DANSK ERHVERV
Børsen
DK-1217 København K

www.danskerhverv.dk
info@danskerhverv.dk
T. +45 3374 6000

Vejledning

Virksomhedens håndtering af medarbejderoplysninger

27. juni 2018

Indhold

1. Kort om vejledningen 2
2. Databeskyttelsesreglerne 2
3. Systematik 3
3.1. Formål, personoplysninger og behandlinger 3
3.2. Grundlæggende ufravigelige principper 4
3.3. Behandling af forskellige typer personoplysninger 5
4. Rekruttering 7
4.1. Find den rette medarbejder 7
4.2. Håndtering af ansøgninger 7
4.3. Brug af google og sociale medier (Linkedin/Facebook mv.) 8
4.4. Referencer 8
4.5. Straffe- og børneattester 9
4.6. Kreditoplysninger 9
4.7. Personlighedstest 9
4.8. Helbredsoplysninger 10
5. Personaleadministration 10
5.1. Almindelige oplysninger 10
5.2. Følsomme oplysninger mv. 11
5.3. Helbredsoplysninger 11
5.4. Fagforeningsmæssige tilhørsforhold 11
5.5. Strafbare forhold 12
5.6. Personnummer (CPR-nummer) 12
6. Kontrol af medarbejdere 12
6.1. Kontrolforanstaltninger og databeskyttelse 12
6.2 Internet og e-mail 13
7. Medarbejderoplysninger på virksomhedens hjemmeside og intranet 13
8. Databeskyttelsesrådgiver 14
8.1. Krav om databeskyttelsesrådgiver for visse virksomheder 14
8.2. Opgaver, stilling og afskedigelsesbeskyttelse 15
9. Oplysningspligt og indsigtsret 15
9.1. Virksomhedens oplysningspligt 15
9.2. Medarbejderens indsigtsret 17
10. Fortegnelse vedrørende personaleadministrationen 17
11. Opbevaring af oplysninger før, under og efter ansættelsesforholdet 17
12. Datasikkerhed ved personaleadministration 18
13. Advarselsregistre 20
14. Samarbejdsudvalg 20

15. Sanktioner 20
16. Øvrige elementer 21
17. Vil I vide mere? 21

1. Kort om vejledningen

Vejledningen gennemgår de grundlæggende regler om databeskyttelse, som en virksomhed skal overholde i forbindelse med behandling af personoplysninger om medarbejderne.[1]

Reglernes anvendelsesområde og systematik gennemgås kort i afsnit 2. I de følgende afsnit er en gennemgang af en række konkrete situationer, hvor en virksomhed behandler personoplysninger om jobansøgere, medarbejdere og tidligere medarbejdere.

Vejledningen henviser løbende til en række værktøjer og skabeloner fra Dansk Erhverv, der kan hentes på www.danskerhverv.dk, bl.a.:

- *Vejledning og eksempel på politik om behandling af medarbejderes personoplysninger*
- *Vejledning og skabelon til en fortegnelse over personaleadministrationen*
- *Sikkerhedspolitik i forbindelse med personaleadministration*
- *Vejledning og skabeloner til behandling af jobansøgninger*
- *Vejledning og skabelon til håndtering af indsigtsret*
- *Samtykke til fotos på virksomhedens hjemmeside.*

Dansk Erhverv rådgiver også medlemmerne om håndtering af medarbejderoplysninger, se kontaktoplysninger i afsnit 17.

2. Databeskyttelsesreglerne

Virksomhedens behandling af oplysninger om medarbejderne reguleres af et kombineret europæisk og dansk regelsæt:

1. Den europæiske databeskyttelsesforordning.
2. Den supplerende danske databeskyttelseslov.
3. Særregler med betydning for virksomhedens behandling af medarbejderoplysninger, f.eks. lovgivningen om helbredoplysninger i ansættelsesforhold.

Justitsministeriet og Datatilsynet m.fl. har udsendt en række vejledninger om regelsættets enkelte dele i foråret 2018. En særlig "*Vejledning om ansættelsesretlige forhold*" er også planlagt, men er p.t. udskudt af Datatilsynet til efteråret 2018.

Denne vejledning er skrevet ud fra det samlede gældende regelsæt og de offentliggjorte vejledninger. Da datareglerne i stort omfang bygger på tidligere databeskyttelseslovgivning, er Datatilsynets tidligere praksis om behandling af medarbejderoplysninger også inddraget i relevant omgang.

[1] Udgangspunkt for vejledningen er det samlede regelsæt om databeskyttelse, som sætter rammerne for virksomhedens håndtering af medarbejderoplysninger fra 25. maj 2018. Det tidligere regelsæt samt overgangsregler omtales ikke.

Dansk Erhverv opdaterer denne vejledning, når "*Vejledning om ansættelsesretlige forhold*" fra Datatilsynet m.fl. er offentliggjort.

3. Systematik

3.1. Formål, personoplysninger og behandlinger

Formål

Formålet med databeskyttelsesreglerne er bl.a. at sikre fysiske personers ret til beskyttelses af personoplysninger og at fastsætte regler om fri udveksling af personoplysninger inden for EU. Reglerne er generelt formuleret og kræver derfor ofte fortolkning, når virksomheden skal anvende dem i forbindelse med personaleadministrationen.

Personoplysninger

Enhver form for information om en identificeret eller identificerbar fysisk person er en "person-oplysning" efter databeskyttelsesreglerne. Her er tale om et bredt begreb.

Eksempler

Personoplysninger kan f.eks. være en medarbejders:

- Navn
- Adresse
- Stilling
- Lønforhold
- Advarsler
- Helbredsoplysninger

Ved personaleadministration vil virksomheden således håndtere en lang række oplysninger, der er omfattet af regelsættet.

Behandling

Regelsættet omfatter to typer af behandling af oplysninger:

1. Elektronisk behandling af personoplysninger.
2. Manuel behandling af personoplysninger, når oplysningerne er eller vil komme i et register.

Når virksomheden behandler personoplysninger på andre måder, gælder regelsættet ikke.

En "*behandling*" skal forstås meget bredt og omfatter bl.a.:

- Indsamling
- Registrering
- Systematisering
- Opbevaring

- Søgning
- Videregivelse
- Sletning.

Reglerne gælder således i en lang række tilfælde, når virksomheden håndterer oplysninger om jobansøgere og medarbejdere.

Eksempler

Databeskyttelsesreglerne skal f.eks. overholdes, når virksomheden:

- Noterer medarbejderoplysninger i et tekstbehandlingsprogram på en PC.
- Sender medarbejderoplysninger i en e-mail.
- Har billeder af medarbejdere på virksomhedens intranet eller hjemmeside.
- Gemmer en medarbejders kontrakt, oplysninger om sygefravær, MUS-skemaer, advarsler mv. i et elektronisk HR-system.
- Opbevarer oplysninger om medarbejderen i elektroniske personalesager eller i et fysisk personaleregister.

3.2. Grundlæggende ufravigelige principper

Loven indeholder en række grundlæggende principper, som *altid* skal overholdes ved behandlingen af personoplysninger om en registreret person. Principperne gælder derfor også, når en virksomhed behandler oplysninger om jobansøgere, medarbejdere og tidligere medarbejdere.

Grundlæggende principper:

- **Lovlighed, rimelighed og gennemsigtighed**: Oplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede.
- **Formålsbegrænsning**: Oplysninger skal indsamles til udtrykkeligt angivne og legitime formål. De må ikke viderebehandles på en måde, der er uforenelig med disse formål. Virksomheden skal gøre sig klart, hvorfor der indsamles oplysninger om en medarbejder og have et sagligt formål med indsamlingen, f.eks. personaleadministrationen.
- **Dataminimering**: Behandlingen af personoplysninger skal begrænses til det, der er nødvendigt for at opfylde formålet.
- **Rigtighed**: Oplysningerne skal være korrekte og nødvendigt ajourførte. Urigtige oplysninger skal som udgangspunkt slettes eller berigtiges.
- **Opbevaringsbegrænsning**: Oplysningerne skal slettes eller anonymiseres, når det ikke længere er nødvendigt for virksomheden at have oplysningerne.
- **Integritet og fortrolighed:** Oplysningerne skal beskyttes mod uautoriseret eller ulovlig behandling. Det skal sikres, at oplysningerne ikke går tabt eller bliver beskadiget.

Virksomheden er ansvarlig for og skal kunne ***påvise***, at disse principper overholdes. Virksomheden skal således sikre sig, at principperne overholdes ved behandlingen af oplysninger om medarbejdere og skal samtidig kunne dokumentere dette.

3.3. Behandling af forskellige typer personoplysninger

Virksomhedens muligheder for at behandle en oplysning om en medarbejder afhænger af hvilken typer oplysning, der er tale om:

1. Almindelige oplysninger.[2] Dette er alle oplysninger, der ikke hører under følsomme oplysninger.
2. Følsomme oplysninger (særlige kategorier af oplysninger).[3]
3. Straffedomme og lovovertrædelser.[4]
4. Personnummeret (CPR-nummeret).[5]

For hver type oplysning lister regelsættet en række forskellige situationer op, hvor behandling af personoplysninger *kan* ske. En virksomhed kan kun behandle oplysninger om medarbejdere mv., når databeskyttelsesreglerne konkret giver mulighed for det (dvs. når der er en behandlingshjemmel).

Datatilsynet anvender også en særlig delmængde af almindelige "fortrolige" oplysninger, hvor særlige beskyttelsesbehov efter Datatilsynets opfattelse kan have betydning ved anvendelsen af databeskyttelsesreglerne. Kategorien nævnes ikke i databeskyttelsesreglerne, men Datatilsynet finder den i straffeloven sammenholdt med forvaltningsloven. Datatilsynets nærmere stillingtagen til betydningen heraf afventes pt.

Almindelige oplysninger

Et behandlingsgrundlag for at behandle almindelige oplysninger kan f.eks. være medarbejderens samtykke, opfyldelse af en (ansættelses)kontrakt, overholdelse af en retlig forpligtelse eller en interesseafvejning (hvis arbejdsgiveren har en berettiget interesse i at behandle personoplysninger, og hensynet til den registrerede ikke overstiger denne interesse).[6]

I et ansættelsesforhold vil virksomheden f.eks. kunne behandle almindelige oplysninger som navn, nærmeste pårørende, oplysning om uddannelse, tidligere beskæftigelse, løn, skat, sygefravær, pensionsforhold, kontooplysninger til lønudbetaling mv. Se afsnit 5 "Personaleadministration".

Følsomme oplysninger

Databeskyttelsesreglerne indeholder særlige behandlingsregler for en række særlige følsomme oplysninger:

- Race eller etnisk oprindelse
- Politisk, religiøs eller filosofisk overbevisning
- Fagforeningsmæssige tilhørsforhold

[2] Databeskyttelsesforordningens art. 6 samt databeskyttelsesloven § 6 og § 12.
[3] Databeskyttelsesforordningens art. 9 samt databeskyttelseslovens § 7 og § 12.
[4] Databeskyttelsesforordningens art. 10 samt databeskyttelseslovens § 8.
[5] Databeskyttelsesforordningens art. 87 samt databeskyttelseslovens § 11.
[6] Databeskyttelsesforordningens art. 6, stk. 1, litra a, b, c og f.

- Behandling af genetisk data
- Biometriske data med henblik på entydigt at identificere en fysisk person
- Seksuelle forhold eller seksuelle orientering
- Helbredsoplysninger.

Udgangspunktet er, at virksomheden ikke må behandle sådanne følsomme oplysninger.

Der er dog en række relevante undtagelser til forbuddet i forbindelse med virksomhedens håndtering af oplysninger om medarbejderne. Et lovligt behandlingsgrundlag kan f.eks. være medarbejderens samtykke, overholdelse af arbejdsretlige forpligtelser eller rettigheder i f.eks. en overenskomst, eller hvis behandlingen vedrører personoplysninger, som er offentliggjort af medarbejderen selv.[7]

Særligt om brug af samtykke i ansættelsesforhold
De forskellige typer af personoplysninger kan alle behandles, hvis virksomheden har fået samtykke til det fra medarbejderen.

Et samtykke skal være en frivillig, specifik, informeret og udtrykkelig viljestilkendegivelse fra medarbejderen, hvor medarbejderen ved samtykket indvilliger i, at virksomheden behandler medarbejderens personoplysninger. Samtykke kan gives ved en erklæring eller klar bekræftelse.

Det er særlige krav til, hvordan samtykket indhentes:

- Indgår et samtykke i en skriftlig erklæring med andre forhold, skal anmodningen om samtykke klart kunne skelnes fra disse andre forhold.
- En anmodning om samtykke skal ske i en lettilgængelig og letforståelig form. Sproget skal være klart og enkelt.

Overholdes kravene ikke, er samtykket ikke bindende for medarbejderen.

Virksomheden skal oplyse om, at samtykket kan trækkes tilbage. Tilbagetrækning af samtykket skal kunne ske lige så let, som samtykket er givet.

Det er virksomhedens ansvar at kunne **dokumentere**, at medarbejderen har givet samtykke.

Selvom medarbejderen har givet samtykke, skal lovens grundlæggende principper være opfyldt, jf. afsnit 3.2. Behandlingen skal f.eks. stadig være nødvendig for virksomheden, selvom virksomheden har fået et samtykke fra medarbejderen til behandlingen.

Når det skal vurderes, om samtykke er givet frit, skal der bl.a. tages størst muligt hensyn til, om opfyldelse af en kontrakt er gjort betinget af et samtykke til behandling af personoplysninger, som ikke er nødvendige for at opfylde kontrakten. Bl.a. dette har givet anledning til overvejelser om

[7] Artikel 9, stk. 2, litra a og e samt § 12, stk. 1 i databeskyttelsesloven.

anvendelse af samtykke i ansættelsesforhold. Justitsministeriet har vurderet, at behandling af oplysninger om medarbejdere i forbindelse med ansættelsesforhold, som efter tidligere praksis kræver samtykke, *også* kan behandles på dette grundlag efter de nye regler i databeskyttelsesforordningen. Det er i forlængelse heraf skrevet ind i databeskyttelsesloven, at behandlinger af personoplysninger i ansættelsesforhold kan finde sted på baggrund af den registrerede medarbejders samtykke i overensstemmelse med kravene i databeskyttelsesforordningen.

4. Rekruttering

4.1. Find den rette medarbejder

Det har stor betydning for en virksomhed at ansætte den rette kandidat, når en stilling er ledig. Virksomheden har derfor en interesse i at have det bedst mulige beslutningsgrundlag, når der skal ansættes en ny medarbejder. I rekrutteringsfasen kan der opstå en række spørgsmål om indsamling og brug af oplysninger om jobansøgere til en ledig stilling.

En virksomhed har med ledelsesretten som udgangspunkt en vid adgang til at indsamle de oplysninger, som er nødvendige, saglige og relevante for, at virksomheden kan træffe den bedst mulige beslutning om, hvem der skal ansættes. Sammen med regelsættet om databeskyttelse sætter en række love dog grænser for indsamlingen, f.eks. ligestillingsloven, forskelsbehandlingsloven og helbredsoplysningsloven.

Gode råd om Rekruttering

Dansk Erhverv har udarbejdet en særskilt publikation om rekruttering med mere generel information og gode råd om udarbejdelse af stillingsannoncer, indhentelse af referencer, informationssøgning på nettet mv. Læs mere i Dansk Erhvervs "*Gode råd om rekruttering*" på www.danskerhverv.dk.

4.2. Håndtering af ansøgninger

I en ansøgning vil virksomheden modtage en række oplysninger om ansøgeren. Det drejer sig typisk om almindelige oplysninger i form af navn, adresse, CV, uddannelse mv.

Datatilsynet har efter de tidligere persondataregler udtalt, at en virksomhed normalt må registrere de oplysninger om en ansøger, som personen selv afgiver i sin ansøgning. Det er forventningen, at denne praksis fortsat er gældende efter de nye regler. Det vil derfor normalt være relevant og sagligt at registrere og behandle de personoplysninger, som fremgår af en ansøgning og eventuelle bilag.

Datatilsynet har i en udtalelse af 30. maj 2018 oplyst, at en virksomhed må modtage jobansøgninger på e-mail, så længe ansøgningerne ikke indeholder følsomme eller fortrolige oplysninger. Oplysningerne skal behandles forsvarligt, når først de er modtaget.

Når en ansøger (opfordret eller uopfordret) søger en stilling, er virksomheden som følge af databeskyttelsesreglerne forpligtet til at give visse oplysninger til ansøgeren. Se også afsnit 9.1.

Vejledning med modtagelseskvittering og afslag ved jobansøgninger

Dansk Erhverv har udarbejdet to skabeloner, som virksomheden kan anvende i forbindelse med jobansøgninger, se www.danskerhver.dk:

- Kvittering for modtagelse af ansøgningen – med alternativer for hhv. opfordrede og uopfordrede ansøgninger
- Afslag på ansøgningen

4.3. Brug af google og sociale medier (Linkedin/Facebook mv.)

Virksomheden må behandle oplysninger om jobansøgere, hvis oplysningerne er relevante og nødvendige for den konkrete stilling. De grundlæggende principper skal således også overholdes ved indsamling af oplysninger om jobansøgere, se afsnit 3.2.

Det er Datatilsynets opfattelse, at virksomheden kan indsamle og i relevant omfang anvende både almindelige og følsomme oplysninger, som en jobansøger har offentliggjort om sig selv, f.eks. på de sociale medier. Også uden jobansøgerens samtykke. Det kan dog være vanskeligt at afgøre, om oplysninger fra internettet, herunder på sociale medier, er offentliggjort af jobansøgere selv. Er det ikke er tilfældet, skal der konkret være et andet behandlingsgrundlag for at virksomheden kan behandle oplysningerne, f.eks. interesseafvejningsreglen.

Virksomheden er forpligtet til at oplyse jobansøgeren om, at der indsamles oplysninger om vedkommende, jf. afsnit 9.1. Oplysningsforpligtelsen kan i mange tilfælde standardiseres, f.eks. ved oplysning om indsamlingen i stillingsopslaget, i en persondatapolitik eller i en bekræftelse i forbindelse med modtagelsen af ansøgningen. Se også Dansk Erhvervs "*Vejledning om modtagelseskvittering og afslag ved jobansøgninger*" under afsnit 4.2.

4.4. Referencer

Om jobansøgere

Referencer fra tidligere arbejdsgivere kan være relevante i rekrutteringsprocessen. Virksomheden bestemmelser selv, om der skal indhentes referencer om en kandidat.

Referencer vil typisk ske på baggrund af jobansøgerens samtykke. Oplysninger om faglige kvalifikationer må efter Datatilsynets praksis generelt forventes at blive videregivet i en sådan referencesituation, i modsætning til negative oplysninger af personlig karakter. Indhentelse af følsomme personoplysninger kræver efter praksis et samtykke vedrørende sådanne oplysninger.

Om en tidligere medarbejder

Virksomheden er ikke forpligtet til at afgive referencer om en tidligere medarbejder til en potentiel ny arbejdsgiver.

Datatilsynet har udtalt, at en virksomhed ikke uden samtykke kan videregive oplysninger om, at en kandidat søger nyt arbejde til den pågældende persons nuværende arbejdsgiver. Her vægter kandidatens interesse i, at den nuværende arbejdsgiver ikke bliver bekendt med jobsøgningen, tungest.

4.5. Straffe- og børneattester

Der kan hentes straffeattester efter reglerne om Det Centrale Kriminalregister. Efter gældende praksis kan en jobansøger således give samtykke til, at virksomheden indhenter en straffeattest i ansættelsessituationen. Læs mere om indhentelse af straffeattest ved samtykke via Nem-ID på Rigspolitiets hjemmeside www.politi.dk.

De grundlæggende principper for behandling af personoplysninger skal altid overholdes. Dette betyder efter Datatilsynets vurdering, at virksomheden alene må anmode om jobansøger om en straffeattest, hvis det er relevant i forhold til den konkrete stilling, og hvis det er realistisk, at jobansøgeren kan komme i betragtning til stillingen.

En "børneattest" indhentes med samtykke fra jobansøgeren ved direkte kontakt til børn under 15 år som led i den kommende ansættelse. Der gælder særlig lovgivning med krav om indhentelse af børneattester i nærmere definerede stillinger. Reglerne gennemgås ikke i dette notat, men Dansk Erhverv kan kontaktes for nærmere rådgivning om børneattester.

4.6. Kreditoplysninger

I visse situationer kan en virksomhed have et ønske om, at indhente nærmere oplysninger om en kandidats økonomiske forhold. Oplysninger om kreditværdighed indhentes almindeligvis fra et af de særlige kreditoplysningsbureauer, f.eks. RKI (Eksperian).

I rekrutteringssituationen betyder de grundlæggende principper, at det skal have betydning for den konkrete stilling, at jobansøgeren er kreditværdig. Jobbet skal således berettige til, at der indhentes kreditoplysninger om jobansøgeren.

Efter Datatilsynets praksis må der kun indhentes kreditoplysninger, hvis der er tale om ansættelse i en særligt betroet stilling, hvor det er nødvendigt at indhente oplysninger om den pågældende jobansøgers kreditværdighed. Det afgørende er den funktion, som jobbet er relateret til. Det er ikke tilstrækkeligt til at blive kvalificeret som en "særlig betroet stilling", at jobansøgeren i stillingen får adgang til kontanter, som f.eks. ansættelse som butiksassistent.

Eksempler fra Datatilsynets praksis:

Særligt betroet stilling:	**Ikke særligt betroet stilling:**
Bogholder	Flaskemedarbejder
Varehuschef	Servicemedarbejder
Butikschef	Butiks- eller salgsassistent
Souschef	Arbejde med post, journalisering, telefonomstilling mv.
Afdelingsleder	

4.7. Personlighedstest

Resultaterne af en personlighedstest vil som udgangspunkt være almindelige oplysninger. I helt særlige tilfælde kan resultaterne af en personlighedstest dog være følsomme oplysninger, f.eks. hvis resultaterne afslører helbredsoplysninger om medarbejderen.

Efter Dansk Erhvervs vurdering må det afhænge af virksomhedens driftsmæssige vurdering, om brug af en personlighedstest er nødvendig i forbindelse med besættelse af en konkret stilling. Anvendelse af personlighedstest vil da enten kunne ske med jobansøgerens samtykke, jf. artikel 6, stk. 1, litra a, eller ud fra interesseafvejningsreglen, jf. artikel 6, stk. 1, litra f.

4.8. Helbredsoplysninger

Helbredsoplysninger er følsomme oplysninger, jf. afsnit 3.3. Brug af helbredsoplysninger ved rekruttering er også reguleret i helbredsoplysningsloven. Formål med loven er at sikre, at helbredsoplysninger ikke uberettiget anvendes til at begrænse mulighederne for at opnå eller bevare ansættelse.

Som udgangspunkt må en virksomhed ikke spørge ind til en jobansøgers helbredsforhold ved ansættelsessamtalen. Virksomheden må dog bede om helbredsoplysninger med det formål at få belyst, om ansøgeren lider eller har lidt af en sygdom, når sygdommen vil have væsentlig betydning for kandidatens arbejdsdygtighed ved udførelsen af det pågældende arbejde. Ved anmodning om helbredsoplysninger skal virksomheden angive, hvilke sygdomme eller symptomer på sygdomme der ønskes oplysninger om.

En jobansøger har selv en pligt til at oplyse om helbredsforhold af væsentlig betydning for ansøgerens arbejdsdygtighed ved det pågældende arbejde.

Orientering om helbredsoplysningsloven
Læs mere om helbredsoplysningsloven og praksis i Dansk Erhvervs *"Orientering om helbredsoplysningsloven"*

5. Personaleadministration

5.1. Almindelige oplysninger

Virksomheden må behandle oplysninger om en medarbejder, hvis det f.eks. er nødvendigt for at opfylde den ansættelseskontrakt, som er indgået mellem parterne. På denne baggrund kan virksomheden i et personaleregister/personalesystem mv. opbevare en række almindelige oplysninger uden samtykke fra medarbejderen. Det kan være oplysninger fra både før og under ansættelsesforholdet.

En virksomhed vil således normalt kunne behandle en række almindelige oplysninger om medarbejderen, hvis det er nødvendigt. F.eks.:

- Stamoplysninger, f.eks. navn, adresse, personnummer, oplysninger om nærmeste familie (navn, adresse, o.l.).
- Skattemæssige oplysninger, bankoplysninger, oplysninger om pensionsforhold mv.
- Uddannelse, tidligere beskæftigelse og andre sædvanlige oplysninger i et CV, anbefalinger.
- Nuværende stilling, arbejdsopgaver, arbejdstider, tjenstlige forhold.
- Oplysninger om løn og skat.
- Sygefravær, sygdomsperioder (oplysninger om sygefravær betragtes normalt ikke i sig selv som en helbredsoplysning) og andet fravær fra arbejdet.

- Tjenstlige forseelser og advarsler, personalebedømmelser o.l.

Sådanne oplysninger kan altså normalt registreres uden samtykke fra medarbejderen, da virksomheden anvender oplysningerne som led i ansættelsesforholdet (kontrakten) med medarbejderen, jf. artikel 6, stk. 1, litra b.

En virksomhed må efter gældende praksis normalt registrere de oplysninger om en medarbejder, som medarbejderen selv har givet i sin jobansøgning.

5.2. Følsomme oplysninger mv.

I praksis må en virksomhed som hovedregel kun registrere følsomme oplysninger om en medarbejder, hvis medarbejderen har givet udtrykkeligt samtykke til det. Se eksempler på følsomme oplysninger i afsnit 3.3.

Virksomheden kan dog behandle følsomme oplysninger om en medarbejder uden samtykke, når virksomheden har mulighed for det efter et andet behandlingsgrundlag i databeskyttelsesreglerne. En række eksempler på dette er nævnt i det følgende.

5.3. Helbredsoplysninger

Helbredsoplysninger dækker over oplysninger om en persons tidligere, nuværende og fremtidige fysiske eller psykiske tilstand samt oplysninger om medicinbrug, misbrug af narkotika, alkohol og lignende. Efter praksis vil oplysninger om sygefravær som udgangspunkt ikke i sig selv være en helbredsoplysning. Se også afsnit 4.8 om helbredsoplysninger generelt.

Eksempel – helbredsoplysninger og sygedagpengerefusion En virksomhed kan registrere helbredsoplysninger i nødvendigt omfang i forbindelse med en aftale om sygedagpengerefusion fra medarbejderens første sygedag efter sygedagpengelovens § 56.

5.4. Fagforeningsmæssige tilhørsforhold

Oplysninger om fagforeningsmæssige tilhørsforhold kan bl.a. behandles, når det er nødvendigt for at overholde virksomhedens eller medarbejderens arbejdsretlige forpligtelser, eller rettigheder fastlagt efter lov eller overenskomst.[8] Derimod vil det ikke være lovligt, hvis virksomheden generelt behandler oplysninger om medarbejderens fagforeningsmæssige tilhørsforhold.

[8] Databeskyttelseslovens § 12, stk. 1.

Eksempel – medlemskab af Lederne

En virksomhed må behandle oplysninger om, at en ledende medarbejder er medlem af Lederne. Denne oplysning er nødvendig for, at virksomheden ved, om den konkrete leders ansættelsesforhold er omfattet af Lederaftalen mellem Dansk Arbejdsgiverforening og Lederne, hvilket også skal fremgå af ansættelseskontrakten.

5.5. Strafbare forhold

Se om straffe- og børneattester i afsnit 4.5.

Der kan være tilfælde, hvor en virksomhed kan registrere oplysninger om strafbare forhold uden samtykke. F.eks. kan en virksomhed efter gældende praksis registrere oplysninger om strafbare forhold uden samtykke med henblik på at bortvise medarbejderen, og hvis virksomheden vil indgive politianmeldelse og afgive vidneforklaring ved domstolene.

Eksempel - butikstyveri

En virksomhed kan registrere oplysninger om en medarbejders butikstyveri med henblik på at bortvise medarbejderen, og hvis virksomheden vil indgive politianmeldelse og eventuelt senere afgive vidneforklaring ved en retssag. Her behøver virksomheden ikke medarbejderens samtykke til behandlingen.

5.6. Personnummer (CPR-nummer)

Databeskyttelsesreglerne har særlige regler om, at behandling af personnummer kan ske, hvis det følger af lovgivningen eller den registrerede har givet sit samtykke. Private kan også behandle personnummeret, når betingelserne for behandling af følsomme oplysninger er opfyldt.[9]

Eksempel – indberetning til SKAT

En virksomhed kan registrere medarbejdernes personnumre, da det blandt andet er nødvendigt for at foretage indberetninger til SKAT.

En virksomhed må som udgangspunkt ikke videregive personnummeret til andre, med mindre særlige betingelser i loven er opfyldt.

6. Kontrol af medarbejdere

6.1. Kontrolforanstaltninger og databeskyttelse

Ud over de arbejdsretlige regler om kontrolforanstaltninger kan databeskyttelsesreglerne spille ind ved virksomhedens kontrol af medarbejderne. Der findes forskellige kontrolforanstaltninger, f.eks. anvendelse af GPS i udstyr, optagelse af telefonsamtaler, TV-overvågning mv.

Kontakt Dansk Erhverv, hvis I har brug for rådgivning om kontrol af medarbejdere.

[9] Databeskyttelseslovens § 11, stk. 2

6.2 Internet og e-mail

En IT-politik kan medvirke til at beskytte og sikre virksomhedens data, systemer og værdier - og i denne forbindelse også omdømme. I politikken kan virksomheden fastsætte retningslinjer overfor medarbejderne om informationssikkerhed, medarbejdernes brug af internet- og e-mail mv. Databeskyttelsesreglerne har bl.a. også betydning ved virksomhedens registrering af medarbejdernes brug af internet og e-mails og håndtering af medarbejderens indbakke ved fratræden.

Gode råd
Læs mere i Dansk Erhvervs Gode-råd-pjecer om internet og e-mail, bl.a. om virksomhedens kontrol af medarbejdernes brug samt sociale medier på www.danskerhverv.dk*:*

- *Gode råd om internet og e-mail*
- *Gode råd om sociale medier*

Eksempel på IT-politik
Dansk Erhverv har også udarbejdet et eksempel på en IT-politik med en tilhørende vejledning, som I kan få tilsendt ved kontakt til Dansk Erhvervs Hotline på 3374 6400.

7. Medarbejderoplysninger på virksomhedens hjemmeside og intranet

Virksomhedens hjemmeside
Virksomheden kan som udgangspunkt offentliggøre arbejdsrelaterede oplysninger om medarbejderne på virksomhedens hjemmeside uden medarbejdernes samtykke, f.eks. medarbejderens:

- Navn
- Arbejdsområde
- Kontaktoplysninger (direkte telefonnummer og e-mailadresse på arbejdet).

Der kan dog være særlige hensyn til medarbejderen, der gør, at oplysningerne alligevel ikke kan ligge på virksomhedens hjemmeside. F.eks. hvis medarbejderen på grund af trusler om vold eller lignende har beskyttet adresse og derfor ikke ønsker sin arbejdsplads offentlig kendt.

Datatilsynet vurderer, at det som udgangspunkt kræver samtykke fra medarbejderen, hvis en virksomhed vil offentliggøre oplysninger af mere privat karakter, f.eks.:

- Et billede af medarbejderen
- Medarbejderens private adresse, e-mailadresse eller telefonnummer.

Virksomhedens intranet
På baggrund af Datatilsynets praksis er det Dansk Erhverv vurdering, at en virksomhed som udgangspunkt kan anvende billeder af medarbejderne på intranettet, for at gøre det muligt for kolleger at sætte ansigt på hinanden, på baggrund af virksomhedens legitime interesse, jf. (nuværende) artikel 6, stk.1, litra f. Dvs. uden medarbejdernes samtykke.

Datatilsynet giver i deres "*Vejledning om samtykke*" et eksempel på, at en virksomhed indhenter samtykke fra medarbejderne ved brug af billeder på intranettet. I forlængelse heraf har Datatilsynet dog tilkendegivet, at eksemplet *ikke* skulle ses som om, at samtykke her var nødvendigt med henblik på virksomhedens anvendelse af fotos på intranettet – og dermed ikke som en ændring af Datatilsynets praksis.

8. Databeskyttelsesrådgiver

8.1. Krav om databeskyttelsesrådgiver for visse virksomheder

Private virksomheder

En række virksomheder skal udpege en databeskyttelsesrådgiver.[10] Det er dog langt fra alle virksomheder. Kravet om en databeskyttelsesrådgiver omfatter:

- Virksomheder, hvis *kerneaktiviteter* består af behandlingsaktiviteter, der i medfør af deres karakter, omfang og/eller formål kræver regelmæssig og systematisk overvågning af registrerede i stort omfang.
- Virksomheder, hvis *kerneaktiviteter* består af behandling af følsomme oplysninger eller oplysninger om straffedomme og lovovertrædelser i stort omfang.

Justitsministeriet vurderer, at en virksomhed, der alene behandler personoplysninger som en biaktivitet i forbindelse med f.eks. **personaleadministration** *ikke* er omfattet af begrebet "kerneaktiviteter". Ministeriet vurderer også, at det forhold, at en virksomhed behandler følsomme oplysninger om fagforeningsmæssige tilhørsforhold eller oplysninger om helbredsmæssige forhold i forbindelse med en virksomheds personaleadministration, heller ikke i sig selv medfører et krav om, at virksomheden skal udpege en databeskyttelsesrådgiver.

Private aktører på det offentlige område

Kravet om en databeskyttelsesrådgiver gælder også ved alle behandlinger foretaget af en" offentlig myndighed" eller et "offentligt organ". Denne afgræsning er særlig relevant for private aktører på det offentlige område.

Justitsministeriet antager, at begreberne må udfyldes af Danmark i overensstemmelse med vores traditionelle afgrænsning af det offentlige. For så vidt angår selvejende institutioner mv. oprettet på privatretligt grundlag (forvaltningslovens § 1, stk. 2, nr. 2), vil der således efter ministeriets vurdering være nogle, som bliver omfattet af kravet om en databeskyttelsesrådgiver, mens andre ikke gør. Ministeriet tilkendegiver i øvrigt, at i det omfang særlovgivning har reguleret, at forvaltningsloven finder anvendelse for private organisationer, vil der ikke være tale om en offentlig myndighed i regelsættets forstand.

Skal vi have en databeskyttelsesrådgiver?
Læs mere om kravene til databeskyttelsesrådgiver på www.danskerhverv.dk under Rådgivning, Persondata (kunder). I kan også kontakte Dansk Erhverv for nærmere rådgivning om dette.

[10] Det danske begreb "databeskyttelsesrådgiver" svarer til det engelske "data protection officer" eller forkortet "DPO", der også i dansk sammenhæng ses anvendt flere steder

8.2. Opgaver, stilling og afskedigelsesbeskyttelse

Databeskyttelsesrådgiveren kan enten være en medarbejder i virksomheden eller en ekstern tjenesteyder. Databeskyttelsesforordningen oplister en række opgaver, som databeskyttelsesrådgiveren som minimum har.

Databeskyttelsesrådgiveren skal bl.a. underrette og rådgive virksomheden og de ansatte, der behandler personoplysninger, om deres forpligtelser efter reglerne om databeskyttelse. Databeskyttelsesrådgiveren skal også overvåge overholdelse af reglerne om databeskyttelse og virksomhedens politikker om beskyttelse af personoplysninger, herunder ansvarsfordeling, oplysningskampagner og uddannelse af de medarbejdere, der medvirker ved behandlingsaktiviteter, og tilhørende revisioner. Databeskyttelsesrådgiveren skal også samarbejde med og være kontaktpunkt for Datatilsynet, der skal have databeskyttelsesrådgiverens kontaktoplysninger.

Virksomheden skal inddrage databeskyttelsesrådgiveren i alle spørgsmål vedr. persondatabeskyttelse og skal støtte databeskyttelsesrådgiveren i udførslen af opgaverne, herunder tilvejebringe nødvendige ressourcer og give adgang til oplysninger og behandlingsaktiviteter.

Virksomheden skal sikre, at databeskyttelsesrådgiverne ikke modtager instrukser vedr. udførslen af deres opgaver og rapporterer direkte til virksomhedens øverste ledelsesniveau.

Er databeskyttelsesrådgiveren en ansat medarbejder med andre opgaver, kan vedkommende dog som udgangspunkt fortsat være underlagt instruktion og ledelse vedr. disse opgaver. Virksomheden skal generelt sikre sig, at der ikke opstår interessekonflikt i forbindelse med andre opgaver, som databeskyttelsesrådgiveren udfører som medarbejder.

Databeskyttelsesrådgiveren må ikke afskediges eller straffes af virksomheden for at udføre sine opgaver som databeskyttelsesrådgiver.

9. Oplysningspligt og indsigtsret

Vejledning fra justitsministeriet
Datatilsynet mv. har udgivet en generel "*Vejledning om den registreredes rettigheder*", der gennemgår oplysningspligten og indsigtsretten. Vejledningen kan hentes på www.datatilsynet.dk evt. via www.danskerhverv.dk.

9.1. Virksomhedens oplysningspligt

Virksomheden skal som udgangspunkt oplyse en registreret jobansøger eller medarbejder om en række forhold, hvis virksomheden indsamler oplysninger om vedkommende.

Virksomheden skal oplyse følgende ved indsamlingen:

- Virksomhedens identitet og kontaktoplysninger.
- Kontaktoplysninger for virksomhedens databeskyttelsesrådgiver. Dette krav gælder kun, hvis virksomheden har en databeskyttelsesrådgiver.

- Hvilken regel i databeskyttelsesreglerne, virksomhedens behandling af oplysningerne om medarbejderen mv. sker efter (retsgrundlaget). Hvis virksomheden behandler oplysninger efter en berettiget interesse, skal virksomheden oplyse denne interesse.
- Eventuelle modtagere eller kategorier af modtagere af oplysningerne.
- Kategorier af oplysninger. Kravet gælder alene, når oplysningerne er indsamlet hos andre end medarbejderen selv.

Samtidig skal virksomheden give en række andre oplysninger, der er nødvendige for at sikre en rimelig og gennemsigtig behandling. Justitsministeriet vurderer her, at det må afhænge af en konkret vurdering, om oplysningerne skal gives:

- Det tidsrum, oplysningerne opbevares i. Hvis dette ikke er muligt, oplyses de kriterier, der anvendes til at fastlægge tidsrummet. Her vurderer Justitsministeriet, at en henvisning til relevante forældelsesregler kan være tilstrækkelig.
- Medarbejderens ret til indsigt, berigtigelse, sletning, indsigelse, begrænsning, dataportabilitet mv.
- Medarbejderens ret til at trække et samtykke tilbage.
- Medarbejderens mulighed for at klage til Datatilsynet over virksomhedens behandling af oplysningerne.
- Om medarbejderens meddelelse af oplysninger er krav efter lovgivning, en kontrakt mv.
- Hvor oplysningerne stammer fra. Kravet gælder alene, når indsamlingen sker hos andre end medarbejdere selv.

Der er særlige regler om overførsler til tredjelande eller internationale organisationer samt automatiserede afgørelser.

Undtagelser til oplysningspligten
Oplysningspligten er ikke uden undtagelser. F.eks. har virksomheden ikke en oplysningspligt, hvis medarbejderens interesse i at få kendskab til oplysningerne bør vige for afgørende hensyn til private interesser, f.eks. virksomhedens forretningshemmeligheder.

Hvis medarbejderen kender oplysningerne, skal virksomheden ikke give medarbejderen oplysninger om disse.

Vejledning og eksempel på persondatapolitik
Dansk Erhverv har udarbejdet en vejledning og eksempel på en politik om behandling af medarbejderes personoplysninger, der også inkluderer virksomhedens oplysningspligt overfor medarbejderen. Vejledningen kan hentes på www.danskerhverv.dk.

9.2. Medarbejderens indsigtsret

Medarbejderen har som udgangspunkt ret til indsigt i de oplysninger, som virksomheden behandler om vedkommende. Medarbejderen kan derimod ikke kræve indsigt i oplysninger om andre personer, f.eks. kolleger. Der er i databeskyttelsesloven fastsat en række undtagelser til indsigtsretten, bl.a. virksomhedens forretningshemmeligheder.

Vejledning og skabelon vedr. medarbejderens indsigtsret

Dansk Erhverv har udarbejdet en særlig vejledning om reglerne om indsigtsret og undtagelserne til denne. Til vejledningen er også knyttet en skabelon, som virksomheden kan tage udgangspunkt i, hvis en medarbejder anmoder om indsigtsret i egne oplysninger.

Hent Dansk Erhvervs *"Vejledning om indsigtsret"* på www.danskerhverv.dk.

10. Fortegnelse vedrørende personaleadministrationen

Efter forordningen skal en virksomhed føre en *intern* fortegnelse over behandlingsaktiviteter vedrørende personoplysninger under virksomhedens ansvar. Kravet om en fortegnelse omfatter al behandling af personoplysninger, dvs. både almindelige oplysninger, følsomme oplysninger og oplysninger om straffedomme mv.

Kravet om en fortegnelse omfatter bl.a. situationen, hvor virksomhedens behandling ikke er lejlighedsvis. Justitsministeriet vurderer, at en virksomhed typisk som minimum skal have en sådan fortegnelse vedrørende sin *personaleadministration*.

Vejledning til fortegnelse vedrørende personaleadministration

Dansk Erhverv har udarbejdet en særlig vejledning om reglerne om fortegnelse i forbindelse med personaleadministration. Til vejledningen er knyttet et eksempel på en fortegnelse over en privat virksomheds personaleadministration.

Hent Dansk Erhvervs *"Vejledning – Fortegnelse vedrørende personaleadministration"* på www.danskerhverv.dk.

11. Opbevaring af oplysninger før, under og efter ansættelsesforholdet

Databeskyttelsesreglerne indeholder et generelt krav om, at en virksomhed ikke må opbevare oplysninger på en måde, der giver mulighed for at identificere den registrerede i længere tid end det, der er nødvendigt til behandlingsformålet. En virksomhed skal derfor løbende overveje, om det er nødvendigt at opbevare en oplysning – og ellers slette den.

Har virksomheden fastsat generelle slettefrister, følger det dog af Datatilsynets tidligere praksis, at virksomheden ikke har pligt til løbende at gennemgå samtlige sager, dokumenter mv. med henblik på at sikre, at der ikke behandles oplysninger i strid hermed. Det forudsætter dog, at virksomheden har procedurer som sikrer, at der sker sletning i overensstemmelse med de fastsatte frister.

Oplysninger vedrørende nuværende medarbejdere må som udgangspunkt opbevares under ansættelsesforholdet. Datatilsynets har f.eks. i en konkret sag vurderet, at en medarbejder ikke havde ret til at få slettet en ældre advarsel fra personalesagen ud fra persondatareglerne.

Det er Dansk Erhvervs vurdering, at en virksomhed som udgangspunkt må have mulighed for at opbevare en personalesag 5 år efter medarbejderens fratræden som følge af den almindelige 5-årige forældelsesfrist i ansættelsesretlige sager. Virksomheden skal også overholde bogføringslovens regler, herunder opbevaring af relevante oplysninger i denne sammenhæng i 5 år efter et regnskabsårs afslutning. Samtidig kan der være situationer, hvor særlige forhold gør en længere opbevaringsperiode relevant, f.eks. verserende arbejdsskadesager, uafsluttede retssager eller arbejdsretlige tvister mellem medarbejderen og virksomheden, pensionsforpligtelser, dagpengerefusion og udbetaling af tilgodehavender.

For så vidt angår jobansøgere, der får afslag, vil der formentlig skulle "mere til" for at dokumentere sagligheden af at opbevare oplysninger om de pågældende i en længere periode. Dansk Erhverv bemærker, at Datatilsynet hidtil har anbefalet, at følsomme oplysninger om ansøgere, der får afslag på ansættelse, slettes hurtigst muligt og senest 6 måneder efter afslaget. Dansk Erhverv er imidlertid i dialog med Datatilsynet om, at virksomheder kan have behov for at gemme ansøgninger i længere tid for at kunne dokumentere, at der ikke er sket ulovlig forskelsbehandling i forbindelse med udvælgelsen. Vi håber, at Datatilsynet vil tage højde for dette i de kommende vejledninger. Hvis formålet med at gemme en ansøgning er at kunne besætte en fremtidig stilling, vil det oftest kræve et samtykke fra ansøgeren. Se også afsnit 4.2.

12. Datasikkerhed ved personaleadministration

Bemærk, at Justitsministeriet endnu ikke har udgivet den varslede "*Vejledning om behandlingssikkerhed*".[11] Indholdet af denne vejledning kan give anledning til ændringer i dette afsnit om sikkerhed.

Reglerne om sikkerhed

Personoplysninger skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende oplysninger. Virksomheden skal træffe de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger, så personoplysningerne beskyttes mod uautoriseret eller ulovlig behandling og mod hændelige tab, tilintetgørelse eller beskadigelse. Disse regler om datasikkerhed gælder også i forhold til oplysninger om virksomhedens medarbejdere.

Det er præciseret i databeskyttelsesforordningen, at virksomheden ud fra

- aktuelle tekniske niveau
- implementeringsomkostninger
- behandlingens karakter, omfang, sammenhæng og formål
- risici af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder

skal gennemføre tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

[11] Vejledningen var varslet med en offentliggørelse i januar 2018, men afventes p.t. (27. juni 2018) fortsat uden ny kendt dato

Vurderingen af, hvilke sikkerhedskrav en virksomhed skal overholde i forbindelse med personaleadministrationen, kan således ændre sig over tid, bl.a. i takt med hvilke muligheder den teknologiske udvikling faktisk giver for at beskytte personoplysninger.

Forordningen indeholder også en række eksempler mv.

Ud over de særlige regler om sikkerhed, er sikkerhed også skrevet ind i forbindelse med forordningens grundlæggende principper. Justitsministeriet vurderer ikke umiddelbart, at denne præcisering i sig selv fastlægger selvstændige krav til datasikkerheden, men at den skal ses som et signal om, at sikkerheden skal tillægges stor betydning ved behandling af personoplysninger.

Anmeldelse af sikkerhedsbrud
Hvis der sker sikkerhedsbrud, skal virksomheden anmelde det til Datatilsynet senest 72 timer efter, at sikkerhedsbruddet er kendt. Bliver anmeldelsen forsinket, skal virksomheden give Datatilsynet en begrundelse. Sikkerhedsbruddet skal dog ikke anmeldes, hvis det er usandsynligt, at sikkerhedsbruddet indebærer en risiko for fysiske personers rettigheder og frihedsrettigheder. Virksomheden skal som udgangspunkt også underrette en registreret medarbejder, hvis sikkerhedsbruddet sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder. Der gælder dog flere undtagelser til denne underretningspligt.

Tidligere praksis fra Datatilsynet
Datatilsynet havde ud fra den tidligere gældende persondatalov oplistet en række specifikke minimumskrav for sikkerhed i forbindelse med personaleadministration. Det var standardkrav, som Datatilsynet anvendte ved tilladelser til personaleadministration i den private sektor. Et tilladelseskrav, der nu er bortfaldet. Grundlæggende krævede Datatilsynet, at virksomheden skulle beskrive, hvordan personaleoplysninger i personaleadministrationen beskyttes – og hvordan Datatilsynets minimumskrav i den forbindelse er gennemført. Det kunne være f.eks. være en del af en it-sikkerhedspolitik.

Politik
Virksomheder med medarbejdere skal også implementere ”passende databeskyttelsespolitikker”, hvis det står i rimeligt forhold til virksomhedens behandling af oplysninger.

Dansk Erhverv vurderer på det foreliggende grundlag, at en virksomhed som udgangspunkt skal have en sikkerhedspolitik for personaleadministrationen. Her beskriver virksomheden, hvordan personaleoplysninger som led i personaleadministration beskyttes. Beskrivelsen kan være i særlige retningslinjer, der indgår i virksomhedens generelle sikkerhedsregler, i en it-sikkerhedspolitik eller på anden måde som en del af virksomhedens instrukser til medarbejderne.

Vejledning og eksempel på sikkerhedspolitik i forbindelse med personaleadministration

Dansk Erhverv har udarbejdet et eksempel på en sikkerhedspolitik i forbindelse med personaleadministration. Eksemplet er udarbejdet ud fra Justitsministeriets foreløbige arbejde med databeskyttelsesforordningen.

Hent Dansk Erhvervs *"Vejledning og eksempel på sikkerhedspolitik i forbindelse med personaleadministration"* på www.danskerhverv.dk.

13. Advarselsregistre

En virksomhed kan indenfor databeskyttelsesreglernes rammer oprette et advarselsregister med henblik på at advare andre mod f.eks. ansættelsesforhold til en registreret. Som eksempel har Datatilsynet tidligere givet tilladelse til et koncernregister over tidligere bortviste medarbejdere. Formålet med advarselsregisteret var at give mulighed for at overveje eventuel genansættelse af medarbejdere, der tidligere er blevet bortvist.

Vil virksomheden oprette et advarselsregister, kræver det tilladelse fra Datatilsynet.

14. Samarbejdsudvalg

En række virksomheder har etableret et samarbejdsudvalg efter Samarbejdsaftalen mellem DA og LO. I Samarbejdsaftalen oplistes en række opgaver, hvor samarbejdsudvalget skal inddrages. Bl.a. skal samarbejdsudvalget inddrages ved fastlæggelse af principper for virksomhedens interne indsamling, opbevaring og brug af persondata.[12]

Læs mere om samarbejdsudvalg på Samarbejdsnævnets hjemmeside http://www.samarbejdsnaevnet.dk.

15. Sanktioner

En person, der har lidt materiel eller immateriel skade som følge af en ulovlig behandling af personoplysninger mv., kan kræve erstatning. Overtrædelse af en række bestemmelser i persondataloven kan også medføre straf i form af fængsel eller bøde.

På nuværende tidspunkt er det dog vanskeligt at sige noget om, hvordan konkrete typer af overtrædelser af reglerne for behandling af oplysninger vil blive vurderet, da reglerne først er trådt i kraft 25. maj 2018.

[12] Samarbejdsaftalen pkt. 3 Samarbejdsudvalget

16. Øvrige elementer

Databeskyttelsesforordningen mv. omfatter også en række andre regler, der kan have direkte eller indirekte betydning for virksomheder, der administrerer personoplysninger om medarbejdere mv. Blandt andet regler om:

- Koncerner
- Datatilsynets virke, herunder det europæiske samarbejde
- Internationale dataoverførsler
- Databeskyttelse by design og default
- Konsekvensanalyser
- Automatiserede afgørelser
- Adfærdskodekser og certificering
- Reglernes geografiske anvendelsesområde

Kontakt Dansk Erhverv, hvis I har behov for særlig rådgivning om sådanne emner i forbindelse med behandling af oplysninger om medarbejderne.

17. Vil I vide mere?

Spørg Dansk Erhverv

Medlemmer af Dansk Erhverv kan kontakte Hotline vedrørende spørgsmål om håndtering af medarbejderoplysninger på tlf. 3374 6400.

Vejledninger og paradigmer fra Dansk Erhverv

Dansk Erhverv har udgivet en række vejledninger og paradigmer om særlige emner, der løbende er henvist til her i vejledningen. De kan hentes på www.danskerhverv.dk under Rådgivning/Persondata(medarbejdere) og omfatter samlet:

- Vejledning og eksempel på en politik om behandling af medarbejderes personoplysninger
- Vejledning og skabelon på en fortegnelse over personaleadministrationen
- Sikkerhedspolitik i forbindelse med personaleadministration
- Vejledning og skabeloner til behandling af jobansøgninger
- Vejledning og skabelon om håndtering af indsigtsret
- Samtykke til fotos på virksomhedens hjemmeside.

"Gode råd" fra Dansk Erhverv

Dansk Erhverv har også udgivet en række pjecer i "Gode Råd Om"-serien. "Gode Råd Om"- serien findes på www.danskerhverv.dk og omfatter bl.a. følgende HR-områder:

- Gode råd om internet og mail
- Gode råd om sociale medier
- Gode råd om rekruttering

Vejledninger fra Datatilsynet mv.
Datatilsynet m.fl. har udgivet en lang række vejledninger om databeskyttelsesreglerne, der kan hentes på www.datatilsynet.dk. Vejledninger med særlig relevans for personaleadministration kan også findes på www.danskerhverv.dk under Rådgivning/Persondata(medarbejdere).

Datatilsynet udgav også en pjece med generel information om virksomhedens interne arbejde med databeskyttelsesreglerne før det nye regelsæts ikrafttræden 25. maj 2018: "*Forberedelser forud for EU's databeskyttelsesforordning - 12 spørgsmål som dataansvarlige allerede nu med fordel kan forholde sig til*". Pjecen kan hentes på tilsynets hjemmeside.

Erhvervsjuridisk rådgivning
Dansk Erhverv har også udgivet en række erhvervsjuridiske materialer, f.eks. en databehandleraftale. Læs mere på www.danskerhverv.dk under Rådgivning/Persondata(kunder).