DATABESKYTTELSE OG DOKUMENTATIONSKRAV

Retsområde: Persondataret

Juridisk kandidat speciale

Katja Diania Joost

Studienummer 20144976

Vejleder

Charlotte Bagger Tranberg

Aalborg Universitet

Maj 2019

INDHOLD

SUMMARY

The purpose of this thesis is to analyze, review and compare the scope of data security as well as the documentation requirement for the same, in connection with the implementation of GDPR (EU 2016/679 of April 27th 2016) and the Danish Data Protection Act, compared to the rules in the Personal Data Act and related directives 95/46 / EC.

The background for the EU Commission's wish to create a new common data protection regulation applicable to all EU Member States, must be found in the rapid development of technology, including the massive transfer of personal data via the Internet.

Specifically, storage of data in a Cloud solution can give the data subject doubts as to where their data is actually stored in the world.

When storing data in a Cloud solution, the data subject has within a few seconds, the opportunity to access his data using a code provided to him regardless of where in the world he is. The data subject thus gets space for his data in a small part of the "cloud".

Precisely the extent of the sharing and storage of data by – typically - external providers, means that data security can be more easily challenged as it can be difficult to see where data is stored, who has access to data and for what purpose the data is processed.

Data security is one of the key elements of the GDPR, as the Regulation states that the data controller must implement the necessary technical and organizational security measures to meet the data security requirement so that the registered rights and freedoms rights are best possible protected.

The data security requirements is not defined in the regulation, but must be assessed by the individual data controller. The regulation aims to use a risk-based approach to this assessment, after which the implementation of security measure can be taken.

The data controller and the data processor is also obligated to provide documentation for the handling of data. Both the data controller and the data processor are required to keep a record of what data they are processing, why, where and how. Such a record can be use as part of the documentation for the control of the data processing itself.

The thesis therefore deals with an analysis and assessment of the data security rules in the Personal Data Act compared with the rules and requirements of the GDPR.

Furthermore, the documentation requirements for compliance with the data security have been analyzed and evaluated in order to find answers to what is required of documentation to be sure that the requirements of the GDPR are met.

The results of the analysis shows that - despite the fact that according to previous practice and wording requirements were also set for data security - the implementation of GDPR has tightened the requirements for the fulfillment of data security.

The access to data security shall seek implemented via a risk-based approach, where documentation must be available for appropriate technical and organizational measures.

This more risk-based approach to data management should avoid that data are subject to any kind of violation.

There are several options for voluntarily obtaining specific statements or introducing codes of conduct or certifications as part of the compliance documentation.

These certifications, has been reviewed separately in relation to the documentation and the value such certificates can give.

Although much of the terminology and provisions of the personal data goes again and seems to be the same from Personal Data Act to GDPR, the introduction of the GDPR seems to be a tightening of the personal data rules, especially in the field of data security.

ANVENDTE FORKORTELSER

DA	Dataansvarlig
DB	Databehandler
GDPR	EU-Parlamentet og Rådets dataforordning (EU) 2016/679 af 27. april 2016
DBL	Databeskyttelsesloven
PDL	Persondataloven
Direktivet	EU-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995
DT	Datatilsynet
MS	Medlemsstat i EU
TEUF	EU traktat om funktions måden inden for den Europæiske Union
EMRK	Europæiske Menneskerettighedskonvention – inkorporeret i DK i 1992
PET	Privacy enhancing technologies
DPIA	Data Protection Impact Assessment

INDLEDNING OG HISTORIK

Tilbage i 2012 fremsatte EU-kommissionen et forslag til en ny datalovgivning for alle EU-lande, og der har op til fremlæggelsen af den samlede forordning i december 2015 og endelig vedtagelsen i april 2016, været lange og indgående forhandlinger mellem Europa-Parlamentet, Ministerrådet og EU-kommissionen.

Forordning 2016/679 "om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger", blev således en realitet, da denne blev vedtaget 27/04/2016, med ikrafttrædelse den 25/05/2018. Forordningen er i daglig tale omtalt GDPR (General Data Protection Regulation)

"Forordninger er retsakter rettet direkte til borgerne"[1]. Dette bevirker, at forordningen har direkte retsvirkning for borgerne i den enkelte stat, ligesom myndigheder og virksomheder er underlagt ordlyden. "En forordning er almengyldig. Den er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat"[2]

Da GDPR ikke omhandler en fuldstændig og udtømmende regulering, har man overladt til de enkelte medlemsstater ved lov, at udfylde de regler i forordningen der giver de enkelte medlemsstater mulighed for fastsættelse af nationale regler, og i nogle tilfælde er det ligefrem nødvendigt at udstede sådanne bestemmelser.[3] Så selvom forordningen er gældende for hele EU, kan der være afvigelser i de respektive lande, idet de nationale myndigheder selv har måttet foretage diverse udfyldninger flere steder i forordningen.

Som supplement til selve forordningen, blev Databeskyttelsesloven - Lov 502 af 23/05/2018[4] derfor vedtaget i Danmark med ikrafttrædelse 25/05/2018.

Databeskyttelsesloven udgør således sammen med forordningen den samlede danske lovgivning på persondatarets området.

---

[1] Carsten Munk-Hansen "Retsvidenskabsteori" s. 260

[2] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:12012E/TXT&from=DA - TEUF artikel 288 stk. 2

[3] Peter Blume "Den nye persondataret" s. 14/15

[4] https://www.retsinformation.dk/Forms/r0710.aspx?id=201319 - Databeskyttelsesloven (DBL)

En af de store og omdiskuterede punkter i GDPR, er risikoen for at blive pålagt en bøde såfremt reglerne i GDPR ikke er overholdt. Bødestørrelsen kan andrage op til 20 mio. EUR eller 4% af en virksomheds samlede omsætning. Alene størrelsen på de bøder der kan blive sanktioneret virker som en præventiv ting for virksomheder der håndterer persondata, hvilket også er tilsigtet jf. forordningens art. 84 stk. 1.

En af de andre skærpede områder i GDPR er kravet om, at virksomheder skal føre fortegnelser over persondata der behandles, ligesom der er indført et decideret krav til at kunne fremvise dokumentation for, at persondata behandles og opbevares på sikkerhedsmæssig korrekt vis.

Der er dog ikke i selve forordningen angivet en konkret måde at føre en sådan dokumentation på. Den dataansvarlige og evt. databehandler skal dog sikre, at der er indført tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici der måtte være forbundet med, at data bliver ødelagt, går tabt, bortkommer eller på anden måde bevirker, at den registreredes data gøres til genstand for uretmæssig håndtering/anvendelse.

Forordningen er således teknologi neutral jf. præambelen til GDPR punkt 15, men spørgsmålet er hvilke sikkerhedstiltag der skal tages, og hvornår man egentlig ved, at behandlingssikkerheden er opfyldt, og ikke mindst at ens dokumentation lever op til kravene.

PROBLEMFORMULERING

På baggrund af ovenstående, vil denne opgaves formål være at analysere og fastlægge rækkevidden af begrebet ”behandlingssikkerhed”, samt at analyserer og vurderer hvad dokumentationskravet indebærer og hvordan dette efterleves.

Dette vil blive belyst ved følgende problemformulering:

Hvad er rækkevidden af databeskyttelseskravene med tilhørende dokumentationskrav jf. GDPR sammenholdt med tidligere krav i PDL?

Som støtte til besvarelsen af problemformuleringen, vil følgende underspørgsmål blive undersøgt og besvaret i delkonklusionerne.

1. Hvordan spiller art. 5 en rolle i forhold til behandlingssikkerheden i art. 32?
2. Hvordan hænger fortegnelsen i art. 30 sammen med behandlingssikkerheden i art. 32?
3. Kan frivillige tiltag anvendes som dokumentation?

Hensigten er at belyse hvilke krav der stilles til databehandlingssikkerhed i GDPR sammenholdt med tidligere regler i PDL, samt hvordan arbejdet med opfyldelse af dokumentationskravet kan gribes an set ud fra en risiko analyserende tilgang.

FOKUS OG AFGRÆNSNING AF OPGAVE

Fokusområdet for opgaven er behandlingssikkerhed og dokumentationskravet til samme baseret på GDPR art. 32 omkring behandlingssikkerhed sammenlignet med tilsvarende bestemmelser i PDL.

Som en naturlig indgangsvinkel til selve behandlingssikkerheden, vil bestemmelserne i art. 5, 24,25 og art. 30 ligeledes blive behandlet, idet øvrige bestemmelser i GDPR alene vil blive inddraget i opgaven hvor dette opfylder et formål.

Bestemmelser fra andre retsområder bliver anvendt såfremt sådanne måtte kunne bidrage til besvarelsen, men vil i øvrigt ikke blive behandlet.

Uagtet at GDPR er gældende for hele EU, vil opgaven alene have fokus på de danske myndigheders opfattelse og fortolkning af bestemmelserne i GDPR. Der vil dog hvor dette giver mening, blive inddraget artikler og andet materiale fra bl.a. Artikel 29-gruppen.

Da der for nuværende ikke findes retspraksis på området fra EU-domstolene, vil der hvor dette opfylder et formål, være henvisninger til tidligere praksis på området jf. tidligere lovgivning efter PDL og databeskyttelsesdirektivet[5].

METODE

Da formålet med opgaven er at analyserer og redegøre nærmere for udstrækningen af kravet om behandlingssikkerhed jf. GDPR art. 32, vil det være nødvendigt også at se på kravet om behandlingssikkerhed jf. tidligere regler og praksis.

Besvarelsen vil derfor være baseret på dels analyse af retsregler i PDL, som nu er af historisk karakter, og dels en analyse af de nu gældende retsregler i GDPR. Der vil efterfølgende anvendes komparativ metode for at fastslå evt. ændringer på området.

Der findes for nuværende ingen retspraksis på området afsagt i henhold til GDPR, så ældre praksis vil blive vurderet for at foretage en vurdering af evt. ændringer GDPR må formodes at medføre omkring behandlingssikkerhed.

Som videnskabeligt redskab anvendes den retsdogmatiske metode, idet metodens opgave er ”*at analyserer og beskrive den i samtidens gældende retstilstand"*[6]

Retsdogmatikken klarlægger og beskriver således gældende ret, og er forbundet med den praktiske anvendelse af samme. Udgangspunktet for at løse juridiske problemer ud fra den retsdogmatiske metode, er derfor retskilder og fortolkningsprincipper udøvet i praksis.

Retskilder skal i denne opgave forstås som love, retspraksis, sædvaner og forholdets natur.

Den retsdogmatiske metode er således baseret på at analyserer og fastlægge de principper der er gældende på det konkrete retsområde, ligesom metoden kan frembringe nye perspektiver på området.

---

[5] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:31995L0046&from=DA - EU direktiv nr. 95/46/EF

[6] Carsten Munk-Hansen ”Retsvidenskabsteori” s. 190

En del af den rets dogmatiske metode er den juridiske metode. Den juridiske metode er baseret på, at faktum sammenlagt med jus leder til et resultat.

Carsten Munk-Hansen beskriver den juridiske metode som følger:[7]

"et faktum (et forhold i den fysiske verden, et hændelsesforløb eller et begreb) *og en retsnorm* (en skreven eller uskreven retsregel) *fører til en konkret løsning* (beslutning, afgørelse, resultat)

Den juridiske metode anvendes således når der er behov for at løse eller redegøre for helt konkrete problemstillinger, ud fra hvad der er gældende ret.

Ved den juridiske metode skal retsreglen findes med baggrund i retskilderne, som danner grundlag for fortolkningen af den retslige løsning.

RETSKILDER

Retskilder deles typisk i 4 hovedgrupper: 1) Lovgivning (herunder andre regler såsom anordninger, bekendtgørelser og cirkulærer, 2) Retspraksis (domstolsafgørelser), 3) Rets sædvaner og kutymer samt 4) Forholdets natur.

I denne opgave behandles både EU-retslig lovgivning samt national lovgivning, ligesom forarbejder og praksis betragtes som retskilder.

EU-retten har forrang for national ret, hvorfor fortolkningen af denne sker i overensstemmelse hermed. Øvrige retskilder bliver indbragt i afhandlingen ud fra den værdi disse måtte tilføre naturligt.

Forarbejder indgår med betydelig vægt for at sikre, at selve teksten i loven fortolkes bedst muligt ud fra lovgivers hensigt.

Der vil endvidere indgå litteratur fra anerkendte forfattere og henvisninger til vejledninger fra DT og andre instanser der måtte have udarbejdet materiale af interesse.

[7] Carsten Munk-Hansen "Retsvidenskabsteori" s. 191-192

DEL 1 – PERSONDATARETTEN

1.1. FRA DIREKTIV TIL FORORDNING

Inden vedtagelsen af GDPR blev persondataretten reguleret af direktiv 95/46/EF. Indholdet af direktivet blev skabt i årene 1990-1995, og altså før internettet for alvor blev taget i brug i begyndelsen af 1995 med frigivelsen af World Wide Web[8], og hvor massive mængder af data begyndte at blive sendt verden rundt og opbevaret på cloud-baseret løsninger.

Der begyndte således at være en massiv udveksling af data på tværs af landegrænserne, ligesom data kunne spredes meget hurtigt via nettet.

Endvidere havde den hastige teknologiske udvikling[9], herunder den enorme brug af internettet med dertil hørende muligheder for opbevaring og håndtering af persondata på flere forskellige internetbaseret platforme bevirket, at der var behov for en mere harmoniseret og opstrammende reform af hele persondataretten.

Som angivet i præambel 3 til GDPR, har Europa-Parlamentets og Rådets direktiv 95/46/EF (4) til formål at "harmonisere beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandlingsaktiviteter… " [10]

Meningen med direktiv 95/46/EF var således allerede ved vedtagelsen, en lovgivning som har en fællesskabsretslig baggrund.[11]

Dette blev fastslået i flere afgørelser afsagt af EU-Domstolen – den første var Österreichischer Rundfunk[12] Sagen omhandlede 2 spørgsmål.

1) Hvorvidt de fællesskabsretslige bestemmelser er en hindring for en national lovgivning
2) Hvorvidt de fællesskabsretslige bestemmelser er direkte anvendelige nationalt

EU-Domstolen slog fast, at såfremt de nationale bestemmelser ikke er forenelige med EMRK's artikel 8, opfylder de nationale bestemmelser heller ikke proportionalitetskravet fastsat i art. 6, stk.

---

[8] Peter Blume "Den nye persondataret" s. 16

[9] https://themis.dk/synopsis/docs/Lovsamling/Persondataforordningen_praeambel.html - Præambel til GDPR pkt. 6

[10] https://themis.dk/synopsis/docs/Lovsamling/Persondataforordningen_praeambel.html - Præambel til GDPR pkt. 3 med henvisning til Europa-Parlamentets og Rådets direktiv 95/46/EF (4)

[11] Waaben og Nielsen "Lov om behandling af personoplysninger" s. 40

[12] De forenede sager C-465/00, C138/01 og C-139/01 – BILAG 1

1 litra c og art. 7, litra c og e i direktiv 95/46/EF samt de grundlæggende frihedsrettigheder der er almindelig rets grundsætninger i praksis.

EU-Domstolen udtalte til spørgsmål 2, at såfremt nationale bestemmelser er i strid med EMRK's art. 8, og ikke opfylder direktivets krav om proportionalitet eller i øvrigt er omfattet af undtagelsen om behandlingsforbud, så er direktivet direkte anvendeligt for den enkelte borger. Den enkelte borger kan derfor støtte ret direkte på direktivets ordlyd.

Den tidligere PDL, der hviler på direktiv 95/46/EF, er ophævet samtidig med ikrafttrædelse af GDPR og DBL.

Dette er dog ikke ensbetydende med, at alt tidligere praksis og den generelle forståelse af persondataretten ændrer sig totalt efter vedtagelsen af GDPR.

Vedtagelsen af GDPR er således langt hen ad vejen en videreførelse af de tidligere regler, dog er der på nogle punkter strammet op på reglerne, ligesom der er indført nye regler – blandt andet på området for behandlingssikkerhed.

"For at sikre effektiv beskyttelse af personoplysninger i Unionen, er det nødvendigt at styrke og præcisere de registreredes rettigheder og de forpligtelser, der påhviler dem, der behandler og træffer afgørelse om behandling af personoplysninger, samt at der gives tilsvarende beføjelser til at føre tilsyn med og sikre overholdelse af reglerne om beskyttelse af personoplysninger og indføres tilsvarende sanktioner ved overtrædelser i medlemsstaterne."[13]

1.1.2 GDPR OG DATABESKYTTELSESLOVEN

Som tidligere nævnt danner GDPR grundstenen i intensionen om, at alle registrerede i EU har krav på beskyttelse af sine personlige data. Forordningen er et omfattende værk, som er forsøgt lavet så udtømmende som muligt for at sikre en ensartet behandling af personoplysninger i EU.

Det har dog ikke med forordningen været muligt at foretage en fuldstændig regulering af alle punkter, hvilket muligvis skyldes de enkelte medlemsstaters ønske om fortsat at have kontrollen.

[13] Præambel til GDPR pkt. 11

Samtidig er der vitale punkter i forordningen der ikke er klart defineret, bl.a. artikel 32 omkring behandlingssikkerhed, hvilket kritiseres af Peter Blume[14] idet han anfører, ”*at der burde være udstedt sekundære retsforskrifter.”*

Peter Blume anfører[15] *”Der er nu en større risiko for, at der allerede af denne grund opstår ujævnheder, således at harmoniseringen reduceres”*

Peter Blume peger samtidig på det forhold, at med den enkelte medlemsstats egen udtømmende regulering, og de enkelte medlemsstaters egne Datatilsyns fortolkning, *”vil der gå en del år, inden forordningen er blevet udfyldt i praksis i de nationale datatilsyn, det Europæiske Databeskyttelsesråd og EU-Domstolen.*[16]

Som supplement til GDPR har de enkelte medlemsstater lovgivet særskilt, hvilket i Danmark har betydet vedtagelse af Databeskyttelsesloven.[17] Databeskyttelsesloven omhandler regler der skal virke som udfyldende regler på de punkter i forordningen, hvor det er overladt til de enkelte medlemsstater at ”bestemme”.

Lovforslag L 68, som ligger til grund for vedtagelsen af Databeskyttelsesloven, og som er baseret på betænkning nr. 1565 om databeskyttelsesforordningen, har i bemærkningerne pkt. 1.1 angivet de kategorier af regler der kan eller skal udfyldes rent nationalt.

I første kategori har MS mulighed for at udnytte det nationale råderum, men er ikke forpligtet hertil. I den anden kategori har MS eksplicitte muligheder for at indføre egne regler med hjemmel i lov, eks. vis valget om hvilken alder der skal betragtes som barn jf. GDPR art. 8.

I tredje kategori kan MS træffe bestemmelser om begrænsninger, mens den fjerde kategori omhandler MS forpligtelsen til at fastsætte nationale regler om oprettelse af uafhængige tilsynsmyndigheder.

En stor del af DBL omhandler dog regler for den offentlige sektor, videregivelse af virksomhedsoplysninger i forbindelse med kreditbureauer og en præcisering af behandlingshjemlen i henhold til forordningen.

Det er således selve GDPR der er det primære og styrende redskab i håndteringen af persondata.

---

[14] Peter Blume ”Den nye persondataret” s. 52

[15] Peter Blume ”Den nye persondataret” s. 52

[16] Peter Blume ”Den nye persondataret” s.52

[17] https://www.retsinformation.dk/Forms/r0710.aspx?id=201319 - Databeskyttelsesloven (DBL) Lov 502 af 23/05/2018

1.2 BESKRIVELSE AF BEGREBER/DATATYPER (SAMMENLIGNING ML. PDL OG GDPR)

1.2.1 HVAD ER PERSONDATA

Mange af de begreber der var gældende i den tidligere Persondatalov går igen i GDPR. Dette skyldes, at både PDL og GDPR bygger på grundprincipperne om, at data skal behandles lovligt, rimeligt, og på en gennemsigtigt måde for den registrerede. Endvidere skal behandlingen være formålsbegrænset, da data alene må indsamles til et udtrykkeligt og sagligt formål, ligesom der skal påses en dataminimering så data ikke anvendes til andet end det indsamlede formål, og i øvrigt ikke opbevares længere end højst nødvendigt.

Det er således den registrerede der er i fokus, og det er dennes interesser der primært skal varetages i forbindelse med enhver form for behandling af persondata.

Det følger således af GDPR art. 1 stk. 2

"Denne forordning beskytter fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger"

Både PDL[18] og GDPR[19] angiver hvad der forstås ved "personoplysninger".

"Enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede).

GDPR udpensler begrebet yderligere ved at angive hvad sådanne data kan være, herunder *navn, ID nummer, lokaliseringsdata, en online identifikation eller et eller flere elementer, der er særlige for denne fysiske fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.*[20]

Opremsningen i GDPR er ikke udtømmende, og det er således næsten kun fantasien der sætter grænser for, hvilke oplysninger der kan anses for enten at være af en karakter der direkte kan identificerer en person eller være af en sådan karakter at de må anses for at være personhenførbare til en bestemt person/registrerede.

---

[18] https://www.retsinformation.dk/forms/r0710.aspx?id=828 – Persondataloven (PDL) kap. 2, § 3 stk. 1

[19] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679&from=DA - GDPR Art. 4, stk. 1

[20] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679&from=DA - GDPR art. 4 stk. 1

I EUD C-582/14 afgjorde EU-Domstolen det principielle spørgsmål, om en dynamisk IP-adresse som udbydes af online-medietjenester må opbevares i forbindelse med en persons søgning på internettet. Domstolen slog fast, at hvis udbyder råder over lovlige hjælpemidler der gør det muligt at få en person identificeret gennem den yderligere viden som denne persons internetudbyder råder over, så anses en IP-adresse for at være en persondata.[21]

Begrebet "persondata" er således et meget bredt begreb og omhandler således også billedmateriale, overvågningsvideo etc.

Da begrebet "personoplysninger" således ikke er noget nyt i GDPR, men allerede eksisterede – også under PDL – burde alle virksomheder, allerede inden GDPR trådte i kraft, have fuldt styr på hvilke data der behandles.

Med den panik der har været omkring ikrafttræden af GDPR, syntes dette ikke at være tilfældet.

1.2.2 BEHANDLING AF ALMINDELIGE DATA (GDPR ART. 6,1 OG PDL § 6,1)

Hverken PDL eller GDPR har et særskilt punkt med angivelse af behandlingsbetingelser for "almindelige data", som tilfældet er med særligt følsomme oplysninger og særlige forhold der er særskilt udskilt i GDPR art. 9, 10 og 87. Dog fastslås det i GDPR art. 6 stk. 1 og PDL § 6 stk. 1 de behandlingsbetingelser, der udgør de generelle betingelser for hvornår en behandling må finde sted.

I GDPR er Art. 6 stk. 1 derfor kernefunktionen i den regulering som forordningen fastlægger.[22] Art. 6 stk. 1 angiver under hvilke forhold en behandling er lovlig, og hvis ikke andet er angivet andetsteds i GDPR (art. 9, 10 og 87), vil det være reglerne i art. 6 stk. 1 der er gældende for behandlingen.

Det er alene én af de nævnte betingelser der skal være opfyldt førend der foreligger en lovlig behandlingshjemmel[23], hvilket åbner muligheder for, at en dataansvarlig frit kan vælge med hvilken

[21] I EUD C-582/14, Retsforskrift 65 stk. 1 – BILAG 2

[22] Peter Blume, "Den nye persondataret" s. 95

[23] http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf - Betænkning 1565 pkt. 3.3.1

hjemmel der behandles. Der kan således principielt godt være tale om, at flere betingelser er opfyldt på én gang.

I betænkningen[24] til GDPR fremgår, at behandlingen af data, uagtet at hjemlen er til stede, også skal påse at de grundæggende principper i Art. 5 stk. 1 om god databehandlingsskik fortsat er opfyldt.

Tidligere praksis fra DT viser også, at tilsynet som oftest har henvisning til mere end én af behandlingsbetingelserne. Dette kan bl.a. illustreres ved kendelse publiceret af DT d. 13.08.2018, afgjort efter reglerne i PDL.[25] Her blev det gjort gældende, at behandlingshjemlen skulle findes i PDL § 6 stk. 1 nr. 5 og § 6 stk. 1 nr. 7.

Da ordlyden i art. 6 stk. 1 er lig den ordlyd der fremgår af PDL kap. 6 stk. 1 forventes det, at gældende praksis fortsat vil blive fulgt fremadrettet jf. bestemmelserne i GDPR.

1.2.3 BEHANDLING AF SÆRLIGT FØLSOMME DATA (GDPR ART. 9 – PDL § 7)

Både PDL og GDPR har særligt udskilt specielle data, som alene må behandles hvis der foreligger en særlig hjemmel hertil. Disse typer af data betegnes som ”særligt følsomme data”.

I PDL[26] er anført følgende *” Der må ikke behandles oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold”.*

I GDPR[27] er omfanget af disse oplysninger udvidet som følger:

”Behandling af personoplysninger 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 er forbudt.”*

---

[24] http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf - Betænkning 1565 pkt. 3.3.2.1

[25] DT afgørelse ”Lasso X ApS offentliggørelse af data indhentet fra CVR – BILAG 3

[26] https://www.retsinformation.dk/forms/r0710.aspx?id=828 – (PDL) § 7 stk. 1

[27] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679&from=DA – (GDPR) art. 9 stk. 1

Disse ”særligt følsomme” data må dog behandles, hvis den registrerede har givet et udtrykkeligt samtykke, eller hvis behandlingen er nødvendig for at overholde den registreredes arbejds-, sundheds-, og sociale rettigheder, eller behandlingen er nødvendig for generelt at beskytte den registrerede eller samfundets interesser.

Årsagen til denne udskillelse af data skal ses i lyset af, at man med loven tilsigter et højt beskyttelsesniveau i forhold til den enkelte borger. [28]

Listen er udtømmende jf. forarbejderne til PDL § 7 stk. 1.

Tilføjelsen af genetiske og biometriske data under de ”særligt følsomme” data i GDPR art. 9 er en ændring i forhold til ordlyden i PDL § 7.

Artikel 29-gruppen har tidligere – i 2012 – udtalt, at behandlingen af biometriske data ”*skal være baseret på et af de legitime grundlag, som er beskrevet i artikel 7 i databeskyttelsesdirektivet”*[29] Dette svarer til PDL § 6.

Endvidere har artikel 29-gruppen[30] anført, at såfremt behandlingen af biometriske data afsløre forhold der vil være omfattet af PDL § 7, falder behandlingen ind under reglerne om behandling af ”særligt følsomme” data i stedet for under § 6 om ”almindelige data”.

DT har tidligere anset genetiske og biometriske data for at være ”almindelige data” omfattet af § 6 i PDL, hvilket illustreres ved udtalelse fra DT i DT’s journal nr. 2009-082-0087[31] i en sag fra Tivoli, som ville benytte ansigtsgenkendelse for kunder der ønskede at gå direkte fra Tivoli og ind i restaurant Wagamama og retur til Tivoli igen.

Problemet i sagen var, at gæster til restauranten både kunne komme ind direkte fra gaden, og via Tivoli. For at undgå, at gæster kom ind i Tivoli direkte fra restauranten uden at betale entre til Tivoli, ønskede man at anvende ansigtsgenkendelse således, at alene folk der var blevet ansigtsscannet fra Tivoli indgangen til restauranten kunne komme retur til Tivoli uden at skulle betale entre til Tivoli igen.

DT udtalte, at *”der er tale om behandling af almindelige ikke følsomme oplysninger omfattet af PDL § 6.”*

---

[28] Waaben og Nielsen, ”Lov om behandling af personoplysninger” s. 281

[29] Artikel 29-gruppen udtalelse – WP 193 s. 10 – BILAG 4

[30] Artikel 29-gruppen udtalelse – WP 193 s. 15 – BILAG 4

[31] DT afgørelse journal nr. 2009-082-0087 – BILAG 5

Efter vedtagelsen af GDPR er det nu til gengæld slået helt fast, at genetiske og biometriske data hører under kategorien ”særligt følsomme” data – det skal dog tilføjes, at dette alene gælder såfremt disse anvendes til at identificere en person jf. sidste led af sætningen i art. 9 stk. 1 der omhandler genetiske og biometriske data.

Såfremt genetiske og biometriske data anvendes til eksempelvis at verificere en person, vil dataene hører under almindelige data jf. art. 6.

Der skal derfor fremadrettet foretages en vurdering af hvad genetiske og biometriske data anvendes til således, at den rette hjemmel anvendes.

”Særligt følsomme” data jf. art. 9 stk. 1, må dog behandles såfremt den registrerede har givet et udtrykkeligt samtykke, eller behandlingen falder ind under andre af de i art. 9 stk. 2 nævnte undtagelser om forhandlingsforbud.

Det forventes ikke, at praksis efter PDL ændrer sig efter ikrafttræden af GDPR – dog er det nu blevet slået fast, at genetiske og biometriske data hører under ”særligt følsomme” data såfremt disse anvendes til klart og entydigt at identificerer en person, hvorfor praksis dog vil ændre sig på dette punkt.

1.2.4 BEHANDLING AF SEMI-FØLSOMME OPLYSNINGER (STRAFFEDOMME OG LOVOVERTRÆDELSER)

Både PDL og GDPR har særligt udskilt personoplysninger der vedrører straffedomme og lovovertrædelser.

Det fremgår af artikel 8 stk. 5 i databeskyttelsesdirektivet[32], at *”Behandling af oplysninger om lovovertrædelser, straffedomme og sikkerhedsforanstaltninger må kun foretages under kontrol af en offentlig myndighed”*

I PDL er sådanne data angivet i § 8 stk. 1 – *” For den offentlige forvaltning må der ikke behandles oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i § 7 stk. 1 nævnte, medmindre det er nødvendigt for varetagelsen af myndighedens opgave.*

[32] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:31995L0046&from=DA - EU direktiv 95/46/EF af 24. oktober 1995

En tilsvarende ordlyd er angivet i GDPR art. 10 der slår fast, at behandling af data om straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger alene må foretages under kontrol af en offentlig myndighed.

Der er hverken i direktiv 95/46/EF eller i GDPR taget stilling til, hvad der nøjagtigt menes med lovovertrædelser, straffedomme eller sikkerhedsforanstaltninger.

Registerudvalget anførte dog i betænkning 1345, at den samlede forståelse af udtrykkene må anses for at være dækket af udtrykket "strafbare forhold".

Det følger af eksisterende praksis, at begrebet "strafbare forhold" kan strækkes vidt i relation til hvad der omfattes af PDL § 8 stk. 1. Således er det angivet[33], at eksempelvis også rettighedsfrakendelser sandsynligvis vil være omfattet af PDL § 8.

Der er i PDL § 8 stk. 4 angivet, at private alene må behandle oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold nævnt i § 7 stk. 1, hvis den registrerede har givet sit udtrykkelige samtykke.

Der er i GDPR art. 10 forskel på, om strafbare forhold behandles af offentlige myndigheder som et nødvendigt og direkte led i en forvaltnings arbejde, eller om oplysningerne behandles af en privat, hvortil der altid kræves udtrykkeligt samtykke eller hvor den privates indsamlings interesse overstiger hensynet til den registrerede.

DBL § 8 stk. 5 udvider reelt ordlyden i GDPR art. 10 ved at give både offentlige myndigheder og private behandlingsret i tilfælde af, at betingelserne i DBL § 7 (GDPR art. 9) er opfyldt.

Det er dog slået helt fast i PDL § 8 stk. 7 samt i GDPR art. 10 sidste linje, at et fuldstændigt/omfattende register over straffedomme kun må føres af en offentlig myndighed. En privat persons indsamling af data omfattet af § 8, er således begrænset til alene at måtte omfatte en begrænset indsamling til et begrænset register.

Bestemmelserne i PDL § 8, GDPR art. 10 og DBL § 8 er stort set ens, og det forventes, at den hidtidige praksis fortsætter fremadrettet.

[33] Waaben og Nielsen "Lov om behandling af personoplysninger" s. 307

1.2.5 BEHANDLING AF CPR NR./NATIONALT IDENTIFIKATIONSNUMMER – ART. 87 OG PDL § 11

Både PDL § 11, DBL § 11 og GDPR art. 87 omhandler behandling af nationale identifikationsnumre – her i Danmark CPR nr.

Det danske CPR nr. består af 6 cifre (fødselsdato og år), som er almindelige data omhandlet af GDPR art. 6, mens de 4 sidste cifre er fortrolige oplysninger der gør en person identificerbar og derfor samlet er omfattet af reglerne om databeskyttelse.

I PDL § 11 er angivet, at offentlige myndigheder kan behandle CPR nr. som journal nr. eller med henblik på entydig identifikation af en person. Private må ligeledes behandle CPR nr. hvis der er givet udtrykkeligt samtykke hertil, eller hvis det følger af lov eller bestemmelser fastsat i.h.t. lov.

I GDPR art. 87 er der lagt op til, at de nationale myndigheder selv kan fastsætte regler omkring behandling af CPR nr.

De hidtidige regler i PDL § 11 er således opretholdt i DBL § 11, dog således, at der er åbnet op for muligheden for, at private også kan behandle CPR nr. under hensyn til, at behandlingen sker efter DBL § 7 (GDPR art. 9 om følsomme data).

Hvorvidt denne udvidelse af privates ret til også at behandle CPR nr. vil føre til uheldige konsekvenser, må fremtidig praksis vise.

KONKLUSION DEL 1

Valget af en forordning i stedet for et direktiv skal ses i lyset af, at det tidligere EU direktiv 95/46/EF ikke gennem årene viste sig at harmoniserer håndteringen af data i det omfang der var ønsket ved indførelsen af direktivet.

Uagtet at de enkelte MS har skulle/kunne foretage udfyldninger, så ligger der en klar signalværdi i valget af en forordning, i stedet for et direktiv.

Peter Blume anfører[34] *"Uanset at opdelingen mellem disse 2 grundformer for retsakter i den sekundære EU-ret på denne måde kan være flydende, sender anvendelsen af en forordning dog under alle omstændigheder et signal om, at den EU-retlig regulering skal tillægges betydelig vægt*"

Det vil primært blive EU-domstolen der fremadrettet skal sættes dagsordenen for udstrækningen og fortolkningen af GDPR, idet der – netop begrundet i, at de enkelte MS selv har sørget for udfyldning – ikke vil være tale om en totalharmonisering. De nationale domstole vil sandsynligvis derfor have forskellige opfattelser og fortolkninger af bestemmelserne, hvorfor EU-domstolen vil få flere præjudicielle sager at forholde sig til.

Opsplitningen af data i "almindelige data" og "følsomme data" i GDPR, er en videreførelse og traditionel persondataretslig opsplitning. Ud over tilføjelsen om håndtering af genetiske og biometriske data i GDPR art. 9, er det de samme typer af data der er nævnt i PDL § 7 og 8.

Ved overgangen fra Registerloven til PDL lagde Folketinget vægt på, at Registertilsynets praksis stadig skulle tages i betragtning ved anvendelsen af PDL.[35]

Der er ikke ved overgangen fra PDL til GDPR angivet samme hensyn, men det må formodes, at tidligere praksis langt hen ad vejen fortsat vil have betydning ved fortolkning og afgørelser også efter GDPR.

DEL 2 – BEHANDLINGSPRINCIPPER OG SIKKERHEDSKRAV

2.1. ART. 5 – ANSVARLIGHED (ACCOUNTABILITY)

Artikel 5 i GDPR omhandler principperne for al databehandling omfattet af GDPR, uanset typen af data der behandles.

Det er således artikel 5 der er det grundlæggende fundament[36] for den lovlighed der skal være til stede for at der må behandles persondata, idet artikel 5 omhandler den ansvarlighed der skal lægges for dagen for enhver der behandler persondata.

[34] Peter Blume "Den nye persondataret" s. 227

[35] Peter Blume "Den nye persondataret" s. 241

[36] Peter Blume "Den nye persondataret" s. 85

Artikel 5 stk. 1a angiver, at personoplysninger skal *"behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede"*

Dette svarer til ordlyden i PDL § 5 stk. 1 der anvender begrebet "god databehandlingsskik", som dog anses for at være indholdsmæssigt lig kravet anført i GDPR art. 5 stk. 1.

Netop kravet om ansvarlighed skal overholdes ved enhver form for behandling af persondata, og det er særligt også denne ansvarlighed den DA skal kunne påvise er overholdt.

Lovlighed

Kravet i GDPR om lovlighed skal forstås således, at der alene må behandles persondata såfremt denne behandling ikke strider imod anden lovgivning. GDPR tager således alene stilling til selve behandlingen, men ikke til hvorvidt der evt. måtte forefindes anden lovgivning hvor en decideret behandling er direkte ulovlig.

Såfremt behandlingen strider imod en anden lovs præceptive regler, vil det derfor ikke være lovligt at foretage behandlingen af persondata med henvisning til GDPR.

Peter Blume anfører[37], at *"Herved betones, at persondataretten må forstås som en del af den samlede retsorden……..".*

Rimelighed og gennemsigtighed

Kravet om rimelighed skal ses i lyset af, at en behandling over for den registrerede skal være gennemskuelig, oplyst i et klart og forståeligt sprog, og at den registrerede har fuld indsigt i behandlingen. Netop kravet om rimelighed har været benyttet flittigt i DT's afgørelser, og Peter Blume anfører[38], at *"Denne del af bestemmelsen har i Datatilsynets praksis fungeret, og vil fortsat kunne fungere som en generalklausul"*

Som eksempel kan nævnes afgørelse fra DT[39], hvor Tivoli ansøgte om tilladelse til at anvende en billeddata base i forbindelse med adgangskontrol til Tivoli, primært for at kunne dæmme op for, at allerede eksisterende kunder snyder ved at lade andre personer anvende de udstedte abonnementskort. DT nævnte i den forbindelse, at *"Tivoli bør basere sin behandling af digitale billeder af årskortholdere på et samtykke fra årskortholderen til, at Tivoli tager et billede af den pågældende og opbevarer det i en database jf. herved PDL § 6 stk. 1 nr. 1, for derved også at*

[37] Peter Blume "Den nye persondataret" s. 85

[38] Peter Blume "Den nye persondataret" s. 85

[39] DT's afgørelse 2005-212-0299 – BILAG 6

sikre den enkelte abonnents mulighed for i stedet at anvende billedlegitimation i forbindelse med årskortet."

Der skal derfor sikres den registrerede en gennemsigtighed så den registrerede forstår og kan overskue behandlingen.

Netop kravet om rimelighed er ikke nærmere defineret i hverken PDL eller GDPR, så der er åbnet op for, at DT selv kan stille betingelser og foretage vurdering af hvorvidt behandlingen må anses for at være rimelig og i tråd med GDPR's regler.

Dette kan besværliggøre den DA's muligheder for at vide hvorvidt denne rent faktisk opfylder kravet om rimelighed i behandlingen, men det må forventes, at den DA loyalt oplyser og sørger for, at behandlingen ikke strider imod principperne i forordningen.

Udtrykkeligt angivne og legitime formål - formålsbestemthed

Artikel 5 omhandler også et krav om, at data alene må indsamles til et *"udtrykkeligt angivet og legitimt formål".* Dette er angivet i artikel 5 stk. 1b

I PDL er angivet, at indsamlingen skal ske til *"udtrykkeligt angivne og saglige formål".*

De forskellige udtryk "legitime" og "saglige" formål anses dog for at have samme betydning.

Artikel 29 gruppen har angivet, at formålsbegrænsningen består af 2 hovedpunkter, nemlig at data alene må indsamles til specificeret, udtrykkelige og saglige formål, og ikke må genbehandles til formål der er uforenelige med den oprindelige indsamling. [40]

Saglighedsbegrebet skal være opfyldt i relation til generel behandling af data og i alle behandlingens faser.

Der må ligeledes ikke være uforenelighed mellem det formål data oprindeligt er indsamlet til og en evt. senere behandling. Årsagen hertil skal findes i forholdet til den registrerede, som jo jf. GDPR art. 5 stk. 1a har krav på gennemsigtighed i den behandling der finder sted. Denne gennemsigtighed ville forsvinde såfremt en DA blot kunne anvende indsamlede data til lige hvad der måtte passe denne.

[40] Udtalelse af Artikel 29-gruppen nr. 3/2013, s. 38 (WP 203) – BILAG 7

Der bør ved vurderingen af hvorvidt en behandling er forenelig med det oprindelige formål ved indsamlingen, tages højde for alle relevante forhold, herunder om den registrerede med rimelighed må forvente at de indsamlede data anvendes til andre formål.

Som eksempel kan nævnes afgørelse fra DT[41] som omhandler Forsvarets videregivelse af personaleoplysninger til brug for markedsføring. Forsvaret havde videregivet personaleoplysninger til forsikringsselskabet Topdanmark i forbindelse med en aftale Forsvaret havde med Topdanmark om, at yde medarbejderrabat på forsikringer til medarbejdere i Forsvaret.

DT lagde vægt på, at *"da de videregivne data er indsamlet og behandlet for at administrere et ansættelsesforhold og, at videregivelse til en privat virksomhed med henblik på markedsføring ikke kan anses som foreneligt med dette formål."*

Det er den dataansvarlige der skal kunne redegøre for, at den evt. nye behandling ikke er uforeneligt med det oprindelige formål. Dette betyder samtidig, at den nye anvendelse af dataene ikke nødvendigvis skal være foreneligt med det oprindelige formål med indsamlingen.

Der er særligt ét punkt der adskiller bestemmelserne i GDPR med bestemmelserne i PDL, nemlig spørgsmålet om samkøring af data.

Udgangspunktet er, at der alene kan ske samkøring af data hvis en sådan samkøring ikke er uforeneligt med det oprindelige indsamlet formål jf. GDPR art. 5 stk. 1b. Dette er dog modificeret i GDPR art. 6 stk. 4 der bestemmer, at hvis behandling sker til andet formål end det oprindelige, og ikke er baseret på den registreredes samtykke, skal den dataansvarlige, for at afgøre om der er et foreneligt formål tage hensyn til[42]

1) Forbindelsen mellem oprindeligt formål og formålet ved senere behandling
2) Sammenhængen mellem den registrerede og den DA oplysninger om anvendelsen ved indsamlingen
3) Dataenes art – art. 9/art. 10
4) Mulige konsekvenser for den registrerede ved viderebehandling
5) Fornødne garantier – eksempelvis kryptering eller pseudonymisering

[41] DT afgørelse 2008-632-0034 – BILAG 8

[42] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679&from=DA – (GDPR) art. 6 stk. 4 samt https://www.retsinformation.dk/Forms/r0710.aspx?id=201319 - Databeskyttelsesloven (DBL) § 5 stk. 2

Peter Blume angiver[43] det uheldige i, at ovennævnte ordlyd er angivet i GDPR art. 6 stk. 4 under "lovlig behandling", og ikke under art. 5 stk. 1b som et princip for behandling, idet selve formålsbestemthedsprincippet og foreneligheds princippet henhører under behandlingsprincipper, og ikke under behandlingsbetingelse.

Sandsynligvis af hensyn til, at særligt offentlige forvaltninger ofte har brug for samme data til flere forskellige formål, og at der sker en større og større digitalisering indenfor forvaltningen, er der derfor i GDPR art. 6 stk. 4 og DBL § 5 stk. 3 angivet en hjælpende hånd, idet der er åbnet op for, at Justitsministeren inden for rammerne af GDPR art. 23, kan sætte nærmere regler op således, at offentlige myndigheder må viderebehandle til andre formål end de oprindelige – uafhængigt af formålenes forenelighed.

Dette gælder dog alene oplysninger der ikke er omfattet af GDPR art. 9 og art. 10 med mindre, at oplysninger omfattet af art. 9 stk. 1 er indsamlet i medfør af DBL § 7 stk. 3 eller sundhedslovgivningen. Sidstnævnte datatyper må dog alene viderebehandles, hvis formålet med viderebehandlingen er foreneligt med det oprindelige formål.

Den nuværende praksis har været, at der skulle søges tilladelse hos DT såfremt der for offentlige forvaltninger skulle ske samkøring af data med det formål at udøve en kontrol. Dette jf. PDL § 45 stk. 1 pkt. 4, som ikke længere er gældende, hvorfor der ikke længere skal søges om tilladelse hos DT.

Det indebærer, at den offentlige forvaltning der ønsker at foretage en samkøring af data med flere afdelinger internt i forvaltningen, og hvor en sådan samkøring ikke er uforenelig med det oprindelige formål dataene blev indsamlet til, kan gøre dette uden specifik tilladelse fra DT.

Da en sådan samkøring kan indebærer en øget risiko for den registrerede, anbefaler Peter Blume[44], at der overvejes hvorvidt en konsekvensanalyse vil være påkrævet som følge af denne samkøring.

Meningen med både GDPR art. 6 stk. 4 og art. 5 stk. 2-3 har været, at skabe større fleksibilitet for offentlige myndigheder til samkøring af data uden skelen til formålsbestemthedsprincippet. Peter Blume anfører dog[45], at *"ved som i artikel 6(4) at sammenblande princip og behandlingsbetingelse begås efter sædvanlig opfattelse en persondataretlig dødssynd"*

[43] Peter Blume "Den nye persondataret" s. 88

[44] Peter Blume "Den nye persondataret" s. 88

[45] Peter Blume "Den nye persondataret" s. 91

Data der behandles til arkiv- videnskabelige- statistiske- eller historisk forskning i samfundets interesse anses ikke for at være uforenelig med det oprindelige formål.

Tilstrækkelige, relevante og begrænset

Det følger endvidere af GDPR art. 5 stk. c, at de indsamlede data skal være tilstrækkelige, relevante og begrænset til hvad der er nødvendigt i forhold til formålet med behandlingen.

Ordet ”dataminimering” er endvidere angivet, hvilket indebærer, at den DA ikke må indsamle data som denne ikke har behov for, hvilket samtidig indebærer, at proportionalitetsprincippet skal overholdes.

Der må derfor ikke indsamles data som ikke tjener et formål hos den DA, og denne skal for så vidt muligt sørge for, at der ikke indsamles og lagres data med mindre dette er påkrævet, altså tjener et formål.

Bevisbyrden for indsamlingen, anvendelsen og opbevaringen af data påhviler den DA, som endvidere skal kunne dokumentere og begrunde formålet hermed.

Netop kravet om dataminimering indebærer, at den DA bør overveje hvorvidt data denne har indsamlet og opbevarer skal beskyttes yderligere i form af enten kryptering eller pseudonymisering som angivet i art. 32 stk. 1a.

Tilsvarende ordlyd er anvendt i PDL, hvorfor det må formodes at praksis og forståelse efter GDPR vil fortsætte uændret.

Korrekte data

I GDPR art. 5 stk. 1 d er angivet, at dataene skal være korrekte og ajourførte i forhold til de formål de behandles, ellers skal dataene straks slettes eller berigtiges.

Tilsvarende ordlyd findes også i PDL § 5 stk. 4, idet der dog her er angivet, at behandlingen skal tilrettelægges så der løbende foretages en ajourføring af disse.

Der er ikke i hverken præamblen til GDPR, i selve GDPR eller i PDL angivet hvad der menes med ”nødvendig ajourføring”, men ifølge Peter Blume[46], *”må det antages, at der er indbygget et vist ressourcemæssigt hensyn, og i praksis er det blevet lagt til grund, at en dataansvarlig, afhængig af*

[46] Peter Blume ” Den nye persondataret” s. 93

hvilke typer personoplysninger der er tale om, har indrettet rutiner, som med passende mellemrum, men altså ikke dagligt, gør det muligt at efterse datakvaliteten."

Når samtidig henses til ordet "straks" i GDPR art. 5 stk. 1d omkring sletning eller berigtigelse, må det formodes at der skal reageres med det samme den DA opdager at dataene er ukorrekte.

Tidsmæssig opbevaring

Både i PDL § 5 stk. 5 samt i GDPR art. 5 stk. 1 e er angivet, at der ikke må opbevares data på en måde hvor det er muligt at identificerer den registrerede i længere tidsrum end nødvendigt end det angivne formål foreskriver.

Den DA skal derfor ved indsamlingen over for den registrerede angive hvor længe denne opbevarer dataene, hvilket skal hænge sammen med det formål dataene er indsamlet til.

Den tidsmæssige begrænsning hænger sammen med kravet om dataminimering og skal sikre at der ikke finder en decideret dataophobning sted blot fordi det er lettere for den DA ikke at have procedurer og politikker for hvornår data skal slettes.

Peter Blume angiver[47], at *"Det er ligeledes antaget i dansk persondataret, at der gælder en vejledende 5-års grænse, som ikke udelukker, at fristen kan være både kortere og længere. Dette kan nok fortsat lægges til grund".*

Den 5-årige praksis kan endvidere hænge sammen med kravet i Bogføringsloven[48], der i kapitel 5 § 10 anfører,

"§ 10. *Den bogføringspligtige skal opbevare regnskabsmaterialet på betryggende vis i 5 år fra udgangen af det regnskabsår, materialet vedrører. Opbevaringen skal ske på en måde, som i hele opbevaringsperioden muliggør en selvstændig og entydig fremfinding af det pågældende regnskabsmateriale."*

Tilstrækkelig sikkerhed

Som noget nyt i GDPR i forhold til PDL, er der i art. 5 stk. 1 f indført et punkt om at implementere de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre og beskytte de data der behandles.

---

[47] Peter Blume "Den nye persondataret" s. 94

[48] Bogføringsloven - LBK nr. 648 af 15/06/2006

Denne passus fandtes ikke i PDL, og der er nu sat ekstra fokus på, at behandlingssikkerheden overholdes.

Selve behandlingssikkerheden er således nu gjort til et decideret behandlingsprincip.

2.1.2 ART. 24 – DEN DA ANSVAR

Som udgangspunkt er det den dataansvarlige der bærer ansvaret for behandling af den registreredes persondata.

Der er derfor i GDPR art. 24 angivet et afsnit alene gående på den dataansvarliges ansvar, hvilket er nyt i forhold ti PDL.

Den dataansvarlige er jf. art. 24 stk. 1 forpligtet til – under hensynstagen til behandlingens karakter, omfang og sandsynlige risici for at der sker krænkelse af den registreredes rettigheder – at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre, at behandlingen er i overensstemmelse med GDPR.

Endvidere skal den dataansvarlige være i stand til at påvise, at bestemmelserne overholdes, ligesom der løbende skal foretages revidering og ajourføring af de sikkerhedsforanstaltninger den dataansvarlige foretager.

GDPR art. 24 stk. 1 er således 2-delt, idet bestemmelsen indeholder

1) et krav om at foretage en risikovurdering og efter bedste evne imødegå en risiko, samt

2) at kunne påvise at reglerne er opfyldt.

Den dataansvarlige er således forpligtet til at foretage en decideret risikovurdering af hvilke risici der kan ramme den registrerede i forbindelse med den dataansvarliges behandling. Dette indebærer, at den dataansvarlige skal forholde sig til typen af data der behandles, i hvilken forbindelse behandlingen sker og hvilke gener/risici behandlingen måtte kunne have for den registrerede.

Denne risikovurdering er beskrevet i præambel 76[49].

[49] https://themis.dk/synopsis/docs/Lovsamling/Persondataforordningen_praeambel.html - Præambel til GDPR pkt. 76

Den dataansvarlige skal nu have et totalt overblik over hele behandlingsforløbet, og skal kunne angive hvor i forløbet data vil kunne misbruges eller på anden måde kompromitteres til skade for den registrerede. En sådan risiko, skal af den dataansvarlige imødegås på bedste vis via tekniske og organisatoriske tiltag.

Meningen er klart at forsøge at imødegå misbrug og kompromittering af data ved allerede ved behandlingens start, at have et overblik over de risici der måtte være i forbindelse med behandlingen.

Som det gamle ordsprog siger, ”Det er bedre at forebygge end at helbrede”.

Der er dog i art. 24 stk. 2 angivet, at de sikkerhedsforanstaltninger den dataansvarlige skal indføre kan være af forskellig karakter.

Dette hænger sammen med, at databehandling kan være forskellig i omfang og risikomæssigt set, hvorfor art. 24 stk. 2 åbner op for muligheden for, at de krav der stilles til den dataansvarlige omkring implementering af sikkerhedsforanstaltninger skal være rimelige i forhold til behandlingsaktiviteterne.

2.1.3 ART. 25 – DATABESKYTTELSE GENNEM DESIGN OG STANDARDINDSTILLINGER

En af – og måske den vigtigste i forhold til databeskyttelse – nyskabelse i forhold til PDL, er ordlyden i GDPR art. 25, der omhandler den dataansvarliges forpligtelse til at implementerer **tekniske og organisatoriske sikkerhedsforanstaltninger.**

Hvad der helt præcis ligger i disse ord er ikke nærmere specificeret i selve GDPR.

Der er dog hjælp at hente i betænkning 1565[50], der beskriver, at *”Begrebet databeskyttelse gennem design” må efter ordlyden opfattes bredt således, at det omfatter både tekniske og organisatoriske foranstaltninger”.*

Tilsvarende er der i præamblen til GDPR pkt. 78[51] angivet, at *”For at kunne påvise overholdelse af denne forordning bør den dataansvarlige vedtage interne politikker og gennemføre*

[50] http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf - Betænkning 1565 for GDPR s. 416

[51] https://themis.dk/synopsis/docs/Lovsamling/Persondataforordningen_praeambel.html - Præambel til GDPR pkt. 78

foranstaltninger, som især lever op til principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger."

Betænkning 1565[52] angiver, at der ved design forstås *"design af IT-systemer, såsom deres tekniske indretning og brugergrænseflade, samt ved indretning af den dataansvarliges organisation"* Dette kan være eksempelvis adgang til PC via personligt brugernavn og kordeord, anvendelse af virusscannere, backup af servere etc.

Den dataansvarlige er således forpligtet til at sikre, at de systemer der anvendes til sikringen af datasikkerheden opfylder kravene i forordningen. Ved indkøb eller udvikling af IT-systemer bør den dataansvarlige sikre sig, at PET (privacy enhancing technologies)[53] indarbejdes i systemet således, at systemet allerede fra start indeholder teknologi der sikre overholdelse af sikkerhedskravene i GDPR.

Såfremt at sikkerhedskravene ikke alene kan opfyldes via design af systemer, er der i art. 25 stk. 2 pålagt den dataansvarlige at implementerer forretningsgange som understøtter databeskyttelsen i designet.

Dette kan eksempelvis være træning af medarbejdere, specifikke procedurer, formåls- og behandlingsbegrænsning etc.

Betænkning 1565[54] anfører, "*Kravet i art. 25 stk. 2, kan således ses som en "tilføjelse" til kravet om databeskyttelse gennem design i art. 25 stk. 1, idet stk. 1 konkret kan indebære, at et system designes med særlige databeskyttelsesfremmende indstillinger indbygget, og bestemmelsen i art. 25 stk. 2, pålægger således den dataansvarlige f.eks. at gøre den mest formålsbegrænsende indstilling af systemet til standardindstillingen"*

Art. 25 er konstrueret således, at der skal tænkes databeskyttelse ind i hele den dataansvarliges proces i det at behandle den registreredes data.

---

[52] http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf - Betænkning 1565 for GDPR s. 417

[53] **Privacy-enhancing technologies** (**PET**) er metoder til beskyttelse af data i overensstemmelse med loven. PET tillader online brugere at beskytte privatlivet for deres personligt identificerbare oplysninger (PII), der leveres til og håndteres af tjenester eller applikationer. – Jf. Wikipedia - https://en.wikipedia.org/wiki/Privacy-enhancing_technologies

[54] http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf - Betænkning 1565 for GDPR s. 421

I art. 25 stk. 1 er ligeledes angivet, at den dataansvarlige skal påse, at tekniske og organisatoriske sikkerhedsforanstaltninger implementeres både på tidspunktet for fastlæggelse af behandlingen, og på tidspunktet for selve behandlingen.

Der skal derfor tænkes datasikkerhed ind allerede i overvejelsesfasen for behandlingen samt løbende i forbindelse med selve behandlingen, idet det forventes, at den dataansvarlige antager en risikobaseret vurdering for at sikre overholdelse af GDPR.

Dette indebærer, at den dataansvarlige ved eksempelvis anskaffelse af nyt IT-udstyr skal tænke datasikkerhed ind allerede ved indkøbet af udstyret. Ligeledes kan der være tale om, at den dataansvarlige ændrer eller omstrukturerer sin organisation for at sikre beskyttelsesniveauet.

Der er i betænkning 1565[55] angivet et eksempel der omhandler det forhold, at hvis et ældre IT-system ikke helt opfylder det tekniske niveau, men udgiften til at bringe systemet op på niveau for at overholde sikkerhedskravene i GDPR er uforholdsmæssig stor i forhold til behandlingen, så kan den dataansvarlige i stedet forsøge at imødekomme sikkerhedskravet ved hjælp af organisatoriske foranstaltninger.

Der skal således ikke anvendes uanede mængder af penge og ressourcer på for enhver pris at opdaterer et ældre system, men der skal generelt tænkes datasikkerhed ind og gøres hvad der må anses for rimeligt ud fra den behandling der foretages, datatyperne og risiciene for integritetskrænkelse for den registrerede.

Der findes således ikke noget konkret krav om hvordan sikkerhedskravet skal løses, men art. 25 stk. 1 peger på, at pseudonymisering og dataminimering kunne være udmærkede indikatorer for, at datasikkerhed er tænkt ind i en generel databeskyttelsespolitik.

Den dataansvarlige bør allerede ved indsamlingen af data tage stilling til hvilke oplysninger der er nødvendige for at opfylde formålet med behandlingen, sørge for at kun de personer der skal håndtere oplysningerne har adgang, sørge for automatisk sletning når oplysningerne ikke længere skal anvendes samt sikre, at oplysningerne ikke deles med andre.

Der er i præambel 78[56] angivet, *"Der bør også tages hensyn til principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i forbindelse med offentlige udbud".*

---

[55] http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf - Betænkning 1565 for GDPR s. 417

[56] https://themis.dk/synopsis/docs/Lovsamling/Persondataforordningen_praeambel.html - Præambel til GDPR pkt. 78

Her nævnes decideret det forhold, at der ved offentlige udbud skal tages hensyn til principperne om databeskyttelse allerede i udbudsprocessen, hvilket betoner vigtigheden af at standardindstillinger i systemer indtænkes allerede på et meget tidligt tidspunkt – ja faktisk før – behandlingsprocessen starter.

Indholdet i art. 25 er nyt i form af, at der decideret nu er indført en forpligtelse for den dataansvarlige til at indføre databeskyttelsen gennem design og standardindstillinger både på tidspunktet før behandlingen påbegyndes og løbende i hele processen.

Selve principperne for databehandlingen og sikkerheden med behandling er som sådan ikke ny, idet kravet om tekniske og organisatoriske foranstaltninger også er anført i direktiv 95/46/EF[57] samt i artikel 29-gruppens udtalelser og praksis fra Datatilsynet.

Uagtet ordlyden i art. 25, så skal den dataansvarlige til alle tider fortsat sikre, at øvrige krav i GDPR er overholdt, herunder bestemmelserne i art. 5 og art. 32 om behandlingssikkerhed.

KONKLUSION DEL 2

Der er ingen tvivl om, at GDPR efter sin ikrafttræden har fået sat stor fokus på begrebet datasikkerhed.

Dette er bl.a. sket gennem forpligtelsen til at påse, at datasikkerhed tænkes ind allerede inden selve behandlingen påbegyndes, og forpligtelsen til hele tiden at følge op på de standardindstillinger ens systemer og processer er sat op til.

Standardindstillinger skal helst følge den teknologiske udvikling så godt som den dataansvarlige formår ud fra en vurdering af behandlingsprincipperne angivet i GDPR art. 5.

Principperne angivet i art. 5 – formålsbegrænsning, dataminimering, kategorien af data, overførselskrav, opbevaringsbegrænsning, grundlaget for behandling og datasikkerhed – skal fortsat overholdes til fulde, uanset hvilke tekniske og organisatoriske foranstaltninger den dataansvarlige måtte have taget. Der er således en direkte sammenhæng mellem

[57] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:31995L0046&from=DA - EU direktiv nr. 95/46/EF artikel 17 samt direktivets præambel nr. 46

behandlingsprincipperne angivet i art. 5, og til de krav der stilles til behandlingssikkerheden i art. 32, hvilket besvarer støttespørgsmål 1 i problemformuleringen.

Hvis de behandlede data er omfattet af art. 9 eller 10, vil der således være et skærpet krav til datasikkerheden end hvis det er almindelige data omfattet af art. 6 stk. 1 der behandles.

Så jo højere risiko der er for at en registreredes rettigheder krænkes, bl.a. typisk ved behandlingen af særligt følsomme data omfattet af art. 9 eller 10, eller hvis en behandling skal omfattes af ny teknologi, til et andet formål eller sammenhæng, så kan den dataansvarlige foretage en konsekvensanalyse[58] (DPIA = Data Protection impact Assessment). Analysen kan anvendes for at få et grundlag til bedømmelse af, om behandlingen overhovedet skal iværksættes, idet analysen samtidig kan påvise, at datasikkerheden er tænkt ind allerede inden behandlingen er påbegyndt, og at tekniske og organisatoriske foranstaltninger er truffet som en konsekvens af analysens resultat.

DEL 3 – FORTEGNELSE OG BEHANDLINGSSIKKERHED

3.1 FORTEGNELSESKRAV ART. 30

Inden ikrafttrædelse af GDPR, var der jf. direktiv 95/46/EF[59] samt PDL[60], angivet en anmeldelsespligt for den DA til DT, i forbindelse med behandling af data for den offentlige forvaltning. Tilsvarende gør sig gældende ved behandling af data for en privat DA, idet disse regler er angivet i PDL § 48 stk. 1

Anmeldelsespligten indebar, at der inden en behandling blev påbegyndt skulle ske anmeldelse af de i PDL § 43 stk. 2 nævnte oplysninger såsom navn og adresse på den DA, formål, behandlingens karakter, kategorier af registrerede etc.

Da PDL § 48 henviser til at det er oplysninger som angivet i PDL § 43 der skal indberettes, er det de samme krav der stilles til anmeldelser til DT uanset om der behandles for private eller offentlige myndigheder.

---

[58] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679&from=DA – (GDPR) art. 35

[59] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:31995L0046&from=DA - EU direktiv nr. 95/46/EF artikel 18

[60] https://www.retsinformation.dk/forms/r0710.aspx?id=828 – (PDL) § 43 stk. 1

Der er dog angivet i PDL § 44, at anmeldelsespligten ikke omfatter behandling af data, som ikke er af fortrolig karakter.

Det fremgår af Waaben og Nielsen[61], at *"begrebet "fortrolig" skal forstås i overensstemmelse med straffelovens § 152 sammenholdt med forvaltningslovens § 27. Efter bestemmelsen i straffelovens § 152 stk. 3, anses en oplysning for at være fortrolig, når den ved lov eller anden gyldig bestemmelse er betegnet som sådan, eller når det i øvrigt er nødvendigt at hemmeligholde den for at varetage væsentlige hensyn til offentlige eller private interesser"*

Denne anmeldelsespligt er bortfaldet efter GDPR er trådt i kraft, idet der nu er indført en generel forpligtelse for den DA og DB samt en eventuel repræsentant til disse, at føre en fortegnelse over den behandling af persondata de hver især udfører.

Der vil i dette afsnit alene blive nævnt den DA, men reglerne omhandler langt hen af vejen også en DB og en evt. repræsentant for henholdsvis den DA og DB.

Dette er angivet i GDPR art. 30.

Hele kravet om at skulle føre fortegnelse hænger sammen med hele princippet om ansvarlighed jf. GDPR art. 5 stk. 2, med tilhørende pligt til at kunne dokumenterer, at GDPR rent faktisk overholdes. Fortegnelserne kan derfor udgøre en del af den dokumentation der skal til for at beskyttelsesreglerne overholdes, og kan samtidig hjælpe den DA med at have et overblik over hvilken form for data og hvordan sådanne behandles.

Fortegnelserne skal forefindes både skriftligt og elektronisk jf. GDPR art. 30 stk. 3.

Til gengæld er der ikke noget specifikt formkrav til hvordan en sådan fortegnelse skal se ud, og fortegnelsen er som udgangspunkt et internt bilag hos den DA. Fortegnelsen skal dog kunne udleveres til DT ved anmodning herom.

Indholdet af fortegnelsen skal som minimum indeholde følgende[62], idet den DA selv kan vælge hvorvidt hans fortegnelse også skal indeholde yderligere oplysninger der kan være relevante at få anført i fortegnelsen.

4. Navn og kontaktoplysninger for DA, denne repræsentant og evt. DPO
5. Formålet med behandlingen
6. Beskrivelse af kategorier af registrerede og kategorier af personoplysninger

[61] Waaben og Nielsen, "Lov om behandling af personoplysninger" s. 578

[62] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679&from=DA – (GDPR) art. 30 stk. 1

7. Kategorier af modtagere data vil blive videregivet til, herunder 3. Lands overførsler og organisationer
8. Forventede slettefrister for de forskellige kategorier af data
9. Generel beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger jf. art. 32

Der skal laves fortegnelse på alle typer af data, uanset om disse falder i kategorien omhandlet i GDPR art. 9, 10 eller blot er almindelige data omhandlet af art. 6.1.

Formål

Som angivet i GDPR art. 30 stk. 1b, så skal formålene med behandlingen være anført i selve fortegnelsen.

Principielt skal alle formål angives i fortegnelsen, men hvis der er situationer hvor flere ”delformål” kan henføres til én sammenhængende behandlingsaktivitet eller samme behandlingshjemmel, vil flere formål kunne slås sammen under én samlet beskrivelse af formål.

Der er i vejledningen fra DT[63] angivet flere forskellige eksempler på en sådan sammenføring af formål under én samlet betegnelse, eksempelvis ”Personaleadministration” hvor både lønudbetaling, barsel, ferie etc. kan henføres.

Der er som noget nyt i GDPR i forhold til PDL, indført et decideret krav om at føre fortegnelse over sine databehandlinger også for en DB.

Oplysningerne som en DB skal føre fortegnelse over, er meget lig dem som en DA er forpligtet til at føre fortegnelse over, men for DB skal der også føres fortegnelse over hvilke aktiviteter DB udfører for hver DA, ligesom der skal angives om der sker dataoverførsel og hvilke sikkerhedsforanstaltninger DB har implementeret.

DB har således fået en mere central rolle og er blevet en ”selvstændig” part der er underlagt særlige krav jf. GDPR i forhold til hvad DB tidligere var jf. PDL.

DB ”nye” status vil ikke blive yderligere behandlet i denne opgave.

Kategorier af data

Der er ligeledes i vejledningen fra DT[64] angivet, at der som minimum for at leve op til kravene om en beskrivelse af kategorierne af personoplysninger skal angives typen af data der behandles.

[63] DT’s ”Vejledning om fortegnelse” af 31.1.2018

[64] DT’s ”Vejledning om fortegnelse” af 31.1.2018

Såfremt der behandles data efter art. 9, skal der angives præcist hvilke af de nævnte data der behandles.

Også inden for de forskellige kategorier, kan det med fordel for den DA angives yderligere oplysninger om de data der behandles – eksempelvis CPR nr., oplysninger om økonomiske forhold etc.

Videregivelse af data

Såfremt data videregives eller vil videregives, skal fortegnelsen ligeledes indeholde oplysninger om hvilke modtagere dataene vil blive videregivet til, herunder om modtagere befinder sig i 3. Land eller er en international organisation.

DT har i sin vejledning angivet, at det alene er oplysninger der regelmæssigt videregives der skal anføres i fortegnelsen.

Dette indebærer, at såfremt en offentlig myndighed ønsker at overføre data fra én afdeling til en anden afdeling, så skal dette anføres i fortegnelsen. Dette kan eksempelvis være fra jobcenteret til SKAT etc.

Hvis data overføres til et andet EU land bør dette ligeledes medtages i fortegnelsen, også uagtet at der ikke kræves særskilt dokumentation når overførslen sker til en anden MS, som jo har samme krav til datasikkerheden efter forordningen. Da der kan være forskelle i de nationale regler, kan en sådan overførsel være vigtig at have med i sin fortegnelse.

Hvis en videregivelse sker til 3. Land, skal der altid i fortegnelsen være vedlagt dokumentation på, at datasikkerheden er undersøgt og at denne kan garanteres. Dette er angivet i GDPR art. 49 stk. 1, 2. afsnit med henvisning til art. 45 om overførsel til 3. lande med godkendt databeskyttelsesniveau, og art. 46 om overførsel omfattet af fornødne garantier.

Ved overførsel af data til 3. lande der ikke allerede har en godkendelse som sikkert overførelsesland fra Kommissionen, skal der anvendes de af Kommissionen udarbejdet overførselsbilag der foreligger på Kommissionens hjemmeside[65]. Der er tale om standardbestemmelser, hvor der skal vælges de korrekte bilag afhængig af om der er tale om overførsel fra en DA i EU til en DA i usikret 3.land, eller om der er tale om overførsel fra en DA i EU til en DB i et usikret land.

[65] http://ec.europa.eu/justice/data-protection/internationaltransfers/transfer/index_en.htm

Beskyttelseskravet er ikke nyt, idet der allerede i PDL § 27 er angivet reglerne for overførsel af data til 3. Lande, herunder at der skal være sikret et tilstrækkeligt beskyttelsesniveau.

Sletning

I Art. 30 stk. 1f er angivet, at hvis det er muligt, skal de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger oplyses.

Dette indebærer, at DA så godt som muligt skal angive hvornår de forskellige kategorier af oplysninger bliver slettet hos DA. Hvis ikke der kan fastsættes en konkret slettetid, skal der angives efter hvilke kriterier en sletning foretages.

Det bør bemærkes, at det ikke er slettefrister for selve behandlingen der er omtalt i art. 30 stk. 1f, men slettefrister for de forskellige kategorier der behandles.

Kravet om angivelse af slettefrister hænger sammen med kravet angivet i GDPR art. 5 stk. 1e om behandlingsbegrænsning, idet der ikke bør opbevares data i længere tid end nødvendigt for at opfylde formålet med databehandlingen.

Tekniske og organisatoriske foranstaltninger

GDPR art. 30 stk. 1g omhandler kravet til en beskrivelse af, hvilke tekniske og organisatoriske foranstaltninger der er foretaget af den DA for at sikre behandlingssikkerheden der er omhandlet i art. 32.

Meningen med selve kravet om at angive de tekniske og organisatoriske foranstaltninger er ikke nøjagtigt at beskrive hvilke tiltag der er taget, men blot en angivelse af hvilke generelle tiltag der anvendes for at sikre behandlingssikkerheden[66].

Også her vil der være hjælp at hente i DT's vejledning om fortegnelse, idet der er angivet eksempler på hvad der evt. vil kunne angives som generelle beskrivelser af foranstaltninger.

Undtaget fra fortegnelsesforpligtelsen

Kravet til at føre fortegnelse over behandlingsaktiviteter har mødt voldsom modstand på virksomhedssiden, idet det er svært ressourcekrævende at føre og vedligeholde et sådant fortegnelses værktøj.

---

[66] http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf - Betænkning 1565, s. 457

Der er således i GDPR art. 30 stk. 5 angivet, at fortegnelsesliste ikke skal laves hvis særlige krav er opfyldt.

Dette betyder bl.a., at virksomheder med under 250 ansatte ikke er forpligtet til at lave fortegnelseslister, med mindre behandlingen vil medføre en risiko for den registreredes rettigheder, eller behandlingen ikke er lejlighedsvis eller omfatter data angivet i art. 9 og/eller art. 10.

Meningen med denne undtagelsesbestemmelse skal ses i lyset af, at det kan virke alt for ressource- og tidskrævende for små og mindre virksomheder at skulle føre sådanne fortegnelser. Dette følger ligeledes af forarbejderne til GDPR[67]

Da de fleste virksomheder behandler data for deres ansatte omkring fagforeningsmæssige forhold, økonomiske forhold etc., vil det nok være forholdsvis begrænset hvor mange virksomheder der rent faktisk er undtaget fra kravet om at føre fortegnelse over deres behandlingsaktiviteter.

Netop den ansvarlighed der skal udvises i henhold til art. 5 er direkte henfør bar til art. 30 jf. art. 5 stk. 2. Fortegnelsen anvendes som en form for dokumentation på, at den DA har tænkt, overvejet og forholdt sig netop til hvilke data der behandles, hvilken hjemmel der er til behandlingen, og ikke mindst, risikoen for krænkelse samt hvordan en krænkelse mødegås samt implementeringen af sikkerhedsforanstaltninger.

Selvom fortegnelsen er intern, må den opfattes som en del af de tekniske og organisatoriske foranstaltninger den DA jf. art. 32 er forpligtet til at tage for at sikre en ordentligt databeskyttelse. Fortegnelsen har således en sammenhæng med den ansvarlighed der skal påses jf. art. 5, som igen skal påses overholdt jf. art. 32. Dette besvarer støttespørgsmål 2 i problemformuleringen.

BEHANDLINGSSIKKERHED

3.2 GENERELT OM DATASIKKERHED

Der har gennem mange år været fokus på begrebet datasikkerhed, og denne fokus er blevet mere og mere skærpet gennem årene, navnlig som følge af den stigende teknologiske udvikling.

[67] https://themis.dk/synopsis/docs/Lovsamling/Persondataforordningen_praeambel.htm - Præambel til GDPR pkt. 13

Selv I tiden hvor der blev benyttet brevduer, kunne data risikeres at blive udsat for undergang, ulovlig tilgang etc., idet man aldrig kunne vide hvem der fik fat i disse.

Samme problemstilling har man sådan set fortsat i dag, særligt når henses til, at enorme mængder af data sendes rundt i hele verden via internettet.

Det er således blevet mere og mere kompliceret at skulle passe ordentligt på persondata, uanset om man er DA eller DB.

Netop fordi data ikke overdrages "face to face", men både via post, mails, filer etc., er kravene til at have styr på sin datasikkerhed blevet øget.

3.3 DATASIKKERHED JF. PDL

Allerede inden GDPR trådte i kraft d. 25.5.2018, indeholdt PDL krav til behandlingssikkerheden.

Det følger af PDL § 41 stk. 1, at enhver der behandler data – dette være sig både den DA samt DB og enhver der får adgang til oplysninger, kun må behandle disse efter instruks fra den dataansvarlige med mindre andet følger af lov eller bestemmelser fastsat i henhold til lov.

Dette indebærer, at der skal være givet en konkret instruks om hvilke oplysninger der må behandles og ikke mindst til hvilket formål.

Der er dog i PDL § 41 stk. 2 en undtagelse om, at ordlyden i § 41 stk. 1 ikke gælder hvis det begrænser den journalistiske frihed, eller er til hinder for frembringelse af et kunstnerisk eller litterært værk.

I betænkningen til GDPR[68] er det anført, at meningen med denne ordlyd må skulle forstås som *"Hvis det imidlertid falder inden for det fastsatte formål at behandle oplysningerne i journalistisk, kunstnerisk eller litterært øjemed, må instruksen ikke lægge hindringer for den nærmere udøvelse af den journalistiske frihed mv. Samtidig må det antages, at behandlede personoplysninger – uanset instruksen – vil kunne anvendes i ikke-personhenførbar form til f.eks. at tilvejebringe et litterært produkt"*

[68] http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf - Betænkning 1565 s. 471

I databeskyttelsesdirektivet[69] er angivet, at MS skal fastsætte bestemmelser om, at den DA skal iværksætte fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang.

Kravet om iværksættelse af tekniske og organisatoriske foranstaltninger er i præamblen til direktivet – pkt. 46 – angivet til både at skulle ske "*under selve udformningen og under iværksættelsen af en behandling"*

Dette beskyttelseskrav er indsat i PDL § 41 stk. 3, som også gælder for evt. databehandlere.

Det fremgår dog ikke af direktivet 95/46/EF, PDL eller forarbejderne til samme hvad der nøjagtigt menes med tekniske og organisatoriske foranstaltninger.

Ordlyden i PDL § 41 stk. 1 er således alene overordnede krav til behandlingssikkerheden som den DA skal opfylde, idet kravene dog svarer til de krav der var stillet i de 2 forudgående registerlove om offentlige myndigheders og private virksomheders behandling.

Betænkning 1565[70] angiver, at når det kommer til beskrivelse af de tekniske og organisatoriske foranstaltninger, så har kommissionen udtalt: *"Kommissionens bemærkninger til direktivudkastet af 24. September 1990, at tekniske datasikkerhedsforanstaltninger omfatter – Sikkerhedsforanstaltninger med hensyn til adgang til databehandling og til datalagre, identifikationskoder til personer, der har adgang hertil, edb-sikkerhedsforanstaltninger som f.eks. brug af password for at få adgang til edb-registre, omsættelse af data til kode (kryptering) og kontrol med hacking og andre usædvanlige aktiviteter i edb-registre.*

Gennem organisatoriske foranstaltninger skal den dataansvarlige efter Kommissionens bemærkninger tage proceduremæssige skridt inden for den offentlige myndigheds eller erhvervsvirksomheds hierarki, f.eks. ved at etablere forskellige autorisationsniveauer for adgangen til registeret."

Uanset om sikkerhedsforanstaltninger ikke er klart angivet, så er meningen helt klart, at den DA skal tage alle fornødne sikkerhedshensyn som muligt – fortsat ud fra en afvejning af både det

[69] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:31995L0046&from=DA - EU direktiv nr. 95/46/EF artikel 17 stk. 1, 1. afsnit

[70] http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf - Betænkning 1565 s. 472

aktuelle tekniske niveau og økonomien, holdt op imod risikoen for den registrerede som den DA's behandling indebærer samt typen af oplysninger der behandles.

I direktivet[71] er ligeledes anført, at *"Disse foranstaltninger skal under hensyn til det aktuelle tekniske niveau og de omkostninger som er forbundet med deres iværksættelse, tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger som skal beskyttes".*

Det er ligeledes i præamblen til direktivet punkt 10 anført, at gennemførelse af direktivet ikke må føre til en forringelse af beskyttelsesniveauet, men at gennemførelsen tværtimod skal have til formål at sikre et højt beskyttelsesniveau overalt i Fællesskabet.

I PDL er der i § 41 stk. 5 angivet, at *"Justitsministeren kan fastsætte nærmere regler om de i stk. 3 anførte sikkerhedsforanstaltninger".*

Ordlyden i PDL § 41 stk. 5 var ny i forhold til ordlyden i de tidligere registerlove.

Hensigten var, at der ved lovens ikrafttrædelse skulle udstedes en bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger der blev behandlet for den offentlige forvaltning ved hjælp af elektronisk databehandling. Tilsvarende bekendtgørelse skulle udstedes for domstolene.[72]

Med hjemlen i PDL § 41 stk. 5, udstedte Justitsministeriet Sikkerhedsbekendtgørelsen[73] der omfatter sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

Endvidere udstedte Justitsministeriet – også med hjemmel i PDL § 41 stk. 5 - Sikkerhedsbekendtgørelsen[74] der omfatter sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for domstolene.

Begge bekendtgørelser ligner meget hinanden, og forskellene vil ikke blive yderligere drøftet i denne opgave.

---

[71] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:31995L0046&from=DA - EU direktiv 95/46/EF artikel 17 stk. 1, 2. afsnit

[72] Waaben og Nielsen, "Lov om behandling af personoplysninger" s. 556

[73] https://danskprivacynet.files.wordpress.com/2008/06/sikkerhedsbekendtgc3b8relse.pdf Bekendtgørelse nr. 528 af 15. juni 2000

[74] https://www.retsinformation.dk/Forms/R0710.aspx?id=850 - Bekendtgørelse nr. 535 af 15. juni 2000

Der er aldrig blevet fastsat regler for behandlingssikkerheden for private virksomheder, idet praksis fra DT viser, at tilsynets opfattelse er, at der må stilles samme krav til datasikkerheden uanset om man er offentlig forvaltning eller en privat virksomhed.

Som eksempler kan nævnes DT's afgørelser[75] som omhandler henholdsvis "Manglende kryptering på hjemmesiden hos Nets" og "Sikkerhedsbrud og optagelse af kundesamtaler hos Natur-Energi A/S".

I sagen der omhandler den manglende kryptering hos Nets, lægger DT til grund, at den manglende kryptering ved anvendelse af Nets hjemmeside der bl.a. skulle overføre CPR nr., pas kørekor etc. ikke levede op til kravet om fornødne sikkerhedsforanstaltninger jf. PDL § 41 stk. 3.

I sagen om sikkerhedsbrud hos Natur-Energi A/S fandt tilsynet det kritisabelt, at 3 års afsluttede supportsager blev tilgængelige for uvedkommende via internettet. DT fandt, at Natur-Energi A/S's behandling ikke levede op til kravet om fornødne sikkerhedsforanstaltninger jf. PDL § 41 stk. 3 samt kravet om sletning af oplysninger der ikke længere var nødvendige jf. PDL § 5 stk. 5.

Det var og er således fortsat forventeligt, at den nu ikke længere gældende Sikkerhedsbekendtgørelse der omfattede den offentlige forvaltning, har haft og muligvis fortsat vil få en afsmittende virkning, også på private virksomheders tiltag for at optimere datasikkerheden.

3.4 DATASIKKERHED JF. GDPR

Datasikkerheden i GDPR er primært angivet i art. 32.

Som det også er tilfældet jf. PDL § 41, så omhandler art. 32 i GDPR ikke en konkret beskrivelse af hvad der skal til for at opfylde et passende sikkerhedsniveau. Det er alene de overordnede retningslinjer for hvordan datasikkerheden opnås der er angivet i selve ordlyden i art. 32.

Det ville være logisk om der blev taget udgangspunkt i "State of the art" ved en vurdering af hvorvidt den DA opfyldte kravet om datasikkerhed, men dette er ikke nødvendigvis tilfældet.

Når den DA skal planlægge datasikkerheden, skal denne tage udgangspunkt i den aktuelle tekniske og organisatoriske situation, både i egen virksomhed, men også på markedet.

[75] DT afgørelse med journalnr. 2013-217-0345 (BILAG 9) og 2013-631-0053 (BILAG 10)

Dette skal ses i lyset af, at sikkerhedsniveauet er forskelligt fra virksomhed til virksomhed, idet en mindre virksomhed måske ikke har behov for samme beskyttelsesniveau som en kæmpe koncern eller, at en virksomhed der behandler følsomme data i store mængder vil have et langt større beskyttelsesniveau end eksempelvis en håndværksvirksomhed.

Dette indebærer dog ikke, at mindre virksomheder er underlagt mere lempelige regler, idet tiltagene der skal tages for at sikre data skal vurderes ud fra den konkrete virksomhed og dennes behandling. Det skal påpeges, at der også kan tages hensyn til ressourcer ved valget af sikkerhedsløsning.

Det er derfor ikke sikkert, at samme sikkerhedsløsning vil være egnet for alle typer og størrelser af virksomheder, ligesom den teknologiske udvikling går så stærkt, at det ville være svært problematisk at angive konkret hvad/hvordan og med hvilke midler de enkelte virksomheder skal tilpasse deres datasikkerhed.

ARTIKEL 32 STK. 1

Ordlyden i art. 32 stk. 1 anfører, at *"Under hensynstagen til de 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, de i pkt. a-d nævnte foranstaltninger."*

For at kunne tilvirke sine systemer og procedurer til et acceptabelt datasikkerhedsniveau, er det vigtigt, at både den DA og DB har foretaget en risikovurdering på de data der behandles således, at der kan tages de rigtige og fornødne sikkerhedstiltag.

Det fremgår af præamblen til GDPR[76], at den DA og DB bør vurdere de risici som en behandling indebærer, og gennemføre foranstaltninger der kan begrænse disse risici, som eksempelvis kryptering.

[76] https://themis.dk/synopsis/docs/Lovsamling/Persondataforordningen_praeambel.html - Præambel til GDPR punkt 83

Hvis ikke den DA er bekendt med, og har foretaget en risikovurdering af hans behandling af de forskellige data, er det også svært at vide med hvilke midler og metoder den bedste datasikkerhed kan gives.

Som omtalt i indledningen til denne opgave, er selve GDPR teknologi neutral hvilket giver god mening, idet teknologien udvikles i et rasende tempo. Hvis der derfor konkret var angivet hvilke tiltag der skulle foretages for at opfylde datasikkerheden jf. GDPR, så ville lovens tekst hurtigt være forældet. Endvidere ville det være utopi at forestille sig, at alle virksomheder - store som små - ville og kunne have og opfylde samme krav til datasikkerheden.

GDPR art. 32 stk. 1 a-d angiver dog nogle forslag til hvad der kunne være løsningen på at opfylde datasikkerheden.

ART. 32 STK. 1 A omtaler at pseudonymisering og kryptering kunne være en måde at opfylde datasikkerheden på. Ved pseudonymisering menes, at data ikke længere kan henføres til en bestemt person uden anvendelse af supplerende oplysninger. Ved kryptering forstås, at data ikke længere kan læses uden anvendelse af en krypteringsnøgle.

Fælles for disse 2 ting er, at såfremt der vælges at sikre ved hjælp af disse metoder, så skal de supplerende oplysninger og krypteringsnøgle være opbevaret særskilt, og særskilt være underlagt egne tekniske og organisatoriske sikkerhedsforanstaltninger.

Kravet til kryptering er senest af DT[77] angivet som et direkte krav i forbindelse med kommunikation via e-mail såfremt, at mails indeholder følsomme oplysninger angivet i art. 9 og 10.

ART. 32 STK. 1 B angiver, at også evnen til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og tjenester, er en sikkerhedsforanstaltning der kan bringes i anvendelse.

Her må forstås den DA's opsætning af sine IT-systemer samt procedurer der skal kunne sikre den registreredes data.

Systemer og procedure skal være af en karakter der er så stabilt, at det både er muligt at validere de data der behandles, at sikre at data altid kan tilgås (eksempelvis ved backup), at data ikke kan ødelægges ved utilsigtet hændelser som eksempelvis brand samt, at nævnte tiltag løbende skal kunne foregå for at sikre den vedvarende tilgængelighed.

[77] Bilag 11

ART. 32 STK. 1 C omhandler den DA evne til rettidigt at kunne genoprette tilgængeligheden af og adgangen til persondata, i tilfælde af at disse skulle komme ud for en fysisk eller teknisk hændelse.

Hermed menes, at den DA skal sikre sig at have en procedure og et beredskab til at kunne genskabe og genoprette adgangen til data i tilfælde af eksempelvis et hackerangreb, brand eller andre hændelser hvor den DA pludselig ikke har adgang til datene.

De fleste virksomheder anvender backup på deres systemer, men der kan også være andre løsninger der kan anvendes, eksempelvis ved at kunne benytte en anden datalinje end den skadede.

Betænkning 1565[78] angiver, at *"evnen til rettidig genoprettelse kan f.eks. demonstreres ved øvelser og test".*

ART. 32 STK. 1 D angiver slutteligt, at hvis der etableres en procedure for regelmæssig afprøvning, vurdering og evaluering af effekten af de tekniske og organisatoriske foranstaltninger, så vil dette også kunne være en del af behandlingssikkerheden.

Hermed menes, at der jævnligt bør testes og afprøves de procedure og systemer der er valgt til at sikre datasikkerheden.

Dette kan være afprøvning af adgangssystemer, firewalls, opbevaringssystemer, krypteringssystemer etc.

Selvom om der hovedsageligt er lagt lægt på de tekniske foranstaltninger når der tales datasikkerhed, så kan rent organisatoriske tiltag også være en løsningsmodel. Det klassiske eksempel er, at kun de medarbejdere der skal anvende dataene har adgang til disse, altså en bevidst adgangskontrol til data.

ART. 32 STK. 2 kan anses for en slags vejledning i hvad der skal tages hensyn til ved vurderingen af, hvilke tiltag der implementeres for at sikre et passende sikkerhedsniveau.

Det anføres[79], at *"Ved vurderingen af, hvilke sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab,*

[78] http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf - Betænkning 1565 s. 482

[79] http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf - Betænkning 1565 s. 483

ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Der er særligt lagt vægt på, at data ikke hændeligt eller ulovligt må forsvinde, hvilket taler for at den fysiske sikkerhed skal være i højsædet.

Tilsvarende gør sig gældende når ordlyden særskilt nævner videregivelse af data samt adgang til samme, idet den øgede udveksling af data, særligt via internettet, øger muligheden for at data fortabes, eller at disse bliver udsat for ulovlig eller utilsigtet adgang.

Peter Blume nævner[80], at *"Det er i denne forbindelse velkendt, at særligt transmission via internettet aktualiserer sikkerhedsrisici, hvilket bl.a. kan aktualisere et krav om, at oplysningerne skal kommunikeres i krypteret form".*

DT udsendte i Juli 2018 nye retningslinjer for transmission af mails der indeholder data omfattet af art. 9 og 10 samt almindelige data der må anses for at være særligt beskyttelsesværdige, eksempelvis CPR nr.[81]

Da offentlige myndigheder allerede var underlagt et sådant krav qua Sikkerhedsbekendtgørelsen der var gældende under PDL, angår retningslinjerne nu også private virksomheder. Der blev således givet private virksomheder ca. 6 måneder til at få indrettet deres systemer således, at mails der indeholder data af særlig karakter, kun må sendes krypteret. Dette krav trådte i kraft pr. 1.1.2019.

Dette kan give nogle udfordringer, idet ikke alle modtagere har systemer der kan modtage mails i krypteret form. Udgangspunktet er, at det er den DA der bærer ansvaret for, at mails afsendes i krypteret form, og herfra overgår risikoen til modtageren.

De fleste systemer i dag kan dog modtage krypteret mails, idet den DA ellers kan være ude i at skulle fremsende særskilte koder for at modtageren rent faktisk kan læse den fremsendte mail.

Generelt skal den DA derfor foretage vurderingen af hvilke risici der kan være i forbindelse med behandlingen, finde de bedste og mest egnede foranstaltninger og herefter implementerer disse for at sikre den tilstrækkelige datasikkerhed.

---

[80] Peter Blume "Den nye persondataret" s. 157

[81] //www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2018/jul/skaerpet-praksis-ift-krypteret-e-mail/ - BILAG 11

ART. 32 STK. 3 nævner, at også godkendte adfærdskodeks som omhandlet i art. 40 eller anden godkendt certificeringsmekaniske som omhandlet i art. 42 kan anvendes for at påvise compliance som nævnt i stk. 1.

Dette vil blive nærmere behandlet i del 4.

ART. 32 STK. 4 er en specifikation af, at den DA og DB skal sikre, at de personer som hos dem behandler persondata, alene behandler ud fra den instruks som er givet fra den DA, dog undtaget behandling der kræves i henhold til EU-retten eller MS nationale ret.

3.5 FORSKELLEN MELLEM PDL OG GDPR

Ordlyden i GDPR art. 32 stk. 1 og 2 minder meget om ordlyden angivet i PDL § 41 stk. 3 samt i direktivets art. 17 stk. 1[82].

Det må derfor formodes, at kravet om tekniske og organisatoriske foranstaltninger skal anses for at have samme betydning jf. GDPR, som det hele tiden har haft jf. PDL.

Selvom det stort set er samme ordlyd, så er det dog nyt jf. GDPR, at der nu jf. art. 32 stk. 1a – 1d er angivet hvilket tiltag der evt. kan anvendes for at opfylde kravene til datasikkerhed. Den i art. 32 stk. 1 litra a-d er ikke udtømmende, hvilket er angivet i art. 32 stk. 1, første afsnit hvori er angivet *"herunder bl.a. alt efter hvad der er relevant".*

Det er således op til den DA at vurdere hvilke tiltag der måtte være den bedste løsning, og den valgte løsning behøver så ikke nødvendigvis at være nævnt i art. 32, men kan evt. findes i helt andre løsningsmodeller.

Løsningen skal dog findes i vurderingen af hvilke risici behandlingen medfører, og så skal sikkerhedsløsningen tilpasses dette behov.

Men set i lyset af den manglende angivelse i PDL om, hvad og hvordan datasikkerheds kravet evt. kan løses, så er der nu i GDPR art. 32 stillet nogle forslag op, der giver den DA en indsigt i forventningen til de sikkerhedstiltag den DA skal tage.

[82] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:31995L0046&from=DA - EU direktiv 95/46/EF

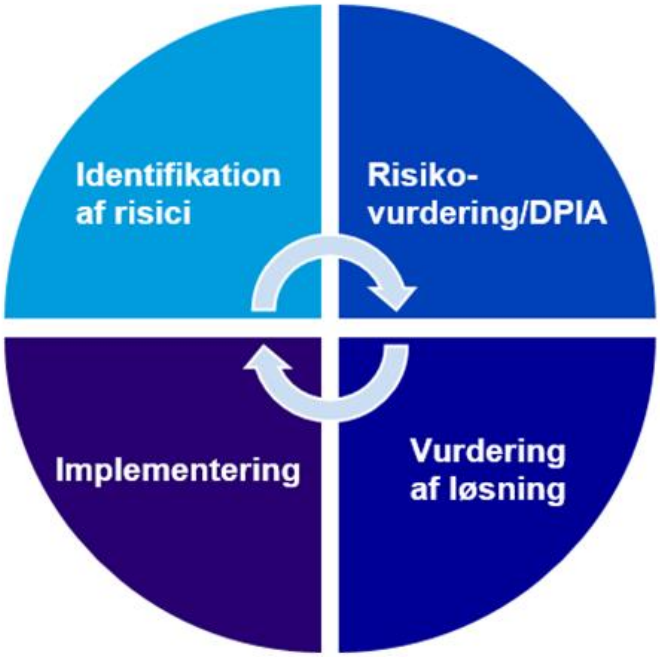
Som tidligere anført, så er GDPR i højere grad end PDL og databeskyttelsesdirektivet baseret på en risikomæssig betragtning forstået på den måde, at den DA allerede inden denne påbegynder en databehandling skal foretage en vurdering af, hvilke risici der måtte være for, at den registreredes rettigheder og frihedsrettigheder kan krænkes.

Ud fra denne risikovurdering skal den DA således implementerer de passende sikkerhedsforanstaltninger.

Peter Blume anfører[83], at *"risikoorientering er et af de nye træk ved forordningen"* samt *"ved at tillægge risiko betydning, bliver persondataretten proaktiv eller har i hvert fald mulighed for at blive det."*

[83] Peter Blume "Den nye persondataret" s. 265

Nedenstående figur angiver blot én af mange muligheder for løsning i forbindelse med processen i, at foretage en risikobaseret tilgang til at opfylde kravene om implementering af korrekt datasikkerhed.



Dette betyder, at ved at foretage risikovurderingen allerede inden en persondatabehandling påbegyndes, så er der mulighed for allerede fra start at få implementeret de korrekte og bedst mulige tekniske og organisatoriske tiltag, og dermed forhåbentlig imødegå og forhindre evt. krænkelse af data. Sikkerhedsløsningen er således tænkt ind allerede ved investeringer af nye systemer samt implementeret i processer. Behandlingssikkerheden burde derfor blive højere sammenlignet med de regler der findes i PDL, da de sikkerhedsforanstaltninger der skal tages efter GDPR, er målrettet mod at dække de risici den DA ved sin risikovurdering har fundet frem til.

Der er ikke anført præcist hvilke foranstaltninger der skal implementeres, idet disse alene hænger sammen med den risikovurdering den DA foretager.

Det er ligeledes den DA ansvar at kunne påvise og ikke mindst dokumenterer, at den implementerede sikkerhedsløsning sikrer den registreredes data den tilstrækkelige sikkerhed.

3.6 SIKKERHEDSNIVEAUET

3.6.1 HVORNÅR OG HVORDAN ER DET RELEVANT AT KIGGE PÅ SIKKERHEDEN?

I forbindelse med den DA's vurdering af risikoen for, at den registreredes data kan blive udsat for forskellige hændelser der kan krænke dennes rettigheder eller frihedsrettigheder, er en af de ting der bør tages højde for, hvilke typer af data der behandles.

Udgangspunktet er, at jo mere følsomme data er, jo bedre/højere beskyttelse skal disse have. Selvom GDPR har kategoriseret data i følsomme, almindelige og særlige data (straffedomme og loveovertrædelser), så kan denne inddeling ofte have en uheldig indvirkning på måden at håndtere de forskellige datatyper på.

Der kan sagtens tænkes data der rent lovmæssigt hører under følsomme data, men hvor behandlingen af disse ikke på nogen måde vil have en integritetskrænkende virkning for den registrerede – eksempelvis som anført af Peter Blume[84] - *et brækket ben og lungekræft hører i samme kategori af data - men der er vist ingen der ville syntes at lungekræfttilfældet ikke skulle høre under begrebet følsomme data, mens det brækkede ben vil syntes noget mere anstrengt at skulle henhøre som en særlig følsom data.*

Det er efterhånden særdeles vanskeligt at finde en type af oplysninger der ikke på en eller anden måde vil kunne henføre til en person, og altså vil være omfattet af begrebet personoplysninger, og dermed være omfattet af reglerne i GDPR.

Det er således ikke alene navne, adresser, e-mailadresser, cpr.nr., etc. der er omfattet, men også IP adresser, nummerplader etc. hører under kategorien personhenførbare data.

Peter Blume anfører[85], *"I forhold til kravet om, at der skal være en behandlingsbetingelse, sker der i overensstemmelse med traditionen en differentiering mellem almindelige og følsomme oplysninger, mens der kun i meget begrænset omfang sker en differentiering med udgangspunkt i behandlingsformålet"*

[84] Peter Blume "Den nye persondataret" s. 266

[85] Peter Blume "Den nye persondataret" s. 266

Peter Blume[86] stiller spørgsmålet, om bredden allerede er blevet for bred, og om det kan være forsvarligt at udskille nogle af de almindelige data som værende trivielle i forhold til reguleringen jf. GDPR.

Han anfører ligeledes, at *"Personoplysninger af denne karakter kunne holdes uden for den persondataretlige regulering og kun inddrages, såfremt behandlingsformålet eller behandlingssammenhængen har en sådan karakter, at det i sig selv udløser en risiko for integritetskrænkelser"*

Ydermere anfører Peter Blume at *"I forhold til trivielle persondata ville man på denne måde anlægge en kontekstuel indfaldsvinkel med vægten lagt på integritetsrisiko frem for på det blotte faktum, at der er tale om en personoplysning.*

Her næsten et år efter GDPR's ikrafttræden, er der fortsat en masse virksomheder der har kæmpeudfordringer med at få implementeret den korrekte datasikkerhed, netop set i lyset af, at selv helt banale oplysninger som navn og adresse skal sikres.

Da der i forvejen er pålagt virksomheder og offentlige myndigheder et massivt administrativt arbejde for at være compliant med GDPR, så kunne det være en stor hjælp hvis sikkerhedskravene skulle baseres på den behandling der rent faktisk fandt sted, i stedet for som anført af Peter Blume, at være baseret på om en data var personhenførbar eller ej.

Dette syntes også at være mere i tråd med tankegangen om, at sikkerheden skal baseres på en risikobetragtning, hvor der altså allerede på et tidligt stadie skal ses på ikke bare typen af data der behandles, men i ligeså høj grad på den behandling der finder sted og skadevirkningen for den registrerede hvis der måtte opstå en hændelse der krænker dennes rettigheder.

3.6.2 HVORDAN VIDES DET OM SIKKERHEDSNIVEAUET ER GODT NOK?

Der er som tidligere nævnt i art. 32 intet der konkret angiver hvad der skal til for, at man med 100% sikkerhed kan siges at overholde kravene til datasikkerhed.

De forskellige tiltag nævnt i art. 32 litra a-d er alene den overordnede ramme for hvad der evt. kan implementeres for at sikre overholdelse af sikkerheden, men der vil sandsynligvis være eksempler

[86] Peter Blume " Den nye persondataret" s. 266/267

på data og disses behandling, hvor ingen af de i art. 32 nævnte tiltag vil have den ønskede effekt, eller hvor helt andre metoder vil være at foretrække.

Et er dog helt sikkert, og det er, at både den DA og DB skal tilstræbe at implementerer en tilstrækkeligt virkende datasikkerhed, så er det ikke afgørende hvordan denne opnås.

Datasikkerheden kan være truet både udefra og indefra, idet mange sikkerhedsbrud skyldes menneskelige fejl begået af en virksomheds egne ansatte, eller virksomhedens egne systemer der ikke er tilstrækkeligt sikret mod diverse angreb.

Motivet til at angribe diverse systemer kan være mange forskellige, men oftest vil motivet være penge, chikane eller blot afstedkommet af et ønske om at vise at "det kan jeg godt".

Hacking har været kendt gennem mange år, og selv helt store internationale koncerner har været udsat for hacking angreb der har forvoldt store gener og ikke mindst kæmpe tab for virksomheden.

Som eksempler på virksomheder der seriøst blev hårdt ramt af sådanne hacker angreb kan nævnes Mærsk, der senest i marts 2018 blev udsat for et sådant angreb.[87] Dette angreb kostede Mærsk omkring 2 mia. for at rette op på skaden.

Tilsvarende var DTU udsat for et angreb der blev opdaget i 2018, men som viste sig at have fundet sted mellem 2016 og 2018. [88]

Her var der tale om, at hackere havde fået franarret et lille antal ansatte til at besvare mails hvorved, at en formodet Iransk gruppe havde fået adgang til data og forskningsresultater.

SDU oplyste i samme sag, at de ikke var blevet ramt hvilket kunne have bragt en masse menneskers personlige data i fare, idet SDU bl.a. håndtere data indeholdende behandlingsforløb for sundhedssektoren.

I takt med den øget teknologi og hastigheden i udviklingen af samme, kan det være svært at følge med rent datasikkerhedsmæssigt. Dette er dog et decideret krav jf. både art. 24 stk. 1 om de tekniske og organisatoriske foranstaltninger (disse foranstaltninger skal om nødvendigt revideres og ajourføres) og art. 32 stk. 1 litra b-d.

---

[87] https://www.computerworld.dk/art/242820/maersk-selskab-ramt-af-nyt-stort-hacker-angreb-hackere-har-stjaalet-60-000-vigtige-mails-gennem-11-maaneder - BILAG 12

[88] https://www.dr.dk/nyheder/indland/hacker-angreb-paa-tre-danske-universiteter-dtu-medarbejdere-gik-i-faelden - BILAG 13

Datasikkerhed er således noget dynamisk, som alle virksomheder bliver nødt til løbende at forholde sig til, hele tiden vurderer hvorvidt sikkerheden er tilstrækkelig og i benægtende fald supplerer, opdaterer og ikke mindst opgraderer systemer og processer løbende.

Der er derfor ikke nogen konkret løsning og svar på hvordan man helt sikkert kan vide om beskyttelsesniveauet er opfyldt eller ej.

Det tætteste på man kommer er således ordlyden angivet i art. 32, med tilhørende kommentarer i præamblen til GDPR og evt. forklaringer i betænkning 1565, men førend de nationale og EU-domstolen har haft nogle sager forelagt, vil det være et skøn der må lægges til grund for vurderingen af, om sikkerhedsniveauet er overholdt.

Det overordnede krav er blot, at den DA og DB skal implementerer et passende sikkerhedsniveau, der tager hensyn til typen af persondata der behandles og de risici der er forbundet med selve behandlingen.

Tiden får vise hvordan datasikkerhedskravet løses i de forskellige MS, idet teknologiniveauet sandsynligvis er forskelligt fra land til land, og datasikkerhedsløsningerne vil derfor sandsynligvis også være forskellige i de enkelte MS.

3.6.3 HVORDAN SIKRES DOKUMENTATIONEN PÅ OVERHOLDELSE AF SIKKERHEDSNIVEAUET

Som det tidligere er omtalt, så er den DA ikke blot ansvarlig for at den fornødne datasikkerhed er til stede, dette skal også kunne dokumenteres.

Selve dokumentationskravet hænger sammen med forpligtelsen til at føre fortegnelse jf. GDPR art. 30 som tidligere er behandlet. Selve fortegnelseslisten jf. art. 30 er en ren intern liste som alene skal kunne forevises DT i tilfælde af, at DT måtte udbede sig denne. Der er i øvrigt ikke noget formkrav til hvordan en sådan fortegnelsesliste skal se ud.

Men hvad er det reelt en fortegnelse jf. art. 30 viser?

Selve fortegnelsen skal gerne hænge sammen med principperne angivet i art. 5 stk. 1 om den ansvarlighed den DA skal udvise samt dennes forpligtelse til at kunne påvise at ansvarligheden rent faktisk overholdes jf. art. 24.

Som tidligere nævnt, så skal fortegnelser foreligge skriftligt og elektronisk.

Som et eksempel på en fortegnelsesliste kan henvises til betænkning 1565[89], hvor kravene angivet i art. 30 stk. 1 er angivet i skemaform delt op i felter, der så kan udfyldes af den DA.

Fortegnelsen viser alle de stamdata omkring den DA tilsynsmyndighederne måtte have brug for i forbindelse med en evt. audit, samt en beskrivelse af kategorien af data der behandles, kategorien af registrerede, formålet med behandlingen, modtagere af oplysninger, evt. dataoverførsel til 3. Land, slettefrister og hvilke tiltag den DA har taget for at sikre data.

Men er dette ikke bare ord i et skema, og fungerer en sådan fortegnelsesliste som dokumentation på noget som helst?

Selve fortegnelseskravet jf. art. 30 afløser den tidligere anmeldelsespligt til DT jf. PDL og direktivet[90], og der syntes ikke at være basis for at ændre fortegnelsen jf. art. 30 i forhold til hvad der tidligere skulle anmeldes til DT.

Det er i betænkning 1565[91] anført at, *"Den dataansvarlige er endvidere i forvejen forpligtet til at udlevere en oversigt over alle behandlinger – inklusiv de behandlingsaktiviteter, der ikke er omfattet af anmeldelsespligten – til enhver der anmoder herom efter gældende ret i persondatalovens § 54 stk. 2. Dermed er den dataansvarlige i et vist omfang allerede omfattet af krav, der svarer til forordningens krav i artikel 30, dog således, at fortegnelse efter art. 30 alene er et internt dokument."*

Der er derfor fortsat den samme fortegnelsesforpligtelse jf. GDPR art. 30 som tidligere, dog er pligten udvidet til også at omfatte behandlinger der ikke tidligere var anmeldelsespligtige. Fortegnelsen skal nu føres skriftligt og elektronisk, men der er ikke længere en anmeldelsespligt som tidligere.

Det er værd at bemærke, at fortegnelsesforpligtelsen også omfatter DB, hvor der er sket en udvidet fortegnelsesforpligtelse, idet også behandlingsaktiviteter omfattet af art. 6 stk. 1 skal være indeholdt i fortegnelsen mod tidligere kun de særligt følsomme data.

---

[89] http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf - Betænkning 1565 s. 461

[90] https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:31995L0046&from=DA - EU direktiv 95/46/EF

[91] http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf - Betænkning 1565 s. 460

Selve fortegnelseslisten kan af DT anvendes til at få et overblik over hvilke data der behandles, hvordan og hvilke sikkerhedstiltag der er taget for at opfylde kravet om datasikkerhed.

Disse angivelser kan efterfølgende afprøves af DT ved en audit, og den DA har så godt som muligt løftet dokumentationskravet ud fra de retningslinjer der nu en gang gælder.

KONKLUSION DEL 3

Da der ikke foreligger et konkret krav på hvordan datasikkerheden dokumenteres, vil det være op til den enkelte DA at føre den dokumentation denne måtte finde korrekt for netop dennes behandling af data. Der ses som udgangspunkt på hvilke typer af data der behandles (art. 9/art. 10), omfanget af behandlingen, kategorier af registrerede, evt. videregivelse af data og til hvem, slettefrister, formålet med behandlingen og hvilke tekniske og organisatoriske tiltag der er taget for at sikre dataene.

Som dokumentation på ansvarligheden angivet i art. 5 benyttes fortegnelsen udarbejdet jf. art. 30, og denne danner så udgangspunktet for dokumentation på, at datasikkerheden er overholdt som angivet i art. 32.

På den måde hænger kravet til datasikkerhed sammen med den ansvarlighed, der generelt skal udvises ved behandlingen af persondata.

4.1.1 PDL VS. GDPR

Som nævnte i afsnittet ovenover, så følger det allerede af PDL § 54 stk. 2, at en DA skal stille en behandlingsfortegnelse til rådighed for enhver som anmoder herom. Denne fortegnelse skal indeholde alle de i PDL § 43 stk. 2 nr. 1, 2 og 4-6 nævnte oplysninger.

Tilsvarende regler gør sig gældende jf. GDPR art. 30 stk. 1.

Ud over fortegnelser over behandlingsaktiviteter, bliver markedet i almindelig samhandel ofte mødt med yderligere krav til dokumentation af, hvordan hele datasikkerhedsområdet er løst.

En stor del af en virksomheds sikkerhedsløsning er af fortrolig karakter, idet det ville gøre det let for hackere og andre personager der måtte ønske at gøre en virksomhed skade ved hjælp af en eller anden form for cyber kriminalitet, hvis virksomhedens sikkerhedspolitik og løsningsmodeller var frit tilgængelig for alle.

Det er således vigtigt, at virksomhederne kan dokumenterer sine sikkerhedsmæssige tiltag uden samtidig at udsætte sig selv for hackerangreb eller anden form for misbrug af sine systemer.

Nogle af de redskaber der fungerer som den vigtigste dokumentation er som nævnt fortegnelsen over behandlingsaktiviteter jf. art. 30 samt dokumenterede procedurer udarbejdet til brug for beskyttelse af persondata. Dette kan være politikker omkring kryptering samt generelle databeskyttelsespolitikker.

Det er ikke nok, at virksomheden udarbejder politikker, værktøjer etc., hvis disse ikke følges og efterleves. Det er derfor vigtigt, at hele datasikkerhedsområdet er sat sammen nøjagtigt møntet på den konkrete virksomhed og de behandlinger der foretages, og altså ikke blot er en slags ”standard” sikkerhedspakke, der egentlig ikke forholder sig til den konkrete behandling.

Som en del af de organisatoriske foranstaltninger kan nævnes medarbejdernes kendskab og anvendelse af de forskellige politikker. Kun de medarbejdere der reelt har behov for at kunne behandle dataene bør have adgang til disse, hvilket typisk løses ved at der alene er givet adgang til de data der måtte vedr. den enkeltes job.

Herved opfyldes også kravet i art. 5 stk. 1 c om dataminimering.

Hele procedure processen skal være en løbende proces hvor der hele tiden skal holdes øje med om det fortsat er de korrekte data der behandles, hjemmelsgrundlaget, ændringer etc. der gør, at tilretning af processer måske skal foretages.

Der er for at løse dokumentationskravet lavet nogle standarder og regler der bevirker, at datasikkerhedskravet kan dokumenteres ud fra nogle gængse og godkendte standarder.

4.1.2 ADFÆRDSKODEKS – ART. 40

Der er i GDPR art. 40 angivet, at *"MS, tilsynsmyndighederne, Databeskyttelsesrådet og Kommissionen tilskynder til udarbejdelse af adfærdskodekser, der under hensynstagen til de særlige forhold i de forskellige behandlingssektorer og mikrovirksomheders og små og mellemstore virksomheders specifikke behov, bidrager til korrekt anvendelse af forordningen"*

Der er alene tale om en tilskyndelse, og således er anvendelse af adfærdskodekser ikke et krav ifølge GDPR.

Ved adfærdskodeks forstås, at der etableres et sæt brede regler for en konkret branche, og et sådant kodeks vil kunne danne grundlag som dokumentation for den pågældende branches generelle overholdelse af reglerne i GDPR, herunder angivelse af de databeskyttelsesregler der følger af bl.a. art. 24, 25 og 32.

Ordlyden i GDPR art. 40 har stort set samme ordlyd og betydning som ordlyden i PDL § 74 som har baggrund i direktiv 95/46/EF artikel 27.

Der er dog som noget nyt i GDPR art. 40 i forhold til PDL § 74 angivet, at der skal tages hensyn til særlige virksomhedstypers forhold, herunder små- og mellemstore virksomheder og mikro-virksomheder.

Dette skyldes jf. betænkning 1565[92], at der er et ønske om at hjælpe små virksomheder der ikke nødvendigvis har en juridisk afdeling eller ressourcer i øvrigt, til at efterleve forordningens regler via adfærdskodekser.

[92] http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf - Betænkning 1565 s. 594

Det følger af præambel til GDPR pkt. 98, 2. Punktum, at *"Sådanne adfærdskodekser bør navnlig kunne justere dataansvarliges og databehandleres forpligtelser, så der tages hensyn til den risiko, som sandsynligvis vil følge af behandlingen for fysiske personers rettigheder og frihedsrettigheder."*

Der skal derfor også tages højde for risikotankegangen ved udarbejdelse af adfærdskodeks. Selvom der ikke direkte i art. 40 er angivet, at den risikobaseret tilgang skal ind tænkes i en adfærdskodeks, så vil dette alligevel ske såfremt kodekset indeholder beskrivelsen af datasikkerhed, idet risikotankegangen indgår som en del af både art. 24, 25 og 32.

En anden nyskabelse er, at der i art. 40 er angivet, at tilsynsorganerne tilskynder anvendelsen af adfærdskodekser, hvorimod der i PDL § 74 er angivet, at et kodeks skal udarbejdes i samarbejde med DT. Det er derfor nu ikke længere DT der skal være en DA behjælpelig med udarbejdelse af en kodeks, idet DT's opgave nu alene er at afgive en udtalelse og evt. godkendelse af det udkast den DA eller DB har udarbejdet.

Det er og kan være en lang og besværlig vej igennem systemet såfremt en branche ønsker at få godkendt og implementeret et adfærdskodeks.

Det er sammenslutninger og repræsentanter for særlige kategorier af DA eller DB der kan udarbejde forslag til adfærdskodekser, hvorefter sådanne forslag skal forelægges for DT der kan udtale sig om hvorvidt forslaget overholder og er i overensstemmelse med reglerne i GDPR.

Hvis kodekset alene omfatter behandling af personoplysninger i DK, kan det danske DT tage stilling til forslaget, men hvis behandlingen også vedrører behandling i andre MS, skal forslaget af DT forelægges også for Databeskyttelsesrådet, der så giver en udtalelse om hvorvidt forslaget overholder reglerne og er i overensstemmelse med GDPR.

Databeskyttelsesrådets udtalelse skal videre forelægges for Kommissionen der så kan fastsætte, at kodeksen anses for at overholde reglerne og er i overensstemmelse med GDPR, hvorefter kodeksen kan offentliggøres og anvendes.

Kravet om offentliggørelse fremgår af art. 40 stk. 10-11.

Anvendelsen af adfærdskodekser har aldrig rigtigt vundet indpas i DK eller nogen af de øvrige MS, og DT har indtil videre ikke fundet anledning til at godkende nogen af de få henvendelser der har været.

Da der i GDPR er indsat et bødeniveau der er væsentligt højere end tidligere set, og da der flere steder i GDPR er nævnt netop implementeringen af adfærdskodekser som en mulig form for dokumentation for bl.a. datasikkerheden og den generelle overholdelse af reglerne i GDPR, så må det forventes, at flere vil forsøge at få implementeret og godkendt et adfærdskodeks for at kunne dokumentere compliance.

4.1.3 CERTIFICERING

Som også angivet i art. 40 omkring anvendelse af adfærdskodekser, så tilskynder MS, tilsynsmyndighederne, Databeskyttelsesrådet og Kommissionen i GDPR art. 42 stk. 1 til, at der bliver anvendt certificeringsordninger. Også her er der angivet, at små- og mellemstore virksomheder samt mikrovirksomheders særlige behov skal tages i betragtning.

Indholdet i GDPR art. 42 er ny i forhold til PDL og direktiv 95/46/EF, der ikke omhandler opfordringer eller regler omkring certificering.

Begrebet "certificering" består i, at en person, virksomhed eller eksempelvis en bestemt software bliver godkendt til at kunne/må håndtere en helt bestemt opgave, herunder omkring datasikkerhed.

Det fremgår af GDPR art. 42 stk. 1, at en sådan certificering skal kunne påvise, at **behandlingsaktiviteterne** overholder reglerne i GDPR.

Peter Blume[93] beskriver certificering som *"Ved certificering er det på sagkyndigt niveau undersøgt og accepteret, at en bestemt teknologi eller fremgangsmåde er egnet til at understøtte persondatabeskyttelse"*

Det er DT eller nogle af DT's akkrediteret organer der kan certificerer, hvilket følger af GDPR art. 43 samt DBL § 25.

Indholdet af en certificering er ikke nærmere angivet i GDPR, men der kan hentes inspiration i andre ordninger – eksempelvis ISO ordningerne. Hvis certificeringskriterierne omfatter og er fælles for alle MS, og disse har været behandlet i Databeskyttelsesrådet, kan der evt. udstedes en certificering eller databeskyttelsesmærkning der omfatter hele EU.

[93] Peter Blume "Den nye persondataret" s. 174

Da teknologien hele tiden udvikler sig, gælder en certificering alene i 3 år jf. GDPR art. 42 stk. 7 men kan fornys på uændret vilkår såfremt de relevante krav fortsat er opfyldt.

En certificering kan – ligesom adfærdskodekser – anvendes som en del af dokumentationen for, at regler og databeskyttelse er i overensstemmelse med forordningens bestemmelser.

4.1.4 ISO 27001

ISO27001 er den internationale standard der er gældende, hvis en virksomhed skal dokumentere, at sikkerhedsstandarden er i orden.

Generelt om ISO27001 kan siges, at dette er et informationsledelsessystem der kan benyttes af virksomheder for at sikre og beskytte virksomhedens data.

Der er tale om en anerkendt og godkendt standard, som tager sit udspring i den enkelte virksomheds risikoprofil.

Pointen er, at det netop er de sikkerhedsforanstaltninger, procedurer og kontrolfunktioner der skal til for at sikre sine data der implementeres, idet standarden dækker alle former for sikkerhedsprocedurer, både i form af systemer, procedurer, de fysiske rammer, kontrakter, fysiske dokumenter etc.

Standarden indeholder både metoder til planlægning, som kontrolsystem inkl. procedurer, og som dokumentationsredskab over for både DT og kunder der måtte ønske dokumentation for, at datasikkerheden overholdes, også i relation til GDPR. Der er således tale om en total standard der omfatter hele informationssikkerheds området.

ISO27001 er obligatorisk for stats- og offentlige institutioner, og skal ligeledes opfyldes for at være IT-leverandør til en stats- eller offentlig institution.

Standarden er forholdsvis omfattende, og dermed også svær at opnå uden en investering i både IT-systemer, processer og stor kontrol over sine data.

Der er dog ingen tvivl om, at såfremt en virksomhed vælger at blive ISO27001 certificeret, så har denne langt hen ad vejen bevist og dokumenteret, at der er foretaget de sikkerhedsmæssige tiltag – både i form af tekniske og organisatoriske tiltag – der kræves for at være compliant med kravene i GDRP. ISO 27001 er således den overordnede ramme for datasikkerhed.

En ISO27001 certificering anvendes i dag også som et strategisk værktøj i relation til kunder, leverandører etc., og kan anvendes også som konkurrence parameter.

For yderligere oplysninger henvises til DS[94] - Dansk Standards hjemmeside omkring ISO certificeringer generelt.

4.1.5A ISAE ERKLÆRINGER

En noget mindre udgave af ISO27001 certificering som værktøj til at dokumentere datasikkerhed, er uvildige revisionserklæringer.

De mest anvendte er ISAE 3000 og ISAE 3402 erklæringer. Begge disse erklæringer fås i type 1 og type 2.

Disse erklæringer består i nogle standardiserede skabeloner udfærdiget af revisionsbranchen. Fælles for disse erklæringer er, at det er internationale erklæringsstandarder, som også er gældende i udlandet.

De forskellige typer af erklæringer dækker over og anvendes til forskellige formål. Omfanget af erklæringerne kan variere alt afhængig af hvad disse skal omfatte. Der kan eksempelvis alene ønskes en erklæring der omhandler et specifikt område – GDPR, eller der kan vælges en erklæring der omfatter hele IT-sikkerheden i en virksomhed.

Virksomhedernes baggrund for at få udfærdiget en ISAE erklæring viser overfor både DT, kunder, leverandører etc., at virksomheden tager datasikkerheden seriøst, og virksomhed vil derfor fremstå mere troværdig ved selv at bekoste og få udarbejdet en uvildig erklæring.

4.1.5B ISAE 3402

ISAE 3402 erklæringen er den største og mest omfattende af de 2 typer erklæringer, og opfattes typisk i markedet som den klassiske IT-revisionserklæring.

[94] https://www.ds.dk/da/standardisering/ledelsesstandarder/informationssikkerhed - BILAG 14

En ISAE 3402 erklæring anvendes primært som dokumentation på, at kvaliteten af it-systemer, sikkerheden og forholdene i øvrigt er i orden på virksomheden.

I ISAE 3402 gennemgås en lang række af kontrolområder og forretningsgange vedr. it-funktionen, med baggrund i, hvad der kan have indflydelse på særligt den økonomiske side af forretningen, herunder drift, udvikling, dokumentation etc.

Det er ISO27001 standarden der ligger til grund for ISAE 3402 erklæringen, hvorfor også de fysiske forhold bliver gennemgået, herunder hvor servere er placeret, adgangen til disse etc.

Det er således hele virksomhedens forhold der bliver gennemgået, kontrolleret og dokumenteret, hvorefter revisionskontoret kan afgive en erklæring delt i de områder der er revideret på.

Dette kan meget vel munde ud i en erklæring der ikke vil være på det niveau virksomheden ønsker, men erklæringen indeholder også forslag til forbedringer således, at virksomheden inden næste års revision, har mulighed for at rette op på de ”gaps” der måtte være blevet påpeget i erklæringen.

Dette er baggrunden for, at der udstedes en ISAE 3402 -1 og en type ISAE 3402-2 erklæring, idet meningen er, at version 1 viser det fuldkomne billede ved første udstedelse, hvorefter virksomheden kan få en version 2 året efter hvis der er rettet op på de ting der blev påpeget ved 1. revision.

4.1.5C ISAE 3000

ISAE 3000 erklæringen er den ”lille” udgave af en revisionserklæring. Den omfatter et helt konkret område – eksempelvis GDPR, men erklæringen kan ”scopes” præcis ud fra det der ønskes erklæring på.

Som nævnt under ISAE 3402 erklæringen, så gennemgås det udvalgte område i form af stikprøver, gennemgang af udleveret dokumentation etc.

Herefter kan revisionen så udstede en revisionserklæring med deres vurdering af de enkelte dele der er gennemgået og dokumenteret. Denne erklæring er som nævnt under ISAE 3402 en version 1 erklæring.

Erklæringen giver også her henvisning og vurdering af hvilke "gaps" virksomheden måtte have inden for det konkrete område, hvorefter virksomheden inden for det næste år så har mulighed for at rette op på de forhold der måtte være, og efterfølgende få en ISAE 3000 type 2 erklæring.

4.1.6 NY ERKLÆRING FOR GDPR

Pr. 1.2.2019 udsendte FSR – danske revisorer en ny skabelon til brug for indhentelse af uafhængig revisions ISAE 3000-erklæring.

Erklæringen minder meget om den tidligere ISAE 3000 erklæring, idet den nye version dog er tilrettet overholdelse af informationssikkerhed og foranstaltninger i henhold til databehandleraftaler mellem den DA og DB. [95]

Erklæringen er tænkt anvendt mellem en DA og en DB som dokumentation for, at DB har orden og styr på både procedurer og regler, og ikke mindst har implementeret de tekniske foranstaltninger for at beskytte de data, som den DA er ansvarlig for over for den registrerede i henhold til GDPR.

Erklæringen er udarbejdet af Cybersikkerhedsudvalget under FSR – danske revisorer i samarbejde med DT, og tilsynet har udtalt at *"Revisionserklæringen fra FSR-danske revisorer har det rette fokus, og vil kunne hjælpe de dataansvarlige i forhold til at føre det fornødne tilsyn med deres databehandlere".*[96]

De i erklæringen angivne krav passer ikke nødvendigvis på alle virksomheder, hvorfor erklæringen skal tilpasses den enkelte virksomheds risikovurdering samt de foranstaltninger der mellem den DA og DB er aftalt.

Det må dog forventes, at erklæringen vil blive den foretrukne anvendte erklæring for at dokumenterer den fornødne datasikkerhed i relation til overholdelse af reglerne i GDPR, idet erklæringen er bygget op omkring den skabelon DT har udsendt til brug for databehandleraftaler.

[95] NY uafhængig ISAE 3000 erklæring - BILAG 15

[96] Artikel fra FSR danske revisorer, www.fsr.dk – BILAG 16

KONKLUSION DEL 4

Der er ingen fastsatte løsninger på hvordan selve dokumentationskravet skal foreligge, idet dette kan være forskelligt fra virksomhed til virksomhed.

For nogle virksomheder vil det være den bedste løsning med en certificering eller indførelse af et adfærdskodeks, men andre vil kunne løse dokumentationskravet bedst ved en erklæring, eller blot ved fremlæggelse af selve fortegnelseslisten udarbejdet jf. GDPR art. 30.

Uanset hvilken løsning der måtte passe den konkrete virksomhed bedst, så vil fremvisning af enten erklæringer, adfærdskodekser eller certificeringer være en form for blåstempling af, at virksomheden har foretaget den fornødne risikovurdering, foretaget de fornødne tekniske og organisatoriske tiltag, implementeret procedurer etc., hvilket er bekræftet af en uvildig part.

I relation til den DA's forpligtelse jf. GDPR art. 28 stk. 1 til kun at benytte DB der kan stille de fornødne garantier for, at DB gennemfører passende tekniske og organisatoriske foranstaltninger der opfylder kravene i.h.t. GDPR, bliver det mere og mere kutyme, at den DA stiller som krav, at DB kan fremlægge en uvildig erklæring som dokumentation for, at også denne overholder beskyttelseskravene i forordningen.

Alternativet til de i del 4 nævnte frivillige tiltag er, at en DA skal føre et tilsyn og foretage audit hos de af den DA anvendte DB for, at den DA kan dokumenterer, at den DA har styr på at den af ham udpeget DB overholder reglerne.

Dette vil bevirke et helt uoverskueligt rend mellem virksomhederne for at kontrollerer, at det der måtte være aftalt i en indgået DBA rent faktisk er overholdt.

Som tidligere nævnt vil fremvisning af uvildige erklæringer, certificeringer og adfærdskodekser langt hen ad vejen kunne anvendes som en del af dokumentationen for overholdelse af sikkerhedskravene. Dette besvarer støttespørgsmål 3 i problemformuleringen.

Det må derfor forventes, at der vil være en stigning i udarbejdelsen af uvildige erklæringer, hvilket både advokatkontorer, revisorer og andre virksomheder udbyder som et nyt fokusområde.

DEL 5 – AFGØRELSER OG PRAKSIS

Det følger af GDPR art. 51-55, at hver MS skal sikre, at der bliver nedsat et eller flere nationale uafhængige tilsynsmyndigheder, og at dette tilsyn skal sikre, at der bliver ført tilsyn og kontrol med, at reglerne i GDPR er og bliver overholdt.

De enkelte MS's datatilsyn er således omdrejningspunktet i GDPR, idet hverken Kommissionen eller Databeskyttelsesrådet har ressourcer til henholdsvis at føre tilsyn på EU niveau eller behandle alle sager i EU regi. Da Kommissionen endvidere ikke er en stat, kan Kommissionen ikke fungerer som et fælles Datatilsyn.[97]

Det er derfor i høj grad op til de enkelte medlemsstaters datatilsyn at fortolke reglerne i GDPR, herunder de enkelte medlemsstaters udfyldning af de områder som forordningen lægger op til skal udfyldes nationalt.

Det må derfor forventes, at Databeskyttelsesrådet ikke vil få forelagt og blive involveret i specielt mange sager, idet forordningen er baseret på, at de lokale DT fortolker og anvender forordningen på en korrekt og ordentlig måde.

Praksis og harmoniseringen skal derfor komme fra de respektive MS's egne datatilsyn.

EU-domstolen har hidtil spillet en væsentlig rolle i harmoniseringen, idet domstolen gennem de sidste mange år har truffet en masse afgørelser der har givet, og lagt en linje inden for persondataretten.

Da der nu i GDPR er indført et sanktionssystem i form af bøder af en anseelig størrelse, må det forventes, at flere af sagerne der i første omgang er afgjort af de nationale domstole vil blive forelagt for EU-domstolen til afgørelse.

Historisk praksis er ikke nævnt, hverken i selve GDPR eller præamblen til samme, men Peter Blume anfører[98] *"Det må antages, at er bestemmelser fra direktivet medtaget i forordningen, vil tilknyttet domspraksis stå ved magt, idet dette ligeledes er tilfældet, når praksis er baseret på primær EU-ret, mens det i andre tilfælde vil afhænge af en konkret fortolkning. En klargørende præambelbetragtning ville have været ønskelig".*

[97] Peter Blume "Den nye Persondataret" s. 24

[98] Peter Blume "Den nye Persondataret" s. 25

Det må formodes, at der vil være forskel på om behandlingen har konsekvenser på tværs i EU, eller om behandlingen alene har konsekvenser nationalt. Dette forstået på den måde, at ønsket om harmonisering vedrører hele EU, men da de fleste sager vil blive afgjort nationalt af de enkelte DT, er spørgsmålet hvor meget harmonisering der rent faktisk vil finde sted.

Peter Blume anfører[99], at hvis det *"lægges til grund, at behovet for harmonisering først og fremmest er relateret til personoplysningers betydning for det indre marked, kan der argumenteres for, at det har mindre interesse, om den nationale form for persondatabehandling vurderes på afvigende måde i de enkelte medlemsstaters praksis forudsat at charteret bliver overholdt. Hvis der er en klar og entydig skillelinje, kunne den rent nationale persondatabehandling for så vidt være holdt uden for forordningen"*

Da mange af bestemmelserne i GDPR går igen fra PDL, må det langt hen ad vejen formodes, at den praksis der allerede foreligger i dag afsagt efter PDL fortsat vil være gældende og samme linje følges.

Indtil vedtagelsen af GDPR var der ikke rigtigt givet bøder i DK der var økonomisk tunge.

Der foreligger ikke nogen praksis jf. GDPR for nuværende, men DT har i enkelte tilfælde være ude og tilkendegive deres fortolkning i forholdet til GDPR.

Dette har i skrivende stund betydet, at flere virksomheder har fået forbud, blevet indstillet til bøder af en noget større værdi end tidligere samt, at flere virksomheder er blevet pålagt at rette op på den datasikkerhed der måtte være blevet implementeret allerede for at sikre, at forordningens ordlyd er overholdt.

Som eksempler på de sager der pt. har været vurderet af DT kan nævnes DT's journalnr. 2018-41-0016[100] der omhandler 4x35's behandling af personoplysninger, nærmere betegnet deres manglende sletning af kundernes oplysninger om bestilling og afvikling af taxature. 4 x 35 oplyste, at kundens navn bliver slettet efter 2 år, mens kundens telefonnummer først slettes efter 5 år. Da telefonnummeret er personhenførbart til de taxature kunden har foretaget, skal telefonnummeret og dermed henvisningen til de foretaget taxature også slettes sammen med kundens navn. Det er således ikke en plausibel undskyldning, at virksomhedens system gør det svært at efterleve reglerne, hvorfor bestemmelserne i GDPR art. 5 stk. 1 litra b,c og e ikke anses for at være overholdt.

[99] Peter Blume "Den nye Persondataret" s. 25

[100] DT's journalnr. 2018-41-0016 – BILAG 17

DT har derfor indgivet politianmeldelse for overtrædelse af GDPR, med begæring om en bøde på DKK 1,2 mio. Sagen afventer nu politiets behandling og vurdering af hvorvidt der skal rejses sigtelse og sagen afgøres ved domstolene.

Et andet eksempel vedr. et forbud givet til TDC om, at der ikke må optages telefonsamtaler uden samtykke.[101]

TDC meddeler ved henvendelse pr. telefon, at samtalen bliver optaget med henblik på uddannelsesmæssigt formål. De personer der ringer ind, har ikke mulighed for at afgive et udtrykkeligt samtykke til at samtalen må båndes.

Dette påtalte DT, idet de gav alvorlig kritik af at samtykke ikke blev indhentet, hvorfor DT gav et midlertidigt forbud mod at optage telefonsamtaler indtil TDC har et system der giver personer på telefonen mulighed for at fravælge at blive optaget.

DT finder således, at der er tale om en overtrædelse af GDPR art. 6 stk. 1.

Fra udlandet kan nævnes et hospital i Portugal, der har modtaget en bøde på EUR 400.000,- for ikke at have begrænset adgangen til patienters journalmateriale.

Uagtet, at ingen sager i øjeblikket har været forelagt de danske domstole eller EU-domstolene til vurdering og afgørelse, så tegner der sig et klart billede af, at det danske DT har tænkt sig at stramme alvorligt op i forhold til GDPR og den hidtil gældende, nu historiske praksis.

DEL 6 – KONKLUSION

Med baggrund i den hastige teknologiske udvikling, herunder den massive anvendelse af internettet og dermed deling af data i et omfang der ikke tidligere var set, var der på EU niveau enighed om, at reglerne om persondatabeskyttelse skulle undergå en gennemgribende opdatering for fortsat, at sikre den enkelte registrerede sine rettigheder og frihedsrettigheder.

Direktiv 95/46/EF var udarbejdet inden internettet for alvor slog igennem, og persondatasikkerhed blev ikke på daværende tidspunkt taget helt så seriøst som i det omfang det er sket med implementeringen af GDPR.

[101] DT afgørelse med journal nr. 2019-31-0977 – BILAG 18

Særligt den øgede anvendelse af opbevaring af data i cloud løsninger har bevirket, at data spredes overalt i verden i løbet af få sekunder, og den registrerede har ofte ingen ide om hvor dennes data reelt befinder sig, og hvem der reelt har adgang til disse. DT hilser principielt den øgede teknologiske udvikling velkommen, men har bl.a. i afgørelse med journal nummer 2010-52-0138 (Odense Kommunes anvendelse af cloud-løsning) udtalt, at den DA skal foretage risikovurderingen i forhold til anvendelsen af en cloud-løsning hvis en sådan tænkes anvendt. Risiko vurderingen skal foretages ud fra de aspekter behandlingen omhandler.

Der er således stor fokus på netop anvendelsen af cloud-computing med tilhørende sikkerhedsforanstaltninger, og både artikel 29-gruppen, DT og flere andre interessenter, herunder anerkendte forfattere, har udtalt sig omkring de risici der måtte være forbundet med og imødegåelsen af risici ved anvendelsen af cloud-computing.

Netop indførelsen af en forordning i stedet for det tidligere direktiv viser med al tydelighed, at der nu er lagt op til, at håndteringen af persondata med dertil hørende sikkerhedsforanstaltninger skal tages særdeles seriøst.

Muligheden for at få tildelt bøder af en anseelig størrelse er værktøjet til at få alle virksomheder og offentlige samt statslige institutioner til at overholde reglerne afstukket i GDPR.

Der er med implementering af GDPR lagt op til en langt mere risikobaseret tilgang til opfyldelsen af datasikkerheden, idet målet med at tilgå sikkerhedsforanstaltningerne ud fra en konkret risikovurdering gerne skulle være, at beskyttelsesniveauet bliver øget.

Både DA og DB er nu blevet forpligtet til at forholde sig til den enkelte behandling, og baseret herpå, foretage de nødvendige sikkerhedsforanstaltninger der er nødvendige for at opfylde sikkerhedskravene netop baseret på de risici den enkelte behandling kræver.

Kravene i GDPR om beskyttelse gennem design- og standardindstillinger er nye tiltag i GDPR. Der er ikke i selve forordningen angivet hvad dette rent faktisk indebærer andet end, at den DA er forpligtet til at gennemføre tekniske og organisatoriske foranstaltninger. Denne forpligtelse gælder både på tidspunktet inden en egentlig behandling påbegyndes, samt på tidspunktet hvor behandlingen pågår.

Da den teknologiske udvikling går så stærkt som tilfældet er, er der ikke angivet konkrete tiltag der skal tages for at opfylde sikkerhedskravene, hvorfor ordlyden i forordningen mere må ses som de overvejelser den DA skal gøre sig inden en egentlig behandling påbegyndes. Teknologien bevæger sig alt andet lige hurtigere end hastigheden for at få ændret ordlyden i selve

forordningen, hvorfor det giver god mening, at der ikke i forordningen er angivet konkrete tiltag på hvad korrekte sikkerhedsforanstaltninger skal være.

Det tætteste på en konkret angivelse af hvad der menes med ”passende tekniske og organisatoriske tiltag” er angivet i GDPR art. 32 stk. 1 litra a-d, men heller ikke dette giver et fyldestgørende svar på hvornår og hvad der reelt menes med hvad der er passende. Listen er således ikke udtømmende, og det er lagt op til den enkelte DA at foretage en vurdering af, hvad der for den konkrete behandling vil være den konkrete korrekte sikkerhedsforanstaltning.

Der er dog angivet at pseudonymisering og kryptering kunne være en af måderne at sikre data på.

Igen her ses eksempel på, at der skal foretages en risikobaseret tilgang til selve behandlingen.

Såfremt der skal indkøbes nye systemer, skal der derfor indtænkes datasikkerhed allerede i designet af systemet, ligesom den DA skal sikre sig, at allerede eksisterende systemer tilrettes og standardindstilles til, at der sker den mindst mulige manuelle behandling af persondata, idet systemerne kan håndtere det meste af behandlingen med den korrekte datasikkerhed inkorporeret i selve systemet.

Uagtet at ordlyden i GDPR er ændret i forhold til ordlyden om behandlingssikkerhed angivet i PDL, er der ikke rent materielt den store forskel i kravene til det beskyttelseskrav der skal opfyldes i relation til selve behandlingssikkerheden.

Det formodes derfor, at der fremadrettet vil ske en skelen til nuværende praksis. Det er ikke på nuværende tidspunkt muligt at komme med en fyldestgørende konklusion på, hvilket niveau domstolene vil lægge sig på ved vurderingen af hvornår kravene til gennemførelse af de tekniske og organisatoriske sikkerhedstiltag er opfyldt på fyldestgørende måde, hvilket også i høj grad vil afhænge af de tiltag den enkelte DA vælger at ”løse” behandlingssikkerheden med.

Rækkevidden af behandlingssikkerheden er derfor dynamisk og fuldstændig afhængig af hvilken behandling der finder sted, hvilke data der behandles og formålet hermed, idet den enkelte DA skal afpasse sine sikkerhedstiltag ud fra samme.

Der er dog ingen tvivl om, at praksis vil blive skærpet efter GDPR i forholdet til PDL, idet alene muligheden for at sanktionere med bøder af en hidtil uset størrelse vil give mulighed for de enkelte nationale DT til at få virksomhederne og offentlige myndigheder til at tage persondatasikkerheden alvorligt.

Som omtalt i del 4 er der flere muligheder for at kunne dokumentere sin behandlingssikkerhed, herunder de frivillige ordninger i form af adfærdskodekser, certificeringer og udstedelse af forskellige typer af erklæringer.

Minimumskravet er fortegnelseskravet angivet i GDPR art. 30, men sådanne fortegnelser angiver kun i overordnet træk den behandling der finder sted, formålet hermed og i overordnede træk hvilke tiltag der er taget for at sikre datasikkerheden.

Det er selvfølgeligt muligt at efterprøve de i fortegnelsen angivne tiltag der er foretaget, hvorfor fortegnelsen vil være udgangspunktet for en evt. audit. Individuelle erklæringer – ISO 27001 og ISAE erklæringer – går mere i dybden omkring særligt IT-sikkerheden, og er ofte et dokumentationskrav fra den DA til evt., DB således, at den DA ikke nødvendigvis behøver at tage på audit, men kan accepterer en uvildig erklæring som dokumentation for overholdelse af datasikkerheden.

De forskellige erklæringer indeholder kontroller af både de angivne processer, de anvendte systemer, adgangen til diverse data, datasikkerheden, 3. Lands overførsler, slettepolitik og generelt hele informationssikkerhedspolitikken hos DB.

Rækkevidden af selve dokumentationskravet er således direkte relateret til de tiltag der er implementeret for at sikre datasikkerheden.

LITTERATURLISTE

Love, betænkninger, bekendtgørelser og præambler

Persondataloven (PDL) Lov nr. 429 af 31. Maj 2000 om behandling af personoplysninger. **Historisk** https://www.retsinformation.dk/forms/r0710.aspx?id=828

Databeskyttelsesloven (DBL) Lov nr. 502 af 23. Maj 2018 om supplerende bestemmelser i forbindelse med behandling af personoplysninger. - https://www.retsinformation.dk/Forms/r0710.aspx?id=201319

Præambel til GDPR - https://themis.dk/synopsis/docs/Lovsamling/Persondataforordningen_praeambel.html

Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger der behandles for den offentlige forvaltning.
https://danskprivacynet.files.wordpress.com/2008/06/sikkerhedsbekendtgc3b8relse.pdf.

Bekendtgørelse nr. 535 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, der behandles for domstolene - https://www.retsinformation.dk/Forms/R0710.aspx?id=850

Betænkning 1565 om Databeskyttelsesforordningen (2016/679) – de retlige rammer for dansk lovgivning.
http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf

Traktater

TEUF om Unionens funktionsmåde.https://eur-lex.europa.eu/legalcontent/DA/TXT/PDF/?uri=CELEX:12012E/TXT&from=DA

Forordninger og direktiver

(GDPR) Europa-Parlamentets of Rådets forordning 679/2016/EU om beskyttelse af personer i forbindelse med behandling af personoplysninger. - https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679&from=DA

EU direktiv 95/46/EF af 24. Oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger. **Historisk -** https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:31995L0046&from=DA

Vejledninger

Datatilsynets vejledning om fortegnelse, Januar 2018 - https://www.datatilsynet.dk/media/6567/fortegnelse.pdf

Litteratur

Carsten Munk-Hansen, Retsvidenskabsteori, Jurist- og Økonomforbundets Forlag 2014, 1. Udgave, 1. oplag.

Peter Blume, Den nye persondataret – Forordning 2016/679 om databeskyttelse/Lov 502/2018 om databeskyttelse, Jurist- og Økonomforbundets Forlag 2018, 2. Udgave, 1. oplag.

Henrik Waaben og Kristian Korfits Nielsen, Lov om behandling af personoplysninger med kommentarer, Jurist- og Økonomforbundets Forlag 2015, 3. Udgave, 2. oplag.

BILAG

Vejledninger

Bilag 4 - Artikel 29-gruppen – WP 193/Opinion 3/2012 om biometriske data

Bilag 7 - Artikel 29-gruppen – WP 203/Opinion 3/2013 om formålsbegrænsning

Bilag 11 - Datatilsynets vejledning om "skærpet praksis i forhold til krypteret e-mail

Praksis

Bilag 1 - De Forenede sager – C-465/00, C-138/01 og C-139/01

Bilag 2 - C-582/14 – Patrick Breyer mod Bundesrepublik Deutschland (Præjudiciel afgørelse om IP-adresser)

Bilag 3 - Datatilsynet journal nummer: 2018-31-0208 – Lasso X ApS om offentliggørelse af data hentet fra CVR registeret

Bilag 5 - Datatilsynet journalnummer: 2009-082-0087 – Tivoli og Logica om adgangskontrol ved brug af ansigtsgenkendelse

Bilag 6 - Datatilsynet journalnummer: 2005-212-0299 – Tivoli om anvendelse af billeddatabase i forbindelse med adgangskontrol

Bilag 8 - Datatilsynet journalnummer: 2008-632-0034 – Forsvarets videregivelse af data til forsikringsselskab med henblik på markedsføring

Bilag 9 - Datatilsynet journalnummer: 2013-217-0345 – Nets om manglende kryptering af bl.a. CPR nr. på hjemmeside

Bilag 10 - Datatilsynet journalnummer: 2013-631-0053 – Manglende overholdelse af sikkerhed omkring afsluttede sager samt manglende oplysning til kunder om optagelse af telefonsamtaler

Bilag 17 - Datatilsynet journalnummer: 2018-41-0016 – 4x35 om manglende sletning af data om taxakørsel

Bilag 18 - Datatilsynet journalnummer: 2018-31-0977 – TDC om forbud om optagelse af telefonsamtaler uden samtykke

Artikler

Bilag 12 - Hacker-angreb på Mærsk - https://www.computerworld.dk/art/242820/maersk-selskab-ramt-af-nyt-stort-hacker-angreb-hackere-har-stjaalet-60-000-vigtige-mails-gennem-11-maaneder

Bilag 13 - Hacker-angreb på universiteter - https://www.dr.dk/nyheder/indland/hacker-angreb-paa-tre-danske-universiteter-dtu-medarbejdere-gik-i-faelden

Bilag 14 - Informationssikkerhed ISO 27001 / DS
https://www.ds.dk/da/standardisering/ledelsesstandarder/informationssikkerhed

Bilag 16 - FSR's lancering af ny erklæring for ISAE 3000 -
https://m.fsr.dk/Faglige_informationer/Om_revisor/Persondataforordningen/FSR%20lancerer%20paa%20baggrund%20af%20samarbejde%20med%20Datatilsynet%20ny%20erklaering%20om%20persondata

Erklæringer

Bilag 15 - Uafhængig revisorers ISAE 3000-érklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med (Dataansvarlig)

ORDOPTÆLLING