JAMMERBUGT KOMMUNE

HR

Tillidsrepræsentanters håndtering af personoplysninger

Som TR behandler du løbende personoplysninger[1] om medarbejdere i Jammerbugt Kommune. Personoplysningerne kan komme fra kommunen, et medlem, en kollega og/eller den faglige organisation, du repræsenterer, f.eks. ved ansættelse, årlige lønforhandlinger eller i evt. personalesager.

Da du typisk behandler personoplysninger på vegne af din faglige organisation, men på arbejdsredskaber[2] udleveret af kommune, er der udarbejdet retningslinjer herfor. Disse er udarbejdet på baggrund af Vejledning om databeskyttelse i forbindelse med ansættelsesforhold (datatilsynet.dk), afsnit 2.2 og 2.3.

Dataansvar
Du, og/eller din faglige organisation, ved, hvad formålet med behandlingen af personoplysninger er, hvorfor du/I er ansvarlige for behandlingen af personoplysninger. Kommunen er alene ansvarlig for, at opbevaring af data sker på forsvarlig vis i it-systemer, aflåste skabe mv., som du som TR har fået stillet til rådighed.

Data behandles på vegne af din faglige organisation og det er kun dig, der har adgang til disse data i kommunes it-systemer, også selvom din faglige organisation er dataansvarlig.

It-understøttelse af tillidsrepræsentantrollen
Det er som udgangspunkt din faglige organisation, der skal stille it-løsninger[3] til rådighed for dig. Det tilbydes dog sjældent, hvorfor kommune tillader, at du i dit arbejde som TR kan bruge kommunens H-drev og OneDrive samt e-mail. Du må **ikke** behandle personoplysninger i andre it-systemer, som f.eks. kommunens ESDH-system, SBSYS eller på andre drev.

H-drev og OneDrive er personlige drev, hvor kun du har adgang. Du opretter en mappe, hvor al TR-arbejde gemmes, så det tydeligt er adskilt fra kommunens data.
Du opretter, i din e-mailpostkasse, en mappe, hvor du opbevarer al e-mailkorrespondance i dit TR-arbejde.
Oplysninger om fagforeningsmæssige tilhørsforhold er følsomme personoplysninger, så husk at markere indkaldelser af ansatte som private indkaldelser, så andre ikke kan tilgå aftalerne i din kalender.
Kommunen må kun tilgå disse personoplysninger, hvis særlige it-sikkerhedsmæssige forhold kræver det.

Overholdelse af databeskyttelseslovgivningen
Du har ansvaret for at sikre, at personoplysningerne behandles i overensstemmelse med databeskyttelseslovgivningen, herunder at:

- du/I kun behandler nødvendige personoplysninger,
- behandlingen har et formål,
- oplysningspligten overholdes
- personoplysningerne ikke unødigt kan tilgås eller gøres tilgængelige for andre,
- oplysningerne slettes, når de ikke længere er nødvendige i forhold til det formål, de er indsamlet.

Vi anbefaler, at du, med din organisation, fastlægger en sletteprocedure for, hvornår du sletter de forskellige typer oplysninger. Hvis du igen får brug for data fra afsluttede sager, kan de indhentes igen hos medlemmet.

[1] Oplysninger, der kan henføres til en person, f.eks. navn, adresse mv.). Helbredsoplysninger og tilhørsforhold til en faglig organisation er følsomme personoplysninger.
[2] Computer, iPad mv.
[3] Kommunen er ansvarlig for it-løsningerne, herunder risikovurderinger af disse.

GDPR-reglerne gælder ikke kun elektroniske oplysninger, men printede oplysninger i papirformat ringbind, kartoteker mv. Husk derfor at de skal opbevares aflåst (aflåst skab eller kontor), når de ikke er i brug og at dokumenterne skal makuleres ved endelig afslutning af den konkrete sag.
Du bør kontakte din organisation for yderligere vejledning om overholdelsen af de databeskyttelsesretlige regler, herunder bl.a. regler for kommunikation med medlemmer og overholdelse af oplysningspligten.

Anmodninger fra medlemmer og sikkerhedsbrud
Du og/eller din organisation er ansvarlig for medlemsanmodninger om f.eks. sletning eller indsigt i personoplysningerne, du/I behandler. Du kan læse nærmere i Datatilsynets vejledning om registreredes rettigheder.

Ved sikkerhedsbrud hjælper kommunens sikkerhedsorganisation med at løse det tekniske på kommunens systemer, selvom bruddet berører oplysninger, som du er ansvarlig for. Du/I skal selv anmelde sikkerhedsbruddet til Datatilsynet ved anmeldelsespligtigt brud[4]. Skyldes sikkerhedsbruddet udelukkende din egen fejl, f.eks. videregivelse af personoplysninger til en forkert modtager, er du selv ansvarlig for egen håndtering af sikkerhedsbruddet, evt. med hjælp fra din faglige organisation.

[4] Læs mere om håndtering af sikkerhedsbrud på Tryk.