

Databeskyttelsesforordningen



JUSTITSMINISTERIET

Program

1. Forordningen
2. Introduktion
3. Behandlingsregler
4. Den registreredes rettigheder
5. Nye krav
6. Sanktioner
7. Erstatning
8. Datatilsynet
9. Den videre proces



Databeskyttelsesrådgivere



JUSTITSMINISTERIET

Databeskyttelsesrådgiveren

- Ny rolle i medfør af forordningen
- Element i forordningens fokus på ansvarlighed
- En databeskyttelsesrådgiver er en form for databeskyttelsesombudsmand
- Funktionen understøtte, at den dataansvarlige overholder forordningen



Udpegning af en databeskyttelsesrådgiver

- Offentlige myndigheder *skal* altid udpege en databeskyttelsesrådgiver
- I de fleste tilfælde *skal* private virksomheder *ikke* udpege en databeskyttelsesrådgiver



Databeskyttelsesrådgiveren

- Offentlige myndigheder skal altid udpege en databeskyttelsesrådgiver
- Myndigheder som i dansk ret henregnes til den offentlige forvaltning i medfør af forvaltningslovens § 1, 1-2
- Se nærmere vejledningen om databeskyttelsesrådgiver og betænkningen side 569-570



Fælles databeskyttelsesrådgiver

- Myndigheder vil kunne udpege og dele en fælles databeskyttelsesrådgiver
- Fælles databeskyttelsesrådgiver er den situation, hvor databeskyttelsesrådgiveren har ét ansættelsesforhold, men udøver sin funktion for flere selvstændige forvaltningsmyndigheder.
- Herudover vil flere myndigheder kunne "dele" en databeskyttelsesrådgiver. Databeskyttelsesrådgiveren vil her kunne udøve sin funktion fx på baggrund af to deltidskontrakter eller være ansat på en deltidskontrakt hos én myndighed og ansat på baggrund af en tjenesteydelseskontrakt i en anden myndighed eller organisation.



Fælles databeskyttelsesrådgiver

- Det er 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.



Fælles databeskyttelsesrådgiver

- Som følge af kravet om, at udpegelsen 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.



Fælles databeskyttelsesrådgiver

- 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 en databeskyttelsesrådgiver for de enkelte forvaltninger, men vil kunne udpege én databeskyttelsesrådgiver for hele kommunen.



Fælles databeskyttelsesrådgiver

- 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, fx huslejenævnet, ligesom der kan være kommunale organer, 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.



Fælles databeskyttelsesrådgiver

- Flere kommuner vil have mulighed for at dele en databeskyttelsesrådgiver. Som udgangspunkt vil en gennemsnitskommune på omkring 45.000 indbyggere godt kunne dele en databeskyttelsesrådgiver med en anden tilsvarende eller en mindre kommune. Det afgørende er, om databeskyttelsesrådgiveren kan efterleve sin funktion retmæssigt, når funktionen også udøves for andre 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.



Databeskyttelsesrådgiveren

- Skal udpeges pba. sine faglige kvalifikationer, ”navnlig ekspertise inden for databeskyttelsesret og –praksis” samt evne til at udføre opgaverne som databeskyttelsesrådgiver
- Databeskyttelsesrådgiveren kan både være intern og ekstern
- Får en central *rådgivnings-* og *overvågningsrolle* i organisationen. Uddannelse af ledelse og medarbejdere.
- Inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger
- Skal være uafhængig



Hvem i organisationen *må* være databeskyttelsesrådgiver?

- Databeskyttelsesrådgiveren *skal* inddrages rettidigt i ”alle spørgsmål”
- Databeskyttelsesrådgiveren kan ikke være afskåret fra at være en *aktiv del* af overvejelserne og beslutningerne om, hvordan compliance sikres
- Databeskyttelsesrådgiveren kan og skal således inddrages i organisationens *implementering* af de krav, der følger af forordningen
- F.eks. ifm. indkøb af nyt IT-system og formulering af kravspecifikationer til leverandører
- Kan være organisationens *compliance officer*



Hvem i organisationen må *ikke* være databeskyttelsesrådgiver?

- Databeskyttelsesrådgiveren kan ikke samtidigt være *øverste ansvarlig* for organisationens lovlige behandling af personoplysninger
- Dvs. databeskyttelsesrådgiveren kan ikke f.eks. være den *øverste* IT-ansvarlige eller *øverste* HR-ansvarlige i organisationen



Databeskyttelsesrådgiveren er beskyttet mod afskedigelse

- Må ikke afskediges for udførelse af opgaverne som databeskyttelsesrådgiver, jf. artikel 38, stk. 3, 2. pkt.
- Bestemmelsen sigter på en alm. saglighedsbeskyttelse som efter funktionærloven
- Databeskyttelsesrådgiveren vil kunne afskediges på et *sagligt* grundlag efter almindelige arbejdsretlige regler. Overtrædelse af artikel 38, stk. 3, 2. pkt.-beskyttelsen kan medføre bødestraf efter artikel 83, stk. 4, litra a



Fortegnelse over behandlingsaktiviteter, artikel 30



JUSTITSMINISTERIET

Nyt krav om fortegnelse over behandlingsaktiviteter

- Forordningens risikobaserede tilgang og fokus på ansvarlighed ("accountability")
- Ny pligt om at føre fortegnelse over behandlingsaktiviteter
- Erstatte anmeldelsespligten efter de gældende regler



Fortegnelseskravet

- Fortegnelsespligten er en *intern* pligt for dataansvarlige og databehandlere
- Eventuelle tidligere anmeldelser til Datatilsynet kan i vidt omfang genbruges som fortegnelse
- Ingen særlige formkrav til fortegnelsen – udover skriftligt og elektronisk



Fortegnelseskravet

- Eksempel i betænkningen på side 461, hvordan en fortegnelse kan laves
- Kravet er ikke tiltænkt som en ”belastning” og medfører ikke i sig selv et krav om udarbejdelse af større analyser af datastrømme mv.
- Det følger dog som hidtil, at den dataansvarlige skal leve op til princippet om ”dataminimering”, dvs. man må ikke behandle oplysninger unødigt
- Stadig kunne håndtere f.eks. indsigtbegæringer



Brud på sikkerheden



JUSTITSMINISTERIET

Brud på sikkerheden artikel 33

- Databeskyttelsesforordningen lægger op til en ordning i artikel 33, hvorefter der generelt i forhold til alle dataansvarlige som udgangspunkt vil komme til at gælde en forpligtelse om at anmelde brud på persondatasikkerheden til tilsynsmyndigheden.
- Eksempler på brud se betænkningen side 495
- Tidsfrist senest 72 timer



Underretning ved brud på sikkerheden artikel 34

- I artikel 34 fastslås, at når et brud på persondata-sikkerheden sandsynligvis vil indebære en **høj risiko** for fysiske personers rettigheder og frihedsrettigheder, skal den dataansvarlige som udgangspunkt uden unødigt forsinkelse underrette den registrerede om bruddet.
- Suppleres af § 22, stk. 6, i lovforslaget til databeskyttelsesloven



Sanktioner



Bøder til offentlige myndigheder

- Lovforslagets § 41, stk. 6, 2. pkt.;
- Uanset straffelovens § 27, stk. 2, kan offentlige myndigheder og institutioner m.v., som er omfattet af forvaltningslovens § 1, stk. 1 eller 2, straffes i anledning af overtrædelser, der begås ved udøvelse af virksomhed, der ikke svarer til eller kan sidestilles med virksomhed udøvet af private.



Bøder til offentlige myndigheder

- Det følger af databeskyttelsesforordningens artikel 83, stk. 7, at hver medlemsstat – uden at det berører tilsynsmyndighedernes korrigerende beføjelser i henhold til artikel 58, stk. 2 – kan fastsætte regler om, hvorvidt og i hvilket omfang administrative bøder må pålægges offentlige myndigheder og organer, der er etableret i den pågældende medlemsstat.
- Med lovforslaget er det hensigten, at offentlige myndigheder skal kunne straffes efter straffebestemmelsen i lovforslagets § 41, herunder modtage bødeforelæg fra Datatilsynet efter lovforslagets § 42, på samme måde som private aktører.



Bøder til offentlige myndigheder

- Råderummet i artikel 83, stk. 7, hvorefter medlemsstaterne også kan bestemme, ”i hvilket omfang” offentlige myndigheder kan pålægges bøder, anvendes med lovforslaget til forudsætningsvis at angive lavere bødeloft for offentlige myndigheders overtrædelser end dem, der fremgår af forordningens artikel 83, stk. 4-6.
- Indføres bødeloft på 2 eller 4 % af driftsbevillingen dog maksimalt 8 eller 16 mio. kr.



Bøder til offentlige myndigheder

- Der skal ved pålæggelse af bøder til offentlige myndigheder også tages hensyn til myndigheders særlige situation, der består i, at myndigheder – i modsætning til private aktører – efter lovgivningen er pålagt at varetage lovbestemte opgaver, og myndigheder derfor heller ikke uden videre i alle tilfælde blot kan standse en behandling for derved at bringe en eventuel ulovlig tilstand til ophør.



Bøder til offentlige myndigheder

- I den forbindelse skal det endvidere bemærkes, at det ikke er en forudsætning med lovforslaget, at der pålægges bøde ved alle overtrædelser af databeskyttelsesforordningen og loven. Sagens konkrete momenter kan således trække i en formildende retning. Dette betyder, at der ikke nødvendigvis skal komme en bestemt reaktion, herunder en bøde, ved overtrædelser af forordningen og lovforslaget.



Bøder til offentlige myndigheder

- Tilsynsmyndigheden kan således – alt efter omstændighederne – beslutte, at en overtrædelse i første omgang sanktioneres med et påbud, og at der først, hvis påbuddet overtrædes, skrives til bødeforelæg efter lovforslagets § 42 eller til politianmeldelse. I valget af sanktion kan tilsynsmyndigheden således f.eks. lægge vægt på, om der er tale om en forsætlig eller uagtsom overtrædelse, overtrædelsens karakter, alvor og varighed eller eventuelle relevante tidligere overtrædelser, jf. momenterne opregnet i artikel 83, stk. 2.



Datatilsynet



JUSTITSMINISTERIET

Datatilsynet

- Overvåge og håndhæve
- Fremme offentlighedens kendskab til/forståelse af risici, regler, garantier og rettigheder -særlig fokus på aktiviteter rettet mod børn
- Rådgive parlamentet, regeringen mv.
- Fremme dataansvarliges/databehandlers kendskab til deres forpligtelser
- Efter anmodning informere registrerede om udøvelsen af deres rettigheder -og i den forbindelse evt. samarbejde med de andre tilsynsmyndigheder
- Behandle klager fra en registreret/bemyndiget
- Samarbejde med, herunder gennem deling af oplysninger, og yde gensidig bistand til andre tilsynsmyndigheder
- Gennemføre undersøgelser (inspektioner)
- Overvåge den relevante udvikling, hvis indvirkning på databeskyttelse



Datatilsynet

- Vedtage standardkontraktbestemmelser
- Udarbejde liste ifm kravet om en konsekvensanalyse
- Rådgive om visse behandlingsaktiviteter
- Tilskynde til/udtalelse om/godkendelse af adfærdskodekser
- Fremme fastlæggelsen af certificeringsmekanismer og databeskyttelsesmærkninger og –mærker + godkende kriterierne for certificering
- Lave udkast til og offentliggøre kriterierne for + foretage akkreditering af et organ med henblik på at overvåge adfærdskodekser og af et certificeringsorgan
- Bidrage til Det Europæiske Databeskyttelsesråds aktiviteter
- Udføre enhver anden opgave i forbindelse med beskyttelse af personoplysninger.....



Datatilsynet

Beføjelser—artikel 58 og artikel 83, stk. 9

- Undersøgelsesbeføjelser
- Korrigerende beføjelser
- Godkendelses-og rådgivningsbeføjelser
- Indbringe overtrædelser for de judicielle myndigheder og indlede/deltage i retssager
- Evt. yderligere beføjelser i national ret
- Tage skridt til bøder med tilsvarende virkning som administrative bøder



Datatilsynet

Beføjelser

- Offentliggøre udtalelser og afgørelser -§33
- Bestemme, at ansøgninger om tilladelser efter loven og ændringer heri kan eller skal indgives på nærmere angiven måde -§35
- Bødeforelæg i visse sager om overtrædelser (ukomplicerede og uden bevismæssige tvivlsspørgsmål) –i øvrigt afgivelse af udtalelser til politiet (obligatorisk) -§42



Datatilsynet

Sammenhængsmekanisme –artikel 63-67

- Det Europæiske Databeskyttelsesråd
- Vejledende udtalelser og bindende afgørelser
- Bredt anvendelsesområde
- Gyldighedsbetingelse
- Detaljerede procesregler
- Simpelt og/eller kvalificeret flertal
- Kommissionen kan gribe ind



Den videre proces



JUSTITSMINISTERIET

Fremover

- Lovforslag til ny databeskyttelseslov fremsat 25. oktober (L 68)
- 1. behandling 16. november
- Loven skal træde i kraft 25. maj 2018



Vejledninger

- Adfærdskodeks
- Betænkningen vil ikke komme til at stå alene
- Centralt med praktisk anvendelige vejledninger
- Disse vil blive udarbejdet i samarbejde mellem Justitsministeriet og Datatilsynet
- Fokus på eksempler



Vejledninger

- *Generel informationspjece om forordningen* september 2017
- *Databeskyttelsesrådgiver* september 2017
- *Vejledning om overførsler af personoplysninger til 3. lande* september 2017
- *Databehandlere og dataansvarlige* oktober 2017
- *Samtykke* oktober 2017
- *Fortegnelse* november 2017
- *Adfærdskodekser og certificeringsordninger* december 2017
- *Behandlingssikkerhed* december 2017
- *Databeskyttelse gennem design og standardindstillinger* december 2017
- *Konsekvensanalyse* december 2017
- *Cloud computing* december 2017
- *Håndtering af brud på persondatasikkerhed* januar 2018
- *Registreredes rettigheder* januar 2018
- *Vejledning på det ansættelsesretlige område* februar 2018



?



JUSTITSMINISTERIET