ERHVERVSSTYRELSEN

JUSTITSMINISTERIET

DIGITALISERINGSSTYRELSEN

DATATILSYNET

Vejledning om databeskyttelses-rådgivere

December 2017

Indhold

1 Forord

Denne vejledning har til formål at redegøre for kravene i forordningen til at udpege en databeskyttelsesrådgiver, dennes opgaver, kvalifikationer, stilling og inddragelse

Databeskyttelsesforordningen og databeskyttelsesloven finder anvendelse i Danmark og resten af EU fra den 25. maj 2018. Forordningen stiller blandt andet krav om, at offentlige myndigheder og organer er forpligtede til at udpege en databeskyttelsesrådgiver. Private er derimod kun i få tilfælde forpligtet til at udpege en databeskyttelsesrådgiver.

I det omfang en organisation er forpligtet til at udpege en databeskyttelsesrådgiver, skal dette senest ske fra den 25. maj 2018.

Afsnit 2 omhandler en beskrivelse af databeskyttelsesrådgiveren.

Afsnit 3 omhandler, hvornår private er forpligtet til at udpege en databeskyttelsesrådgiver, muligheden for at udpege en fælles databeskyttelsesrådgiver og frivillig udnævnelse af en databeskyttelsesrådgiver.

Afsnit 4 omhandler offentlige myndigheder og organers forpligtelse til at udpege en databeskyttelsesrådgiver og muligheden for at udpege en fælles databeskyttelsesrådgiver.

Afsnit 5 omhandler selve funktionen som databeskyttelsesrådgiver, herunder kravene til dennes faglige kvalifikationer, stilling, opgaver og inddragelse i organisationen.

1.1 Databeskyttelsesrådgivere – øget fokus på ansvarlighed (”accountability”)

Forpligtelsen til at skulle udpege en databeskyttelsesrådgiver kan ses som et element i databeskyttelsesforordningens fokus på ansvarlighed, når det kommer til efterlevelse af databeskyttelsesreglerne.

Alle dataansvarlige skal således, uanset om de er underlagt forpligtelsen til at udpege en databeskyttelsesrådgiver eller ej, efterleve kravene i forordningens artikel 24, der generelt fastlægger den dataansvarliges forpligtelser.

Endvidere er det en forudsætning for at kunne overholde de grundlæggende principper om behandling af personoplysninger i forordningens artikel 5, at alle dataansvarlige og databehandlere har et overblik over, *hvilke* personoplysninger der behandles, og *hvordan* disse behandles i organisationen.

Som følge af princippet om ansvarlighed, bør alle organisationer, både private og offentlige dataansvarlige og databehandlere, uanset om de er forpligtede til at udpege en databeskyttelsesrådgiver, derfor tage stilling til, hvor i organisationen ansvaret for og håndteringen af databeskyttelsesspørgsmål bør ligge.

Der kan i den forbindelse henvises til Datatilsynets vejledning om forberedelse forud for EU's databeskyttelsesforordning, som er tilgængelig på tilsynets hjemmeside: www.datatilsynet.dk.

Der kan ligeledes henvises til en oversigt over de øvrige supplerende vejledninger om databeskyttelsesforordningen, som vil blive offentliggjort forud for, at forordningen finder anvendelse.

1.2 Andre relevante kilder

Der kan i øvrigt henvises til Artikel 29-gruppens udtalelser, herunder om databeskyttelsesrådgivere:http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf . Artikel 29-gruppen er rådgivende og uafhængig og består af en repræsentant fra hvert af medlemsstaternes tilsynsmyndighed.

2 Hvad er en databeskyttelsesrådgiver?

En databeskyttelsesrådgiver er en rådgiverfunktion i en organisation, der skal inddrages i alle spørgsmål om databeskyttelse og rådgive om de databeskyttelsesretlige regler.

Databeskyttelsesrådgiverens funktion er at understøtte, at den dataansvarlige overholder reglerne i databeskyttelsesforordningen. Databeskyttelsesrådgiveren er en integreret del af den dataansvarliges organisation, der efter omstændighederne kan have andre opgaver for den dataansvarlige. Databeskyttelsesrådgiveren er altså ikke en del af Datatilsynet og fungerer heller ikke som tilsynets repræsentant.

Databeskyttelsesrådgiveren har dog en særlig stilling i forhold til Datatilsynet, idet databeskyttelsesrådgiveren er kontaktled til og skal samarbejde med Datatilsynet. Databeskyttelsesrådgiveren kan på den måde bl.a. være opdateret om og tage bestik af nye afgørelser, vejledninger mv.

Forpligtelsen til i visse tilfælde at skulle udpege en databeskyttelsesrådgiver er et element i databeskyttelsesforordningens fokus på ansvarlighed, når det kommer til at overholde databeskyttelsesreglerne.

2.1 Relationen mellem den dataansvarlige og databeskyttelsesrådgiveren

Det er den dataansvarlige, der har *ansvaret* for at sikre, at databeskyttelsesforordningen og databeskyttelseslovens regler overholdes.

Den dataansvarlige udpeger databeskyttelsesrådgiveren. Det er databeskyttelsesrådgiverens opgave at *rådgive* den dataansvarlige om de databeskyttelsesretlige regler, og rådgiveren kan således på bedste vis understøtte en god databeskyttelse hos den dataansvarlige.

Den dataansvarlige skal tage højde for databeskyttelsesrådgiverens opfattelse af en given situation, men det er den dataansvarlige, der skal overholde reglerne. Det er således også den dataansvarlige, der i sidste ende afgør til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger. Det er ligeledes den dataansvarlige, som sanktioneres, såfremt reglerne ikke overholdes, også selvom dette skyldes ukorrekt rådgivning fra databeskyttelsesrådgiverens side.

3 Privates forpligtelse til at udpege en databeskyttelsesrådgiver

I de fleste tilfælde skal private *ikke* udpege en databeskyttelsesrådgiver.

3.1 Hvornår skal private udpege en databeskyttelsesrådgiver?

I de fleste tilfælde skal den private sektor *ikke* udpege en databeskyttelsesrådgiver. Kun private virksomheder, der som deres kerneaktivitet behandler følsomme oplysninger eller oplysninger om strafbare forhold i et stort omfang eller foretager regelmæssig og systematisk overvågning af personer i stort omfang, er forpligtede til at udpege en databeskyttelsesrådgiver. Forpligtelsen for private virksomheder til at udpege en databeskyttelsesrådgiver gælder både den dataansvarlige og databehandleren.

Det betyder, at de fleste private virksomheder i Danmark, der foretager "gængs" behandling af personoplysninger, herunder administration af HR-oplysninger, kundeoplysninger, online bookingsystemer mv., *ikke* er forpligtede til at udpege en databeskyttelsesrådgiver.

Konkret skal en virksomhed opfylde tre betingelser for at være forpligtet til at udpege en databeskyttelsesrådgiver (se nedenfor).

Alle betingelser skal være opfyldt, og en virksomhed, der f.eks. kun opfylder én eller to af betingelserne ud af de tre, vil *ikke* være forpligtet til at udpege en databeskyttelsesrådgiver.

Følgende tre betingelser skal alle være opfyldt:

1. **Behandling af personoplysninger skal være virksomhedens *kerneaktivitet***
2. **Der skal behandles personoplysninger i et *stort omfang***
3. **Behandlingsaktiviteten består i *regelmæssig* og *systematisk overvågning* af personer eller behandlingen vedrører *følsomme oplysninger* eller oplysninger om *strafbare forhold***

Generelt kan det bemærkes om betingelserne, at de knytter sig til, hvilke personoplysninger man har, og hvordan disse behandles i virksomheden.

3.1.1. Betingelse nr. 1: ”kerneaktivitet”

Behandling af personoplysninger skal være virksomhedens kerneaktivitet. Med ”kerneaktivitet” forstås *ikke* den gængse behandling af personoplysninger, som de fleste virksomheder foretager.

Alle virksomheder behandler således personoplysninger i et vist omfang, for at virksomheden kan fungere. Det drejer sig navnlig om behandling af HR-oplysninger og kundeoplysninger i forbindelse med kontakt, salg og support mv. Virksomhedens behandling af disse oplysninger er en forudsætning for, at virksomheden kan udøve sin hovedaktivitet, f.eks. udbyde tjenesteydelser eller sælge et produkt.

Disse almindelige behandlinger af personoplysninger udgør ikke i sig selv en ”kerneaktivitet”. De kan i stedet anses for en ”biaktivitet”, idet oplysningerne behandles for at kunne understøtte virksomhedens hovedaktivitet.

Når en virksomhed behandler personoplysninger som en biaktivitet, vil virksomheden *ikke* være forpligtet til at udpege en databeskyttelsesrådgiver.

Eksempler på behandling, der udgør ”biaktivitet”

- **Kundekontakt- eller support**
- **HR-oplysninger**
- **Salg**
- **Kundekartotek**
- **Online bookingsystem**
- **Bonuskort**
- **Behandling af klientoplysninger (revisorer, advokater, ingeniører mv.)**
- **IT-support**

Eksempler på brancher, der som udgangspunkt *ikke* har behandling af personoplysninger som kerneaktivitet:

- **Privatskoler og døgninstitutioner**
- **Forsyningsselskaber**
- **Håndværksfaget**
- **Hotel- og restaurationsbranchen**
- **Servicebranchen**
- **Detailhandel**

Omfattet af begrebet ”kerneaktivitet”

Behandling af personoplysninger skal være virksomhedens ”hovedaktivitet”, før det kan anses for omfattet af begrebet kerneaktivitet.

Det betyder, at virksomheder, hvis produkt eller tjeneste direkte *består* i behandling af personoplysninger, kan anses som kerneaktivitet. Det kan f.eks. være virksomheder, der udbyder marketingsundersøgelser, som er baseret på personoplysninger eller cloud-virksomheder, når det indebærer lagring af personoplysninger.

På samme måde kan virksomheder, hvis produkt eller tjeneste er *uløseligt forbundet* med behandlingen af personoplysninger, anses for at have behandling af personoplysninger som deres kerneaktivitet. Det kan f.eks. være forsikringsselskaber, der sælger forsikringer til sine kunder, bl.a. på baggrund af personoplysninger indsamlet om kommende og nuværende kunder. Et andet eksempel kan være privathospitaler.

Eksempler på behandling, der udgør "kerneaktivitet":

- **Cloud-computing**
- **Hosting af hjemmesider/data**
- **Privathospitaler**
- **Forsikringsselskaber**
- **Reklamebureauer, der udbyder marketingsundersøgelser**
- **Søgemaskiner**
- **Tele- eller internetudbydere**
- **Applikationer/mobile tjenester baseret på personoplysninger**
- **Stillingsbesættende virksomhed**

Virksomheder, hvis kerneaktivitet består af behandling af personoplysninger, skal dog også opfylde de to øvrige betingelser, inden virksomheden er forpligtet til at udpege en databeskyttelsesrådgiver.

3.1.2. Betingelse nr. 2: "et stort omfang"

Hvis behandlingen af personoplysninger er virksomhedens kerneaktivitet, er det *også* en betingelse, at behandlingen af personoplysninger sker i "et stort omfang", før virksomheden er forpligtet til at udpege en databeskyttelsesrådgiver.

Artikel 29-gruppen[1] anbefaler i deres udtalelse om databeskyttelsesrådgivere, at der ved vurderingen af, om der er tale om en behandling af personoplysninger "i et stort omfang", lægges vægt på fire kriterier:

1. Antallet af personer, der behandles oplysninger om – enten det specifikke antal personer eller som andel af den relevante population (befolkningen).

[1] Artikel 29-gruppens udtalelse nr. 16/2016 om "Guidelines on Data Protection Officers ('DPOs')", (WP 243 rev.01).

2. Volumen af personoplysninger og/eller de forskellige typer af personoplysninger, der bliver behandlet.

3. Tidsperioden, der behandles oplysninger i, samt hvorvidt behandlingen er permanent.

4. Den geografiske udstrækning af behandlingsaktiviteterne

Behandling af personoplysninger "i et stort omfang" kan således indebære behandling af:

- **en stor mængde af personoplysninger**
- **oplysninger om et stort antal personer**
- **lang varighed, herunder permanent**
- **stor geografisk udstrækning af behandlingsaktiviteter**

Eksempel – mindre forsikringsselskab
Et mindre forsikringsselskab, der f.eks. kun udbyder sin forretning til en bestemt mindre landsdel, vil formentlig behandle et så begrænset omfang af oplysninger, at det *ikke* kan anses for at være i et stort omfang. Det skyldes, at der ikke behandles en stor mængde af personoplysninger om et stort antal personer samt den begrænsede geografiske udstrækning.

I modsætning hertil vil et landsdækkende forsikringsselskab anses for at behandle personoplysninger i et stort omfang, både som følge af mængden af oplysninger, antallet af personer og den geografiske udstrækning.

Eksempel – lægepraksis
Behandling af patientdata i en lægepraksis med et begrænset antal læger tilknyttet kan som følge af den begrænsede mængde oplysninger, der behandles, heller ikke anses for at behandle personoplysninger i et stort omfang.

Omvendt vil en stor lægepraksis med mange læger tilknyttet formentlig behandle en stor mængde personoplysninger om deres patienter. Her vil mængden af oplysninger, der behandles, medføre, at der foretages behandling af personoplysninger i et stort omfang.

I overvejelserne om fastlæggelse af størrelsen af en privat lægepraksis/klinik/hospital er det relevant at foretage en vurdering af både antallet af patienter og af tilknyttede læger.

Behandling i et stort omfang

Eksempler på virksomheder, der behandler personoplysninger "i et stort omfang":

- **Privathospitaler**
- **Større forsikringsselskaber**
- **Sporing via f.eks. rejsekort**
- **Søgemaskines behandling af personoplysninger**
- **Tele- eller internetudbydere**

Virksomheder, hvis *kerneaktivitet* består af behandling af personoplysninger *i et stort omfang*, skal dog opfylde én af de to sidste betingelser, inden virksomheden er forpligtet til at udpege en databeskyttelsesrådgiver.

3.1.3. Betingelse nr. 3: "regelmæssig og systematisk overvågning" eller "behandling af følsomme oplysninger eller oplysninger om strafbare forhold"

Virksomheder, hvis *kerneaktivitet* består af behandling af personoplysninger *i et stort omfang* skal enten:

- foretage regelmæssig og systematisk overvågning af registrerede personer

  eller

- behandle følsomme oplysninger/oplysninger om strafbare forhold,

for at være forpligtede til at udpege en databeskyttelsesrådgiver.

Regelmæssig og systematisk overvågning af registrerede personer
Regelmæssig og systematisk overvågning af de registrerede omfatter en virksomheds sporringer (tracking) eller profilering bl.a. via internettet.

Det kan bl.a. omfatte drift af telenet eller services forbundet hermed, profilering i forbindelse med risikovurdering, herunder kreditvurderinger, vurdering af forsikringspræmie, lokationstracking via applikationer og adfærdsbaseret annoncering.

Eksempel – marketingsfima
Et marketingsfirma, der foretager marketingsundersøgelser, hvor der indgår personoplysninger i et stort omfang, og undersøgelsen er baseret på adfærdsbaseret annoncering, er omfattet, da de foretager en regelmæssig og systematisk overvågning af de registrerede personer.

Behandling af følsomme oplysninger eller oplysninger om strafbare forhold
Oplysninger kan anses for *følsomme*, hvis de omhandler oplysninger om:

- race eller etnisk oprindelse
- politisk, religiøs eller filosofisk overbevisning
- fagforeningsmæssigt tilhørsforhold
- behandling af genetisk data eller biometrisk data med det formål entydigt at identificere en fysisk person
- helbredsoplysninger
- oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Oplysninger om strafbare forhold omfatter oplysninger om straffedomme og lovovertrædelser.

Eksempel – skadesforsikringsselskaber
Skadesforsikringsselskaber kan man opdele i de selskaber, der behandler følsomme oplysninger, og de selskaber der ikke (eller i begrænset omfang) behandler følsomme oplysninger.

For så vidt angår de selskaber, der *ikke* behandler denne type oplysninger kan nævnes specialselskaber, som typisk forsikrer ting (f.eks. glasforsikring) og ikke risiko for personskader. Forsikringsselskaber, der i *begrænset* omfang, jf. betingelsen ovenfor, behandler de omhandlede oplysninger vil typisk være forsikringsselskaber, der tegner privatforsikringer, herunder eksempelvis indbo- og bilforsikringer, eller erhvervsforsikringer for mindre virksomheder. Her indhentes de nævnte oplysninger i forbindelse med tegning af ulykkesforsikringer og ved behandling af personskader under ulykkesforsikringer.

For så vidt angår skadesforsikringsselskaber, der opfylder betingelse nr. 3 – idet de behandler følsomme oplysninger – kan nævnes specialiserede rejseforsikringsselskaber for såvel rejsegods som syge- og ulykkesforsikringer. En betydelig del af disse selskabers forsikringer er personforsikringer, hvor der både ved tegning og ved behandlingen af personskader (ulykker og sygdomme) indhentes følsomme oplysninger. Endvidere kan sygeforsikringsselskaber, som dækker medicin og en række andre udgifter til helbredelse, nævnes, idet der indhentes helbredsoplysninger ved optagelses- og refusionssager.

Eksempel – HR-oplysninger
Virksomheder vil typisk behandle oplysninger om ansattes fagforeningsmæssige tilhørsforhold og helbredsoplysninger i forbindelse med virksomhedens HR-funktion. Her er der netop tale om følsomme oplysninger, men det medfører ikke i sig selv, at virksomheden er forpligtet til at udpege en databeskyttelsesrådgiver. Hertil kræves, at behandling af personoplysninger er virksomhedens *kerneaktivitet* og foretages *i et stort omfang*.

Eksempler på virksomheder, der kan opfylde <u>alle tre</u> betingelser

- **Privathospitaler**
- **Større forsikringsselskaber**
- **Tele- eller internetudbydere**
- **Marketingsfirma, der udbyder marketingsundersøgelser**

Eksempler på virksomheder, der blot opfylder <u>nogle</u> af betingelserne

- **Mindre privathospitaler**
- **Mindre forsikringsselskab**
- **Mindre lægepraksis**
- **Større virksomheder, hvor behandling af personoplysninger kun er en biaktivitet**

Eksempel – Livs- og pensionsforsikringsselskaberne
Store eller middelstore forsikringsselskaber, der dels tegner livs- og pensionsforsikringer for enkeltpersoner og dels firmapensionsordninger, hvor de sikrede er en virksomheds ansatte, indhenter og behandler følsomme oplysninger, især helbredsoplysninger ved såvel tegning/indmeldelse som ved behandlingen af tab af erhvervsevne, dødsfald, sygdom m.v. Henset til, at behandling af personoplysninger endvidere er disse forsikringsselskabers *kerneaktivitet,* samt at de grundet størrelse og geografiske udstrækning behandler personoplysningerne i *stort omfang,* vil de som udgangspunkt skulle udpege en databeskyttelsesrådgiver.

Det bemærkes, at det er vigtigt at have sig for øje, at der er tale om betingelser, der alle skal være opfyldt. Der skal altså være tale om, at virksomhedens *kerneaktivitet* er behandling i *stort omfang* af *følsomme oplysninger* eller *oplysninger om strafbart forhold*. Eller at virksomhedens *kerneaktivitet* består af behandlingsaktiviteter i *stort omfang* af *regelmæssig og systematisk overvågning* af personer.

Virksomheder, der ikke er forpligtede til at udpege en databeskyttelsesrådgiver, kan med fordel dokumentere vurderingen, så denne kan fremvises til Datatilsynet.

3.2 Frivillig udnævnelse af en databeskyttelsesrådgiver

Private kan under alle omstændigheder frivilligt vælge at udpege en databeskyttelsesrådgiver.

I de tilfælde, hvor der frivilligt udpeges en databeskyttelsesrådgiver, gælder de samme krav til databeskyttelsesrådgiveren, som hvis virksomheden var forpligtet til at udpege en databeskyttelsesrådgiver.

Det betyder, at kravene til databeskyttelsesrådgiverens opgaver, kvalifikationer, stilling, beskyttelse og inddragelse skal efterleves.

Vælger en virksomhed derimod at udpege en medarbejder, der f.eks. er compliance-rådgiver, er virksomheden ikke forpligtet til at efterleve forordningens krav til en databeskyttelsesrådgiver.

3.3 Fælles databeskyttelsesrådgiver

En koncern har mulighed for at udpege en fælles databeskyttelsesrådgiver for hele koncernen, forudsat at alle etableringer af koncernen har let adgang til databeskyttelsesrådgiveren.

Andre private dataansvarlige og databehandlere end koncerner har også mulighed for at udpege en fælles databeskyttelsesrådgiver. Et konsulentfirma kan udøve funktionen som databeskyttelsesrådgiver for flere dataansvarlige på samme tid på baggrund af tjenesteydelseskontrakter.

Det er dog en forudsætning for, at private kan udpege en fælles databeskyttelsesrådgiver, at databeskyttelsesrådgiveren kan efterleve forordningens krav til vedkommende, når opgaven lø-

ses for flere private på én gang. Dette må i praksis forudsætte, at der f.eks. er adgang til at kommunikere med databeskyttelsesrådgiveren på et sprog, som de berørte medarbejdere kan forstå. Det må ligeledes forudsætte, at der er afsat sådanne ressourcer til databeskyttelsesrådgiveren, at det spejler omfanget af de organisationer, der skal dækkes. Der vil derfor i praksis ikke være noget til hinder for, at f.eks. en virksomhed udpeger en fælles databeskyttelsesrådgiver på tværs af flere større koncernforbundne virksomheder, når blot de ressourcer, der afsættes til databeskyttelsesrådgiveren i form af medarbejdere, rejsebudget, it-understøttelse mv. i tilstrækkelig omfang sikrer, at databeskyttelsesrådgiveren kan møde sine forpligtelser.

3.4 Opsummering

- Der skal rigtig meget til før, en privat virksomhed er forpligtet til at udpege en databeskyttelsesrådgiver.

- Helt konkret skal tre betingelser, der knytter sig til en virksomheds behandling af personoplysninger, alle være opfyldt, før der en pligt til at udpege en databeskyttelsesrådgiver.

- Alle virksomheder bør foretage en konkret vurdering af, om de tre betingelser er opfyldt. Er alle tre betingelser ikke opfyldt, skal der ikke udpeges en databeskyttelsesrådgiver.

4 Offentlige myndigheders forpligtelse til at udpege en databeskyttelsesrådgiver

Offentlige myndigheder og offentlige organer skal *altid* have en databeskyttelsesrådgiver, uanset om de er dataansvarlige eller databehandlere.

4.1 Hvornår skal offentlige myndigheder udpege en databeskyttelsesrådgiver?

I det omfang behandling foretages af en offentlig myndighed eller et offentligt organ skal myndigheden eller organet *altid* have en databeskyttelsesrådgiver, hvad enten de er dataansvarlige eller databehandlere.

Det betyder, at der også skal udpeges en databeskyttelsesrådgiver, hvis den offentlige myndighed eller organ behandler personoplysninger på vegne af en privat eller selv outsourcer sin databehandling til en privat, som ikke er forpligtet til at udpege en databeskyttelsesrådgiver. Det kan f.eks. være tilfældet, når offentlige myndigheder eller organer vælger at overlade til en anden at udføre selve den praktiske behandling af personoplysninger på den dataansvarliges vegne.

Den eneste undtagelse hertil er domstole, der *ikke* er forpligtede til at udpege en databeskyttelsesrådgiver, når de handler i deres egenskab af domstole.

4.2 Hvornår er man en offentlig myndighed?

De myndigheder, der i dansk ret henregnes til den offentlige forvaltning i medfør af forvaltningslovens § 1, stk. 1-2, skal anses for offentlige myndigheder eller organer, og er dermed forpligtede til at udpege en databeskyttelsesrådgiver. Det fremgår heraf, at følgende virksomheder omfattes af loven: *al virksomhed, der udøves af den offentlige forvaltning, og al virksomhed, der udøves af selvejende institutioner, foreninger, fonde m.v., der er oprettet ved lov eller i henhold til lov, og selvejende institutioner, foreninger, fonde m.v., der er oprettet på privatretligt grundlag, og som udøver offentlig virksomhed af mere omfattende karakter og er undergivet intensiv offentlig regulering, intensivt offentlig tilsyn og intensiv offentlig kontrol.*

I forhold til *selvejende institutioner m.v. oprettet på privatretligt grundlag*, vil der således være nogle, som omfattes af kravet om at have en databeskyttelsesrådgiver, mens andre ikke omfattes. Det vil bero på en konkret vurdering.

Selvejende institutioner m.v. oprettet på privatretligt grundlag, som udøver offentlig virksomhed af mere omfattende karakter og er undergivet intensiv offentlig regulering, intensivt offentlig tilsyn og intensiv offentlig kontrol vil være omfattet.

Det spiller endvidere ind, om det offentlige har instruktionsbeføjelser over for institutionen, om det offentlige skal godkende institutionens vedtægter, og om det offentlige yder sekretariatsbistand

til institutionen. Herudover må man se på, om det offentlige skal godkende institutionens regnskaber, og om institutionens drift og virksomhed er detaljeret reguleret ved regler og retningslinjer udstedt af det offentlige. Endelig kan man tage hensyn til, om det offentlige overtager institutionens rettigheder og forpligtelser, hvis den nedlægges.

Eksempler på selvejende institutioner m.v., der er omfattet
- Universiteter
- Institutioner hvor kommunalbestyrelsen har indgået overenskomst til opfyldelse af sine forpligtelser efter lov om social service
- Gymnasieskoler

Eksempler på selvejende institutioner og foreninger der ikke er omfattet
- Danske Regioner og KL
- Dansk Flygtningehjælp

For så vidt angår *statslige og kommunale institutioner, der er organiseret i selskabsform*, f.eks. som aktieselskab eller interessentskab vil disse umiddelbart aldrig være omfattet. Dette er også tilfældet for koncessionerede selskaber og selskaber, hvori staten eller en kommune er aktionær, interessent eller lignende, uanset om staten eller kommunen ejer selskabet 100 %. Det har i den forbindelse ingen betydning, hvilke aktiviteter organet udfører, ligesom det ikke i sig selv kan føre til et andet resultat, at selskabet måtte være oprettet ved lov eller i henhold til lov.

Dog er kommunale fællesskaber, jf. § 60 i lov om kommunernes styrelse, hvortil to eller flere kommuner overfører opgaver til selvstændig varetagelse, altid offentlige myndigheder. Det gælder, uanset at kommunale fællesskaber normalt etableres som interessentskaber. Det kommunale fællesskab er selvstændigt dataansvarligt og skal udpege en databeskyttelsesrådgiver.

Eksempel på institution, der er organiseret i selskabsform, der ikke er omfattet
- Staten og Kommunernes Indkøbs Service A/S

Såfremt der ikke er tale om en offentlig myndighed eller organ, skal bedømmelsen af hvorvidt man har pligt til at udpege en databeskyttelsesrådgiver foretages i henhold til betingelserne beskrevet ovenfor under punkt 3 vedrørende privates forpligtelse til at udpege en databeskyttelsesrådgiver.

4.3 Fælles databeskyttelsesrådgiver for offentlige myndigheder

Flere myndigheder eller organer vil i mange tilfælde kunne have en fælles databeskyttelsesrådgiver forudsat, at det er i overensstemmelse med deres organisatoriske struktur og størrelse. I den forbindelse kan det være relevant at overveje, om rådgiveren skal fungere på baggrund af én ansættelseskontrakt for to forskellige myndigheder eller to deltidskontrakter.

Herudover vil en databeskyttelsesrådgiver kunne være ansat på en deltidskontrakt hos én myndighed og ansat på baggrund af en tjenesteydelseskontrakt i en anden myndighed eller organisation.

Såfremt flere myndigheder har en fælles databeskyttelsesrådgiver, er det dog en forudsætning, at databeskyttelsesrådgiveren kan efterleve kravene i databeskyttelsesforordningen til en databeskyttelsesrådgiver, herunder til dennes stilling, opgaver, uafhængighed og tilgængelighed mv., når denne løser opgaven for flere myndigheder på én gang.

For så vidt angår *tilgængelighed* er der ikke et krav om fysisk tilstedeværelse på alle lokationer, såfremt der anvendes en fælles databeskyttelsesrådgiver. De enkelte myndigheder har i den forbindelse mulighed for at aftale, hvordan den fysiske tilgængelighed i praksis kan løftes, herunder f.eks. ved hjælp af mail, telefon, internet m.m. Det er i relation til kravet om tilgængelighed endvidere værd at bemærke, at flere myndigheder som nævnt godt kan have en fælles rådgiver, men at databeskyttelsesrådgiveren skal kunne (nå at) varetage sin rådgivningsopgave fyldestgørende for alle de myndigheder, for hvilke den pågældende varetager opgaven som databeskyttelsesrådgiver. Her kan det bl.a. være relevant at se på mængden af personoplysninger, der behandles i en given myndighed.

I relation til *uafhængighedskriteriet* bemærkes, at det kan være betænkeligt at lade visse myndigheder have en fælles databeskyttelsesrådgiver, jf. nedenfor under afsnittet ”*Eksempel – Ministerier og underordnede myndigheder*”.

Der henvises i øvrigt til afsnit 5 i denne vejledning.

Det er endvidere et krav, at der er én, der er personligt ansvarlig for hvervet som databeskyttelsesrådgiver.

Som følge af kravet om, at udpegningen af en fælles databeskyttelsesrådgiver skal være i overensstemmelse med myndigheden eller organets organisatoriske struktur og størrelse, stilles der krav til selve ansættelsen af databeskyttelsesrådgiveren.

Den retlige grænse for at dele en databeskyttelsesrådgiver vil i et sådan tilfælde være de gældende standarder om offentlige ansattes bierhverv, de almindelige habilitetsregler og muligheden for at efterleve kravene i forordningen, herunder tilstrækkelige ressourcer i forhold til at udføre hvervet.

Eksempel - *Rigspolitiets databeskyttelsesenhed*

Rigspolitiet har udpeget en fælles databeskyttelsesrådgiver for landets 12 politikredse og Rigspolitiet, for så vidt angår behandlingen af personoplysninger til brug for retshåndhævelsesformål.

Den fælles databeskyttelsesrådgiver understøttes i den forbindelse af en central datebeskyttelsesenhed i Rigspolitiet, hvor de enkelte medarbejdere besidder stort kendskab til persondateretlige og forretningsmæssige forhold med relevans for enhedens opgavevaretagelse. På denne baggrund kan databeskyttelsesrådgiveren samlet set leve op til sine forpligtelser som databeskyttelsesrådgiver i medfør af lov om retshåndhævende myndigheders behandling af personoplysninger, som er lig dem, der følger af databeskyttelsesforordningen.

Kommuner

Det antages ikke at være i overensstemmelse med en offentlig myndigheds struktur eller størrelse, hvis en databeskyttelsesrådgiver fungerer på baggrund af én ansættelseskontrakt i to forskellige kommuner. Det antages derimod omvendt at være i overensstemmelse hermed, såfremt rådgiveren udøver sin funktion på baggrund af to deltidskontrakter i to kommuner på samme tid.

Eksempel – En kommune

En kommune vil typisk være dataansvarlig for alle de behandlinger af personoplysninger, som foretages inden for den kommunale enhedsforvaltning. Derfor er en kommune ikke forpligtet til at udpege én databeskyttelsesrådgiver for de enkelte forvaltninger, men vil kunne udpege én databeskyttelsesrådgiver for hele kommunen.

Eksempel – organer med selvstændig kompetence på det kommunale område

Det bemærkes, at der på det kommunale område kan være organer, som ikke er en del af den kommunale enhedsforvaltning, men har selvstændig kompetence på det kommunale område, f.eks. huslejenævnet, ligesom der kan være kommunale organer, som er en del af enhedsforvaltningen, der i visse henseender har en – i forhold til kommunalbestyrelsen – selvstændig kompetence, herunder f.eks. skoleledere.

Når det i lovgivningen er fastsat eller forudsat, at disse organer sekretariatsbetjenes af kommunen, og kommunen yder sekretariatsbetjening, kan organerne have fælles databeskyttelsesrådgiver med kommunen og er ikke forpligtet til selvstændigt at udpege en databeskyttelsesrådgiver ved siden af kommunens. Databeskyttelsesrådgiverens ydelser vil i den forbindelse være en del af sekretariatsbetjeningen.

Eksempel – Flere kommuner

Flere kommuner vil have mulighed for at dele en databeskyttelsesrådgiver. Som udgangspunkt vurderes det, at f.eks. en gennemsnitskommune på omkring 45.000 indbyggere godt vil kunne dele en databeskyttelsesrådgiver med en anden tilsvarende eller en mindre kommune, eller at en lidt større kommune vil kunne dele med en mindre kommune, hvis databeskyttelsesrådgiveren

samlet set vurderes at kunne varetage opgaverne som databeskyttelsesrådgiver. Der skal således foretages en konkret vurdering i det enkelte tilfælde, idet det afgørende er, om man som databeskyttelsesrådgiver kan efterleve sin funktion retmæssigt, når funktionen udøves for flere kommuner på samme tid.

Herudover vil to eller flere kommuner kunne oprette et *kommunalt fællesskab*, til hvilket de går sammen om at løse opgaven som databeskyttelsesrådgiver i de deltagende kommuner.

Eksempel - Regioner
En region vil typisk også være dataansvarlig for alle de behandlinger af personoplysninger, der foretages inden for regionen, herunder drift af hospitaler, forskning og sociale tilbud mv. Hver region vil som udgangspunkt kunne udpege én databeskyttelsesrådgiver.

Eksempel - Ministerier og underordnede myndigheder
Departementer og underordnede myndigheder kan have en fælles databeskyttelsesrådgiver.

Dog kan der være hindringer, som f.eks. myndighedens størrelse, der bevirker, at man ikke kan dele en databeskyttelsesrådgiver. Som eksempel herpå kan nævnes Justitsministeriet og politiet, der ikke kan have en fælles rådgiver.

Det skyldes, at politiet anses for at være så stor en enhed, at en fælles databeskyttelsesrådgiver ikke vil kunne efterleve kravene til en databeskyttelsesrådgiver (om bl.a. tilgængelighed), hvis denne både skulle udføre sin opgave for politiet som helhed og med andre myndigheder under Justitsministeriets ressort.

Dog vil politiet – i en ordning svarende til den ovenfor beskrevne på retshåndhævelsesområdet – kunne have en fælles databeskyttelsesrådgiver under forordningen, der udfører sin funktion for alle politikredse.

Det bemærkes endvidere, at forordningens krav om uafhængighed skal være opfyldt for alle de myndigheder, der deler en databeskyttelsesrådgiver.

I den forbindelse – samt i relation til en underordnet myndigheds eventuelt særlige uafhængighed ift. den overordnede myndighed – kan der være visse situationer, hvor det kan være betænkeligt at lade en underordnet myndighed dele databeskyttelsesrådgiver med et departement.

Som eksempel herpå kan nævnes Datatilsynet og Justitsministeriets departement. Dette er bl.a. henset til Datatilsynets funktionelle uafhængighed i forhold til Justitsministeriet samt tilsynets specielle kompetence og rolle i forhold til databeskyttelsesforordningen. Som et andet eksempel kan nævnes Ankestyrelsens relation til (på nuværende tidspunkt) Økonomi- og Indenrigsministeriets departement. Her kan bl.a. peges på mængden og karakteren af data, som behandles i Ankestyrelsen samt styrelsens faglige uafhængighed af departementet.

Organisatoriske ændringer kan også bevirke, at det i visse situationer – af praktiske årsager – kan være mere oplagt for en underordnet myndighed at have sin egen databeskyttelsesrådgiver fremfor at dele med sit departement. Hvis en underordnet myndighed således har sin egen databeskyttelsesrådgiver kan denne blot fortsætte under samme kontrakt, vilkår m.v. uanset, at en

myndighed, efter eksempelvis et regeringsskifte, organisatorisk placeres under et andet ministerium.

Eksempel - Selvejende institutioner
I det omfang selvejende institutioner kan anses for en offentlig myndighed eller et organ, vil disse myndigheder også have mulighed for at udpege en fælles databeskyttelsesrådgiver med en anden selvejende institution omfattet af samme lovgivning eller f.eks. den kommune, som institutionen har driftsoverenskomst med, i det omfang kommunen yder sekretariatsbistand til institutionen.

4.4 Opsummering

- Alle offentlige myndigheder og organer skal udpege en databeskyttelsesrådgiver fra den 25. maj 2018.

- Det er i høj grad muligt at udpege en fælles databeskyttelsesrådgiver, der fungerer på vegne af flere myndigheder på én gang.

- Muligheden for at have en fælles databeskyttelsesrådgiver begrænses af, at denne skal kunne leve op til sine forpligtelser efter databeskyttelsesforordningen.

- Databeskyttelsesrådgiveren kan understøttes af en enhed for at kunne udføre sit hverv i overensstemmelse med forordningens krav. Dette gælder uanset, om databeskyttelsesrådgiveren fungerer for én myndighed eller for flere myndigheder og organer.

5 Databeskyttelsesrådgiveren

5.1 Krav til faglige kvalifikationer

En databeskyttelsesrådgiver skal udpeges på baggrund af sine faglige kvalifikationer. Dette gælder navnlig evnen til at udføre sine opgaver som databeskyttelsesrådgiver og ekspertise inden for databeskyttelsesret- og praksis.

Der er ikke krav om, at en databeskyttelsesrådgiver skal have en bestemt uddannelsesmæssig baggrund, f.eks. som jurist.

Dermed er det op til den enkelte organisation at vurdere, hvem der er bedst egnet til at varetage stillingen som databeskyttelsesrådgiver.

Kravene til stillingen afhænger til en vis grad af kompleksiteten af den behandling af personoplysninger, som den pågældende organisation foretager. Dermed kan der for nogen organisationer være behov for at ansætte en databeskyttelsesrådgiver med stor erfaring inden for feltet, og i andre tilfælde kan en eksisterende medarbejder på baggrund af diverse kurser varetage funktionen.

Hvis der udpeges en databeskyttelsesrådgiver fra egen organisation, kan det med fordel være en person, som i forvejen har et vist kendskab til eller indsigt i håndtering af databeskyttelsesretlige spørgsmål i organisationen.

5.2 Hvem kan være databeskyttelsesrådgiver?

Som udgangspunkt kan alle, som organisationen finder kvalificeret til at være databeskyttelsesrådgiver, varetage funktionen.

Følgende kan derfor være databeskyttelsesrådgivere:

- En intern medarbejder
- En fælles databeskyttelsesrådgiver for hele eller flere organisationer
- En ekstern databeskyttelsesrådgiver.

Intern medarbejder
En organisation kan vælge at udpege en eksisterende medarbejder som databeskyttelsesrådgiver.

Det er ikke et krav, at den medarbejder, der varetager funktionen som databeskyttelsesrådgiver, udøver sin funktion på fuld tid.

Dermed kan en intern medarbejder, der varetager funktionen som databeskyttelsesrådgiver, udføre andre opgaver og have andre pligter i organisationen.

Således kan en medarbejder, der f.eks. arbejder i IT-sektionen i en organisation, godt varetage funktionen som databeskyttelsesrådgiver på deltid eller 10 timer om ugen, alt efter behovet i den enkelte organisation.

Det afgørende er, at den pågældende medarbejder fyldestgørende kan udøve sit erhverv som databeskyttelsesrådgiver i organisationen.

Den person, der udpeges, kan med fordel være en person, som i forvejen har et vist kendskab til eller indsigt i håndtering af databeskyttelsesretlige spørgsmål i organisationen.

Selve vurderingen af, hvor meget tid en medarbejder skal bruge på fyldestgørende at kunne efterleve kravene til en databeskyttelsesrådgiver i organisationen, afhænger af en konkret vurdering af behovet hos organisationen.

Interne ansatte, der ikke kan være databeskyttelsesrådgiver
En databeskyttelsesrådgiver skal både være uafhængig og være i stand til at udøve uvildig rådgivning til organisationen.

Derfor kan en databeskyttelsesrådgiver ikke være den øverste IT-ansvarlige eller øverste HR-ansvarlige i en organisation.

> **Medarbejdere, *som ikke har det øverste ansvar*, kan være databeskyttelsesrådgivere. Det betyder, at ledende IT-medarbejdere, compliance-officerer eller en it-sikkerheds koordinator mv., kan udøve funktionen som databeskyttelsesrådgiver i organisationen.**

Eksempel – virksomhed med få ansatte
Virksomheder med få ansatte, herunder f.eks. enkeltmandsvirksomheder, vil have svært ved at opfylde betingelsen om, at en databeskyttelsesrådgiver ikke kan være øverste IT-ansvarlige eller øverste HR-ansvarlige i en organisation (forudsat at virksomheden i øvrigt opfylder betingelserne for, hvornår private skal udpege en databeskyttelsesrådgiver, jf. nærmere om privates forpligtelse under punkt 3). I en sådan situation kan virksomheden enten benytte sig af muligheden for at udpege en fælles databeskyttelsesrådgiver eller anvende en konsulent til opgaven.

Databeskyttelsesrådgiverenhed
Der kan også udpeges én databeskyttelsesrådgiver for den pågældende organisation, som understøttes af en enhed, så den pågældende kan leve op til sine forpligtelser efter forordningen, jf. den ovenfor beskrevne ordning for politiet.

Fælles databeskyttelsesrådgiver
Såvel private som offentlige myndigheder kan udpege en fælles databeskyttelsesrådgiver afhængig af deres struktur og størrelse.

Ekstern medarbejder

Man kan også vælge at udpege en ekstern databeskyttelsesrådgiver. Dette kan enten være en rådgiver (konsulentvirksomhed), såsom en bestemt advokat eller revisor, eller andre kvalificerede eksterne parter. Udøvelsen af hvervet som databeskyttelsesrådgiver vil dog i sagens natur alene kunne udøves i det omfang, dette er foreneligt med eventuelle regler – herunder etiske krav – for den relevante type af rådgivervirksomhed mv.

5.3 Databeskyttelsesrådgiverens opgaver

Databeskyttelsesrådgiveren funktion består i at rådgive den dataansvarlige og hjælpe med at organisationen efterlever de databeskyttelsesretlige regler.

En databeskyttelsesrådgiver skal desuden prioritere sine opgaver og fokusere på de behandlinger af personoplysninger i den pågældende organisation, som konkret indebærer en højere risiko for brud på de databeskyttelsesretlige regler. Dog skal øvrige databeskyttelsesretlige områder, som indebærer en lavere grad af risiko ikke undlades.

Der er en række opgaver, som databeskyttelsesrådgiveren *som minimum* skal varetage. Der er dog ikke noget til hinder for, at der overlades flere opgaver til databeskyttelsesrådgiveren. Databeskyttelsesrådgiverens rolle som central rådgivningsfigur i organisationen samt dennes opgaver kan med fordel beskrives nærmere i en (ansættelses)aftale.

Nedenfor følger en nærmere beskrivelse af de opgaver, som databeskyttelsesrådgiveren som minimum skal varetage i en organisation.

Underrette og rådgive organisationen og de ansatte om databeskyttelse

Det indebærer:

- Konkret rådgivning om beskyttelse af personoplysninger i organisationen samt overvejelser og beslutninger om, hvordan compliance sikres m.v., f.eks. i forbindelse med følgende:
    - Organisationens indkøb af nyt IT-system,
    - kravsspecifikationer til leverandører,
    - udarbejdelse af organisationens data-politikker,
    - iværksættelse af behandling af personoplysninger,
    - overvejelser om, hvorvidt en given behandling af personoplysninger overholder de generelle behandlingsregler
- Stå til rådighed for ansatte samt ledelsen i organisationen vedrørende spørgsmål om databeskyttelse

- Rådgivning i forbindelse med udarbejdelse af organisationens konsekvensanalyser, jf. afsnit 3 nedenfor

- Modtage underretning om og rådgive organisationen i forbindelse med brud på persondatasikkerheden

Overvåge overholdelsen af de databeskyttelsesretlige regler i organisationen

Det indebærer bl.a. også at overvåge:

- organisationens politikker om databeskyttelse
- uddannelse af personale i databeskyttelse
- oplysningskampagner
- fordeling af ansvar
- revisioner

Som led i overvågningsopgaven kan databeskyttelsesrådgiveren foretage følgende:

- **indsamle oplysninger til at identificere behandlingsaktiviteter**
- **informere, rådgive og komme med anbefalinger til den dataansvarlige og databehandleren.**

Det skal hertil bemærkes, at databeskyttelsesrådgiverens opgave med at overvåge overholdelsen af de databeskyttelsesretlige regler i organisationen ikke medfører, at rådgiveren overtager selve ansvaret for, at behandlingen af personoplysninger sker i overensstemmelse med reglerne. Dette ansvar ligger fortsat hos den dataansvarlige.

Rådgivning i forbindelse med udarbejdelse af organisationens konsekvensanalyser

I visse tilfælde skal organisationer udarbejde en konsekvensanalyse af en planlagt behandling af personoplysninger.

I de tilfælde, hvor en organisation har udpeget en databeskyttelsesrådgiver, skal denne rådføres, når der foretages en konsekvensanalyse.

Herudover skal databeskyttelsesrådgiveren rådgive med hensyn til konsekvensanalysen, når der anmodes herom.

Rådgivning i forhold til konsekvensanalyser kan bl.a. indebære rådgivning vedrørende:

- **om der skal gennemføres en konsekvensanalyse**
- **hvilken fremgangsmåde der skal anvendes ved gennemførelse af konsekvensanalysen**
- **om konsekvensanalysen kan gennemføres internt, eller om gennemførelsen kræver antagelse af ekstern bistand**
- **hvilke sikkerhedsforanstaltninger (tekniske og organisatoriske) som skal anvendes for at begrænse risici i forhold til de registreredes rettigheder og interesser**
- **om konsekvensanalysen er korrekt gennemført, og om dens konklusioner er i overensstemmelse med de databeskyttelsesretlige regler**

I tilfælde af uenighed mellem organisationen og databeskyttelsesrådgiveren anbefales det, at det specifikt fremgår af selve konsekvensanalysen, hvorfor databeskyttelsesrådgiverens indstilling ikke er blevet fulgt.

Samarbejde med Datatilsynet på vegne af organisationen

En organisation er forpligtet til at høre Datatilsynet inden behandling, hvis en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen af personoplysninger vil føre til høj risiko i mangel af foranstaltninger truffet af organisation for at begrænse risikoen.

Det følger af forordningen, at databeskyttelsesrådgiveren skal *samarbejde* med tilsynsmyndigheden og fungere som tilsynsmyndighedens kontaktperson. Det kan f.eks. være databeskyttelsesrådgiveren, der på vegne af den dataansvarlige, hører tilsynsmyndigheden.

Være kontaktpunkt for tilsynsmyndigheden (Datatilsynet) angående alle spørgsmål om behandling af personoplysninger for de personer, der behandles oplysninger om

Databeskyttelsesrådgiveren skal inddrages af den dataansvarlige i tilfælde af, at konkrete klagesager indbringes for Datatilsynet. Databeskyttelsesrådgiveren bør ligeledes orienteres, når Datatilsynet beslutter at gennemføre et eventuelt tilsyn af den dataansvarlige.

Herudover skal databeskyttelsesrådgiveren også være i stand til at vejlede den person, der behandles personoplysninger om. Det betyder, at databeskyttelsesrådgiveren skal være i stand til at vejlede om, hvilke rettigheder den pågældende har, og hvordan de kan udnyttes.

Det indebærer endvidere, at den dataansvarlige skal give meddelelse om kontaktoplysninger på databeskyttelsesrådgiveren.

Det anbefales i øvrigt, at organisationen i en funktionsbeskrivelse klart definerer, hvilke opgaver der påhviler databeskyttelsesrådgiveren. En funktionsbeskrivelse vil gøre det tydeligt, hvornår

den pågældende virker som databeskyttelsesrådgiver og i denne egenskab ikke kan instrueres. Det vil samtidig blive tydeligt, hvornår den pågældende udfører andre opgaver i sit ordinære ansættelsesforhold i organisationen.

5.4 Krav til organisationen – rettidig og tilstrækkelig inddragelse af databeskyttelsesrådgiveren

En organisation skal sikre, at databeskyttelsesrådgiveren inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger. En sådan inddragelse bør også ske på øverste ledelsesmæssige niveau (f.eks. ved deltagelse på direktions- og ledelsesmøder)

Det anbefales, at organisationen implementerer procedurer, som sikrer dette.

I hvilke tilfælde skal databeskyttelsesrådgiveren inddrages?
Databeskyttelsesrådgiveren skal inddrages i alle de overvejelser og vurderinger, som organisationen gør sig for at overholde kravene i databeskyttelsesforordningen, databeskyttelsesloven og øvrige regler for behandling af personoplysninger.

Eksempel på spørgsmål, hvor databeskyttelsesrådgiveren bør inddrages:

- ved overvejelser og beslutninger om hvordan organisationens compliance med databeskyttelsesreglerne sikres,
- ved overvejelser i forbindelse med datasikkerhed, herunder databeskyttelse gennem design og standardindstillinger og
- ved udarbejdelse af konsekvensanalyser.

Såfremt databeskyttelsesrådgiveren udpeges før den 25. maj 2018, kan denne inddrages i organisationens implementering af de krav, der følger af forordningen.

Eksempel på spørgsmål, hvor databeskyttelsesrådgiveren ikke skal inddrages

- **Konkrete vurderinger ift. registreredes rettigheder, f.eks. anmodning på indsigt, ret til at blive glemt mv.**
- **Deltagelse i mindre praktiske eller almindelige driftsopgaver eller driftsmæssige spørgsmål knyttet til opsætning af it-systemer.**
- **Udarbejdelse af konkrete databehandleraftaler.**
- **Behandling af personoplysninger, der finder sted i overensstemmelse med interne regler, som den dataansvarlige har fastsat, forudsat at disse regler er fastsat under inddragelse af databeskyttelsesrådgiveren.**

Hvordan skal databeskyttelsesrådgiveren inddrages?
For at sikre at databeskyttelsesrådgiveren inddrages tilstrækkeligt og rettidigt, er organisationen forpligtet til at holde databeskyttelsesrådgiveren tilstrækkeligt og rettidigt orienteret om alle spørgsmål om beskyttelse af personoplysninger.

Som tommelfingerregel skal databeskyttelsesrådgiveren have mulighed for at vurdere overholdelsen af de databeskyttelsesretlige regler og komme med bemærkninger eller lignende, *inden* en behandling af personoplysninger igangsættes.

Hvornår er inddragelsen rettidig?
Databeskyttelsesrådgiveren skal inddrages i så god tid, som det er muligt forud for iværksættelsen af behandling af personoplysninger.

Det er afgørende, at databeskyttelsesrådgiveren inddrages i tide til at kunne foretage en reel vurdering af, om den påtænkte behandling af personoplysninger er i overensstemmelse med de databeskyttelsesretlige regler, og dermed kan komme med kvalificerede bemærkninger herom med henblik på at rådgive organisationen.

Eksempler på rettidig inddragelse:

- **Inddrages forud for beslutning om nødvendige foranstaltninger i IT-systemer for at efterleve kravene om databeskyttelse gennem design og standardindstillinger**
- **Inddrages forud for udstedelse af retningslinjer og procedurer for, hvordan de databeskyttelsesretlige regler skal overholdes i organisationen**
- **Inddragelse før offentliggørelse af udbudsmateriale i en udbudsproces eller lignende**

Eksempler på ikke-rettidig inddragelse

- **Inddragelse af databeskyttelsesrådgiveren efter et nyt IT-system er færdigudviklet**
- **Inddragelse af databeskyttelsesrådgiveren efter indkøb af IT-systemer (dermed ikke en del af overvejelserne vedr. kravspecifikation og databeskyttelse gennem design og standardindstillinger)**
- **Inddragelse af databeskyttelsesrådgiveren efter at en konsekvensanalyse er udarbejdet**
- **Inddragelse af databeskyttelsesrådgiveren efter større ændringer i organisationens procedurer, der vedrører databeskyttelse, såsom håndtering af anmodninger fra registrerede personer**

Behandlingsaktiviteter igangsat før en databeskyttelsesrådgiver udpeges
Når en organisation udpeger en databeskyttelsesrådgiver, vil der selvsagt være behandlinger af personoplysninger, der allerede er igangsat i organisationen.

Databeskyttelsesrådgiveren bør ved udpegelsen primært have fokus på de fremadrettede compliance aktiviteter. Derudover kan databeskyttelsesrådgiveren – ud fra en risikovurdering i forhold til de behandlinger, som konkret indebærer højere risiko – inddrages i organisationens overvejelser om, hvorvidt de igangværende aktiviteter overholder de databeskyttelsesretlige regler.

Hvornår er inddragelsen tilstrækkelig?
Der skal ske en reel inddragelse af databeskyttelsesrådgiveren i organisationens overvejelser og beslutninger vedrørende databeskyttelse.

Det indebærer, at organisationen skal inddrage og tage højde for databeskyttelsesrådgiverens bemærkninger og rådgivning i øvrigt, samt dennes rapportering til øverste ledelsesniveau om overholdelse af de databeskyttelsesretlige regler.

Såfremt databeskyttelsesrådgiverens rådgivning ikke følges, anbefales det, at organisationen dokumenterer dette i overensstemmelse med kravet om accountability.

Ressourcer og adgang
Ressourcer
For at databeskyttelsesrådgiveren rent faktisk kan udføre sine opgaver, er det nødvendigt, at organisationens tilvejebringer de nødvendige ressourcer til støtte for databeskyttelsesrådgiveren.

Det er endvidere et krav, at organisationen tilvejebringer de fornødne ressourcer, for at databeskyttelsesrådgiveren kan opretholde sin ekspertise inden for området.

Fastsættelsen af de fornødne ressourcer beror på en konkret vurdering, som afhænger af de organisatoriske forhold i organisationen, såsom størrelsen, antallet af behandlingsaktiviteter, kompleksiteten af behandlingen af personoplysninger samt de forbundne risici.

Jo større en organisation er, des større er behovet for ressourcer til støtte for databeskyttelsesrådgiveren.

Selve behovet for ressourcer beror på en konkret vurdering, som organisationen er ansvarlig for at foretage. Som eksempler på fornødne ressourcer kan nævnes:

- **Faciliteter og arbejdsredskaber**
- **Økonomiske ressourcer**
- **Personaleressourcer og lignende**

Adgang
Databeskyttelsesrådgiveren skal også have adgang til organisationens personoplysninger og den behandling af disse, som organisationen foretager.

Der skal være tale om en vid adgang, som kan tilvejebringes efter behov.

Uafhængighed
Det er et grundlæggende krav, at en databeskyttelsesrådgiver ikke må blive instrueret af andre om, hvordan rådgiveren skal udføre sine opgaver. Der gælder således følgende for databeskyttelsesrådgiveren:

- Må ikke som led i sin funktion som databeskyttelsesrådgiver modtage instruks om hvordan denne skal udføre sine opgaver (eller f.eks. om en bestemt vurdering eller fortolkning af forordningen)
- Må ikke afskediges eller sanktioneres for at udføre sine opgaver
- Rapporterer direkte til øverste ledelsesniveau

Databeskyttelsesrådgiverens interne reaktionsmuligheder er i praksis tæt forbundne med, at ovenstående krav til uafhængighed efterleves. Idet en databeskyttelsesrådgiver ikke har instruktionsbeføjelser over for andre dele af den dataansvarliges organisation, er det i praksis muligheden for at kunne rapportere direkte til øverste ledelsesniveau, der er rådgiverens interne virkemiddel overfor konstaterede brud på forordningen.

Hvor det øverste ledelsesniveau er, afhænger af organiseringen hos den konkrete dataansvarlige eller databehandleren.

I forhold til det private erhvervsliv fremgår det af selskabsloven, at det er bestyrelsen, der er det centrale eller øverste ledelsesorgan i selskaber, der både har en bestyrelse og en direktion. Når der i databeskyttelsesforordningen henvises til det øverste ledelsesniveau, må det i det private forstås i relation til den daglige drift og dermed direktionen, såfremt selskabet har både en bestyrelse og en direktion. Det vil i praksis betyde, at direktionen skal orientere bestyrelsen om væsentlige forhold, som påpeges af databeskyttelsesrådgiveren.

For statslige myndigheder må den øverste ledelse forstås som den øverste administrative ledelse.

For så vidt angår kommuner og regioner gælder, at databeskyttelsesrådgiveren rapporterer direkte til kommunalbestyrelsen henholdsvis regionsrådet. Denne rapportering forelægges for kommunalbestyrelsen henholdsvis regionsrådet uden den forudgående udvalgsbehandling, som de kommunale og regionale sager ellers normalt skal undergives. Dette udelukker dog ikke, at en kommune kan indhente en erklæring fra økonomiudvalget forinden forelæggelse for kommunalbestyrelsen.

5.5 Beskyttelse af databeskyttelsesrådgiveren

Funktionen som databeskyttelsesrådgiver er beskyttet ved et forbud mod at kunne blive afskediget for udførelse af opgaverne som databeskyttelsesrådgiver.

Usaglig afskedigelse af en databeskyttelsesrådgiver er sanktioneret med en bøde.

Databeskyttelsesrådgiveren vil kunne afskediges på et *sagligt* grundlag efter almindelige ansættelsesretlige regler.

Eksempler på tilfælde, hvor en databeskyttelsesrådgiver kan afskediges:

- **Ikke udfører sine arbejdsopgaver**
- **Misligholder ansættelsesforholdet**
- **Samarbejdsvanskeligheder**

5.6 Opsummering

- En databeskyttelsesrådgiver udpeges på baggrund af sine faglige kvalifikationer. Databeskyttelsesrådgiveren kan både være en intern medarbejder, en fælles databeskyttelsesrådgiver for hele eller flere organisationer eller en ekstern databeskyttelsesrådgiver.

- Databeskyttelsesrådgiveren har en række opgaver denne som minimum skal varetage. Derudover anbefales det, at man klart definerer, hvilke opgaver der påhviler databeskyttelsesrådgiveren.

- En organisation skal rettidig og tilstrækkelig inddrage databeskyttelsesrådgiveren i alle spørgsmål vedrørende beskyttelse af personoplysninger.

- Databeskyttelsesrådgiveren nyder en særlig beskyttelse mod usaglig afskedigelse og kan ikke afskediges eller sanktioneres for at udføre sine opgaver som Databeskyttelsesrådgiver.

Dato
20. december 2017

Justitsministeriet
Slotsholmsgade 10
1216 København K

Telefon
72 26 84 00

Email
jm@jm.dk

ISBN
978-88-98564-35-7

Foto
Scanpix