ERHVERVSSTYRELSEN

JUSTITSMINISTERIET

DIGITALISERINGSSTYRELSEN

DATATILSYNET

Databeskyttelses-forordningen

En introduktion til de kommende, nye regler om beskyttelse af personoplysninger

Oktober 2017

Indhold

1.0 Forord

Formålet med denne vejledning er at give en første introduktion til de nye databeskyttelsesregler, som fra den 25. maj 2018 afløser persondataloven, som har været gældende herhjemme siden 1. juli 2000. De nye regler findes først og fremmest i en forordning, som blev endelig vedtaget i april 2016, og som officielt hedder: Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger mv. (databeskyttelsesforordningen).

Denne vejledning beskriver reglerne i hovedtræk. Hvis du vil læse den fuldstændige forordningstekst, kan du finde link til den på Datatilsynets hjemmeside, www.datatilsynet.dk.

Databeskyttelsesforordningen består af 11 kapitler:

- Kapitel 1 (artikel 1-4) i forordningen vedrører forordningens formål, anvendelsesområde og definitioner.
- Kapitel 2 (artikel 5-11) indeholder en bestemmelse med en række grundlæggende principper, som altid skal iagttages, når personoplysninger behandles, ligesom det fastslår under, hvilke betingelser behandling af personoplysninger må finde sted.
- Kapitel 3 (artikel 12-23) omhandler de registreredes rettigheder.
- Kapitel 4 (artikel 24-43) indeholder bl.a. bestemmelser om den dataansvarliges og databehandlerens generelle forpligtelser og regler om, at der skal være passende sikkerhedsforanstaltninger bl.a. mod, at uvedkommende får adgang til personoplysninger.
- Kapitel 5 (artikel 44-50) vedrører overførsel af personoplysninger til lande mv. uden for EU.
- Kapitel 6 og 7 omhandler de uafhængige tilsynsmyndigheder og deres indbyrdes samarbejde.
- Kapitel 8 indeholder regler om retsmidler, ansvar og sanktioner.
- Kapitel 9 indeholder bestemmelser om specifikke behandlingssituationer.
- Kapitel 10 (artikel 92-93) tager stilling til spørgsmålet om gennemførelsesbeføjelser og udvalgsprocedure.
- Kapitel 11 (artikel 94-99) indeholder en række afsluttende bestemmelser.

Mange af databeskyttelsesforordningens begreber, principper og regler er kendt fra den nuværende persondatalov. Forordningen indeholder imidlertid også en række nyskabelser, der har til formål at styrke beskyttelsen af personoplysninger.

Den 24. maj 2017 offentliggjorde Justitsministeriet betænkning nr. 1565 om databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning. Betænkningen er udformet i samarbejde med samtlige ministerier, Datatilsynet, Digitaliseringsstyrelsen og Erhvervsstyrelsen. Betænkningen giver svar på en lang række spørgsmål og danner samtidig grundlag for det videre arbejde med lovforslag og vejledninger. Der vil således i den kommende tid blive udsendt en række vejledninger – opdelt i temaer - om forståelsen af forordningen.

Betænkningen, der falder i to dele og består af tre bind, kan rekvireres hos Schultz http://jm.schultzboghandel.dk/.

Justitsministeriet har på baggrund af betænkningen endvidere den 7. juli 2017 sendt et lovforslag til en ny persondatalov i høring. Lovforslaget forventes fremsat i Folketinget til efteråret. Denne vejledning vil blive fulgt op med en anden vejledning i løbet af foråret 2018, når ovennævnte lovforslag er endelig vedtaget.

Hvis du ønsker yderligere oplysninger om reglerne i databeskyttelsesforordningen, er du velkommen til at kontakte Datatilsynet.

2.0 Hvornår gælder forordningen?

Databeskyttelsesforordningen gælder for behandling af oplysninger om personer, dvs. fysiske personer, som foretages af offentlige myndigheder og af private virksomheder, foreninger, mv.

Begrebet "fysisk person" omfatter ikke kun et menneskeligt individ, men også enkeltmandsvirksomheder. Dette skyldes, at det i praksis ikke er muligt at skelne mellem oplysninger om ejeren som individ og oplysninger om virksomheden. Oplysninger om andre typer af virksomheder, f.eks. et A/S eller et ApS, er til gengæld ikke beskyttet af databeskyttelsesforordningen. Det samme gælder oplysninger om myndigheder.

Forordningen finder anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk behandling, og på anden ikke-automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register. Det er nemlig, når personoplysninger bruges på en måde, som gør dem let og hurtigt søgbare, at interessen for at beskytte dem aktualiseres.

Behandling af personoplysninger med henblik på aktiviteter, der falder uden for EU-retten mv., som f.eks. statens sikkerhed, er ikke omfattet af forordningen. Det samme gør sig gældende i forhold til myndigheders behandling af personoplysninger inden for det strafferetlige område. I sidstnævnte tilfælde finder Europa-Parlamentets og Rådets direktiv (EU) 2016/680 (retshåndhævelses-direktivet) anvendelse. Direktivet er gennemført i dansk ret ved lov nr. 410 af 27. april 2017.

Privatpersoners behandling af personoplysninger er i mange tilfælde også helt undtaget fra forordningen. Forordningen gælder således ikke for behandling af personoplysninger, som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter. Det vil sige, at de ikke har forbindelse med en erhvervsmæssig eller kommerciel aktivitet. Sådanne aktiviteter kan omfatte korrespondance og føring af en adressefortegnelse og i et vist omfang også sociale netværksaktiviteter og onlineaktiviteter.

I Danmark gælder databeskyttelsesforordningen som hovedregel, hvis

- den dataansvarlige myndighed eller virksomhed m.v. er etableret i Danmark, og
- behandlingen af personoplysningerne foregår inden for EU's område,

eller hvis der foretages behandling af oplysninger om personer, der befinder sig i Danmark, hvis behandlingen vedrører

- udbud af varer eller tjenester til personer, der befinder sig i Danmark, eller
- der foretages overvågning af personers adfærd, hvis denne adfærd finder sted i Danmark.

I langt de fleste tilfælde vil en behandling af personoplysninger, som foregår i Danmark, være omfattet af den danske lovgivning, dvs. forordningen og eventuelle relevante danske særregler. Men der kan være situationer, hvor den dataansvarlige er etableret i et andet EU-land. I så fald vil det være lovgivningen i dette land, der gælder. Det betyder, at f.eks. Facebooks aktiviteter er reguleret af irsk lovgivning, fordi Facebook har sit europæiske domicil i Irland. Hvis sådanne forhold giver anledning til tvivl, kan Datatilsynet hjælpe.

Bemærk, at de andre EU-lande har gennemført eller er ved at gennemføre lignende supplerende lovgivning som i Danmark som følge af de mange steder i forordningen, hvor der er åbnet op for, at dette er en mulighed.

Dataansvarlig

Typisk en virksomhed, offentlige myndighed eller andet organ, der – alene eller sammen med andre – afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.

Databehandler

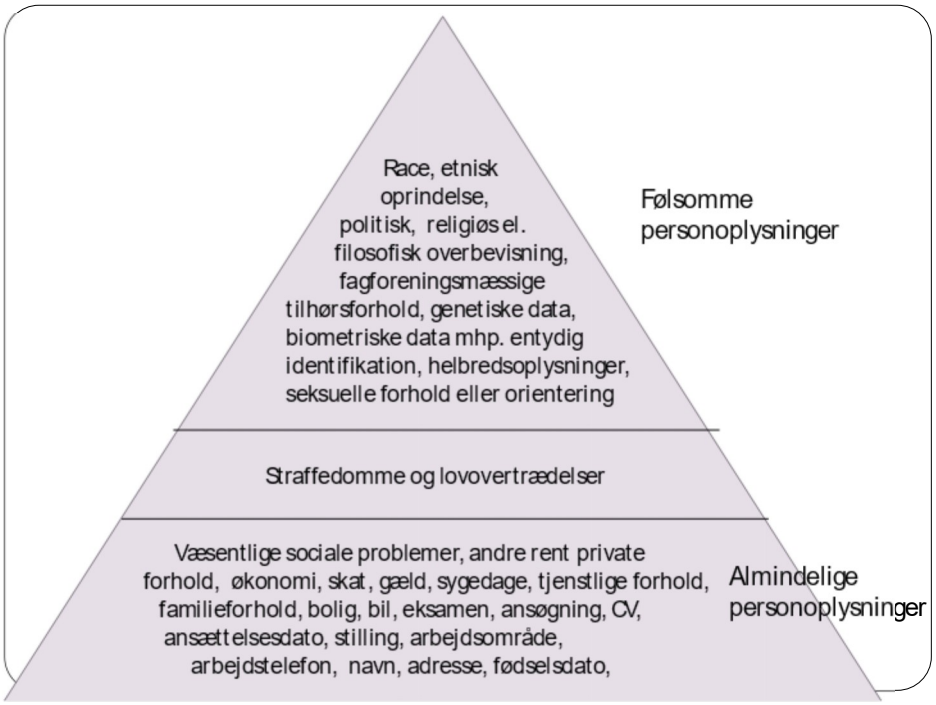
Typisk en virksomhed, offentlig myndighed eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne og efter instruks fra den dataansvarlige.

3.0 Hvad er en personoplysning?

Personoplysninger er enhver form for information, der kan henføres til bestemte personer, også selv om dette forudsætter kendskab til et personnummer, registreringsnummer eller lignende. Også oplysninger i form af f.eks. et billede eller et fingeraftryk er personoplysninger.

Selv om oplysninger som et navn eller en adresse er erstattet af en kode, er det stadig en personoplysning, hvis koden kan føres tilbage til den oprindelige personoplysning. F.eks. er oplysninger, der er krypteret, fortsat personoplysninger, så længe der er nogen, der kan gøre oplysningerne læsbare og identificere de personer, det drejer sig om.

Forordningen sondrer mellem følsomme og almindelige personoplysninger.



Figur 1: En anden måde at se de forskellige kategorier af personoplysninger på. Jo højere oppe i trekanten oplysningerne er, desto strengere betingelser for at behandle dem.

3.1 Følsomme personoplysninger

Oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering. Det er kun de oplysninger, der er nævnt her, der anses for følsomme oplysninger i forordningen.

3.2 Almindelige personoplysninger

De personoplysninger, der ikke falder ind under kategorien ”følsomme personoplysninger”, kan kaldes ”almindelige personoplysninger”. Almindelige personoplysninger kan f.eks. være identifikationsoplysninger som f.eks. navn og adresse, oplysninger om økonomiske forhold, kundeforhold eller andre lignende ikke-følsomme oplysninger.

3.3 Oplysninger om strafbare forhold

Oplysninger om strafbare forhold kan være en oplysning om, at en person har begået en bestemt lovovertrædelse, men det kan også f.eks. være en oplysning om, at en person har adresse i et fængsel. Med andre ord er der tale om en oplysning om strafbare forhold, hvis det ud fra oplysningen kan udledes, at en person har begået noget strafbart. Regler om behandling af oplysninger om strafbare forhold fremgår ikke af forordningen, men vil blive fastsat i de enkelte lande.

3.4 Oplysninger om CPR-nummer

Regler om behandling af nationalt identifikationsnummer (i Danmark CPR-nummer) fremgår ikke af forordningen. Forordningen giver de enkelte lande mulighed for selv at fastsætte regler herom.

3.5 Klageadgang

Hvis man er utilfreds med den måde, ens personlige oplysninger er blevet behandlet på, kan man klage til Datatilsynet, som derefter undersøger sagen og træffer en afgørelse.

4.0 Hvad er behandling af personoplysninger?

Begrebet ”behandling” omfatter enhver form for håndtering af personoplysninger. Det er først og fremmest elektronisk behandling af oplysninger, der er omfattet af reglerne. Det kan f.eks. være indsamling, registrering, systematisering, opbevaring, søgning, brug, videregivelse eller sletning af oplysninger.

Det betyder bl.a., at en virksomhed, der stiller en server til rådighed, som oplysningerne opbevares på, også foretager en behandling af oplysningerne ved at opbevare dem.

Behandling kan også være offentliggørelse af oplysninger på en hjemmeside eller registrering af oplysninger i et elektronisk sags- og dokumenthåndteringssystem.

Forordningen indeholder 26 definitioner af en række af forordningens centrale begreber. Visse af begreberne er nyskabelser; andre enten svarer til eller er ændrede i forhold til den indholdsmæssige betydning, de har i dag. De to helt centrale begreber fra forordningen, som er gennemgået ovenfor (”personoplysning” og ”behandling”), hører til i gruppen af begreber, hvor forordningens definitioner i vidt omfang svarer til, hvad der er gældende ret i dag. Det samme gør sig gældende med begreberne ”dataansvarlig” og ”databehandler”.

5.0 Hvornår må man behandle personoplysninger?

Reglerne for, under hvilke betingelser offentlige myndigheder og private virksomheder, foreninger m.v. må behandle personoplysninger, er i vidt omfang skønsmæssige. Det vil derfor ofte afhænge af en konkret vurdering i den enkelte situation, om betingelserne for at behandle personoplysninger er opfyldt. Er man i tvivl, kan man søge råd hos Datatilsynet. Når en offentlig myndighed eller en privat virksomhed m.v. behandler personoplysninger, er der nogle generelle og grundlæggende principper, som altid skal være opfyldt. Reglerne giver ikke i sig selv nogen ret til at behandle personoplysninger, men hvis en behandling kan finde sted på grundlag af en af de øvrige regler i loven, skal de grundlæggende principper altid være opfyldt.

De grundlæggende principper er:

5.1 Lovlighed, rimelighed og gennemsigtighed

Den dataansvarlige skal overholde reglerne for behandling af oplysninger og skal give let tilgængelig information om behandlingen af oplysninger. Det indebærer bl.a., at den person, der behandles oplysninger om, som udgangspunkt skal have oplyst, hvem der er ansvarlig for behandlingen af oplysninger, og hvad der er formålet med behandlingen.

5.2 Formålsbegrænsning

Når der indsamles oplysninger, skal den dataansvarlige gøre sig klart, hvilke formål oplysningerne indsamles til, og det skal være saglige formål. Man må ikke indsamle oplysninger med den begrundelse, at det måske senere kan vise sig nyttigt at være i besiddelse af oplysningerne. Det er i første omgang den virksomhed eller myndighed mv., der indsamler oplysninger, som skal vurdere, om en bestemt indsamling af oplysninger er saglig. Det kan bl.a. bedømmes ud fra, om indsamlingen sker i forbindelse med løsningen af en opgave, som det er naturligt for virksomheden eller myndigheden at løse.

5.3 Dataminimering

Behandlingen af personoplysninger skal begrænses til det, der er nødvendigt for at opfylde formålet.

5.4 Rigtighed

Oplysningerne skal være rigtige og ajourførte, og hvis oplysningerne viser sig at være urigtige, skal de som udgangspunkt slettes eller berigtiges.

5.5 Opbevaringsbegrænsning

Personoplysninger skal slettes eller gøres anonyme, når det ikke længere er nødvendigt for den dataansvarlige at have oplysningerne. Det er i første omgang op til den enkelte dataansvarlige at vurdere, hvor længe det er nødvendigt at opbevare oplysningerne ud fra det formål, som oplysningerne oprindelig blev indsamlet til.

5.6 Integritet og fortrolighed

Oplysninger skal beskyttes mod uautoriseret eller ulovlig behandling, ligesom det skal sikres, at oplysninger ikke går tabt eller bliver beskadiget.

Forordningen indeholder en række regler om, hvornår man må indsamle og registrere personoplysninger, videregive dem osv. Også andre regelsæt end forordningen kan indeholde regler om, at en behandling af personoplysninger kan eller skal finde sted. Hvilke regler man skal følge i den enkelte situation, afhænger af oplysningernes karakter og formålet med databehandlingen.

Samtykke er ofte anvendt som grundlag for at kunne behandle personoplysninger, og andre eksempler på lovligt behandlingsgrundlag kan være, at det er nødvendigt for at opfylde en aftale, f.eks. for at ekspedere en ordre, eller fordi det er en del af den offentlige myndighedsudøvelse, f.eks. i forbindelse med skatteansættelse.

Samtykke

I mange tilfælde vil man kunne give samtykke til behandling af personoplysninger, uanset hvilke oplysninger det drejer sig om.

En anmodning om samtykke skal være let tilgængelig og forståelig og være i et klart og enkelt sprog.

Der behøver ikke at være tale om et skriftligt samtykke, men den dataansvarlige skal kunne bevise, at der er givet samtykke.

Et samtykke kan til enhver tid trækkes tilbage. Herefter må den dataansvarlige ikke længere behandle oplysninger på grundlag af samtykket, men i nogle tilfælde kan der være et andet behandlingsgrundlag, f.eks. myndighedsudøvelse.

Inden man giver samtykke, skal man have oplysning om, at samtykket kan trækkes tilbage. Det skal være lige så let at trække samtykket tilbage som at give det.

Ved udbud af informationssamfundstjenester til **børn** gælder der særlige regler om samtykke.

Det er vigtigt at være opmærksom på, at begrebet "behandling" dækker over en række forskellige måder at håndtere personoplysninger på. Har man ret til at foretage én bestemt form for databehandling – f.eks. indsamling – af oplysninger, medfører det ikke automatisk, at man også har ret til at foretage andre former for behandling – f.eks. videregivelse – af de samme oplysninger. Normalt giver det ikke anledning til tvivl, at når en offentlig myndighed eller privat virksomhed må indsamle bestemte oplysninger, så må den også systematisere, registrere, bruge og slette dem. Men det er f.eks. ikke uden videre givet, at oplysningerne også må videregives til andre. Dette skal vurderes særskilt på baggrund af reglerne om behandling.

6.0 De registreredes rettigheder

Databeskyttelsesforordningen indeholder i kapitel 3 regler, som giver den enkelte registrerede en række rettigheder over for de myndigheder, virksomheder, foreninger m.v., som behandler oplysninger om den pågældende. Reglerne har til formål at styrke den enkelte persons retsstilling, bl.a. ved at skabe åbenhed omkring behandlingen af oplysninger og ved at give registrerede personer adgang til at gøre indsigelse over for nærmere bestemte former for behandling af oplysninger

De vigtigste rettigheder er:

- Retten til at modtage oplysning om en behandling af sine personoplysninger (oplysningspligt)
- Retten til at få indsigt i sine personoplysninger (indsigtsret)
- Retten til at få urigtige personoplysninger berigtiget (retten til berigtigelse)
- Retten til at få sine personoplysninger slettet (retten til at blive glemt)
- Retten til at gøre indsigelse mod at personoplysninger anvendes til direkte markedsføring
- Retten til at gøre indsigelse mod automatiske individuelle afgørelser, herunder profilering
- Retten til at flytte sine personoplysninger (dataportabilitet)

For alle rettighederne gælder, at når en myndighed eller virksomhed mv. opfylder dem, skal det ske i en kortfattet, letforståelig og lettilgængelig form og i et klart og enkelt sprog. Det gælder særligt, hvis oplysningerne er specifikt rettet mod et barn. Hvis en person henvender sig til den dataansvarlige og f.eks. beder om indsigt, berigtigelse, sletning, mv. af oplysninger, skal den pågældende hurtigst muligt – og normalt senest efter en måned – have besked om, hvad der vil blive gjort som følge af henvendelsen.

Om nogle af rettighederne kan særligt fremhæves følgende:

6.1 Ret til at få besked om, at der behandles personoplysninger (oplysningspligt)

Den enkelte registrerede skal som udgangspunkt have besked om, at der behandles oplysninger om den pågældende. Man skal bl.a. have besked om, hvem der er dataansvarlig, om formålet med behandlingen, om eventuelle modtagere af oplysningerne, mv.

6.2 Ret til at se oplysninger (indsigtsret)

Den registrerede kan bede om at få at vide, hvilke oplysninger om den pågældende selv, som en myndighed eller virksomhed mv. behandler. Hvis den registrerede beder om det, skal der også gives en udskrift eller kopi af oplysningerne.

6.3 Ret til at få oplysninger rettet eller slettet (retten til at blive glemt)

Hvis der behandles forkerte oplysninger om en person, kan den pågældende bede om at få oplysningerne rettet. Desuden har man i visse tilfælde ret til at få personoplysninger slettet. Det kan f.eks. være, hvis oplysningerne ikke længere er nødvendige til at opfylde de formål, hvortil de blev indsamlet, hvis et samtykke, som er nødvendigt for behandlingen, trækkes tilbage eller hvis behandlingen er ulovlig.

6.4 Ret til at transmittere oplysninger (dataportabilitet)

Den registrerede har ret til at modtage personoplysninger om sig selv i et struktureret, almindeligt anvendt og maskinlæsbart format og har ret til at transmittere oplysningerne til en anden myndighed eller virksomhed. Den registrerede kan også bede om at få oplysningerne sendt direkte fra den dataansvarlige til en anden myndighed eller virksomhed.

6.5 Begrænsninger i rettigheder

I særlige situationer gælder de almindelige rettigheder ikke. Det kan f.eks. skyldes hensyn til den offentlige sikkerhed, hensyn til efterforskning eller tilsyn, eller forretningshemmeligheder og andre hensyn til private interesser. Endvidere er de enkelte rettigheder i visse tilfælde begrænset. Som eksempler kan nævnes, at oplysningspligten under visse omstændigheder kan begrænses af ressourcemæssige hensyn, at retten til dataportabilitet ikke gælder behandling, der er nødvendig i forbindelse med offentlig myndighedsudøvelse, og at retten til sletning bl.a. er begrænset i forhold til offentlige myndigheders behandling af personoplysninger.

For nærmere oplysninger om de registreredes rettigheder henvises til Datatilsynets hjemmeside og den vejledning om emnet, der vil blive udarbejdet i begyndelsen af 2018.

7.0 Hvad med behandlingssikkerheden?

For at opretholde sikkerheden og hindre behandling i strid med reglerne om beskyttelse af personoplysninger, bør den dataansvarlige vurdere de risici, som en behandling indebærer, og gennemføre foranstaltninger, der kan begrænse disse risici, f.eks. kryptering.

Behandlingssikkerhed

Brug og håndtering af personoplysninger skal foregå betryggende og med et passende niveau af sikkerhed og privatlivsbeskyttelse. Sikkerhedsniveauet skal afspejle den konkrete risiko for, at oplysningerne stjæles, mistes, skades, eller behandles ulovligt.

Hvis risikoen må antages at være stor, må behandlingen af personoplysninger ikke påbegyndes, før der er gennemført en konsekvensanalyse vedrørende databeskyttelse og eventuelt en høring af Datatilsynet.

Når it-løsninger designes og udvikles, skal databeskyttelse tænkes ind fra starten, og standardindstillinger skal sikre, at der kun behandles de personoplysninger, som er nødvendige i forhold til formålet med behandlingen.

Hvis det går galt, og man som dataansvarlig bliver bekendt med et brud på persondatasikkerheden, skal man uden unødig forsinkelse give besked til Datatilsynet og i visse tilfælde også til de personer, hvis oplysninger er berørt af sikkerhedsbruddet. Databehandlere, som bliver bekendt med et brud på persondatasikkerheden, skal uden unødig forsinkelse underrette den dataansvarlige.

For nærmere oplysninger om reglerne om persondatasikkerhed, databeskyttelse gennem design og standardindstillinger, konsekvensanalyser mv. henvises til Datatilsynets hjemmeside og de vej-ledninger, der vil blive udarbejdet om disse emner. Ved tvivl kan man endvidere altid rette henvendelse til Datatilsynet.

8.0 Andre særlige nyskabelser?

8.1 Fortegnelser over behandlingsaktiviteter

Den pligt, der er efter persondataloven i dag til i visse situationer at foretage anmeldelse til Data-tilsynet, forsvinder med databeskyttelsesforordningen. Der lægges i stedet op til anden ordning, som indebærer, at den dataansvarlige og databehandleren i visse tilfælde skal føre interne fortegnelser over deres behandling af personoplysninger. Dette er i tråd med forordningens risikobaserede tilgang og fokus på ansvarlighed (”accountability”).

I Justitsministeriets betænkning nr. 1565 af 24. maj 2017 om databeskyttelsesforordningen findes på side 461 et eksempel på en fortegnelse hos en dataansvarlig. For nærmere oplysninger om, hvem der skal udarbejde en fortegnelse og indholdet af en sådan henvises endvidere til Datatilsynets hjemmeside og den vejledning, der vil blive udarbejdet.

8.2 Konsekvensanalyser

Virksomheder skal foretage en konsekvensanalyse forud for databehandlinger, som sandsynligvis vil indebære en høj risiko. Formålet med konsekvensanalysen er navnlig at vurdere risikoens oprindelse, karakter, særegenhed og alvor. Det vil bl.a. være relevant at foretage en konsekvensanalyse i tilfælde, hvor nye teknologier anvendes, eller hvor der behandles meget store mængder følsomme personoplysninger.

Analysen skal mindst omfatte:

- systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen,
- en vurdering af, om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene,
- en vurdering af de risici behandlingen indebærer for de personer, der behandles oplysninger om,
- garantier, sikkerhedsforanstaltninger og mekanismer, der skal sikre beskyttelse af personoplysninger og påvise overholdelse af databeskyttelsesforordningen.

For nærmere oplysninger om reglerne om udarbejdelse af en konsekvensanalyse mv. henvises til Datatilsynets hjemmeside og den vejledning, der vil blive udarbejdet herom.

8.3 Databeskyttelsesrådgiver

Offentlige myndigheder og visse private virksomheder skal udpege en såkaldt databeskyttelsesrådgiver, hvad enten de er dataansvarlige eller databehandlere. I de fleste tilfælde skal der i den private sektor ikke udpeges en databeskyttelsesrådgiver. Det er altså kun visse private virk-

somheder, der skal udpege en databeskyttelsesrådgiver. Det vil f.eks. være tilfældet for privathospitaler, større forsikringsselskaber, teleselskaber og marketingsvirksomheder.

For nærmere oplysninger om reglerne om udpegning af en databeskyttelsesrådgiver, hvilke opgaver mv., han/hun skal udføre mv. henvises til Datatilsynets hjemmeside og vejledningen om databeskyttelsesrådgivere.

8.4 Adfærdskodekser, certificering mv.

Med forordningen bliver reglerne om adfærdskodekser mere detaljerede og begrænser sig – i modsætningen til persondataloven – ikke nødvendigvis til private dataansvarlige. Da kodekser nævnes i flere af forordningens bestemmelser om behandlingssikkerhed og den potentielt positive effekt det kan have på administrative bøder, har kodekser potentiale til at få stor betydning fremover.

For at støtte op om den praktiske implementering af forordningen og for at have visse værktøjer, der kan hjælpe dataansvarlige og databehandlere til efterlevelse af forordningen, skal der efter forordningen også tilskyndes til, at der fastlægges certificeringsmekanismer for databeskyttelse og databeskyttelsesmærkninger og -mærker, som tilkendegiver, at en virksomhed lever op til forordningen. Dette skal ske på nationalt og på EU-plan.

For nærmere om adfærdskodekser, certificering mv. henvises til Datatilsynets hjemmeside og de vejledninger, der vil blive udarbejdet herom.

9.0 Overførsel af personoplysninger til lande uden for EU

Forordningen indeholder i kapitel 5 regler om, hvornår personoplysninger kan overføres til lande uden for EU, dvs. såkaldte tredjelande. Disse regler bygger i vid udstrækning på indholdet af de regler, der er på området allerede i dag.

For nærmere om overførsel af personoplysninger til lande uden for EU henvises til Datatilsynets hjemmeside og vejledningen om overførsel af personoplysninger til tredjelande.

10.0 Nye tider for Datatilsynet

Forordningen indeholder mange regler om oprettelse af tilsynsmyndigheder og tilsynsmyndighedernes indbyrdes samarbejde. Forordningen indeholder en væsentlig udbygning af tilsynsmyndighedernes europæiske samarbejde. Der oprettes bl.a. et Europæisk Databeskyttelsesråd, som sammensættes af repræsentanter fra medlemsstaternes tilsynsmyndigheder, og som i visse sager kan træffe afgørelser, som er bindende for de nationale tilsynsmyndigheder.

Når de nye databeskyttelsesregler finder anvendelse fra den 25. maj 2018, fortsætter Datatilsynet med at være den centrale uafhængige myndighed, der fører tilsyn med, at reglerne på området overholdes. Der sker endvidere en udvidelse af Datatilsynets tilsynsbeføjelser, idet tilsynet fremover vil have adgang til lokaler hos alle private dataansvarlige. I dag er Datatilsynets beføjelser i forhold til disse dataansvarlige begrænset til de typer af behandlinger, som er undergivet et krav om forudgående tilladelse.

Datatilsynet udøver allerede i dag – som forudsat i forarbejderne til persondataloven – i første række sin virksomhed gennem generelle retningslinjer og ved en serviceorienteret rådgivning og vejledning. Med forordningen bliver denne opgave større. Datatilsynet skal således ifølge databeskyttelsesforordningen fremme offentlighedens kendskab til og forståelse af risici, regler, garantier og rettigheder i forbindelse med behandling, og der skal – som noget nyt – sættes særligt fokus på aktiviteter, der er direkte rettet mod børn. Datatilsynet skal endvidere fremme dataansvarliges og databehandleres kendskab til deres forpligtelser i henhold til forordningen.

Selvom Datatilsynet allerede nu i et vist omfang – på frivillig basis – har samarbejdet med de andre europæiske tilsynsmyndigheder i enkeltsager, må navnlig databeskyttelsesforordningens regler om den såkaldte ”one-stop-shop-mekanisme” og ”sammenhængsmekanisme” forventes at skabe en ny virkelighed for især tilsynet, men i et vist omfang også for danske virksomheder, der opererer i flere medlemsstater.

Dette skyldes bl.a., at der med ”one-stop-shop-mekanismen” vil komme til at gælde nogle meget detaljerede regler for, hvordan visse grænseoverskridende sager i den private sektor fremover skal behandles. Reglerne indebærer bl.a., at én national tilsynsmyndighed ("den ledende tilsynsmyndighed") vil være enekompetent til – efter en udveksling af forskellige udkast til afgørelser med andre berørte tilsynsmyndigheden i en proces med meget korte svarfrister – at træffe afgørelse i konkrete sager.

De europæiske datatilsyn må indstille sig på at skulle samarbejde om en ensartet anvendelse af forordningen i markant flere sager, end det hidtil er sket på frivillig basis.

Databeskyttelsesforordningen indebærer også, at de europæiske tilsynsmyndigheder fremover er forpligtede til på anmodning fra et andet tilsyn at foretage en ønsket aktivitet. Det kan eksempelvis være indhentning af oplysninger eller gennemførelse af et tilsynsbesøg. Anmodnin-

gen skal besvares inden for en måned, og den må kun afslås, hvis tilsynet ikke har kompetence, eller hvis anmodningen vil stride imod forordningen eller anden ret. Endvidere er der i forordningen regler om, at flere tilsyn kan arbejde sammen med henblik på behandling af visse sager.

Det forudsættes endvidere i forordningen, at det øgede samarbejde blandt de europæiske tilsyn har til formål at harmonisere fortolkningen af databeskyttelsesreglerne i EU.