RUTINER FOR TILLITSVALGTES HÅNDTERING AV PERSONOPPLYSNINGER

1. Rutinens formål

Personopplysningsloven stiller krav til internkontroll i form av etablering og vedlikehold av planlagte og systematiske tiltak. Tiltakene skal oppfylle kravene i eller i medhold av personopplysningsloven. Denne rutinen regulerer hvordan tillitsvalgte håndterer og sikrer personopplysninger på Finansforbundets 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 SAMU, samt grupper/prosjekter opprettet av arbeidsgiver, følger tillitsvalgte arbeidsgivers regler og rutiner.

2. Den behandlingsansvarlige

Finansforbundets sekretariat v/Forbundsstyret er ansvarlig for at behandlingen av personopplysninger foregår etter personopplysningslovens bestemmelser (behandlingsansvarlig).

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

Sekretariatet har utviklet et opplæringsprogram alle tillitsvalgte plikter å gjennomføre (https://www.finansforbundet.no/tillitsvervet/personvern-gdpr/).

3. Personvernombud

Finansforbundets personvernombud er:

Advokat Ida Flaatten
Mobil 40855501
ida.flaatten@finansforbundet.no

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

4. Hvilke opplysninger behandles og hvorfor

Tillitsvalgte i Finansforbundet 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 Finansforbundet behandler opplysninger om medlemmer med hjemmel (behandlingsgrunnlag) i personvernforordningens art 6 (1) 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 låst skap. Ved arbeidsdagens slutt skal saksbehandler sørge for at aktuelle dokumenter blir lagt til oppbevaring i låst skap.

Elektroniske dokumenter
Tilgang til elektroniske dokumenter er rollestyrt. Det vil si at kun saksbehandler har tilgang til saksbehandlingsrelaterte personopplysninger om medlemmet. Dokumentene lagres på eget område kun saksbehandler har tilgang til.

Fellesområde
Elektroniske dokumenter alle tillitsvalgte har saklig behov for tilgang til, kan lagres på eventuelt fellesområde.

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 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. Felles postkasse

Der medlemmene sender e-post om bistand til felles postkasse, slettes e-posten umiddelbart etter overføring til saksbehandler.

9. Sikring av kvalitet av personopplysninger

Den enkelte tillitsvalgt har ansvaret for at opplysningene er så korrekte og oppdaterte som mulig i forhold til formålet med behandlingen, se for øvrig pkt. 12.

10. Sikker kommunikasjon

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

Skal du sende sensitive Word, Excel eller Powerpoint-dokumenter som vedlegg til e-post må du passordbeskytte Office-dokumentet.

Slik passordbeskytter du Office-dokumenter:

1. Klikk Fil i menyen øverst
2. Klikk «Informasjon»
3. Klikk »Beskytt dokument»
4. Klikk «Krypter med passord»
5. Passordet du lager må sendes via SMS til mottaker. Ikke send passordet i en separert mail.

Slik passordbeskytter du PDF-dokumenter:

1. For PDF-dokumenter anbefales det at du bruker et ZIP-program (WinZip, 7-Zip e.l) for å zippe dokumentet og passordbeskytte det.
2. Passordet du lager må sendes via SMS til mottaker. Ikke send passordet i en separert mail.

Informasjon til medlemmer via e-post sendes ut med skjult adresseliste. E-post skal fortrinnsvis sendes direkte fra Finansforbundets medlemsregister der hver tillitsvalgt har tilgang til sine medlemmer. Når e-post sendes fra dette systemet,blir mottakerlisten automatisk skjult. Ved bruk av vanlig e-postprogram MÅ Blindkopi-feltet brukes ved flere mottakere (ikke Til-feltet).

11. Digitale arrangementer

Medlemsarrangementer

Ved avholdelse av digitale kurs, møter og øvrige medlemsarrangementer sendes invitasjon via e-post ut med skjult adresseliste. Dersom identiteten til deltakerne blir gjort kjent for de øvrige deltakerne skal det i invitasjonen tydelig opplyses om dette:

«Vi gjør deg oppmerksom at ved påmelding til arrangementet vil din identitet bli gjort kjent for de øvrige deltakerne.»

Lenke til møtet sendes ut til alle påmeldte medlemmer i mail med skjult adresseliste, og de må selv legge møtet inn i kalenderen hvis de ønsker dette.

Tillitsvalgtarrangementer

Tillitsvalgte har et verv i virksomheten og således en synlig rolle. Invitasjon kan sendes ut med åpen adresseliste, og møtet kan legges direkte inn i kalenderen.

12. 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 og passordbeskyttet, jf. pkt. 10. Eventuelle kopier, duplikater samt overskuddsmateriale slettes/makuleres umiddelbart etter oversendelsen.

Overføringen skjer etter avtale med saksbehandler i Sekretariatet, samt det enkelte medlem. Der medlemmet sender sensitiv informasjon direkte til saksbehandler på Sekretariatet, oppfordrer tillitsvalgte medlemmet å bruke sikker kommunikasjon.

13. Skifte av tillitsvalgt

Ved skifte av tillitsvalgt gjennomgår tidligere tillitsvalgt lagrede personopplysninger og sletter de som ikke lenger er nødvendige, for deretter å overføre opplysningene til personen som tar over vervet eller den nærmere oppfølgingen.

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

14. 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 eget medlemsregister, og skal sørge for at personopplysninger relatert til medlemsforholdet til enhver tid er oppdaterte og korrekte, og at opplysningene slettes ved utmelding. Medlemsregisteret vaskes hver måned.

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) Tillitsvalgte er ansvarlig for fortløpende sletting av dokumenter med personopplysninger lagret på eventuelt fellesområde. Dokumentene slettes når det ikke lenger er saklig behov for å oppbevare dem.

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

5) Lønnslister i forbindelse med lønnsforhandlinger slettes senest etter 4 år, dette for å kunne foreta nødvendige beregninger, vise til historikk, sikre likt grunnlag og lønnsvekst, samt følge opp lokale bestemmelser om automatisk opprykk og sikringsbestemmelser.

15. Community

Community er et kommunikasjonsverktøy tilpasset våre tillitsvalgte. Community er frivillig, og alle tillitsvalgte må følge de interne retningslinjene ved bruk. Tillitsvalgte informeres om bruk og lagring av personopplysninger i forbindelse med første innlogging.

16. 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. Personvernombudet i Finansforbundet 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, for å kunne dokumentere svartid.

17. Avvikshåndtering

Ved brudd på rutinen, skal tillitsvalgte umiddelbart ta kontakt med personvernombudet i Finansforbundet som står for dialogen med Datatilsynet og de berørte medlemmene.

Personvernombudet skal melde fra til Datatilsynet, med mindre det er lite trolig at bruddet vil medføre risiko for fysiske personers rettigheter og friheter. Varsling må skje senest 72 timer etter at tillitsvalgte har fått kjennskap til bruddet. Også de berørte medlemmene skal varsles, med mindre det er truffet etterfølgende tiltak som sikrer at det er lite trolig at den høye risikoen vil oppstå.

18. Tekniske sikkerhetstiltak

Arbeidsgiver skal sørge for at IT-systemene ivaretar krav til ansvarlig sikkerhet.

Der sensitive personopplysninger sendes elektronisk, skal dette være kryptert.

Ekstern tilkobling til arbeidsplassen skjer gjennom kryptert VPN-tunnel eller liknende sikkerhetstiltak.

Mobilt utstyr med jobb-epost har automatisk tastelås etter kort tid.

19. Egenkontroll

Rutiner og tiltak beskrevet i dette dokument gjennomgås årlig, i november måned, for å bekrefte at de fungerer etter hensikten. Hovedtillitsvalgte i samarbeid med Finansforbundets personvernombud er ansvarlig for å gjennomføre egenkontrollen og dokumentere resultatet.