt grupper/prosjekter opprettet av arbeidsgiver, følger tillitsvalgte arbeidsgivers regler og rutiner.

2. Den behandlingsansvarlige

STAFOs servicekontor v/Forbundsstyret er ansvarlig for at behandlingen av personopplysninger foregår etter personopplysningslovens bestemmelser (behandlingsansvarlig). I saker som behandles av servicekontoret.

Medlemsorganisasjonene v/styret er ansvarlige for behandlinger av personopplysninger i saker som behandles av tillitsvalgte.

Styret plikter å sørge for at innholdet i denne rutinen gjøres kjent for tillitsvalgte. Alle tillitsvalgte plikter å sette seg inn i rutinens innhold, og oppfylle dens forpliktelser.

Dette dokumentet er grunnlag for opplæring av tillitsvalgte

3. Personvernombud

Medlemsorganisasjonene og STAFOs personvernombud er:

Are Sand
Mob: 926 12 724
E-post: are@stafo.no

Tillitsvalgte og medlemmer kan alltid henvende seg til personvernombudet med personvernrelaterte spørsmål**.**

4. Hvilke opplysninger behandles og hvorfor

Tillitsvalgte i STAFO behandler personopplysninger for å ivareta medlemmenes interesser. Tillitsvalgte behandler i denne forbindelse medlemsopplysninger, lønnsopplysninger, opplysninger knyttet til konfliktberedskap, samt opplysninger tilknyttet individuell bistand til det enkelte medlem.

Tillitsvalgte i STAFO behandler opplysninger om medlemmer med hjemmel (behandlingsgrunnlag) i personvernforordningens art 6 (1) a, b og 9 (2) d.

5. Utlevering av personopplysninger

Tillitsvalgte skal ikke utlevere medlemmenes personopplysninger til tredjeparter.

6. Oppbevaring av personopplysninger

Papirdokumenter

Alle papirdokumenter med personopplysninger oppbevares i områder med normal generell sikring som kontor eller hjem i låst skap/skuff. Ved arbeidsdagens slutt skal tillitsvalg sørge for at aktuelle dokumenter blir lagt til oppbevaring i låst skap/skuff.

Elektroniske dokumenter

Tillitsvalgt skal sikre at dokumenter som inneholder informasjon om medlemmene er lagret med tilstrekkelig beskyttelse. Dokumentene lagres på eget område som er beskyttet med normal tilgangsstyring og passord for pålogging.

Lagring av sensitiv informasjon kan gjøres på de normale lagringsområdene, når det lagres som passordbeskyttede/krypterte dokumenter, hvor passordet på dokumentet ikke er det samme som påloggingspassordet. Se eget punkt om sikring av kommunikasjon. Alternativ til krypterte eller i tillegg til kryptering, så kan 2 faktor autentisering benyttes for tilgang til områder med dokumenter som inneholder sensitive personopplysninger.

Fellesområde og fildeling

Elektroniske dokumenter den tillitsvalgte har saklig behov for tilgang til, kan lagres på eventuelt fellesområder eller det benyttes fildelingstjenester som har tilgangskontroll og lagrer dokumenter innenfor EU/EØS området i henhold til GDPR regelverket. Sensitive dokumenter passordbeskyttes/krypteres før de deles på denne type tjenester, med mindre tjenesten allerede er tilrettelagt for deling av sensitiv informasjon.

Brukerutstyret

Alt brukerutstyr som PC, Mac, PAD eller telefon skal ha automatisk tidsstyrt skjermlås som slår seg automatisk på dersom bruker glemmer å logge ut/aktivere skjermlås når han/hun forlater utstyret.

Skjermlås/avlogging skal alltid aktiveres når en forlater brukerutstyret. Brukerutstyret skal alltid oppbevares i områder med normal sikkerhet knytte til tilgangskontroll (kontor/hjemme) når det forlates.

Alt utstyr som skal ha brukerpålogging med passord, pinkode eller tofaktor autentisering.

7. E-postadresse

Tillitsvalgte kan opprette en egen e-postkonto for korrespondanse knyttet til tillitsvalgtvervet. På denne måten skilles det mellom korrespondanse knyttet til tillitsvalgvervet og virksomhetsrelatert e-post.

Ved bruk av egen e-post eller arbeidsgivers e-post løsning skal tillitsvalgte holde korrespondanse tilknyttet tillitsvalgtvervet adskilt fra øvrig virksomhetsrelatert e-postkorrespondanse. E-poster som er relatert til tillitsvervet lagres i et mappesystem som tydelig viser at innholdet er tillitsvalgtrelatert.

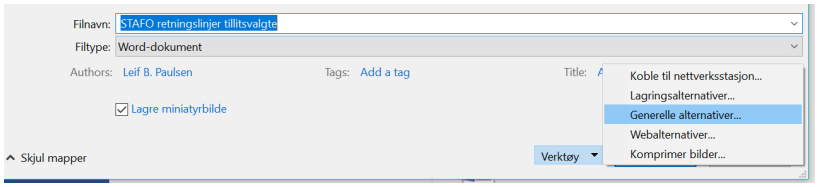
8. Sikring av kvalitet på personopplysningene

Den enkelte tillitsvalgt har ansvaret for at opplysningene er så korrekte og oppdaterte som mulig i forhold til formålet med behandlingen.

9. Sikker kommunikasjon

Dokumenter som inneholder sensitive personopplysninger, herunder medlemslister og helseopplysninger, skal ikke sendes elektronisk med mindre det er tilstrekkelig sikkerhet gjennom kryptering eller passord.

Microsoft Office 2016 og Office 365 (Word og Excel) og som er oppdatert etter april 2018 inneholder tilstrekkelig kryptering. Funksjonen finnes på lagringsmenyen til Word og Excel kan beskyttes med passordfunksjonen som sikrer kryptering av dokumentene.

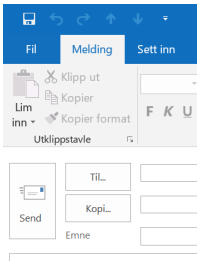


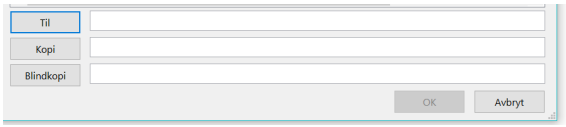
Viktig å benytte et passord som er minimum 8 karakterer og inneholder store og små bokstaver, samt tall, eller skrive passordet som en kort setning. Passord skrives inn i feltet for **åpning** av dokumentene. Mottaker må nå ha passordet for å kunne lese dokumentet.

Menyvalgene kan se litt forskjellig ut fra Word og Excel, samt justeres med oppdateringer vil kunne forekomme.

Passordet sendes da til mottaker over annen kanal, som f.eks SMS, eller gis på telefon.

Informasjon til flere medlemmer via e-post sendes ut med skjult adresseliste/Blindkopi.





Har du ikke Blindkopi feltet tilgjengelig, så får du det fram ved å trykke på til eller kopi knappen i e-post, og undermenyen med Blindkopi kommer fram. Alle mottakerne settes da i dette feltet. Sett gjerne deg selv i Til feltet, slik at dette ikke er tomt.

10. Oversendelse av personopplysninger til Sekretariatet

Den enkelte tillitsvalgt er ansvarlig for oversendelse av personopplysninger til Sekretariatet i forbindelse med overføring av sak. Sendes dokumenter med sensitive personopplysninger elektronisk, skal disse være kryptert eller passordbeskyttet, jf. pkt. 9 Eventuelle kopier, duplikater samt overskuddsmateriale slettes/makuleres umiddelbart etter oversendelsen.
Overføringen skjer etter avtale med saksbehandler i Sekretariatet, samt det enkelte medlem.

11. Skifte av tillitsvalgt

Ved skifte av tillitsvalgt skal tidligere tillitsvalgt gjennomgå lagrede personopplysninger og sletter de som ikke lenger er nødvendige, for deretter å overføre opplysningene til personen som tar over vervet.

Medlemmet informeres om overføring som krever oppfølgning av vedkommende tillitsvalgt som tar over oppfølgingen/vervet.

12. Sletting av personopplysninger

Personopplysninger skal slettes når det ikke lenger er saklig behov for å oppbevare dem.
1) Tillitsvalgte er ansvarlig for personopplysninger i forbindelse med uttrekk fra medlemsregister til f.eks. Excel, og skal sørge for at personopplysninger relatert til medlemsforholdet til enhver tid er oppdaterte og korrekte, og at opplysningene slettes ved utmelding.

2) Den enkelte tillitsvalgt er ansvarlig for personopplysninger i forbindelse med oppfølging av det enkelte medlem. Tillitsvalgt skal påse at det ikke lagres/oppbevares flere personopplysninger om medlemmet enn nødvendig for formålet. Etter avsluttet saksbehandling slettes opplysningene. Tillitsvalgte oppfordrer medlemmet til å ta vare på relevant dokumentasjon.

3) Dokumenter tilknyttet tillitsvalgtes rolle i ansettelsesutvalget slettes etter 5 år, dette for å sikre likt grunnlag og lønnsvekst.

4) Lønnslister i forbindelse med lønnsforhandlinger etter 3 år, dette for å kunne vise til historikk, sikre likt grunnlag og lønnsvekst.

13. Innsyn i behandling av personopplysninger

Når medlemmet ber om innsyn skal følgende informasjon gis:

- Formålene med behandlingen (behandlingsgrunnlag)
- Hva slags personopplysninger som behandles
- Hvor lenge personopplysningene skal lagres, hvis dette ikke er mulig skal det gis informasjon om kriteriene som brukes for å fastsette dette tidsrommet
- Om medlemmet har rett til å kreve retting, sletting eller begrensning av behandling av personopplysninger
- Om medlemmet har rett til å gjøre innsigelse mot behandlingen
- Om retten til å klage til en tilsynsmyndighet
- Dersom opplysningene ikke er samlet inn fra den medlemmet, hvor personopplysningene stammer fra

Medlemmet kan kreve at denne informasjon blir gitt skriftlig.

STAFO og medlemsorganisasjonene har felles personvernombud. Personvernombudet kan alltid kontaktes.

Innsyn og/eller utskrift av lagrede personopplysninger skal gis uten unødig opphold og senest innen 30 dager fra forespørsel er mottatt.

Tillitsvalgt kan be om skriftlig forespørsel fra medlemmet, for å kunne dokumentere svartid.

14. Avvikshåndtering

Ved mistanke om lekkasje eller lekkasje av personopplysninger, eller mistanke om andre brudd på personvernlovgivningen skal tillitsvalgte umiddelbart ta kontakt med personvernombudet i STAFO.

Personvernombudet er ansvarlig for å vurdere varsling og ev. gjennomføre varsling til Datatilsynet og de berørte medlemmene.

15. Egenkontroll

Rutiner og tiltak beskrevet i dette dokument gjennomgås årlig, i november måned, for å bekrefte at de fungerer etter hensikten. Personvernombudet, lederen i STAFO, styrene i medlemsorganisasjonene er ansvarlige for å gjennomføre egenkontrollen og dokumentere resultatet.

GDPR, Begreper og definisjoner

Personopplysning: opplysninger og vurderinger som kan knyttes til en enkeltperson – f.eks opplysninger registret om det enkelte medlemmet. Dette er typisk: Telefonnummer, personnummer, epost adresse, adresse, arbeidsted, stilling, alder, kjønn etc.

Sensitive personopplysninger: Medlemskap i fagforeninger, Rase, etnisitet, livssyn og politisk oppfatning, Informasjon om straffbare handlinger, Helseopplysninger, Seksuelle forhold. Denne listen over sensitive personopplysninger er komplett.

Behandling: enhver bruk av personopplysninger, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering.

Behandlingsansvarlig: den som bestemmer formålet med behandlingen og hvilke hjelpemidler som skal brukes.

Databehandler: den som behandler personopplysninger på vegne av den behandlingsansvarlige.

Den registrerte: den som personopplysninger kan knyttes til (f.eks det enkelte medlemmet)

Behandlingsgrunnlag: Det er 3 hovedgrunnlag for å behandle personopplysninger lovlig:

Grunnlag i lov/forskrift. F.eks. regnskap, hvitvasking, arbeidsmiljøloven
Nødvendig for å **o**ppfylle avtale med den registrerte eller ivareta berettiget interesse.
Samtykke, som må være frivillig, uttrykkelig og informert

Personvernombud: Personvernombudets hovedoppgave er å informere og gi råd om de forpliktelsene virksomheten har etter personvernlovgivningen til den behandlingsansvarlige eller databehandleren, samt til de ansatte og tillitsvalgte som utfører behandlingen av personopplysninger.