FOLKETINGET

**Erhvervsudvalget, Retsudvalget og Europaudvalget**

**EU-konsulenterne**

**EU-note**

**Til:** Udvalgets medlemmer
**Dato:** **8. november 2017**

Kontaktperson:

Julia Ballaschk (3655)

**Nye databeskyttelsesregler for virksomheder**

*Den 25. maj 2018 afløser EU's persondataforordning den danske persondatalov. De væsentligste konsekvenser af forordningen er, at de, der behandler persondata, vil få større forpligtelser. De, hvis data bliver behandlet, får udvidede rettigheder, og de nationale tilsynsmyndigheder får skærpede håndhævelsesmuligheder. Noten sammenfatter og forklarer de vigtigste af forordningens ændringer og nyskabelser og deres retlige konsekvenser for den private sektor.*

Da EU-Kommissionen i 2012 foreslog en helt ny databeskyttelsespakke for flere sektorer, var forventningen intet mindre end en revolution af det persondataretlige område i EU. Databeskyttelseslovgivningen skulle føres ind i det digitale 21. århundred og tage højde for persondatas status som det "nye guld". Under forhandlingerne lagde EU-Kommissionen stor vægt på, at fælles databeskyttelsesregler er en afgørende faktor i etableringen af det digitale indre marked. De vil bane vejen for data-baserede forretningsmodeller og vil kunne markedsføre virksomheder i EU som frontløbere i privatlivs- og databeskyttelse.

Den endeligt vedtagne forordningstekst må dog hellere betegnes som evolution frem for revolution, skønt den indeholder nogle store ændringer. Den største af dem er, at forordningen, der erstatter det eksisterende direktiv, vil virke direkte i alle medlemslande og skal anvendes direkte i sin ordlyd. Dermed etableres en fælles standard for behandlingen af persondata i hele EU.

Derudover videreudvikler forordningen de fleste af de databeskyttelsesprincipper, som er kendt fra direktivet eller den hidtil gældende danske lovgivning. Forordningen indarbejder desuden den seneste retspraksis ved EU-domstolen på persondataområdet. F.eks. gælder forordningen for alle virksomheder, der tilbyder tjenester til EU-borgere, uanset om de befinder sig i EU eller ej.

**Oversigt over de vigtigste ændringer i forhold til virksomheder**

| |
|---|
| ÆNDRING<br>**Udvidet territorial anvendelsesområde.**<br>Forordningen gælder for alle virksomheder, der "effektivt og faktisk" udøver aktiviteter i EU. Uanset om det f.eks. er en filial eller datterselskab. |
| ÆNDRING<br>**Kategorier af persondata**<br>Forordningen præciserer at lokaliseringsdata (metadata), DNA og IP-adresser er personoplysninger. Lovforslaget til databeskyttelsesloven omfatter desuden afdødes personoplysninger. |
| ÆNDRING / NYT<br>**Styrkelse af de registreredes rettigheder**<br>Forordningen styrker bl.a. indsigtsretten og indfører nye regler om dataportabilitet og en udvidet ret til sletning ("retten til at blive glemt"). |
| ÆNDRING<br>**Skærpede regler om samtykke**<br>Forordningen skærper kravene til samtykke. Det er nu virksomheden eller myndigheden (den dataansvarlige), der har bevisbyrden for at samtykke er indhentet. |
| STORE ÆNDRINGER<br>**Dokumentationskrav**<br>Forordningen stiller større krav til virksomheder og myndigheder ift. til at dokumentere deres overholdelse af forordningen. Kravet gælder dog ikke for virksomheder med under 250 ansatte. Dokumentationskravet erstatter i stort omfang anmeldesystemet ved Datatilsynet. |
| NYT<br>**"Privacy by design" og "privacy by default"**<br>Databeskyttelse skal være indbygget i de tekniske systemer, hvor data behandles. Standardindstillinger skal sikre, at kun nødvendige data behandles, og at der kun sker nødvendigt indsamling og opbevaring i forhold til behandlingsformålet (mængde, omfang og periode). |
| NYT<br>**Notifikationspligt ved sikkerhedsbrud**<br>Ved brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring eller ubeføjet adgang til personoplysninger, skal Datatilsynet informeres indenfor 72 timer. |
| NYT<br>**Databeskyttelsesrådgiver ("DPO")**<br>Offentlige myndigheder og virksomheder, der behandler persondata som deres kerneaktivitet, skal have en databeskyttelsesrådgiver (DPO). DPO'en skal involveres i alle spørgsmål, som vedrører beskyttelse af personoplysninger. |

NYT

**Krav til databehandlere**

Databehandlere er de virksomheder eller myndigheder, der behandler personoplysninger på en andens vegne. Forordningen giver nu databehandlere et egentligt selvstændigt ansvar.

ÆNDRING

**Overførsel til tredjelande**

Forordningen indfører nye muligheder for overførsel af personoplysninger til tredjelande på baggrund af godkendte adfærdskodekser og certificeringer.

STOR ÆNDRING

**Bøder**

Overtrædelser af forordningen kan sanktioneres med bøder på et væsentligt højere niveau end hidtil. Bødeniveauet er fastsat op til 10 mio. Euro eller op til 2 pct. af virksomhedens globale, årlige omsætning, afhængig af overtrædelsens art.
I Danmark vil bøderne blive pålagt af domstolene som en strafferetlig sanktion.
Forordningen giver også mulighed for, at offentlige myndigheder kan pålægges bøde for overtrædelser af forordningens regler.

**Generelle ændringer**

Forordningen fastslår, at alle virksomheder, der er etableret i EU, udbyder varer eller tjenester til personer i EU eller overvåger personer i EU, er omfattet af forordningens regler. Dermed ligestiller forordningen i stor grad virksomheder i EU med virksomhederne i tredjelande.
I praksis betyder det, at f.eks. store internationale sociale medie-udbydere vil være omfattet af reglerne. Det samme gælder for e-handelsbutikker, der tilbyder varer i EU eller streamingtjenester, der er målrettet mod europæiske brugere.

Forordningen opdaterer derudover de kategorier af data, der nu falder under forordningens anvendelsesområde. Forordningen præciserer at lokaliseringsdata (metadata) og IP-adresser er personoplysninger. Derudover blev biometriske og genetiske data tilføjede som følsomme oplysninger, når de bliver brugt til entydigt at identificere en person. Følsomme oplysninger nyder en særlig høj beskyttelsesstatus og må kun behandles, når der er givet udtrykkeligt samtykke til det og når behandlingen finder sted til et specifikt formål. De allerede kendte kategorier af følsomme oplysninger er: oplysninger om race eller etnisk baggrund, politisk, religiøs, eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, helbredsforhold eller seksuelle forhold.

*En IP-adresse kan sammenlignes med et telefonnummer for computere.*

*Biometriske data er oplysninger, der relaterer sig til de fysiske eller adfærdsmæssige karakterer hos en person (f.eks. fingeraftryk eller bevægelsesmønster).*

I praksis er betydningen af udvidelsen af datakategorier begrænset, da forordningen faktisk blot kodificerer de seneste års retspraksis ved EU-Domstolen og den Europæiske Menneskerettighedsdomstol. Man kan dog argumentere, at den nøje adskillelse mellem personoplysninger og følsomme oplysninger

og de dermed forbundne forpligtelser har fået tilføjet en monetær værdi ud over den retlige forpligtelse: Dataansvarlige, der ikke opfylder forpligtelsen kan i fremtiden idømmes betydelig straf.

**Styrkede rettigheder for registrerede**

Persondataloven giver allerede de personer, hvis data indsamles og behandles (de registrerede) en række rettigheder og mulighed for en vis selvbestemmelse. Forordningen opretholder og styrker alle hidtil gældende rettigheder og tilføjer tre nye – retten til at blive glemt, retten til begrænsning og retten til dataportabilitet.

*Ret til sletning ("retten til at blive glemt")*
Forordningen forpligter den dataansvarlige til at slette oplysninger, hvis de ikke længere er nødvendige, eller hvis behandlingen er ulovlig eller sletningen lovpligtig. Retten til sletning kræver en proaktiv tilgang fra den dataansvarlige, der ikke kun skal reagere på henvendelser fra registrerede, men selv skal slette oplysningerne, hvis betingelserne er opfyldte.

*Ret til at begrænse behandlingen*
Forordningen indfører en ny ret til at begrænse behandlingen af personoplysninger i den periode, fra den registrerede har gjort indsigelse mod behandlingen og til indsigelsen kontrolleres. I denne periode må den dataansvarlige kun opbevare oplysningerne, men må ikke behandle dem.

*Ret til dataportabilitet*
Retten indebærer, at den registrerede kan få sine data udleveret og overført i et struktureret, maskinlæsbart format, så den registrerede kan gå til en anden dataansvarlig og anvende sine oplysningerne der. EU-Kommissionen fremhæver, at retten til dataportabilitet bl.a. skal styrke små entreprenørvirksomheder, hvis kunder får mulighed for at tage deres data med, når de vil skifte udbyder.

*Samtykke og børns samtykke*
Ligesom med de andre rettigheder for registrerede pålægger forordningen bevisbyrden for, at den registrerede har givet sit samtykke til behandlingen nu den dataansvarlige eller databehandleren. Derudover skal samtykke gives skriftligt og formuleringen skal være letforståelig, i et klart og enkelt sprog, og teksten skal adskille sig fra den øvrige tekst.

For første gang indeholder databeskyttelsesforordningen særlige regler for børn. Det betyder bl.a. at hvis en tjeneste er rettet mod børn, skal samtykketeksten formuleres på en måde, så børn kan forstå den. Der gælder specielle

regler for informationssamfundstjenester. Det er tjenester, der normalt ydes mod betaling og som formidles elektronisk. Her er det kun barnets forældre, der kan give samtykke eller skal godkende barnets samtykke.

Sammenfattet medfører de styrkede rettigheder for registrerede nye krav til virksomheder: Bevisbyrden for, at der blev indhentet samtyke, ligger nu hos den, der indsamler persondata. Derudover er det blevet indført skarpe tidsfrister (1 måned) for at opfylde indsigtsretten, og i udgangspunktet skal opfyldelsen af de registreredes rettigheder være gratis.
Det skal dog huskes, at det fortsat kun vil være et begrænset antal personer, der vil gøre brug af deres rettigheder. Bortset fra oplysningspligten er alle nuværende og fremtidige rettigheder betinget af en anmodning fra den registrerede. Denne forudsætningen om initiativ indebærer, at det kun er en mindre del af de registrerede, der faktisk udnytter rettighederne.

**Privacy by design og Privacy by default**

Forordningen indfører to nye principper i dansk persondatalovgivning. Nemlig ”databeskyttelse gennem design” og ”databeskyttelse gennem standardindstillinger”. De to principper går ud på, at der skal træffes passende tekniske og organisatoriske foranstaltninger, som understøtter databeskyttelsesprincipperne. Beskyttelsen af personoplysningerne skal være udgangspunktet i forbindelsen med behandlingen og være reglen, i stedet for et tilvalg.

I praksis betyder det eksempelvis, at systemerne skal opbygges sådan, at de automatisk sletter oplysningstyper eller begrænser adgangsrettigheder for brugerne. Det er dog ikke klart, om forordningen kræver at principperne også skal implementeres i eksisterende systemer – især ældre it-systemer kan blive dyre at opruste. Justitsministeriet vurderer i sin betænkning til forordningen, at ældre it-systemer ikke skal re-designes, hvis der kan træffes organisatoriske sikkerhedsforanstaltninger, der er tilstrækkelige.

Forordningen lægger desuden op til, at tilsynsmyndighederne kan udarbejde certificeringsordninger, der kan anvendes som et element i dokumentationen for privacy by design og privacy by default. Det vil således være muligt, at certificere en software eller it-løsning. Hensigten af forordningen er, at dataansvarlige og databehandlere kan opfylde forordningens krav om sikkerhedsforanstaltninger ved indkøb eller brug af disse certificerede løsninger.

**Databeskyttelsesrådgiveren (DPO)**

Et af de krav, der har vakt størst bekymring i det danske erhvervsliv, er kravet om udnævnelsen af en databeskyttelsesrådgiver (DPO). Advokatbranchen har derimod glædet sig over nye jobmuligheder for jurister med en speciale i databeskyttelsesret.

Mens alle offentlige myndigheder forpligtes til at udpege en DPO, skal den private sektor i de fleste tilfælde ikke have en DPO. Forordningens regler er dog ikke helt entydige. Generelt lister forordningen to tilfælde, hvornår en privat virksomhed skal udpege en databeskyttelsesrådgiver:

- Når virksomhedens kerneaktivitet består i behandling af personoplysninger, som kræver regelmæssig og systematisk overvågning af registrerede i stort omfang, eller
- Når virksomhedens kerneaktivitet består i behandling af følsomme oplysninger eller oplysninger om strafbare forhold i stort omfang.

Det er muligt for national lovgivning at stille krav om, at virksomheder udpeger en databeskyttelsesrådgiver i andre tilfælde end de nævnte. Regeringens lovforslag til databeskyttelsesloven indeholder ikke flere krav.

*Databehandling som kerneaktivitet*
Hvis en virksomheds produkt eller tjeneste direkte består i behandling af personoplysninger, betegnes denne behandling som kerneaktivitet. Det samme gælder for virksomheder, hvis produkt eller tjeneste er uløseligt forbundet med behandlingen af personoplysninger.

Eksempler på virksomheder, der skal udpege en DPO, er således:

- Et hospital, der ikke kan yde sundhedspleje uden at behandle sundhedsdata. Derfor er databehandlingen en kerneaktivitet.
- Et privat vagtselskab, der overvåger private indkøbscentre og det offentlige rum. Overvågningen er virksomhedens kerneaktivitet og er uløseligt forbundet med behandling af persondata.

Virksomheder, der blot betaler løn til deres ansatte, skal ikke ansætte en DPO, da det betragtes som støtteaktivitet. Det samme gælder for virksomheder, der behandler kundeoplysninger i forbindelse med kontakt, support og salg mv.

*Databehandling i et stort omfang*
Forordningen definerer ikke, hvor stort et omfang databehandlingen skal udgør i en virksomhed, før en virksomhed er forpligtet til at ansætte en DPO. I

sin betænkning om databeskyttelsesforordningen definerer Justitsministeriet heller ikke, hvad der skal forstås ved ”i et stort omfang”, men henviser til arbejdet i Art. 29-gruppen, som består af repræsentanter fra de nationale tilsynsmyndigheder. Gruppen anbefaler, at der skal lægges vægt på enten det specifikke antal personer eller som andele af den relevante befolkning. Derudover skal der lægges vægt på omfanget af de oplysninger, der indsamles, tidsperioder og den geografiske udstrækning.

Justitsministeriet vurderer, at behandlingen af patientdata på et hospital kan anses som behandling i stort omfang, mens behandlingen af patientdata i en lægepraksis ikke vil opfylde dette kriterium.

*Regelmæssig og systematisk overvågning*
Regelmæssig og systematisk overvågning omfatter alle former for sporing (tracking) og profilering på internettet. Art. 29-gruppen udtaler desuden, at drift af telekommunikationsnetværk, profilering i forbindelse med risikovurdering (herunder kreditvurdering), lokalitetstracking via applikationer samt adfærdsbaseret annoncering også skal anses som regelmæssig og systematisk overvågning.

For eksempel vil et marketingsfirma, der foretager marketingsundersøgelser, hvor der indgår personoplysninger i et stort omfang, og undersøgelsen er baseret på adfærdsbaseret annoncering, være omfattet af kravet om at udpege en DPO.

Moderniseringsstyrelsen vurderer i sin vejledning om databeskyttelsesrådgivere, at der vil kun være få virksomheder, der faktisk skal udpege en DPO. Forordningen lægger desuden op til, at koncerner har mulighed for at udpege en fælles databeskyttelsesrådgiver for hele koncernen. Andre private dataansvarlige og databehandlere har også mulighed for at udpege en ekstern databeskyttelsesrådgiver, som f.eks. et konsulentfirma.

**Udblik – databeskyttelsesregler i praksis**

Med harmoniseringen af databeskyttelsesreglerne har EU’s medlemslande prøvet at bane vejen for nye forretningsmodeller, der er baseret på behandling og videregivelse af persondata. Ét af formålene med forordningen var, at tage højde for den teknologiske udvikling, men samtidig at sikre en stærk persondatabeskyttelse. Det følgende afsnit ser på to nyere ”teknologier” og deres fremtidige regulering

*Cloud computing og databeskyttelse*
Kendetegnet for cloud computing er, at løsninger afvikles via internettet "i skyen" og ikke på kundens server eller pc. Cloud computing indebærer, at it-løsningen leveres til kunden som en tjeneste i stedet for som et produkt.
Ved anvendelsen af cloud computing overlader kunden (den dataansvarlige) personoplysningerne til behandling hos udbyderen af tjenesten (databehandlereren).

Forordningen forstærker mulighederne for cloud computing og understøtter en videre udbredelse i den private og offentlige sektor. Som noget nyt gør forordningen databehandleren mere synligt i processen og skærper dermed forpligtelserne for cloud-leverandører. Uanset om leverandørerne er placeret i tredjelande, skal de leve op til de samme tekniske og organisatoriske sikkerhedskrav som de dataansvarlige i EU. De kan derudover straffes med bøder, hvis de ikke lever op til kravene.

*Big data og databeskyttelse*
Big data spiller en stor rolle EU's strategi for det digitale indre marked, hvor Kommissionen betragter big data som "en katalysator for økonomisk vækst, innovation og digitalisering i alle økonomiske sektorer og i samfundet som helhed". Samtidig findes der en vis mistillid over for automatisk behandling af data og brugen af algoritmer.

Forordningen afspejler de forskellige holdninger til big data og giver ikke et entydigt svar på, hvordan big data skal håndteres:
Forordningen giver den registrerede ret til "ikke at blive genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende". Samtidig har personer ret til at vide, hvorfor deres persondata bliver brugt og har ret til at have adgang til deres data og rette forkerte oplysninger. Det kan give nogle udfordringer, for virksomheder, der arbejder med big data, da værdien af big data nogle gange først vises, når data er blevet indsamlet, og databehandleren ikke altid ved, hvordan data kan blive brugt i fremtiden. En mulig løsning for virksomheder er at bruge anonymisering eller pseudonomisering. Anonyme data er per definition ikke personhenførbar og er dermed ikke omfattet af forordningens anvendelsesområde. Derudover indeholder forordningen visse undtagelser fra individuelle rettigheder, hvis data bliver indsamlet til statistiske, videnskabelige eller historiske formål.

*Begrebet "big data" dækker grundlæggende over de værktøjer og processer, der skal bruges, for at man kan håndtere og udnytte ekstremt store datamængder. Big data bliver f.eks. brugt af danske supermarkeder for at forudsige hyppigheden af børnefamiliers indkøb eller af medicinalvirksomheder for at forudsige, i hvilke lande der vil være brug for diabetesmedicin.*

*Profilering betegner den algoritmiske logisk slutning, der drages af data om et individ og er det primære værktøj, der bruges for at analysere big data.*

**Sammenfatning**

Med sine 173 indledende betragtninger og 99 artikler er forordningen et omfattende og kompliceret regelværk, der alligevel ikke vælter den hidtil kendte persondatalovgivning.
De største forandringer, forordningen medfører, er reguleringsformen som forordning og dermed direkte virkende lovgivning, kravet om udpegelsen af en databeskyttelsesrådgiver, det øgede dokumentationskrav og de betydelig hårdere sanktioner.

Virksomheder, der allerede lever op til de nuværende regler, vil storset kunne fortsætte, som de gør og eventuelt undersøge, om de skal udpege en databeskyttelsesrådgiver. De virksomheder, der har stolet på de hidtil lave bøder i Danmark, venter en større revisionsopgave, hvor der skal indhentes et 20 års fremspring. Det bliver dyrt og besværligt, men konsekvenserne for ikke at leve op til kravene kan blive endnu dyrere – nemlig op til 70 mio. kr.