Forordning 2016/679

Forholdet mellem dataansvarlig og databehandler -set i lyset af behandlingssikkerheden

Peter Gottschalck – 2012-0485

10. august 2017

Kandidatafhandling

Juridisk Institut

Aalborg Universitet

Vejleder: Søren Sandfeld Jakobsen

Antal anslag: 140.344

Summary

Over the past decade, the rapid technological development has pushed the privacy regulation to its outer boundaries. New technologies surface almost on daily basis, offering new and more efficient ways to store our personal information. Cloud Computing is one of the well-known products of the technological evolution, allowing everyone to purchase a "piece of space in the cloud".

Cloud Computing has been pointed out by the Danish Professor, Peter Blume, as one of the main reasons for the creation new General Data Protection Regulation 2016/679.

When using technologies like Cloud Computing, you are able to store all your information on a server, and when you need the information again, you access it in a few seconds, regardless where you are located. Using such a service, means that your information is stored on a server placed anywhere in the world. You might now the name of the service provider, Gmail, Dropbox etc. but often you will find it hard to find the exact location where your information are physically stored. This scenario is similar for companies and public authorities in relation to how manage the information regarding customers, clients etc.

In regards to the privacy regulation, the applicable law has strict limitations and provisions regarding how data controllers are allowed to process personal data. However, there is a lack of responsibility and provisions when it comes to the data processor. The data processor is becoming increasingly important in terms of the processing of personal data. The above-mentioned technologies has been one of the main reasons for that, but has also been caused by the increased use of outsourcing.

The new General Data Protection Regulation offers a new range of responsibilities and provisions concerning the data processor, along with an independent liability with regard to violations of the Regulation. It has been said by Peter Blume, that the Data Processor has been forced "out of the shadow", underlining the new degree of independence that characterizes the data processors role in the Regulation.

This thesis aims to clarify how the General Data Protection Regulation affects the applicable law, in terms of the current provisions regarding the security of processing.

Furthermore, the goal is to clarify how the relationship between the data controller and the data processor will be affected by the regulation, in terms of their obligations related to the security of processing.

The results of the analysis shows that although the provisions regarding the security of processing have not been changed materially, there are significant changes in terms of more clarified obligations. The General Data Protection Regulation also implements a new risk-based assessment in terms on how you comply with the rules regarding the security of processing. The analysis shows, that the data controller and the data processor, who are both directly responsible for complying with the rules, now have to implement the appropriate technical and organizational measures based on a risk-assessment. This new framework has applauded by several experts on privacy regulation, and generally seems to form a basis for a higher level of data protection.

The analysis has furthermore shown that the relationship between the data controller and data processor has become far more regulated and clarified in terms on the parties' individual responsibilities. The data controller is still in full control of the processing, however, the data processor has been given more obligations to assist the data controller. The individual liability causes the data processor to become vulnerable in terms of non-compliance, and the new regulations on the data processing agreements offers both parties a chance to create a transparent setup in regards to a given act of data processing.

Indledning

Den 25. maj 2018 træder forordning 2016/679 >>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)<< i kraft. Denne forordning er vidtrækkende, og dens størrelse og omfang vidner om et område, hvorpå der har været et markant behov for en mere ensrettet regulering.[1]

Der var gennem en længere årrække op til forordningsforslagets fremsættelse, en udbredt enighed om at en reformering af den persondataretlige regulering var påkrævet. Baggrunden for denne enighed var, at Persondatadirektivet, som er den EU-fællesskabsretlige rettesnor for gældende ret på området, i sin tid blev udformet uden hensyntagen til internettet.[2]

Den informationsteknologiske udvikling er nærmest eksploderet siden internettets fremkomst i 1995 og i dag foregår en betydeligt del af al persondatabehandling via et utal af forskellige internetbaserede services og platforme. Begreber som cloud computing, der har gjort det muligt at opbevare sine data således, at man på få sekunder har dem tilgængelige, selvom de i realiteten opbevares hos en ekstern udbyder, og Big Data som er en metode der tillader de, der formår at analysere og finde sammenhænge i ekstremt store mængder data gennem datamining, at kende forbrugermønstre ud fra en sammenkobling af alle de oplysninger, man som forbruger afgiver[3], er vundet frem, og har ændret den måde vi behandler persondata på radikalt. Et eksempel herpå er, at mere end hver tredje danske virksomhed i dag vælger at bruge cloud-computing.[4]

Peter Blume har skrevet at cloud computing har været en af de grundlæggende årsager til at databehandleren i Persondataforordningen har fået sin egen position[5], og det samme kan læses i Justitsministeriets betænkning om persondataforordningen[6]. Som det fremgår i en artikel, af Peter Blume, der blev skrevet i tilknytningen til fremsættelsen af forordningsforslaget, anfører han at

[1] Blume, P. (2017), s. 13-14
[2] Ibid., s. 15
[3] Ibid., s. 203
[4] https://www.version2.dk/artikel/mindre-end-hver-tredje-danske-virksomhed-bruger-cloud-computing-55337
[5] Blume, P. (2017), s. 204
[6] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 559

databehandleren, i forordningsforslaget, er blevet selvstændiggjort med en handlepligt, og et heraf følgende ansvar, på baggrund af brugen af cloud computing[7].

De ovenfornævnte begreber, og den øvrige informationsteknologiske udvikling, har medført at grænsen mellem den dataansvarlige og databehandleren gradvist er blevet udvisket på visse områder. Mange dataansvarlige vælger i dag at gøre brug af forskellige tjenesteudbydere, som så står for behandlingen på deres vegne. Dette skyldes både, at det i mange tilfælde kan være en økonomisk fordel, men også at mange behandlingsopgaver ganske enkelt er for krævende for den dataansvarlige.[8]

En sådan situation medfører selvsagt et behov for en fleksibel regulering, som på den ene side kan varetage den registreredes rettigheder, og på den anden side tillader de dataansvarlige, at kunne behandle personoplysninger på en effektiv og økonomisk forsvarlig facon.

Uanset hvorledes en konstellationen bag en databehandling ser ud, er det essentielt at databeskyttelsen er i højsædet, således at der ikke sker brud på datasikkerheden. I gældende ret, er den dataansvarlige pålagt ansvaret for at behandlingen overholder reglerne, og det er dennes pligt at implementere passende foranstaltninger, med henblik på at beskytte personoplysninger.

Med den nye forordning er der lagt op til et øget fokus på databehandlerrollen, herunder forholdet mellem denne og den dataansvarlige. Bestemmelserne herom, vil sammen med Persondataforordningens bestemmelser omkring behandlingssikkerhed danne rammen for dette speciale.

[7] Blume, P. (2015), s. 129
[8] Ibid., s. 114

Problemformulering

Som det fremgår af indledningen, har databehandleren i dag fået en langt større rolle, end hvad den havde for ganske få år tilbage. Teknologien og lovgivningen har medført at den dataansvarlige, i mange tilfælde, ikke længere kan rumme alle behandlinger af personoplysninger selv. Med den hastige teknologiske udvikling følger også et krav om, at man som dataansvarlig formår at sikre sig, at uvedkommende ikke får adgang til personoplysninger ved hjælp af direkte angreb, systemnedbrud eller fejlagtige videregivelser.

På denne baggrund findes det relevant, at undersøge hvorledes Persondataforordningen påvirker de gældende bestemmelser omkring behandlingssikkerheden. Med udgangspunkt i Persondataforordningens betydning for kravene til behandlingssikkerheden, findes det endvidere relevant, at foretage en analyse af det retlige forhold mellem den dataansvarlige og databehandleren, med henblik på at klarlægge ansvarsfordelingen mellem disse i relation til de forpligtelser der er relateret til behandlingssikkerheden.

Specialets problemformulering er på baggrund af ovenstående formuleret således:

"Hvilke ændringer medfører forordning 2016/679, set i forhold til de sikkerhedskrav den dataansvarlige og databehandleren er underlagt efter gældende ret? Set i lyset heraf, ønskes det afklaret hvorledes det retlige forhold mellem disse påvirkes med den nye forordning?"

Afgrænsing

Dette speciale har to primære fokusområder. Det første er behandlingssikkerhed og de krav der følger hertil. Det andet område er forholdet mellem den dataansvarlige og databehandleren, set i forhold til deres forpligtelser i relation til behandlingssikkerheden og det retlige forhold mellem dem.

Målet med specialet er at skabe et overblik over hvilke ændringer Persondataforordningen medfører for bestemmelserne om behandlingssikkerhed, set i forhold til gældende ret. På baggrund heraf vil de relevante retskilder fra henholdsvis gældende lovgivning og Persondataforordningen blive inddraget, til brug for en analyse af hvilken betydning eventuelle forskelle vil have for retstilstanden på området.

For at kunne belyse det retlige forhold mellem den dataansvarlige og databehandleren, vil de relevante retskilder i både gældende ret og Persondataforordningen blive anvendt. Der vil ikke blive foretaget en gennemgang af den registreredes rettigheder i relation til dette formål, udover hvad der findes nødvendigt for at belyse forholdet mellem den dataansvarlige og databehandleren på fyldestgørende vis.

I forbindelse med anvendelsen af bestemmelserne omkring databehandleraftaler, vil der ikke blive foretaget en uddybende gennemgang af de forpligtelser der vedrører den registreredes rettigheder. Sådanne bestemmelser vil være angivet for at danne et billede af databehandleraftalens omfang, men indholdet vil ikke blive anvendt i analysen.

Tilsynsmyndighedernes roller er ikke en del af specialets fokus, hvorfor disse kun vil blive omtalt i et omfang der er nødvendigt for at belyse databehandleren og den dataansvarliges relevante forpligtelser i henhold til problemformuleringen. De steder hvor tilsynsmyndigheden optræder, vil denne være angivet som Datatilsynet.

Grundet specialets omfang, vil reglerne omkring overførsler til tredjelande ikke blive medtaget i nærværende speciale. Emnet vil blive berørt i det omfang der er nødvendigt for at bidrage til en bedre forståelse af det retlige forhold mellem den dataansvarlige og databehandleren.

Specialet vil hovedsageligt beskæftige sig med Persondataforordningens betydning for gældende ret i Danmark, og på baggrund heraf, vil den anvendte praksis også primært være fra Datatilsynet, medmindre andet er nødvendigt for at skabe en bedre forståelse af et givent emne.

Metode

Med udgangspunkt i den retsdogmatiske metode, vil der i dette speciale blive foretaget en gennemgang af gældende ret med henblik på en analyse af Persondataforordningens betydning for bestemmelserne om behandlingssikkerhed. Der vil endvidere blive foretaget en gennemgang af gældende ret, med henblik på en analyse af hvorledes Persondataforordningen påvirker det retlige forhold mellem den dataansvarlige og databehandleren, herunder ansvarsfordelingen mellem disse i relation til de forpligtelser, der følger af bestemmelserne om behandlingssikkerheden.

Fremgangsmåden vil være således, at hvert emne indledes med en gennemgang af gældende ret indenfor området, efterfulgt af en gennemgang af Persondataforordningens bestemmelser på det pågældende område. Dette vil skabe grundlag for en analyse af hvilken betydning Persondataforordningen må forventes at få. Denne analyse vil blive foretaget løbende, og der er derfor ikke foretaget en specifik opdeling af henholdsvis analyserende og beskrivende afsnit.

Gennemgangen af gældende ret, samt fremtidig ret, skal føre en til en besvarelse af problemformuleringen, som i tråd med teorien bag den retsdogmatiske metode, vil blive besvaret objektivt, således at det er lovgivers, EU, hensigt med Persondataforordningen der lægges til grund for konklusionen.

Peter Blume har i sin udgivelse "Juridisk metodelære" angivet en række retningslinjer for hvad der udgør den gode juridiske tekst. Specialet vil i henhold til disse retningslinjer blive udformet således at opbygning, sprog og indhold gøres letforståeligt for læseren.[9]

I forbindelse med besvarelsen af problemformuleringen vil de relevante retskilder i form af den gældende regulering på området, samt vejledninger, betænkninger og administrativ praksis. Da Persondataforordningen endnu ikke er trådt i kraft, findes der hverken megen litteratur eller praksis på området. På denne baggrund vil der i forbindelse blive anvendt de tilgængelige litterære udgivelser, som vurderes at kunne give et sagligt bidrag til fortolkningen af de nye regler. De to

[9] Blume, P. (2009), s. 159-160

primære kilder til fortolkning vil være Peter Blumes bog om Persondataforordningen[10], samt Justitsministeriets betænkning om samme forordning[11]. Betænkningen er blandt andet udarbejdet i samarbejde med Datatilsynet, hvilket medfører at de fortolkningsbidrag der er anført i denne, må være i tråd med den praksis der forventes at blive anvendt efter 25. maj 2018.

Kapitel 1 - Persondataretten og den teknologiske udvikling

Historisk perspektiv

Den moderne teknologiske informationsteknologi og dennes udvikling har dannet grundlag for interessen omkring emnet persondata. I løbet af 1960'erne og 70'erne var teknologien på et niveau hvor man primært så den elektroniske informationsteknologi komme til udtryk i form af store centrale mainframe-computere, som primært blev benyttet af staten.[12] Der var altså tale om en forholdsvis eksklusiv teknologi, med en meget afgrænset kreds af brugere.

Disse store datacentraler, blev anvendt til registre indeholdende personoplysninger m.v. som derved dannede grundlaget for et behov for en regulering på dette område. Lovene blev udformet således at der ved hver eneste oprettelse af et givent register, krævede udstedelse af en specifik registerforskrift, som i lovmæssig forstand er det samme som en bekendtgørelse, som angiver hvorledes de gældende regler skulle anvendes på registret. På daværende tidspunkt var loven tidssvarende, da elektroniske registre var forbeholdt statslige institutioner og store virksomheder, hvorved disse blev holdt indenfor en ganske snæver kreds.[13] Man havde altså en situation hvor de der behandlede personoplysninger, var udvalgt ved lov og derved var der ikke mulighed for at uddelegere behandlingen, eller videregive oplysninger til andre end de, der var angivet i loven. Databehandlerbegrebet havde på denne baggrund ingen relevans.

I forbindelse med den teknologiske udviklings hastige fremskridt op gennem 1980'erne og 90'erne blev det efterhånden åbenlyst, at registerlovene ikke længere var tidssvarende, i og med at datacentraler og edb-maskiner blev langt mere udbredt[14]. Det fulgte endvidere af registerlovenes § 1, om end denne paragraf ikke var blevet håndhævet, at privatpersoner ikke må have edb-registre.

[10] Blume, P. (2017)
[11] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning
[12] Blume, P. (2017), s. 29
[13] Ibid., s.29
[14] Ibid., s. 33

Inden registerlovene blev afløst, fandtes der mere end 3000 registrerforskrifter[15], hvilket i høj grad understregede at der var behov for ny regulering på området.

I 1992 fremsatte Finansministeriet en række udspil, som havde til formål at liberalisere lovgivningen på persondataområdet betydeligt. Et særligt formål med disse udspil var blandt andet, at lette samkøring af data, med den begrundelse, at en borger ikke skulle afkræves de samme informationer fra flere myndigheder. Der var betydelige holdninger, der talte for en gennemførelse af en ændring af loven, men dette lod sig ikke gennemføre da EF d. 28 oktober 1995 udstedte Persondatadirektiv 95/46 EF[16].

Direktivet dannede grundlag for en ny måde at betragte brugen af personoplysninger på, da man fokuserede reguleringen på begrebet "behandling" af personoplysninger. Behandlingsbegrebet medførte at reguleringen ikke længere havde sigte på bestemte måder at bruge personoplysninger på, men derimod omfattede alle aktiviteter i relation til personoplysninger, hvilket var en afgørende faktor i forhold til reguleringens evne til at følge med den teknologiske udvikling. Den danske implementeringsproces var lang, og først ved det tredje lovforslag (L 147 af 9. december 1999) blev persondataloven vedtaget d. 26 maj 2000.[17]

Siden direktivets ikrafttrædelse i 1995, er den teknologiske udvikling nærmest eksploderet. Som nævnt i indledningen er mange nye begreber kommet frem siden internettets fremkomst i 1995. Disse begreber har medført et stigende pres på den persondataretlige regulering, da denne gennem flere år har vist sig at være utidssvarende og alt andet en omstillingsparat.[18]

Persondataforordningen

Persondataforordningen er resultatet af den stigende anvendelse af digitaliseret information, som i dag er en primær faktor i samfundsøkonomien. Peter Blume, har kaldt Persondata for nutidens olie, og begrundet dette med at adgangen til at bruge persondata er centralt for markedets effektivitet. På denne baggrund er det nødvendigt med en lovgivning der tillader at personoplysninger kan udveksles frit, men samtidigt sikrer at beskyttelsen af disse er tilstrækkelig.[19]

[15] Blume, P.(2017), 31
[16] Ibid., s. 34
[17] Ibid., s. 35
[18] Ibid., s. 15
[19] Ibid., s. 16

Som følge af fremkomsten af teknologier som cloud computing, der er nævnt i indledningen, er brugen af databehandlere blevet øget væsentligt. Et af hovedtrækkende ved denne Persondataforordningen er netop at disse databehandlere har fået flere selvstændige forpligtelser og et selvstændigt ansvar.[20]

Persondataforordningen medtager ikke alle detaljer i reguleringen. Dette skyldes en frygt for at, denne hurtigt ville forældes.[21] Dette ses blandt andet i forhold til sikkerhedskravene, som er behandlet i kapitlet nedenfor.

Behandlingssikkerhed

Datasikkerhed er en fundamental grundsten i databeskyttelsen, som det fremgår af ovenstående kapitel udgør det det teknologiske udvikling, og herunder det informationstekniske niveau, en konstant voksende trussel mod beskyttelsen af personoplysninger[22]. Såfremt denne sikkerhed ikke kan tilvejebringes, kan personoplysningerne blive udsat for angreb både indefra og udefra hvilket, ifølge Peter Blume, medfører, at lovgivningen ikke har en praktisk betydning, men blot optræder som en række fine ord[23]. Som det også fremgår af både indledningen og ovenstående kapitel, har begreber som cloud computing medført, at det kan være svært at overskue hvor hurtigt personoplysninger kan skifte hænder.

"Det er en almindelig erkendelse, at det kun er muligt at opnå det tilstræbte databeskyttelsesniveau, såfremt den dataansvarlige tilvejebringer en tilstrækkeligt virkende beskyttelse."[24] *Peter Blume, 2017*

Den konstant frembrusende teknologiske udvikling udgør en udfordring for både de registrerede, de dataansvarlige, databehandlere, lovgivere og alle andre der på den ene eller anden måde er forbundet til persondatarettens uigennemskuelige univers.

Som det fremgår af ovenstående citat, er det kun muligt at opnå et ønsket beskyttelsesniveau såfremt man tilvejebringer en tilstrækkelig beskyttelse. Begrebet tilstrækkelig beskyttelse er

[20] Blume, P. (2017), s. 61
[21] Ibid., s. 44
[22] Ibid., s. 119
[23] Ibid., s. 118
[24] Ibid., s. 118

anvendt i den nye persondataforordning, og det vidner også om de begrænsede muligheder for at regulere specifikt, når det kommer til databeskyttelse. Den ene dag kan en given foranstaltning være skudsikker og næste dag kan den være forældet. Dermed står den dataansvarlige, eller databehandleren, med ansvaret for at navigere rundt i blandt de tilgængelige sikkerhedsforanstaltninger, i kampen for at opnå en tilstrækkelig beskyttelse.

Ovenstående danner baggrund for nedenstående gennemgang af de sikkerhedskrav der følger af henholdsvis gældende ret og persondataforordningen. Herudover er der medtaget en gennemgang af to nye forpligtelser, der relaterer sig til datasikkerheden, databeskyttelse gennem design og – standardindstillinger.

Krav om behandlingssikkerhed

Gældende ret

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 jf. Persondatalovens § 41, stk. 3, 1. pkt. Af § 41, stk. 3, 2.pkt følger det, at denne forpligtelse ligeledes gælder for databehandlere.

Denne bestemmelse har sit udgangspunkt i Persondatadirektivets artikel 17, stk. 1, 1. afsnit, og det følger af præambelbetragtning nr. 46 til Persondatadirektivet at de ovenfor nævnte foranstaltninger både skal træffes under udformningen og under iværksættelsen af en behandling. Det følger af Persondatadirektivets præambelbetragtning nr. 10, at implementeringen af direktivet i national lovgivning ikke må føre til en forringelse af den beskyttelse som denne allerede yder. Formålet er derimod at sikre et højt beskyttelsesniveau overalt i EU. På baggrund heraf har Registerudvalget også udtrykt at det er en forudsætning for direktivets implementering at dette ikke ville føre til en forringelse af beskyttelsen[25].

Hverken Persondataloven eller Persondatadirektivet indeholder en nærmere beskrivelse af hvilke foranstaltninger man som dataansvarlig skal træffe. Dette kan dog læses af Kommissionens

[25] Betænkning nr. 1345/1997 om behandling af personoplysninger s. 325-326

bemærkninger til direktivudkastet af 24. september 1990, at de tekniske datasikkerhedsforanstaltninger omfatter:

Sikkerhedsforanstaltninger med hensyn til adgang til databehandling og til datalagre, identifikationskoder til personer, der har adgang hertil, edb-sikkerhedsforanstaltninger som f.eks. brug af password for at få adgang til edb-registre, omsættelse af data til kode (kryptering) og kontrol med hacking og andre usædvanlige aktiviteter i edb-registret. Gennem organisatoriske foranstaltninger skal den dataansvarlige efter Kommisionens bemærkninger tage proceduremæssige skridt inden for den offentlige myndigheds eller erhvervsvirksomheds hierarki, f.eks. ved at etablere forskellige autorisationsniveauer for adgangen til registret.[26]

Af Registerudvalgets betænkning nr. 1345 fremgår det, at Registerudvalget, på baggrund af ovenstående bemærkninger, finder at sikkerhedsforanstaltninger grundlæggende bør indeholde elementerne *fysisk sikkerhed, organisatoriske forhold, systemtekniske forhold, samt uddannelse og instruktion.*[27]

Herudover fremgår det at visse sikkerhedsforanstaltninger, afhængigt af den givne situation, kan komme på tale. Disse foranstaltninger er *sikring af bygninger og lokaler, formel autorisation af brugerne, adgangskoder (password), benyttelsesstatistik, logning af transaktioner, registrering af uautoriserede adgangsforsøg, kryptering, regler for udskrifter, regler for destruktion, uddannelse, samt tilsyn.* [28]

I forbindelse med de ovenfor nævnte tekniske foranstaltninger, fremgår det, af Persondatadirektivet, at der ved igangsættelsen af disse, skal foretages en afvejning af risikoen, der er forbundet med behandlingen, i forhold til det aktuelle tekniske niveau, samt de omkostninger der er forbundet med foranstaltningerne jf. artikel 17, stk. 1, 2. afsnit.

Datatilsynet har siden 2014 udgivet en række IT-sikkerhedstekster, hvori der er fokus på særlige sikkerhedsmæssige problemstillinger i IT-regi. Her er der tale om praktiske sikkerhedsmæssige problemstillinger, som opstår i forbindelse med behandling af personoplysninger.[29] Et eksempel

[26] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 473
[27] Betænkning nr. 1345/1997 om behandling af personoplysninger, s. 325-326.
[28] Ibid.
[29] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 473

herpå er udgivelser omkring Krypteret dataudveksling via websider – set fra den dataansvarliges synsvinkel, hvori man som dataansvarlig vil kunne finde anbefalinger om god praksis på det konkrete område[30].

I relation til ovenstående udgivelse om kryptering, kan der henvises til en sag fra 2004, hvor Biblioteksstyrelsen havde fremsendt en forespørgsel til Datatilsynet om, hvorvidt det var acceptabelt at man fra bibliotek.dk udsendte reserverings- og kvitteringsmeddelelser, indeholdende oplysninger om låneren og det bestilte/lånte materiale, via ikke-krypteret e-mail. Datatilsynet udtalte, at man betragtede informationer om borgeres lån/reservationer som fortrolige oplysninger, og henviste indstillede i den forbindelse til at man i overensstemmelse med sikkerhedsbekendtgørelsens § 14, implementerede tekniske foranstaltninger som tillod reserverings- og kvitteringsmeddelelserne at blive udsendt via en krypteret linje. Det bør dog bemærkes, at Datatilsynet, grundet den begrænsende brug af krypterede e-mail i befolkningen i 2004, tilkendegav at man accepterede at der fortsat blev anvendt en ikke-krypteret linje i en periode på fem år, hvor Bibiliotheksstyrelsen i mellemtiden kunne arbejde på en teknisk løsning på problemet.

Af Persondatalovens § 41, stk. 4 følger "krigsreglen" som foreskriver at der for oplysninger som behandles for den offentlige forvaltning, og som er af særlig interesse for fremmede magter, skal træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.

I relation til databehandlere, fremgår det af Persondatalovens § 42, stk. 1, at den dataansvarlige ved brugen af en databehandler, skal sikre sig at denne kan overholde kravene i § 41, stk. 3-5, samt udøve tilsyn med, at dette rent faktisk sker.

Hvis behandlingen af personoplysninger overlades til en databehandler, pålægger bestemmelsen, at den dataansvarlige skal sikre sig, at databehandleren også opfylder kravene til behandlingssikkerhed i § 41, stk. 3-5, herunder også bestemmelser i sikkerhedsbekendtgørelsen, hvis der er tale om behandling for den offentlige forvaltning. Endvidere pålægger bestemmelsen den dataansvarlige at føre kontrol med, at databehandleren træffer de nødvendige

[30] Datatilsynet, IT-sikkerhedstekst ST13, 2016

sikkerhedsforanstaltninger.[31] Dette medfører at den dataansvarlige, naturligvis, ikke blot kan overlade en behandling til en databehandler uden at foretage et aktivt tilsyn med denne. I kapitlet omkring forholdet mellem den dataansvarlige og databehandleren, er der angivet et eksempel fra Datatilsynet, på en manglende udøvelse af den ovenfor omtalte tilsyn.

Der er i Persondataloven forskel på hvorledes datasikkerhed skal overholdes i den offentlige og private sektor. For den offentlige sektor er der udstedt en bekendtgørelse, som indeholder specifikke krav til hvorledes man skal overholde sikkerhedskravene, hvor det for den private sektors vedkommende er op til den enkelte dataansvarlige at vurdere hvorledes man indrette sin behandling, således at den overholder reglerne.

Nedenfor følger en gennemgang af reglerne i sikkerhedsbekendtgørelsen.

Sikkerhedsbekendtgørelsen

Justitsministeren kan på baggrund af Persondatalovens § 41, stk. 5, udstede nærmere regler omkring sikkerhedsforanstaltninger. Årsagen til denne bemyndigelse, skal findes i at man ikke anså det for praktisk muligt at angive alle de nødvendige sikkerhedsforanstaltninger på tværs af de forskellige sektorer, hvorfor det syntes mere korrekt at anvende denne model.[32]

Beføjelsen i denne bestemmelse blev brugt til at udstede sikkerhedsbekendtgørelsen med nr. 528 af 15. juni 2000, som er gældende for behandling af personoplysninger, som foretages for den offentlige forvaltning helt eller delvist ved hjælp af elektronisk behandling jf. bekendtgørelsens § 1. Denne er efterfølgende blevet ændret ved bekendtgørelse nr. 201 af 22. marts 2001 og samme år udgav Datatilsynet en vejledning til bekendtgørelsen.[33]

Den praktiske anvendelse af bekendtgørelsens behandlingsregler foretages på baggrund af om der er tale om oplysninger der er omfattet af anmeldelsespligten i Persondatalovens kapitel 12 til Datatilsynet. Dette vil sige at såfremt der er tale om oplysninger der ikke er omfattet af anmeldelsespligten, skal der behandles i overensstemmelse med bestemmelserne i kapitel 1 og kapitel 2. Såfremt oplysningerne er omfattet af anmeldelsespligten, skal behandlingen også være i overensstemmelse med kapitel 3, med enkelte undtagelser.

[31] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 479
[32] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 475
[33] Datatilsynets vejledning nr. 37 af 2. april 2001

Bekendtgørelsens § 3 har samme krav om tekniske og organisatoriske foranstaltninger som Persondatalovens § 41, stk. 3, dog med den undtagelse at sidste punktum "Tilsvarende gælder for databehandlere". Af Datatilsynets vejledning til § 3, fremgår det at man kan finde en mere dækkende vejledning om etablering af tekniske og organisatoriske foranstaltninger i forbindelse med elektronisk databehandling i Dansk Standard DS 484, Norm for edb-sikkerhed.[34] Denne er dog blevet afløst af informationssikkerhedsstandarden ISO 27001, som statslige myndigheder skal følge og som offentlige myndigheder skal følge principperne i.[35]

Udover behandlingsbestemmelserne i kapitel 1, indeholder sikkerhedsbekendtgørelsen endvidere en række mere specifikke regler vedrørende sikkerhed på områderne:

Udarbejdelse og kontrol af uddybende sikkerhedsregler, instruktion af medarbejdere, databehandleraftaler, pc-arbejdspladser uden for den dataansvarlige myndigheds lokaliteter, sikring af de fysiske rammer, reparation og service af dataudstyr, herunder salg og kassation af anvendte datamedier, ind- og uddatamateriale, som indeholder personoplysninger, autorisation og adgangskontrol og eksterne kommunikationsforbindelser.

Disse regler findes i bekendtgørelsens kapitel 2, og der er uddybende krav under hvert punkt, som blandt andet medfører at myndigheden skal fastsætte interne retningslinjer for hvorledes man overholder loven, herunder de organisatoriske forhold. Retningslinjerne skal også omfatte organiseringen i forhold til sikkerheden, herunder adgangskontrol, autorisation og kontroller heraf jf. sikkerhedsbekendtgørelsens § 5.

Myndigheden skal endvidere fastsætte instrukser for anvendelse af IT-udstyr, og fastsætte procedurer for bortskaffelse af oplysninger, reparation af IT-udstyr, samt for hvorledes man indretter og bruger en hjemmearbejdsplads efter Persondataforordningens regler. Alt dette følger af sikkerhedsbekendtgørelsens § 5, som ikke udgør en udtømmende liste, men eksempler på hvorledes man kan overholde kravene. Som det er nævnt længere oppe har myndigheden også pligt til at instruere sine medarbejdere i at behandle personoplysninger i overensstemmelse med lovgivningen jf. sikkerhedsbekendtgørelsens § 6. Herudover er det også et krav, at man indgår

[34] Datatilsynets vejledning nr. 37 af 2. april 2001
[35] Den fælles offentlige digitaliseringsstrategi for 2016-2020

databehandleraftaler med de databehandlere anvender, således at man kan sikre sig at de overholder reglerne jf. § 7.

I relation til den risiko der er forbundet med menneskelige handlinger, herunder undladelser, fejl mv, samt ovenstående bestemmelse om databehandleraftaler, kan der nævnes en sag fra Odense Kommune, hvor fundet af 19 sagsmapper med følsomme personoplysninger i en container i Vollsmose, medførte kritik fra Datatilsynet, som påpegede at man ikke havde udvist den fornødne omhu der er krævet efter Persondatalovens § 41, stk. 3. I denne sag var den en privat leverandør, som kommunen havde indgået aftale med, der havde aflæsset mapperne i containeren. Sagen omhandlede dermed en databehandler, og kritikken fra Datatilsynet gik bl.a. på at denne ikke havde udøvet sine forpligtelser i relation til sikkerhedsbekendtgørelsens bestemmelser om instruktion af medarbejdere og databehandleraftaler.[36]

Lovens kapitel 3 indeholder, som tidligere nævnt, en række yderligere krav som stilles til behandlinger der er omfattet af anmeldelsespligten i Persondatalovens kapitel 12. Disse krav vedrører områderne *autorisation og adgangskontrol, kontrol med afviste adgangsforsøg og logning.*

Som tidligere nævnt gælder sikkerhedsbekendtgørelsen kun for offentlige dataansvarlige, og dermed har Justitsministeren stadig til gode at udstede en uddybende bekendtgørelsen til den private sektor. Det fremgår dog flere steder, at udgangspunktet er, at man stiller samme krav til private dataansvarlige, som sikkerhedsbekendtgørelsen stiller til offentlige. Dette er blandt andet nævnt i den kommenterede persondatalov[37], og Datatilsynet har ligeledes udvist gennem praksis, at dette er tilfældet i en sag, hvor man konkret opfordrede en privat virksomhed til at tilrettelægge sine sikkerhedsforanstaltninger ud fra sikkerhedsbekendtgørelsen[38]. Det må dog kunne antages, at en dataansvarlig, kan anvende de foranstaltninger fra bekendtgørelsen som findes relevante i relation til en given behandling, og at denne ikke er låst på samme måde som de offentlige dataansvarslige. Det er endvidere relevant at bemærke, at det efter Persondataloven ikke er givet, at man som privat skal følge sikkerhedsbekendtgørelsens krav, såfremt man kan opfylde lovens krav om behandlingssikkerhed på anden vis.

[36] Datatilsynets j.nr. 2011-632-0104
[37] Waaben, H m.fl., 2015, s. 556
[38] Datatilsynets j.nr. 2013-631-0053

Sikkerhedsbekendtgørelsen udgør, som ovenfor nævnt, ikke en udtømmende bestemmelse, men skal derimod suppleres med de udstedte vejledninger og de heri nævnte standarder, samt bl.a. en risikovurdering af hvad der er specifikt er nødvendigt under en given behandling, for at kunne sikre personoplysningerne på tilfredsstillende vis.[39] Det skal dog bemærkes, som det, af Henrik Udsens IT-Ret, fremgår at Datatilsynet antager at sikkerhedsbekendtgørelsen i vidt omfang vil være udfyldende for hvad der udgør "fornødne tekniske og organisatoriske sikkerhedsforanstaltninger" i private virksomheder[40].

Persondataforordningen

Persondataforordningens bestemmelser om behandlingssikkerhed findes i artikel 32. Af Artikel 32, stk. 1, fremgår det at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål, samt risiciene af varierende sandsynlighed og for alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

I litra a-d i denne bestemmelse oplistes en række foranstaltninger, som vil blive gennemgået nedenfor.

Litra a omhandler pseudonymisering og kryptering af personoplysninger. Det første led i bestemmelsen, pseudonymisering, beskrives i præambelbetragtning nr. 28 som værende en foranstaltning, som kan mindske risikoen for de berørte registrerede og gøre det lettere for dataansvarlige og databehandlere at opfylde deres databeskyttelsesforpligtelser. Det angives endvidere at det ikke er tanken med den udtrykkelige indførelse af pseudonymisering i Persondataforordningen, at udelukke andre databeskyttelsesforanstaltninger. I Persondataforordningens artikel 4, defineres pseudonymisering som:

"behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske

[39] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 477
[40] Udsen, H, (2016), s. 354

foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person".

Det andet led i litra a, kryptering, omhandler omsættelse af data til kode, og kan såfremt den er korrekt implementeret, medvirke til at mindske risikoen for manglende fortrolighed, integritet, uafviselighed og autentifikation.[41]

Litra b omhandler evnen til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og –tjenester. Af Justitsministeriets betænkning nr. 1565 fremgår det at disse begreber skal forstås på følgende måde:

"Med udtrykket integritet sigtes bl.a. til, at det er muligt at validere, om data på disse systemer er korrekte, pålidelige, nøjagtige og/eller fuldstændige.

For så vidt angår behandlingssystemer og -tjenesters tilgængelighed sigtes bl.a. til, at behandlingssystemer og -tjenester og data i disse er tilgængelige ved anmodning fra autoriseret bruger, eksempelvis ved at sikre en velfungerende backup eller dublerede systemer altafhængig af, om det er relevant. Det er normalt en forudsætning, at der er fastlagt organisatoriske processer for, hvorledes disse opgaver udføres, og hvordan f.eks. backup testes.

Med udtrykket robusthed sigtes bl.a. til at sikre behandlingssystemer og -tjenesters tekniske og organisatoriske modstandsdygtighed, f.eks. ved at sikre dem imod skadelige hændelser. Der kan f.eks. sikres imod udfald ved dublerede diske, køling, nødstrømsanlæg, automatisk brandslukning, mv. alt afhængig af, om det er relevant.

Med udtrykket vedvarende menes, at evnen til at sikre fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og –tjenester ikke blot skal opfyldes én gang, men er en løbende teknisk og organisatorisk forpligtelse. "[42]

Litra c omhandler evnen til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse. Her menes der hvorledes man sikrer sig at man kan genoprette adgang til personoplysningerne i tilfælde af udefrakommende angreb,

[41] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 481
[42] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 481-482

skader eller andre hændelser som kan lukke for adgangen. I Justitsministeriets betænkning til Persondataforordningen nævnes bl.a. planer for alternative datakommunikationslinjer og muligheder for backup. [43]

Litra d omhandler en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed. Som det relativt klart kan læses ud af formuleringen, tænkes der her på at man fastlægger rutiner for tests af sine sikkerhedsmæssige foranstaltninger, hvad enten det er firewalls, krypterede forbindelser, backupsystemer, alternative datalinjer, adgangsbegrænsende foranstaltninger m.v., og foretager evalueringer og vurderinger ud fra disse tests.

De ovenstående foranstaltninger i litra a-d omhandler den tekniske del af foranstaltningerne i artikel 32, stk. 2.

Man kan jf. artikel 32, stk. 3, vælge at følge et godkendt adfærdskodeks, som omhandlet i artikel 40 eller en godkendt certificeringsmekanisme, som omhandlet i artikel 42, som et element til at påvise at man overholder kravene i artikel 32 stk. 1. En nærmere gennemgang af betydningen af at anvende sådanne frivillige virkemidler, følger i afsnittet om forholdet mellem den dataansvarlige og databehandleren.

Den organisatoriske del af foranstaltninger kan eksempel komme til udtryk i form af indretningen af en arbejdsplads, hvor man via denne indretning udelukkende giver adgang til de givne personoplysninger til en afgrænset gruppe af medarbejdere.

Man kan, ifølge Peter Blume, også komme til udtryk i særlige instrukser til personalet[44]. Han skriver i relation hertil:

"Det kan herved fremhæves, at det netop er den menneskelige faktor, der ganske ofte er det svage led, og som foranlediger sikkerhedsbrud. Det er på sin vis lettere at styre en computer end et menneske. Errare humanum est."[45]

[43] Ibid., s. 482
[44] Blume, P. (2017) s. 120
[45] Ibid., s. 120-121

I relation til denne bemærkning, kan der henvises sagen om Odense Kommune, som er nævnt i kapitlet om Sikkerhedsbekendtgørelsen, hvor en manglende instruktion, blandt andre ting, blev lagt til grund for et brud på persondataloven.

Der skal ved tilrettelæggelsen af datasikkerheden tages hensyn til det aktuelle teknologiske niveau hvilket medfører, at man vil skulle foretage en vurdering af risikoen ved en given behandling set i forhold til de ressourcemæssige omkostninger implementeringen af en række foranstaltninger vil medføre.

Dette betyder, at der ikke altid foreligger et krav om at man skal benytte state of the art-teknologi. Der er dog en minimumsgrænse og Peter Blume nævner som et eksempel, at man i situationer hvor der behandles særligt integritetskrænkende personoplysninger, typisk de som er omfattet af Persondataforordningens artikel 9 og 10, vil skulle opretholde et særligt højt niveau, hvilket kan medføre at en dataansvarlig kan være nødt til at afstå fra at foretage den konkrete behandling, grundet manglende ressourcer.[46]

Som det fremgår af ovenstående, tilbyder Persondataforordningen, i lighed med gældende, relativt få konkrete eksempler på relevante sikkerhedsforanstaltninger. Årsagen hertil må dog findes i den teknologiske udvikling, som er omtalt i specialets indledning. Persondataretten er nødt til at være omstillingsparat og det er nødvendigt at den kan tilpasse sig nye teknologier, således at den ikke bliver utidssvarende før den endnu er trådt i kraft.

Datatilsynet medtog i årsberetningen for 2012, en definition af begrebet cloud computing:

"Cloud computing kan defineres som en model for internetbaseret adgang til en delt puljeaf konfigurerbare it-ressourcer (net, servere, datalagre, programmer og services), der hurtigt kan etableres og afvikles med en minimal indsats eller interaktion med tjenesteleverandøren. Et eksempel på en cloud-løsning er software udbudt som en service, der ikke skal installeres eller vedligeholdes på kundens egne systemer, men i stedet ligger hos leverandøren og tilgås via brugerens internetbrowser. Som eksempel herpå kan nævnes e-mailtjenester som gmail og hotmail,

[46] Blume, P. (2017), s. 120

som er tjenester, der tilgås af brugeren via en internetbrowser, og hvor data ikke gemmes på brugerens egen computer, men i et datacenter hos cloud-leverandøren (i "skyen")."[47]

Ved gennemlæsning af ovenstående citat, fremgår det relativt klart, hvor vanskeligt det ville være at opstille specifikke sikkerhedskrav til dette ene område. Når dette så sammenholdes med det faktum, at informationsteknologien i dag udklækker teknologiske begreber og muligheder på samlebånd, synes opgaven umulig, da man i givet fald ville have låst lovgivningen fast til forældede teknologier på relativt kort tid.

Det må derfor, på baggrund af de ovenstående bestemmelser, og det faktum, at de konkrete tekniske foranstaltninger der nævnes, er meget begrænsede, kunne antages, at dataansvarlige vil kunne søge råd i de råd og vejledninger der udsendes fra Datatilsynet, samt sikkerhedsbekendtgørelsens bestemmelser. Denne antagelse beror på, at Persondataforordningen på en lang række områder bygger på de samme principper som gældende ret jf. fx Persondataforordningens artikel 5, hvoraf det fremgår af de grundlæggende principper overordnet set fremstår uændret i forhold til Persondatadirektivets bestemmelser herom. At Persondataforordningen på mange områder viderefører en stor del af gældende ret, kommer også kommer til udtryk i forhold til sikkerhedskravene jf. ovenstående gennemgang.

Peter Blume har udtrykt bekymring over at man i Persondataforordningen har fjernet Kommissionens mulighed for at udstede delegerede retsakter og gennemførelsesakter, som ellers ville give mulighed for at specificere sikkerhedskravene yderligere. Denne mulighed forelå ellers i Kommissionens 2012-forlsag artikel 30 (3-4)[48].

Det fremgår af justitsministeriets betænkning at man som dataansvarlig ikke har en forpligtelse til at efterleve sikkerhedskravene alene rent teknisk, såfremt at man ud fra en konkret vurdering finder at det er tilstrækkeligt at anvende organisatoriske foranstaltninger. En sådan organisatorisk foranstaltning i relation hertil være at man omskoler eller underviser sit personale i at anvende de nuværende it-systemer på en måde som gør, at sikkerhedskravene vurderes at være opfyldt.[49]

[47] Datatilsynet, Årsberetning 2012, s. 40
[48] Blume, P. (2017), s. 119
[49] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 483

Som det fremgår af ovenstående er der i forhold til formuleringen af bestemmelserne om behandlingssikkerhed i artikel 32, ikke de store ændringer at spore i formuleringen i forhold til gældende ret. Det nye, som det fremgår af bl.a. Justitsministeriets betænkning nr. 1565 og Peter Blumes bog "Den nye persondataret", er fremhævelsen af kravet om en risikobaseret tilgang til persondatasikkerhed.

Risikobaseret tilgang til behandlingssikkerheden

Selvom man i artikel 32 finder konkrete foranstaltninger som kan være relevante i forhold til databeskyttelse, er bestemmelsen ikke udtømmende. Dette betyder at man til trods for at disse foranstaltninger er nævnt i Persondataforordningen, ikke kan være sikker på at man lever op til Persondataforordningens krav til databeskyttelse, alene på baggrund af overholdelse af disse.

Derfor skal man, som dataansvarlig, foretage en konkret vurdering ved hver enkelt behandling, hvor man ud fra den risici behandlingen medfører, for fysiske personers rettigheder og frihedsrettigheder, fastsætter hvilke foranstaltninger der er nødvendige for at sikre en tilfredsstillende beskyttelse.

Charlotte Bagger Tranberg har udtrykt følgende om den risikobaserede tilgang til behandlingssikkerheden:

"Det er almindeligt anerkendt, at der ikke kan opnås 100 procent sikkerhed, selvom alle de ovenfor nævnte sikkerhedsparametre opfyldes. Det er en forudsætning, at der tilvejebringes et tilstrækkeligt sikkerhedsniveau efter en afvejning af det aktuelle tekniske niveau og omkostningerne forbundet med iværksættelsen i forhold til de risici, der er forbundet med behandlingen og arten af de beskyttede oplysninger."[50]

Ifølge Peter Blume, er dette øgede fokus på risikovurdering, et positivt element i Persondataforordningen.[51] Han fremhæver at risikoorienteringen tilføjer dynamik til persondataretten, hvilket, til trods for at det medfører mere arbejde for den dataansvarlige og de der fører tilsyn, er en god måde at underbygge god databeskyttelse.[52]

[50] Tranberg, Charlotte Bagger, (2014), s. 1
[51] Blume, P. (2017), s. 207
[52] Ibid., s. 208

Dette underbygger han i samme kapitel ved at beskrive risiko som et dynamisk moment, som kan medføre fleksibilitet og nuancering, og som taler for en differentiering, der medfører, at man ikke kan skære alle tilfælde over samme kam.[53]

Han fremhæver at der med det øgede fokus på risikomomentet, skabes en mulighed for at gøre persondataretten proaktiv[54], hvilket underbygges yderligere af Persondataforordningens krav om beskyttelsen gennem design- og standardindstillinger jf. afsnittet " Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger" nedenfor.

Peter Blumes antagelser om at Persondataforordningens fokus på risikovurderingen, understøttes af Justitsministeriets betænkning, hvoraf det fremgår af man formoder at den risikobaserede tilgang til behandlingssikkerhed i praksis vil kunne danne grundlag for en højere behandlingssikkerhed sammenlignet med den der følger af Persondataloven og den dertilhørende sikkerhedsbekendtgørelsen, blandt andet på baggrund af at de foranstaltninger der implementeres, må antages at blive implementeret mere målrettet, grundet den forudgående risikovurdering.[55]

Som det anføres i Justitsministeriets bekendtgørelsen, er den risikobaserede tilgang til beskyttelse ikke et ukendt fænomen. Der nævnes som eksempel, den ovenfor nævnte, informationssikkerhedsstandard, ISO 27001, som beskriver en række krav for hvad der udgør et dækkende informationssikkerheds-ledelsessystem, også kaldet ISMS. Et sådant system har til formål at sikre en *risikobaseret*, effektiv og fleksibel styring af sikkerheden.[56]

I forhold til den ovenfor nævnte risikoafvejning fremgår det af artikel 32, stk. 2, at der er særlige momenter der skal lægges vægt på i vurderingen. Det er angivet, at man skal foretage en vurdering af hvilke foranstaltninger, der er nødvendige for at undgå hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse eller at der gives adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Det fremgår af bestemmelsen at det navnlig er de momenter man skal vurdere ud fra, hvilket betyder at der ikke er tale om en komplet eller udtømmende oplistning af hvad der skal indgå i

[53] Blume, P. (2017), s. 207
[54] Ibid.
[55] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 486
[56] Ibid., s. 486

risikovurderingen. Her må den dataansvarlige igen søge hjælp i de udstedte vejledninger på området, eller i de konkrete eksempler der findes i gældende ret.

I betænkningen er der udarbejdet en vejledende fire trins guide, som vil kunne indgå i den dataansvarliges overvejelser, når denne skal vurdere hvorledes der, rent praktisk, skal gennemføres passende tekniske og organisatoriske foranstaltninger jf. Persondataforordningens krav hertil. Disse fire trin består af en Identifikation og vurdering af risici, hernæst en Identifikation af mulige foranstaltninger. Dette efterfølges af en gennemgang af hvilke foranstaltninger som imødegår relevante risici, så et passende sikkerhedsniveau opnås, og slutteligt en implementering af de foranstaltninger det besluttes at gennemføre.[57]

Sagen om Odense Kommunes påtænkte brug af cloud-løsning

Der findes i Datatilsynets praksis, en udtalelse vedrørende netop risikovurderingen i forbindelse med etableringen af sikkerhedsforanstaltninger. Udtalelsen er baseret på gældende ret, men jf. ovenstående analyse, er de grundlæggende principper vedrørende behandlingssikkerhed ikke væsentligt forskellige. Sagen vurderes at være særligt relevant, da den vedrørende brugen af en cloud-leverandør, og dermed berører de centrale elementer i dette speciale. Sagen indeholder flere interessante aspekter i forhold til dette speciale, hvorfor den vil blive anvendt igen i afsnittet omkring databehandleraftaler.

I forbindelse med denne sag, hvor Odense Kommune havde fremsendt anmodning om Datatilsynets forudgående udtalelse i forbindelse med dennes påtænkte anvendelse af en online kontorpakke fra Google Apps til kalender og dokumenthåndtering.[58]

I relation til overholdelsen af de sikkerhedskrav der følger af gældende ret, understregede Datatilsynet indledningsvist, at risikovurderingen er essentiel i relation til overholdelsen af disse krav.

"For at leve op til persondatalovens sikkerhedskrav, må den dataansvarlige efter Datatilsynets opfattelse foretage en risikovurdering i forhold til de forskellige aspekter af en mulig cloud-løsning, der påtænkes anvendt til behandling af følsomme personoplysninger. "[59]

[57] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 487
[58] Datatilsynets j.nr. 2010-52-0138
[59] Ibid.

Selvom Odense Kommune anførte at der var blevet foretaget en risikovurdering, ud fra DS-484 standarden, dog med mindre modifikationer, kunne Datatilsynet ved gennemgangen af denne vurdering konstatere at der forelå flere alvorlige mangler.[60]

Datatilsynet fandt det først og fremmest problematisk, at Odense Kommune ikke havde foretaget en risikovurdering med fokus på den specifikke kontekst oplysningerne ville blive behandlet i.

Det fremgik endvidere, at Odense Kommune havde undladt at foretage en vurdering af den teknologi der blev anvendt i den påtænkte cloud-løsning. I relation hertil kunne Datatilsynet konkludere, at der ikke blev foretaget kryptering, således at de oplysninger der blev opbevaret hos databehandleren, ikke var omfattet af en sådan beskyttelse.[61] Datatilsynet udtalte på den baggrund:

"Odense Kommune har ikke i det fremsendte materiale foretaget en vurdering af risici forbundet med manglende kryptering hos Google Ireland Limited og Google Inc.'s datacentre. Dette er således et eksempel på et punkt, hvor Odense Kommune efter Datatilsynets opfattelse er indstillet på i givet fald at løbe en uafklaret risiko." [62]

Datatilsynet fandt på ovenstående baggrund ikke, at Odense Kommune havde levet op til sine forpligtelser efter Persondatalovens § 41, stk. 3, og man henviste i samme ombæring til at man i forbindelse med sådanne risikovurderinger, anvendte en specifik fremgangsmåde.[63] Modellen for den nævnte fremgangsmåde kan findes i en publikation fra ENISA, med titlen "Cloud computing - Benefits, risks and recommendations for information security", på side 71-82. Modellen vil ikke blive gennemgået nærmere i dette speciale.

Den ovenstående sag falder i tråd med det der synes at være hovedelementet i den risikovurdering, der har fået en større rolle i Persondataforordningen; nemlig at selve risikovurderingen skal være sagligt funderet og baseres på den kontekst som oplysningerne behandles ud fra. Justitsministeriets vejledende 4-trins guide virker som et nyttigt redskab til at sikre, at den dataansvarlige og databehandleren formår at opfylde deres forpligtelser korrekt. Det må i hvert fald, på baggrund af ovenstående sag, kunne udledes at der med Persondataforordningen er opstillet større

[60] Datatilsynets j.nr. 2010-52-0138
[61] Ibid.
[62] Ibid.
[63] Ibid.

forventninger til risikovurderingen, og særligt evnen til at iagttage de særlige risici, der er forbundet med teknologier som cloud-computing mv.

Som det fremgår af ovenstående, står den dataansvarlige, og databehandleren, med en udfordrende opgave, i relation til at skulle foretage risikovurderinger på hver enkelt behandling. Der findes dog en lang række udgivelser fra Artikel 29-gruppen, som vejleder i identifikation af risici i forbindelse med anvendelsen af en række nye teknologier. I relation til indledningen, kan det nævnes at der blandt andet er udstedet vejledninger omkring cloud-computing[64]. Herudover kan der også søges inspiration i IT-sikkerhedsteksterne fra Datatilsynet, som nævnt længere oppe, og det må antages at sådanne vejledninger vil komme fra flere sider i en lind strøm, når Persondataforordningen træder i kraft. Herudover vil Datatilsynets udtalelser i sager som den ovenfor gennemgåede også være brugbare, og hen ad vejen vil ny praksis selvsagt være med til at skabe en bedre forståelse af Persondataforordningens rammer for behandlingssikkerheden.

To nye forpligtelser i relation til datasikkerheden

Databeskyttelse gennem design

Af Persondataforordningens artikel 25, stk. 1, fremgår det, at den dataansvarlige under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, som behandlingen indebærer, både på tidspunktet for fastlæggelse af midlerne til behandling og på tidspunktet for selve behandlingen gennemfører passende tekniske og organisatoriske foranstaltninger, såsom pseudonymisering, som er designet med henblik på effektiv implementering af databeskyttelsesprincipper, såsom dataminimering, og med henblik på integrering af de fornødne garantier i behandlingen for at opfylde kravene i denne forordning og beskytte de registreredes rettigheder.

Af justitsministeriets betænkning nr. 1565, fremgår det at begrebet ”databeskyttelse gennem design skal forstås bredt, hvilket betyder at det både omfatter den tekniske og de organisatoriske foranstaltninger. Det antages derfor at der i begrebet design både kan være tale om opbygning af et IT-system og den organisatoriske opbygning hos databehandleren.[65]

[64] Artikel 29-gruppen, udtalelse 05/2012 om Cloud Computing
[65] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 416

Det fremgår endvidere af justitsministeriets betænkning, at man, på baggrund af ordlyden i artikel 25, stk. 1, må antage at foranstaltningerne skal gennemføres både på "tidspunktet for fastlæggelse af midlerne til behandling" (forberedelsesfasen) og "på tidspunktet for selve behandlingen" (den dag hvor behandlingen påbegyndes).[66] Det antages, i betænkningen, derfor at bestemmelsen medfører en forpligtelse for den dataansvarlige til, allerede i forberedelsesfasen, at have fokus på de relevante foranstaltninger, som skal sikre at Persondataforordningen overholdes[67], hvilket er en nyskabelse i forhold til gældende ret.[68]

Justitsministeriet gav på deres stormøde om Persondataforordningen d. 9 februar 2017, udtryk for at artikel 25, stk. 1, ikke var en forpligtelse til noget bestemt, men derimod en generel overvejelsesforpligtelse for den dataansvarlige, til at tænke databeskyttelse ind i forberedelsesfasen af en behandling.[69]

Bestemmelsen indebærer, ifølge Peter Blume, ikke en forpligtelse til at benytte state of the art-teknologi, da kravet udelukkende går på at teknologien, under hensyntagen til databeskyttelsen, skal være egnet til at realisere formålet.[70] Præambelbetragtning nr. 78 indeholder et krav om at der i offentlige udbud skal tages hensyn til principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger. På baggrund heraf, mener Peter Blume, at man som dataansvarlig bør anvende teknologier der er udformet med henblik på databeskyttelse, såfremt disse ikke er særligt omkostningsbelastende.[71]

Den dataansvarlige pålægges efter bestemmelsen en pligt til at anvende tiltag, der påviseligt har en fremmende effekt på implementeringen af Persondataforordningens beskyttelsesprincipper og øvrige regler. Dette medfører at den dataansvarlige skal overveje sine databeskyttelsesforanstaltninger i forhold til alle Persondataforordningens bestemmelser, når denne indretter sine IT-systemer, organisation mv.[72] Herunder kan man trække den tidligere nævnte sag om Biblioteksstyrelsen og deres manglende brug af en krypteret linje til udsendelse af

[66] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 416
[67] Ibid., s. 417
[68] Ibid., s. 422
[69] Justitsministeriet, Powerpoint-præsentation fra stormøde om persondataforordningen, 2017, slide nr. 25
[70] Blume, P. (2017, s. 112
[71] Ibid.
[72] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 417

lånereservationer og –kvitteringer. I relation til en situtation, hvor den dataansvarlige ikke kan løse opgaven tilfredsstillende via sine nuværende systemer, må reglerne om databeskyttelse gennem design antages at være særligt relevante i forbindelse med etableringen af nye systemer.

Der er i præambelbetragtning nr. 78 angivet eksempler på foranstaltninger, som er i tråd med kravet om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger. Det er angivet at sådanne foranstaltninger kan være dataminimering, hvilket betyder at man udelukkende behandler identificerbare personoplysninger, når dette er konkret nødvendigt for formålet[73]. Et andet eksempel der nævnes, er pseudonymisering af personoplysningerne så hurtigt som muligt, hvor man erstatter enkelte identificerbare parametre med koder, således at man ikke umiddelbart kan identificere oplysningerne, men kan genfinde disse ved hjælp af en anden liste eller lignende[74]. Herudover er gennemsigtighed for så vidt angår personoplysningernes funktion og behandling, således at den registrerede kan overvåge databehandlingen og den dataansvarlige kan tilvejebringe og forbedre sikkerhedselementer.

Det fremgår af justitsministeriets betænkning, at den dataansvarlige, på grund af kravet i artikel 25, stk. 1 om at de fornødne sikkerhedsforanstaltninger skal opfylde kravene i Persondataforordningen, må antages at være forpligtet til at sikre at de midler, fx et IT-system, man anvender, er medvirkende til at sikre at Persondataforordningen overholdes. Her anføres det at den dataansvarlige kan sikre dette ved at indarbejde såkaldte Privacy Enhancing Technologies, såfremt denne selv udvikler sine systemer.[75]

Den dataansvarlige skal anvende foranstaltninger, som er designet med henblik på effektiv implementering af databeskyttelsesprincipper, og med henblik på integrering af de fornødne garantier i behandlingen. Af justitsministeriets betænkning fremgår det at begrebet garantier i Persondataforordningens artikel 25, stk. 1, skal forstås i overensstemmelse med formuleringen i Persondataforordningens engelske sprogversion, hvori man anvender betegnelsen ”safeguards”, hvilket i denne sammenhæng kan forstås som ”værn” eller ”beskyttelse”.[76]

[73] Blume, P. (2017), s. 111-112
[74] Datatilsynet, Vejledning om anonymisering, 2016 - https://www.datatilsynet.dk/offentlig/anonymisering/
[75] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 418
[76] Ibid., s. 419-420

Artikel 5 i Persondataforordningen angiver konkret principperne om formålsbegrænsning, dataminimering, begrænsede opbevaringsperioder, datakvalitet, retsgrundlag for behandling, behandling af særlige kategorier af personoplysninger, foranstaltninger til at sikre datasikkerhed og krav til videreoverførsel. Disse må derfor betegnes som eksempler på de databeskyttelsesprincipper, der følger af artikel 25, stk. 1, som den dataansvarlige efter artikel 5 har pligt til at følge.[77]

Af justitsministeriets betænkning fremgår det slutteligt, at man bør se artikel 25, stk. 1 i sammenhæng med bestemmelsen om konsekvensanalyser vedrørende databeskyttelse i artikel 35. Det anføres her, at en sådan konsekvensanalyse kan danne grundlag for at designe tekniske databeskyttelsesforanstaltninger ind i fx et IT-system fra starten.[78]

Det fremgår af artikel 25, stk. 3, at en godkendt ceritificeringsmekanisme i medfør af artikel 42 kan blive brugt som et element til at påvise overholdelse af kravene i artikel 25, stk. 1.

Databeskyttelse gennem standardindstillinger

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

Det fremgår af justitsministeriets betænkning, at standardindstillinger skal forstås bredt, efter ordlyden af artikel 25, stk. 2. Dette medfører at både tekniske og organisatoriske foranstaltninger er omfattet. Det anføres herudfra at standardindstillinger fx både kan være IT-tekniske indstillinger, men også almindelige forretningsgange i relation til persondatabeskyttelse, som fx adgangen til personoplysninger der kan være arbejdsbetingede og ikke tilgængelige for alle.[79]

[77] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 420
[78] Ibid.
[79] Ibid.

Det anføres i justitsministeriets betænkning, at denne bestemmelse er et udtryk for at den dataansvarlige skal sikre at de indstillingsmuligheder, der er i IT-systemer, online-tjenester eller anden software, som standard kan indstilles således at de understøtter kravene i artikel 25, stk. 2.[80] Som eksempel herpå angives at, et IT-system eller lignende, når det stilles til rådighed for en medarbejder første gang, skal være indstillet således at det som standard indebærer den mindst mulige deling af personoplysninger, i overensstemmelse med de dataminimeringsprincip som følger af artikel 5.[81]

Af betænkningen fremgår det også, at når en fysisk person eksempelvis anvender en app på en computer, tablet, smartphone eller lignende, så har den dataansvarlige en pligt til, gennem standardindstillinger, at sikre, at en sådan app ikke indsamler flere personoplysninger end hvad der er nødvendigt for at opnå formålet med den givne app. Dette medfører at en sådan app, ikke må have standardindstillinger, som medfører en deling af oplysninger om en persons fx aktiviteter, opholdssteder eller hvem denne har været sammen med, medmindre at en sådan deling er selve formålet med den pågældende app. [82]

På baggrund af ovenstående udledes det derfor, i betænkningen, at der foreligger en manglende overholdelse af kravet af artikel 25, stk. 2, såfremt man ikke kan regulere delingen af personoplysninger i en given app eller et andet elektronisk program.[83]

Artikel 25, stk. 2, fastslår, som det fremgår af formuleringen, at de behandlede oplysninger ikke, uden den pågældende persons indgriben, må stilles til rådighed for et ubegrænset antal fysiske personer. Dette medfører at bestemmelsen eksempelvis tager sigte på online platforme som fx sociale medier, hvor det følger af denne, at sådanne platforme kun må lade personoplysninger være tilgængelige for et ubegrænset antal fysiske personer, såfremt den pågældende person selv foranlediger dette.[84]

Af betænkningen fremgår det, at systemer, der er skabt før Persondataforordningens ikrafttrædelse i 2018 og som er designet og indrettet efter gældende ret, ikke nødvendigvis skal ændres efter

[80] Ibid., s. 421
[81] Ibid., s. 421
[82] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 421
[83] Ibid., s. 422
[84] Ibid.

artikel 25, stk. 2. Dog bemærkes det, at såfremt det er muligt at ændre standardindstillingerne i et system som er skabt før Persondataforordningens ikrafttrædelse, skal dette gøres efter bestemmelsen.[85]

Det fremgår af artikel 25, stk. 3, at den godkendt certificeringsmekanisme i medfør af artikel 42 kan blive brugt som et element til at påvise overholdelse af kravene i artikel 25, stk. 2, som det også er tilfældet med artikel 25, stk. 1.

Det må på baggrund af ovenstående kunne konkluderes, at der med indførelsen af artikel 25 er skabt en forpligtelse for den dataansvarlige, til at inkorporere databeskyttelse i sin generelle tilgang til behandling af personoplysninger. Artikel 25, stk. 1 medfører, som det fremgår ovenfor, at den dataansvarlige allerede skal tænke databeskyttelse i forberedelsesfasen, med henblik på at kunne etablere de nødvendige foranstaltninger. Artikel 25, stk. 1 omhandler en forpligtelse til at iagttage at man som dataansvarlig indretter sine systemer således, at de gennem deres standardindstillinger udgør den mindst mulige risiko i forhold til personoplysninger. Det skal bemærkes, i relation til specialets fokus, at disse forpligtelse er pålagt den dataansvarlige.

Delkonklusion

Til trods for at de, i artikel 32, stk. 1, litra a-d, angivne eksempler for sikkerhedsforanstaltninger, ikke udgør en udtømmende liste over foranstaltninger, må man som dataansvarlig regne disse for de eneste konkrete foranstaltninger der følger af loven. Det skal endvidere bemærkes at de oplistede eksempler ikke er påkrævede i hver eneste behandling, men at brugen heraf derimod beror på en konkret risikovurdering i forhold til den enkelte behandlingsaktivitet.

Som det også fremgår af ovenstående afsnit, er der med Persondataforordningens bestemmelser omkring behandlingssikkerhed skabt en ny ramme for hvorledes den dataansvarlige og databehandleren, skal tilgå opgaven med at sikre en betryggende databeskyttelse. Persondataforordningens sikkerhedskrav er i højere grad centreret omkring en risikoafvejning af de enkelte behandlinger, set i forhold til hvilke foranstaltninger der er nødvendige for at kunne afveje de, af den dataansvarlige, identificerede risici således at beskyttelsen opretholdes.

[85] Ibid.

Der er fra flere sider, jf. ovenstående gennemgang, udtrykt begejstring over denne tilgang til databeskyttelsen, og det er anført at den risikobaserede tilgang vil medføre en bedre beskyttelse.

Samtidigt skal det dog anføres, at en risikobaseret tilgang vil medføre en langt mere differentieret arbejdsproces for den dataansvarlige og databehandleren, da disse proaktivt vil skulle kunne vurdere eventuelle fremtidige risici i forbindelse med iværksættelsen af en given behandling.

Persondataforordningens bestemmelser omkring behandlingssikkerhed understøttes af de ovenfornævnte krav omkring databeskyttelse gennem design og –standardindstillinger. Kravene i artikel 25, stk. 1 og 2, afviger, ligesom sikkerhedskravene i artikel 32, ikke væsentligt fra gældende ret, men har ligeledes den forskel at kravene er eksplicitte. Som det fremgår ovenfor, medfører artikel 25, stk. 1 og 2, at den dataansvarlige, og databehandleren, nu har en pligt til at tænke databeskyttelse, ved hjælp af tekniske og organisatoriske foranstaltninger, ind i designfasen af de systemer hvori personoplysningerne behandles. Bestemmelserne medfører endvidere, at man fra første dag skal have ovenstående momenter inkorporeret som standard i programmer mv. Den risikobaserede tilgang til databeskyttelsen kommer igen til udtryk i disse bestemmelser, da den dataansvarlige og databehandleren på forhånd skal udtænke hvorledes man indretter sine systemer og indstillinger således at man opvejer de risici behandlingen medfører.

Det kan på denne baggrund derfor udledes, at Persondataforordningen har medført at den dataansvarlige og databehandleren, er blevet pålagt at have en langt mere proaktiv og fremsynet tilgang til de behandlingsaktiviteter der udføres. Risikovurderingen skal være en fast del af både forberedelses- og behandlingsfasen, og der er med Persondataforordningen stillet klarere krav til hvorledes man skal tilgå denne opgave. Det synes også at kunne udledes af praksis fra gældende ret, at den dataansvarlige og databehandleres er forpligtet til vurdere behandlinger, der anvender teknologier som cloud-computing og lign. på en måde, der afspejler den reelle risiko ved brugen af sådanne.

Ovenstående falder i tråd med de to nye forpligtelser der følger af artikel 25, stk. 1 og 2, hvor der med indførelsen af artikel 25 er skabt en forpligtelse for den dataansvarlige, til at inkorporere databeskyttelse i sin generelle tilgang til behandling af personoplysninger. Artikel 25, stk. 1 medfører, som det fremgår ovenfor, at den dataansvarlige allerede skal tænke databeskyttelse i forberedelsesfasen, med henblik på at kunne etablere de nødvendige foranstaltninger. Artikel 25,

stk. 1 omhandler en forpligtelse til at iagttage at man som dataansvarlig indretter sine systemer således, at de gennem deres standardindstillinger udgør den mindst mulige risiko i forhold til personoplysninger. Disse forpligtelser, særligt artikel 25, stk. 1, indeholder også en risikovurdering, hvilket understøtter den ovenfor anførte antagelse om at Persondataforordningens generelle tilgang til datasikkerhed har rykket sig over mod en risikobaseret platform.

Bestemmelserne om behandlingssikkerheden er altså formuleret bredt, med henblik på at skabe plads til nye teknologier, samt til at afdække den enkelte behandlings risici med konkrete foranstaltninger. Foranstaltningerne har ingen påkrævet form, dette beror helt og aldeles på hvad der vurderes at være nødvendigt for at opnå en tilstrækkelig beskyttelse.

Afslutningsvist skal det påpeges, at det faktum, at både den dataansvarlige og databehandleren er underlagt de sikkerhedskrav der følger af artikel 32, understreger vigtigheden i at få klarlagt det retlige forhold mellem disse parter. En analyse af netop dette forhold, er på denne baggrund, hovedelementet det følgende afsnit.

Kapitel 2 - Dataansvarlig og databehandler

Som det fremgår af ovenstående, har den dataansvarlige og databehandleren pligt til at træffe de passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici der er tilknyttet behandlingen. Af delkonklusionen ovenfor følger det, at den dataansvarlige og databehandleren, skal anvende en risikobaseret tilgang til denne forpligtelse. For at kunne udføre deres forpligtelser på tilfredsstillende vis, er det nødvendigt, at der skabes en retlig ramme, som afspejler det faktiske forhold mellem den dataansvarlige og databehandleren, således at en egentlig overholdelse af reglerne er realistisk i praksis.

I det nedenstående afsnit, søges det afklaret, hvorledes det retlige forhold mellem den dataansvarlige og databehandleren påvirkes med Persondataforordningen. Dette vil ske i lyset af delkonklusionen på ovenstående kapitel, således at behandlingssikkerheden bliver et gennemgående tema i dette speciale.

Indledningsvist vil der blive foretaget en analyse af hvorledes definitionen af henholdsvis den dataansvarlige og databehandleren har indflydelse på det retlige forhold mellem disse, herunder på ansvarsfordelingen i relation til behandlingssikkerheden.

Definitioner og ansvar

Dataansvarlig

I Persondatalovens § 3, nr. 4 defineres den dataansvarlige som 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 oplysninger.

I persondatadirektivets Artikel 2, litra d, er den dataansvarlige benævnt som "den registeransvarlige" og defineres som 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; er formålet med og hjælpemidlerne ved behandlingen fastlagt ved nationale love eller forskrifter eller på fællesskabsplan, kan den registeransvarlige, eller de specifikke kriterier for udpegelse af denne, angives i den pågældende nationale ret eller i fællesskabsretten.

Persondataforordningens artikel 7 definerer den dataansvarlige som *en fysisk eller juridisk person, en offentligt myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger; hvis formålene og hjælpemidlerne til en sådan behandling er fastlagt i EU-retten eller medlemsstaternes nationale ret, kan den dataansvarlige eller de specifikke kriterier for udpegelse af denne fastsættes i EU-retten eller medlemsstaternes nationale ret*.

Som det fremgår af ordlyden af de ovenstående definitioner, medfører Persondataforordningen ingen ændringer i definitionen af den dataansvarlige. Definitionerne er bygget op omkring en række "nøgleord", som findes relevante at gennemgå med henblik på at klarlægge hvornår man kan betegnes som værende dataansvarlig.

"en fysisk eller juridisk person, en offentligt myndighed, en institution eller et andet organ"

Som det fremgår ovenfor, kan en dataansvarlig være *"en fysisk eller juridisk person, en offentligt myndighed, en institution eller et andet organ"*. Udfra denne formulering kan alle være dataansvarlig, hvad enten der er tale om en privatperson, en international koncern eller en offentlig myndighed, der synes altså ikke at være begrænsninger for hvem der kan antage rollen. Som Peter Blume har anført, er definitionen måske for bred, og han udtrykker en bekymring for om en

privatperson vil kunne magte opgaven som dataansvarlig, set i lyset af de krav Persondataforordningen stiller[86].

"alene eller sammen med andre afgør"

Der åbnes i definitionen op for et delt dataansvar, da muligheden for at fastsætte formål og hjælpemidler, ikke er afgrænset til en enkelt aktør. En behandling kan altså efter definitionerne i både gældende ret og Persondataforordningen, have flere dataansvarlige på samme tid.

"afgør til hvilke formål og med hvilke hjælpemidler"

Med brugen af ordet afgør, lægges der vægt på det faktum, at den dataansvarlige står med magten til at beslutte formålet med behandlingen, samt de hjælpemidler der skal anvendes i forbindelse med denne. Det er den dataansvarlige, der har råderetten over oplysningerne, og da denne har beføjelsen til at fastsætte formålet, er det også i dennes interesse behandlingen foregår.

"behandling af personoplysninger"

Behandling defineres i artikel 4, nr. 2 som:

"*enhver aktivitet eller række af aktiviteter — med eller uden brug af automatisk behandling — som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse"*

Behandlingsbegrebet er vidt formuleret, både i gældende ret og i Persondataforordningen, og under behandling hører enhver aktivitet, eller række af aktiviteter relateret til en personoplysninger. Bestemmelsen er ikke udtømmende formuleret, hverken i Persondataloven, Persondatadirektivet eller Persondataforordningen, men det afgørende er, at der ikke er nogen handling eller undladelse, der falder uden for Persondataforordningen.[87]

"fastlagt i EU-retten eller medlemsstaternes nationale"

Den sidste del af definition fastslår, at den dataansvarlige, eller kriterierne herfor, kan fastsættes efter EU-retten eller national lovgivning. Det kan ske i tilfælde hvor *"formålene og hjælpemidlerne til en sådan behandling er fastlagt i EU-retten eller medlemsstaternes nationale ret".*

[86] Blume, P. (2017), s. 61
[87] Blume, P. (2017), s. 59

I gældende ret findes der altså ikke en klar og utvetydig bestemmelse omkring det ansvar der påhviler den dataansvarlige. Dette følger i stedet implicit af den definition af "den dataansvarlige" jf. ovenstående gennemgang, samt de krav og forpligtelser denne er underlagt[88].

Af definitionerne i Persondataloven og Persondatadirektivet følger det altså, at det er den dataansvarlige, der alene, eller sammen med andre, skal afgøre til hvilket formål og på hvilken måde der må foretages behandling af personoplysninger. Heraf kan det udledes, at det er den dataansvarlige, der har ret til at disponere over de pågældende personoplysninger, og dermed også den direkte indflydelse på behandlingen af disse. Dette medfører at det som hovedregel også er den dataansvarlige der har ansvaret for at personoplysningerne behandles efter gældende ret på området.[89]

Risikobaseret ansvarsmodel

I Persondataforordningens artikel 24 fastlægges den dataansvarliges ansvar, og det følger af stk. 1, at den dataansvarlige under hensyntagen til behandlingens karakter, sammenhæng, omfang og formål samt sandsynligheden for og graden af de risici, der er for den registreredes rettigheder og frihedsrettigheder, skal gennemføre passende tekniske og organisatoriske foranstaltninger og kunne demonstrere, at behandlingen af personoplysninger er i overensstemmelse med Persondataforordningen. Det fremgår endvidere at disse foranstaltninger skal revideres og ajourføres.

Kravet om at der skal gennemføres passende tekniske og organisatoriske foranstaltninger, er ikke et krav der er afledt af artikel 32. Disse to bestemmelser indeholder separate krav, hvilket betyder at begge skal overholdes. Det skal dog, som det også fremgår af justitsministeriets betænkning, bemærkes, at artikel 24 kun er gældende for den dataansvarlige, i modsætning til artikel 32 som også gælder for databehandleren.[90]

Af Artikel 24, stk. 1 fremgår det ikke konkret, hvilke foranstaltninger man, som dataansvarlig, skal anvende. Det følger af bestemmelsen at det er behandlingens karakter, sammenhæng, omfang,

[88] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 405
[89] Ibid.
[90] Ibid., s. 407

formål og risiciene for de registreredes rettigheder og frihedsrettigheder der skal danne grundlag for vurderingen.

Som det fremgår af ovenstående afsnit om behandlingssikkerhed, er det i relation til risikovurderingen, risikoen for den registreredes rettigheder og frihedsrettigheder, der er afgørende for hvilke foranstaltninger man bør implementere. Det fremgår af artikel 29-gruppens udtalelse om princippet ansvarlighed, at afgørende momenter i risikovurderingen bør være omfanget af en given databehandling, samt antallet af planlagte overførsler[91].

Som Peter Blume anfører, er den fremtidsorientering, som den risikobaserede tilgang er et udtryk for, en nyskabelse i forhold til persondataretten. Den medfører et krav til den dataansvarlige om at denne skal have et klart overblik over selve behandlingsforløbet, men også at denne kan forudse hvorledes de pågældende oplysninger vil kunne misbruges eller kompromitteres.[92] Den dataansvarlige tvinges, ifølge Peter Blume, til at tænke og agere dynamisk, hvilket kan være forbedrende for databeskyttelsen[93].

Artikel 29-gruppen nævner en række eksempler på foranstaltninger, herunder bl.a. at den dataansvarlige kortlægger procedurer således at man kan identificere alle databehandlinger, og at man kan lave en oversigt over disse. Uddannelse i databeskyttelse, etablering af interne procedurer for henholdsvis sikkerhedsbrister, anmodninger fra de registrerede om indsigt, korrektion eller sletning samt udarbejdelse af mekanismer til behandling af klager mv., er angivet som eksempler på tekniske og organisatoriske foranstaltninger.[94]

Det fremgår endvidere af Artikel 29-gruppens udtalelse at den dataansvarlige skal anvende de risici som behandlingen indebærer, samt oplysningernes art, når denne skal træffe beslutning om hvorledes foranstaltningernes implementeres effektivt.[95] I relation til dette fremgår det at justitsministeriets betænkning nr. 1565, at der ved større og mere komplekse eller risikobetonede behandlinger bør foretages regelmæssige kontroller på om de implementerede foranstaltninger er

[91] Artikel 29-gruppen, udtalelse nr. 3/2010 om princippet ansvarlighed (WP173), s. 14
[92] Blume, P. (2017), s. 111
[93] Ibid.
[94] Artikel 29-gruppen, udtalelse nr. 3/2010 om princippet ansvarlighed (WP173), s. 11 ff.
[95] Ibid., s. 15

effektive. Den anføres at dette kan gøres ved hjælp af interne eller eksterne revisioner eller overvågning.[96]

Af artikel 24, stk. 2, fremgår det endvidere at den dataansvarlige skal implementere passende databeskyttelsespolitikker, såfremt det er proportionalt med den givne behandling. Eksempler på sådanne politikker kan være interne procedurer i relation til hvorledes man håndterer klager eller anmodninger om aktindsigt fra de registrerede.[97] Det må antages at en seriøs og proaktiv tilgang til sådanne politikker vil medføre et bedre udgangspunkt i forhold til databeskyttelsen, men også at dette vil være et brugbart element i forhold til dokumentationskravet, som omtales længere nede.

Det fremgår af artikel 24, stk. 1, at den dataansvarlige skal kunne påvise at denne overholder sine forpligtelser efter denne bestemmelse. I artikel 24, stk. 3, er overholdelse af godkendte adfærdskodekser eller godkendte certificeringsmekanismer, efter henholdsvis artikel 40 og 42, nævnt som metoder til at påvise overholdelse af reglerne. Det fremgår dog af justitsministeriets betænkning, at brugen af sådanne kodekser og mekanismer, ikke vil kunne stå alene som bevis for at den dataansvarliges behandling overholder Persondataforordningens bestemmelser[98].

Der er ikke den store forskel på indholdet af gældende ret i forhold til Persondataforordningens, når det kommer til den dataansvarliges forpligtelser efter artikel 24. De fleste af kravene i bestemmelsen, fremgår implicit af gældende ret i dag. Den umiddelbare forskel ligger i at der med Persondataforordningens artikel 24, er kommet eksplicitte krav til den dataansvarliges forpligtelser, samt til at denne kan påvise at forpligtelserne overholdes.

Databehandler

I Persondatalovens § 3, nr. 5 defineres databehandleren som *"den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne".*

Persondatadirektivet og Persondataforordningen indeholder også samme definition med undtagelse af at disse indledes med "en" i stedet for "den". Det giver ikke anledning til en anderledes

[96] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 409
[97] Ibid., s. 408
[98] Ibid., s. 409

forståelse af definitionen, hvorfor der definitionsmæssigt er tale om samme ordlyd og dermed en videreføring af gældende ret.

"en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ"

Som det fremgår ovenfor, kan alle være dataansvarlig på baggrund af denne formulering, og det samme med derfor antages at være tilfældet med rollen som databehandler, da ordlyden, i forhold til personkredsen, er ens i de to definitioner. Det må også antages, at Peter Blumes bekymringer omkring privatpersoners evne til at udfylde rollen efter Persondataforordningens regler jf. ovenstående, kan være gældende i relation til databehandleren.

"behandler oplysninger"

Behandlingsbegrebet er defineret og gennemgået under definitionen af den dataansvarlige, og i relation til databehandleren, er der ikke forskel på selve behandlingsbegrebet. Det må altså antages at der ikke findes en handling eller undladelse i relation til personoplysninger, som ikke er omfattet af Persondataforordningen.

"på den dataansvarliges vegne"

Det angives med denne ordlyd, at man for at være databehandler, skal udføre behandling på vegne af en dataansvarlig. Dette medfører at man jf. ovenstående afsnit om den dataansvarlige, kan udlede at råderetten over personoplysningerne, ikke må være til stede. Artikel 29-gruppen har i forbindelse med en udtalelse omkring Persondatadirektivet og definitionen af databehandleren, brugt ordet "delegation" i forbindelse med behandling på den dataansvarliges vegne[99]. Det må altså antages, at der skal være tale om en situation hvor man fra den dataansvarlige, har fået delegeret en behandlingsbeføjelse.

Artikel 29-gruppen har endvidere, i deres udtalelse om begreberne "registerfører" og "registeransvarlig", fremsat to betingelser for hvornår der er tale om en databehandler. Den første betingelse er, at der skal være tale om en retlig selvstændig enhed i forhold til den dataansvarlige, hvilket medfører at der ikke eksempelvis ikke er tale om en databehandler såfremt en anden afdeling i samme virksomhed eller myndighed foretager behandlingen. Det er hernæst et krav at databehandleren foretager behandling af personoplysninger på vegne af den dataansvarlige.[100] I

[99] Artikel 29-gruppen, udtalelse nr. 1/2010 om begreberne "registeransvarlig" og "registerfører", (WP 169, side 26
[100] Ibid., s. 25

justitsministeriets betænkning nr. 1565, er der som eksempel herpå nævnt virksomheder som leverer hosting-ydelser på nettet eller cloud-leverandører.[101]

Det må på denne baggrund kunne udledes, at databehandleren ikke kan eksistere uden den dataansvarlige og at der ikke kan foretages behandling af en databehandler hvis den dataansvarlige ikke har uddelegeret behandlingen. Det underbygges yderligere af Artikel 29-gruppen i den ovenfor nævnte udtalelse, med sætningen: *The existence of a processor depends on a decision taken by the controller*[102]*.*

Hvorledes forholdet er konstrueret afhænger af aftaleforholdet mellem den dataansvarlige og databehandleren. Som udgangspunkt er der ikke noget til hinder for, at databehandleren anvender underbehandlere, så længe dette sker inden for det retlige ramme. En kort gennemgang af begrebet underbehandleren følger nedenfor.

Flere databehandlere og underbehandlere

Der findes ingen specifik regulering, i hverken Persondatadirektivet eller Persondataloven, af de tilfælde hvor behandlingen af personoplysninger overlades flere databehandlere på én gang. Men det må lægges til grund, at de krav der gælder for en databehandler, er gældende uagtet om der også er andre databehandlere inde i billedet.

Af Artikel 29-gruppens udtalelse af om begreberne ”registeransvarlig” og ”registerfører” følger det at der ikke er noget i vejen for at en databehandler kan overlade en given behandling af personlysninger, til flere databehandlere på én gang.[103] Ovenstående gælder både for situationer hvor der er flere databehandlere, men også situationer hvor en databehandlere overlader en del af behandlingen til en underbehandler.[104]

Selvom disse underbehandlere også er underlagt forpligtelserne i Persondatalovens §§ 41 og 42, anbefaler Artikel 29-gruppen, i den tidligere nævnte udtalelse om begreberne ”registeransvarlig” og ”registerfører”, at man undgår at have en kæde af databehandlere og underbehandlere. Denne anbefaling er baseret på at man i gruppen mener at en sådan kæde kan forringe eller hindre en

[101] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 431
[102] Artikel 29-gruppen, udtalelse nr. 1/2010 om begreberne ”registeransvarlig” og ”registerfører”, (WP 169, s. 25
[103] Ibid., s. 27
[104] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 434

effektiv kontrol, medmindre man har en meget klar fordeling af ansvaret i en sådan kæde. Emnet vil blive gennemgået yderligere i det følgende kapitel.

Efter Persondataforordningens regler kræver brugen af underbehandlere specifik godkendelse fra den dataansvarlige jf. artikel 28, stk. 2, og herudover følger det af artikel 28, stk. 4, at eventuelle underbehandlere er underlagt de samme forpligtelser, som der fremgår af kontrakten mellem den dataansvarlige og databehandlere. Det følger videre af artikel 28, stk. 4, at det er databehandleren der er ansvarlig for underbehandlerens eventuelle misligholdelse af sine forpligtelser.

Som det også fremgår af det ovenstående afsnit, er det afgørende at man kan identificere den dataansvarlige og eventuelle databehandlere og underbehandlere. Såremt denne identifikation ikke er mulig, er der risiko for en mangelfund opfyldelse af forpligtelser der følger af lovgiviningen. En sådan situtaion vil endvidere medføre, at det vil være svært at identificere den ansvarshavende ved brud.

Det må på denne baggrund kunne konstateres at det er den dataansvarlige der har den overordnede ansvar for behandling, den denne har instruktionsbeføjelsen, og retten til at fastsætte formål og hjælpemidler. Databehandleren er en aktuel aktør, såfremt den dataansvarlige vælger at uddelegere sine behandlingsaktiviteter. Databehandlerens beføjelser er placeret indenfor den ramme, som dannes af den instruks der afgives for fra den dataansvarlige, herunder det angivne formål og hjælpemidlerne. Såfremt en databehandler agerer uden for disse rammer, og derved påvirker instruksen, formålet eller hjælpemidlerne, påtager den sig rollen som dataansvarlig for denne del af behandlingen. Dette må kunne udledes af definitionerne i de to ovenstående afsnit.

Det retlige forhold mellem dataansvarlig og databehandler

I det følgende kapitel behandles det retlige forhold mellem den dataansvarlige. Der vil på denne baggrund blive foretaget en gennemgang af den retlige regulering mellem parterne. Som det fremgår ovenfor, kan databehandleren ikke eksistere uden den dataansvarlige. Dette er dog ikke ensbetydende med, at databehandleren ikke kan stå på egne ben i relation til databehandlingen, så længe denne holder sig inden for de retlige rammer.

Valg af databehandler

Den retlige regulering af forholdet mellem databehandler og dataansvarslig er relevant allerede i forbindelse med udvælgelsen af databehandleren. Nedenfor følger en gennemgang af de

forpligtelser der påhviler den dataansvarlige og databehandleren, i forbindelse med indgåelsen af en aftale omkring databehandling.

Af gældende ret, Persondatadirektivets artikel 17, stk. 2, følger det at:

"*Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige, hvis oplysninger behandles for dennes regning, skal vælge en registerfører, som frembyder den fornødne garanti med hensyn til de tekniske sikkerhedsforanstaltninger og organisatoriske foranstaltninger, der skal træffes, og skal påse, at disse foranstaltninger overholdes."*

Persondataforordningens artikel 28, stk. 1, har følgende ordlyd:

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

Af præambelbetragtning nr. 81 fremgår det at sådanne garantier kan bestå i ekspertise, pålidelighed og ressourcer.[105] Det fremgår endvidere af artikel 28 nr. 6 at såfremt en databehandler overholder et godkendt adfærdskodeks, som omhandlet i artikel 40, eller en godkendt certificeringsmekanisme, som omhandlet i artikel 42, vil dette kunne anvendes som en del af beviset for at man kan stille de fornødne garantier der kræves af artikel 28 nr. 1.

Som det fremgår af ovenstående bestemmelser, er der, i forhold til bestemmelserne i gældende ret, ikke ændret på at det er den dataansvarliges opgave at sikre sig, at de databehandlere, denne vælger at benytte, kan stille de nødvendige garantier for, at de kan overholde de regler, der følger af den persondataretlige regulering. Dette medfører selvsagt en vigtig opgave for den dataansvarlige, da denne vil være pålagt visse forpligtelser i relation til at sikre sig, at databehandlerens garantier er tilstrækkelige. Som det også fremgår af Datatilsynets praksis, baseret på gældende ret, bliver den dataansvarlige vurderet på dennes evne til både at overvåge og vurdere databehandlerens evne til at sikre personoplysningerne efter reglerne.

[105] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 435

Et konkret eksempel på manglende overholdelse af pligten til at udøve et aktivt tilsyn, kan findes i den praksis der foreligger på baggrund af gældende ret. I relation til gennemgangen af den dataansvarliges forpligtelser ovenfor, antages det dog at Datatilsynet udtalelse ville være uændret såfremt den var baseret på Persondataforordningens bestemmelser. Sagen omhandlede en række danske virksomheder og foreninger, som i forbindelse med et videresalg af en række harddiske, havde overladt sletningen af disse til en databehandler. Datatilsynet var blevet gjort opmærksomme på, at man i udlandet havde fundet nogle af disse harddiske, og havde kunnet konstatere at der ikke var blevet foretaget en effektiv sletning af harddiskene før de var blevet solgt videre. Datatilsynet udtalte, databehandleren ikke havde levet op til sine forpligtelser efter Persondatalovens § 41, stk. 1, i forhold til at følge instruksen, og derved foretage en effektiv sletning. Databehandleren havde heller ikke overholdt sine selvstændige forpligtelser efter § 41, stk. 3 omkring iværksættelsen af sikkerhedsforanstaltninger. Det blev videre udtalt, at der efter § 42, stk. 1, burde havde været udført en vis kontrol med sletningen, herunder fx stikprøver.[106]

Det må på baggrund heraf, kunne udledes at den dataansvarlige, i relation til ovenstående vurdering, må sikre sig at denne, enten via interne ressourcer, eller ekstern hjælp, kan overskue hvilke foranstaltninger der er nødvendige for at sikre at en given behandlingen overholder Persondataforordningens regler. Dette til trods for at den dataansvarlige, i mange tilfælde, vælger at outsource en behandling, da denne ikke selv magter opgaven[107].

I tilfælde hvor databehandleren vælger at benytte en underbehandler, er det databehandleren der hæfter såfremt underbehandleren misligholder sine forpligtelser. På den baggrund er det nærliggende at antage, at udvælgelsesprocessen i forbindelse med en databehandlers uddelegering til en underbehandler, vil få mange lighedstræk med den dataansvarliges udvælgelse af en databehandler. En nærmere gennemgang af betingelserne for brugen af underbehandlere findes i afsnittet om databehandleraftaler.

Som det også er anført længere oppe, medfører en forlængelse af databehandlerkæde, at gennemsigtigheden i behandlingen mindskes. Dette er et risikomoment for både den dataansvarlige

[106] Datatilsynets j.nr. 2000-631-0057
[107] Blume, P. (2017), s. 115

og databehandleren, da disse på hver deres måde, står med et ansvar der bliver sværere at leve op til.

På baggrund af ovenstående, må det kunne konkluderes at den dataansvarlige står med en vigtig opgave, når denne vil uddelegere en behandlingsaktivitet. Outsourcing kan være medføre økonomiske fordele, effektivisering og et bedre slutprodukt, men hensynet til datasikkerheden, gør at man skal vurderingsopgaven alvorligt. Det samme er gældende for databehandlere, der ønsker at bruge underbehandlere. Dette skyldes først og fremmest at databehandleren er blevet et selvstændigt pligtsubjekt i Persondataforordningen, hvilket medfører at en underbehandlers misligholdelse kan medføre et erstatningsansvar eller andre sanktioner.

Brugen af adfærdskodekser og certificering

I relation til udvælgelsen af en databehandler, kan denne, som nævnt ovenfor, anvende brugen af godkendte certificeringsmekanismer og adfærdskodekser, som et led i bevisførelsen for at denne kan overholde Persondataforordningens regler i forhold til at indføre tilstrækkelige foranstaltninger.

Brugen af frivillige virkemidler er af Peter Blume omtalt i følgende uddrag:

"Disse fremgangsmåder har den styrke, at de mere eller mindre er udtryk for selvregulering inden for Persondataforordningens brede rammer. Selvregulering har en særlig styrke, fordi den dataansvarlige eller databehandleren selv har valgt at benytte de pågældende regler og de i hvert fald i et vist omfang opleves som de berørtes >>egne<< regler. Regler og fremgangsmåder af denne karakter har en særlig overbevisende kraft. Inden for bestemte sektorer kan ordninger af denne karakter bistå til at fremme overholdelsen af forordningen. Det er frivilligt at anvende disse mekanismer, men de kan have den fordel, at de underbygger en formodning om, at de formelle regler bliver overholdt…"[108]

Som det fremgår af ovenstående uddrag, kan både den dataansvarlige og databehandleren altså bruge sådanne frivillige virkemidler til at udvælge henholdsvis databehandlere og underbehandlere, samt til at påvise, at man overholder sine egne forpligtelser, indenfor de forskellige områder i Persondataforordningen.

[108] Blume, P. (2017), s. 131-132

Som Peter Blume anfører, må valget af databehandleren, herunder den ovenfor nævnte vurdering, betragtes som en af den dataansvarliges primære opgaver, og det er derfor vigtigt at man ikke lader sig friste at billige løsninger.[109] Når det kommer til situationer hvor databehandleren ønsker at anvende en underbehandler, er der i Persondataforordningen også indsat bestemmelser herom, der henvises til afsnittet om underbehandlere længere oppe.

Instruktionsbeføjelsen

Af Persondatalovens § 41, følger det at Personer, virksomheder m.v., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, må kun behandle disse efter instruks fra den dataansvarlige, medmindre andet følger af lov eller bestemmelser fastsat i henhold til lov. Denne bestemmelse er baseret på Persondatadirektivets artikel 16.

I Persondataforordningens artikel 29, er der en lignende bestemmelse omkring instruksen, dog med et øget fokus på databehandleren, og underbehandlere:

"Databehandleren og enhver, der udfører arbejde for den dataansvarlige eller databehandleren, og som har adgang til personoplysninger, behandler kun disse oplysninger efter instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-retten eller medlemsstaternes nationale ret."

Da det følger af Persondataloven og Persondatadirektivets bestemmelser at der er tale om enhver person, må det antages at der er tale om en videreføring af gældende ret. Dog må det, i forhold til Persondataforordningen bemærkes, at databehandlerens rolle, også i dette tilfælde, er fremhævet i højere grad en hvad der er tilfældet i gældende ret.

I Persondataforordningen er der dog den nyskabelse, i forhold til instruksen, at denne skal være dokumenteret. Dette er fastsat i bestemmelserne om indholdet af en databehandleraftale, hvor det af artikel 28, stk. 3, litra a fremgår, at databehandleren *"kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige…"*. Det fremgår ikke af litra a, hvorledes en sådan instruks skal dokumenteres,[110] men som det fremgår af justitsministeriets betænkning, må det antages, at begge parter har ansvaret for at dokumentere instruksen[111].

[109] Blume, P. (2017). 115
[110] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 439
[111] Ibid., s. 438

I "Persondataloven med kommentarer" er der, som eksempel, angivet, at en databehandler, f.eks. et edb-servicebureau, ikke må anvende oplysningerne til noget andet formål end til brug for løsning af netop den opgave, som databehandleren efter aftale med den dataansvarlige har påtaget sig. Det anføres videre, at databehandleren på den baggrund ikke er berettiget til at videregive oplysninger fra et edb-system, som denne drifter, til en tredjemand uden forudgående instruks fra den dataansvarlige.[112]

Datatilsynet har også påpeget vigtigheden af instruksen, i forbindelse med en sag vedrørende Odense Kommunes brug af en online kontorpakke fra Google Apps, som anvendes via en cloud-løsning. I forbindelse med denne sag påpegede Datatilsynet vigtigheden af, at man i databehandleraftalen sikrede sig at Google udelukkende måtte behandle oplysninger på baggrund af instruktion fra Odense Kommune.[113] Denne sag er gennemgået nærmere i afsnittet om databehandleraftalen.

Umiddelbart efter artikel 28, stk. 3, litra h, følger det i tilknytning til første afsnit, at databehandleren, i tilfælde hvor denne mener at den dataansvarliges afgivne instruks er i strid med lovgivningen, skal give den dataansvarlige underretning herom.

Databehandleren er altså pålagt en pligt til "at sige fra", såfremt denne mener at den dataansvarliges instruks indebærer en overtrædelse af Persondataforordningens regler. Såfremt databehandleren ikke siger, må der altså antages at være tale om behandling på et ulovligt grundlag, hvilket er i strid med Persondataforordningens regler.

Instruksen er altså en afgørende faktor i forholdet mellem den dataansvarlige og databehandleren. Kravet om instruks følger sågar af definitionen af databehandleren, og man kan på den baggrund argumentere for at databehandlerforholdet ikke kan etableres uden instruksens tilstedeværelse.

Databehandleraftalen

Det fremgår af § 42, stk. 2, med baggrund i artikel 17, stk. 3 og 4, at der i enhver situation hvor en dataansvarlig overlader en behandling til en databehandler, skal være en skriftlig aftale herom. Af denne aftale skal det fremgå at databehandleren handler efter instruks fra den dataansvarlige, og det skal endvidere fremgå at databehandleren også er underlagt de forpligtelser som følger af § 41,

[112] Waaben, H. m.fl., (2015), s. 547
[113] Datatilsynets j.nr. 2010-52-0138

stk. 3-5. Det skal også fremgå af aftalen, at bestemmelserne om sikkerhedsforanstaltninger, som er gældende i den stat hvor databehandleren er hjemmehørende, er gældende for den pågældende aftale.[114]

Der er ikke fremsat specifikke krav til hvorledes en databehandleraftale skal være udformet, udover at de ovenfor nævnte krav skal være indeholdt. En vurdering af om en databehandleraftale er udformet på tilstrækkelig vis, må bero på en vurdering af om der i den enkelte situation er behov for en særligt detaljeret eller omfattende aftale for at den dataansvarlige, på betryggende vis, kan sikre sig at databehandleren overholder sine forpligtelser.[115] Som tidligere nævnt skal sikkerhedsbekendtgørelsens regler iagttages, når der er tale om en databehandling der udføres for en dataansvarlig der er en offentlig myndighed. Det følger af Sikkerhedsbekendtgørelsens § 7, at det ligeledes skal fremgå af databehandleraftalen, at dette er tilfældet.

Af Persondataforordningens artikel 28, stk. 3, fremgår det at såfremt en databehandler foretager behandling for den dataansvarlige, skal dette være reguleret af en kontrakt eller et andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, som skal være bindende for databehandleren overfor den dataansvarlige. Det er et krav at en sådan aftale fastsætter behandlingens genstand og varighed, dens karakter og formål, typen af personoplysninger der behandles, kategorierne af de registrerede, samt den dataansvarliges forpligtelser og rettigheder.[116]

Der er i artikel 28, stk.3, litra a-h, oplistet en række specifikke krav til indholdet af en databehandleraftale. Disse krav er langt mere omfattende og detaljerede end de krav der følger af gældende ret, og de vil i det følgende blive gennemgået med henblik på analysere deres betydning for det retlige forhold mellem den dataansvarlige og databehandleren.

Artikel 28, stk. 3, litra a omhandler kravet om at databehandleraftalen skal fastsætte at databehandleren udelukkende må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel af personoplysninger til et tredjeland eller en international organisation, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Såfremt dette er tilfældet skal databehandleren

[114] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 434
[115] Ibid.
[116] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 439

underrette den dataansvarlige om et sådant krav inden behandlingen foretages, medmindre den pågældende forbyder underretningen af hensyn til vigtige samfundsmæssige interesser.

Databehandleren pålægges altså denne begrænsning i alle behandlingstilfælde, da databehandleraftalen er et krav ved alle behandlinger, hvor den dataansvarlige overlader en behandlingsaktivitet til en databehandler jf. artikel 28, stk. 3. For en nærmere gennemgang af instruks-reglen, henvises til afsnittet herom længere oppe.

Artikel 28, stk. 3, litra b omhandler et krav om at det i databehandleraftalen skal fastsættes, at databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller en underlagt en passende lovbestemt tavshedspligt.

Der følger af gældende ret ikke en forpligtelse for databehandleren til at sikre sig at personer som arbejder under denne er underlagt tavsheds- eller fortrolighedspligt. Det kan dog påpeges at offentlige myndigheder som udgangspunkt opfylder denne forpligtelse, da offentligt ansatte har tavshedspligt efter forvaltningslovens § 27, stk. 1 og straffelovens § 152, 152 c-f.[117]

Det fremgår af *Artikel 28, stk. 3, litra c*, at det i databehandleraftalen skal fastsættes at databehandleren skal iværksætte alle foranstaltninger, som kræves i henhold til artikel 32 om behandlingssikkerhed. Kravet er i tråd med gældende ret jf. ovenfor.

Disse sikkerhedskrav findes nærmere beskrevet i kapitel 2 om behandlingssikkerheden.

Artikel 28, stk. 3, litra d omhandler kravet om at en databehandler skal opfylde kravene i artikel 28, stk. 2 og 4. Det følger af stk. 2 at en databehandler kun kan gøre brug af en anden databehandler efter specifik eller generel skriftlig godkendelse fra den dataansvarlige, som tidligere gennemgået i afsnittet om databehandlerens generelle forpligtelser efter Persondataforordningen. Stk. 4 omhandler det ansvar der påhviler de underbehandlere, som databehandleren vælger at gøre brug, nærmere gennemgang heraf findes i afsnittet om underbehandlere.

Artikel 28, stk. 3, litra e, foreskriver at en databehandleraftale skal indeholde en bestemmelse om at databehandleren, så vidt muligt og under hensyntagen til behandlingens karakter, skal bistå den dataansvarlige med opfyldelsen af den dataansvarliges forpligtelse til at besvare anmodninger om

[117] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 439

udøvelse af de registreredes rettigheder der følger af Persondataforordningens kapitel 3, ved hjælp af passende tekniske foranstaltninger. Dette medfører at databehandleren ikke blot selv skal overholde de forpligtelser denne pålægges i artikel 28, stk. 3, litra c, men det medfører også, at denne pålægges et ansvar for at bistå den dataansvarlige med overholdelsen heraf, samt de øvrige krav der følger af Persondataforordningens kapitel 3. Denne bestemmelse vil ikke blive behandlet yderligere i dette speciale, men er medtaget for at give et billede af omfanget af Persondataforordningens krav til databehandleraftalen.

I artikel 28, stk. 3, litra f, fremgår det at databehandleraftalen skal indeholde en bestemmelse om at databehandleren, under hensyntagen til behandlingens karakter og de oplysninger denne har til rådighed, skal bistå den dataansvarlige med at overholde de forpligtelser som følger af artikel 32-36.

Dette betyder at databehandleren efter indgåelse af en databehandleraftale er forpligtet til at hjælpe den dataansvarlige i forhold til kravene i artikel 32 om behandlingssikkerheden. Det skal dog bemærke at denne forpligtelse allerede følger af artikel 32, hvor databehandleren er nævnt på lige fod med den dataansvarlige. Herudover skal databehandleren, ifølge artikel 33, bistå den dataansvarlige med anmeldelser af eventuelle brud på datasikkerheden til Datatilsynet, og ligeledes bistå med underretning til de registrerede i forbindelse med brud jf. artikel 34. Bestemmelsen medfører endvidere at databehandleraftalen skal indeholde et krav om at databehandleren skal bistå den dataansvarlige med at udarbejde konsekvensanalyser vedrørende databeskyttelse efter artikel 35, samt foretage forudgående høring af Datatilsynet, såfremt en sådan konsekvensanalyse viser at en behandling vil medføre høj risiko jf. artikel 36. Denne bestemmelse må siges at være omfattende i forhold til vurderingen af databehandlerens ansvar. Det må følge af artiklens ordlyd, at vurderingen af i hvor høj grad databehandleren skal bistå med overholdelse, må bero på den konkrete behandlings karakter, herunder hvor stor en rolle databehandleren spiller. Artikel 32 er gennemgået i afsnittet omkring behandlingssikkerhed, og der henvises derfor hertil for yderligere gennemgang. Artikel 33-36 vil, grundet specialets omfang, ikke blive gennemgået yderligere.

Af databehandleraftalen skal det endvidere fremgå at databehandleren efter endt behandling, skal slette eller tilbagelevere alle personoplysninger til den dataansvarlige jf. *artikel § 28, stk. 3, litra g.* Herunder gælder også et krav om sletning af alle kopier, medmindre EU-retten eller

medlemsstaternes nationale ret foreskriver at oplysningerne skal opbevares. Om personoplysningerne skal tilbageleveres eller slettes afgøres af den dataansvarlige. I relation til denne forpligtelse, kan der drages paralleller til sagen om sletningen af harddiske, som er nævnt i afsnittet om behandlingssikkerhed. Det må antages, at såfremt en dataansvarlig vælger at lade oplysningerne slette hos databehandleren, vil denne kunne ifalde et ansvar for manglende tilsyn, såfremt et sådant ikke udøves i forbindelse med denne sletning.

Slutteligt skal aftalen jf. artikel 28, stk. 3, litra h, indeholde en bestemmelse om at databehandleren skal stille alle de oplysninger, der er nødvendige for at kunne påvise overholdelse af kravene i artikel 28, til rådighed for den dataansvarlige og samtidigt giver mulighed for og bidrager til revisioner som foretages af den dataansvarlige eller en anden revisor, der er bemyndiget af den dataansvarlige. Det må antages at betegnelsen "anden revisor" ikke er ment som en stillingsbetegnelse, da der ikke i Persondataforordningen findes et krav om at den dataansvarlige skal have en bestemt stilling[118]. Dette er i tråd med Persondataforordningens krav om en transparens i behandlingen af personoplysninger, og må selvsagt være en nødvendighed for at den dataansvarlig kan udøve et tilfredsstillende tilsyn.

Ovenstående krav til databehandleraftalen er suppleret med et krav om at databehandleraftalen, hvad enten der er tale om en kontrakt eller et andet retligt dokument, skal foreligge skriftligt, herunder elektronisk jf. artikel 28, stk. 9.

I tilfælde hvor databehandleren foretager behandling, der rækker udenfor de i kontrakten fastsatte rammer, eller instruksen, bliver denne anset som værende dataansvarlig for den givne del af den samlede behandling jf. artikel 28, stk. 10. Dette gælder også for tilfælde, hvor databehandleren fortsætter en allerede afsluttet databehandling. En sådan situation vil selvsagt medføre at databehandleren, pludselig er underlagt en lang række forpligtelser, hvoraf bestemmelserne omkring bl.a. formål, kan blive vanskelige at overholde. I forhold til denne bestemmelse, skal det bemærkes at den dataansvarlige vil skulle have opfyldt sin tilsynspligt, da denne ellers vil kunne ifalde ansvar herfor.[119]

[118] Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 441
[119] Blume, P. (2017), s. 116

Præambelbetragtning nr. 79 uddyber grundlaget for at man i Persondataforordningen har valgt at opstille specifikke krav til en databehandleraftale. Som det fremgår af præambelbetragtningen forudsætter beskyttelsen af registreredes rettigheder og frihedsrettigheder, samt de dataansvarliges og databehandlernes ansvar, herunder erstatningsansvar, også i forbindelse med tilsynsmyndighedernes kontrol og foranstaltninger, at der er en klar fordeling af ansvarsområderne i medfør af Persondataforordningen. Herunder nævnes når en dataansvarlig fastlægger formålene med og hjælpemidlerne til behandling sammen med andre dataansvarlige, eller når en behandlingsaktivitet foretages på vegne af en dataansvarlig.

Sagen om Odense Kommune og Google Apps

I tråd med afsnittet om instruksens betydning for det retlige forhold mellem den dataansvarlige og databehandleren, påpeger Datatilsynet i denne sag vigtigheden af at have en instruksbestemmelse i sin databehandleraftale med en cloud-leverandør. Generelt understreges vigtigheden af en databehandleraftale, og Datatilsynet giver klart udtryk for at minimumskravene til en databehandleraftale skal være opfyldt. Sagen er afgjort på baggrund af gældende ret, men da de nye krav jf. ovenstående gennemgang er langt mere omfattede, må det ikke antages at Datatilsynet ville have vurderet sagen mildere efter Persondataforordningens regler.

I den konkrete sag udtalte Datatilsynet, at den fremlagte databehandleraftale ikke var i overensstemmelse med reglerne i Persondataloven. Selve databehandleraftalen var en del af Google Apps vilkår, og bestod af to punkter fra Google Apps standardbetingelser.

"1.4 Privacy Policies. Customer acknowledges that it has chosen to have its End Users personal data processed by Google as part of the Services within the scope of the Services' capabilities, which are reflected in the Google Privacy Policies. Customer therefore instructs Google to provide the Services and process End User personal data in accordance with the Google Privacy Policies and Google agrees to do the same. The Google Privacy Policies are hereby incorporated by reference into this Agreement. Customer agrees to protect the privacy of End Users by complying with a policy communicated to End Users which is no less protective than the Google Privacy Policies.

1.5 Data Protection. In Section 1.4 and Section 1,5, the terms "personal data", "processing", "data controller" and "data processor" shall have the meanings ascribed to them in the EU Directive. For the purposes of this Agreement and in respect of the personal data of End Users, the parties agree

that Customer shall be the data controller and Google shall be a data processor. Google shall take and implement appropriate technical and organisational measures to protect such personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access."

Ved en gennemgang af disse betingelser, fandt Datatilsynet det ikke godtgjort at reglerne omkring databehandlerens behandling ud fra en instruks var opfyldt. Som Datatilsynet påpegede, omhandlede instruksen udelukkende en forpligtelse til at behandle oplysningerne i relation til de aftalte services indenfor Googles egne privatlivspolitikker. En sådan betingelse virker begrænsende, da instruksen dermed ikke efterleves på den dataansvarliges vilkår, men derimod databehandlerens.

Det fandtes endvidere problematisk, at de betingelser der udgjorde databehandleraftalen, medførte at det reelt set var Google Apps, altså databehandleren, der havde den egentlige kontrol over formålet med behandlingen. Årsagen hertil kan findes i det faktum, at såfremt instruksen og selve databehandleraftalen er baseret på databehandlerens egne vilkår, er disse materielt set uden indhold, da databehandleren derned har retten til at ændre sådanne vilkår og dermed grundlaget for behandlingen af personoplysningerne.

Sagen afspejler databehandleraftalens vigtig i relation til beskyttelsen af de behandlede oplysninger. Som det følger af Persondataforordningens krav til databehandleraftalen, vil Datatilsynet i en lignende sag, have en endnu bredere vifte af krav, som den dataansvarlige skal sørge for at få indsat i en databehandleraftale. Sagen understreger også den problematik der kan opstå i de tilfælde, hvor databehandleraftalen er en del af databehandlerens standardvilkår. For mange databehandlere vil dette være den mest enkle løsning, da disse i mange tilfælde vil behandle data for en stor kreds af dataansvarlige. På denne baggrund synes sagens omstændigheder at være et godt eksempel på hvorledes den stigende brug af databehandlere, samt den teknologiske udvikling, er kommet til udtryk gennem kravene i artikel 28, stk. 3.

Artikel 28, stk. 4 fastslår at såfremt en databehandler vælger at benytte en underbehandler, pålægges denne underbehandler de samme forpligtelser, som de der er fastsat i databehandleraftalen mellem den dataansvarlige og databehandleren. Det følger desuden af artikel 28, stk. 2, at brugen af underbehandlere specifik godkendelse fra den dataansvarlige. Det følger

videre af artikel 28, stk. 4, at det er databehandleren der er ansvarlig for underbehandlerens eventuelle misligholdelse af sine forpligtelser.

Det følger af artikel 28, stk. 7, at Kommissionen eller Datatilsynet kan udstede standardkontrakter. Såfremt dette bliver gjort, er der ingen forpligtelse til at bruge sådanne, men det må antages at være et brugbart redskab for mange.

På en række områder i artikel 28, stk. 3, er der sket en videreføring af gældende ret. Dette er bl.a. sket i forhold til kravet om overholdelse af sikkerhedskravene, men der er samtidigt også indført en række nye forpligtelser for databehandleren, som denne pålægges ved indgåelse af databehandleraftalen. Databehandleren har nu, pligt til at give den dataansvarlige meddelelse om brud på datasikkerheden inden for 72 timer. Databehandleren skal endvidere bistå den dataansvarlige med at foretage konsekvensanalyser i de tilfælde hvor en behandling potentielt vil medføre en høj risiko, og såfremt det er nødvendigt, skal databehandleren også bistå med pligten til at foretage forudgående høring hos Datatilsynet, på baggrund af konsekvensanalysens resultater.

Erstatningsansvar

Både den dataansvarlige og databehandleren er underlagt Persondataforordningens artikel 82.

Af bestemmelsens stk. 2, fremgår følgende omkring deres erstatningsansvar:

"Enhver dataansvarlig, der er involveret i behandling, hæfter for den skade, der er forvoldt af behandling, der overtræder denne forordning. En databehandler hæfter kun for den skade, der er forvoldt af behandling, hvis pågældende ikke har opfyldt forpligtelser i denne forordning, der er rettet specifikt mod databehandlere, eller hvis pågældende har undladt at følge eller handlet i strid med den dataansvarliges lovlige instrukser."

Dette skal ses i lyset af artiklens stk. 1, hvoraf det fremgår at:

"Enhver, som har lidt materiel eller immateriel skade som følge af en overtrædelse af denne forordning, har ret til erstatning for den forvoldte skade fra den dataansvarlige eller databehandleren."

De to bestemmelser ovenfor medfører at både den dataansvarlige og databehandleren kan gøres direkte erstatningsansvarlige efter Persondataforordningen. Dette er en nyskabelse i forhold til gældende ret, hvor databehandleren tidligere har været pakket ind under den dataansvarlige. Med

disse bestemmelser kan databehandleren altså ifalde ansvar efter det betingelser der fremgår af artikel 82, stk. 2, og efter artikel 82, stk. 1, kan den der har lidt skade, rette kravet direkte imod denne.

Som det fremgår af ovenstående gennemgang af Persondataforordningens regler om databehandleraftaler, er der blevet ændret markant i de krav der stilles til reguleringen med dataansvarlig og databehandler. Som det også fremgår flere steder i ovenstående analyse, er den dataansvarliges rolle blevet langt mere markant, grundet den hastige teknologiske udvikling. Baseret på de nye krav til aftalens indhold, samt præambelbetragtning nr. 79, synes det naturligt at konkludere, at man har ønsket at skubbe databehandleren frem i lyset, med henvisning til Peter Blumes udsagn om dennes rolle længere oppe.

En mere tidssvarende rolle

I henhold til gældende ret, kan det på baggrund af ovenstående kapitel, sammenholdt med de øvrige kapitler, konstateres at det er den dataansvarlige der bærer det primære ansvar for at reglerne overholdes. Dette kommer først og fremmest til udtryk gennem det faktum, at databehandleren ikke optræder som selvstændigt pligtsubjekt i gældende ret.

Ovenstående kan også udledes på baggrund af de beføjelser den dataansvarlige er tildelt. Det fremgår af gældende ret, at denne har retten til at angive formålet med behandlingen, samt vælge de hjælpemidler der skal bruges hertil. Den dataansvarlige står endvidere med retten til at, og ansvaret for, at vælge databehandlere, der på betryggende vis, kan udføre en behandlingsaktivitet på dennes vegne. Dette er for så vidt ikke anderledes end i Persondataforordningen, men forskellen ligger i, at databehandleren ikke i gældende ret har væsentlige selvstændige pligter, udover sikkerhedskravene, og at denne ikke er angivet som pligtsubjekt.

Med Persondataforordningen ændres ovenstående billede markant, set fra databehandlerens side. Denne er først og fremmest blevet "opgraderet" til et selvstændigt pligtsubjekt, hvilket medfører et selvstændigt ansvar for de forpligtelser denne er underlagt efter Persondataforordningen. Dette ansvar er underbygget ved introduktion af en række bestemmelser, der er specifikt rettet mod databehandleren. Artikel 28 sætter den overordnede grænse for databehandlerens beføjelser og forpligtelser, og særligt reglerne om databehandleraftalen i artikel 28, stk. 3, medfører at databehandleren står med et selvstændigt, og klart, ansvar.

Som det fremgår af ovenstående analyse, er databehandleren blevet pålagt at deltage mere aktivt i beskyttelsen af personoplysninger. Dette kommer først og fremmest til udtryk gennem det selvstændige krav om overholdelse af sikkerhedskravene, som dog også følger af gældende ret. Som det er fremkommet i kapitlet om behandlingssikkerhed, har den risikobaserede tilgang til databeskyttelse vundet indpas i forhold til hvorledes man kan overholde sine forpligtelser. Grundet databehandlerens selvstændige forpligtelser i relation til behandlingssikkerheden, er denne også pålagt at tillægge sig en risikobaseret tilgang i forbindelse med sine behandlingsaktiviteter.

Det skal dog samtidigt bemærkes, at det stadig er den dataansvarlige der er den centrale aktør i Persondataforordningen. Som det er nævnt i dette kapitel, kan databehandleren ikke eksistere uden den dataansvarlige, hverken efter gældende ret eller Persondataforordningen. Den dataansvarlige er underlagt en række pligter i forbindelsen med brugen af databehandleren, og ligeledes er databehandleren underlagt en række forpligtelser. Fordelingen af disse forpligtelser, er med Persondataforordningen blevet langt tydeligere, og det synes nærliggende at konkludere, at denne fordeling giver et mere realistisk billede af den rolle parterne har i relation til databehandling i praksis. Samtidigt med at rollerne er blevet opdelt, medfører Persondataforordningen også en mulighed for at tilpasse sin databeskyttelse specifikt til den enkelte behandling. Dette må siges at være et positivt element for dataansvarlige og databehandlere, da disse kan indrette sig mere målrettet efter deres egentlige virke, fremfor at iagttage forpligtelser der ikke ordentlig effekt, grundet behandlingens natur.

Som det både fremgår af Peter Blumes udgivelse om Persondataforordningen, samt Justitsministeriets betænkning, er den risikobaserede tilgang et positivt element i persondataretten. Det er anført at et øget fokus på identifikation af risici, og handlinger på baggrund heraf, vil kunne føre en til en øget databeskyttelse. Der kan argumenteres for, at en sådan løsning, vil kunne medføre tilfælde hvor der indføres færre foranstaltninger end hvad der ville have været tilfældet i henhold til gældende ret, men dette må opvejes af, at de konkrete foranstaltninger der indføres, forhåbentligt, er mere målrettede og effektive.

Som det fremgår af indledningen, er databehandlerens øgede betydning for persondataretten et resultat af en teknologisk udvikling, der er eksploderet siden 90'erne.

Persondataforordningen synes at danne en ramme for et forhold mellem den dataansvarlige og databehandleren, der vil gave alle parter, herunder særligt de registrerede, hvis oplysninger er genstand for behandling. Med databehandlerens selvstændige forpligtelser, er der dannet grundlag for en mere seriøs tilgang til databeskyttelse. Der kan argumenteres for, at det mere selvstændige ansvar til databehandleren, kan medføre at indgåelsen af et dataansvarlig-databehandler forhold vil blive genstand for en mere omfattende forhandlingsproces end tidligere, da begge parter nu har "hånden på kogepladen".

For dataansvarlige og databehandlere medfører Persondataforordningen, som tidligere nævnt, en tung administrativ opgave. Det må dog kunne antages at de, der på bedste vis kan løse denne opgave, står med et stærkt kort på hånden i forhold til sine konkurrenter. For databehandlere vil et stærkt databeskyttelses-setup medføre, at en dataansvarlig vil kunne få stillet tilstrækkelige garantier i forbindelse med udvælgelsen, og på denne baggrund kan persondata-compliance blive et konkurrenceparameter, såfremt den dataansvarlige har flere valgmuligheder. Datatilsynets direktør, Cristina Angela Gulisano, har udtalt at "det "at behandle personoplysninger sikkert" ligefrem begynder at være et konkurrenceparameter for virksomheder - noget, der således med fordel kan bruges i virksomheders markedsføring over for forbrugerne. "[120] Der foreligger altså en bred vifte af incitamenter til at sætte sig grundigt ind i forordningens regler, hvad enten man er dataansvarlig eller databehandler.

[120] Kromann Reumert, Persondata – Det nye sort, 2017

Konklusion

Indledningsvist kan det konkluderes, at Persondataforordningens krav om behandlingssikkerhed er blevet ændret med Persondataforordningen.

Som det fremgår af kapitel 2 om behandlingssikkerheden, er der for det første sket en præcisering af de sikkerhedsmæssige foranstaltninger, man som dataansvarlig og databehandler, har pligt til at indføre. Målet er fortsat at sikre en tilstrækkelig beskyttelse af fysiske personer i forbindelse med behandlingen af personoplysninger, og relation til sikkerhedskravene, skal dette stadig ske ved implementeringen af passende tekniske og organisatoriske foranstaltninger. I Persondataforordningens artikel 32, stk. 1, litra a-d, angives en række konkrete eksempler på sikkerhedsforanstaltninger, og uagtet at disse ikke udgør en udtømmende liste over foranstaltninger, må man, som dataansvarlig og databehandler, regne disse for de eneste konkrete foranstaltninger der følger af loven.

Dog må det antages at der kan hentes inspiration fra den praksis og de vejledninger der er baseret på gældende ret, da kravene ikke, rent materielt, har ændret sig væsentligt.

Det må i relation til formuleringen af bestemmelserne omkring behandlingssikkerheden konkluderes at disse i mange tilfælde, og som det også er tilfældet i gældende ret, er formuleret meget bredt. Dette understreger den trussel som den teknologiske udviklings indvirkning på informationsteknologien udgør mod beskyttelsen af personoplysninger. Som det fremgår af det indledende kapitel, har man gennem flere år måttet sande at det lovmæssige grundlag i gældende ret har været utilstrækkeligt og ufleksibelt set i forhold til den måde personoplysninger, som følge af udviklingen, behandles på. Som det også fremgår af ovenstående gennemgang, har Datatilsynet, i relation til cloud-computing, udtalt, at man ser positivt på den moderne teknologi. Det kan dog udledes af tidligere praksis, at man i relation til samme emne, stiller store krav til at man bevare kontrollen over personoplysningerne i forbindelse med brug af sådanne tjenester.

Den vigtigste ændring, i relation til behandlingssikkerheden, er det rammeskifte Persondataforordningen medfører, i forhold til hvorledes man som dataansvarlig og databehandler skal tilgå udøvelsen af sine forpligtelser. Persondataforordningens sikkerhedskrav er i højere grad

centreret omkring en risikoafvejning af de enkelte behandlinger, set i forhold til hvilke foranstaltninger der er nødvendige for at kunne afveje de identificerede risici således at beskyttelsen opretholdes. Denne risikobaserede tilgang møder begejstring fra flere sider, og der er udtrykt en forventning om, at en risikobaseret tilgang til datasikkerhed, vil medføre et højnet beskyttelsesniveau. Der kan i relation hertil også nævnes, at selvom en risikobaseret tilgang i nogle tilfælde, vil medføre brug af færre foranstaltninger end hvad der er tilfældet i gældende ret, så må det antages at de anvendte foranstaltninger, grundet risikovurderingen, kan være mere effektive.

Persondataforordningen har medbragt to nyskabelser i relation til behandlingssikkerheden, i form af databeskyttelse gennem design og –standardindstillinger. Som det fremgår af ovenstående, skal kravene ikke ses som egentlige sikkerhedskrav, men derimod som overvejelsesforpligtelser. Dette skal forstås således, at den dataansvarlige har pligt til at overveje databeskyttelse allerede i forberedelsesfasen i forbindelse med en behandling. Dette vil medføre, at eventuelle nye systemer vil få inkorporeret databeskyttelse i selve designet. Herudover er det yderligere et krav, at alle systemer skal udvikles og indstilles således, at deres standardindstillinger medfører den mindst mulige behandling af personoplysninger.

For den dataansvarlige og databehandleren venter der selvsagt en tung administrativ opgave, i forbindelse med at skulle omstille sin tilgang til databehandling. På den anden side, må det også kunne antages at en risikobaseret tilgang vil medføre at både den dataansvarlige og databehandleren vil kunne udføre behandlinger, med mindsket risiko for at disse fører til brud på datasikkerheden. Herved mindskes risikoen for bøder, erstatningssager og lignende, og dette må være ønskeligt, set i lyset af Persondataforordningens markant større bødesummer.

I relation til den dataansvarlige og databehandleren, og forholdet mellem disse, er der med Persondataforordningen, blevet sat en langt skarpere retlig ramme for hvilke forpligtelser disse parter er underlagt. Databehandleren er med Peter Blumes ord ”trådt ud af skyggen”, og er blevet et selvstændigt pligtsubjekt i Persondataforordningen. Dette er en nyskabelse, og som en naturlig følge heraf, har denne også fået specificeret sine forpligtelser eksplicit i flere af Persondataforordningens bestemmelser.

I tråd med Persondataforordningens krav om transparens, er der med artikel 28 skabt et udgangspunkt for hvorledes ansvarsfordelingen mellem den dataansvarlige og databehandleren er

indrettet. Persondataforordningens indholdsmæssige krav til databehandleraftalen stiller langt flere krav til hvorledes forholdet mellem den dataansvarlige og databehandleren skal indrettes. Databehandleren pålægges efter aftalen, en række yderligere forpligtelser til at bistå den dataansvarlige med varetagelsen af sine forpligtelser i relation til databehandlingen. Herunder er databehandleren pålagt at bistå den dataansvarlige med at overholde de nye forpligtelser i form at meddelelseskravet, kravet om udarbejdelse af konsekvensanalyser og kravet om at foretage forudgående høring af Datatilsynet.

Herudover vidner Persondataforordningens nye krav om at instruksen fra den dataansvarlige til databehandleren skal være skriftligt, om et øget fokus på vigtigheden af at den dataansvarlige beholder styringen og overblikket i en tid hvor den informationsteknologiske udvikling skaber forvirring i det persondataretlige landskab. For det ér stadig den dataansvarlige, der er den centrale aktør i Persondataforordningen, og som det fremgår ovenfor afhænger databehandlerens identitet af at denne er underlagt den dataansvarliges beføjelser efter Persondataforordningen.

Det synes passende at afslutte denne konklusion med en ganske kort opsummering over de to hovedkonklusioner fra dette speciale, som tilsammen skaber svaret på problemformuleringen.

Forordning 2016/679 påvirker sikkerhedskravene efter gældende ret, således at disse nu er blevet åbnet mere op for den informationsteknologiske udvikling, herunder begreber som cloud computing. Nøgleordet i de forpligtelser der er pålagt den dataansvarlige og databehandleren efter Persondataforordningen, er risici. Risikovurderingen er i højsædet, og denne skal danne grundlag for en mere fleksibel databeskyttelse, som beror på de faktiske omstændigheder omkring den enkelte behandlingsaktivitet. Der er fra flere sider enighed om, at denne model risikomodel har potentiale til at medføre et højere beskyttelsesniveau.

Det retlige forhold mellem den dataansvarlige og databehandleren påvirkes af forordning 2016/679 således, at der med artikel 28, er sat en række skarpere krav til hvorledes forholdet skal indrettes for at være i overensstemmelse med Persondataforordningen. Databehandleraftalen er blevet langt mere omfattede, og pålægger databehandleren en længere vifte af forpligtelser, end hvad der er tilfældet i gældende ret. Man kan sige det er blevet mere ligetil at anvende både databehandlere og underbehandlere, som følge af den klarere ansvarsfordeling. Databehandlerens ydre grænse i relation til behandlingsbeføjelser er databehandleraftalen, herunder særligt instruksen fra

databehandleren, og krydses denne grænse, er konsekvenserne efter Persondataforordningen blevet alvorlige.

Litteraturliste

Forordinger og direktiver

- Europa-Parlamentets og Rådets forordning 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) (2016/679/EU).
- Europa-Parlamentet og Rådets direktiv af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (95/46/EF).

Danske love, bekendtgørelser og forarbejder

- Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som skal
- Bekendtgørelse nr. 528 af 15. juni 2000, om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning
- Betænkning nr. 1345/1997 om behandling af personoplysninger
- Betænkning nr. 1565/2017 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning
- Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer
- Lov nr. 654 af 20. september 1991 om offentlige myndigheders registre

Dokumenter fra Artikel 29-gruppen

- Artikel 29-gruppen, WP 196, Opinion 05/2012 on Cloud Computing, vedtaget 1. juli 2012
- Artikel 29-gruppen, WP 173, Opinion 3/2010 on the principle of accountability, vedtaget 13. juli 2010
- Artikel 29-gruppen, WP-169, Opinion 1/2010 on the concepts of "controller" and "processor", vedtaget 16. februar 2010

Vejledninger, årsrapporter og sikkerhedstekster fra Datatilsynet

- Datatilsynets vejledning nr. 37 af 2. april 2001
- Datatilsynet, IT-sikkerhedstekst ST13, Krypteret dataudveksling via websider - set fra den dataansvarliges synsvinkel, 2016, version 1.

Praksis fra datatilsynet

- Datatilsynets journalnummer 2000-631-0057
- Datatilsynets journalnummer 2010-52-0138
- Datatilsynets journalnummer 2011-632-0104
- Datatilsynets journalnummer 2013-631-0053

Litteratur

- Blume, Peter , *Den nye persondataret – Forordning 2016/679 om persondatabeskyttelse – Med en omtale af direktiv 2016/680 (politipersondataret)*, Jurist- og Økonomforbundets Forlag, 1. udgave, 2. oplag, 2016, ISBN: 978-87-574-3392-0
- Blume, Peter, *Juridisk metodelære*, Jurist- og Økonomforbundets Forlag, 5. udgave, 1. oplag, 2009
- Udsen, Henrik, *IT-ret*, Ex Tuto Publishing A/S, 3. udgave, 1. oplag, 2016, ISBN: 978-87-92598-45-5
- Waaben, Henrik, Kristian Korfits Nielsen, *Persondataloven med kommentarer*, Jurist- og Økonomforbundets forlag, 3. udgave, 1.oplag, 2015, ISBN: 978-87-57431-09-4

Artikler

- Blume, Peter, Persondatabeskyttelse i et stormfyldt hav, Tidsskrift for Rettsvidenskap vol. 128, 2015, ISSN 0040-7143

Hjemmesider

- Datatilsynet, vejledning om anonymisering, 2016
  Tilgængelig på: https://www.datatilsynet.dk/offentlig/anonymisering/
- Den fælles offentlige digitaliseringsstrategi for 2016-2020.
  Tilgængelig på: https://www.digst.dk/strategier/strategi-2016-2020
- Justitsministeriet, stormøde om persondataforordningen d. 9 februar 2017
  Tilgængelig på: https://erhvervsstyrelsen.dk/sites/default/files/media/praesentation_fra_stormoede_om_databeskyttelsesforordningen.pdf
- Kromann Reumert, *Persondata – Det nye sort*, 2017
  - Tilgængelig på: https://www.kromannreumert.com/Insights/2015/Persondata-det-nye-sort
- Tranberg, Charlotte Bagger, *Sikker behandling af personoplysninger*, 2014

- Tilgængelig på: http://www.advokatsamfundet.dk/Service/Publikationer/Tidligere%20artikler/2014/Advokaten%205/Persondataret.aspx