Mars 2019

VEILEDER FOR TILLITSVALGTES INFORMASJONSSIKKERHET

Det norske maskinistforbund (Dnmf)

1. Innledning

Målgruppen for dette dokumentet er alle tillitsvalgte i Dnmf; lokale tillitsvalgte i den enkelte virksomhet, samt medlemmer av Forbundsstyre og kontrollkomiteen. Dokumentet gjelder også overfor medlemmer av forhandlingsutvalg, samt forum og arbeidsgrupper i regi av Dnmf. Medlemmene i Dnmf skal oppleve at personopplysningene om dem behandles på en tillitvekkende og trygg måte. Også opplysninger om andre personer enn medlemmer må behandles på samme måte.

Som tillitsvalgt får du tilgang til ordinære personopplysninger og til særskilt beskyttede personopplysninger, som vi kan kalle sensitive eller fortrolige. Personopplysningsloven gjelder alle personopplysninger. Vær oppmerksom på at også ordinære personopplysninger skal behandles etter de nye og strengere GDPR-reglene. Blant de særskilt beskyttede opplysningene er opplysning om medlemskap i fagforening. Denne opplysningen har vi behov for å innhente i flere sammenhenger, og dette er tillatt. Andre særskilt beskyttede opplysninger er opplysninger om religion, rase, etnisitet o.l. (se 3. nedenfor). Disse opplysningene samler vi ikke inn, og om vi har slike opplysninger fra tidligere skal de slettes.

Det er derfor viktig at du er kjent med og oppfyller kravene som lovgivning og annet regelverk stiller.

Denne veilederen bygger også på Dnmf's personvernerklæring og beredskapsperm, og er laget spesielt for tillitsvalgte. Veilederen har som formål å gi en oppsummering slik at du som tillitsvalgt lett skal få oversikt over hvilke regler og krav som gjelder.

2. Tillitsvalgtes taushetsplikt

Alle tillitsvalgte som via sitt verv får tilgang til personopplysninger og fortrolig informasjon, har taushetsplikt om opplysningen. Taushetsplikten skal overholdes fullt ut i alle situasjoner hvor du utøver ditt verv.

3. Særskilte krav ved håndtering av særskilt beskyttede personopplysninger.

Det stilles skjerpede krav i personopplysningsloven og den tilhørende forordningen til behandling av særlig beskyttede personopplysninger. Dette er opplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger. Se Artikkel 9 i forordningen https://lovdata.no/dokument/NL/lov/2018-06-15-38/*#KAPITTEL_gdpr-9

Vær oppmerksom på at disse opplysningene bare kan innhentes eller behandles dersom den registrerte har gitt uttrykkelig samtykke til behandling av slike personopplysninger for ett eller flere spesifikke formål. Vær derfor særlig varsom med opplysninger om hvem som er fagorganisert, og husk at formålet avgrenser bruken. Dette gir bl.a. særlige krav til rask sletting av medlemsinformasjon som i medlemslister, i mailer som inneholder informasjon om dette o.l.

4. For alle personopplysninger gjelder krav til innhenting, behandling og sletting

Alle opplysninger om fysiske personer, f.eks. e-postadresser, opplysninger om bopel, lønnsnivå, relasjoner til andre personer, også opplysninger om forhold som man ikke vil anse som fortrolig, er beskyttet av lovgivningen. Kravene til behandlingen er sammenfattet i pkt. 4 nedenfor.

5. Fortrolig informasjon for øvrig

Vi må ivareta informasjon som ikke inneholder personopplysninger, men som er fortrolig av andre grunner. Det kan dreie seg om virksomhetskritisk informasjon, som forretningshemmeligheter og opplysninger om lønnsnivå i en bedrift. Våre egne opplysninger i fagbevegelsen f.eks. planer for forhandlinger, mekling og streik er også fortrolige.

6. Rutiner for tillitsvalgtes håndtering av personopplysninger og fortrolig informasjon

Kravene i personopplysningsloven og Dnmf sitt behov for å beskytte annen viktig informasjon, innebærer at du som tillitsvalgt må håndtere personopplysninger og fortrolig informasjon slik som beskrevet nedenfor.

Elektronisk lagring: - Elektronisk lagring skal kun skje dersom det er behov for det, og kun så lenge det er behov for det - Elektronisk lagring skal skje på medier som er sikret med kryptering eller passord, slik at arbeidsgiver eller andre ikke har tilgang - Medier som brukes til elektronisk lagring, bør være beskyttet mot virusangrep og såkalte ondsinnede angrep (phishing osv.) som bidrar til vilkårlige e-postutsendelser eller til at personopplysninger på annen måte kommer på avveie - All programvare som benyttes på utstyr, bør grunnet behovet for høy grad av informasjonssikkerhet være mest mulig oppdatert.

Fysisk oppbevaring: - Fysisk oppbevaring skal kun skje dersom det er behov for det, og kun så lenge det er behov for det - Fysisk oppbevaring skal finne sted i låst skap, skuff etc., slik at arbeidsgiver eller andre ikke har tilgang til informasjonen - Når behovet for oppbevaring er over, skal dokumentene makuleres og eventuelle originaldokumenter (signerte avtaler etc.) tilbakeleveres medlemmet.

Utskrifter - Utskrift av dokumenter skal kun foretas dersom det er behov for det - Utskrifter av dokumenter bør om mulig foretas på egen printer for tillitsvalgte - Skrives det ut på felles skriver på arbeidsstedet, skal utskrifter umiddelbart fjernes fra skriver og oppbevares utilgjengelig for uvedkommende - Ved bruk av felles skriver anbefales mulighet for kodet utskrift, dvs. at utskrift først skjer ved etterfølgende manuell godkjenning på skriver.

Bruk av mobiltelefon som er synkronisert med e-post - Dersom du bruker mobiltelefon i jobbsammenheng og denne er synkronisert mot samme e-postkonto som du bruker som tillitsvalgt, bør du sørge for at låsekode aktiveres automatisk på telefonen etter noen minutter

uten bruk av e-post - Bruk av e-post er ansett som risikofylt grunnet personvernhensyn ved oversendelse av informasjon med krav om vern. Bruk av e-post bør i denne sammenhengen derfor minimeres i størst mulig grad og stor varsomhet må utvises - Bruk av e-post i tillitsvalgtarbeidet bør om mulig skje fra en separat e-postkonto eller privatkonto i stedet for fra jobbkonto på arbeidsgivers nettverk. Vi anbefaler at det legges inn en standardtekst i den signatur du benytter i tillitsvalgtarbeidet, som ber mottaker av feiladressert e-post melde fra og slette e-posten og avholde seg fra å lese eller videresende e-posten. Dnmf har en standardformulering som anbefales brukt.

7. Avviksrapportering

Ifølge personopplysningsloven er vi pålagt å rapportere om hendelser som kan indikere at de lovbestemte krav til informasjonssikkerhet ikke er oppfylt. Rapporteringsplikten påhviler alle som håndterer personopplysninger eller fortrolig informasjon jf. Punkt 1.

Alle avviksmeldinger vil bli behandlet fortrolig, og melding av avvik kan skje via skjema som du kan laste ned fra Dnmf nettsider. Idet avviksmelding kan omhandle egne eller andres feil – for eksempel at en e-post er sendt til feil mottaker – understreker vi at all avviksrapportering er ønsket. Rapporteringen vil bidra til læring og til at vi klarer å opprettholde en høy grad av informasjonssikkerhet, til beste for våre medlemmer og Dnmf.

Du finner avviksskjemaet på hjemmesiden på Dnmf, under dine sider.

Avviksskjema sendes til:

Det norske maskinistforbund v/ GDPR-ansvarlig, Postboks 2000 Vika – N-0125 Oslo

Eller som e-postvedlegg til GDPR-ansvarlig i Dnmf: hmb@dnmf.no

8. Takk til deg

Takk for jobben du gjør som tillitsvalgt og for at du gjør ditt beste for å opprettholde en høy grad av informasjonssikkerhet til beste for våre medlemmer og Dnmf sitt omdømme!

Ta kontakt med sikkerhetsansvarlig hvis du har spørsmål om informasjonssikkerhet eller denne veilederen.

Den øverste ansvarlige for GDPR i Dnmf

Administrerende direktør
Hege-Merethe Bengtsson

E-post: hmb@dnmf.no
Telefon: +47 24 14 83 79
Mobil: +47 414 41 818