VEJLEDNING

DATABESKYTTELSESRÅDGIVER

(DATA PROTECTION OFFICER)

**Databeskyttelsesrådgiver:**

Med Databeskyttelsesforordningens indførelse kom der et øget fokus på, at de enkelte virksomheder og organisationer selv bærer ansvaret for, at reglerne overholdes.

Som led i dette fokus på ansvarlighed er det i Databeskyttelsesforordningen bestemt, at alle offentlige myndigheder samt visse private virksomheder og organisationer, skal udpege en databeskyttelsesrådgiver (Data Protection Officer/DPO).

En databeskyttelsesrådgiver er en rådgiver, der skal involveres i alle forespørgsler vedr. databeskyttelse, som virksomheden, organisationen eller myndigheden måtte have. Herudover skal databeskyttelsesrådgiveren kunne vejlede om reglerne i Databeskyttelsesforordningen.

Databeskyttelsesrådgiveren udpeges/ansættes af den dataansvarlige. Databeskyttelsesrådgiveren skal hjælpe og rådgive den dataansvarlige med at sørge for, at alle forpligtelser, der er pålagt den dataansvarlige, i henhold til Databeskyttelsesforordningen, overholdes.

Databeskyttelsesrådgiveren kan også have andre funktioner inden for virksomheden eller i myndigheden. I forhold til Datatilsynet, skal databeskyttelsesrådgiveren fungere som formidler mellem Datatilsynet og virksomheden/organisationer, og databeskyttelsesrådgiveren skal derfor være indstillet på et samvirke med Datatilsynet. Dette betyder ikke, at databeskyttelsesrådgiverne hører under Datatilsynet eller agerer som repræsentant herfor, men betyder blot, at databeskyttelsesrådgiveren og Datatilsynet skal indgå i et samarbejde.

Selvom der er udpeget en databeskyttelsesrådgiver, er det fortsat den dataansvarlige, der står med det overordnede ansvar for at forordningens regler og krav overholdes. Samtidig er det den dataansvarlige, der bliver sanktioneret i tilfælde af, at reglerne ikke overholdes. Det gælder også i tilfælde af, at sanktionen sker på baggrund af databeskyttelsesrådgiverens fejlagtige rådgivning.

**Hvornår skal offentlige myndigheder udpege en databeskyttelsesrådgiver?**

Alle offentlige myndigheder og organer skal have en databeskyttelsesrådgiver. Dette gælder uanset om myndigheden agerer som dataansvarlig eller databehandler. Efter omstændighederne kan nogle offentlige myndigheder deles om én databeskyttelsesrådgiver.

**Hvornår skal private virksomheder (og andre organisationer) udpege en databeskyttelsesrådgiver?**

Det er kun i ganske få tilfælde, at en privat virksomhed (og andre organisationer) skal udpege en databeskyttelsesrådgiver.

En privat virksomhed skal opfylde tre betingelser (alle tre), før virksomheden er forpligtet til at udpege en databeskyttelsesrådgiver. Alle tre betingelser skal være opfyldt, førend det påkræves en virksomhed at udpege en databeskyttelsesrådgiver.

1) Behandling af personoplysninger skal være virksomhedens kerneaktivitet

2) Der skal ske behandling af personoplysninger i et stort omfang

3) Behandlingen skal bestå i regelmæssig og systematisk overvågning af personer *eller* behandling af følsomme oplysninger eller oplysninger om strafbare forhold

Selvom private virksomheder ikke er forpligtet til at udpege en databeskyttelsesrådgiver, er udvælgelsen af en databeskyttelsesrådgiver en frivillig beslutning. Dette kan være fordelagtigt, hvis det drejer sig om en organisation, der har en vis størrelse, hvor der eksisterer et behov for at al håndtering af Databeskyttelsesforordningen er forankret ved en enkelt person. Hvis man frivilligt udnævner en databeskyttelsesrådgiver, gælder de samme krav til denne, som hvis virksomheden havde været forpligtiget til at udpege en databeskyttelsesrådgiver.

Hvis en virksomhed i stedet vælger at udpege en medarbejder, som skal stå for at rådgive og for overholdelsen af kravene omkring persondata, er virksomheden *ikke* forpligtiget til at efterleve kravene til databeskyttelsesrådgivere.

**Betingelse nummer 1 – ”kerneaktivitet”**

Den første betingelse, der skal være opfyldt, før en virksomhed er forpligtiget til at udpege en databeskyttelsesrådgiver er, at virksomhedens behandling af personoplysninger skal klassificeres som virksomhedens kerneaktivitet. Det vil sige, at virksomhedens hovedaktivitet skal bestå af behandling af personoplysninger.

Stort set alle organisationer og virksomheder i Danmark behandler personoplysninger som en biaktivitet til deres hovedaktivitet. Eksempelvis vil behandlingen af personoplysninger om kunder og medarbejdere for en håndværksvirksomhed være en biaktivitet. Det samme er en specialskoles behandling af personoplysninger om elever og forældre.

En virksomheds behandling af personoplysninger kan betegnes som en kerneaktivitet, hvis behandling af personoplysninger primært udgør virksomhedens produkter eller tjenester. Eksempelvis vil virksomheder, som foretager marketingsundersøgelser, indsamle og behandle personoplysninger. Denne aktivitet vil i så fald være uløseligt forbundet med virksomhedens kerneaktivitet. Det samme gælder forsikringsselskaber, privathospitaler, tele/internet udbydere og lignende virksomheder.

**Betingelse nummer 2 – ”behandling af personoplysninger i et stort omfang”**

Den anden betingelse, der skal være opfyldt før en virksomhed skal udpege en databeskyttelsesrådgiver er, at virksomheden skal behandle personoplysninger i et ”stort omfang”.

Hvorvidt virksomheden behandler personoplysninger i et stort omfang, anslås ud fra fire betingelser, der omhandler behandlingen af personoplysninger i forhold til:

* Antal personer
* Volumen/mængden af personoplysninger
* Varighed
* Geografisk udstrækning

Datatilsynet giver i deres vejledning om databeskyttelsesrådgivere to eksempler på virksomheder, der ikke behandler oplysninger i et stort omfang. Det ene eksempel er et forsikringsselskab, der udelukkende tilbyder forsikringer i en mindre landsdel af Danmark. Det andet eksempel er en lægepraksis, som består af et begrænset antal læger.

Det kan ud fra ovenstående konkluderes, at der skal behandles personoplysninger i et relativt stort omfang, før betingelse nummer 2 er opfyldt.

**Betingelse nummer 3 – ”regelmæssig eller systematisk overvågning, behandling af følsomme oplysninger eller behandling af oplysninger om strafbare forhold”**

Den sidste betingelse, der skal være opfyldt før virksomheden skal have en databeskyttelsesrådgiver indebærer, at virksomheden enten 1) skal implementere en regelmæssig eller systematisk overvågning af personer eller 2) skal behandle personoplysninger af følsom karakter eller oplysninger om strafbare forhold (se evt. Enkel-GDPRs vejledning om typer af personoplysninger i step 1).

En *”regelmæssig og systematisk overvågning af de registrerede”* indebærer en virksomheds sporinger, som eksempelvis lokationsregistrering via applikationer, eller profilering, som eksempelvis sker igennem internettet.

Det vil sige, hvis en virksomhed, som behandler personoplysninger som deres kerneaktivitet i et stort omfang, foretager regelmæssig og systematisk overvågning af registrerede personer eller følsomme oplysninger/oplysninger om strafbare forhold, *skal* virksomheden udpege en databeskyttelsesrådgiver.

Det er en god idé for alle virksomheder at foretage en skriftlig vurdering af, hvorvidt virksomheden er forpligtiget til at udpege en databeskyttelsesrådgiver eller ej. Dette gælder også selvom konklusionen måtte være, at virksomheden ikke er forpligtiget. Grunden hertil er, at en sådan vurdering vil kunne fremvises til Datatilsynet som dokumentation.

*Kilde til betingelserne for udpegning af DPO: Datatilsynets vejledning om databeskyttelsesrådgivere*

**Krav til databeskyttelsesrådgiveren:**

Der er ikke noget krav om, at databeskyttelsesrådgiveren skal have en specifik uddannelse, men der er krav om, at vedkommende har de nødvendige faglige kvalifikationer, der skal til for at løfte opgaven med at bistå virksomheden med databeskyttelsesretlige problemstillinger og opfyldelse af Databeskyttelsesforordningen.

Disse krav til stillingen som databeskyttelsesrådgiver varierer i forhold til kompleksitetsniveauet for behandlingen af personoplysninger, som virksomheden foretager. Nogle virksomheder kan have behov for en databeskyttelsesrådgiver med meget erfaring inden for området, mens andre, ofte mindre virksomheder, kan nøjes med en medarbejder eller en anden, som har mindre erfaring.

Det er aldrig et krav, at en databeskyttelsesrådgiver skal ansættes på fuld tid. Det vil sige, at en intern medarbejder, der er udpeget som databeskyttelsesrådgiver, fortsat kan foretage andre arbejdsopgaver i virksomheden samtidig med, at vedkommende er udpeget som databeskyttelsesrådgiver. En databeskyttelsesrådgivers arbejdstid varierer fra virksomhed til virksomhed, da arbejdstiden afhænger af kompleksiteten og størrelsen på persondatabehandlingen.

Selvom enhver som udgangspunkt kan udpeges som databeskyttelsesrådgiver, er der visse begrænsninger. En databeskyttelsesrådgiver skal være uafhængig og skal være i stand til at rådgive uafhængigt af andres meninger og holdninger. På denne baggrund kan de øverste ansvarlige i en virksomhed eller i en organisation ikke udpeges som databeskyttelsesrådgivere.

**Fælles databeskyttelsesrådgiver**

Virksomheder, der tilsammen udgør en koncern, kan vælge at udpege en fælles databeskyttelsesrådgiver for hele koncernen. Det er dog en forudsætning, at alle dele af koncernen har mulighed for at have adgang til databeskyttelsesrådgiveren.

Dataansvarlige eller databehandlere kan også have en fælles databeskyttelsesrådgiver. Et konsulentfirma kan f.eks. godt agere som databeskyttelsesrådgiver for flere forskellige virksomheder på baggrund af tjenesteydelseskontrakter. Databeskyttelsesrådgiveren skal blot kunne overholde alle forordningens krav til en databeskyttelsesrådgiver.

**Databeskyttelsesrådgiverens opgaver**

Som tidligere beskrevet så er det databeskyttelsesrådgiverens opgave at rådgive den dataansvarlige og hjælpe denne med at overholde alle Databeskyttelsesforordningens krav.

Der er en række af opgaver, som databeskyttelsesrådgiveren som minimum skal varetage og udføre. Der er dog aldrig noget i vejen for allokering af yderligere opgaver til databeskyttelsesrådgiveren.

En af de opgaver, databeskyttelsesrådgiveren som minimum skal varetage, er at meddele og rådgive om databeskyttelse. Dette skal ske til organisationen og/eller virksomheden samt til de ansatte. Databeskyttelsesrådgiveren skal ydermere være tilgængelig for både ansatte og for ledelse, hvis der skulle opstå spørgsmål om virksomheden/organisationens behandling af personoplysninger. Herudover skal databeskyttelsesrådgiveren bidrage med rådgivning, når virksomheden/organisationen skal have foretaget en konsekvensanalyse. Slutteligt skal databeskyttelsesrådgiveren rådgive og meddele om tilfælde af databrud.

En anden opgave, som databeskyttelsesrådgiveren som minimum skal varetage, er at tilse om de databeskyttelsesretlige regler bliver efterlevet i virksomheden/organisationen. Dette indebærer blandt andet at tilse om de interne politikker i virksomheden/organisationen respekteres, at medarbejder og personale undervises i de persondataretlige regler, fordelingen af ansvar osv. Dette betyder ikke, at det er databeskyttelsesrådgiveren, som har det overordnede ansvar for at databeskyttelsesreglerne overholdes i virksomheden og blandt medarbejderne. Selvom databeskyttelsesrådgiveren indtræder i en overvågende position, er det fortsat den dataansvarlige, der har ansvaret for at reglerne efterleves.

Som tidligere nævnt, er det ligeledes databeskyttelsesrådgiveren, der er bindeled til Datatilsynet. Databeskyttelsesrådgiveren skal optræde og samarbejde med Datatilsynet på vegne af virksomheden/organisationen.

**Den dataansvarliges ansvar i forhold til databeskyttelsesrådgiveren**

Den dataansvarlige står med ansvaret for, at databeskyttelsesrådgiveren inddrages rettidigt og tilstrækkeligt vedrørende beskyttelsen af personoplysninger. For at garantere dette, anbefaler Datatilsynet, at der udarbejdes procedurer for dette.

Databeskyttelsesrådgiveren skal inkluderes i alle overordnede beslutninger samt overvejelser vedrørende virksomhedens strategi for at beskytte personoplysninger. Det er dog ikke meningen, at databeskyttelsesrådgiveren skal være med i praktiske eller almindelige driftsopgaver, konkrete vurderinger af f.eks. den registreredes rettigheder, eller i forhold til de enkelte databehandleraftaler. Generelt skal databeskyttelsesrådgiveren ikke inddrages i selve behandlingen af personoplysninger. Databeskyttelsesrådgiveren skal hjælpe med at sætte rammerne for, at virksomheden/organisationen samt dens medarbejder selv kan behandle personoplysninger sikkert og i overensstemmelse med reglerne.

Som virksomhed/organisation er det også et krav, at man stiller tilstrækkelige ressourcer til rådighed for databeskyttelsesrådgiveren. Dette vedrører både faciliteter og arbejdsredskaber, økonomi osv. Derudover er det vigtigt, at databeskyttelsesrådgiveren har adgang til de personoplysninger, som virksomheden/organisationen foretager behandling af.

Det er som tidligere nævnt også et krav, at databeskyttelsesrådgiveren skal fungere som en selvstændig, uafhængig enhed. Databeskyttelsesrådgiveren må derfor ikke gives instrukser om, hvorledes vedkommende skal udføre sine opgaver. Dernæst må databeskyttelsesrådgiveren hverken sanktioneres eller afskediges for at udføre de pågældende opgaver. En usaglig afskedigelse af en databeskyttelsesrådgiver vil udløse en bøde. Databeskyttelsesrådgivere kan på sagligt grundlag afskediges efter de almindelige ansættelsesretlige regler.

Slutteligt må nævnes, at databeskyttelsesrådgiveren skal referere direkte til det øverste ledelsesniveau i virksomheden/organisationen. Almindelige kommandoveje i en virksomhed eller en organisation skal derfor ikke følges. For at sikre, at virksomheden inddrager databeskyttelsesrådgiveren rettidigt og ikke mindst tilstrækkeligt, skal kontakten til databeskyttelsesrådgiveren bestå mellem denne og det øverste ledelsesniveau.