

Persondata-vejledning

Til Djøf Privats tillidsvalgte



Tillidsrepræsentanter og persondata	2
1. Indledning	2
2. Djøf er dataansvarlig for dig som tillidsrepræsentant	2
3. Hvornår er persondata omfattet af databeskyttelsesreglerne	2
4. Databeskyttelsesreglerne	4
4.1. Databrud	4
4.2. Behandlingsregler og lagring af data	4
4.2.1. Generelle principper for behandling af persondata.....	4
4.2.2. Hjemmel til behandling af persondata	6
4.3. Oplysningspligten	7
4.4. Indsigtsret	8
4.5. Berigtigelse og sletning af data	8
4.5.1. Berigtigelse.....	8
4.5.2. Retten til at blive glemt	8
5. Ophør af tillidsrepræsentanthvervet	8
6. Kontakt Djøf	9
Relevante links:	9

Private tillidsrepræsentanter og persondata

1. Indledning

Denne vejledning er tænkt som en hjælp og en instruks til Djøfs tillidsrepræsentanter¹ i den private sektor. Vejledningen indeholder en beskrivelse af reglerne vedrørende persondata og Djøfs forståelse af reglerne.

Den 25. maj 2018 trådte Databeskyttelsesforordningen (GDPR) og databeskyttelsesloven (DBL) i kraft. Den 30. november 2018 udsendte Datatilsynet en særlig vejledning på HR området, der også indeholder vejledning til håndteringen af de særlige udfordringer, der er på tillidsrepræsentantområdet.

I forbindelse med vejledningen har Djøf ligeledes udarbejdet en FAQ med svar på nogle af de spørgsmål, som tillidsrepræsentanter løbende stiller til Djøf og med de fortolkningsbidrag, som kommer fra Datatilsynet. Både denne vejledning og FAQ'en vil løbende blive opdateret, efterhånden som der kommer mere praksis.

Til sidst i dette dokument, kan du finde links til relevant lovgivning, Datatilsynets vejledning på HR-området og Djøfs privatlivspolitik.

2. Djøf er som udgangspunkt dataansvarlig for dig som tillidsrepræsentant

Tillidsrepræsentanten betragtes som en lokal repræsentant for Djøf på arbejdspladsen. Djøf har i forbindelse med dine kollegaers valg af dig som tillidsrepræsentant delegeret en række beføjelser til dig. Disse beføjelser følger af det bemyndigelsesbrev, du har fået tilsendt eller af overenskomsten.

Når du agerer i din funktion som tillidsrepræsentant, er du således underlagt Djøfs instruktion om, hvordan tillidsrepræsentanthvervet skal udfyldes. I relation til databeskyttelsesreglerne betyder det, at Djøf er dataansvarlig for din overholdelse af reglerne (GDPR og DBL).

Dette betyder også, at Djøf kan give dig **bindende instrukser** i forhold til din håndtering af persondata, og at du er forpligtet til at leve op til reglerne i denne vejledning.

Det er *kun* i din funktion som tillidsrepræsentant, at du er omfattet af Djøfs dataansvar og instruktionsbeføjelse. I alle andre situationer er du omfattet af din arbejdsgivers dataansvar og instruktionsbeføjelse.

Er du ikke omfattet af en overenskomst, der er indgået med en eller flere AC-organisationer, eller fremgår det ikke af klubbens vedtægter, at Djøf har en instruktionsbeføjelse over for dig som tillidsrepræsentant, er Djøf ikke dataansvarlig for dig. Det skyldes, at Djøfs dataansvar forudsætter at Djøf har instruktionsbeføjelserne over for dig. Du vil i dette tilfælde være selvstændig dataansvarlig.

3. Hvornår er persondata omfattet af databeskyttelsesreglerne

For at din håndtering af persondata er omfattet af databeskyttelsesreglerne, skal der være tale om en *behandling af personoplysninger*.

¹ Tillidsrepræsentanter skal i det følgende forstås som både tillidsrepræsentanter og tillidsrepræsentantsuppleanter.

En *behandling* er fx en indsamling, registrering, systematisering, opbevaring og videregivelse af personoplysninger. Det vil sige, at når du som tillidsrepræsentant indkalder til et klubmøde, udsender et nyhedsbrev eller udsender lønoversigter via e-mail, behandler du personoplysninger.

En *personoplysning* er en oplysning, der knytter sig til en bestemt person (personhenførbart). Oplysninger, der ikke knytter sig til en bestemt person (anonyme oplysninger), er derimod ikke omfattet af databeskyttelsesreglerne, fx generel lønstatistik.

Personoplysninger kan opdeles i *almindelige* og *følsomme* oplysninger:

- **Følsomme oplysninger:** Fagforeningsmæssige tilhørsforhold, oplysninger om helbred, seksuel orientering, racemæssig /etnisk oprindelse, politisk, filosofisk eller religiøs overbevisning samt genetiske og biometriske data. Oplistingen af følsomme oplysninger er udtømmende.
- **Almindelige oplysninger:** De oplysninger som ikke er "følsomme oplysninger", fx navn, privat adresse, privat telefonnummer, CV, uddannelse, lønforhold og billeder af medarbejdere. Du skal være opmærksom på, at der er særlige regler vedrørende strafbare forhold og CPR-numre.

Tillidsrepræsentanter må som udgangspunkt behandle de oplysninger, der er væsentlige og nødvendige for, at de kan udføre deres tillidshverv, fx opgaver der følger af overenskomsten.

Almindelige oplysninger er alle oplysninger, der ikke falder ind under kategorien følsomme oplysninger. Når du behandler almindelige oplysninger som tillidsrepræsentant, vil du typisk have hjemmel i DBL § 12 og GDPR art. 6, stk. 1, litra f. Heraf fremgår det, at behandling er lovlig, hvis behandling er nødvendig for, at Djøf eller en tredjemand kan forfølge en legitim interesse, med mindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor. Behandler du personoplysninger, som er væsentlige for dit tillidsrepræsentanthverv, vil interesseafvejningen som hovedregel falde ud til, at du er berettiget til at behandle oplysningerne.

Følsomme oplysninger kræver som hovedregel samtykke fra den registrerede for, at du kan behandle oplysningerne. Er der tale om oplysninger, som det er nødvendigt, at du behandler efter lov eller overenskomst, vil du kunne gøre dette efter reglerne i DBL § 12 og GDPR art. 9, stk. 2, litra d.

Som det fremgår ovenfor er medlemskab af en faglig organisation en følsom oplysning efter databeskyttelsesreglerne. Det betyder, at du ikke hverken *direkte* eller *indirekte* må videregive en oplysning om, at en person er medlem af Djøf eller en anden faglig organisation med mindre, personen har givet dig et klart samtykke. Dette gælder også, selvom dine kolleger taler åbent om deres medlemskab. Du skal derfor bruge **BCC-feltet**, når du udsender mails til dem, du er TR for, fx i forbindelse med indkaldelse til arrangementer, udsendelse af nyhedsbreve eller deling af lønoplysninger.

CPR-nummer er en kategori for sig, og betragtes derfor ikke som en følsom oplysning, men skal beskyttes lige så godt som følsomme oplysninger. Et CPR-nummer kan derimod betragtes som en nøgle, der kan bruges til entydigt at identificere enkeltpersoner i et it-system, hvorfor det falder inden for lovens område. Du kan som tillidsrepræsentant modtage oplysninger om en persons cpr. nummer fx i forbindelse, med at du skal være bisidder. Du kan behandle disse oplysninger, hvis det er nødvendigt for, at du kan varetage dine opgaver som tillidsrepræsentant jf. DBL § 11, stk. 2, nr. 4 jf. DBL § 7, stk. 2 og DBL § 12, stk. 1.

4. Databeskyttelsesreglerne

Der er særligt fem hovedelementer i regelkomplekset, som Djøf (og dermed du som tillidsrepræsentant) er forpligtet til at leve op til:

1. Databrud
2. Behandlingsregler og lagring af data
3. Oplysningsforpligtelsen
4. Indsigtsret
5. Berigtigelse og sletning af data

4.1. Databrud

Det følger af reglerne, at såfremt der sker et databrud / en sikkerhedshændelse, så skal den dataansvarlige vurdere, om der er pligt til at anmelde hændelsen til Datatilsynet. Anmeldelse skal ske indenfor 72 timer efter hændelsen er konstateret.

Eksempler på sikkerhedshændelser:

- Forkert behandling af persondata fx videresendelse af oplysninger til en forkert modtager
- Mistet hardware fx USB-nøgle, telefon, laptop
- Hacking fx angreb udefra med risiko for tyveri af persondata
- Phishingmail fx hvor man har åbnet en fil fra en falsk afsender, og der er risiko for tyveri af persondata

Hvis du bliver opmærksom på, at de oplysninger du behandler som *tillidsrepræsentant* kan være udsat for en sikkerhedshændelse, skal du straks tage kontakt til Djøf på e-mail: topdesk@djoef.dk. Det er derefter Djøfs opgave at vurdere, om der skal foretages anmeldelse til Datatilsynet. Du skal som tillidsrepræsentant bidrage med oplysninger om hændelsesforløbet, så Djøf får det fulde billede af forløbet.

4.2. Behandlingsregler og lagring af data

I databeskyttelsesreglerne findes der nogle generelle principper, der altid skal være overholdt, når du behandler persondata. Herudover skal der konkret være hjemmel til at behandle persondata og endelig skal data være opbevaret sikkert.

4.2.1. Generelle principper for behandling af persondata

For behandling af personoplysninger gælder der en række generelle principper som fremgår af GDPR art. 5. Disse principper skal *altid* være opfyldt, når du behandler personoplysninger. Dette gælder også, selvom den, du behandler oplysninger om (den registrerede), har givet et samtykke til behandlingen.

- Oplysningerne skal behandles lovligt (hjemmel i GDPR eller DBL), og må kun behandles i forhold til det formål, de er indsamlet til. Opstår der et nyt formål, skal det være foreneligt med det oprindelige formål.

Du kan fx lovligt indsamle lønoplysninger / få lønoplysninger fra din arbejdsgiver og dele dem med dine medlemmer, så de er godt klædt på til en kommende lønforhandling. Men du må ikke dele lønoplysningerne med et analysebureau, der interesserer sig for løndannelse og lønstatistik, da det ville være et andet formål end det, lønoplysningerne er indsamlet til.

- Oplysningerne der behandles, skal begrænses til, hvad der er nødvendigt i forhold til formålet; ”dataminimering”.

Du kan fx godt indsamle lønoplysninger med navn og anciennitet, men fremgår der oplysninger på lønoversigten, som ikke er relevante for løndannelsen, må de ikke behandles. Det betyder også, at når du skal forhandle løn for et medlem, skal du kun behandle den information, som er relevant for den konkrete lønforhandling.

Prøv at undgå at indhente eller få tilsendt oplysninger, som ikke er nødvendige for din funktion i en given sag.

- Oplysningerne skal være rigtige.

Oplysningerne skal være korrekte og ajourførte. Hvis oplysningerne er forkerte, skal de slettes eller rettes.

- Oplysningerne må ikke opbevares i længere tid end nødvendigt.

Du kan fx godt gemme den årlige lønoversigt fra HR efter den årlige lønforhandling er overstået, så længe du bruger lønoversigten i forbindelse med lønforhandlinger og rådgivning af dem, du er tillidsrepræsentant for. Lønoversigter, du ikke længere anvender, skal kasseres.

Vil du gerne opbevare oplysningerne af hensyn til vidensopsamling, efter de ikke længere er nødvendige for, at du kan varetage din funktion som tillidsrepræsentant, skal oplysningerne anonymiseres, så de ikke hverken *direkte* eller *indirekte* kan henføres til en bestemt person.

En gang om året bør du gå dit tillidsrepræsentantmateriale igennem og sikre, at det materiale du gemmer, fortsat er relevant for din funktion som tillidsrepræsentant.

Når du holder op som tillidsrepræsentant, skal du sortere i de oplysninger, du har liggende, videregive de oplysninger som er nødvendig for hvervet til den nye tillidsrepræsentant og kassere resten. Hvis der ikke kommer en ny tillidsrepræsentant, skal du kassere det materiale, du har liggende.

- Behandlingen skal foretages på en sikker og fortrolig måde.

Medlemmernes personoplysninger skal *altid* behandles fortroligt. Det betyder, at lønoplysninger, kontrakter, ansøgninger m.m. ikke må ligge frit tilgængeligt på et skrivebord eller i en mappe på netværket eller i en fysisk mappe, som andre end du som tillidsrepræsentant har adgang til. Du bør derfor få et skab, der kan låses og en del af netværket fx et lokalt drev, som kun du og teknisk support fra IT-afdelingen har adgang til. Du skal derfor huske:

1. Kun printe personoplysninger når det er nødvendigt at have dem på papir
2. Rydde op på dit fysiske og virtuelle skrivebord

3. "låse" computeren, når du forlader din plads
4. Aldrig dele dit password med andre
5. Makuler papir med personoplysninger, der ikke længere er nødvendigt og relevant at opbevare
6. Send BCC, når du sender mails til flere modtagere
7. Efterlad aldrig personoplysninger så de kan læses af uvedkommende

4.2.2. Hjemmel til behandling af persondata

For at kunne varetage dine kollegaers interesse som tillidsrepræsentant, har du brug for at kunne indsamle og behandle persondata, der er nødvendige for at udfylde dit hverv, herunder sikre at overenskomsten bliver overholdt. Grundlæggende er der hjemmel til at behandle persondata, der er *nødvendige* for, at du kan varetage dit hverv som tillidsrepræsentant. Det drejer sig fx om behandling af lønoplysninger i forbindelse med lønforhandlinger og behandling af CV m.m. i forbindelse med ansættelser. Hvis et medlem har bedt dig deltage i en tjenstlig samtale, kan du ligeledes lovligt behandle oplysninger, du har fået i den forbindelse.

Du skal dog altid overholde de "generelle principper for behandling af persondata", der er redegjort for ovenfor.

Du må *ikke* videregive informationer til andre, hvor der indgår følsomme oplysninger fx om personers fagforeningstilhørsforhold. Det betyder, at du hverken direkte eller indirekte må afsløre, om en person er medlem af Djøf eller en anden organisation. Det kan du mest praktisk håndtere ved at bruge **BBC-feltet** ved mailudsendelser.

Det at være uorganiseret er ikke en følsom oplysning, men der kan alligevel være hensyn, der gør, at heller ikke en sådan oplysning kan deles. Du anbefales derfor, heller ikke at dele denne oplysning.

4.2.2.1. Oplysninger fra og til arbejdsgiver

Arbejdsgiver har pligt til at *videregive* oplysninger til dig i alle tilfælde, hvor det er en forudsætning for, at du kan varetage dit hverv som tillidsrepræsentant, herunder de opgaver der følger af overenskomsten, fx hvor der skal vælges tillidsrepræsentant, er arbejdsgiver forpligtet til at oplyse, hvem der er ansat på overenskomsten indenfor Djøfs forhandlingsområde, så du ved, hvem der skal stemme ved valget.

Arbejdsgiver kan som udgangspunkt ikke *videregive* personoplysninger til dig vedr. ansatte, du ikke er tillidsrepræsentant for (uden for dit valgområde / funktionsområde). Dette vil som udgangspunkt kræve samtykke fra den oplysningerne vedrører (den registrerede).

Du kan *videregive* persondata til din arbejdsgiver, hvis det er relevant i forbindelse med varetagelsen af dit hverv. Fx hvis du deltager i en advarselsamtale, hvor du efter aftale med medlemmet videregiver oplysninger til arbejdsgiver, som arbejdsgiver ikke havde kendskab til.

Du kan modtage lønoplysninger, begrundelser for tillæg m.m. fra din arbejdsgiver. Tilsvarende kan din arbejdsgiver sende oplysninger i forbindelse med ansættelse af personer, fx C.V., anciennitet og lønindplacering.

4.2.2.2. Oplysninger fra og til Djøf

Du har via "[Mit Djøf](#)" adgang til relevante informationer om medlemmerne på din arbejdsplads. Ligesom du kan henvende dig til Djøf med konkrete spørgsmål for at kunne varetage dit hverv som tillidsrepræsentant. Udgangspunktet er, at udveksling af oplysninger mellem Djøf og dig som tillidsrepræsentant lovligt kan finde sted.

Søger du råd eller vejledning fra Djøf, vil du kunne videregive personoplysninger til Djøf, så du kan få et korrekt og fyldestgørende svar.

Du og Djøf behandles i denne sammenhæng som en samlet enhed, og der er derfor tale om en intern behandling. Det betyder, at de oplysninger, du i øvrigt har modtaget lovligt og kan behandle, kan du som udgangspunkt også videregive til Djøf.

4.2.1.3. Oplysninger fra og til kollegaer

Hvis du modtager oplysninger fra den person, oplysningerne vedrører, som du skal bruge i dit hverv som tillidsrepræsentant, vil du kunne behandle oplysningerne. Det kan fx være i forbindelse med, at du skal forhandle løn for vedkommende, eller skal deltage i en advarsels- eller sygesamtale med ledelsen.

Hvis du videregiver oplysninger til om en person til andre medlemmer / ikke-medlemmer på arbejdspladsen, skal du være opmærksom på, at du som udgangspunkt ikke må videregive personlige oplysninger til andre uden samtykke.

4.2.1.4. Hvor opbevarer du de oplysninger, du behandler i din egenskab af TR

Du skal opbevare de persondata, som du behandler som tillidsrepræsentant, sikkert. Det betyder, at fysiske persondata skal låses inde i et skab, elektronisk persondata skal opbevares sikkert på en server, og du skal have adgangskode på din skærm og låse skærmen, når du forlader din arbejdsplads.

Det er ikke endeligt afklaret, hvorvidt Djøf skal indgå en databehandleraftale med din arbejdsgiver, når du som tillidsrepræsentant anvender arbejdsgivers IT-system. Såfremt din arbejdsgiver kontakter dig med henblik på at udarbejde en databehandleraftale, skal du kontakte Djøf, som vil varetage kontakten til din arbejdsgiver vedrørende dette spørgsmål.

4.3. **Oplysningspligten**

Efter databeskyttelsesreglerne skal den dataansvarlige bl.a. oplyse de registrerede om, at der behandles personoplysninger om dem, samt om formålet med behandlingen, og efter hvilke regler behandlingen foretages. Dette gælder også, når du i din egenskab af tillidsrepræsentant registrerer og behandler personoplysninger for de personer, du er tillidsrepræsentant for.

Djøf har for at opfylde oplysningspligten bekræftet tillidsrepræsentantens behandling af personoplysninger. Du skal derfor jævnligt i dine mails indsætte denne tekst inkl. link til Djøfs privatlivspolitik, hvor Djøf har beskrevet de oplysninger, du behandler som tillidsrepræsentant:

"Der kan ske behandling af personoplysning i forbindelse med, at jeg som Djøfs tillidsrepræsentant udfører mit hverv. Du kan læse mere om Djøf og TR's behandling af personoplysning i Djøfs privatlivspolitik, som du finder her:

<https://www.djoef.dk/omdjoef/dj-oe-fs-privatlivspolitik.aspx>.”

4.4. Indsigtsret

Medlemmer og ikke medlemmer har ret til at se, hvilke personoplysninger du som TR har behandlet om vedkommende. Det betyder, at du skal kunne udlevere de pågældende oplysninger til den person, du behandler oplysninger om, hvis vedkommende efterspørger materialet.

Formålet med reglerne er, at alle personer, der får behandlet personoplysninger, skal kunne se, hvilke oplysninger der behandles om vedkommende, om der er tale om en lovlig behandling, samt kontrollere om oplysningerne er korrekte.

Det betyder, at du bør opbevare dine persondata på en måde, hvor du lettest muligt kan fremfinde materialet igen, og hvor du kan sikre dig, at du kan slette data.

Såfremt du modtager en anmodning, fx indsigtsanmodning fra en, du behandler oplysninger om, skal den pågældende have indsigt i de oplysninger, du behandler. Du skal sende det materiale du har liggende vedrørende den pågældende person til Djøf på mail djoef@djoef.dk. Djøf vil derefter give den registrerede indsigt på baggrund af de oplysninger, du har sendt til Djøf.

4.5. Berigtigelse og sletning af data

4.5.1. Berigtigelse

Den, du behandler persondata om som tillidsrepræsentant, har ret til at få berigtiget forkerte oplysninger. Hvis du er enig med personen i, at de persondata, du har registreret er forkerte, skal du med det samme rette oplysningerne. Er du uenig med personen i, at oplysningerne er forkerte, skal du sikre, at du ligeledes får registreret personens opfattelse af de persondata som uenigheden vedrører.

4.5.2. Retten til at blive glemt

Du skal slette persondata, når det ikke længere er nødvendigt at opbevare data i forhold til de formål, hvortil de behandles (dataminimering).

Det betyder fx, at når en evt. sag er forhandlet på plads, har medlemmet ret til at få slettet persondata, som du har fået som en del af sagsbehandlingen, med mindre du har brug for dem fortsat for at kunne varetage dine forpligtelser efter overenskomsten. Hvis du vil gemme oplysningerne yderligere tid, er det et krav, at du anonymiserer oplysningerne, så oplysningerne ikke længere kan henføres til en person.

Hvis du er i tvivl, om du er forpligtet til at slette oplysningerne, skal du kontakte Djøf.

5. Ophør af tillidsrepræsentanthvervet

Når dit tillidsrepræsentanthverv ophører, er du forpligtet til at gå de persondata, du har modtaget som tillidsrepræsentant igennem, og videreoverdrage de persondata, du vurderer fortsat er nødvendige til

varetagelse af tillidsrepræsentanthvervet til den nye tillidsrepræsentant. Eventuelle persondata du opbevarer, som ikke længere er nødvendige at opbevare, er du forpligtet til at slette.

Såfremt der ikke bliver valgt en ny tillidsrepræsentant i stedet for dig, skal du slette *alle* de persondata, du har modtaget i dit hverv som tillidsrepræsentant.

Sletning af persondata gælder alle persondata, både data der er elektronisk og på papir.

6. Kontakt Djøf

Hvis du har spørgsmål til forståelsen af denne vejledning eller i øvrigt spørgsmål til forståelsen af persondatareglerne, er du velkommen til at kontakte Djøf.

Djøf vil løbende opdatere dig i TR Nyt, på mail og på Djøfs hjemmeside om ny viden og praksis fra Datatilsynet. Djøf vil tilsvarende udarbejde en FAQ på Djøfs hjemmeside, hvor vi vil svare på centrale spørgsmål inden for persondataretten.

Relevante links:

Databeskyttelsesforordningen: <https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679&from=DA>

Databeskyttelsesloven: <https://www.retsinformation.dk/Forms/R0710.aspx?id=201319>

Vejledning om databeskyttelse i forbindelse med ansættelsesforhold: <https://www.datatilsynet.dk/media/6931/databeskyttelse-i-forbindelse-med-ansaettelsesforhold.pdf>

Du kan finde yderligere materiale om databeskyttelse på Datatilsynets hjemmeside www.datatilsynet.dk

Djøfs privatlivspolitik: <https://www.djoef.dk/omdjoef/dj-oe-fs-privatlivspolitik.aspx>