

Krypteringskravet i forhold til videregivelse af fortrolige og følsomme personoplysninger i transit

Kandidatspeciale af Rasmus Jensen - Aalborg Universitet, 2018

The encryption requirement in relation to the transmission of confidential and sensitive personal data in transit

Indholdsfortegnelse:

Abstract:	3
1. Indledning:	4
1.1. Problemfelt:.....	5
1.2. Problemformulering:.....	5
1.3. Afgrænsning:.....	5
2. Metode:	6
2.1. Den retsdogmatiske metode:.....	6
3. Formålet med persondatalovgivningen:	9
3.1. Privatlivsbeskyttelse:	10
3.2. Integritetsbeskyttelse.....	12
3.3. Teoretisk løsningsmodel:	14
3.4. Sammenfatning:	17
4. Retsgrundlag:	17
4.1. Registerlovene:.....	17
4.2. Persondatadirektivet og persondataloven:.....	18
4.3. Persondataforordningen:	19
4.4. Sikkerhedsbekendtgørelsen:.....	21
4.5. Sammenfatning:	22
5. Grundlæggende princip:	23
5.1. Sammenfatning:	25
6. Pligtssubjekter:	26
6.1. Dataansvarlig:	26
6.2. Databehandler:	27
6.3. Sammenfatning:	28
7. Personoplysningsbegrebet:	28
7.1. Sammenfatning:	32
8. Behandlingsbegrebet:	32
8.1. Sammenfatning:	34
9. Sikkerhedsniveau:	34
9.1. Sikkerhedsniveauets øvre og nedre grænse:.....	36
9.2. Samtykke og sikkerhedsniveau:	38
9.3. Sammenfatning:	40
10. Sikkerhedsforanstaltninger:	40
10.1. Det aktuelle tekniske niveau og implementeringsomkostninger:.....	41
10.2. Sammenfatning:	45
11. Krypteringskravet:	46
11.1. Ekstern transmission:	47
11.2. Retsgrundlag:	51
11.3. Sammenfatning:	52
12. Konklusion	53
13. Perspektivering:	55
14. Litteraturfortegnelse:	56
15. Bilag	59

Abstract:

The processing of personal data involves personal data security rules. Without sufficient security the personal data protection becomes insufficient. Personal data security requires a fair balance risk assessment. In the Danish practice from the legislation of personal data there is an unconditional encryption requirement for external transmission of personal data by e-mail, which is not subject to a risk assessment as such. In other words, all e-mails in the public and private sectors must be sent encrypted, if it contains confidential or sensitive personal data.

The focus of this thesis is to investigate whether this legal obligation of a unconditional encryption requirement is in accordance with the General Data Protection Regulation (GDPR). This thesis will firstly interpret the rule of law that regulates personal data protection. Hereafter, the thesis will apply the derived legal conditions and principles to the legal position and compare whether the legal protection is in accordance with current law. The abovementioned parts will provide a basis for a discussion and an assessment of whether the encryption requirement is in accordance with article 32 (1) and (2) of the GDPR.

The author of this thesis concludes that the unconditional encryption requirement for external transmission of personal data by e-mail containing confidential and sensitive personal data should always be subject to a risk assessment as required by article 32 (1) and (2). However, the current legal situation requires that the unconditional encryption requirement must be implemented regardless of how confidential the data is. For instance, order confirmation of music purchases or loan receipts from the library is also subject to the encryption requirement. This means that any e-mail containing confidential or sensitive personal data must be legally encrypted. However, an absolute encryption of all outgoing e-mails including common personal data will not be in accordance with the legal basis, as this will go beyond of what a risk assessment will require. This entails that data administrators and their outsourced data providers are facing a big task that will lead to significant administrative costs in the public and private sectors. They face a great challenge of identifying and categorizing the personal data they process, because they have to determine whether the personal data should be encrypted if sent by using e-mail.

The current state of the law is relatively unclear in regard to what the term confidential entails, whereas the sensitive personal data is thoroughly regulated by law. Hopefully, the future practice will clarify which personal data should be encrypted, so that there is transparency of which obligations are required. This will benefit the citizen's legal protection of personal data privacy, and make the legal practise clear for those who use personal data in their every day administration and have the need to disclose the personal data by e-mail.

1. Indledning:

I persondatalovgivningen er der pålagt den dataansvarlige og databehandleren en behandlingsforpligtelse til at iværksætte persondatasikkerhed omkring de behandlinger af personoplysninger, de foretager. Det medfører visse sikkerhedskrav, som skal imødegå sikkerhedsbrud, der kan kompromittere de behandlede personoplysninger.

Transmission af skriftlig kommunikation via e-mail indebærer særligt en risikoprofil med risici for uvedkommendes tilegnelse. I den forbindelse er kryptering en måde, hvorpå videregivelse af personoplysninger i transit kan beskyttes. Ved korrekt anvendelse vil en sådan sikkerhedsforanstaltning i almindelighed opfylde lovgivningens sikkerhedsmål.

Det persondataretlige retsgrundlag er fra d. 25 maj 2018 den såkaldte persondataforordning i alle de europæiske medlemsstater.¹ Ifølge sikkerhedsreglen i forordningen skal den dataansvarlige og databehandleren iværksætte passende sikkerhedsforanstaltninger, således der er etableret et passende sikkerhedsniveau. Dette gennemføres ved en risikobaseret vurdering, hvor de relevante sikkerhedsrisici ved behandling af personoplysninger inddrages. Dermed er reguleringsgrundlaget en retlig standard, der skal udfyldes af pligtssubjekterne ved en skønsæssig hensynsafvejning. Det skønsæssige råderum medfører en usikkerhed om, hvornår det risikobaserede retsfaktum er opfyldt. Samtidigt giver det en mulighed for, at foranstalte et persondatasikkerhedsniveau ud fra samtlige relevante omstændigheder.

Det har tidligere været Datatilsynets opfattelse, at krypteringskravet alene var pålagt offentlige myndigheder. Indtil nu har det været anbefalet den private sektor, at følge den samme praksis om obligatorisk kryptering. På baggrund af forordningen og den informationsteknologiske udvikling har tilsynet skærpet sin praksis, hvorefter sikkerhedskravet nu både gælder den offentlige og private sektor.² Derfor skal enhver transmission af fortrolige og følsomme personoplysninger over et netværk via e-mail krypteres. Denne praksisændring medfører en betydelig indskrænkning i det persondatasikkerhedsmæssige skøn, som er tillagt aktørerne, idet en håndhævende retsfølge allerede er fastlagt. Specialet behandler det principielle spørgsmål om et udfald af gældende ret, der beror på en retlig standard, kan berettige en almengyldig forestilling om kryptering, som en ideel sikkerhedsforanstaltning. Med andre ord om et generelt sikkerhedskrav om kryptering har tilstrækkelig hjemmel, ud fra en praktisk indsigt i det retlige grundlag.

¹ Europa-Parlamentets og Rådets Forordning 2016/679 af 27. april 2016 (PDF)

² <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2018/jul/skaerpet-praksis-ift-krypteret-e-mail/>

1.1. Problemfelt:

Specialet vil undersøge, hvordan retsgrundlaget definerer persondatasikkerhed med udgangspunkt i krypteringskravet. Det omfatter fastlæggelse af pligtsubjekter, retsfaktum og de betingelser, der opfylder sikkerhedsreglen PDF art. 32, stk. 1 og 2.

1.2. Problemformulering:

Dette speciale vil undersøge det persondatasikkerhedsmæssige krypteringskrav i forhold til videregivelse af fortrolige og følsomme personoplysninger ved ekstern transmission. På den baggrund søger specialet at besvare følgende problemformuleringsspørgsmål:

- Hvordan defineres persondatasikkerhed, og hvad er gældende ret?
- Er Datatilsynets praksis angående et obligatorisk sikkerhedskrav om kryptering i overensstemmelse med hjemmelsgrundlaget i PDF art. 32, stk. 1 og 2?

1.3. Afgrænsning:

Specialet har sit udgangspunkt i krypteringskravet inden for persondatasikkerhed. Lovbestemmelserne i PDF art. 32, stk. 1 og 2 om sikkerhedsforanstaltninger og sikkerhedsniveau vil udgøre den grundlæggende juridiske forforståelse. Derfor vil de andre ikke-udtømmende eksempler på sikkerhedsforanstaltninger i bestemmelsen kun blive behandlet sporadisk, fordi krypteringskravet relaterer sig til PDF art. 32, stk. 1, litra a).

Problemformuleringen skal ikke forveksles med det offentligtretlige princip om forbud mod at sætte skøn under regel, idet Datatilsynets administrative praksis i undtagelsestilfælde ved en skønsudøvelse tilsidesætter krypteringskravet. Dette anses ikke for en afstandtagen fra det generelle sikkerhedskrav, fordi tilsynet fastholder en praksis om, at der skal foretages obligatorisk kryptering, når der afsendes en e-mail med fortrolige eller følsomme personoplysninger. Fremstillingens fokus angår det principielle spørgsmål om ubetingede sikkerhedskrav må påkræve tilstrækkelig hjemmel i reguleringsgrundlaget i medfør af legalitetsprincippet.

Der vil blive foretaget en inddragelse af tidligere persondataretlig lovgivning, når retstilstanden angående persondatasikkerhed forekommer videreført. Da det skal medvirke til en forforståelse af gældende ret. Af hensyn til omfanget af specialet vil der ikke blive foretaget en nærmere fortolkning af de øvrige behandlingsbestemmelser, men de vil blive inddraget, hvor de har indvirkning på retstilstanden af persondatasikkerhed i relation til krypteringskravet. Den retsdogmatiske analyse vil ikke tage komparativ form af udenlandsk

ret, imidlertid vil norsk retslitteratur blive inddraget som inspiration, fordi der er et fælles lovmæssigt grundlag.

2. Metode:

2.1. Den retsdogmatiske metode:

Med henblik på at beskrive, fortolke og systematisere den i samtiden gældende ret er dette speciale udarbejdet i overensstemmelse med den retsdogmatiske metode betegnet *de lege lata*.³ Specialets hensigt er ud fra en metodisk tilgang at fastlægge, hvad gældende ret er på det persondataretlige retsområde angående persondatasikkerhed i relation til krypteringskravet.

Ved brug af den retsdogmatiske metode vil specialet udgøre en teoretisk beskrivelse af gældende ret, som vil skabe sammenhæng mellem teori og praksis. Det nødvendiggør en forståelse af, at det persondataretlige retsområde har fået ny lovgivning fra den 25. maj 2018 i form af en forordning. Det medfører, at tidligere lovgivning på retsområdet ophæves, idet forordningen vil virke som en almenyldig lov i Danmark.

Forståelsen af gældende ret nødvendiggør en retsdogmatisk analyse af gældende ret både før og efter forordningens ikrafttrædelse, fordi den nye lovgivning kan medføre ændringer af den tidligere retstilstand. De forskellige retskilder vil igennem specialet blive vurderet og sammenlignet i forhold til deres retskildemæssige værdi. Der vil blive inddraget fortolkningsbidrag, såsom retslitteratur og Datatilsynets vejledninger, fordi retskildegrundlaget er beskedent. De er således subsidiære i forhold til de traditionelle retskilder, fordi de almindeligvis ikke har retskildemæssig værdi. Der hvor lovbestemmelsen er uklar, vil inddragelse af ikke-bindende retskilder tjene som et bidrag til udfyldning af retsstillingen.

Da retsgrundlaget er en EU-retlig retsakt, vil specialets fortolkningsstil blive udført på baggrund af den hermeneutiske fortolkningslære, der er en del af den retsdogmatiske metode. Omdrejningspunktet er den hermeneutiske cirkel, hvori man ved juridisk forforståelse og retsområdets helhed skaber meningssammenhæng, som fjerner uklarheder, hvorefter man opnår den ønskede retlige sandhed.⁴ Med andre ord skaber den juridiske forforståelse grundlag for den praktiske og teoretiske behandling af retsreglen på baggrund af

³ Munk-Hansen, Retsvidenskabsteori, s. 86

⁴ Munk-Hansen, Retsvidenskabsteori, s. 41

retsgrundlagets historicitet.⁵ Den antages særlig anvendelig på teleologiske tekster, hvor formålsforståelsen af ordlyden søges opfyldt ved en meningssammenhæng. Det vil formentlig skabe kohærens til EU-Domstolens fortolkningsstil, der anvender en formålsbestemt fortolkning. Det indebærer en fortolkning af bestemmelseernes formål ud fra formålsangivelserne i præambel-betragtningerne og de indledende formålsbestemmelser.⁶ Det kan illustreres med sag C-553/07, Rijkeboer, hvor EU-domstolen anlægger en formålsfortolkning, når den skal vurdere omfanget af en persondataretlig forpligtelse. Det fremgår af præmis nr. 45 *”denne artikel fortolkes på grundlag af sit **formål** vurderet i lyset af **målene** med direktivet.*” [Fremhævet her]. Ved fortolkning af retsreglen PDF art. 32, stk. 1 og 2 forudsætter det metodisk, en forståelse af den kontekst, hvori den indgår i forordningen, hvorefter meningsindholdet skal vurderes i lyset af målsætningen med retsakten. Det er i overensstemmelse med den hermeneutiske fortolkningslære, der påkræver en forståelse af de enkelte dele i form af regler og principper samt lovens formål, før der opnås en meningssammenhæng.

For at opnå en helhedsorienteret meningssammenhæng i overensstemmelse med den hermeneutiske fortolkningslære forudsætter det kendskab til retsgrundlagets historie. Det nødvendiggør en inddragelse af reglens udvikling i form af forarbejder og lovændringer, fordi de momenter indgår i en meningsforståelse af retsreglens tiltænkte anvendelsesområde. For at forstå helheden ved fortolkning af den administrative praksis i henhold til krypteringskravet skal det forstås, at Datatilsynet er bundet af legalitetsprincippet efter Grundloven § 3, samt at domstolene kan afprøve tilsynets afgørelse ifølge Grundloven § 63 om øvrigmyndighedernes grænser. I forlængelse heraf udøver Datatilsynets sin tilsynsvirksomhed i fuld uafhængighed efter PDF art. 52, stk.1, hvilket har medført manglende rekursmulighed.

På det persondataretlige retsområde er der ikke tradition for, at Datatilsynets afgørelser indbringes for domstolene. Det skyldes formentlig, at sanktionsniveauet for overtrædelse af persondatalovgivningen har været begrænset.⁷ I mangel af retspraksis, der kan fastlægge en persondataretlig retsopfattelse, er det Datatilsynets afgørelser, som fastlægger, hvorledes den persondataretlige lovgivning skal fortolkes. Den administrative praksis bliver dermed en væsentlig retskilde og vigtigere end retspraksis.⁸ Når den administrative praksis anses for en væsentlig retskilde, medfører det, at Datatilsynet bliver den præjudikatskabende retsinstans.⁹ Den retskildemæssige værdi understøttes af, at den administrative praksis er en bindende

⁵ Munk-Hansen, Retsvidenskabsteori, s. 181

⁶ Tranberg, Nødvendig behandling af personoplysninger, s. 74

⁷ Tranberg, m.fl., Internetretten (2017), s. 98

⁸ Blume, Retssystemet og juridisk metode, s. 248

⁹ Tranberg, Nødvendig behandling af personoplysninger, s. 81

retskilde for Datatilsynet. Borgeren kan herefter med tillid indrette sig efter forståelsen for reglernes anvendelse ud fra de konkrete afgørelser.¹⁰ Dette speciale vil anvende den administrative praksis som udgangspunkt for de persondataretlige reglers anvendelse i praksis. Det skal imidlertid erkendes, at en autoritativ fortolkning af PDF kun opnås ved EU-domstolen, men ved manglende retspraksis af en relevant retsregel vil Datatilsynets administrative praksis blive en præjudikatskabende retskilde.

Den beskrivende del af specialet vil indebære en gennemgang af det retsgrundlag, forarbejder og retslitteratur, der gør sig gældende for besvarelse af retsstillingen. Med udgangspunkt i den hermeneutiske fortolkningslære skal denne beskrivelse afgive en juridisk forforståelse af den retskilde, hvori meningssammenhængen skal findes.¹¹ Det, der søges forstået, er retskilden i relation til krypteringskravet inden for persondatasikkerhed. Derefter hvordan det kommer til udtryk i den administrativ praksis på det persondataretlige retsområde. Ud fra den hermeneutiske fortolkningslære forudsætter det en forståelse af helheden ved den autoritære tekst i retskilden. Før der opnås indsigt i helheden, forudsætter det en forståelse af de enkelte dele. Ved forståelse af krypteringskravet skal man således forstå den bagvedliggende opbygning og struktur af den persondataretlige lovgivning. Det indebærer en forståelse af formålet med PDF, som både er beskyttelse af personoplysninger på baggrund af grundlæggende rettigheder, samt sikring af den frie udveksling af personoplysninger ifølge PDF art. 1, stk. 2 og 3. Hertil skal den tidligere persondatalovgivning bemærkes, idet registerlovene fra 1979 alene var dansk lov.¹² Det efterfølgende PDD var et direktiv fra 1995, der blev implementeret ved PDL i 2000.¹³ PDF blev vedtaget i 2016 med virkningspunkt fra d. 25. maj 2018. Forordningen er almen gyldig, bindende i alle enkeltheder og gælder umiddelbart i Danmark som medlemsstat ifølge art. 288, 1. og 2. pkt. i TEUF.¹⁴ Dermed er det et relativt nyt supranationalt retsområde, hvor en del fortolkningsspørgsmål endnu ikke er afklaret i retspraksis

Den retsdogmatiske analyse vil på baggrund af den beskrivende del efterfølgende analysere og systematisere de anvendte retskilder og fortolkningsbidrag. Den analyserende del vil omfatte retsgrundlaget, den administrative praksis og retspraksis i forhold til krypteringskravet og sikkerhedsreglen i PDF art. 32, stk. 1 og 2. Den systematiserende del

¹⁰ *Munk-Hansen*, Retsvidenskabsteori, s. 340

¹¹ *Munk-Hansen*, Retsvidenskabsteori, s. 43

¹² Lov om offentlige myndigheders registre nr. 294 af 08/06/1978 (LOMR), Lov om private register m.v. nr. 293 af 08/06/1978 (LPRG)

¹³ Europa-Parlamentets og Rådets direktiv 1995/46 af 24. oktober 1995 (PDD), Lov om behandling af personoplysninger nr. 429 31/5/2000 (PDL)

¹⁴ Traktaten om Den Europæiske Unions Funktionsmåde (TEUF)

angår de generelle principper og betingelser, der kan udledes af analysen. De vil være afgørende for, om den retlige subsumption i Datatilsynets administrative praksis med retsfølgen om et generelt krypteringskrav er i overensstemmelse med hjemmelsgrundlaget. Det vil ende med en diskuterende og vurderende konklusion i overensstemmelse med den beskrivende, fortolkende og systematiserende retsdogmatiske metode, med udgangspunkt i den hermeneutiske fortolkningslære.

3. Formålet med persondatalovgivningen:

Før der kan foretages en formålsorienteret analyse af persondatasikkerheden skal formålet med lovgivningen og de bagvedliggende beskyttelsesinteresser introduceres. Dette afsnit vil definere persondaterettens formål, hvilket vil udgøre den ramme, hvori hensyn skal afvejes ved fortolkning af de persondataretlige regler.

Målsætningen med PDF er en videreførelse fra PDD med ønske om en skærpet harmonisering af persondatalovgivningen på fællesskabsniveau. Det kan formuleres som medlemsstaternes sikring af fysiske personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger, især retten til privatlivets fred og retten til beskyttelse af personoplysninger.¹⁵

Forordningen er ikke en absolut beskyttelseslov, idet den tilstræber at aktørerne kan behandle personoplysninger i et rimeligt omfang inden for lovgivningens rammer. Det var allerede tilkendegivet i PDL' forarbejder ved implementeringen af PDD, hvor formålet med daværende lov var en sikring af borgernes privatliv og personlige integritet på den ene side, og på den anden side hensynet til at bevar og udbygge en effektiv offentlig administration og et privat erhvervsliv, som ikke pålægges unødige byrder.¹⁶ Af samme forarbejder fremgår det, at særligt persondatalovgivnings beskyttelsesinteresser skal forstås i sammenhæng med den informationsteknologiske udvikling. Derfor var formålet med lovgivningen både at sikre beskyttelsen af den enkeltes integritet i det informationsteknologiske samfund, samtidig med at anvendelsen af nye teknikker i samfundsudviklingen ikke hæmmes.¹⁷

Formålet er således en personbeskyttelse, som særligt relaterer sig til informationsteknologi, idet PDF' materielle afgrænsning for det første angår elektronisk

¹⁵ Jf. PDF art. 1, stk. 2

¹⁶ Betænkning 1345/1997 om behandling af personoplysninger, s. 151

¹⁷ Betænkning 1345/1997 om behandling af personoplysninger, s. 173

persondatabehandling.¹⁸ Denne afgrænsning afspejler beskyttelsesinteressen, fordi denne aktualiseres, når personoplysninger anvendes elektronisk, fordi de bliver let tilgængelige.¹⁹ Det kan medføre en behandling, som er krænkende for den personlige integritet og privatlivets fred, hvilket påkræver en dynamisk retsbeskyttelse, der både fungerer som et retsværn for den registrerede, samtidig med den tilgodeser de behov, som forekommer fra aktørerne i det informationsteknologiske samfund.²⁰

Det overordnede formål med PDF kan på baggrund af ovennævnte generelt defineres som en beskyttelse mod misbrug af personoplysninger vedrørende beskyttelsesobjektet (»den registrerede«), hvor beskyttelsesniveauet reguleres ved en hensynsafvejning af interesserne fra beskyttelsesobjektet (»personoplysninger«) og pligtsubjekterne (»dataansvarlige« og »databehandlere«).

3.1. Privatlivsbeskyttelse:

En af de gennemgående beskyttelsesinteresser i persondatalovgivningen er retsbeskyttelsen af privatlivets fred. Der er ikke en entydig retlig definition af begrebet »privathed« hvilket skyldes begrebets mange facetter.²¹ *Tranberg* anfører, at det enkelte menneskes personlige præference afgrænser og karakteriserer den offentlige og den private sfære.²² Det medfører den vanskelighed det er at udforme en retlig regulering, hvori privatlivet har en beskyttelsesmæssig værdi, som ikke må krænkes. Denne uklare kontur medfører, at man udnævner en beskyttelsesinteresse til at være målet, som der alene er visse vage forestillinger om, hvorefter man forsøger at konkretisere og tilnærme sig beskyttelsesinteressens meningsindhold i lovreguleringen.²³

Blume og Herrmann anfører, at retten til privatliv har sit grundlag i den retligt funderede respekt for individets integritet og værdighed.²⁴ Den retlige fundering kan fremhæves ved Registerudvalgets udtalelse om, at der er en almindelig antagelse i dansk ret, hvor personligheden og privatlivets fred er beskyttet af almindelige retsgrundsætninger.²⁵ Den

¹⁸ Jf. PDF art. 2, stk. 1 om helt eller delvis elektronisk databehandling, og på anden manuel behandling af personoplysninger, der er eller vil blive indeholdt i et register.

¹⁹ *Blume*, Den nye persondataret – Persondataforordningen, s. 49

²⁰ *Andersen*, IT-retten, s. 601: »Den registrerede» er et terminologibegreb for den fysiske person, hvis personoplysninger er genstand for behandling.

²¹ *Blume og Herrmann*, Ret, privatliv og teknologi, s. 62: Uden en skarp skillelinje skelnes der faktisk og retligt mellem fysisk, psykisk, informationelt, kommunikativt og territorielt privatliv.

²² *Tranberg*, m.fl., Internetretten (2017), s. 97

²³ Betænkning 767/1976 om offentlige registre, s. 13

²⁴ *Blume og Herrmann*, Ret, privatliv og teknologi, s. 69

²⁵ Betænkning 687/1973 om private registre, s. 28

egentlige retskildemæssige betydning af sådanne retsgrundsætninger er tvetydig. Alligevel kan antagelsens karakteristik fra Registerudvalget anvendes som grundlag for, at der i dansk ret er en bred beskyttelsesinteresse af privatlivets fred i retsordenen.

Registerudvalget beskrev privatlivets fred som *”Man kan tale om beskyttelse af privatlivets fred, når der sættes grænser for blotlæggelse af forhold, der ikke umiddelbart er tilgængelige for andre, der kommer i forbindelse med den pågældende, f.eks. blotlæggelse af en person gennem videregivelse af systematisk indsamlede oplysninger om ham.”*.²⁶ I en samlebetegnelse anvender *Udsen* et privatlivshensyn, hvilket indebærer, en ret til at blive ladet i fred, samt en selvbestemmelsesret (med indskrænkninger) til hvilke personoplysninger andre må behandle om den pågældende.²⁷ Der er således en kontinuitet i den overordnede forståelse af begrebet, som er en retsbeskyttelse af privatsfæren.

I videre forstand anvender *Udsen* et personlighedshensyn, som er en beskyttelse mod udbredelse af oplysninger, der er ukorrekte eller kan nedsætte en persons omdømme.²⁸ Det kan i modsætning til privatlivshensynet bestå i personoplysninger, som umiddelbart kan iagttages af den, der kommer i kontakt med den pågældende, som derefter anvendes uden tilladelse.²⁹ Dermed omfatter personlighedshensynet en bredere beskyttelse af personoplysninger af mere almindelige karakter, hvorimod privatlivshensynet taler for beskyttelsen af personoplysninger af privat karakter.

Formuleringerne betragter sammenfaldende privatlivets forhold som noget internt, der ikke er umiddelbar tilgængelig, hvorved det opstår en privatsfære. Når sfæren brydes ved blotlæggelse indtræder krænkelsen af privatlivsbeskyttelsen. Derimod indeholder definitionerne ikke en normativ grænseværdi for, hvornår der er indtrådt en krænkelse af privatsfæren, udover ved en manglende iagttagelse af individets selvbestemmelsesret. En blotlæggelse af privatsfæren kan være krænkende, men det er ikke entydigt normeret, hvornår det er en personoplysningskrænkelse.

Den aktuelle privatlivsbeskyttelse bør dog betragtes ud fra den teknologiske udvikling, der muliggør den elektroniske persondatabehandling. Problematikken er af Straffelovsrådet fremhævet som *”En krænkelse af privatlivets fred eller en persons ære vil (...) kunne udbredes hurtigere og til en større personkreds og dermed med en betydelig større*

²⁶ Betænkning 687/1973 om private registre, s. 28

²⁷ *Udsen*, Lærebog i informationsret, s. 62

²⁸ *Udsen*, Lærebog i informationsret, s. 60

²⁹ Betænkning 601/1971 om privatlivets fred, s. 40

skadevirkning for den krænkede end for blot få årtier siden.”.³⁰ Straffelovsrådet henviser til PDF’ præambelbetragtninger, hvori samme antagelse kan findes i nr. (6) ” Den hastige teknologiske udvikling og globaliseringen har skabt nye udfordringer, hvad angår beskyttelsen af personoplysninger. Omfanget af indsamlingen og delingen af personoplysninger er steget betydeligt.(...)”, samt nr. (7) ”Denne udvikling kræver en stærk og mere sammenhængende databeskyttelsesramme i Unionen (...). Fysiske personer bør have kontrol over deres personoplysninger. **Sikkerheden både retligt og praktisk** bør styrkes for fysiske personer, erhvervsdrivende og offentlige myndigheder.”[Fremhævet her]. Det fremhævede er udtryk for, at persondatasikkerheden i PDF art. 32, stk. 1 og 2 både retligt og faktisk er en forudsætning for reel beskyttelse af personoplysninger. Den skal sikre en privatlivsbeskyttelse, som er omgivet af en forståelseshorisont, der er forskellig fra den tidligere persondatalovgivning, hvor den informationsteknologiske udvikling ikke havde samme omfang. Den forståelse af situation skal medtages, når det informationelle privatliv fremadrettet skal dimensioneres gennem fortolkning. Privatlivssituationen er således en anden, end den var tidligere, fordi privatsfæren udsættes for en videre eksponering.

Det nødvendiggør en formålsbestemt fortolkning, når den retlige regulering omfatter privatlivsbeskyttelse ved elektronisk behandling af personoplysninger.³¹ På den måde kan PDF lovteknisk ved brug af teknologineutrale retsregler indeholdende brede definitioner, der skal underlægges en dynamisk formålsfortolkning være sit ansvar bevidst ved fremtidige informationsteknologier, eftersom den retlige regulering af behandlingssituationer både skal varetage privatliv og teknologi.

3.2. Integritetsbeskyttelse

Integritetsbeskyttelse har som et begreb hverken en legal eller almengyldig definition, selv om persondatalovgivningen anses for et integritetsværn.³² Det er således krænkelse af den personlige integritet, som er beskyttelsesinteressen. Den ubestemte kontur er fremhævet af Registerudvalget, der i mangel af bedre anførte, at en væsentlig bestanddel af begrebet kan defineres som ”Et krav om en retsbeskyttet adgang til at leve uden kontrol, indblanding eller overvågning på **alle områder**, hvor en sådan indblanding ikke er uskadelig eller pånøder sig af samfundsmæssige grunde.”[Fremhævet her].³³ Dermed er et væsentligt moment i

³⁰ Betænkning 1563/2017 om freds- og ærekrænkelser, s. 47

³¹ Tranberg, Nødvendig behandling af personoplysninger, s. 79

³² Udsen, Lærebog i informationsret, s. 302, Blume, Den nye persondataret, s. 48, Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, s. 92, Lind, Medarbejders integritetsbeskyttelse i dansk ret, s. 30

³³ Betænkning 687/1973 om private registre, s. 15

integritetsbeskyttelsen en udvidet privatsfære uden indblanding, medmindre en sådan indskrænkning har et rimeligt formål.

På baggrund af Registerudvalgets definition betragter *Lind* integritetsbeskyttelsen som værende udtryk for en ukrænket sfære i videre forstand end privatlivets fred, med den erkendelse, at der ikke er en bredere enighed om det sproglige eller juridiske indhold af den personlige integritet. Dermed omfatter privatlivsbeskyttelsen eksempelvis fortrolige tanker, egne livsytringer, adfærd alene eller sammen med andre, og skal afgrænses som en mindre del af integritetsbeskyttelsen, som derimod omfatter uønsket indgreb i liv, bevægelsesfrihed, retten til egen identitet og omdømme, samt heriblandt retten til privatlivets fred. *Lind* overvejer en anvendelse af et samlebegreb under betegnelsen den private integritet. Det angår en bred beskyttelse af individets privatsfære, hvor terminologien både omfatter de forskellige integritetsproblematikker og privatlivets fred.³⁴

I praksis anvender Datatilsynet integritets- og privatbeskyttelsen som to adskilte begreber, som dog kan indgå i samme skønsmæssige hensynsafvejning. Det fremgår af en afgørelse om tilladelse til behandling af personoplysninger ved førelse af en spærreliste over spærrede rejsekort. I sagen anføres det af tilsynet, at årsagen til den konkrete spærring af rejsekortet ikke må fremgå af spærrelisten var på grund af en afvejning af hensyn til kundens integritetsbeskyttelse og privatliv.³⁵ I en anden afgørelse om en kommunes tv-overvågning af skoler og daginstitutioner anføres det, at ifølge det grundlæggende princip i PDL § 5, stk. 3 (nu PDF art. 5, stk. 1, litra b) om formålsbegrænsning er den dataansvarliges behandling af oplysninger undergivet et proportionalitetsprincip. Dette princip fører til, at tv-overvågning skal gennemføres på en sådan måde, at den virker mindst muligt integritetskrænkende for den almindelige borger.³⁶ Da begreberne anvendes adskilt i praksis bør sondringen opretholdes af hensyn til en ensartet terminologi, på trods af den glidende overgang, fordi det kan skabe begrebsforvirring. Ud fra Datatilsynets afgørelsespraksis kan der udledes en støtte for, at integritets- og privatlivsbeskyttelse ved skønsmæssige hensynsafvejninger indgår som en beskyttelsesinteresse.

Der er således en prioriteret beskyttelsesinteresse af individets privatlivs- og integritetsbeskyttelse i persondataretten. De indeholder et retligt indhold, der kan anvendes, som retlig begrundelse for en bestemt retsfølge. Beskyttelsesinteresserne i PDF fungerer som en modvægt til andre hensyn fra pligtsubjekterne. Overordnet danner informations- og

³⁴ *Lind*, Medarbejders integritetsbeskyttelse i dansk ret, s. 15f

³⁵ J.nr. 2006-44-0051 (Advarselsregister hos Rejsekort A/S (I))

³⁶ J.nr. 2004-52-2442 (Kommunes tv-overvågning af skoler og daginstitutioner)

ytringsfrihedshensyn en modvægt, herunder konkrete hensyn til en effektiv forvaltning, kommercielle interesser og kriminalitetsbekæmpelse.³⁷ De modsatrettede hensyn taler således for en indskrænkning af persondatabeskyttelsen, samt hermed individets privatlivs- og integritetsbeskyttelse. Derfor skal hensynene afvejes over for hinanden for at opnå en rimelig regulering.

På baggrund af begrebsanalysen af integritets- og privatlivsbeskyttelse kan det konstateres, at der er et indholdsmæssigt sammenfald. Terminologien omfatter i begge begreber en retsbeskyttelse af privatsfæren. Det forudsætter en sfære, hvor individet kan forholde sig fortrolig uden indblanding. Dermed hænger den personlige integritet og privatlivets fred begrebsmæssigt sammen.³⁸ På trods af en præcisering af de væsentlige momenter, der indgår i begge begreber, forekommer afgrænsningen vag, hvilket gør definitionerne vanskeligt håndterbare. Derfor bør de anvendes med en vis forsigtighed, når der foretages en retlig kvalifikation af de faktiske omstændigheder, der henholdsvis er krænkende for den personlige integritet og privatlivets fred.

3.3. Teoretisk løsningsmodel:

Det kan tilsluttes, at integritetsbeskyttelsen består af et beskyttelseshensyn i bredere forstand end privatlivsbeskyttelsen, som det er anført af *Lind* og med *Udsen*' personlighedshensyn. Denne beskyttelse går videre i den forstand, at det kan angå beskyttelse af personoplysninger, der umiddelbart kan iagttages af den, der kommer i kontakt med den registrerede, hvilket bl.a. indebærer en retsbeskyttelse af egen identitet og omdømme.

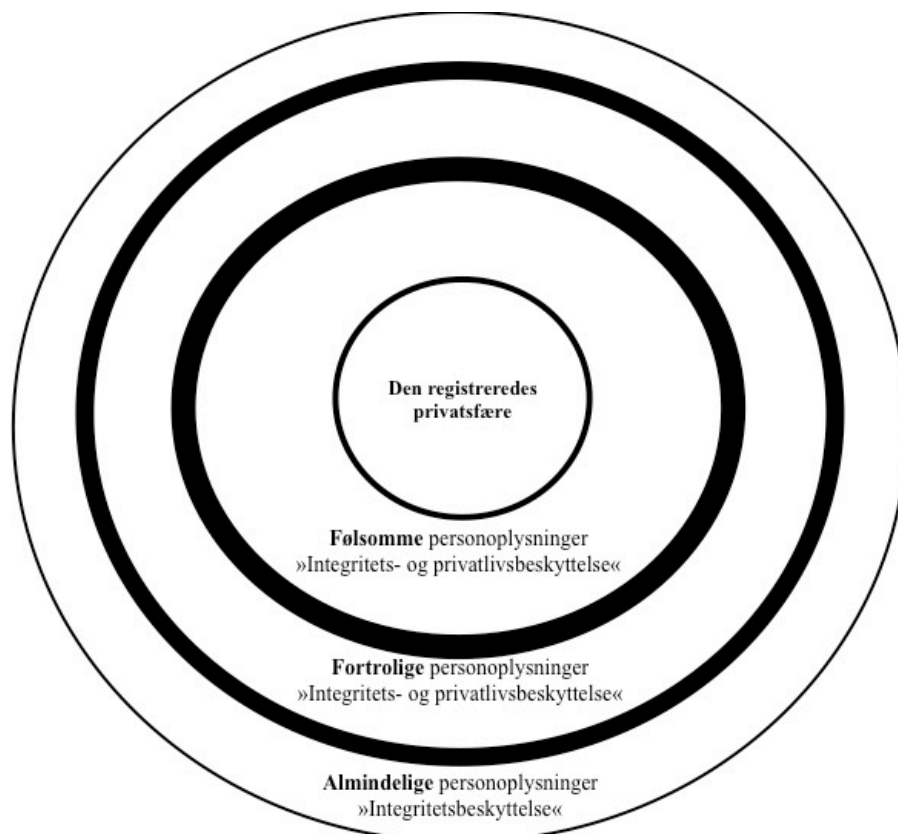
Fremstillingsmæssigt kan standpunktet sammenfattes som en cirkelillustration, hvor omdrejningspunktet er den registreredes privatsfære.³⁹ De omkredsende cirkler demonstrerer den registreredes privatsfære. Det udgør tre ydre cirkler, hvor den 1. omfatter følsomme personoplysninger i PDF art. 9, stk. 1. Behandling af de personoplysninger kan være særligt krænkende for den personlige integritet og privatlivets fred. 2. cirkel ud fra den registreredes privatsfære omfatter fortrolige personoplysninger, som både kan være almindelige og følsomme personoplysninger. Ved en behandling af fortrolige personoplysninger skal der ligeledes prioriteres privatlivs- og integritetsbeskyttelse. Til sidst omfatter den 3. ydre cirkel fra privatsfæren almindelige personoplysninger. Det er alle personoplysninger, der ikke er fortrolige eller følsomme. Modsat de andre cirkler kan det forsigtigt antages, at de almindelige personoplysninger kun kan være integritetskrænkende, idet de vedrører forhold, der som

³⁷ *Udsen*, IT-ret, s. 300

³⁸ *Lind*, Medarbejderes integritetsbeskyttelse i dansk ret, s. 13

³⁹ *Lind*, Medarbejderes integritetsbeskyttelse i dansk ret, s. 21ff: Cirkelillustrationen er en forklaringsmodel, hvor teorien tager udgangspunkt i en sfæremodel.

udgangspunkt ikke er af privat karakter. De er således kun omfattet af den særligt udvidende integritetsbeskyttelse af den registrerede. Imidlertid forudsætter det alligevel en prioriteret beskyttelse af den personlige integritet, der dog er mindre integritetsfølsom, idet personoplysningerne er placeret i den yderste cirkel. Jo tættere en cirkel omkredser den registreredes privatsfære, jo mere skal integritets- og privatlivsbeskyttelsen prioriteres, hvorved det antages, at behandling af almindelige personoplysninger ikke nødvendigvis skal iagttage hensyn, der er privatlivsfremmende.⁴⁰



Ud fra cirkelillustrationen kan man beskrive persondataretlige retsstillinger, når der skal argumenteres for eller imod, at en behandling af personoplysninger er krænkende for den personlige integritet eller privatlivets fred. En behandling af helbredsoplysninger skal henføres i den 1. ydre cirkel, fordi hjemmelsgrundlaget skal findes i PDF art. 9, stk. 2, litra a-j). Det skønsmæssige udgangspunkt for en sådan behandling er, at den går tæt på den registreredes privatliv, hvilket er illustreret med cirkelns tætte sammenhæng med privatsfæren.

Svagheden ved at opdele prioriteringsgraden af integritets- og privatlivsbeskyttelsen i forhold til personoplysningskategorierne er som ovenfor nævnt af *Tranberg*, at den registreredes personlige præference er afgørende for, om en bestemt personoplysning anses for privat eller

⁴⁰ Indtræden i sfærecirklen vil altid forudsætte behandlingshjemmel.

offentlig. Derfor kan opdelingen ikke anses for almen gyldig, idet de registreredes følelser af, hvilke personoplysninger de anser for mest integritets- og privatlivsfølsomme kan variere. Teorien tager ligeledes ikke hensyn til hvordan personoplysningerne behandles. Forskellige behandlingssituationer kan være mere eller mindre integritets- og privatlivskrænkende f.eks. anses ekstern behandling i form videregivelse og samkøring almindeligvis for mere indgribende over for den registrerede end intern behandling ved indsamling.⁴¹ De indgribende behandlinger kan dog placeres tæt på privatsfæren i cirkelomslutningen, således det illustrerer, at integritets- og privatlivsbeskyttelsen intensiveres. Derudover er det vanskeligt at bedømme den registreredes forståelse af, hvordan behandlingen reelt foretages, samt hvilke konsekvenser det kan have for den pågældende, især i lyset af den informationsteknologiske udvikling. Det kan næppe forudsættes, at alle registrerede personer indeholder samme evner og ressourcer i forhold til forståelsen af de mangeartede integritets- og privatlivsproblematikker.

På trods af svaghederne ved cirkelillustrationen kan den fungere som et teoretisk udgangspunkt. Teorien har afsat i PDF' formål, hvor beskyttelsens subjekt (den registrerede) er omdrejningspunktet, hvorefter beskyttelsens objekt (personoplysninger) kan identificeres og placeres i forhold til, hvor tæt de forekommer på beskyttelsesinteressen (privatsfæren). Gradsopdelingen illustrerer i bred forstand, i hvilket omfang beskyttelsesinteresserne normativt skal prioriteres. Det kan være behjælpeligt ved, at begreberne »den personlige integritet« og »privatlivets fred« deskriptive karakter overføres til en normativ placering af, hvordan forholdene bør gradueres. Derefter kan man med udgangspunkt i begrebernes brede beskrivelse, fortolke lovgivningen på en måde, der afspejler hensynenes intensitet.

På den måde kan beskyttelsesinteresserne integreres, når den retlige løsning findes ved lovfortolkning og inddragelse af hensyn fra persondatarettens primære, sekundære og subsidære retskilder. De vil danne et retligt indhold, der kan anvendes som principper i den retlige argumentation. Ved beskrivelse af persondatasikkerhedsmæssige retsstillinger kan de indgå, idet de vil blive mødt med en modvægt fra modsatrettede hensyn. Ved overtrædelse af persondatasikkerheden i PDF art. 32 vil beskyttelsesinteresserne således have en vis styrke ved fastlæggelse af en efterfølgende kompenserende eller sanktionerende retsfølge. Med andre ord kan sfæreteorien fungere som målestok for opfyldelse af et persondataretligt retsfaktum f.eks. om der er iværksat et *passende sikkerhedsniveau* efter PDF art. 32, stk. 2, eller om en behandling af oplysninger er *proportionel* ifølge PDF art. 5, stk. 1, litra b) i forhold til beskyttelsesinteresserne. I medfør af cirkelillustrationen kan man således afveje,

⁴¹ Tranberg, m.fl., Internetretten (2017), s. 117

hvilken skønsmæssig intensitet fortolkningen af et retsfaktum, som udgangspunkt skal tillægges, når der foretages en behandling af personoplysningskategorien i 1. 2. eller 3. sfærecirkel.

3.4. Sammenfatning:

Det overordnede formål med PDF er en regulering mod misbrug af personoplysninger, hvorefter aktørerne kan behandle personoplysninger i et rimeligt omfang inden for lovgivningens rammer. Persondataretten er således en retsbeskyttelse af individets privatlivs- og integritetsbeskyttelse, når aktørerne behandler oplysninger om registrerede personer. Disse beskyttelsesinteresser fungerer som en modvægt til andre hensyn fra pligtsubjekterne.

Både integritets- og privatlivsbeskyttelsen angår retsbeskyttelse af den registreredes privatsfære. Begreberne har ingen almengyldig eller legal definition, derfor bør de anvendes med en vis forsigtighed, når der foretages en retlig kvalifikation af de faktiske omstændigheder, der henholdsvis er krænkende for den personlige integritet og privatlivets fred. Det teoretiske beskrivelsesproblem kan løses ved en cirkelillustration, hvori beskyttelsesinteresserne kan placeres normativ i forhold til personoplysningstyperne. På den måde kan sfæreteorien fungere som målestok for opfyldelse af et persondataretligt retsfaktum, når den retlige argumentation skal beskrive af retsstillingen.

4. Retsgrundlag:

Dette afsnit har til formål at beskrive og fortolke fremstillingens primære retsgrundlag. Der vil blive inddraget tidligere persondatalovgivning, som har til formål at skabe forforståelse af den fremadrettede lovhjemmel om persondatasikkerhed i PDF art. 32, stk. 1 og 2.

4.1. Registerlovene:

Det første retlige grundlag for persondatasikkerhed var i registerlovene. Sikkerhedsreglerne i registerlovene foreskrev ifølge LOMR § 12, stk. 1 og LPRG § 6, stk. 1, med ens ordlyd:

*”Der skal træffes de **fornødne sikkerhedsforanstaltninger** mod, at oplysningerne misbruges eller kommer til uvedkommendes kendskab.”* [Fremhævet her]

Opfyldelse af persondatasikkerheden forudsætter ud fra ordlyden en iværksættelse af sikkerhedsforanstaltninger, der skal anses for *”fornødne”* i forhold til en kompromittering af de behandlede personoplysninger. Da der ikke er udtømmende eksempler på fornødne sikkerhedsforanstaltninger, fastlægger LOMR § 12, stk. 1 og LPRG § 6, stk. 1 en retlig standard, hvori det materielle meningsindhold skal fastlægges ved en skønsafvejning.

Registerudvalget tog bl.a. hensyn til at formindske risikoen ved f.eks. driftsforstyrrelse.⁴² Dette er udtryk for en risikobaseret tilgang, der skal imødegå en sandsynlighed for, at noget uønsket sker i fremtiden, der kan medføre negative konsekvenser for persondatabeskyttelsen. Derfor må det antages, at opfyldelsen af det materielle indhold i registerlovenes sikkerhedsregler indeholdte et risikobaseret skøn.

4.2. Persondatadirektivet og persondataloven:

Ved implementeringen af PDD ved PDL blev persondatasikkerhedens anvendelsesområde udvidet, idet registerlovenes retsfaktum foreskrev kravet om persondatasikkerhed i en mere snæver og traditionel forstand.⁴³

PDD art. 17, stk. 1 har følgende ordlyd:

*”Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige skal iværksætte de **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, navnlig hvis behandlingen omfatter fremsendelser af **oplysninger i et net**, samt mod enhver anden form for ulovlig behandling.*

*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.”* [Fremhævet her]

De kompromitteringssituationer, der skal sikres imod i retsfaktum, er udvidet ifølge PDD art. 17, stk. 1, 1. led, hvor det præciseres, at navnlig fremsendelse af personoplysninger i et net påkræver persondatasikkerhed. Det er udtryk for, at internettet er et hensyn, der tillægges særlig vægt, men det indgår samtidig i en samlet skønsafvejning, hvorefter andre hensyn kan inddrages.

Ifølge PDD art. 17, stk. 1, 2. led er der et krav om et *”tilstrækkeligt sikkerhedsniveau”*. Det er betegnelsen for den skønsafvejning, der skal iværksættes ud fra en risikovurdering af behandlingen af personoplysningerne. Denne vurdering skal foretages på et forberedelsesstadium, således sikkerhedsforanstaltningerne gennemføres under udformningen og iværksættelsen af behandling.⁴⁴

⁴² Betænkning 767/1976 om offentlige registre, s. 167

⁴³ Betænkning 1345/1997 om behandling af personoplysninger, s. 323

⁴⁴ PDD præambel betragtning nr. 46

Implementeringsbestemmelsen PDL § 41, stk. 3 har følgende ordlyd:

*”Den dataansvarlige skal træffe de **fornødne tekniske og organisatoriske sikkerhedsforanstaltninger** mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.”*
[Fremhævet her]

Ordlyden i PDL § 41, stk. 3 er ikke identisk med PDD art. 17, stk. 1, men udvalget forudsætter, at de samme beskyttelsesinteresser og skønsafvejninger stadig er gældende betingelser. På trods af udvidelsen af ordlyden mente udvalget, at meningsindholdet i PDL § 41, stk. 3 svarede til sikkerhedsreglerne i registerlovene.⁴⁵ Retsanvenderen havde således ikke en forudsigelig ordlyd i PDL § 41, stk. 3 uden kendskab til den bagvedliggende PDD art. 17, stk. 1. Denne retssikkerhedsmæssige prognoseproblematik ophører ved ikrafttrædelsen af PDF, der vil fungere som eneste primær lov på retsområdet.

4.3. Persondataforordningen:

Med PDF' ikrafttrædelse erstattes PDD art. 17, stk. 1 og PDL § 41, stk. 3 med PDF art. 32, stk. 1 og 2. Lovreguleringen er en EU-retlig sekundær retsakt i form af forordning, hvorved den er almen gyldig, og lovteksten er den autoritære tekst for retstilstanden.

PDF art. 32, stk. 1 har følgende ordlyd:

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

PDF art. 32, stk. 1 regulerer gennemførsel af sikkerhedsforanstaltninger. Sammenlignet med ordlyden i registerlovene, PDD og PDL indeholder PDF art. 32, stk. 1 i vidt omfang samme betingelser. Det er bl.a. det aktuelle tekniske niveau og et omkostningshensyn, som kan legitimere gennemførsel af sikkerhedsforanstaltninger, der ikke er på det højeste udviklingsniveau, hvis de øvrige hensyn ikke vejer tungere.

⁴⁵ Betænkning 1345/1997 om behandling af personoplysninger, s. 496

PDF art. 32, stk. 2 har følgende ordlyd:

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

PDF art. 32, stk. 2 omhandler vurdering af sikkerhedsniveau. Ligesom PDD og PDL indebærer sikkerhedsbestemmelsen i PDF art. 32, stk. 2 en betingelse om iværksættelse af et sikkerhedsniveau inden for en retlig standard. I registerlovene var der ikke i ordlyden anvendt et begreb om sikkerhedsniveau som retningslinje for persondatasikkerheden. Det må dog antages, at skønnet i sikkerhedsreglerne LOMR § 12, stk. 1 og LPRG § 6, stk. 1 forudsatte et vist niveau, før der var tale om, at *”fornødne”* sikkerhedsforanstaltninger var gennemført.

Ud fra ordlyden indeholder PDF art. 32, stk. 1 og 2 i vidt omfang samme retsfaktum i form af begreber og beskyttelsesinteresser, som de tidligere lovgivninger. Udvalget tilkendegiver ligeledes, at sikkerhedsbestemmelsen i PDF art. 32, stk. 1 og 2 viderefører den gældende retstilstand, idet reglen fremstår med samme indholdsmæssige betydning.⁴⁶ Dermed er sikkerhedsreglen i PDF ligeledes en retlig standard, som opfyldes ved et risikobaseret skøn henført til den private og offentlige dataansvarlige og databehandler. Den skønsafvejning opfyldes ved risikobaserede overvejelser i en risikovurdering, der er normerende for, hvilke relevante sikkerhedsforanstaltninger som opfylder et afvejet sikkerhedsniveau.⁴⁷

Den retlige standard opfyldes ved, at der gennemføres relevante sikkerhedsforanstaltninger efter PDF art. 32, stk. 1, som modsvarer et afvejet sikkerhedsniveau ud fra en risikovurdering ifølge PDF art. 32, stk. 2. Derfor skal betingelserne forstås i sammenhæng, idet de er afhængige af hinanden. Det kan defineres som en begrebsmæssig cirkelslutning, hvor de to behandlingsforpligtelser er kumulative, idet den ene betingelse ikke kan skønnes at være passende iværksat, uden at den anden ligeledes er det.

Forarbejderne til PDL betragtede lovens retstilstand omkring persondatasikkerhed videreført fra registerlovene. Det medfører, at meningsindholdet af de videreførte begreber fra registerlovene kan anvendes som fortolkningsbidrag. Det aktuelle udvalg til PDF betragter retstilstanden videreført fra PDL. Derfor antages retstilstanden inden for persondatasikkerhed

⁴⁶ Betænkning 1565/2017 om Databeskyttelsesforordningen, s. 484

⁴⁷ Betænkning 1565/2017 om Databeskyttelsesforordningen, s. 485

ikke ændret siden registerlovene, fordi forarbejdernes fortolkning af retsgrundlaget i vidt omfang er videreført.

4.4. Sikkerhedsbekendtgørelsen:

Med hjemmel i bemyndigelsesbestemmelsen PDL § 41, stk. 5 er sikkerhedsbekendtgørelsen (SB) udstedt i medfør af sikkerhedsreglen PDL § 41, stk. 3.⁴⁸ Denne specificerer visse sikkerhedskrav, der skal gennemføres i den offentlige forvaltning.

Datatilsynet har tilkendegivet, at deres praksis forudsætter samme krav til persondatasikkerheden i den private sektor, som i den offentlige forvaltning, når omstændighederne er ensartede.⁴⁹ Derfor mener tilsynet, at de sikkerhedskrav, som fremgår af SB, i vidt omfang er gældende for den private sektor, på trods af at bekendtgørelsen er udstedt til den offentlige forvaltning. Den retstilstand kan forekomme tvivlsom, idet lovgiver kunne have udstedt en særskilt sikkerhedsbekendtgørelse for den private sektor.

Ifølge Datatilsynets praksis var SB § 14 daværende hjemmelsgrundlag for et minimumskrav om gennemførsel af obligatorisk kryptering af e-mails, der indeholdte fortrolige eller følsomme personoplysninger.

SB § 14 har følgende ordlyd:

*”Der må kun etableres eksterne **kommunikationsforbindelser**, hvis der træffes **særlige foranstaltninger** for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.”* [Fremhævet her]

En afsendt e-mail over internettet er en videregivelse i form af en transmission, der anvender en ”ekstern kommunikationsforbindelse”, hvorefter der skal træffes ”særlige” sikkerhedsforanstaltninger. Bestemmelsen lægger op til skønsafvejning ud fra de sikkerhedsrisici, der kan forekomme fra uvedkommendes adgang, fordi reglen ikke angiver en specificering eller udtømmende opregning af konkrete foranstaltninger. En sådan skønsafvejning er i tråd med den persondatasikkerhedsmæssige risikovurdering.

⁴⁸ Bekendtgørelse 2000-06-15 nr. 528 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning

⁴⁹ Datatilsynets årsberetning (2001), s. 68

På baggrund af SB har Datatilsynet udstedt en vejledning til sikkerhedsbekendtgørelsen (VSB), der udtrykker en opfattelse af det gældende meningsindhold i bekendtgørelsen.⁵⁰ Det er ikke en bindende retskilde, der hverken forpligter forvaltningen eller domstolene.⁵¹ Alligevel har vejledningens retningslinjer givet udslag i en administrativ praksis om et generelt krypteringskrav.

Det fremgår af VSB til SB § 14, at der ved ekstern datatransmission over internettet forudsættes følgende ”*transmission af fortrolige oplysninger, herunder personnummer, skal der som **minimum** foretages en kryptering.*” [Fremhævet her] og hvis ”*transmitterede oplysninger er af følsom karakter, skal der anvendes en stærk kryptering, baseret på en anerkendt algoritme.*”. Ifølge VSB er det Datatilsynets opfattelse, at SB § 14 påkræver kryptering som et minimumskrav ved ekstern transmission indeholdende fortrolige eller følsomme personoplysninger. Dette til trods for, at bekendtgørelsesreglens ordlyd indeholder en skønsafvejning, hvilket er i overensstemmelse med hjemmelsgrundlaget i PDL § 41, stk. 3 (nu PDF art. 32, stk. 1 og 2).

Med ikrafttrædelsen af PDF art. 32 ophæves bemyndigelsesbestemmelsen i PDL § 41, stk. 5, der har gjort udgjort hjemmelsgrundlaget for SB i medfør af PDL art. 41, stk. 3.⁵² Derfor ophæves SB ligeledes, hvorefter hjemmelsgrundlaget for persondatasikkerhed alene er PDF art. 32. Det er således ikke længere muligt, at den nationale lovgiver fastlægger en nærmere regulering af sikkerhedskrav i bekendtgørelsesform. *Tranberg* antager, at en række af sikkerhedsreglerne i SB formentlig kan videreføres med hjemmel i PDF art. 32, stk. 1 og 2, fordi retsreglen er mere detaljeret end PDL art. 41, stk. 3.⁵³ Det understøttes af forarbejderne til PDF, hvor det anføres af udvalget, at retstilstanden i vidt omfang videreføres, hvilket ligeledes må omfatte sikkerhedskravene fra SB.⁵⁴

4.5. Sammenfatning:

Det kan udledes, at sikkerhedsreglerne i registerlovene, PDD, PDL og i den fremadrettede lovhjemmel PDF art. 32, stk. 1 og 2 ud fra en ordlydsfortolkning indeholder en skønsafvejning i form af en risikovurdering. Det er en behandlingsforpligtelse, hvor den dataansvarlige og databehandleren skal foretage en risikobaseret skønsafvejning af de sikkerhedsrisici, der relaterer sig til en behandling af personoplysninger. Der er tale om en

⁵⁰ Vejledning nr. 37 af 2. april 2001 til bekendtgørelse nr. 528 af 15. juli 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning

⁵¹ *Munk-Hansen*, Retsvidenskabsteori, s. 339

⁵² Betænkning 1565/2017 om Databeskyttelsesforordningen, s. 484

⁵³ *Tranberg*, m.fl., Internetretten (2017), s. 136

⁵⁴ Betænkning 1565/2017 om Databeskyttelsesforordningen, s. 484

begrebsmæssig cirkelslutning, hvor behandlingsforpligtelserne er kumulative, idet gennemførte sikkerhedsforanstaltninger kun kan anses for passende, når det skønsmæssige sikkerhedsniveau er passende.

5. Grundlæggende princip:

Dette afsnit vil fastlægge den retstilling, der kan udledes af, at persondatasikkerhed ved ikrafttrædelsen af PDF bliver et grundlæggende princip i lovgivningen.

I PDF art. 5 er der fastsat grundlæggende principper for enhver behandling af personoplysninger. De skal ses i sammenhæng med behandlingsreglerne PDF art. §§ 6-11, der anvendes som behandlingsgrundlag, idet der altid skal være et retligt grundlag for en behandling af personoplysninger.

De grundlæggende principper i PDF art. 5 regulerer, hvorvidt en behandling *kan eller må* foretages.⁵⁵ Principperne afgiver ikke et selvstændigt behandlingsgrundlag. En sådan hjemmel skal findes i de øvrige behandlingsregler PDF art. 6-11. Når der foreligger et behandlingsgrundlag, skal de grundlæggende principper i PDF 5, stk. 1, litra a-f) og stk. 2 altid iagttages.⁵⁶ En manglende iagttagelse kan medføre, at en behandling af personoplysninger har et behandlingsgrundlag, der er i overensstemmelse med de øvrige behandlingsregler, men ende med at være ulovlig, fordi de grundlæggende principper ikke er overholdt.⁵⁷ Sikkerhedsreglen i PDF art. 32, stk. 1 og 2 indtræder, når der er fastlagt et behandlingsgrundlag. Derfor er persondatasikkerheden en behandlingsforpligtelse, som regulerer hvordan en behandling af personoplysninger efterfølgende *skal* foretages.

Ansaret for overholdelsen af de grundlæggende principper er pålagt den dataansvarlige efter det grundlæggende princip om »ansvarlighed« i PDF art. 5, stk. 2. Det er betinget af et dokumentationskrav, hvor det skal være påviseligt, at PDF i sin helhed er overholdt. Dermed bærer den dataansvarlige bevisbyrden for, at behandlingen af personoplysningerne er legitim.

Det grundlæggende princip »integritet og fortrolighed« i PDF art. 5, litra f) er en nyskabelse i det persondataretlige retsområde, fordi persondatasikkerhed bliver et grundlæggende princip. Begreberne »integritet« og »fortrolighed«, der fremgår af princippet overskrift, er ligeledes anvendt inden for informationssikkerhedsstandard ISO 27001, som fastlægger krav til et dækkende informationssikkerheds-ledelsessystem, hvori principperne skal følges af alle

⁵⁵ Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, s. 190

⁵⁶ Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, s. 192

⁵⁷ Tranberg, m.fl., Internetretten (2017), s. 118

statslige og offentlige myndigheder.⁵⁸ De indgår ligeledes i ISO/IEC DIS 29134 *”Information technology – Security techniques – Privacy impact assessment – Guidelines”*. Det er internationale standarder, som er udarbejdet af den internationale standardiseringsorganisation.⁵⁹ ISO 29134 fastlægger, hvordan persondatasikkerhed skal iagttages og indarbejdes i IT-løsninger. Udvalget antager, at de europæiske tilsynsmyndigheder og Databeskyttelsesrådet, der er efterfølgeren af Artikel 29-gruppen, vil tage ISO 29134-standarden i betragtning, når meningsindholdet af forordningens bestemmelser om persondatasikkerhed skal fastlægges.⁶⁰ Det er udtryk for, at ISO-standarden bliver et fortolkningsbidrag, som en subsidær retskilde, idet Databeskyttelsesrådet formentlig i samme omfang som Artikel 29-gruppen vil få betydelig indflydelse på forståelsen af PDF ud fra deres vejledninger. Det kan understøttes af, at når den offentlige eller private sektor indretter sig efter den faglige standard, er det med hensigt på at overholde den lovbestemte persondatasikkerhed.

Personoplysninger skal ifølge PDF art. 5, stk. 1, litra f) *”behandles på en måde, der sikrer **tilstrækkelig** sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af **passende** tekniske eller organisatoriske foranstaltninger (»integritet og fortrolighed«)”. [Fremhævet her]*

Det er en retlig standard, hvor der alene skal være *”tilstrækkelig”* persondatasikkerhed ved anvendelse af *”passende”* sikkerhedsforanstaltninger. Derfor fastsætter det grundlæggende princip om persondatasikkerhed formentlig ikke yderligere sikkerhedskrav end efter PDF art. 32, stk. 1 og 2, fordi bestemmelsen indeholder samme begreber og beskyttelsesinteresser. Udvalget mener ikke, at det grundlæggende princip fastsætter selvstændige sikkerhedskrav til persondatasikkerheden, der ikke allerede følger af sikkerhedsreglen.⁶¹

Udvalget betragter PDF art. 5, stk. 1, litra f), som et signalværdi om, at persondatasikkerhed skal tillægges stor betydning i forbindelse med behandling af personoplysninger efter forordningen.⁶² Taget på ordet kan der ikke udledes en retsstilling fra det forhold, at den fremadrettede persondatasikkerhed får karakter af et betydeligt signalværdi. Til gengæld er et behandlingsgrundlag i almindelighed ikke legitimt, når den pågældende behandling ikke overholder de grundlæggende principper. Derfor kan det grundlæggende princip i PDF art. 5,

⁵⁸ Betænkning 1565/2017 om Databeskyttelsesforordningen, s. 486

⁵⁹ ISO, International Organization for Standardization

⁶⁰ Betænkning 1565/2017 om Databeskyttelsesforordningen, s. 486

⁶¹ Betænkning 1565/2017 om Databeskyttelsesforordningen, s. 100

⁶² Betænkning 1565/2017 om Databeskyttelsesforordningen, s. 101

litra f) medføre, at en behandling af personoplysninger under udformningen og inden iværksættelsen ikke kan gennemføres, fordi princippet ikke er overholdt. Det kan overvejes om udvalgets brug af terminologi er hensigtsmæssigt, da overtrædelse af de grundlæggende principper kan føre til, at behandlingen af personoplysningerne er ulovlig. Udvalget har imidlertid nok en interesse i at undgå, at deres formuleringer kan udlægges på en måde, der ikke svarer til retstilstanden i praksis.

Denne retstilling om de grundlæggende princippers forrang tog Datatilsynets stilling til i sag nr. 2014-632-0081 (Brug af fingeraftryk ved bloddonation). Den dataansvarlige havde et behandlingsgrundlag til at gøre brug af en biometrisk løsning for at kunne foretage en entydig identifikation af bloddonorer. Alligevel var den valgte behandling, som indebar personoplysninger i form af billeder af bloddonorernes fingeraftryk, betydeligt mere indgribende over for den registrerede, end hvad der kunne kræves til opfyldelse af formålet. Det var i strid med det grundlæggende proportionalitetsprincip i PDL § 5, stk. 3 (nu PDF art. 5, stk. 1, litra c), hvorefter behandlingsgrundlaget var retsstridigt.

Ifølge ovenstående vil det grundlæggende princip om persondatasikkerhed efter PDF art. 5, litra f) indebære, at et behandlingsgrundlag kan tilsidesættes, når persondatasikkerheden ikke er opfyldt. Derfor får persondatasikkerheden et større anvendelsesområde, fordi det skal tages i betragtning ved fastlæggelsen af ethvert behandlingsgrundlag i PDF art. 6-11. Baggrunden for udvalgets formodning om princippet signalværdi må antages at være på grund af, at reguleringsområdet for PDF art. 32, stk. 1 og 2 og PDF art. 5, litra f) anses for materielt sammenfaldende. Når de to bestemmelser systematisk indgår i forskellige kapitler i lovgivningen, samt har forskellige reguleringsformål, idet art. 5, litra f) fastlægger, om en behandling *kan og må* foretages, og PDF art. 32 regulerer, hvordan behandlingen efterfølgende *skal* foretages, kan de to bestemmelser på den baggrund ikke sidestilles med hinanden. Det er to lovregler, som regulerer hver sin retsstilling.

5.1. Sammenfatning:

Det grundlæggende princip om persondatasikkerhed i PDF art. 5, litra f) regulerer, om en behandling *kan eller må* foretages, hvorimod sikkerhedsreglen PDF art. 32, stk. 1 og 2 foreskriver, hvordan en behandling efterfølgende *skal* foretages. Den førstnævnte regulerer, om et behandlingsgrundlag er legitimt. Den sidstnævnte fastlægger, om en behandling opfylder sine behandlingsforpligtelser. Derfor er det to lovregler, der som udgangspunkt har hvert sit materielle indhold, som regulerer forskellige retsstillinger.

6. Pligtssubjekter:

Dette afsnit vil beskrive, hvilke pligtssubjekter der er underlagt krypteringskravet. Ifølge PDF art. 32, stk. 1 ”gennemfører den dataansvarlige og databehandleren” persondatasikkerhed. Med henblik på en forforståelse af behandlingsforpligtelsen vil følgende afsnit gennemgå, hvem der henholdsvis er dataansvarlig og databehandler.

6.1. Dataansvarlig:

Definitionen på en dataansvarlig fremgår af PDF art. 4, nr. 7). Bestemmelsen har identisk ordlyd med definitionen af dataansvarlige i PDD art. 2, litra. d) og PDL § 3, nr. 4), som er:

*”Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre **afgør**, til hvilket **formål** og med hvilke **hjælpemidler** der må foretages behandling af personoplysninger.”* [Fremhævet her]

Ud fra ordlyden er det afgørende, hvem der bestemmer ”formålet” og ”hjælpemidler”. Det er de kriterier, der definerer den dataansvarlige. Det medfører, at dataansvarlige har det umiddelbare ansvar for behandlingen og dispositionsretten over personoplysningerne.⁶³ De dataansvarlige har dataansvaret efter PDF art. 24, stk. 1, hvorved efterlevelsen af PDF skal påvises ved dokumentation i form af en behandlingsfortegnelse over behandlingsaktiviteterne ifølge PDF art. 30, stk. 1, litra a-g) og PDF art. 5, stk. 2. Ved iværksættelse af persondatasikkerhed vil det indebære, at sikkerhedsforanstaltninger og sikkerhedsniveau skal dokumenteres som værende gennemført ved en skønsafvejede risikovurdering, der kan anses for ”passende” ifølge PDF art. 30, stk. 1, litra g), jf. PDF art. 32, stk. 1 og 2.

Den dataansvarliges retspligt til iværksættelse af persondatasikkerhed har EU-domstolen fastslået i sag C-342/12, Worten. Domstolen udtalte, at sikkerhedsreglen PDD art. 17, stk. 1 (nu PDF art. 32) ikke selvstændigt forpligter medlemsstaterne til at iværksætte persondatasikkerhed, bortset fra de tilfælde, hvor de fungerer som dataansvarlig.⁶⁴ Derfor påhviler behandlingsforpligtelsen den, der kan defineres som dataansvarlig.

I Google Spain-sagen har EU-domstolen fastslået rækkevidden af definitionen på en dataansvarlige. Sagen omhandlede udbyderen af en søgemaskine, som blev anset for at være den dataansvarlige efter PDD art. 2, litra d). Det var udbyderen af søgemaskinen, der afgjorde formålet og hjælpemidlerne med den behandling, som den selv foretog.⁶⁵ Domstolen udtalte

⁶³ Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, s. 163

⁶⁴ Worten sag C-342/12, præmis nr. 25

⁶⁵ Google Spain sag C-131/12, præmis nr. 33

på baggrund af en ordlyds- og formålsfortolkning, at definitionsbestemmelsen skal *”sikre en effektiv og fuldstændig beskyttelse af de berørte personer ved at fastsætte en bred definition af begrebet »ansvarlig«*”.⁶⁶ Derfor skal dataansvaret pålægges en dataansvarlig ud fra en bred definition efter kriterierne om formål og hjælpemidler. Det er udtryk for et ønske om en vidtrækkende beskyttelse af de registreredes persondatabeskyttelse, idet definitionens anvendelsesområde skal fortolkes udvidende.

En dataansvarlig, der er forpligtet til at iværksætte persondatasikkerhed, kan f.eks. være en kommune⁶⁷, et universitet⁶⁸, en privat virksomhed⁶⁹ eller en offentlig myndighed⁷⁰, hvilket er i overensstemmelse med den brede definition.

6.2. Databehandler:

Definitionen på en databehandler fremgår af PDF art. 4, nr. 8), der har identisk ordlyd med PDD art. 2, litra e) og PDL § 3, nr. 5), som er:

*”Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges **vegne**.”* [Fremhævet her]

Det afgørende for definitionen på en databehandler er, at denne behandler oplysninger på den dataansvarliges *”vegne”*. Modsætningsvis fastlægger databehandleren ikke formålet med behandlingen, idet tilknytningen indebærer, at denne alene har sin rolle på baggrund af den dataansvarliges formål med behandlingen.

Den dataansvarlige skal efter PDF art. 28, stk. 1 udvælge en databehandler, der kan opfylde behandlingsreglerne og persondatasikkerheden, hvorefter en retlig bindende databehandleraftale vil regulere, hvilke aktiviteter databehandlere må foretage på den dataansvarliges vegne ifølge PDF art. 28, stk. 3, litra a-h). I relation til persondatasikkerhed skal databehandleraftalen navnlig fastlægge, at databehandleren selvstændigt er i stand til at iværksætte og bistå den dataansvarlige med persondatasikkerheden, jf. PDF art. 28, stk. 3, litra c) og litra f). Det indebærer bl.a. underretning af brud på persondatasikkerheden til Datatilsynet og de registrerede ifølge PDF art. 32, stk. 1 og art. 33, stk. 1.

⁶⁶ Google Spain sag C-131/12, præmis nr. 34

⁶⁷ J.nr. 2018-632-0225 (Kalundborg Kommunes brug af en FTP-server til personhenførbare oplysninger)

⁶⁸ J.nr. 2017-331-0667 (Uberettiget adgang til personnumre på studerende hos Det Sundhedsvidenskabelige Fakultet på Københavns Universitet)

⁶⁹ J.nr. 2017-631-0159 (Offentliggørelse af kontaktoplysninger på jobansøgere hos Novo Nordisk A/S)

⁷⁰ J.nr. 2016-632-0197 (Sikkerhed ved bestilling af en nye TastSelv-kode hos SKAT)

Hvis databehandleren foretager behandlinger, der ikke kan rummes inden for det formål, som følger af databehandleraftalen, vil databehandleren blive anset for dataansvarlig, fordi denne selv har fastlagt et nyt formål efter PDF art. 28, stk. 10. Dermed vil den pågældende behandling af personoplysninger blive ulovlig, fordi databehandleren foretager en behandling, der ikke sker på ”vegne” af den dataansvarliges fastsatte formål.⁷¹ Med andre ord er forholdet mellem de to retssubjekter reguleret ved den dataansvarliges instruktionsbeføjelse overfor databehandleren i form af en databehandleraftale.

Iværksættelse af persondatasikkerhed er en selvstændig retspligt, der er uafhængig af en databehandleraftale.⁷² Derfor skal databehandleren selvstændigt risikovurdere, om en anvendt sikkerhedsforanstaltning, f.eks. kryptering, er passende til at sikre et sikkerhedsniveau. Det indebærer, at de to pligtsubjekter er ligestillet ved opfyldning af det materielle indhold i PDF art. 32, stk. 1 og 2, uanset det over- og underforhold der følger af en databehandleraftale.

6.3. Sammenfatning:

Den dataansvarlige og databehandleren har et selvstændigt ansvar for at opfylde persondatasikkerheden, herunder krypteringskravet ifølge PDF art. 32, stk. 1 og 2.

Databehandleren kan således ikke alene forholde sig til de instrukser fra den dataansvarlige, der følger af databehandleraftalen, når det omhandler persondatasikkerhed. Derfor er de to pligtsubjekter ligestillet i en persondatasikkerhedsmæssig henseende.

7. Personoplysningsbegrebet:

Dette afsnit vil beskrive de personoplysninger, der er genstand for persondatasikkerhed. Krypteringskravet afgrænser fortrolige og følsomme over for almindelige personoplysninger. Derfor er det relevant for den juridiske for forståelse at fastlægge, hvordan personoplysningskategorierne defineres.

Definitionen på personoplysninger fremgår af PDF art. 4, nr. 1, der har identisk ordlyd med PDD art. 2, litra a) og PDL § 3, nr. 1), som er:

”»personoplysninger«: enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«)”

⁷¹ Tranberg, m.fl., Internetretten (2017), s. 117

⁷² Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, s. 549

Ud fra ordlyden omfatter definitionen enhver personhenførbare oplysning. Det omfatter oplysninger, der er direkte tilknyttet til en person, samt de oplysninger der er personidentificerbare. Der er et fysisk aspekt i definitionen, idet oplysningen skal angå én fysisk person, hvorefter oplysninger om juridiske personer ikke er omfattet.⁷³

Personoplysninger, der er genstand for persondatasikkerhed, kan f.eks. være oplysninger om personer, som abonnerer på meddelelser om jobstillinger,⁷⁴ over 700 CPR-numre,⁷⁵ personers egne e-mail-adresser eller telefonnumre⁷⁶. Den fremhævede praksis fastslår, at en oplysning er omfattet af sikkerhedsreglen, når de er personhenførbare.

Formålet med behandlingen af personoplysningerne er afgørende for kategoriseringen af, om det centrale er en behandling af følsomme, fortrolige eller almindelige personoplysninger. Det indebærer en konkret vurdering af behandlingssituationen, hvori formålet definerer personoplysningstypen. Der anvendes en systematik i forordningen, hvor de følsomme oplysninger negativt afgrænser de almindelige oplysninger.⁷⁷ Det er pålagt retssubjekterne, at foretage sondringen og identificere de forskellige personoplysningskategorier. Derfor er det afgørende at fastlægge, om en personoplysning er følsom, idet den modsætningsvis vil være almindelig.

Ifølge den udtømmende opregning i PDF art. 9, stk. 1 er personoplysninger følsomme, når det omhandler oplysninger omkring *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*. Personoplysninger, der ikke er defineret i PDF art. 9, stk. 1, er således almindelige, som har behandlingshjemmel i PDF art. 6.

I Datatilsynets administrative praksis om krypteringskravet anvendes en yderligere personoplysningskategori, der karakteriseres som »fortrolige«. De personoplysninger har ikke udtrykkelig hjemmel i PDF art. 6, stk. 1 om almindelige personoplysninger eller følsomme personoplysninger i art. 9. *Waaben* og *Nielsen* forudsætter, at fortrolige personoplysninger

⁷³ *Tranberg*, m.fl., Internetretten (2017), s. 112 og PDF præambel betragtning nr. 14

⁷⁴ J.nr. 2017-631-0159 (Offentliggørelse af kontaktoplysninger på jobansøgere hos Novo Nordisk A/S)

⁷⁵ J.nr. 2018-632-0225 (Kalundborg Kommunes brug af en FTP-server til personhenførbare oplysninger)

⁷⁶ J.nr. 2016-632-0197 (Sikkerhed ved bestilling af en nye TastSelv-kode hos SKAT)

⁷⁷ *Tranberg*, m.fl., Internetretten (2017), s. 113f

utvivlsomt omfatter de følsomme i PDF art. 9 samt de tidligere semi-følsomme personoplysninger i PDL § 8. De fortrolige personoplysninger afgrænses ved, om personoplysningen er af en sådan karakter, at den efter en almindelig opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab. Det skal forstås i overensstemmelse med sontringerne i Straffelovens § 152, stk. 3, hvor en oplysning kan være lovbestemt fortrolig eller nødvendig at hemmeligholde i forhold til væsentlige offentlige eller private interesser, og Forvaltningslovens § 27, stk. 1-4 der angiver de hensyn og tilfælde, hvor en oplysning er fortrolig og undergivet tavshedspligt. Hvis der ikke kan nægtes aktindsigt i personoplysningerne efter Offentlighedsloven, vil de ikke være af fortrolig karakter.⁷⁸

Lovgivningsmæssigt hviler karakteriseringen af fortrolige oplysninger overordnet på et offentligretligt tavshedshensyn overfor uvedkommende, der påkræver et beskyttelsesbehov. Derimod skal den private sektor ligeledes iagttage den fortrolige personoplysningskategori, fordi kategorien persondataretligt ikke sondrer mellem offentlige og private dataansvarlige og databehandlere. I den tidligere persondatalovgivning var der specificeret fortrolige personoplysninger efter PDL § 43, stk. 1 om undtagelse fra anmeldelsespligten af visse behandlinger, som blev foretaget for den offentlige forvaltning, hvilket omhandlede ikke-fortrolige personoplysninger. Med hjemmel i bemyndigelsesbestemmelsen PDL § 44, stk. 2 blev der udstedt en Anmeldelsesbekendtgørelse, hvori der fremgik specificerede fortrolige personoplysninger fra forskellige behandlingstyper, der ligeledes blev undtaget fra anmeldelsespligten.⁷⁹ De personoplysningstyper fremgår blandt andre af skemaerne i *Bilag 1* og *2*, hvilket er resultatet af en fortrolighedsvurdering, som indebærer en sontring mellem private og økonomiske forhold.⁸⁰ Fortrolighedsvurderingen indebærer en toleddet vurdering af personoplysningens karakter sammenholdt med den sammenhæng, hvori personoplysningen indgår, hvorefter en samlet vurdering af, om personoplysningen er af en sådan art, at den efter en almindelig opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab, kan statuere en personoplysning som fortrolig. I vurderingen kan bl.a. indgå den potentielle skadevirkning fra en udbredelse ved kompromittering, såsom repressalier og nærliggende risiko for økonomiske tab. Derudover kan en sammenkædning mellem offentligt og ikke-offentligt tilgængelige personoplysninger statuere en fortrolig personoplysning f.eks. en bopælsadresse til et fængsel eller psykiatrisk hospital. Det er

⁷⁸ *Waaben og Nielsen*, Lov om behandling af personoplysninger med kommentarer, s. 578f

⁷⁹ Bekendtgørelse 2000-06-15 nr. 529 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning

⁸⁰ Se afsnit 15 side 59-60 bilag 1 og bilag 2

således en retlig standard med betydelige skønselementer, som ændrer sig i takt med opfattelsen af fortrolighedsbegrebet i samfundet.⁸¹

Spørgsmålet er, om fortrolighedsvurderingen i sig selv har et tilstrækkeligt hjemmelsgrundlag til at gennemføre et retskrav i praksis, når det vedrører en personoplysningskategori, der ikke er lovreguleret i det fremadrettede hjemmelsgrundlag. Især i medfør af, at krypteringskravet får en uoverskuelig karakter ved den fortrolighedsvurdering, som den dataansvarlige og databehandler skal foretage, når de behandler almindelige personoplysninger.

Hvis en e-mail indeholder forskellige personoplysningstyper, er det den mest sensitive, der fastlægger sikkerhedsniveauet.⁸² Det kan medføre, at personoplysningerne ud fra en umiddelbar vurdering anses for almindelige, når definitionen på fortrolige personoplysninger ikke indeholder en klar lovhjemmel. Det kan f.eks. være lånekvitteringer fra bogudlejning med lånerens navn, e-mailadresse og titlen på det bestilte materiale afsendt via e-mail, hvorefter personoplysningerne alligevel er fortrolige, som skal krypteres, når de transmitteres over det åbne internet.⁸³ Det indebærer en usikkerhed for den dataansvarlige og databehandleren, når de skal identificere og kategorisere en uspecificeret og abstrakt personoplysningskategori. Et minimumskrav om kryptering bør ud fra en retssikkerhedsmæssig betragtning indeholde en klarhed om fortrolighedsbegrebet i retsfaktum.

Ud fra *bilag 1* og *2* fremstår den toleddet vurdering med få undtagelser, som en mangeartede sammenslutning af enhver personoplysning, der angiver et væsentligt privat eller socialt problem af særlig følsom karakter inden for private eller økonomiske forhold samt identifikationsoplysninger. Det er således en retsstilling, som vil berøre en stor del af den offentlige og private sektor. Den vil have en central betydning for integritets- og privatlivsbeskyttelse af den registrerede, hvis oplysninger er genstand for transmission via e-mail over internettet. Det nødvendiggør et tilstrækkeligt hjemmelsgrundlag i forhold til retssikkerheden for den dataansvarlige og databehandleren, men ligeledes for en klar retsbeskyttelse af den registrerede.

Ovennævnte konkrete vurdering medfører den usikre retsstilling, hvor visse almindelige personoplysning i PDF art. 6 kan være fortrolige personoplysninger. *Bønsing* anfører, at en konstatering af at visse almindelige personoplysninger kan være fortrolige ikke angiver en

⁸¹ *Fenger*, Forvaltningsloven med kommentarer, s. 689

⁸² Datatilsynets IT-sikkerhedstekst, *ST2*, side 2

⁸³ J.nr. 2004-082-0118 (Elektronisk reserverings- og kvitteringsmeddelelser fra bibliotekerne)

rettesnor for, hvornår det er tilfældet.⁸⁴ En målestok for hvornår en personoplysning kan kategoriseres som fortrolig, kan forsigtigt illustreres ved, at den fortrolige personoplysningskategori går halvt ind i den almindelige personoplysningskategori i PDF art. 6 af særligt private personoplysninger såsom interne familieforhold og ulykkestilfælde, der nærmer sig de konkrete følsomme personoplysninger i PDF art. 9, stk. 1, der utvivlsomt er fortrolige personoplysninger. Med andre ord forekommer tvivlstilfældet i forhold til fortrolighedsbegrebet som retsfaktum i krypteringskravet, når der videregives almindelige personoplysninger via e-mail.

7.1. Sammenfatning:

Personoplysningsbegrebet har en bred definition, der omfatter enhver personhenførbare oplysning. Krypteringskravet afgrænser mellem almindelige, fortrolige og følsomme personoplysninger, hvorefter de følsomme og fortrolige er underlagt retskravet. På baggrund af definitionen på fortrolige personoplysninger antages krypteringskravet at have et betydeligt anvendelsesområde, der medfører en usikker retsstilling, fordi fortrolige personoplysninger som en mellemkategori ikke har direkte lovhjemmel. Derfor vil der forekomme et større antal e-mails i den offentlige og private sektor, der skal krypteres for at honorere sikkerhedskravet i PDF art. 32, stk. 1, litra a) og stk. 2 ifølge Datatilsynets praksis. Da retskravet ud fra en konkret vurdering både tvivlsomt angår visse almindelige personoplysninger i PDF art. 6, stk. 1, og utvivlsomt angår følsomme personoplysninger i PDF art. 6, stk. 1.

8. Behandlingsbegrebet:

Dette afsnit vil beskrive behandlingsbegrebet, fordi det tilsvarende personoplysningsbegrebet har en central betydning for persondatasikkerhedens anvendelsesområde.

Ifølge PDF art. 32, stk. 1 skal de dataansvarlige og databehandleren gennemføre sikkerhedsforanstaltninger under hensyntagen til *”den pågældende behandlings karakter, omfang, sammenhæng og formål”*. Foranstaltningerne skal modsvare et sikkerhedsniveau, hvor der navnlig tages *”hensyn til de risici, som behandling udgør”* efter PDF art. 32, stk. 2. Behandlingsbegrebet medvirker til at normere, hvilken grad af persondatasikkerhed der skal iværksættes. Persondatasikkerheden er således kontekstbestemt ud fra behandlingsbegrebet.

Definitionen på behandling af personoplysninger fremgår af PDF art. 4, nr. 2, der i vidt omfang har samme ordlyd som definitionen i PDD art. 2, litra a) og PDL § 3, nr. 2), som er:

⁸⁴ Bønsing, Forvaltningsloven 25 år, Tavshedspligtsreglerne og persondataloven, s. 45

”»behandling«: enhver aktivitet eller række af aktiviteter — med eller uden brug af automatisk behandling — som personoplysninger eller en samling af personoplysninger gøres til genstand for”

Ud fra ordlyden samt de i reglens øvrige eksemplifikationer, som definitionen i PDF art. 4, nr. 2 indeholder, er behandlingsbegrebet en bred definition, idet eksemplifikationerne ikke er udtømmende.⁸⁵ Derfor er det en bred fortolkning af enhver aktivitet, der relaterer sig til en personoplysning.⁸⁶

Det fremgår bl.a. af definitionen, at ”*transmission*” er en behandling. Det er relevant for afsendelse af personoplysninger via e-mail, idet denne disposition udgør en behandling. Dermed er behandlingsbegrebet som retligt faktum i krypteringskravet opfyldt, når der afsendes en e-mail via internettet.

Den materielle afgrænsning af elektronisk behandling af personoplysninger har højesteret behandlet i U.2011.2343.H. Højesteret lagde vægt på, at personoplysningen fandtes i elektronisk form ved en mundtlig videregivelse via telefon, hvorefter den efterfølgende videregivelse ligeledes var omfattet af loven efter PDL § 1, stk. 1 (nu PDF art. 2, stk. 1). På baggrund af dommen ligger det fast, at en elektronisk registrering af en personoplysning medfører lovens anvendelse.⁸⁷ Det er bemærkelsesværdigt, at hverken byretten eller landsretten kommer frem til, at behandlingen »*helt eller delvis foretages ved hjælp af edb*«. Da EU-domstolen i *Lindqvist-sagen* før domsafsigelserne i U.2011.2343.H udtalte, at en operation, hvorved personoplysninger lægges ud på en internetside via en server ”*Disse operationer udføres i det mindste delvis ved hjælp af edb.*”[Fremhævet her].⁸⁸ Ud fra EU-Domstolens praksis er der tale om et bredt anvendelsesområde, eftersom en delvis anvendelse er tilstrækkeligt. Derfor vil enhver brug af et edb-teknisk middel til en behandling opfylde PDF art. 2, stk. 1, der i det mindste blot skal være delvis, selv om en efterfølgende behandling har karakter af at være manuel.

Til illustration af behandlingsbegrebets brede anvendelsesområde kan behandling af personoplysninger være en gennemgang eller læsning af en anden persons søgehistorik på en

⁸⁵ *Waaben og Nielsen*, Lov om behandling af personoplysninger med kommentarer, s. 146

⁸⁶ *Tranberg*, m.fl., *Internetretten* (2017), s. 117

⁸⁷ *Waaben og Nielsen*, Lov om behandling af personoplysninger med kommentarer, s. 146: ”Enhver tekstbehandling ved anvendelse af pc eller lignende, hvori der indgår personoplysninger (...) uanset hvor kortvarig behandlingen er.”

⁸⁸ C-101/01, *Lindqvist*, præmis nr. 26

pc eller tablet, uanset om betjeningen overtages. Dermed er alene læsningen en behandling.⁸⁹ Dette påviser, at behandlingsbegrebet kan anvendes bredt på alle tilfælde, hvor en aktivitet relaterer sig til en personoplysning.

De forskellige behandlingssituationer har forskellig karakter, idet nogen anses for mere indgribende end andre. Når den dataansvarlige videre giver eller samkører personoplysninger, hvor andre end den dataansvarlige får indblik i personoplysningerne, anses denne behandlingssituation for potentielt indgribende. Hvorimod indsamling, der alene sker til intern anvendelse, hvor udefrakommende ikke får indblik, anses for mindre indgribende.⁹⁰ Der er således en afgrænsning mellem ekstern og intern behandling i forhold til den potentielle krænkelse af den registreredes integritets- og privatlivsbeskyttelse. Da de forskellige typer af behandlinger ikke udgør samme sikkerhedsrisici, skal der i den skønsafvejede risikovurdering ifølge PDF art. 32, stk. 1 og 2 foretages en karakterisering af behandlingssituationen.

8.1. Sammenfatning:

Behandlingsbegrebets definition har et bredt anvendelsesområde. Begrebet normerer, hvilken grad af persondatasikkerhed der skal iværksættes ifølge PDF art. 32, stk. 1 og 2. En afsendt e-mail er en behandling af personoplysninger efter PDF art. 4, nr. 2). Det påkræver, at den dataansvarlige og databehandleren foretager en karakterisering af de sikkerhedsrisici, der relaterer sig til afsendelse af en e-mail over internettet.

9. Sikkerhedsniveau:

Dette afsnit har til formål at definere begrebet »sikkerhedsniveau«. Ud fra sikkerhedsbestemmelsens systematik er det nærliggende først at fastlægge reglens formål, der er et passende sikkerhedsniveau i PDF art. 32, stk. 2. Før det fastsættes, hvordan formålet opfyldes ved gennemførelse af sikkerhedsforanstaltninger i PDF art. 32, stk. 1, selvom foranstaltningerne lovteknisk er foreskrevet før formålet.

EU-lovgiver har i forbindelse med begrebet »sikkerhedsniveau« indsat udtrykket »passende«. Ud fra en ordlydsfortolkning skal begrebet forstås som et sikkerhedsniveau, der skal være af et omfang, som er tilstrækkeligt til, at det opfylder et påkrævet behov. Dette omfang er en lovreguleret retlig standard, der alene foreskriver hvilke formål, hensyn og relevante foranstaltninger, der kan opfylde bestemmelsen. Normeringen af den retlige standard i sikkerhedsniveauet sker ved en skønsafvejede risikovurdering, der skal vurdere

⁸⁹ J.nr. 2016-216-0569 (Kritik af skoles gennemgang af elevers søgehistorik)

⁹⁰ *Tranberg, m.fl., Internetretten (2017), s. 117*

sandsynligheden for uønsket sikkerhedsbrud, samt de konsekvenser der herefter kan forekomme. Det antages ikke, at risikovurderingen omfatter hver enkelt singulære behandling af personoplysning. Den angår hvert generelle oplæg for behandling, hvilket vil være enhver databaseløsning eller beslutningssystem, hvori der forekommer et behandlingsgrundlag.⁹¹

Når lovgiver anvender en retlig standard ved regulering af persondatasikkerhed, må det antages at være udtryk for, at et absolut værn mod kompromittering ved behandling af personoplysninger ikke er muligt. En retlig standard er især hensigtsmæssig, såfremt reglen tilstræber at regulere brugen af teknologi, som påvirkes af den teknologiske udvikling.⁹² Der henvises i PDF art. 32, stk. 1 til, at der kan tages hensyn til ”det aktuelle tekniske niveau”, som relaterer til udviklingen inden for systemtekniske sikkerhedsforanstaltninger. Dermed kan sikkerhedsniveauets følge den informationsteknologiske udvikling.

Sikkerhedsniveauets risikovurdering i PDF art. 32, stk. 2 skal ud fra behandlingen af personoplysningernes karakter fastlægge et niveau, der opfylder sikkerhedsmålene *tilgængelighed, fortrolighed og integritet*. Hensynene findes reguleret i PDF art. 32, stk. 1, litra b) og c) om evnen til at sikre en vedvarende fortrolighed, integritet, tilgængelighed og robusthed samt rettidigt at genoprette tilgængeligheden. *Tilgængelighed* er udtryk for, at personoplysninger er tilgængelige ved anmodning fra autoriserede personer.⁹³ De retsmæssige personer skal have rettidig adgang til personoplysninger, der skal behandles. Sikkerhedsniveauet skal ligeledes sikre, at de personoplysninger, der indgår i en behandling, er korrekte, dvs. *integritet*, samt at de kun må være tilgængelige for retmæssige personer, dvs. *fortrolige*.⁹⁴

Formålet med fastsættelse af et ”*passende*” sikkerhedsniveau er en sikring mod brud på persondatasikkerheden. Derfor fremgår de samme hensyn i PDF art. 32, stk. 2 også i PDF art. 4, nr. 4 om definitionen på »brud på persondatasikkerheden«, hvorefter sikkerhedsniveauet skal fastsættes ud fra de kompromitteringssituationer, der skal søges at undgås, idet dette vil statuere et brud på persondatasikkerheden. Det indebærer, at sikkerhedsniveauet skal sikre mod brud ved ”*hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet*”. De hensyn, der er foreskrevet i PDF art. 32, stk. 2, angiver hvilke hensyn, der ”*navnlig*” skal indgå, hvorved det ikke er en udtømmende opregning. Bestemmelsen fremstår

⁹¹ Schartum, m.fl., Informationsikkerhet, s. 117

⁹² Blume, Retssystemet og juridisk metode, s.161

⁹³ Betænkning 1565/2017 om Databeskyttelsesforordningen, s. 482

⁹⁴ Betænkning 1565/2017 om Databeskyttelsesforordningen, s. 481

dermed alene som en vejledning angående de sikkerhedsrisici, der især skal tages hensyn til, når et ”*passende*” sikkerhedsniveau skal gennemføres ved sikkerhedsforanstaltninger efter PDF art. 32, stk. 1.⁹⁵ Derfor skal alle relevante sikkerhedsrisici inddrages.

På baggrund af definitionerne og formålet skal sikkerhedsniveauet i relation til krypteringskravet fastlægges ud fra de sikkerhedsrisici, der potentielt kan forekomme ved en ekstern transmission via e-mail, således at en kompromittering ved et sikkerhedsbrud imødegås i medfør af PDF art. 32, stk. 2, jf. PDF art. 4, nr. 4. Sikkerhedsreglen er imidlertid en retlig standard, som er et lovgivningsideal om, at behandling af personoplysninger er sikret ved persondatasikkerhed med et passende sikkerhedsniveau. Det er alene abstrakte begreber, hvor det er overladt til retsudøveren i praksis at fastlægge meningsindholdet i lovreglen.⁹⁶ I den henseende har Datatilsynet ved en fortolkning af PDL § 41, stk. 3 og SB § 14 fastlagt et generelt krypteringskrav, som fremadrettet får hjemmel i PDF art. 32, stk. 1, litra a) og stk. 2. På den måde er den dataansvarlige og databehandleren indskrænket i deres risikovurdering af e-mails sendt over internettet, selv om sikkerhedsniveauet lægger på til en skønsmæssig hensynsafvejning i hvert konkrete tilfælde.

9.1. Sikkerhedsniveauets øvre og nedre grænse:

Følgende afsnit vil fastlægge rækkevidden af behandlingsforpligtelsen. Da det er en retlig standard, skal meningsindholdet fastlægges ved en fortolkning af praksis.

For det første vil det blive fastlagt, om der er tilfælde, hvor en skønsmæssig risikovurdering af sikkerhedsniveauet efter PDF art. 32, stk. 2 vil føre til, at der ikke skal iværksættes persondatasikkerhed. Med andre ord om behandlingsforpligtelsen har en nedre grænse.

I Datatilsynets sag nr. 2018-632-0225 (Kalundborg Kommunes brug af en FTP-server til personhenførbare oplysninger) har tilsynet vurderet udstrækningen af forpligtelsen i sikkerhedsreglen PDL § 41, stk. 3. Tilsynet udtalte generelt, at ”§ 41, stk. 3, indeholder en forpligtelse for den dataansvarlige til at beskytte såvel følsomme oplysninger som fortrolige og ikke-følsomme oplysninger”. Udtalelsen må udledes som et generelt princip om, at enhver behandling af personoplysninger skal være underlagt et sikkerhedsniveau, fordi forpligtelsen omfatter alle personoplysningskategorier. Der foreligger således ikke en nedre grænse for, hvornår der skal iværksættes et sikkerhedsniveau, idet alle personoplysningstyper er omfattet. I visse behandlingssituationer kan risikoen for sikkerhedsbrud forekomme minimal, f.eks. ved behandling af almindelige personoplysninger efter PDF art. 6, stk. 1, litra a-f), såsom en

⁹⁵ Betænkning 1565/2017 om Databeskyttelsesforordningen, s. 483

⁹⁶ Munk-Hansen, Retsvidenskabsteori, s. 276

fysisk persons navn og adresse, men det kan ikke fravige forpligtelsen til at iværksætte persondatasikkerhed.

På baggrund af det generelle princip om, at enhver persondatabehandling medfører en behandlingsforpligtelse til at iværksætte et sikkerhedsniveau, skal det fastlægges, om denne brede retspligt har en øvre grænse. Hermed menes, om den dataansvarlige eller databehandleren kan iværksætte et sikkerhedsniveau, der går ud over, hvad behandlingsforpligtelsen tilsigter i sit skøn.

Datatilsynet har i klagesag nr. 2002-215-0094 (Opbevaring af sikkerhedskopier af e-post) taget stilling til den øvre grænse for sikkerhedsniveauet. En dataansvarlig e-postserviceudbyder havde gennemført en teknisk sikkerhedsforanstaltning, der sørgede for arkivering og sikkerhedskopiering af programmer og data fra driftssystemerne i tilfælde af nedbrud, hvor den registreredes e-post blev sikkerhedskopieret og arkiveret på en server i et år. Datatilsynet fastslog, at opbevaringen på et år var langt ud over, hvad en almindelig bruger må formodes at forvente. Derefter udtalte Datatilsynet *”opbevaring hos udbyderen af sikkerhedskopier af slettet e-post i en så lang periode ikke kunne antages at følge af udbyderens forpligtelser efter persondatalovens § 41, stk. 3”*.⁹⁷ Der er således en øvre grænse for et sikkerhedsniveau, som ikke må iværksættes højere, end det retlige skøn kan anse for passende.

En sådan øvre grænse for sikkerhedsniveauet er i overensstemmelse med, at risikovurderingen altid er en skønsafvejning, der skal ende med en passende vurdering. Det er ikke en bestemt grænse, men der er en skønsmæssig øvre grænse. I den ovennævnte klagesag nr. 2002-215-0094 (Opbevaring af sikkerhedskopier af e-post) blev opbevaringsperioden af sikkerhedskopierne nedsat til 3 måneder tillagt mulighed for 14 dages forlængelse. Det er således Datatilsynets udtryk for en efterfølgende korrekt skønsafvejning i risikovurderingen, der har resulteret i et passende sikkerhedsniveau. Den øvre grænse antages at medføre, at kryptering af e-mails indeholdende almindelige personoplysninger, som ikke er fortrolige, vil indebære et for højt sikkerhedsniveau. En sådan sikkerhedsforanstaltning kan ikke anses at følge af den dataansvarliges eller databehandlerens behandlingsforpligtelse efter PDF art. 32, stk. 1 og 2.

⁹⁷ Datatilsynets årsberetning (2003), s. 113-114

9.2. Samtykke og sikkerhedsniveau:

Afsnittet vil undersøge om sikkerhedsniveauet kan fraviges, hvis den registrerede, ikke ønsker persondatasikkerhed omkring sine personoplysninger. Dermed om et samtykke fra den registrerede kan legitimere et lavere eller intet sikkerhedsniveau.

Datatilsynets har tilkendegivet, at persondatasikkerheden er en præceptiv behandlingsforpligtelse.⁹⁸ Derfor kan den registrerede ikke efter behandlingsreglerne om samtykke i PDF art. 6, stk. 1, litra a) om almindelige personoplysninger eller PDF art. 9, stk. 2, litra a) om følsomme personoplysninger samtykke til et lavere eller fravær af et sikkerhedsniveau.

Blume tilslutter sig Datatilsynets opfattelse, fordi der tilknytter sig visse behandlingsforpligtelser til en behandling af personoplysninger, herunder persondatasikkerhed, der ikke kan fraviges, selv om den registrerede har givet sit samtykke.⁹⁹ *Svanberg* er af samme opfattelse, idet han mener, at opfyldelsen af behandlingsreglerne ved et eventuelt samtykke er en forudsætning for, at sikkerhedsreglen er relevant. Dertil vil det undergrave sikkerhedsreglerne i praksis, hvis en dataansvarlig eller databehandler ved et samtykkekrav kan legitimere, at de ikke behøver at efterleve sikkerhedsreglerne.¹⁰⁰ Det er således et omgåelseshensyn, der er forfatterens standpunkt for en indskrænkning af den registreredes selvbestemmelsesret ved samtykke.

Spørgsmålet er, om den registrerede selv skal være rådig over, hvorvidt de behandlingsforpligtelser, der fremgår af lovgivningen, skal aktiveres.

Andersen og *Udsen* er af modsat holdning, fordi den registrerede kan samtykke til, om personoplysninger *må* behandles ifølge PDF art. 6, stk. 1, litra a) og PDF art. 9, stk. 2, litra a). Hvorefter det bør følge logisk, at samme samtykke ligeledes kan legitimere, *hvordan* de skal behandles.¹⁰¹ Forfatterne mener, at det er uhensigtsmæssigt, at et samtykke bl.a. kan legitimere en offentliggørelse af personoplysninger, men ikke til en fravigelse af sikkerhedskrav, der skal sikre de samme personoplysninger mod offentliggørelse.¹⁰² Den opfattelse er *Scartum* enig i, idet et frivilligt samtykke fra den registrerede til offentliggørelse

⁹⁸ Datatilsynets årsberetning (2005), s. 70

⁹⁹ *Blume*, Den nye persondataret – Persondataforordningen, s. 64

¹⁰⁰ *Svanberg*, U.2006B.43, "Samtykke og datasikkerhed", s. 2

¹⁰¹ *Andersen* og *Udsen*, U.2005B.378, "Krav om kryptering af e-mails med fortroligt indhold?", s. 3

¹⁰² *Andersen* og *Udsen*, U.2006B.110, "Kryptering af e-mails og persondatalovens § 41, stk. 3 - en replik", s. 2

af personens oplysninger vil være et undtagelsestilfælde, hvor der ikke er behov for fortrolighedsbeskyttelse gennem persondatasikkerhed.¹⁰³

Ud fra en formålsfortolkning er persondatasikkerheden i PDF art. 32 en præceptiv behandlingsforpligtelse, hvorimod et samtykke i PDF art. 6, stk. 1, litra a) og PDF art. 9, stk. 2, litra a) er et frivilligt behandlingsgrundlag blandt andre. Behandlingsgrundlaget ved samtykke er foreskrevet i PDF kapitel 2 med overskriften ”Principper”, som har til formål at regulere, hvorvidt en behandling *kan eller må* foretages.¹⁰⁴ Sikkerhedsreglen er placeret i PDF kapitel 4 med overskriften ”Dataansvarlige og databehandlere”, hvilket tilkendegiver, at reglerne heri har til formål at regulere forpligtelser rettet mod de to pligtsubjekter.

Persondatasikkerheden regulerer en behandlingsforpligtelse, som indtræder, når der er fastlagt et behandlingsgrundlag efter behandlingsreglerne i PDF kapitel 2 f.eks. ved et samtykke. Behandlingsforpligtelsen regulerer, hvorledes en behandling af personoplysninger efterfølgende *skal* foretages. Det er en præceptiv behandlingsforpligtelse uden en nedre grænse, derfor er enhver personoplysningstype der behandles genstand for persondatasikkerheden.¹⁰⁵ Det understøttes af, at EU-domstolen ved fortolkning af PDD generelt har udtalt ”*at en generel undtagelse fra at anvende direktivet for så vidt angår offentliggjorte oplysninger i vid udstrækning vil gøre direktivet indholdsløst*”.¹⁰⁶ Dermed nyder offentliggjorte personoplysninger beskyttelse, samt de behandlingsforpligtelser der relaterer sig hertil bl.a. persondatasikkerhed. På baggrund af det ovennævnte kan den registrerede, der frivilligt samtykker til offentliggørelse af sine personoplysninger eller fravigelse af sikkerhedsniveau ved behandling af sine personoplysninger, ikke legitimere, at den dataansvarlige eller databehandleren ikke skal opfylde deres retspligt til at iværksætte persondatasikkerhed efter PDF art. 32, stk. 1 og 2.

I relation til krypteringskravet kan den registrerede således ikke samtykke til, at den dataansvarlige eller databehandler, der er afsender af en e-mail, ikke skal gennemføre kryptering. Det er en gældende retspligt, uanset om de fortrolige eller følsomme personoplysninger, der afsendes, allerede er offentliggjort. Derfor kan Datatilsynets praksis om kryptering, som et minimumskrav ikke fraviges, idet hjemmelsgrundlaget er præceptivt.

¹⁰³ Schartum, m.fl., Informationsikkerhet, s. 129

¹⁰⁴ Waaben og Nielsen, Lov om behandling af personoplysninger med kommentarer, s. 190

¹⁰⁵ Jf. J.nr. 2018-632-0225 (Kalundborg Kommunes brug af en FTP-server til personhenførbare oplysninger)

¹⁰⁶ Google Spain sag C-131/12, præmis nr. 30

9.3. Sammenfatning:

Begrebet »sikkerhedsniveau« fastlægger formålet med PDF art. 32, stk. 1 og 2, hvorved behandling af personoplysninger skal sikres ved persondatasikkerhed med et passende sikkerhedsniveau. Bestemmelsens retlig standard opfyldes ved en skønsafvejning i form af en risikovurdering af de sikkerhedsrisici, der relaterer sig til en behandling af personoplysninger. Datatilsynet har som retsudøver udfyldt sikkerhedsniveauets retlige standard med en fortolkning, der har medført, at der som minimum skal foretages kryptering af eksterne transmissioner via e-mail indeholdende fortrolige og følsomme personoplysninger.

Persondatasikkerhed er en præceptiv behandlingsforpligtelse, der ikke kan fraviges ved den registreredes samtykke. Begrebet indeholder ikke en nedre grænse, hvilket medfører, at enhver behandling af personoplysninger uanset oplysningens format skal være underlagt et sikkerhedsniveau. Derimod har sikkerhedsniveauet en øvre grænse, der indebærer en grænse for, hvor højt et sikkerhedsniveau må fastsættes.

10. Sikkerhedsforanstaltninger:

Dette afsnit vil fastlægge begrebet »sikkerhedsforanstaltninger«. Det er en forudsætning for den juridiske for forståelse af, hvordan et passende sikkerhedsniveau opfyldes.

Der er i PDF art. 32, stk. 1, litra a-d) specificeret visse sikkerhedsforanstaltninger, der *”alt efter hvad der er relevant”* kan iværksættes. Det er ikke en udtømmende liste, hvorefter de alene skal gennemføres, når den dataansvarlige og databehandleren i deres risikovurdering finder det *”relevant”*. Det er som udgangspunkt en skønsafvejning af, hvilket behov der er for forskellige sikkerhedsforanstaltninger, der alene kræver et resultat, hvor de gennemførte foranstaltninger udgør et passende sikkerhedsniveau. I litra a) fremgår det, at kryptering kan anvendes som en sikkerhedsforanstaltning, hvori Datatilsynets praksis om krypteringskravet fremadrettet vil have sit hjemmelsgrundlag.

En relevant sikkerhedsforanstaltning skal gennemføres under selve udformningen og iværksættelsen af en behandling af personoplysninger.¹⁰⁷ Iværksættelsen har til formål at opretholde sikkerhedsniveauet og hindre ulovlig behandling, hvorefter den dataansvarlige og databehandleren skal *”vurdere de risici, som en behandling indebærer, og gennemføre foranstaltninger, der kan begrænse disse risici, som f.eks. kryptering.”*¹⁰⁸ Derfor skal

¹⁰⁷ Jf. PDD præambel betragtning nr. 46

¹⁰⁸ Jf. PDF præambel betragtning nr. 83

sikkerhedsforanstaltningerne ikke proaktivt eliminere sikkerhedsrisiciene, de skal alene præventivt imødegå dem.

10.1. Det aktuelle tekniske niveau og implementeringsomkostninger:

Når en dataansvarlig eller en databehandler efter PDF art. 32, stk. 1 skal gennemføre en sikkerhedsforanstaltning, kan de i deres risikovurdering inddrage et legitimt hensyn til implementeringsomkostninger og det aktuelle tekniske niveau.

Ud fra ordlyden "*det aktuelle tekniske niveau*" skal en konkret sikkerhedsforanstaltning vurderes i forhold til det niveau, der teknisk er muligt at opnå på daværende tidspunkt. Med andre ord er det højest mulige tekniske niveau såkaldt "state of the art".¹⁰⁹

Implementeringsomkostninger må ud fra en naturlig sproglig forståelse omfatte de forskellige udgifter, der tilknytter sig til en sikkerhedsforanstaltning. Det må antages at omfatte alle udgifter, der kan forekomme ved gennemførelsen. Hensynet indebærer, at en implementering af sikkerhedsforanstaltninger, der skal modsvare et aktuelt tekniske niveau, kan være en uforholdsmæssig økonomisk byrde. Det kan lempe sikkerhedskravet, men det kan ikke legitimere, at der ikke skal iværksættes en sikkerhedsforanstaltning. Omkostningshensynet kan alene inddrages ved en skønsafvejning af, hvilken foranstaltning der skal iværksættes i forhold til, at den dataansvarlige eller databehandleren ikke skal udsættes for en uforholdsmæssig økonomisk byrde.¹¹⁰

Gennemførelsen af sikkerhedsforanstaltninger omfatter således en afvejning af på den ene side det aktuelle tekniske niveau og omkostningerne i forbindelse med iværksættelsen, og på den anden side de sikkerhedsrisici som behandlingen indebærer, samt de personoplysningstyper der indgår i behandlingen. Det kan resultere i, at relevanskriteriet for en bestemt sikkerhedsforanstaltning kan sænkes. Derfor indebærer risikovurderingen både, om et pågældende informationssystem modsvare det aktuelle tekniske niveau. Hvis det ikke er tilfældet, må det herefter vurderes, om andre sikkerhedsforanstaltninger kan kompensere for dette ud fra et omkostningshensyn, således der stadig er gennemført et tilstrækkeligt sikkerhedsniveau. I den situation kan der vælges mellem *fysiske*, *tekniske* og *organisatoriske* sikkerhedsforanstaltninger, som kan være relevante for at opretholde det påkrævede sikkerhedsniveau.

¹⁰⁹ Betænkning 1565/2017 om Databeskyttelsesforordningen, s. 483

¹¹⁰ Betænkning 1565/2017 om Databeskyttelsesforordningen, s. 483

I henhold til PDD art. 17, stk. 1 udtalte udvalget, at sikkerhedsforanstaltningerne indebærer *fysisk* sikkerhed. Det kunne bl.a. være fysiske forholdsregler ved sikring af bygning og lokaler, med henblik på at forhindre uvedkommendes adgang.¹¹¹ Det er en retstilstand, som er videreført fra registerlovene i LOMR § 12, stk. 1 og LPRG § 6, stk. 1.¹¹² Det er en udvidende fortolkning af den retlige standard, fordi denne retstilstand udvider anvendelsesområdet af i forhold til ordlyden, idet den alene foreskriver tekniske og organisatoriske sikkerhedsforanstaltninger. Det medfører, at fysiske sikkerhedsforanstaltninger kan opfylde et sikkerhedsniveau, uanset de foreskrevne betegnelser i ordlyden. Fysiske sikkerhedsforanstaltninger kan forebygge tilgængelighed, fortrolighed og integritet, men særligt kan de forebygge beskyttelsesinteressen om "*hændelig eller ulovlig tilintetgørelse*" ifølge PDF art. 32, stk. 2 f.eks. ved brand eller tyveri af personoplysninger i forhold til fysiske konstruktioner. På trods af den eksakte ordlyd kan det ikke antages at være lovgivers intention, at fysiske sikkerhedsforanstaltninger ikke er en del af persondatasikkerhedens retlige standard, fordi informationssystemer både kan blive mødt med digitale og fysiske krænkelser.

Ud fra ordlyden i PDF art. 32, stk. 1 og tidligere PDD art. 17, stk. 1, 1. led samt PDL § 41, stk. 3, 1. led fremgår det, at sikkerhedsforanstaltninger kan være af *teknisk* karakter. Allerede under registerlovene var der opmærksomhed på den systemtekniske sikring ifølge LOMR § 12, stk. 1 og LPRG § 6, stk. 1. Registerudvalget udpegede særligt tre grundlæggende tekniske sikkerhedsforanstaltninger i form af kendeord, kodning af data og logning, hvoraf de to første var af forebyggende karakter. Kendeord må forstås som udtryk for password, der kan anvendes som en teknisk adgangskontrol mod uvedkommende på flere niveauer, bl.a. ved opstart af programmer, åbning og lukning af datasæt, sletning af data og afslutning af programmer. Kodning af data, som er et udtryk for kryptering, kan ligeledes forhindre uvedkommendes adgang, idet oplysningerne omskrives og bliver ulæselige uden brug af rette krypterings kode. Logning opsummerer brugen af anlægget. Det indebærer en oversigt over, hvilke og hvor mange operationer der er udført. Denne oversigt kan kobles sammen med, om de loggede operationer er i overensstemmelse med de planlagte og fastlagte normer.¹¹³ Ifølge det grundlæggende princip om »rigtighed« i PDF art. 5, litra d) og den registreredes ret til berettigelse af personoplysninger i PDF art. 16 forudsætter det, at der kan ske autoriseret ændring af personoplysninger, ud fra hensynet til, at der kun behandles korrekte oplysninger. Derfor skal persondatasikkerheden sikre mod en uautoriseret ændring. De systemtekniske sikkerhedsforanstaltninger kan særligt beskytte imod "*ændring, uautoriseret videregivelse af*

¹¹¹ Betænkning 1345/1997 om behandling af personoplysninger, s. 325

¹¹² Betænkning 767/1976 om offentlige registre, s. 167

¹¹³ Betænkning 767/1976 om offentlige registre, s. 168

eller adgang til personoplysninger” efter PDF art. 32, stk. 2. Derefter kan logning bevirke, at det kan undersøges eller indsnævres, hvilke operationer der har været foretaget i forbindelse med en kompromittering.

Sikkerhedsforanstaltninger kan have *organisatorisk* karakter efter PDF art. 32, stk. 1. Det er ligeledes foreskrevet i PDD art. 17, stk. 1, 1. led og PDL § 41, stk. 3, 1. led, hvorved den gældende retstilstand er videreført inden for lovtekstens ordlyd. De har til formål, at sikre personalet varetager deres behandling af personoplysningerne med den fornødne fortrolighed.¹¹⁴ På den måde tildeles medarbejderne hos den dataansvarlige og databehandleren den nødvendige viden til at udføre behandlingen sikkerhedsmæssigt korrekt. De kan begrænses i deres omgang med personoplysninger, således de kun forbliver fortrolige for det autoriserede personale. Det kan f.eks. gennemføres ved en adgangsbegrænsning af medarbejdere i forhold til følsomme personoplysninger.¹¹⁵ Eller adgangskontrol i form af nøgler og identifikationskoder.¹¹⁶ Desuden omfatter det dataetik, hvilket er en holdning indeholdende en norm for medarbejderne om respekt for persondatasikkerhed og medvirken til effektiv persondatabeskyttelse. Det skulle under registerlovene ikke ligestilles med god lægeetik, fordi der grundlæggende ikke var faste dataetiske normer, som havde haft tid til at danne sig.¹¹⁷ De organisatoriske sikkerhedsforanstaltninger angår således både den håndterlige organisering ved tildeling af autorisation med henblik på adgangsbegrænsning, og den normbaserede tilgang angående dataetik, som personalet skal oplæres i. Derfor har de særlig betydning i forhold til sikring af de menneskelige sikkerhedsrisici, som forekommer ved behandling af personoplysning.

De beskrevne systemtekniske, fysiske og organisatoriske sikkerhedsforanstaltninger kan i risikovurderingen kompensere for hinanden på baggrund af det aktuelle tekniske niveau og omkostningshensynet. Det er f.eks. situationen, hvis en samlet skønsafvejning resulterer i, at relevanskriteriet for en bestemt sikkerhedsforanstaltning kan sænkes, når en kompenserende sikkerhedsforanstaltning i tilstrækkeligt omfang er i stand til at reducere sandsynligheden i risikovurderingen for at en trussel realiseres til en sikkerhedshændelse.¹¹⁸ Af gennemgangen fremgår det, at kompromitteringssituationerne er mangeartede, hvilket taler imod den almen gyldig forestilling i gældende ret om kryptering som ideel sikkerhedsforanstaltning, idet

¹¹⁴ Blume, Databeskyttelsesret, s. 151

¹¹⁵ Betænkning 1565/2017 om Databeskyttelsesforordningen, s. 483

¹¹⁶ Betænkning 767/1976 om offentlige registre, s. 168

¹¹⁷ Betænkning 767/1976 om offentlige registre, s. 169

¹¹⁸ Mortensen, RR.5.2018.32, Sikkerhedsforanstaltninger - i henhold til databeskyttelsesforordningen, s. 4

den potentielle sikkerhedsbrist ved afsendelse af e-mails over internettet ikke alene relaterer sig til transmissionen.

Blume betragter implementeringsomkostninger som en forpligtende omkostning, som den dataansvarlige og databehandleren må bære, når de behandler personoplysninger. Derfor skal sikkerhedskravene anses for de samme uanset platform, hvorefter sikkerhedskravene ikke er mindre ved omkostningskrævende teknologi.¹¹⁹ I samme retning er Datatilsynets opfattelse angående krypteringskravet ved afsendte e-mails indeholdende fortrolige eller følsomme personoplysninger, idet oplysningernes karakter medfører, at behovet for at beskytte personoplysningerne vejer tungest i forhold til de ulemper, et krav om kryptering medfører for den dataansvarlige eller databehandler.¹²⁰

Der er i sag C-553/07, Rijkeboer foretaget en hensynsafvejning af en uforholdsmæssig byrde for den dataansvarlige, der omhandler opbevaringsbegrænsning af oplysninger. EU-domstolen udtalte, at fristen for opbevaringsperioden skal fastlægges ved en vurdering, der *”udgør en rimelig afvejning af, på den ene side, hensynet til den registreredes interesse i beskyttelse af hans privatliv (...) og, på den anden side, hensynet til den byrde, som forpligtelsen til at opbevare denne information udgør for den registeransvarlige.”* [Fremhævet her].¹²¹ Det fremgår yderligere af sagen, at sikkerhedsreglen PDF art. 17 (nu PDF art. 32) er en bestemmelse, hvori der kan *”tages hensyn til, at visse foranstaltninger kan være uforholdsmæssige”*.¹²² Den samme rimelighedsvurdering kan ud fra en analogibetragtning overføres til en hensynsafvejning af det aktuelle tekniske niveau og implementeringsomkostningerne foreskrevet i PDF art. 32, stk. 1, overfor den registreredes interesse i beskyttelse af hans privatliv gennem persondatasikkerhed.

Analogibetraktningen vil medføre en rimelighedsvurdering af, om omkostningshensynet og det aktuelle tekniske niveau udgør en rimelig afvejning over for den registreredes interesse i persondatasikkerhed, hvorved det skal godtgøres, at de iværksatte sikkerhedsforanstaltninger afspejler et passende sikkerhedsniveau i forhold til, om det er en uforholdsmæssig stor byrde for den dataansvarlige eller databehandleren. Hvis en behandling af personoplysninger påkræver et højt sikkerhedsniveau, må en sådan afvejning resultere i, at privatlivsbeskyttelsen vejer tungest over for implementeringsomkostningerne. Ved det resultat skal der anvendes de

¹¹⁹ *Blume*, Databeskyttelsesret, s. 152

¹²⁰ Datatilsynets høringsnotat fra 01.06.2007 om *Sikkerhed ved transmission af personoplysninger via internettet i den private sektor*, s. 15

¹²¹ Rijkeboer sag C-553/07, præmis nr. 64

¹²² Rijkeboer sag C-553/07, præmis nr. 62

teknologiske muligheder, der i praksis giver den mest sikre beskyttelse af den registreredes personoplysninger. Til gengæld kan samme rimelighedsvurdering legitimere, at den registreredes interesse for beskyttelse af hans privatliv er af mindre grad, således at byrden fra implementeringsomkostninger ved opnåelse af det aktuelle tekniske niveau kan tilsidesættes, idet dette udgør en uforholdsmæssig byrde at gennemføre for den dataansvarlige og databehandleren i forhold til den potentielle privatlivskrænkelser, f.eks. ved mindre krænkende fortrolige personoplysninger.

Den udlagte rimelighedsvurdering fra EU-domstolen muliggør, at der kan være tale om en uforholdsmæssig byrde, som den dataansvarlige eller databehandleren ikke skal pålægges. Til gengæld vil det altid være en konkret vurdering, som det var i sag C-553/07, Rijkeboer. Krypteringskravet har fastlagt omkostningshensynets vægt, uden der kan foretages en konkret rimelighedsvurdering ved bl.a. *”basisoplysningernes mere eller mindre følsomme karakter”* såsom mindre beskyttelsesværdige fortrolige personoplysninger.¹²³ Det statiske omkostningshensyn i krypteringskravet er således formentlig ikke overensstemmende med EU-domstolens fortolkning, hvor sikkerhedsforanstaltninger og opbevaringsfrister indeholder tilsvarende betragtninger, hvilket kan medføre, at visse sikkerhedsforanstaltninger er uforholdsmæssige. EU-domstolens rimelighedsvurdering kan således tillægges betydning inden for persondatasikkerhed, selvom sagens rækkevidde omfatter opbevaringsbegrænsning. Da præmisserne bør kunne bruges i videre omfang, særligt når den daværende sikkerhedsregel PDD art. 17 nævnes i præmisserne som en lignende bestemmelse.¹²⁴

10.2. Sammenfatning:

Ovenstående begrebsanalyse af PDF art. 32, stk. 1 definerer »sikkerhedsforanstaltninger«, som værende fysiske, tekniske og organisatoriske, der hver for sig kan kompensere for hinanden. Deres formål er opretholdelse af et sikkerhedsniveau, der kan anses for passende ifølge PDF art. 32, stk. 2. Fastlæggelsen af sikkerhedsniveauet skal således ske efter en kontekstbestemt afvejning af, på den ene side det aktuelle tekniske niveau og omkostningerne i forbindelse med sikkerhedsforanstaltningernes iværksættelse, og på den anden side de sikkerhedsrisici som behandlingen indebærer, samt hvilke personoplysningstyper der er tale om. Heri kan der foretages en rimelighedsafvejning af den persondatasikkerhedsmæssige byrde, da forordningen næppe kræver, at den dataansvarlige og databehandleren pålægges at iværksætte uforholdsmæssige sikkerhedsforanstaltninger.

¹²³ Rijkeboer sag C-553/07, præmis nr. 63

¹²⁴ Zahle, Praktisk Retsfilosofi, s. 156

11. Krypteringskravet:

Den første del af den retsdogmatiske analyse har fastlagt forordningens formål, beskyttelsesinteresser og meningsindhold i PDF art. 32, stk. 1 og 2. Derfra er der udledt persondatasikkerhedsmæssige principper og kriterier, som danner juridisk forforståelse for denne del af analysen.

Med brug af den hermeneutiske fortolkningslære vil det blive vurderet, om Datatilsynets opfattelse af det obligatoriske krypteringskrav med udgangspunkt i sag nr. 2014-313-0389 er i overensstemmelse med meningsindholdet i hjemmelsgrundlaget. Med andre ord om krypteringskravet reelt opfylder retsfaktum. Det indebærer en analyse af de faktiske omstændigheder omkring den eksterne transmission via e-mail i forhold til, om de er ensartede i et omfang, der overflødiggør retspligten om en skønsmæssig risikovurdering i hvert konkrete tilfælde.

Kryptering er en sikkerhedsforanstaltning, hvor teksten i en e-mail låses for uvedkommende ved, at kun en krypteringsnøgle kan åbne for krypteringsalgoritmen ved dekryptering. Medmindre algoritmen kan brydes, fordi den er utilstrækkelig. Den kryptografiske algoritme omsætter klarteksten til et særligt meta-sprog, der er ulæseligt for den, som ikke besidder dekrypteringsnøglen. Det kan sikre tekstens fortrolighed, da uvedkommende skal være i besiddelse af krypteringsnøglen. Indholdet kan ikke ændres, når teksten er krypteret, hvilket sikrer integritet.¹²⁵ Derfor kan brug af kryptering særligt etablere persondatasikkerhed i behandlingen af beskyttelsesværdige personoplysninger, når de afsendes via e-mail, således den registrerede opnår integritets- og privatlivsbeskyttelse.

Retsstillingen fremgår af Datatilsynets klagesag nr. 2014-313-0389 (Manglende sikkerhed ved transmission af fortrolige og følsomme oplysninger via e-mail), hvor en offentlig dataansvarlig på grund af en forglemmelse hos en medarbejder havde sendt fortrolige og følsomme oplysninger om klagers kone og datter, der omfattede personnummer og medicinbevilling via ukrypteret e-mail. På den baggrund lægger tilsynet til grund, at den offentlige sektor generelt ikke må sende fortrolige og følsomme personoplysninger via det åbne internet, medmindre fremsendelsen sker krypteret i medfør af PDL § 41, stk. 3, jf. SB § 14 (nu PDF art. 32, stk. 1 og 2). De faktiske omstændigheder omkring transmission af personoplysninger via e-mail over internettet er med tilsynets praksis statisk, idet skønnet i risikovurderingen alene udgør et resultat, hvor kryptering vil iværksætte et passende sikkerhedsniveau. Tilsynet har tidligere tilkendegivet, at samme sikkerhedskrav gælder for

¹²⁵ Andersen, IT-retten, s. 188f

den private sektor, når omstændighederne er ensartede.¹²⁶ Derfor er det ikke en reel skærpelse af praksis, når den private sektor fremover er underlagt krypteringskravet, fordi faktum altid har været statisk fastlagt.

Det principielle spørgsmål er, om et udfald af gældende ret, der beror på en retlig standard, kan berettige en almenyldig forestilling om kryptering, som en ideel sikkerhedsforanstaltning. Da det obligatoriske krypteringskrav ikke forudsætter en egentlig skønsafvejning af potentielle krypteringsrelaterede sikkerhedsrisici, fordi retsfaktum alene er opfyldt, når der er iværksat kryptering.

11.1. Ekstern transmission:

Den følgende analyse vil illustrere, hvad en ekstern transmission via e-mail indebærer, samt hvilke sikkerhedsproblemer der relaterer sig hertil. Den faktiske beskrivelse af kryptering, vil således udgøre et teknisk kompleksitetsniveau, hvorved det er muligt, at anlægge en retlig sondring af, om kryptering reelt kan opfylde retsfaktum.¹²⁷

Når transmissionen er ekstern, er det en videregivelse af personoplysninger over internettet, hvilket Datatilsynet klassificerer som et generelt usikkert åbent net med adgang for uvedkommende.¹²⁸ Modsat et privatnetværk, der er isoleret fra andre net og uden trådløse opkoblingspunkter. I dag er de fleste net opkoblet trådløst eller har adgang til internettet, hvorefter enhver videregivelse via e-mail foretages ved ekstern transmission.¹²⁹ Dermed er det en statisk risikovurdering af det åbne internet, der ikke er genstand for en løbende skønsafvejning med yderligere skønselementer. Til gengæld anføres det af *Andersen og Udsen*, at truslen mod e-mails er i kommunikationens terminalpunkter hos henholdsvis afsenderen og modtageren fremfor i transmissionen.¹³⁰ Det netværk den registrerede og dataansvarlige eller databehandleren er opkoblet på under afsendelsen vil således have hvert sit sikkerhedsniveau f.eks. ved brug af en tilstrækkelig eller utilstrækkelig firewall, som vil resultere i forskellige skønsafvejede sikkerhedsniveauer i forhold til uvedkommendes adgang, når den afsendte tekst er modtaget eller opbevaret inden afsendelse.

¹²⁶ Datatilsynets årsberetning (2001), s. 68

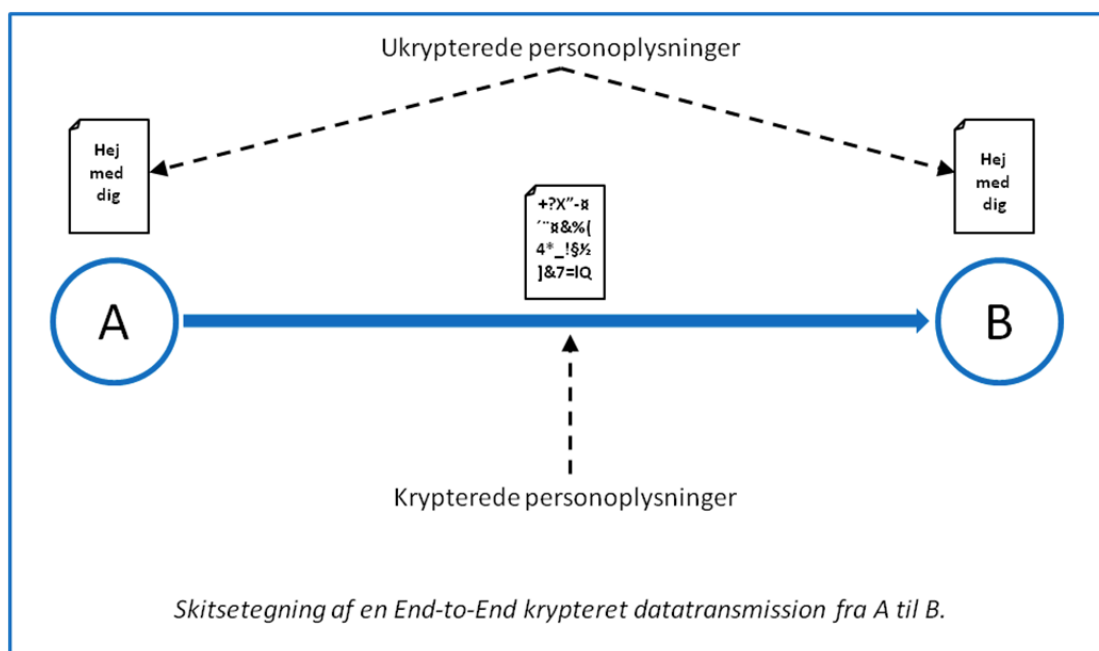
¹²⁷ *Andersen*, IT-retten, s. 101, om IT-retlige beskrivelsesproblematikker

¹²⁸ Datatilsynets høringsnotat fra 01.06.2007 om *Sikkerhed ved transmission af personoplysninger via internettet i den private sektor*, s. 14

¹²⁹ Datatilsynets IT-sikkerhedstekst, ST4, s. 2

¹³⁰ *Andersen og Udsen*, U.2005B.378, ”Krav om kryptering af e-mails med fortroligt indhold?”, s. 2

En ukrypteret og krypteret ekstern transmission kan illustreres med *figur 1*. En transmission er en behandling af personoplysninger efter PDF art. 4, nr. 1) og nr. 2), der som minimum indeholder to parter. Til gengæld kan den indeholde betydelige kombinationer af antal parter, hvor dataansvarlige, databehandlere og registrerede kan afsende og modtage personoplysninger ved brug af transmission over internettet.



*Figur 1*¹³¹

Ifølge PDF art. 4, nr. 7) vil den dataansvarlige være den, der beslutter at foretage transmissionen. Efter *figur 1* er den dataansvarlige (A), når denne beslutter, at der skal ske en transmission. Omvendt vil det være (B), hvis denne pålægger (A) at foretage en transmission. Med andre ord er den dataansvarlige den, der efter en konkret vurdering er initiativtageren, fordi denne fastlægger formålet med behandlingen, som er en transmission med hjælpemidlet e-mail.¹³²

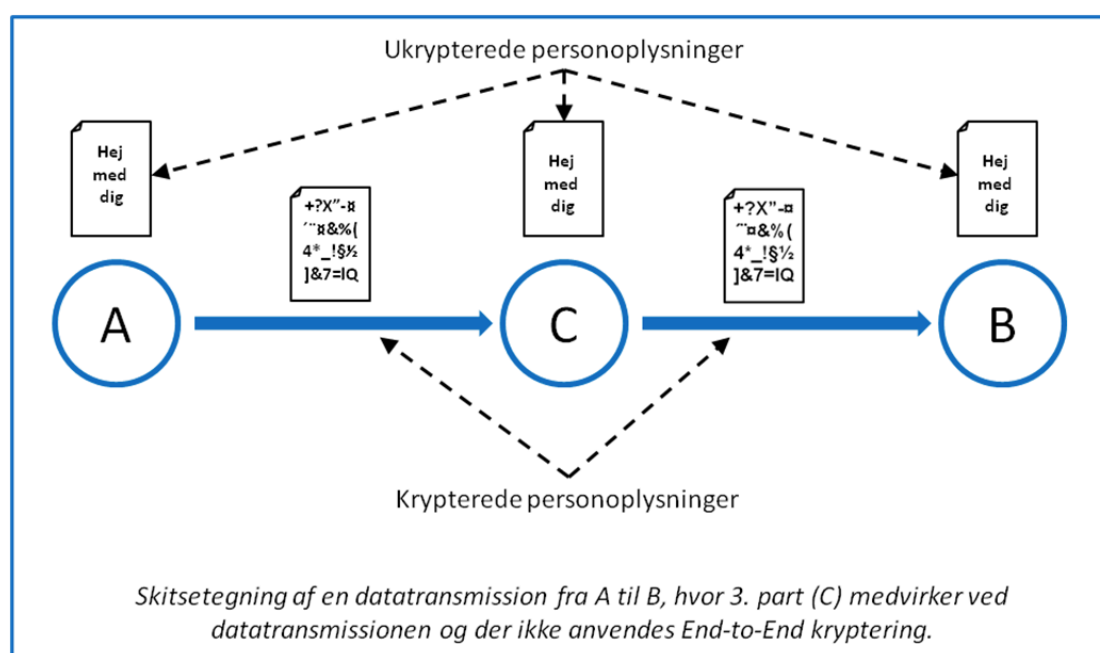
Databehandleren vil ifølge PDF art. 4, nr. 8), være den, som den dataansvarlige på dennes vegne har overladt at udføre den praktiske behandling af personoplysninger, f.eks. foretage behandlingsskridt om en videregivelse ved en ekstern transmission via e-mail. På trods af en databehandleraftale skal databehandleren selvstændigt iværksætte persondatasikkerhed efter PDF art. 32, stk. 1, hvilket ifølge praksis er kryptering, selv om det eventuelt ikke fremgår af instruktionerne i databehandleraftalen.

¹³¹ Datatilsynets IT-sikkerhedstekst, ST2, s. 3

¹³² Datatilsynets IT-sikkerhedstekst, ST2, s. 1

Den registrerede er ikke pligtsubjekt i en persondatasikkerhedsmæssig henseende, hvorefter denne ikke er forpligtet til at iværksætte persondatasikkerhed. Derimod er den dataansvarlige og databehandleren ansvarlige for, at den registrerede, som modtager, kan dekryptere krypteringen. Det medfører en usikkerhed i krypteringskravet, fordi der kan forekomme tilfælde, hvor der er en utilstrækkelig kontrol med den registreredes dekryptering.

En datatransmission, der både indeholder en dataansvarlig (A) og en databehandler eller dataansvarlig (B) og en modtager (C), som kan være den registrerede kan illustreres med *figur 2*. Den foreviser, at der foretages en kryptering hos den dataansvarlige (A) før afsendelse. En dataansvarlig eller databehandler (B) modtager og dekrypterer indholdet i et vist tidsrum, før de krypteres igen før endnu en afsendelse. Den sidste modtager (B), f.eks. den registrerede, hvis personoplysninger kan være genstand for transmissionen, foretager til sidst en dekryptering efter modtagelse.



Figur 2¹³³

En risikovurdering i *figur 2* kan bl.a. omfatte den dataansvarlige (A)'s utilstrækkelige kontrol med databehandleren (B) samt uvedkommendes adgang til de dekrypterede personoplysninger hos (B). Sikkerhedsrisiciene øges dermed, når flere parter medvirker i en transmission. Den kompleksitet skal modsvares i sikkerhedsniveauet, som vil forudsætte yderligere beskyttelsesbehov. Derfor er det Datatilsynet anbefaling, at en End-to-End kryptering er nødvendig, hvilket indebærer, at krypteringen kun kan dekrypteres mellem

¹³³ Datatilsynets IT-sikkerhedstekst, ST2, s. 5

afsender og modtager.¹³⁴ End-to-End krypteringen vil sikre transmissionen mellem (A) til (B) og mellem (B) til (C).

Dermed kan det slutes, at der knytter sig visse sikkerhedsproblematikker til det obligatoriske krypteringskrav, som kan krænke den registreredes integritets- og privatlivsbeskyttelse. Ved iværksættelsen af kryptering bør det bl.a. overvejes om, der er anvendt en krypteringsalgoritme, som har vist sig modstandsdygtig i praksis. De krypteringsnøgler, der kan dekryptere indholdet, skal have en tilstrækkelig længde. En evt. adgangskontrol via password bør være have samme kompleksitet, som den krypteringsnøgle den skal beskytte. Derudover kan det være relevant at sikre en begrænsning på antal af forsøg til at indtaste et password. Distributionen af krypteringsnøglerne og eventuelle tilhørende password bør tilrettelægges på en måde, der ligeledes sikrer det nødvendige beskyttelsesbehov f.eks. hvor de afsendes hver for sig via e-mail og sms.¹³⁵

De yderligere sikkerhedsforanstaltninger kan selvstændigt udgøre sikkerhedsrisici f.eks. en algoritme i en krypteringsnøgle, der er påvirket af den teknologiske udvikling, som med tiden vil blive forældet, eller en utilstrækkelig distribution af krypteringsnøglerne, hvilket vil eksponere den for uvedkommende. Det vil medføre, at sikkerhedsniveauet vil blive skærpet, hvorved krypteringen i PDF art. 32, stk. 1, litra a) ikke vil opfylde risikovurderingen fra PDF art. 32, stk. 2.

På baggrund af de ovenforstående betragtninger kan kryptering som et minimumskrav ikke absolut opfylde et fastlagt sikkerhedsniveau, fordi niveauet vil ændre sig i takt med omstændighederne, herunder når krypteringen ikke er etableret og anvendt korrekt. Fremfor at være et minimumskrav vil det være nærliggende, at krypteringskravet undergives en konkret skønsafvejet risikovurdering ifølge PDF art. 32, stk. 1, litra a) og stk. 2, idet opfyldelse af den retlige standard nødvendigvis vil forudsætte, at alle relevante sikkerhedsrisici ved en behandling af personoplysninger inddrages som skønselementer, herunder krypteringens yderligere etablerings- og anvendelsesrisici.

Princippet om en øvre grænse for persondatasikkerheden kan begrunde en skønsafvejning i hver konkrete situation, fordi kryptering kan medføre et for højt sikkerhedsniveau efter PDF art. 32, stk. 2.¹³⁶ Det kan være tilfældet, hvor sikkerhedsrisikoen er lav, f.eks. ved mindre beskyttelsesværdige fortrolige personoplysninger. Det kan understøttes af, at kryptering er en

¹³⁴ Datatilsynets IT-sikkerhedstekst, ST2, s. 5f

¹³⁵ Datatilsynets IT-sikkerhedstekst, ST2, s. 4

¹³⁶ Jf. J.nr. 2002-215-0094 (Opbevaring af sikkerhedskopier af e-post)

sikkerhedsforanstaltning, som efter en rimelighedsvurdering kan være en uforholdsmæssig byrde at gennemføre for den dataansvarlige og databehandleren i den offentlige eller private sektor.¹³⁷

Modsat den ovenfor nævnte tilslutning til en konkret afvejet risikoprofil ved hver behandlingssituation, vil der formentlig ikke opstå situationer, hvor det ikke er nødvendigt at sikkerhedsforanstalte en fortroligheds-, integritets- og autenticitetsbeskyttelse ved ekstern transmission via kryptering af visse særligt fortrolige personoplysninger og altid af følsomme personoplysninger. Det kan sammenholdes med Datatilsynets risikovurdering af det åbne internet, hvor tilsynet fastlægger en generel høj sikkerhedsrisiko for kompromittering fra uvedkommende. Det understøttes af ISO-standarden, hvor kryptografiske kontroller kan sikre en korrekt og effektiv brug for at beskytte oplysningernes fortrolighed, autenticitet og/eller integritet.¹³⁸ Sammenholdt med persondatasikkerhedens nedre grænse kan disse betragtninger støtte et obligatorisk krypteringskrav, når der er tale om ensartede omstændigheder.

11.2. Retsgrundlag:

På baggrund af forarbejderne til registerlovene, PDL og PDF forudsætter meningsindholdet i sikkerhedsreglen ingen retspligt til at gennemføre bestemte sikkerhedsforanstaltninger, der ikke kan anses for nødvendig for at opnå et passende sikkerhedsniveau. Sikkerhedsreglens formål er at forhindre potentielle sikkerhedsrisici, hvorved risikovurderingen er det bærende for, at reglen finder anvendelse. Hvis en risikovurdering ikke resulterer i et beskyttelsesbehov, vil den retlige standard i sikkerhedsreglens materielle indhold i PDF art. 32, stk. 1 og 2 ligeledes ikke påkræve et bestemt sikkerhedskrav. Kryptering fremhæves i PDF art. 32, stk. 1, litra a), men det er alene en sikkerhedsforanstaltning, der skal anvendes ”*bl.a. alt efter hvad der er relevant*” ud fra risikovurderingen. Det grundlæggende princip om persondatasikkerhed i PDF art. 5, litra f) forudsætter ligeledes, at princippet opfyldes ved en skønsafvejning. Dermed kan det konstateres, at hverken en ordlyds- eller formålsfortolkning af sikkerhedsreglerne i registerlovene, PDD, PDL og PDF eller reglernes forarbejder understøtter et generelt krypteringskrav af alle e-mails indeholdende fortrolige eller følsomme personoplysninger, men nærmere opstiller en formodning for, at det skal afgøres ved en konkret skønafvejet risikovurdering ud fra behandlingerne af personoplysningerne, herunder variationen af personoplysningstyper.

¹³⁷ Jf. Rijkeboer sag C-553/07, præmis nr. 62 og 64

¹³⁸ DS/ISO/IEC 27002, 1. udgave, *Informationsteknologi – Sikkerhedsteknikker - Regelsæt for styring af informationssikkerhed*, afsnit 10.1.1.

Retstillingen er ikke særlig klar, idet den retlige standard medfører en fleksibel regulering ved en skønsafvejning, hvorefter Datatilsynet som retsudøver har ment, at et obligatorisk krypteringskrav kan rummes inden for gældende ret. Det er således uklart, om der er et tilstrækkeligt hjemmelsgrundlag, når udfaldet af gældende ret beror på en retlig standard, hvor meningsindholdet berettiges med en almenfyldig forestilling om kryptering, som en ideel sikkerhedsforanstaltning. En sådan retsstilling med betydelige etablerings- og anvendelsesrisici medfører et behov for autoritative afgørelser fra de danske domstole og EU-domstolen, der tager stilling til meningsindholdet og udstrækningen af den retlige standard i PDF art. 32, stk. 1 og 2, da de ikke er bundet af administrativ praksis.

11.3. Sammenfatning:

En gennemført kryptering er ikke en garanti for, at den er etableret og anvendt korrekt af afsender og modtager, idet der knytter sig yderligere sikkerhedsforanstaltninger, før den kan anses for uomgængelig. Forhenværende og nuværende forarbejder til persondatalovgivningen indeholder ikke et fortolkningsbidrag, der underbygger, at den betydelige skønsafvejning i sikkerhedsreglen PDF art. 32, stk. 1 og 2 kan fraviges ved et generelt krav om kryptering ved ekstern transmission via e-mail indeholdende fortrolige og følsomme personoplysninger. Derfor foreligger der ingen retspligt til at gennemføre bestemte sikkerhedsforanstaltninger, som ikke kan anses for nødvendige for at opnå et passende sikkerhedsniveau. Det kan således ikke være en tilsidesættelse af sikkerhedsreglen, hvis kryptering ikke er nødvendig ifølge risikovurderingen. Imedens vil der utvivlsomt være konkrete tilfælde, hvor kryptering kan opfylde det materielle indhold i PDF art. 32, stk. 1 og 2, hvilket er Datatilsynets hensigt med minimumskravet.

12. Konklusion

Et af dette speciales formål var at besvare, hvordan persondatasikkerhed defineres, og hvad der i den henseende kan anses for gældende ret. Det kan på den baggrund konkluderes, at persondatasikkerhed defineres som en retlig standard. Det er et lovgivningsideal om, at behandling af personoplysninger er sikret af et passende sikkerhedsniveau. Pligtssubjekterne er den dataansvarlige og databehandleren i den offentlige og private sektor, hvorved de er ligestillet i en persondatasikkerhedsmæssig henseende uanset over- og underforholdet fra en databehandleraftale. De skal opfylde behandlingsforpligtelsen om iværksættelse af persondatasikkerhed, når de foretager behandling af personoplysninger ifølge PDF art. 32, stk. 1 og 2. Den persondataretlige selvbestemmelsesret medfører ikke, at den registrerede selv kan være rådig over, hvorvidt de behandlingsforpligtelser, der fremgår af lovgivningen, skal aktiveres. Derfor kan den registrerede ikke ved sit samtykke legitimere, at den dataansvarlige og databehandleren ikke har en behandlingsforpligtelse til at iværksætte persondatasikkerhed.

Den retlige standard opfyldes, når der er gennemført en skønsafvejet risikovurdering, som vil afgøre, hvilke relevante sikkerhedsforanstaltninger efter PDF art. 32, stk. 1, der kan modsvare et passende sikkerhedsniveau ifølge PDF art. 32, stk. 2. Derfor foreligger der ingen retspligt til at gennemføre bestemte sikkerhedsforanstaltninger, som ikke kan anses for nødvendige for at opnå et passende sikkerhedsniveau. Fremadrettet har det obligatoriske krypteringskrav sit hjemmelsgrundlag i PDF art. 32, stk. 1, litra a) og stk. 2, hvor kryptering i ordlyden alene fremhæves som en sikkerhedsforanstaltning, der skal anvendes, når den er relevant for at opfylde sikkerhedsniveauet.

Det andet formål med specialet var at besvare, om Datatilsynets praksis angående et generelt krypteringskrav er i overensstemmelse med hjemmelsgrundlaget. Datatilsynets praksis viser, at kryptering er obligatorisk, når der foretages en ekstern transmission via e-mail indeholdende fortrolige eller følsomme personoplysninger. Den administrativ praksis anvender alene en statisk risikovurdering, hvor gennemførsel af kryptering er en almen gyldig sikring af persondatabeskyttelsen, som en ideel sikkerhedsforanstaltning. Praksis tilsidesætter således den forudsatte skønsafvejede risikovurdering. Der vil utvivlsomt være konkrete tilfælde, hvor krypteringskravet opfylder sikkerhedsreglens materielle indhold, særligt når en afsendt e-mail indeholder følsomme personoplysninger ifølge PDF art. 9, stk. 1. Imidlertid er kryptering ingen garanti for, at den er etableret og anvendt korrekt af afsender og modtager, idet der knytter sig yderligere sikkerhedsforanstaltninger, før den kan anses for uomgængelig. Det i sig selv vil udgøre sikkerhedsrisici, der vil skærpe sikkerhedsniveauet, hvorved en statisk risikovurdering bliver formålsløs.

Krypteringskravet er et minimumskrav med abstrakte personoplysningskategorier, hvor retsfaktum er uklart, idet den dataansvarlige og databehandleren ikke præcist ved, hvornår det obligatoriske retskrav indtræder. Den konkrete vurdering af, om en personoplysningstype er fortrolig, indeholder et betydeligt skønselement. Det medfører en usikker retsstilling for den dataansvarlige og databehandleren, der skal identificere og kategorisere enhver personoplysning, som angiver et væsentligt privat eller socialt problem af særlig følsom karakter inden for fysiske personers private eller økonomiske forhold. Tvivlsspørgsmålet omkring retsfaktum opstår således, når der afsendes e-mails indeholdende almindelige personoplysninger efter PDF art. 6, da de kan være fortrolige, hvorimod de følsomme personoplysninger, der er udtømmende opregnet i PDF art. 9, stk. 1, altid skal krypteres.

Datatilsynets har som retsudøver foretaget en fortolkning af sikkerhedsreglens meningsindhold, hvori det generelle krypteringskrav menes at være i overensstemmelse med hjemmelsgrundlaget. Da Datatilsynets administrative praksis er en væsentlig retskilde på det persondataretlige retsområde, må det obligatoriske krypteringskrav anses for retsstillingens gældende præjudikat, der danner præcedens for retstilstanden. Det er udgangspunktet, indtil der foreligger afgørelser fra de danske domstole eller EU-domstolen, som ved en autoritativ fortolkning kan tage stilling til meningsindholdet og udstrækningen af den retlige standard i PDF art. 32, stk. 1 og 2.

Det kan endelig konkluderes, at krypteringskravet i forhold til videregivelse af fortrolige og følsomme personoplysninger i transit ved brug af e-mail er udtryk for gældende ret, fordi Datatilsynet er den præjudikatskabende retsinstans på det persondataretlige retsområde. Dette på trods af denne fremstillings retsdogmatiske analyse af, at sikkerhedsreglen PDF art. 32, stk. 1 og 2 ved en ordlyds- og formålsfortolkning af at realisere forordningens målsætning om reel og faktisk persondatabeskyttelse af fysiske personer, nærmere skaber en formodning for, at kryptering som et sikkerhedskrav skal afgøres ved en konkret skønssafvejet risikovurdering af behandlingssituationen og personoplysningstyperne.

13. Perspektivering:

Sanktionsniveauet under PDL ved tilsidesættelse af persondatasikkerheden har ikke været skræmmende. Brud på persondatasikkerheden efter PDL § 41, stk. 3 har generelt medført, at Datatilsynet reaktivt har udtalt kritik som »meget beklageligt« ved offentliggørelse af fortrolige og følsomme personoplysninger.¹³⁹ Det fremadrettede sanktionsniveau i PDF lægger op til en ensretning i medlemsstaterne.¹⁴⁰ Det vil formentlig medføre en skærpelse af de danske strafferetlige retsfølger i persondataretten ved et markant højere bødeniveau. Ved overtrædelse af persondatasikkerheden skal der tages hensyn til, den dataansvarliges eller databehandlerens grad af ansvar under hensyntagen til tekniske og organisatoriske foranstaltninger, som de har gennemført i henhold til artikel 32 ifølge PDF art. 83, stk. 2, litra d). Ved vurderingen af ansvaret må det strafferetligt forudsætte, at der er en klarhed i retsgrundlaget, således den dataansvarlige og databehandleren bliver i stand til forudse de strafferetlige konsekvenser af gennemførte eller undladte krypteringer.¹⁴¹

Det kan overvejes, om retstilstanden med rimlighed kan forudsiges i mangel af kravspecifikationer til de systemer, der skal implementere kryptering, samt de vage parametre for, hvad der er en egentlig fortrolig personoplysning. Det er ikke angivet, om den offentlige sektor indebærer en større sikkerhedsrisiko for kompromittering f.eks. af straffeoplysninger, hvorimod den private sektor i visse tilfælde har en betydelig lavere skadevirkning ved utilsigtet offentliggørelse af f.eks. ordrebekræftelser fra indkøb. Dermed kan det diskuteres, om den offentlige sektor har et større ansvar end den private sektor til at sikre en integritets- og privatlivsbeskyttelse med brug af kryptering.

Sanktionering af personoplysningskrænkelser i relation til krypteringskravet bør formentlig fortolkes indskrænkende på grund af den uklare retstilstand. Den fremadrettede retspraksis vil konstatere, om ensretningskravet af bødefrekvensen og bødestørrelserne i Danmark opnår samme niveau, som i de øvrige medlemsstater.¹⁴² Til illustration har det franske datatilsyn den 7. maj 2018 idømt en dataansvarlig brillebutik en markant bøde på 250.000 EUR for brud på persondatasikkerheden efter den daværende franske persondatalov. Der var tale om en andengangsforseelse, hvor identifikationsoplysninger og følsomme personoplysninger fra de registrerede kunder var utilsigtet blotlagt for uvedkommende på internettet.¹⁴³

¹³⁹ *Tranberg*, m.fl., *Internetretten* (2012), s. 541

¹⁴⁰ Betænkning 1565/2017 om Databeskyttelsesforordningen, s. 936

¹⁴¹ *Baumbach*, *Strafferet og menneskeret*, s. 142f

¹⁴² *Udsen*, *Eksponeret – Grænser for privatliv i en digital tid*, ”Effektivt tilsyn med persondatabeskyttelsen er en udfordring”, s. 264

¹⁴³ <http://www.bechbruun.com/da/Videncenter/Nyheder/2018/Bde-p-250000-EUR-til-fransk-brillebutik-for-sikkerhedsbrud>

14. Litteraturliste:

Retslitteratur:

- Charlotte Bagger Tranberg, m.fl., *Internetretten*, 3. udgave, Ex Tuto A/S, 2017
- Charlotte Bagger Tranberg, m.fl., *Internetretten*, 2. Udgave, Ex Tuto A/S, 2012
- Charlotte Bagger Tranberg, *Nødvendig behandling af personoplysninger*, Forlaget Thomson A/S, 2007
- Carsten Munk-Hansen, *Retsvidenskabsteori*, 1. udgave, Jurist- og Økonomforbundets Forlag, 2014
- Dag Weise Schartum, m.fl., *Informasjonssikkerhet – Rettslige krav til sikker bruk af IKT*, Fagbokforlaget, 2005
- Henrik Udsen, *Eksponeret – Grænser for privatliv i en digital tid, "Effektivt tilsyn med persondatabeskyttelsen er en udfordring"*, Gads Forlag, 2018
- Henrik Udsen, *IT-ret*, 3. udgave, Ex Tuto A/S, 2016
- Henrik Udsen, *Lærebog i informationsret*, Jurist- og Økonomforbundets Forlag, 2016
- Henrik Waaben og Kristian Korfits Nielsen, *Lov om behandling af personoplysninger med kommentarer*, 3. Udgave, Jurist- og Økonomforbundets Forlag, 2015
- Henrik Zahle, *Praktisk Retsfilosofi*, Christian Ejlers' Forlag, 2005
- Mads Bryde Andersen, *IT-retten*, 2. udgave, Gjellerups Forlag, 2005
- Martin Gräs Lind, *Medarbejderes integritetsbeskyttelse i dansk ret – med særlig fokus på databeskyttelse, kontrol og overvågning i den private sektor*, Jurist- og Økonomforbundets Forlag, 2016
- Niels Fenger, *Forvaltningsloven med kommentarer*, 1. udgave, Jurist- og Økonomforbundets Forlag, 2013
- Peter Blume, *Retssystemet og juridisk metode*, 3. udgave, Jurist- og Økonomforbundets Forlag, 2016
- Peter Blume, *Den nye persondataret – Persondataforordningen*, Jurist- og Økonomforbundets Forlag, 2016
- Peter blume og Janne Rothmar Herrmann, *Ret, privatliv og teknologi*, 3. udgave, Jurist- og Økonomforbundets Forlag, 2013
- Peter Blume, *Databeskyttelsesret*, 4. udgave, Jurist- og Økonomforbundets Forlag, 2013
- Sten Bønsing, *Tavshedspligtsreglerne og persondataloven, Forvaltningsloven 25 år*, Jurist- og Økonomforbundets Forlag, 2012
- Trine Baumbach, *Strafferet og menneskeret*, 1. udgave, Karnov Group, 2014

Dansk lovgivning:

- Lov om offentlige myndigheders registre nr. 294 af 08/06/1978 (LOMR)
- Lov om private register m.v. nr. 293 af 08/06/1978 (LPRG)
- Lov om behandling af personoplysninger nr. 429 31/5/2000 (PDL)
- Straffeloven, Lovbekendtgørelse 2017-08-09 nr. 977
- Forvaltningsloven, Lovbekendtgørelse 2014-04-22 nr. 433

Bekendtgørelser:

- Bekendtgørelse 2000-06-15 nr. 529 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning
- Bekendtgørelse 2000-06-15 nr. 528 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning

Betænkninger:

- Betænkning nr. 601/1971, *Om privatlivets fred* (Straffelovsrådet)
- Betænkning nr. 687/1973, *Delbetænkning om private registre* (Registerudvalget)
- Betænkning nr. 767/1976, *Delbetænkning om offentlige registre* (Registerudvalget)
- Betænkning nr. 1345/1997, *Behandling af personoplysninger* (Registerudvalget)
- Betænkning nr. 1563/2017, *Om freds- og ærekrænkelser* (Straffelovsrådet)
- Betænkning nr. 1565/2017, *Om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning*

Retspraksis:

- U.2011.2343.H

EU-retsakter:

- Europa-Parlamentets og Rådets Forordning 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (PDF)
- Europa-Parlamentets og Rådets direktiv 1995/46 af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (PDD)

EU-domme:

- C-342/12 Worten
- C-131/12 Google Spain
- C-101/01 Lindqvist
- C-553/07 Rijkeboer

Datatilsynets praksis:

- J.nr. 2002-215-0094 (Opbevaring af sikkerhedskopier af e-post)
- J.nr. 2004-082-0118 (Elektronisk reserverings- og kvitteringsmeddelelser fra bibliotekerne)
- J.nr. 2004-52-2442 (Kommunens tv-overvågning af skole og dagsinstitutioner)
- J.nr. 2006-44-0051 (Advarselsregister hos Rejsekort A/S (I))
- J.nr. 2011-082-0234 (National Sundheds-it (NSI))
- J.nr. 2014-313-0389 (Manglende sikkerhed ved transmission af fortrolige og følsomme oplysninger via e-mail)
- J.nr. 2014-632-0081 (Brug af fingeraftryk ved bloddonation).
- J.nr. 2016-632-0197 (Sikkerhed ved bestilling af en nye TastSelv-kode hos SKAT)
- J.nr. 2016-216-0569 (Kritik af skoles gennemgang af elevers søgehistorik)
- J.nr. 2017-631-0159 (Offentliggørelse af kontaktoplysninger på jobansøgere hos Novo Nordisk A/S)
- J.nr. 2017-331-0667 (Uberettiget adgang til personnumre på studerende hos Det Sundhedsvidenskabelige Fakultet på Københavns Universitet)
- J.nr. 2018-632-0225 (Kalundborg Kommunes brug af en FTP-server til personhenførbare oplysninger)

Datatilsynets vejledninger:

- Datatilsynets IT-sikkerhedstekst, ST2, *Overvejelser om sikring mod, at personoplysninger kommer til uvedkommendes kendskab i forbindelse med datatransmission*, 2014
- Datatilsynets IT-sikkerhedstekst, ST4, *Datatransmission af personoplysninger på åbne net*, 2014
- Vejledning nr. 37 af 2. april 2001 til bekendtgørelse nr. 528 af 15. juli 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning

Datatilsynets årsberetninger:

- Datatilsynets årsberetning, 2001
- Datatilsynets årsberetning, 2003
- Datatilsynets Årsberetning, 2005

Juridiske tidsskrifter:

- Christian Wiese Svanberg, *U.2006B.43 "Samtykke og datasikkerhed"*
- Henning Mortensen, *Sikkerhedsforanstaltninger - i henhold til databeskyttelsesforordningen*, RR.5.2018.32
- Mads Bryde Andersen og Henrik Udsen, *Krav om kryptering af e-mails med fortroligt indhold?*, U.2005B.378
- Mads Bryde Andersen og Henrik Udsen, *Kryptering af e-mails og persondatalovens § 41, stk. 3 - en replik*, U.2006B.110

Artikler:

- <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2018/jul/skaerpet-praksis-ift-krypteret-e-mail/>
- <http://www.bechbruun.com/da/Videncenter/Nyheder/2018/Bde-p-250000-EUR-til-fransk-brillebutik-for-sikkerhedsbrud>

Andet materiale:

- Datatilsynets høringsnotat fra 01.06.2007 om *Sikkerhed ved transmission af personoplysninger via internettet i den private sektor*
- ISO/IEC DIS 29134 *"Information technology – Security techniques – Privacy impact assesment – Guidelines"*
- DS/ISO/IEC 27002, 1. udgave, *Informationsteknologi – Sikkerhedsteknikker - Regelsæt for styring af informationssikkerhed*

Bilag 1

Fortrolighedsvurdering af personoplysninger:	Afgørende er bl.a. en vurdering af, om personoplysningen er af en sådan art, at den efter en almindelig opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab.
Vurdering af personoplysningens karakter:	Private forhold – omfatter bl.a.: • <i>Interne familieforhold</i> - Hjemlige forhold, opdragelsesmåde, familiestridigheder, separations- og skilsmissebegæringer, adoptionsforhold - Administration af ventelister til institutioner om særlige ønsker, beliggenhed og tidspunkter mv. • <i>Sensitive personlige forhold</i> - Personlighedstest, følelsesliv, legemlige kendetegn, kostvaner - Alkohol- eller narkotikatest - Kvitteringer fra biblioteket og e-handel - Ulykkestilfælde med væsentlige personlige eller sociale konsekvenser - Selvmord og selvmordsforsøg • <i>Arbejdsomæssige forhold (privat sektor)</i> - Disciplinære sanktioner og andre ledelsesreaktioner f.eks. hjemsendelse eller bortvisning, fratrædelsesgrund - Langvarig arbejdsløshed, afslag på jobansøgninger, modtagelse af førtidspension • <i>Arbejdsomæssige forhold (offentlige sektor)</i> - I særlige tilfælde kan der ske beskyttelse af særlige arbejdsgrupper, hvor en potentiel offentliggørelse kan medføre repressalier f.eks. navne på behandlingspersonale i psykiatrien • <i>Uddannelsesforhold</i> - Eksamenskarakterer vedrørende den enkelte - Oplysninger om sygefravær og sygdomsperioder - Oplysninger om begrundelsen for andet fravær end fravær på grund af sygdom - Oplysninger om særlige undervisningsforanstaltninger og dispensationer fra undervisning • <i>Foreningsmæssige forhold end oplysninger om fagforenings-mæssige tilhørsforhold</i> - Tilhørsforhold til en modstandsbevægelse - Loger hvor medlemsskabet forudsætter fortrolighed • <i>Strafbare forhold</i> - Kvalificerede oplysninger om overtrædelse af lovgivningen, der ikke har udløst (eller kan udløse) et strafansvar, men kan udløse andre sanktioner f.eks. rettighedsfrakendelse - En myndigheds konklusion om grundlag for strafansvar om en fysisk person - Oplysninger om de bagvedliggende årsager til, at der er blevet begået en lovovertrædelse f.eks. sygdom, personlige problemer eller karakterologiske forhold - Oplysninger om lovovertræderens personlige egenskaber • <i>Identifikationsoplysninger</i> - Personnumre - Adgangskoder til selvbetjeningsløsninger indeholdende fortrolige og følsomme personoplysninger, f.eks. NemID, pinkoder
Vurdering af den sammenhæng, hvori personoplysningen indgår:	• Den potentielle skadevirkning fra en udbredelse ved kompromittering. - Det kan bl.a. omfatte økonomisk tab, repressalier, forulempelser eller lignende • Sammenkædning mellem offentligt og ikke-offentligt tilgængelige personoplysninger kan statuere en fortrolig personoplysning. - Det kan f.eks. være en almindelig adresseoplysning til et psykiatrisk hospital eller fængsel • Røber oplysningen et væsentligt privat eller socialt problem af særlig følsom karakter
Undtagelser:	• Hvis der ikke kan nægtes aktindsigt i personoplysningen efter Offentlighedsloven, vil den ikke være af fortrolig karakter. • Personoplysninger om private forhold der i forvejen er offentligt tilgængelige anses ikke for fortrolige personoplysninger - Når de fremgår af offentligt tilgængelige registre f.eks. folkeregisteret, tingbogen, skattelister - Når fysiske personer har optrådt offentligt med sine holdninger, f.eks. tilkendegivet politiske eller religiøse holdninger, vil forholdende efterfølgende ikke være fortrolige personoplysninger

Bilag 2

Fortrolighedsvurdering af personoplysninger:	Afgørende er bl.a. en vurdering af, om personoplysningen er af en sådan art, at den efter en almindelig opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab.
Vurdering af personoplysningens karakter:	Økonomiske forhold – omfatter bl.a.: • <i>Indtægts- og formueforhold om privat personer</i> - Skattepligtig årsindkomst, skattegæld - Skyldige restancer, manglende betalingsevne eller betalingsvilje, f.eks. rykkerbreve - Regninger, fakturerer - Modtagelse af boligsikring af en bestemt størrelse - Indtægtsafhængig pension - Kreditkort og hævekort transaktioner - Økonomiske forhold i forbindelse med bankforretninger • <i>Indtægts- og formueforhold om personligt drevne enkeltmandsvirksomheder</i> - Påtænkte omstrukturering, strategiske overvejelser eller lignende - Ny og hidtil ukendt produktionsmetode, hvis andres kendskab hertil vil skade den pågældende virksomhedsejer - afsætningsmuligheder eller konkurrenceevne - Transaktioner og saldi fra fysiske personer - Forbrugsregnskaber - Fakturaer - Oplysninger om bestilte og købte varer i e-handels-løsninger fra fysiske personer f.eks. ordrebekræftelser - Betalingsoplysninger - Indkøbsmønstre • <i>Arbejdsmæssige forhold (privat sektor)</i> - Personaleforhold - Lønforhold og tillæg • <i>Strafbare forhold vedrørende personligt drevne enkeltmandsvirksomheder</i> - Kvalificerede oplysninger om overtrædelse af lovgivningen, der ikke har udløst (eller kan udløse) et strafansvar begået i nærings- eller forretningsforhold - Meddelte påbud og forbud og lignende - Oplysninger om de bagvedliggende årsager til, at der er blevet begået en lovovertrædelse f.eks. sygdom, personlige problemer eller karakterologiske forhold • <i>Identifikationsoplysninger</i> - Kreditkort- og hævekortnummer - Kontonummer f.eks. hvortil løn skal anvises
Vurdering af den sammenhæng, hvori personoplysningen indgår:	• Afslører de økonomiske forhold noget om den fysiske persons privat økonomi • Er der tale om en personligt drevet enkeltmandsvirksomhed eller en juridiske person i selskabsform, idet oplysninger om juridiske personer ikke er personoplysninger • Kan kompromittering medføre en nærliggende risiko for, at personen eller enkeltmandsvirksomheden påføres et væsentligt økonomisk tab - Er oplysninger om en enkeltmandsvirksomheds drifts- og forretningsforhold af en sådan karakter, at det kan skade virksomhedsejeren, hvis oplysninger videregives til uvedkommende f.eks. konkurrenter
Undtagelser:	• Hvis der ikke kan nægtes aktindsigt i personoplysningen efter Offentlighedsloven, vil den ikke være af fortrolig karakter. • Personoplysninger om økonomiske forhold der i forvejen er offentligt tilgængelige anses ikke for fortrolige personoplysninger. - Når de fremgår af offentligt tilgængelige registre f.eks. skattelister

Kilder: Niels Fenger, Forvaltningsloven med kommentarer (s. 688-694), Henrik Waaben og Kristian Korfits Nielsen, Lov om behandling af personoplysninger med kommentarer (s.578f og s. 307-313), Bekendtgørelse 2000-06-15 nr. 529 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning.