Ref.: Randi Høj Brarup

Varde Kommune

DEN NYE DATATBESKYTTELSESFORORDNING GENERELT

Den nye persondataforordning træder i kraft den 25. maj 2018. Der er i forordningen hjemmel til, at de enkelte medlemsstater i et vist omfang kan fastsætte egne supplerende regler.

Databeskyttelsesforordningen findes her: http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=celex:32016R0679

Justitsministeriet har udarbejdet betænkning nr. 1565 - Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, bestående af del I og II, på i alt ca. 1.200 sider, hertil kommer vejledninger til selve forordningen udstedt af EU kommissionen http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2017/nye-regler-styrker-beskyttelsen-af-persondata-i-europa

Lovforslaget databeskyttelseslove kan man finder her - http://ft.dk/samling/20171/lovforslag/l68/20171_l68_som_fremsat.htm

KL har lovet at udfærdige en tjekliste for kommunernes arbejde med persondataforordningen, denne tjekliste er endnu ikke modtaget.

Justitsministeriet udarbejder løbende vejledninger. Tidsplan for vejledninger ligger her: http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/plan_for_vejledninger_om_forordningen.pdf

Pt. er der udarbejdet

- vejledning om databeskyttelsesrådgivere September 2017 https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_DPO.pdf
- Vejledning om samtykke https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledning_om_samtykke__formateret_.pdf

Datatilsynet har udfærdiget 12 spørgsmål, som dataansvarlige allerede nu med fordel kan forholde sig til, dokumentet findes her: https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/12_spoergsmaal_-_GDPR.pdf

Artikel 29 gruppen udarbejder løbende guidelines til forordningen:

http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

https://www.datatilsynet.dk/nyheder/nyhed/artikel/vejledninger-fra-artikel-29-gruppen-foreligger-nu-i-endelig-form/

https://www.datatilsynet.dk/nyheder/nyhed/artikel/guidelines-fra-artikel-29-gruppen/

Eksempler på væsentlige ændringer der skal inkorporeres:

1. Øgede dokumentationskrav for overholdelse af personforordningen, som bl.a. omfatter kortlægning af:
   - Hvilke typer data behandles
   - Formålet med behandlingerne
   - Kategorier af registrerede personer og modtagere af oplysninger
   - Eventuelle videregivelser til usikre tredjelande
   - Angivelse af tidsfrister for sletning af oplysninger

2. Pligt til at udarbejde konsekvensanalyser (Privacy Impact Assessments), hvis behandlingen af personoplysninger indebærer høje risici for registreredes rettigheder og friheder. Kravet om konsekvensanalyse vil navnlig kunne aktualiseres, hvor der er tale om:
   - Systematiske profileringsaktiviteter
   - Behandling af følsomme oplysninger
   - Omfattende videoovervågning af offentlige arealer

3. Pligt til at sørge for "privacy by design og by default", dvs. til at tænke databeskyttelse ind fra start ved udviklingen af nye IT-løsninger, services m.v.

4. Pligt til udpegning af en databeskyttelsesansvarlig - "data protection officer"/"DPO" . DPO'en skal have en særlig viden om persondatabeskyttelse og bl.a. sikre, at forordningens regler overholdes i myndighedens daglige drift.

5. En række pligter overfor den personoplysningerne vedrører.

Københavns kommune har igangsat arbejdet. Deres procedure er gennemgået findes på:

http://www.bechbruun.com/-/media/Files/Videncenter/Kursusmateriale/2017+-+DOU+-+VM/Lektion+6+-+spor+3+-+Implementering+af+persondataforordningen+i+Kbenhavns+Kommune.PDF?la=da

Følgende forhold er efter min opfattelse en del af implementeringen:

1. ***Fortegnelse over behandlingsaktiviteter***
2. ***Undersøgelse af om der foreligger databehandler aftaler***
3. ***Udpegning af dataansvarlig på de enkelte områder – kontaktperson til DPOen***
4. ***Uddannelse af personale***
5. ***Undersøgelse af om der foreligger passende tekniske og organisatoriske foranstaltninger for at sikre sikkerhedsniveauet – overholder vi informationsstandarter?***
6. ***Sikre øvrige dokumentationskrav overholdes***
   a. Dok for at kommunens behandling er i overensstemmelse med forordningen og at proceduren følges op.
7. ***Databeskyttelsespolitikker/procedure***

Som led i dokumentationskravet kan det ifølge Kromann Reumert overvejes, at implementere passende procedurer, forholdsregler m.v. Her kan I overveje følgende procedurer/dokumenter:

a) Generel IT-politik

b) Politikker eller retningslinjer for håndtering af personoplysninger – helst pr. type (f.eks. medarbejderdata, kundedata osv.) – som tager stilling til indsamling, løbende behandling, sletning, blokering mv.
c) Procedure for håndtering af opfyldelse af oplysningspligt
d) Politik for håndtering af indsigtsbegæringer, som bør kunne læses af tredjepart
e) Politik for håndtering af de registreredes øvrige rettigheder
f) Håndtering af internationale dataoverførsler
g) Procedure for håndtering af sikkerhedsbrud, herunder også pligten til anmeldelse til Datatilsynet fra den 25. maj 2018
h) Håndtering af databehandleraftaler – hvornår skal disse indgås, standardordlyd mv
i) Vejledning om brug af cloud-baserede løsninger og/eller ydelser fra IT-leverandører i øvrigt
j) Privatlivspolitik til virksomhedens hjemmeside osv

Hertil kommer:

k) Procedure for konsekvensanalyse, hvornår og hvem har ansvaret
l) Procedure for kontrol af overholdelse af privacy by design og standartindstillinger, herunder hvornår det påses, og hvem der er ansvarlig
m) Procedure der sikre, alle databehandlinger identificeres og fortegnelse føres.

KORT GENNEMGANG AF DE VÆSNETLIGE ASPEKTER I FORHOLD TIL IMPLEMENTERING

Dette er ikke udtryk for en tilbundsgående gennemgang, men er alene en gennemgang af de væsentligste aspekter, med det formål at give direktionen et indblik i mange af de processer der er nødvendige for arbejdet med implementering af databeskyttelsesforordningen. Arbejdet med implementeringen vil forudsætte en mere tilbundsgående gennemgang.

KORT OM DATABESKYTTELSESRÅDGIVER /DPO

DPO er beskrevet i forordningens artikel 37-39.

Varde kommune skal have en DPO, senest den 25. maj 2018.

OBS FSVA. Selvejende institutioner - 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. Der vil f.eks. være tale om offentlig virksomhed af mere omfattende karakter, hvis der er tale om virksomhed der traditionelt betragtes som faktisk forvaltningsvirksomhed, såsom undervisning og sygepleje.

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.

Eksempel på selvejende institution der er omfattet:

- Universiteter
- Institutioner hvor kommunalbestyrelsen har indgået overenskomst til opfyldelse af sine forpligtelser efter lov om social service[1]

Fælles DPO

Der er ifølge forordningens art. 37 stk. 3 i et vist omfang mulighed for, at flere offentlige myndigheder kan udnævne en fælles DPO.

Flere kommuner vil i de fleste tilfælde 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 dog, om

[1] Vejledning om databeskyttelsesrådgiver s. 14

man som databeskyttelsesrådgiver kan efterleve sin funktion retmæssigt, når funktionen også udøves for andre kommuner på samme tid.

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.

Det kan på baggrund af ordlyden i artikel 37, stk. 3, antages, at det ikke er "i overensstemmelse med en offentlig myndigheds struktur og størrelse", hvis en fælles databeskyttelsesrådgiver fungerer på baggrund af én ansættelseskontrakt i f.eks. to forskellige kommuner.

I modsætning hertil må det dog antages, at det er i overensstemmelse med bestemmelsens ordlyd, at en databeskyttelsesrådgiver udøver sin funktion på baggrund af to deltidskontrakter i to kommuner på samme tid. Den retlige grænse for at dele en databeskyttelsesrådgiver vil i et sådant tilfælde være de gældende standarder om offentligt ansattes bierhverv og de almindelige habilitetsregler.

Dette må ligeledes antages at gøre sig gældende, når en databeskyttelsesrådgiver har ansættelse i én kommune og er ansat på baggrund af en tjenesteydelseskontrakt i en anden kommune.

Det må endvidere antages, at to eller flere kommuner kan oprette et kommunalt fællesskab, jf. § 60 i lov om kommunernes styrelse, til hvilket de kan gå sammen om at løse opgaven som databeskyttelsesrådgiver i de deltagende kommuner.

Endelig må det antages, at et konsulentfirma kan udøve funktionen som databeskyttelsesrådgiver for flere offentlige myndigheder og/eller organer på samme tid på baggrund af tjenesteydelseskontrakter.[2]

DPO Kvalifikationer og stilling:

Databeskyttelsesrådgiveren udpeges på grundlag af sine faglige kvalifikationer, navnlig ekspertise inden for databeskyttelsesret og -praksis samt evne til at udføre de opgaver, der er omhandlet i artikel 39 jf. art 37.

Der stilles ifølge justitsministeriet ikke krav om bestemt uddannelsesmæssig baggrund, såsom f.eks. jurist, men der sigtes til en person med juridiske kompetencer inden for databeskyttelsesret samt en vis praktisk erfaring. Niveauet afhænger af mængden, følsomheden og kompleksiteten.[3]

Af Artikel 29 gruppens guidelines vedrørende DPO fremgår

"Relevant skills and expertise include:

- *expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR*
- *understanding of the processing operations carried out*
- *understanding of information technologies and data security*
- *knowledge of the business sector and the organisation*
- *ability to promote a data protection culture within the organisation"*[4]

---

[2] Betænkningen del 1 bind 1 fremgår 5.18.3.2

[3] Justitsministeriets besvarelse af FAQ https://erhvervsstyrelsen.dk/sites/default/files/media/praesentation_fra_stormoede_om_databeskyttelsesforordningen.pdf

[4] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Den nærmere fastlæggelse af, hvad der skal forstås ved udtrykket 'ekspertise inden for databeskyttelsesret og -praksis', må endvidere skulle ses i lyset af databeskyttelsesrådgiverens opgaver, der er opregnet i artikel 39. På baggrund heraf må der ved udtrykket antages at sigte mod en person med juridiske kompetencer inden for databeskyttelsesret, som har en vis erfaring med at håndtere sådanne spørgsmål. Niveauet vil afhænge af mængden, følsomheden og kompleksiteten af de oplysninger, der behandles.[5]

Ansatte eller ekstern

Databeskyttelsesrådgiveren kan være den dataansvarliges eller databehandlerens medarbejder eller kan udføre hvervet på grundlag af en tjenesteydelseskontrakt jf. artikel 37 stk. 6.

Databeskyttelsesrådgiveren kan udføre andre opgaver og have andre pligter. Kommunen skal sikrer, at sådanne opgaver og pligter ikke medfører en interessekonflikt jf. artikel 38 stk. 6.

DPO'en kan altså være en eksisterende medarbejder, hvis vedkommende opfylder kravene hertil, eller en ekstern person, der på kontrakt hyres ind til opgaven eksempelvis en advokat eller revisor.[6]

Kommunen skal sikre, at der er tid nok til opgaverne som DPO[7]

Såfremt man udpeger en medarbejder, må der dog ikke være interessekonflikt i forhold til medarbejderens øvrige opgaver for kommunen, hvorfor DPO'en ikke samtidigt kan være øverste ansvarlig for organisationens lovlige behandling af personoplysninger dvs. DPO'en kan f.eks. ikke være den øverste IT ansvarlige eller øverste HR-ansvarlige i organisationen.[8]

Databeskyttelsesrådgiveren er underlagt tavshedspligt eller fortrolighed vedrørende udførelsen af sine opgaver i overensstemmelse med EU-retten eller medlemsstaternes nationale ret jf. artikel 38 stk. 5.

DPOen skal jf. artikel 38 stk. 1 inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger.

DPOen skal altså inddrages i alle de overvejelser og vurderinger, som det forudsættes, at den dataansvarlige eller databehandleren har gjort sig og foretaget med henblik på at overholde forordningens regler og andre relevante EU-retlige og nationale regler om databeskyttelse.

Det vil sige, at databeskyttelsesrådgiveren skal inddrages ved vurderingen af, om de behandlinger af personoplysninger, som foretages eller iværksættes for den dataansvarlige eller databehandleren, overholder reglerne i forordningens kapitel II om de grundlæggende behandlingsprincipper og behandlingsbetingelserne.

Overvejelser og vurderinger af, om behandlingen på baggrund af det udtrykkeligt angivne formål er saglig, proportional eller kræver samtykke fra den registrerede, registreredes rettigheder og overholdelse heraf, fastsættelse af sikkerhedsforanstaltninger, jf. artikel 32, samt passende foranstaltninger, som er designet med henblik på effektiv implementering af databeskyttelsesprincipper, og passende

---

[5] Betænkningen pkt. 5.20.3.2
[6] Betænkningen pkt.5.20.3.3 og Justitsministeriets besvarelse af FAQ https://erhvervsstyrelsen.dk/sites/default/files/media/praesentation_fra_stormoede_om_databeskyttelsesforordningen.pdf

[7] Betænkning pkt. 5.20.3.5
[8] Justitsministeriets besvarelse af FAQ https://erhvervsstyrelsen.dk/sites/default/files/media/praesentation_fra_stormoede_om_databeskyttelsesforordningen.pdf

foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun nødvendige personoplysninger behandles, jf. artikel 25.[9]

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.[10]

Den dataansvarlige skal rådføre sig med databeskyttelsesrådgiveren, når der foretages en konsekvensanalyse vedrørende databeskyttelsen.

Kommunen er forpligtet til at holde DPOen tilstrækkeligt og rettidigt orienteret om alle spørgsmål af relevans vedrørende databeskyttelsesretlige regler.[11]

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.[12]

Uafhængig

Kommunen skal sikrer, at databeskyttelsesrådgiveren ikke modtager instrukser vedrørende udførelsen af sine opgaver. Den pågældende må ikke afskediges eller straffes af kommunen for at udføre sine opgaver.

Databeskyttelsesrådgiveren rapporterer direkte til det øverste ledelsesniveau hos den dataansvarlige eller databehandleren jf. artikel 38 stk. 3. Det vil sige, at DPO'en alene er underlagt byrådet, og nyder en beskyttelse der i vidt omfang svarer sikkerhedsrepræsentanter.[13]

DPOen rapportere direkte til byrådet. Det udelukker dog ikke, at en kommune kan indhente en erklæring fra økonomiudvalget forinden forelæggelsen for kommunalbestyrelsen.[14][15]

Organisatorisk indgår DPOen som en alm del af forvaltningen, og dermed være underlagt et udvalg. Indenrigsministeriet kan dog meddele dispensation til at DPO er direkte under byrådet.[16]

Borgerne/den registrerede kan tage direkte kontakt til DPOen der skal vejlede denne om sine rettigheder

DPO'ens opgaver

Databeskyttelsesrådgiveren har som minimum følgende opgaver jf. art 39:

a) *at underrette og rådgive organisationen og de ansatte, der behandler personoplysninger, om deres forpligtelser i henhold til denne forordning og anden EU-ret eller national ret i medlemsstaterne om databeskyttelse.*

---

[9] Betænkning pkt. 5.20.3.4.1
[10] Vejledningen s. 24
[11] Betænkningen pkt. 5.20.3.4.2
[12] Vejledningen s.26
[13] Betænkningen pkt.5.20.3.6.1
[14] Vejledningen s. 26
[15] Adv. Charlotte Bagger Tranberg fra Bech Bruun – har på et kursus den 1 november 2017 udtalt, at DPOen kan rapportere til direktionen.
[16] Betænkning pkt. 5.20.3.6.1

- Overvejelser og beslutninger om hvordan compliance sikres ved: nyt it system, kravsspecifikation til leverandører, datapolitikker, iværksættelse af behandlinger af personoplysninger, overvejelser om hvorvidt en behandling overholder behandlingsregler, stå til rådighed for leder og organisation fsva. spørgsmål om databeskyttelse, konsekvensanalyse, modtage underretning og rådgive om sikkerhedsbrist.[17]

b) *at overvåge overholdelsen af denne forordning, af anden EU-ret eller national ret i medlemsstaterne om databeskyttelse og af den dataansvarliges eller databehandlerens politikker om beskyttelse af personoplysninger, herunder fordeling af ansvar, oplysningskampagner og uddannelse af det personale, der medvirker ved behandlingsaktiviteter, og de tilhørende revisioner*
   - Overvåge: politikker om databeskyttelse, uddanne personale, oplysningskampagne, fordeling af ansvar, revisioner. (OBS - DPO overtager ikke ansvaret for overholdelse)[18]

c) *at rådgive, når der anmodes herom, med hensyn til konsekvensanalysen vedrørende databeskyttelse og overvåge dens opfyldelse i henhold til artikel 35*
   - Eksempelvis, skal der gennemføres en konsekvensanalyse, sikkerhedsforanstaltninger, er den korrekt gennemført og i overensstemmelse med databeskyttelses regler.[19]

d) *at samarbejde med tilsynsmyndigheden*
   - DPOen skal samarbejde med Datatilsynet. DPOens funktion er at understøtte, at kommunen overholder reglerne i databeskyttelsesforordningen.
   - Datatilsynet skal høres hvis konsekvensanalyse medfører høj risiko.[20]

e) *at fungere som Datatilsynets kontaktpunkt i spørgsmål vedrørende behandling, herunder den forudgående høring, der er omhandlet i artikel 36, og at høre tilsynsmyndigheden, når det er hensigtsmæssigt, om eventuelle andre spørgsmål.*
   - Vejlede den person, der behandles personoplysninger om.[21]

Da der er tale om minimumsopgaver, kan Kommunen godt overlade flere opgaver til DPOen.

DPO'en bliver kontaktpunkt for de registrerede vedrørende udøvelse af disses rettigheder, f.eks. indsigtsret, retten til sletning mv. DPO'en vil ligeledes være registreret som kontaktpunkt for tilsynsmyndigheder.

[17] Vejledningen s. 20
[18] Vejledningen s. 21
[19] Vejledningen s. 21
[20] Vejledningen s. 22
[21] Vejledningen s. 22

KORT OM DOKUMENTATIONS KRAV VEDRØRENDE COMPLIANCE MED FORORDNINGEN

Art 24

1. Under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder ***gennemfører den dataansvarlige passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise****, at behandling er i overensstemmelse med denne forordning. Disse foranstaltninger skal om nødvendigt revideres og ajourføres.*

2. Hvis det står i rimeligt forhold til behandlingsaktiviteter, skal de foranstaltninger, der er omhandlet i stk. 1, omfatte den dataansvarliges implementering af passende databeskyttelsespolitikker.

3. Overholdelse af godkendte adfærdskodekser som omhandlet i artikel 40 eller godkendte certificeringsmekanismer som omhandlet i artikel 42 kan bruges som et element til at påvise overholdelse af den dataansvarliges forpligtelser.

"De kriterier, der skal anvendes til at vurdere, hvilken type foranstaltninger der bør træffes, er behandlingens karakter, sammenhæng, omfang og formål samt de risici for de registreredes rettigheder og frihedsrettigheder, som databehandlingen indebærer. For så vidt angår vurderingen af risici, betyder dette, at graden af risikoen for den registreredes grundlæggende rettigheder og frihedsrettigheder er bestemmende for, hvilke foranstaltninger der er passende til den pågældende behandling."

"Af konkrete typer af foranstaltninger, der som udgangspunkt kan sikre efterlevelse af databeskyttelsesreglerne, nævner Artikel 29-gruppen bl.a. kortlægning af procedurer hos den dataansvarlige for at sikre, at alle databehandlinger kan identificeres, og der kan føres fortegnelse over disse.

Desuden nævner Artikel 29-gruppen uddannelse af personale hos den dataansvarlige i databeskyttelse, etablering af interne procedurer for henholdsvis sikkerhedsbrister, anmodninger fra de registrerede om indsigt, korrektion eller sletning samt udarbejdelse af mekanismer til behandling af klager mv., som passende tekniske og organisatoriske foranstaltninger.

Hvis det er proportionalt i forhold til den behandling af personoplysninger, som finder sted, skal de foranstaltninger, som iværksættes efter artikel 24, stk. 1, omfatte den dataansvarliges implementering af passende databeskyttelsespolitikker, jf. artikel 24, stk. 2.

Disse politikker kan f.eks. bestå af interne politikker og procedurer til behandling af anmodninger om indsigt, klager fra de registrerede mv. De pågældende politikker må ligeledes antages at skulle være relevante og tilstrækkelige i forhold til, hvad der kræves til at opfylde formålet med at efterleve forordningens krav om den dataansvarliges ansvar efter artikel 24, stk. 1."

"Den dataansvarlige skal desuden efter artikel 24, stk. 1, være i stand til at påvise, at behandlingen er i overensstemmelse med forordningen. Dermed skal den dataansvarlige kunne påvise over for interne såvel som eksterne interessenter, såsom tilsynsmyndighederne, at de valgte og gennemførte foranstaltninger er effektive, således at de pågældende behandlingsaktiviteter rent faktisk overholder

forordningens regler. Det er derfor ikke nok til at efterleve forpligtelserne efter artikel 24, stk. 1, at denne blot gennemfører passende tekniske og organisatoriske foranstaltninger uden løbende at følge op på, om disse rent faktisk er effektive."

"Som et element til at påvise, at den dataansvarlige overholder sine forpligtelser efter artikel 24, stk. 1, kan denne som følge af forordningens artikel 24, stk. 3, bruge overholdelsen af godkendte adfærdskodekser efter forordningens artikel 40 eller godkendte certificeringsmekanismer efter artikel 42. Disse kodekser og mekanismer vil således kunne bidrage til at bevise, at den dataansvarlige overholder sit ansvar efter artikel 24, stk. 1, og at denne derfor har defineret og gennemført passende foranstaltninger, som jævnligt er blevet revideret."[22]

Sammenfattende krav:

- Kortlægning af procedurer hos den dataansvarlige for at sikre, at alle databehandlinger kan identificeres og at der føres fortegnelse over disse.
- Uddannelse af personale
- Databeskyttelsespolitikker
- Påvise, at behandlingen er i overensstemmelse med forordningen – bl.a. ved overholdelsen af godkendte adfærdskodekser efter forordningens artikel 40 eller godkendte certificeringsmekanismer efter artikel 42.

Vi afventer i øjeblikket en vejledning om dataansvarlig og databehandler der skulle udkomme til oktober. Den er endnu ikke færdig.

Vejledning om fortegnelser burde ifølge tidsplanen foreligge i november. Formodentlig bliver denne også forsinket.

[22] Betænkningen del I pkt. 5.1.3

KORT OM PRIVACY BY DESIGN Artikel 25

Databeskyttelse gennem design

"1. Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, som behandlingen indebærer, gennemfører den dataansvarlige både på tidspunktet for fastlæggelse af midlerne til behandling og på tidspunktet for selve behandlingen passende tekniske og organisatoriske foranstaltninger, såsom pseudonymisering, som er designet med henblik på effektiv implementering af databeskyttelsesprincipper, såsom dataminimering, og med henblik på integrering af de fornødne garantier i behandlingen for at opfylde kravene i denne forordning og beskytte de registreredes rettigheder."

Det fremgår af artikel 25, stk. 1, at den dataansvarlige forpligtes til at opfylde kravene i forordningen og beskytte de registreredes rettigheder ved gennemførelse af passende tekniske og organisatoriske foranstaltninger, som er designet med henblik på effektiv implementering af databeskyttelsesprincipper og med henblik på integrering af de fornødne garantier i behandlingen af personoplysninger for at opfylde kravene i forordningen og beskytte de registreredes rettigheder.

> "Begrebet "databeskyttelse gennem design" må efter ordlyden forstås bredt, således at det omfatter både tekniske og organisatoriske foranstaltninger. Design må derfor antages at omfatte både et middel, eksempelvis et IT-systems tekniske indretning og brugergrænseflade, samt den måde den dataansvarlige organisatorisk er indrettet på."
>
> "På baggrund af ordlyden i artikel 25, stk. 1, skal foranstaltningerne gennemføres både på "tidspunktet for fastlæggelse af midlerne til behandling" (forberedelsesfasen) og "på tidspunktet for selve behandlingen". Sidstnævnte tidspunkt må antages at betyde den første dag, behandlingen begynder.
>
> Forordningens artikel 25, stk. 1, må antages at indebære en overvejelsesforpligtelse og en håndteringsforpligtelse for den dataansvarlige til allerede i forberedelsesfasen at indtænke de relevante foranstaltninger til sikring af overholdelse af databeskyttelsesforordningen."
>
> "Den dataansvarlige skal overveje og håndtere, hvordan databeskyttelse generelt, dvs. alle forordningens bestemmelser, kan efterleves med konkrete foranstaltninger i design af IT-systemer, såsom deres tekniske indretning og brugergrænseflade, samt ved indretningen af den dataansvarliges organisation."
>
> "Forordningens artikel 25, stk. 1, medfører med andre ord ikke et krav om, at eksempelvis ældre systemer skal re-designes, hvis der eksempelvis findes organisatoriske sikkerhedsløsninger, der må anses for tilstrækkelige. Dette skyldes, at forordningen først finder anvendelse den 25. maj 2018, og at artikel 25, stk. 1, således ikke finder anvendelse på allerede eksisterende systemer."
>
> "Eksempler på foranstaltninger, der efterlever principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, følger af præambelbetragtning nr. 78, hvoraf det fremgår, at sådanne foranstaltninger bl.a. kan bestå i minimering af behandlingen af personoplysninger, pseudonymisering af personoplysninger så hurtigt som muligt og gennemsigtighed for så vidt angår personoplysningers funktion og behandling, således at den

registrerede kan overvåge databehandlingen, og den dataansvarlige kan tilvejebringe og forbedre sikkerhedselementer."

"Blandt de foranstaltninger, som en dataansvarlig i hvert fald må antages at være forpligtet til at implementere, må være en sikring af, at de midler - f.eks. et IT-system - der bringes i anvendelse, medvirker til en efterlevelse af forordningens øvrige krav. Dette følger af kravet i artikel 25, stk. 1, om, at de fornødne sikkerhedsforanstaltninger skal "opfylde kravene i denne forordning"

"Efter omstændighederne vil design af et IT-system omfattet af artikel 25, stk. 1, der ikke sikrer, at den registreredes anmodning om f.eks. indsigt (artikel 15), ret til dataportabilitet (artikel 20) eller ret til begrænsning af behandling (artikel 18), kan imødekommes, således kunne udgøre en overtrædelse af forpligtelsen til databeskyttelse gennem design i artikel 25, stk. 1

Det må dog antages, at en sådan situation delvist vil kunne afhjælpes ved implementering af organisatoriske foranstaltninger, der gør den registrerede i stand til at gøre sin ret til indsigt gældende"

"Artikel 25, stk. 1, indebærer endvidere, at den dataansvarlige blandt andet skal anvende foranstaltninger, der er designet med henblik på effektiv implementering af databeskyttelsesprincipper og med henblik på integrering af de fornødne garantier i behandlingen. Begrebet garantier i forordningens artikel 25, stk. 1, skal også forstås i overensstemmelse med den engelske sprogversion, hvor der skrives safeguards, hvilket i denne sammenhæng kan forstås som "værn" eller "beskyttelse".[23]

Sammenfattende krav

Det består af en generel overvejelsesforpligtelse og en håndteringsforpligtelse for den dataansvarliges virksomhed til:

- I forberedelsesfasen at overveje, hvilke foranstaltninger der skal håndteres ved en behandling af personoplysninger for at efterleve databeskyttelsesretten.
- Fremtidige it-systemer skal designes med henblik på effektiv implementering af databeskyttelsesprincipper – f.eks. dataminimering.
    - F.eks. hvis den dataansvarlige selv udvikler et system, vil dette kunne afhjælpes ved at indarbejde Privacy Enhancing Technologies
    - F.eks. ved at stille krav herom til leverandøren af et itsystem.

OBS: organisatoriske foranstaltninger vil i visse tilfælde kunne være tilstrækkelige, hvis dette kan etablere et passende sikkerhedsniveau for behandlingen af personoplysninger f.eks. interne procedurer og undervisning af ansatte"

Databeskyttelse gennem standartindstilling

Art. 25 stk. 2. *"Den dataansvarlige gennemfører passende tekniske og organisatoriske foranstaltninger med henblik på gennem **standardindstillinger** at sikre, at **kun personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen, behandles.** Denne forpligtelse gælder den mængde personoplysninger, der indsamles, og omfanget af deres behandling samt deres opbevaringsperiode og tilgængelighed. Sådanne foranstaltninger skal navnlig gennem standardindstillinger sikre, at personoplysninger ikke uden den pågældende fysiske persons indgriben stilles til rådighed for et ubegrænset antal fysiske personer."*

[23] Bekendtgørelsens pkt. 5.2.3.1.

”Bestemmelsen foreskriver, at den dataansvarlige skal sikre, at det kun er de personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen, der bliver behandlet. Det skal også sikres, at personoplysninger ikke uden den pågældende fysiske persons indgriben stilles til rådighed for et ubegrænset antal fysiske personer.

Standardindstillinger skal efter ordlyden af artikel 25, stk. 2, forstås bredt, således at det omfatter både tekniske og organisatoriske foranstaltninger. Standardindstillinger kan derfor forstås som både IT-tekniske indstillinger og de almene forretningsgange, som understøtter databeskyttelse, herunder eksempelvis, at adgang til personoplysninger – analoge såvel som digitale – er arbejdsbetingede og ikke lige tilgængelige for alle i den dataansvarliges organisation.

Til forskel fra bestemmelsen i artikel 25, stk. 1, der vedrører selve designfasen, ses artikel 25, stk. 2, at udtrykke en pligt for den dataansvarlige til at sikre, at når f.eks. et softwareprogram, en online tjeneste, et IT-system eller lignende anvendes til at behandle personoplysninger, skal de indstillingsmuligheder, som systemet mv. indeholder, som standard indstilles på en måde, der understøtter bestemmelsens krav om bl.a. formålsspecifik behandling af personoplysninger.”

” Forordningens artikel 25, stk. 2, 2. pkt. fastslår endvidere udtrykkeligt, at de behandlede personoplysninger ikke uden den pågældende persons indgriben må stilles til rådighed for et ubegrænset antal fysiske personer. Dette må bl.a. antages at sigte mod, at systemer eller tjenester, der giver fysiske personer adgang til at oprette profiler på online-platforme, kun må lade personoplysninger være tilgængelige for et ubegrænset antal fysiske personer, på baggrund af den pågældende persons egen konkrete indgriben.”[24]

Sammenfattende krav?

Fremtidige systemers standardindstillinger skal indstilles, så de fremmer dataminimering og formålsspecifik behandling.

Eksisterende it-systemer hvor standardindstillingerne ikke kan ændres:

- Ingen nye krav til it-systemet pr. den 25. maj 2018

Eksisterende it-systemer hvor standardindstillingerne kan ændres:

- Virksomheden er pr. den 25. maj 2018 forpligtet til at ændre systemets standardindstillinger på en måde, der understøtter forordningens krav om bl.a. formålsspecifik behandling[25]

I det omfang et systems indstillinger skal ændres for at kunne overholde de krav, der i øvrigt følger af forordningen, herunder eksempelvis artikel 5, kapitel III om den registreredes rettigheder og artikel 32, er den dataansvarlige dog forpligtet til at ændre disse indstillinger, så det lever op til forordningens artikel 25, stk. 2, fra den 25. maj 2018.

Godkendt certificeringsmekanisme

Forordningens artikel 25, stk. 3, giver mulighed for, at der kan anvendes godkendte certificeringsmekanismer efter forordningens artikel 42 som et element til at påvise overholdelse af kravene om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

[24] Betænkningen 5.2.3.2
[25] Justitsministeriets FAQ
https://erhvervsstyrelsen.dk/sites/default/files/media/praesentation_fra_stormoede_om_databeskyttelsesforordningen.pdf

Certificering efter en godkendt certificeringsmekanisme i medfør af artikel 42, kan imidlertid ikke stå alene som bevis for overholdelse af forordningens krav.[26]

DATABEHANDLER ART. 28

Art. 28

1. Hvis en behandling skal foretages på vegne af en dataansvarlig, benytter den dataansvarlige udelukkende databehandlere, der kan stille de fornødne garantier for, at de vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandling opfylder kravene i denne forordning og sikrer beskyttelse af den registreredes rettigheder.

3. En databehandlers behandling skal være reguleret af en kontrakt eller et andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, der er bindende for databehandleren med hensyn til den dataansvarlige, og der fastsætter genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger og kategorierne af registrerede samt den dataansvarliges forpligtelser og rettigheder. Denne kontrakt eller dette andet retlige dokument fastsætter navnlig, at databehandleren:

a) kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel af personoplysninger til et tredjeland eller en international organisation, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser

b) sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt

c) iværksætter alle foranstaltninger, som kræves i henhold til artikel 32

d) opfylder de betingelser, der er omhandlet i stk. 2 og 4, for at gøre brug af en anden databehandler

e) under hensyntagen til behandlingens karakter, så vidt muligt bistår den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder som fastlagt i kapitel III

f) bistår den dataansvarlige med at sikre overholdelse af forpligtelserne i medfør af artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren

g) efter den dataansvarliges valg sletter eller tilbageleverer alle personoplysninger til den dataansvarlige, efter at tjenesterne vedrørende behandling er ophørt, og sletter eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne

h) stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene i denne artikel, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige

--//--

[26] Betænkningen pkt. 5.2.3.3

”Forordningens artikel 28 indeholder specifikke regler om databehandleren og dennes forpligtelser. Det følger således af artikel 28, stk. 1, at hvis en behandling skal foretages på vegne af en dataansvarlig, benytter den dataansvarlige udelukkende databehandlere, der kan stille de fornødne garantier for, at de vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandling opfylder kravene i denne forordning og sikrer beskyttelse af den registreredes rettigheder.”

”Dette taler for, at det kan lægges til grund, at artikel 28, stk. 4, skal forstås således, at kravet om, at der skal indgås en kontrakt eller et andet retligt dokument, omhandler det retlige forhold mellem databehandleren og de eventuelle underdatabehandlere, denne gør brug af. Dermed stilles der i artikel 28, stk. 4, ikke krav om, at det er den dataansvarlige, der skal indgå særskilte aftaler med eventuelle underdatabehandlere. Den dataansvarlige kan i stedet blot holde sig til den databehandleraftale, der på baggrund af artikel 28, stk. 3, er indgået med databehandleren, og herefter give konkret eller generel tilladelse til, at databehandleren overlader behandlingen til underdatabehandlere. I stedet er det derfor databehandleren, der i medfør af artikel 28, stk. 4, skal indgå en kontrakt eller et andet retligt dokument i medfør af national eller EU-retten, med de underdatabehandlere, denne måtte vælge af gøre brug af.”

Sammenfattende krav:

Databeskyttelsesforordningen indeholder nye krav til databehandleraftalen.

Samtlige kontrakter bør gennemgås for undersøgelse af hvorvidt der er indgået databehandler aftaler.

KOMMUNEN SKAL FØRE FORTEGNELSER OVER BEHANDLINGSAKTIVTETER UNDER DENNES ANSVAR ART. 30

Art. 30

1. Hver dataansvarlig og hvis det er relevant, den dataansvarliges repræsentant fører fortegnelser over behandlingsaktiviteter under deres ansvar. Disse fortegnelser skal omfatte alle af følgende oplysninger:

a) navn på og kontaktoplysninger for den dataansvarlige og, hvis det er relevant, den fælles dataansvarlige, den dataansvarliges repræsentant og databeskyttelsesrådgiveren

b) formålene med behandlingen

- "Fortegnelsen efter artikel 30 af enhver behandlingsaktivitets formål må i lighed med direktivet skulle forstås på den måde, at der vil kunne formuleres et samlet, logisk sammenhængende formål med en behandling eller en række af behandlinger, som hermed angives som ét formål ud af alle samlede formål hos den dataansvarlige. Det må således antages, at den dataansvarlige kan samle de behandlingsaktiviteter, som kan formuleres som et samlet, logisk sammenhængende formål, i én fortegnelse over de forskellige behandlingsaktiviteter."
- "Offentlig myndighed kunne samle sine behandlingsaktiviteter under forskellige delformål, såsom behandling af oplysninger i forbindelse med sagsbehandling, pensionsområdet, vielse, beskæftigelse og kommunale ydelser mv. i overensstemmelse med indholdet af de eksisterende fortegnelser i de kommunale fællesanmeldelser i Datatilsynets fortegnelse. Som et konkret eksempel herpå kan nævnes en kommunes behandling af personoplysninger i forbindelse med beskæftigelse og kommunale ydelser, hvor der vil være flere forskellige delformål, såsom kommunal udbetaling af kommunale ydelser, råd og vejledning, kommunal indsats vedrørende jobformidling mv. I et sådant tilfælde har disse delformål et samlet, logisk sammenhængende formål, som vil kunne angives som kommunens behandling af personoplysninger i forbindelse med dennes forpligtelser inden for beskæftigelse og kommunale ydelser."
- Der ses ikke med forordningens artikel 30, stk. 1, litra b, at være tale om et nyt krav til betingelserne for den dataansvarliges behandling af oplysninger, men blot at denne nu udtrykkeligt skal føre en fortegnelse over disse i forvejen definerede formål.[27]

c) en beskrivelse af kategorierne af registrerede og kategorierne af personoplysninger

- "Det vil sige, om det f.eks. er oplysninger om nuværende eller tidligere ansatte, kunder, borgere, andre virksomheder mv. Endvidere indebærer beskrivelsen af de typer af oplysninger, der behandles om de registrerede, at det angives, hvilke oplysninger der behandles om disse, såsom f.eks. identifikationsoplysninger, oplysninger om løn, arbejdstid, køb af ydelser mv."
- "Der ses ikke med forordningens artikel 30, stk. 1, litra c, at være tale om et nyt krav til betingelserne for den dataansvarliges behandling af oplysninger, men blot at denne nu

[27] Betænkningen pkt. 5.7.3.1

udtrykkeligt skal føre en fortegnelse over disse i forvejen definerede typer af oplysninger, der behandles om de registrerede personer."[28]

d) de kategorier af modtagere, som personoplysningerne er eller vil blive videregivet til, herunder modtagere i tredjelande eller internationale organisationer

- Det må antages, at det alene er de overførsler, der er regelmæssige, der skal anføres i fortegnelsen i overensstemmelse med gældende ret. Dette krav er ligeledes en videreførelse af kravet efter gældende ret, som følger af direktivets artikel 19, stk. 1, litra c, og persondatalovens § 43, stk. 2, nr. 5 og 6.[29]
-

e) hvor det er relevant, overførsler af personoplysninger til et tredjeland eller en international organisation, herunder angivelse af dette tredjeland eller denne internationale organisation og i tilfælde af overførsler i henhold til artikel 49, stk. 1, andet afsnit, dokumentation for passende garantier

- *Det er allerede et krav efter gældende ret, at den dataansvarlige skal angive en slettefrist i en anmeldelse til Datatilsynet. Den dataansvarlige skal endvidere efter gældende ret angive starttidspunktet for behandlingen, hvilket er mere omfattende end forordningens krav efter litra f. Dog skal det bemærkes, at det efter forordningen ikke er slettefristen for hele behandlingen, der skal angives i fortegnelsen, men slettefristerne for de forskellige kategorier af oplysninger.[30]*

f) hvis det er muligt, de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger

g) hvis det er muligt, en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger omhandlet i artikel 32, stk. 1.

- *Forordningens krav herom svarer således – efter sin ordlyd – til det, der følger af gældende ret, idet fortegnelsen dog alene skal indeholde en beskrivelse af sikkerhedsforanstaltningerne, såfremt det er muligt, hvorimod der efter gældende ret altid skal være en sådan beskrivelse i en anmeldelse efter persondataloven.[31]*

Det følger således af forordningens artikel 30, at den dataansvarlige og databehandleren i visse tilfælde skal føre interne fortegnelser over deres behandling af personoplysninger.

"Det fremgår af forordningens artikel 5, stk. 2, at den dataansvarlige er ansvarlig for og skal kunne påvise, at principperne for behandling af personoplysninger i artikel 5, stk. 1, er overholdes. I lighed med gældende ret skal den dataansvarlige således have et overblik over de behandlinger af personoplysninger, som denne foretager for at efterleve forordningens artikel 5, herunder stk. 2."

Fortegnelsen over behandlingsaktiviteter, som føres af den dataansvarlige og databehandleren samt deres eventuelle repræsentanter, skal i medfør af artikel 30, stk. 3, foreligge skriftligt, herunder skal den efter bestemmelsens ordlyd foreligge elektronisk. Forpligtelsen til fortegnelse er således underlagt et formkrav om, at denne ikke alene må føres i et fysisk dokument eller efter hukommelsen. Dette må forstås således, at fortegnelsen kan opbevares elektronisk med henblik på at kunne udprintes i fysisk form, f.eks. med henblik på at udlevere til tilsynsmyndigheden, hvis der anmodes herom."

"Ved artikel 30 indføres således forpligtelsen for de dataansvarlige og databehandlere til at opbevare intern dokumentation for behandling, der udføres under deres ansvar, i stedet for en generel anmeldelse til tilsynsmyndigheden, som krævet i artikel 18, stk. 1, og artikel 19 i databeskyttelsesdirektivet."

---

[28] Betænkningens pkt. 5.7.3.1
[29] Betænkningens pkt. 5.7.3.1
[30] Betænkningens pkt. 5.7.3.1
[31] Betænkningens pkt. 5.7.3.1

Det må efter bestemmelsens ordlyd antages, at fortegnelsesforpligtelsen efter artikel 30 omfatter al behandlingsaktivitet, det vil sige både behandling af ikke-følsomme oplysninger efter artikel 6, følsomme oplysninger efter artikel 9 samt oplysninger vedrørende straffedomme og lovovertrædelser efter artikel 10."

"Generelt kan det om kravene til en dataansvarliges fortegnelse i medfør af artikel 30, stk. 1, litra a-g, bemærkes, at disse i høj grad er i overensstemmelse med de krav, der for så vidt angår anmeldelsespligtige behandlinger stilles til en dataansvarliges anmeldelse til Datatilsynet for både private og offentlige myndigheder, jf. persondatalovens § 43, stk. 2 og § 48, stk. 2, jf. § 43, stk. 2."[32]

Sammenfattende krav:

Fortegnelsen skal som minimum indeholde de i litra a-g oplistede oplysninger.

De fleste oplysninger skulle efter gældende ret være angivet i anmeldelse til datatilsynet, hvorfor man i vidt omfang kan tage udgangspunkt i disse – hvis de er opdateret. Det er dog væsentligt at holde sig for øje, at fortegnelsen også skal indeholde fortrolige ikke følsomme oplysninger.

Udkast til fortegnelse er vedlagt betænkningen som bilag. Vejledning om fortegnelse skulle foreligge i november. Den foreligger endnu ikke.

Arbejdet med fortegnelsen bør igangsættes straks, da det medfører en gennemgang af mange systemer og det må formodes, at ikke alle systemer er anmeldt i dag.

[32] Betænkningen pkt. pkt. 5.7.3 og 5.7.3.1

KORT OM KONSEKVENSANALYSE ARTIKEL 35-36:

ART 35

*1. Hvis en type behandling, navnlig ved brug **af nye teknologier** og i medfør af sin **karakter, omfang**, **sammenhæng og formål**, sandsynligvis vil indebære **en høj risiko for fysiske personers rettigheder og frihedsrettigheder**, foretager den dataansvarlige forud for behandlingen **en analyse af de påtænkte behandlingsaktiviteters konsekvenser** for beskyttelse af personoplysninger. En enkelt analyse kan omfatte flere lignende behandlingsaktiviteter, der indebærer lignende høje risici.*

2. Den dataansvarlige rådfører sig med databeskyttelsesrådgiveren, hvis en sådan er udpeget, når der foretages en konsekvensanalyse vedrørende databeskyttelse.

*3. En konsekvensanalyse vedrørende databeskyttelse som omhandlet i stk. 1 er **navnlig påkrævet** i følgende tilfælde:*

a) en systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer, der er baseret på automatisk behandling, herunder profilering, og som er grundlag for afgørelser, der har retsvirkning for den fysiske person eller på tilsvarende vis betydeligt påvirker den fysiske person

b) behandling i stort omfang af særlige kategorier af oplysninger, jf. artikel 9, stk. 1, eller af personoplysninger vedrørende straffedomme og lovovertrædelser, jf. artikel 10, eller

c) systematisk overvågning af et offentligt tilgængeligt område i stort omfang.

4. Tilsynsmyndigheden udarbejder og offentliggør en liste over de typer af behandlingsaktiviteter, der er underlagt kravet om en konsekvensanalyse vedrørende databeskyttelse i henhold til stk. 1. Tilsynsmyndigheden indgiver disse lister til det i artikel 68 omhandlede Databeskyttelsesråd.

5. Tilsynsmyndigheden kan også udarbejde og offentliggøre en liste over de typer af behandlingsaktiviteter, for hvilke der ikke kræves nogen konsekvensanalyse vedrørende databeskyttelse. Tilsynsmyndigheden indgiver disse lister til Databeskyttelsesrådet.

6. Inden vedtagelsen af listerne i stk. 4 og 5 anvender den kompetente tilsynsmyndighed den sammenhængsmekanisme, der er omhandlet i artikel 63, hvis sådanne lister omfatter behandlingsaktiviteter, der vedrører udbud af varer eller tjenesteydelser til registrerede eller overvågning af sådanne registreredes adfærd i flere medlemsstater, eller som i væsentlig grad kan påvirke den frie udveksling af personoplysninger i Unionen.

*7. **Analysen skal mindst omfatte:***

a) en systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen, herunder i givet fald de legitime interesser, der forfølges af den dataansvarlige

- ”Skal ske en systematisk beskrivelse af de forskellige former for behandling, som personoplysningerne vil blive genstand for. Personoplysningerne, som skal behandles, skal også være klart beskrevet og defineret. Dette gælder også i forhold til oplysninger omfattet af artikel 9 og 10. Endvidere skal en konsekvensanalyse indeholde en beskrivelse af formålet med behandlingen, herunder dataansvarliges legitime interesser. Det kan eksempelvis være

behandling af personoplysninger, som enten har hjemmel i lov, eller som skal ske som led i offentlig myndighedsudøvelse."[33]

b) en vurdering af, om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene

- "Der er således tale om en bestemmelse, som blandt andet har til formål at hindre dataophobning og blandt andet også sikre, at der kun behandles personoplysninger, der er nødvendige, og som kan rummes inden for formålene med behandlingen. Behandlingen af personoplysninger må dermed ikke gå videre, end hvad der kræves for at opfylde de formål, som den dataansvarlige er berettiget til at forfølge."[34]

c) en vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder som omhandlet i stk. 1, og

- Det betyder, at de registreredes rettigheder og frihedsrettigheder skal vurderes i forhold til den planlagte behandling og formålet med denne. Litra d bør læses i sammenhæng med litra c, således at der kræves en vurdering af de foranstaltninger, der påtænkes for at imødegå disse risici, herunder garantier, sikkerhedsforanstaltninger og mekanismer, som kan sikre beskyttelse af personoplysninger og påvise overholdelse af forordningen og dansk lovgivning i øvrigt, under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser.

d) de foranstaltninger, der påtænkes for at imødegå disse risici, herunder garantier, sikkerhedsforanstaltninger og mekanismer, som kan sikre beskyttelse af personoplysninger og påvise overholdelse af denne forordning, under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser.

8. Overholdelse af godkendte adfærdskodekser, jf. artikel 40, inddrages behørigt ved vurderingen af konsekvenserne af de behandlingsaktiviteter, der udføres af de pågældende dataansvarlige eller databehandlere, navnlig i forbindelse med en konsekvensanalyse vedrørende databeskyttelse.

9. Den dataansvarlige indhenter, hvis det er relevant, de registreredes eller deres repræsentanters synspunkter vedrørende den planlagte behandling, uden at det berører beskyttelse af kommercielle eller samfundsmæssige interesser eller behandlingsaktiviteternes sikkerhed.

10. Hvis behandling i henhold til artikel 6, stk. 1, litra c) eller e), har et retsgrundlag i EU-retten eller i den medlemsstats nationale ret, som den dataansvarlige er underlagt, og denne ret regulerer den eller de pågældende specifikke behandlingsaktiviteter, og der allerede er foretaget en konsekvensanalyse vedrørende databeskyttelse som led i en generel konsekvensanalyse i forbindelse med vedtagelsen af dette retsgrundlag, finder stk. 1-7 ikke anvendelse, medmindre medlemsstaterne anser det for nødvendigt at foretage en sådan analyse inden behandlingsaktiviteter.

11. Den dataansvarlige foretager, hvis det er nødvendigt, en fornyet gennemgang for at vurdere, hvorvidt behandling er foretaget i overensstemmelse med konsekvensanalysen vedrørende databeskyttelse, i hvert fald når der er en ændring af den risiko, som behandlingsaktiviteterne udgør.

---//---

" Det fremgår af artikel 35, stk. 1, at hvis en type behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, foretager den dataansvarlige forud for behandlingen

[33] Betænkningens pkt.5.13.3.4
[34] Betænkning pkt.5.13.3.4

en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger. En enkelt analyse kan omfatte flere lignende behandlingsaktiviteter, der indebærer lignende høje risici."

Som det fremgår af artikel 35, stk. 1, kan det navnlig være relevant at vurdere behovet for en konsekvensanalyse, hvis der er tale om en type behandling, som indebærer brug af nye teknologier.

"Nye teknologier" kan eksempelvis være brugen af biometriske data, herunder anvendelse af iris-scanning, eller af kunstig intelligens, men også adgangen til eksempelvis at kommunikere med det offentlige via apps på mobile enheder eller brug af elektroniske identiteter. Med "ny teknologi" skal der være tale om objektivt set ny teknologi. Det forhold, at der for den dataansvarlige konkret er tale om ny teknologi i form af eksempelvis skift af ITplatform, kan ikke i sig selv være afgørende for, at der skal udarbejdes en konsekvensanalyse, hvis ikke der derved vurderes at være en høj risiko for fysiske personers rettigheder og frihedsrettigheder."

"Det er imidlertid ikke et krav, at der skal være tale om brug af nye teknologier. Der bør derfor også, i de tilfælde, hvor der ikke gøres brug af nye teknologier, konkret tages stilling til, om en behandling sandsynligvis vil indebære en høj risiko."

"Det følger af artikel 35, stk. 1, at der alene skal foretages en konsekvensanalyse, når der sandsynligvis vil være høj risiko for fysiske personers rettigheder og frihedsrettigheder."

"Den dataansvarlige skal i forbindelse med udarbejdelsen af en konsekvensanalyse inddrage de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger. Det bør eksempelvis vurderes, hvilke konsekvenser et brud på persondatasikkerheden vil kunne medføre i forhold til den valgte behandlingsaktivitet. Mængden af data skal også vurderes i forhold til den valgte behandlingsaktivitet og indgå i vurderingen af, om en identificeret risiko må karakteriseres som værende høj."

"Artikel 35, stk. 1, 2. pkt., må antageligvis betyde, at det kan være tilstrækkeligt at udarbejde en konsekvensanalyse for flere lignede behandlingsaktiviteter, uanset størrelsen af den samlede mængde af data, som behandlingsaktiviteterne omfatter. Endvidere må det betyde, at flere dataansvarlige kan foretage en fælles konsekvensanalyse vedrørende databeskyttelse (dog således, at de hver især har ansvaret herfor), forudsat at der er tale om samme type system, den samme behandlingsaktivitet af de samme personoplysninger, samt at det indebærer lignende høje risici. Det vil eksempelvis være tilstrækkeligt for flere kommuner at udarbejde én konsekvensanalyse vedrørende databeskyttelse i det samme system (som leveres af samme leverandør), hvis systemet behandler de samme typer af personoplysninger og behandlingsaktiviteterne indebærer samme høje risici."

Præamblet pkt. 91 næver tilfæde hvor der bør foretages konsekvensanalyse:

- " omfattende behandlings aktiviteter til behandling af meget store mængder personoplysninger på regionalt, nationalt eller overnationalt plan, der kan berøre mange registrerede, og som sandsynligvis vil indebære en høj risiko, f.eks. på grund af behandlingsaktiviteternes følsomhed, hvis der i overensstemmelse med det opnåede niveau af teknologisk viden sker omfattende brug af ny eller innovativ brug af teknologi, samt i forbindelse med andre behandlingsaktiviteter, der indebærer en høj risiko for registreredes rettigheder og frihedsrettigheder, navnlig hvis disse aktiviteter gør det vanskeligere for registrerede at udøve deres rettigheder."
- "hvis personoplysninger behandles med det formål at træffe afgørelser vedrørende specifikke fysiske personer efter en systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer baseret på profilering af disse oplysninger eller efter behandling af særlige kategorier af personoplysninger, biometriske data eller oplysninger om straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger."
- "omfattende overvågning af offentligt tilgængelige områder, navnlig ved brug af optoelektronisk udstyr, eller ved alle andre aktiviteter, hvor den kompetente tilsynsmyndighed mener, at den pågældende behandling sandsynligvis indebærer en høj risiko for registreredes rettigheder og frihedsrettigheder, navnlig fordi den hindrer registrerede i at udøve en rettighed eller gøre brug af en tjeneste eller en kontrakt, eller fordi den foretages på systematisk og omfattende vis."

”Det bemærkes, at hvis udfaldet af en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko, som den dataansvarlige ikke kan begrænse ved passende foranstaltninger, indtræder der en pligt for den dataansvarlige til at høre tilsynsmyndigheden efter forordningens artikel 36, stk. 1.”

”I forhold til udarbejdelse af konsekvensanalyse vedrørende databeskyttelse, kan der henvises til den internationale standard ISO 29134 omhandlende ”Privacy Impact Assessment” (konsekvensanalyse vedrørende privatliv). Ved at benytte denne standard kan den dataansvarlige øge sandsynligheden for at afdække væsentlige elementer i sin databehandling og samtidig få vejledning i processen og rapporteringen. Denne standard kan anvendes af både offentlige myndigheder og private virksomheder.”

”Hvis behandlingsaktiviteternes risiko ændres, eller det af anden grund vurderes nødvendigt, skal den dataansvarlige foretage en gennemgang af ændringer med henblik på at vurdere, hvorvidt behandlingen er foretaget i overensstemmelse med den oprindelige konsekvensanalyse. Dette skal på baggrund af ordlyden ”i hvert fald” ske i de tilfælde, hvor der sker en ændring af den risiko, som behandlingsaktiviteterne udgør. Det må efter bestemmelsen også være påkrævet med en fornyet konsekvensanalyse i andre situationer. Det må eksempelvis skulle vurderes, om der er behov for en fornyet gennemgang, når der sker ændringer, som betyder, at formålet med behandlingen ændres. Endvidere vil dette skulle ske, hvis behandlingen ændres, således at der fremover skal behandles andre personoplysninger end dem, som aktuelt bliver behandlet, herunder hvis der fremover skal behandles personoplysninger, som er omfattet af en anden kategori af personoplysninger. Dette kunne eksempelvis være, hvis et system, der omfatter behandlingsaktiviteter af personoplysninger efter artikel 9, ændres, således at der fremover skal ske behandling af personoplysninger omfattet af artikel 10. Derudover kunne det være tilfældet, hvis et eksisterende system, der behandler oplysninger efter artikel 6, udvides til også at behandle oplysninger efter artikel 9. ”

Sammenfattende krav:

Det kan ud fra karakteren af de eksempler, der nævnes i artikel 35, stk. 3, og i præambelbetragtning nr. 91 – med henvisningen til ”meget store mængder personoplysninger på regionalt, nationalt eller overnationalt plan” – samt ud fra ordlyden af artikel 35, stk. 1, konstateres, at området for, hvornår en konsekvensanalyse er påkrævet er snævert. Dataansvarlige må således i de fleste tilfælde antages ikke at skulle udarbejde en konsekvensanalyse.

Såfremt en konsekvensanalyse er påkrævet, angiver forordningens artikel 35, stk. 7, hvad en sådan analyse mindst skal omfatte.

Forordningen angiver ikke tidsfrister for, hvornår tilsynsmyndighedens liste(r) skal foreligge. Af hensyn til listens/listernes funktion vil det være hensigtsmæssigt, at de foreligger snarest efter forordningens anvendelsestidspunkt. Som beskrevet ovenfor skal der ske forelæggelse for Databeskyttelsesrådet.

I tilknytning til kravet om konsekvensanalyse vedrørende databeskyttelse kræver databeskyttelsesforordningen ved visse behandlinger, at tilsynsmyndigheden høres, før behandlingen påbegyndes jf. Art. 36.

Kravet om at udarbejde konsekvensanalyser gælder alene for behandling af personoplysninger, der indledes efter den 25. maj 2018, hvor forordningen finder anvendelse. Artikel 29-gruppen anbefaler

imidlertid, at der også udarbejdes konsekvensanalyser for databehandlingsprocesser, der starter før, hvis de forventes fortsat at være i gang efter den 25. maj 2018.[35]

Se i øvrigt artikel 29 gruppens Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679[36]

BEHANDLINGSIKKERHED ART. 32

1. Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder ***gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau****, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:*

a) pseudonymisering og kryptering af personoplysninger

- Det fremgår således af denne bestemmelse, at med pseudonymisering menes behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person.
- Kryptering er omsættelse af data til kode og kan anvendes som en foranstaltning, der, hvis den er behørigt implementeret, kan mindske risikoen for manglende fortrolighed, integritet,uafviselighed og autentifikation[37]

b*) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og –tjenester*

- Med udtrykket integritet sigtes bl.a. til, at det er muligt at validere, om data på disse systemer er korrekte, pålidelige, nøjagtige og/eller fuldstændige.
- For så vidt angår behandlingssystemer og -tjenesters tilgængelighed sigtes bl.a. til, at behandlingssystemer og -tjenester og data i disse er tilgængelige ved anmodning fra autorise ret bruger, eksempelvis ved at sikre en velfungerende backup eller dublerede systemer alt afhængig af, om det er relevant. Det er normalt en forudsætning, at der er fastlagt organisatoriske processer for, hvorledes disse opgaver udføres, og hvordan f.eks. backup testes.
- Med udtrykket robusthed sigtes bl.a. til at sikre behandlingssystemer og -tjenesters tekniske og organisatoriske modstandsdygtighed, f.eks. ved at sikre dem imod skadelige hændelser. Der kan f.eks. sikres imod udfald ved dublerede diske, køling, nødstrømsanlæg, automatisk brandslukning, mv. alt afhængig af, om det er relevant.
- Med udtrykket vedvarende menes, at evnen til at sikre fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og –tjenester ikke blot skal opfyldes én gang, men er en løbende teknisk og organisatorisk forpligtelse.[38]

c) evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

---

[35] Kromann Reumerts nyhedsbrev https://www.kromannreumert.com/Nyheder/2017/04/Artikel-29-gruppen-udgiver-guidelines-om-reglerne-om-konsekvensanalyse?utm_source=Persondata+og+whistleblower-ordninger&utm_medium=email&utm_campaign=newsletter

[36] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

[37] Betænkning del I pkt. 5.10.3

[38] Betænkning del I pkt. 5.10.3

- Der sigtes hermed til, at organisationen har et beredskab for, hvordan adgangen til personoplysninger genoprettes i tilfælde af hændelser som f.eks. brand, hacking, ransomware eller overgravede datakommunikationskabler. Det kan kræve, at organisationen har planlagt, hvorledes IT-driften i pågældende tilfælde kan genoprettes inden for et nærmere bestemt tidsrum, f.eks. ved brug af backup eller overgang til alternative datakommunikationslinjer alt afhængig af, om det er relevant. Evnen til rettidig genoprettelse kan f.eks. demonstreres ved øvelser og test.[39]

d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

- Det sigtes hermed til f.eks. med jævne mellemrum at teste/afprøve, vurdere og evaluere – alt afhængig af om det er relevant – firewalls, krypterede forbindelser, krypterede lagringer, foranstaltninger imod forsøg på overbelastelsesangreb, foranstaltninger imod forsøg på at gætte adgangsgivende faktorer, adgangskontrol, brugeradministrationsprocessen og meget andet.[40]

2. Ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

3. Overholdelse af en godkendt adfærdskodeks som omhandlet i artikel 40 eller en godkendt certificeringsmekanisme som omhandlet i artikel 42 kan bruges som et element til at påvise overholdelse af kravene i nærværende artikels stk. 1.

Af præambelbetragtning nr. 83 fremgår endvidere, at for at opretholde sikkerheden og hindre behandling i strid med denne forordning bør den dataansvarlige eller databehandleren vurdere de risici, som en behandling indebærer, og gennemføre foranstaltninger, der kan begrænse disse risici, som f.eks. kryptering. Disse foranstaltninger bør under hensyntagen til det aktuelle tekniske niveau og implementeringsomkostningerne sikre et tilstrækkeligt sikkerhedsniveau, herunder fortrolighed, i forhold til risiciene og karakteren af de person oplysninger, der skal beskyttes. Ved vurderingen af datasikkerhedsrisikoen bør der tages hensyn til de risici, som behandling af personoplysninger indebærer, såsom hændelig eller ulovlig tilintetgørelse, tab, ændring eller uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet, og som navnlig kan føre til fysisk, materiel eller immateriel skade.[41]

Afslutningsvis skal det bemærkes, at som det fremgår af ordlyden af artikel 32, stk. 1, kan den dataansvarlige også leve op til bestemmelsen ved brug af organisatoriske foranstaltninger.

Sådanne organisatoriske foranstaltninger vil eksempelvis kunne være, at en arbejdsplads begrænser medarbejdernes adgang til personoplysninger, således at det kun er bestemte medarbejdere, som har adgang til f.eks. følsomme personoplysninger. Det fremgår, som anført af forordningens artikel 32, stk. 1, at der skal tages hensyn til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, når der fastsættes passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.[42]

En risikobaseret tilgang til sikkerhed kendes allerede i dag i form af for eksempel informationssikkerhedsstandarden ISO 27001, som alle statslige myndigheder skal følge, og alle andre

[39] Betænkning del I pkt. 5.10.3
[40] Betænkning del I pkt. 5.10.3
[41] Betænkning del I pkt. 5.10.3.
[42] Betænkning del I pkt. 5.10.3

offentlige myndigheder skal følge principperne i.575 Standarden beskriver kravene til et dækkende informationssikkerheds-ledelsessystem (ISMS), som skal sikre en risikobaseret, effektiv og fleksibel styring af sikkerheden.

Den risikobaserede tilgang kendes også fra ISO/IEC DIS 29134 "Information technology – Security techniques – Privacy impact assesment – Guidelines". Der er tale om en international standard vedrørende privacy impact assesments udarbejdet af den internationale standardiseringsorganisation. 576 ISO 29134 standarden er en vejledning i, hvorledes en Privacy Impact Assessment proces (analogt en konsekvensanalyse) kan udføres. Standarden beskriver processen i en række trin, hvoraf et trin f.eks. vedrører identifikation af risici og et senere trin f.eks. vedrører beslutning om foranstaltninger. Standarden sætter bl.a. fokus på, at behandlingssikkerhed bliver iagttaget og indarbejdet i f.eks. design og implementeringen af IT-løsninger. ISO 29134 standarden vedrører privacy impact assessment. Det må antages, at de europæiske tilsynsmyndigheder og Databeskyttelsesrådet også vil tage standarden i betragtning i forbindelse med overvejelser om forordningens bestemmelser om behandlingssikkerhed og beskyttelse af fysiske personers rettigheder og frihedsrettigheder.

Som udgangspunkt er det den dataansvarlige, som beslutter den nærmere fremgangsmåde og systematik. Det er nærliggende, at de følgende, vejledende fire trin vil kunne indgå i den dataansvarliges overvejelser:

1. Identifikation og vurdering af risici

2. Identifikation af mulige foranstaltninger

3. Gennemgang af, hvilke foranstaltninger som imødegår relevante risici, så et passende sikkerhedsniveau opnås.

4. Implementering af de foranstaltninger som det besluttes at gennemføre.[43]

YDERLIGERE DOKUMENTATIONSKRAV

- Den dataansvarlige skal altid kunne dokumentere, at have modtaget et datasubjekts samtykke til behandling af personoplysninger jf. artikel 7 stk. 1
- Den dataansvarlige skal kunne påvise, at principper for behandling af personoplysninger overholdes jf. art 5 stk. 2.

    a) behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (»lovlighed, rimelighed og gennemsigtighed«)
    b) indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål (»formålsbegrænsning«)
    c) være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (»dataminimering«)
    d) være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges (»rigtighed«)
    e) opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles; personoplysninger kan opbevares i længere tidsrum, hvis personoplysningerne alene behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i

[43] Betænkning del I pkt. 5.10.4

overensstemmelse med artikel 89, stk. 1, under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger, som denne forordning kræver for at sikre den registreredes rettigheder og frihedsrettigheder (»opbevaringsbegrænsning«)

f) behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (»integritet og fortrolighed«).

- Dokumentation af brud på persondatasikkerhed, samt faktiske omstændigheder ved bruddet, virkning, afhjælpende foranstaltninger jf. artikel 33 stk. 5
- Den dataansvarlige er ansvarlig for og skal kunne påvise og dokumentere, at personoplysninger behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger jf. art. 32.

CERTEFICERING OG ADFÆRDSKODEKS ART 40 OG 42

Af forordningens artikel 40, stk. 1, fremgår det, at medlemsstaterne, tilsynsmyndighederne, Databeskyttelsesrådet og Kommissionen tilskynder til udarbejdelse af adfærdskodekser, der under hensyntagen til de særlige forhold i de forskellige behandlingssektorer og mikrovirksomheders og små og mellemstore virksomheders specifikke behov bidrager til korrekt anvendelse af denne forordning.

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 databeskyttelsesforordningens artikel 42 tilskyndes til, at der fastlægges certificeringsmekanismer for databeskyttelse og databeskyttelsesmærkninger og -mærker. Dette skal ske både på nationalt og på EU-plan. Udover ovennævnte hensigtserklæring indeholder artikel 42 også en række krav til certificeringsprocessens indhold.

DATAPORTABILITET ART 20

"1. Den registrerede har ret til i et struktureret, almindeligt anvendt og maskinlæsbart format at modtage personoplysninger om sig selv, som vedkommende har givet til en dataansvarlig, og har ret til at transmittere disse oplysninger til en anden dataansvarlig uden hindring fra den dataansvarlige, som personoplysningerne er blevet givet til, når:

a) behandlingen er baseret på samtykke, jf. artikel 6, stk. 1, litra a), eller artikel 9, stk. 2, litra a), eller på en kontrakt, jf. artikel 6, stk. 1, litra b), og

b) behandlingen foretages automatisk.

2. Når den registrerede udøver sin ret til dataportabilitet i henhold til stk. 1, har den registrerede ret til at få transmitteret personoplysningerne direkte fra en dataansvarlig til en anden, hvis det er teknisk muligt.

3. Udøvelsen af den ret, der er omhandlet i denne artikels stk. 1, berører ikke artikel 17. Den nævnte ret finder ikke anvendelse på behandling, der er nødvendig for udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

4. Den ret, der er omhandlet i stk. 1, må ikke krænke andres rettigheder eller frihedsrettigheder."

"Ved forordningens artikel 20 indføres en ny rettighed for den registrerede til dataportabilitet, som indebærer en ret til i visse tilfælde at modtage personoplysninger – som vedkommende har givet til en dataansvarlig – om sig selv i et struktureret, almindeligt anvendt og maskinlæsbart format.

Herudover indebærer retten til dataportabilitet en rettighed for den registrerede til i visse tilfælde at få transmitteret disse oplysninger om sig selv fra én dataansvarlig til anden uden hindring fra den dataansvarlige, som personoplysningerne er blevet givet til.

Formålet med denne nye rettighed er at øge den registreredes kontrol over egne personoplysninger ved at fremme mulighederne for let at få flyttet, kopieret eller overført vedkommendes personoplysninger til sig selv eller fra én tjenesteudbyder til en anden. Retten til dataportabilitet finder ikke anvendelse på behandling, der er nødvendig for at udføre en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, jf. artikel 20, stk. 3, 2. pkt.[44]

Herudover udtaler Artikel 29-gruppen, at retten til dataportabilitet ikke medfører en forpligtelse for den tidligere dataansvarlige til at beholde den registreredes personoplysninger længere end nødvendigt blot for at imødekomme en fremtidig anmodning om dataportabilitet.

Artikel 29-gruppen bemærker, at der ikke i forordningen angives specifikke anbefalinger til selve formatet, men at det må antages, at valget i forhold til formatet skal foretages med "operationalitet" for øje samt at give den registrerede en stor grad af dataportabilitet.

Endvidere bemærker Artikel 29-gruppen, at formater, der er genstand for omkostningsfulde licenser, ikke kan anses for en hensigtsmæssig fremgangsmåde i forhold til formatet." [45]

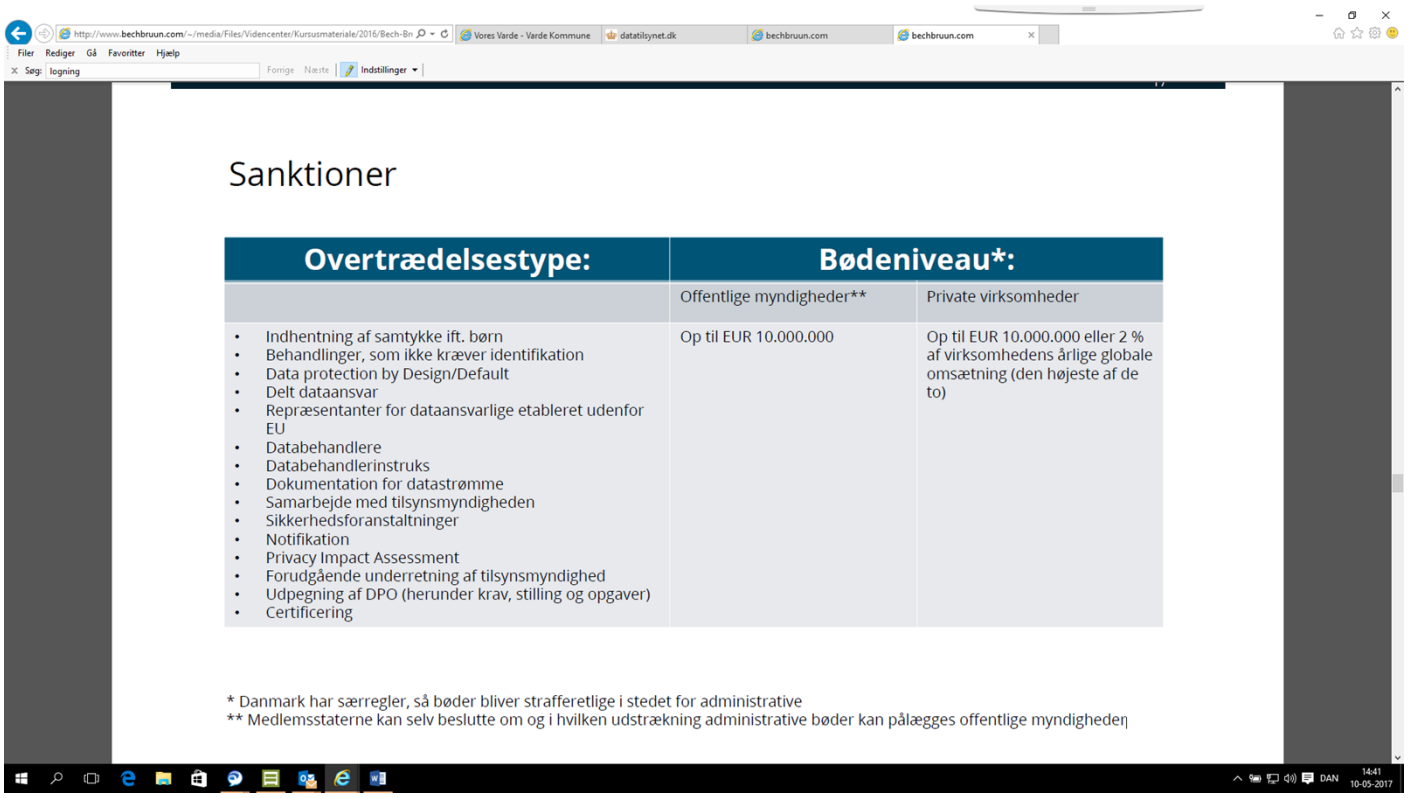
Se i øvrigt artikel 29 gruppens Guidelines on the right to data portability[46]

EKSEMPEL PÅ PLIGTER OVERFOR DEN PERSON OPLYSNINGERNE ANGÅR:

- Oplyse om at samtykke kan trækkes tilbage jf. art 7 stk. 3
- Ret til at få personoplysninger om sige selv slettet og berigtiget jf. art 17
- Ret til begrænsning af behandling art 18
- Ret til at gøre indsigelser imod behandling af sine personlige oplysninger baseret på art 6 stk. 1 litra e og f) – kommunen skal gøre opmærksom på denne ret senest på tidspunktet for den første kommunikation jf. art 21
- Ret til ikke at være genstand for en afgørelse der alene er baseret på automatisk behandling, herunder profilering

[44] Betænkning del I pkt. 4.10.1
[45] Betænkningen del I pkt. 4.10.3
[46] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

SANKTIONER



Sanktioner

Overtrædelsestype:	Bødeniveau*:	
	Offentlige myndigheder**	Private virksomheder
• Indhentning af samtykke ift. børn • Behandlinger, som ikke kræver identifikation • Data protection by Design/Default • Delt dataansvar • Repræsentanter for dataansvarlige etableret udenfor EU • Databehandlere • Databehandlerinstruks • Dokumentation for datastrømme • Samarbejde med tilsynsmyndigheden • Sikkerhedsforanstaltninger • Notifikation • Privacy Impact Assessment • Forudgående underretning af tilsynsmyndighed • Udpegning af DPO (herunder krav, stilling og opgaver) • Certificering	Op til EUR 10.000.000	Op til EUR 10.000.000 eller 2 % af virksomhedens årlige globale omsætning (den højeste af de to)

* Danmark har særregler, så bøder bliver strafferetlige i stedet for administrative
** Medlemsstaterne kan selv beslutte om og i hvilken udstrækning administrative bøder kan pålægges offentlige myndigheden