Retsudvalget 2015-16
REU Alm.del Bilag 369
Offentligt

Rapport om kortlægning af beskyttelsen af oplysninger om borgernes elektroniske betalinger mv.

Afgivet af en arbejdsgruppe under Justitsministeriet, juni 2016

Indholdsfortegnelse

1. Indledning

1.1. Arbejdsgruppens nedsættelse og kommissorium

1.1.1. BT bragte i foråret 2014 en historie om, at en ansat hos IBM Danmark via sin adgang til Nets' systemer gennem en årrække angiveligt havde forsynet Se og Hør med oplysninger om kongelige og kendte personers brug af kreditkort. Kort tid herefter blev der i medierne bragt historier om, at også ansatte hos flyselskabet SAS, Naviair og Rigshospitalet havde forsynet Se og Hør med oplysninger om kongelige og kendte personer.

Afsløringerne blev fulgt op af en række andre historier i medierne om læk og andre former for misbrug af personoplysninger.

Som følge af afsløringerne er der blevet iværksat undersøgelser hos de relevante offentlige myndigheder og implicerede virksomheder af, hvad der er foregået i de pågældende sager, hvilke regelsæt der eventuelt måtte være blevet overtrådt, og om der er grundlag for sanktioner i den anledning.

Københavns Vestegns Politi indledte således den 28. april 2014 en efterforskning i sagen. Desuden iværksatte Finanstilsynet i efteråret 2014 en ordinær og planlagt undersøgelse af sikkerheden hos Nets, ligesom Datatilsynet i foråret 2014 iværksatte undersøgelser af Se og Hør og Rigshospitalet.[1] Derudover har Digitaliseringsstyrelsen – som følge af de brud på sikkerheden, der øjensynligt har været – krævet, at Nets strammer yderligere op på den i forvejen høje sikkerhed omkring NemID. Endvidere anmodede transport- og bygningsministeren på baggrund af de forlydender, der har været om, at også ansatte hos SAS har udleveret oplysninger om kongelige og kendte til Se og Hør, Trafik- og Byggestyrelsen om at iværksætte en undersøgelse af, hvordan luftfartsselskaberne og de større lufthavne beskytter personoplysninger.[2] Herudover iværksatte Datatilsynet en undersøgelse af SAS. Endelig er det fremgået af mediernes omtale af sagen, at også IBM, Nets og Aller Media har iværksat undersøgelser i sagen, ligesom Naviair har afsluttet en intern undersøgelse og afskediget en medarbejder i sagen.

For nærmere oplysninger om status vedrørende disse undersøgelser henvises til punkt 4 nedenfor.

Den daværende regering besluttede i forlængelse af sagerne at kortlægge beskyttelsen af oplysninger om borgernes elektroniske betalinger mv. med henblik på at få klarlagt, om der er behov for nye initiativer på området.

---

[1] Datatilsynet har efterfølgende oversendt Se og Hør-sagen til Københavns Vestegns Politi, idet Aller Media er sigtet af politiet i sagen og derfor ikke ønskede at udtale sig.

[2] Trafik- og Byggestyrelsen har efterfølgende oversendt de oplysninger, styrelsen har modtaget fra luftfartsselskaberne og de større lufthavne, til Datatilsynet, som er tilsynsmyndighed på området.

Den daværende justitsminister tilkendegav, at kortlægningen skal danne udgangspunkt for en politisk drøftelse. Den daværende justitsminister tilkendegav desuden – i forbindelse med besvarelsen af forespørgsel nr. F 36 om beskyttelse af danskernes personoplysninger den 3. juni 2014, hvor et enigt Folketing tilsluttede sig en vedtagelsestekst herom – at den politiske drøftelse også vil omfatte udarbejdelsen af en samlet strategi til sikring af danskernes personoplysninger.

1.1.2. Justitsministeriet har på den baggrund nedsat en arbejdsgruppe, der ved arbejdets afslutning havde følgende sammensætning:

- Kontorchef Jakob Lundsager, Justitsministeriet (formand)
- Kommitteret Birgit Kleis, Datatilsynet
- Fungerende kontorchef Mette Tams Kitaj, Erhvervs- og Vækstministeriet
- Kontorchef Ulla Brøns Petersen, Finanstilsynet
- Chefkonsulent Annette Creve-Fræmohs, Forbrugerombudsmanden
- Kontorchef Charlotte Jacoby, Digitaliseringsstyrelsen
- Poul Thorlacius-Ussing, Center for Cybersikkerhed
- Afdelingschef Birgitte Drewes, Sundhedsdatastyrelsen
- Specialkonsulent Per Strand, Trafik- og Byggestyrelsen

Souschef Anders Lotterup og fuldmægtig Kristian Gyde Poulsen, begge Justitsministeriet, har fungeret som sekretærer for arbejdsgruppen.

Arbejdsgruppen har fået følgende kommissorium:

> ”I lyset af de afsløringer af ugebladet Se og Hørs overvågning af kongelige og kendte personers brug af kreditkort mv., som har været fremme i medierne i den seneste tid, er der rejst spørgsmål om nye initiativer til beskyttelse af personoplysninger.
>
> På den baggrund nedsættes der en arbejdsgruppe, som har til opgave at kortlægge beskyttelsen af oplysninger om borgernes elektroniske betalinger mv. Kortlægningen skal ske i lyset af Se og Hør-sagen og de spørgsmål om it-sikkerhed, som denne sag giver anledning til. I den forbindelse skal regelgrundlaget beskrives, herunder tilsynet med, at reglerne overholdes.
>
> Arbejdsgruppen skal herudover afklare, om der – inden for de EU-retlige rammer – er grundlag for at gennemføre nye initiativer på området, herunder ændring af reglerne om behandlingssikkerhed (it-sikkerhed), skærpelse af straffen for overtrædelse af persondataloven og anden relevant lovgivning, styrkelse af reaktionsmuligheder og tilsynsbeføjelser for Datatilsynet eller andre tilsynsmyndigheder samt ændring af grænsedragningen mellem tilsynsmyndighedernes kompetencer. I bekræftende fald skal arbejdsgruppen komme med anbefalinger til, hvordan disse initiativer kan gennemføres, og om der er behov for lovændringer.

Arbejdsgruppen skal bestå af repræsentanter for Justitsministeriet (formanden), Erhvervs- og Vækstministeriet, Finansministeriet (Digitaliseringsstyrelsen) samt Forsvarsministeriet (Center for Cybersikkerhed). Arbejdsgruppen kan efter behov udvides med yderligere medlemmer. Sekretariatsfunktionen varetages af Justitsministeriet.

Arbejdsgruppen nedsættes som en selvstændig myndighed.

Arbejdsgruppen anmodes om at færdiggøre sit arbejde snarest muligt og inden udgangen af oktober 2014."

1.1.3. Kortlægningsarbejdet er mundet ud i nærværende rapport, der er inddelt således, at afsnit 2 indeholder en beskrivelse af relevante regler på området, som er gældende i dag. Afsnit 3 indeholder en beskrivelse af, hvordan personoplysninger i praksis beskyttes på sundhedsområdet. Afsnit 4 indeholder en – overordnet – omtale af den sikkerhedsbrist, som den såkaldte Se og Hør-sag primært har handlet om. Afsnit 5 indeholder en beskrivelse af regeringens arbejde med informationssikkerhed, mens afsnit 6 indeholder en beskrivelse af arbejdsgruppens overvejelser.

Under punkt 1.2 umiddelbart nedenfor følger en sammenfatning af arbejdsgruppens overvejelser og anbefalinger ligeledes.

1.2. Sammenfatning af arbejdsgruppens overvejelser og anbefalinger

Arbejdsgruppens overvejelser og anbefalinger kan sammenfattes således:

- Der gælder i vidt omfang regler om, hvordan personoplysninger, herunder oplysninger om, hvor betalere har anvendt deres betalingsinstrument, skal beskyttes mod uvedkommendes adgang mv. Disse regler sikrer efter arbejdsgruppens opfattelse en god beskyttelse af personoplysninger (jf. punkt 6.1.1).
- Arbejdsgruppen vurderer dog, at der med fordel kan foretages en yderligere præcisering af kravene i bekendtgørelsen om ledelse og styring af pengeinstitutter m.fl. fsva. indretning, styring og kontrol af it-systemer med særlig fokus på rettighedstildelinger og kontroller (jf. punkt 6.1.5.2).
- Arbejdsgruppen anbefaler videre som opfølgning på rapporten at undersøge fordele og ulemper ved at indføre en pligt for finansielle virksomheder, betalingsinstitutter samt fællesejede datacentraler og datacentraler, der udfører væsentlig it-drift og it-udvikling for den fælles betalingsinfrastruktur, til at indberette til Finanstilsynet, hvis udenlandske myndigheder har pålagt dem at udlevere personoplysninger (jf. punkt 6.5.1).
- Arbejdsgruppen støtter også, at Finanstilsynet styrkes med 1-2 årsværk med henblik på at styrke tilsynet med it-sikkerhed (jf. punkt 6.5.3).

- Det er arbejdsgruppens vurdering, at de fælles retningslinjer vedr. beskyttelse af fortrolige kundeoplysninger, som den finansielle sektor selv har taget initiativ til at udarbejde, ventes at højne sektorens fokus på behovet for løbende at styrke og udbygge god it-adfærd og vil kunne sikre, at branchen selv tager ansvar for kontinuerligt at følge de højeste standarder for it-sikkerhed (jf. punkt 6.1.5.1).Bødeniveauet for overtrædelse af persondataloven kan efter arbejdsgruppens opfattelse passende hæves. Det er imidlertid arbejdsgruppens opfattelse, at det ikke er hensigtsmæssigt at ændre bødeniveauet for overtrædelse af persondataloven på nuværende tidspunkt (jf. punkt 6.2.2).
- Arbejdsgruppen har noteret sig, at et udvalg under Erhvervs- og Vækstministeriet netop har færdiggjort sit arbejde med at se på sanktionsniveauet for overtrædelse af lov om finansiel virksomhed og at udvalget på den baggrund har foreslået en væsentlig forhøjelse af bødeniveauet for overtrædelser begået af virksomheder og fysiske personer. (jf. punkt 6.2.3).
- Det er arbejdsgruppens opfattelse, at sikkerhedsstandarden ISO27001 ikke bør gøres obligatorisk for virksomheder og organisationer i Danmark. Det skyldes *dels*, at de tilfælde af misbrug, som afsløringerne om Se og Hørs overvågning har afdækket, efter arbejdsgruppens opfattelse næppe kunne være undgået ved, at Nets eller andre implicerede var forpligtet til at efterleve ISO27001, *dels* at krav om anvendelse af ISO27001 for alle virksomheder og organisationer vil risikere at medføre en uproportional byrde, særligt i virksomheder og organisationer, hvis it-anvendelse ikke er forbundet med en høj risiko for misbrug af personoplysninger. Det er dog arbejdsgruppens generelle anbefaling, at sikkerhedsstandarden med fordel kan implementeres af private virksomheder og organisationer i situationer, hvor virksomheden eller organisationen ud fra en risikobaseret tilgang vurderer, at det vil understøtte deres sikkerhedsarbejde på konstruktiv vis (jf. punkt 6.1.3).
- Det er arbejdsgruppens opfattelse, at der ikke i medfør af persondatalovens § 41, stk. 5, bør fastsættes nærmere regler om behandlingssikkerhed for den private sektor. Det skyldes *dels*, at de tilfælde af misbrug, som afsløringerne om Se og Hørs overvågning har afdækket, efter arbejdsgruppens opfattelse næppe kunne være undgået ved, at der blev fastsat nærmere regler om behandlingssikkerhed for den private sektor, *dels* at det i lyset af den nye databeskyttelsesforordning vil være uhensigtsmæssigt at fastsætte nærmere regler om behandlingssikkerhed på nuværende tidspunkt (jf. punkt 6.1.2).
- Det er arbejdsgruppens opfattelse, at der ikke på nuværende tidspunkt bør indføres en ordning med såkaldte databeskyttelsesansvarlige. Arbejdsgruppen har herved lagt vægt på *dels* det, der er anført i Registerudvalgets betænkning nr. 1345/1997 om baggrunden for ikke at indføre en sådan ordning i Danmark, *dels*

at den nye databeskyttelsesforordning indeholder regler om databeskyttelsesrådgivere (jf. punkt 6.1.4).

- Det er arbejdsgruppens opfattelse, at der ikke er behov for eller i øvrigt bør foretages en styrkelse af tilsynsbeføjelser og reaktionsmuligheder for tilsynsmyndighederne på området på nuværende tidspunkt. Det skyldes *dels*, at de tilfælde af misbrug, som afsløringerne om Se og Hørs overvågning har afdækket, efter arbejdsgruppens opfattelse næppe kunne være undgået ved, at de myndigheder, som fører tilsyn med overholdelsen af reglerne på området, havde haft yderligere tilsynsbeføjelser og reaktionsmuligheder, *dels* at det i lyset af databeskyttelsesforordningen vil være uhensigtsmæssigt at fastsætte nærmere regler om tilsynsbeføjelser og reaktionsmuligheder på nuværende tidspunkt (jf. punkt 6.3).
- Arbejdsgruppen foreslår desuden, at det i forbindelse med den forestående revision af lov om betalingstjenester og elektroniske penge som følge af det reviderede betalingstjenestedirektiv og tilpasningen af lovgivningen som følge af databeskyttelsesforordningen overvejes, hvordan man bedst fastlægger et klart og entydigt tilsyn på området og sikrer en klar grænsedragning mellem de relevante myndigheders kompetencer. (jf. punkt 6.4).

2. Gældende ret

2.1. Persondatalovens regler om beskyttelse af personoplysninger

Persondataloven[3] er i vidt omfang baseret på – og gennemfører – EU's databeskyttelsesdirektiv[4]. Direktivet indeholder bl.a. bestemmelser om, hvornår der må ske behandling af personoplysninger, og om, hvordan personoplysninger skal beskyttes. Direktivet sætter således visse grænser i forhold til, hvilke regler der kan fastsættes herom i de enkelte medlemsstater.[5]

2.1.1. Persondatalovens anvendelsesområde

Persondatalovens anvendelsesområde er nærmere beskrevet i lovens kapitel 1 om lovens område (§§ 1-2) og kapitel 2 om lovens geografiske område (§ 4). Disse regler omtales i det følgende.

2.1.1.1. Lovens område

Persondatalovens § 1 beskriver nærmere, hvornår loven som udgangspunkt finder anvendelse. Det følger således af lovens § 1, stk. 1, at loven gælder for behandlinger af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehand-

[3] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.
[4] Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.
[5] Jf. pkt. 2 i de almindelige bemærkninger til lovforslag nr. L 147 af 9. december 1999 og Registerudvalgets betænkning nr. 1345 (1997) om behandling af personoplysninger, s. 32-34.

ling, og for ikke-elektronisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Loven gælder tillige for anden ikke-elektronisk systematisk behandling, som udføres for private, og som omfatter oplysninger om personers private eller økonomiske forhold, som med rimelighed kan forlanges unddraget offentligheden, jf. § 1, stk. 2.

Lovens § 5, stk. 1-3, §§ 6-8, § 10, § 11, stk. 1, § 38 og § 40 gælder også for manuel videregivelse af personoplysninger til en anden forvaltningsmyndighed, jf. § 1, stk. 3.

Endvidere gælder persondataloven i et vist omfang for behandling af oplysninger om virksomheder mv., jf. § 1, stk. 4-7.

Persondataloven gælder endelig for enhver form for behandling af personoplysninger i forbindelse med tv-overvågning, jf. § 1, stk. 8.

Lovens § 2 beskriver en række tilfælde, hvor persondataloven ikke finder anvendelse.

Heraf skal særligt nævnes lovens § 2, stk. 1, hvorefter regler om behandling af personoplysninger i anden lovgivning, som giver den registrerede en bedre retsstilling, går forud for reglerne i persondataloven. Et eksempel herpå er tavshedspligtsreglerne i den finansielle lovgivning.

Persondataloven finder anvendelse, hvis regler om behandling af personoplysninger i anden lovgivning giver den registrerede en dårligere retsstilling. Dette gælder dog ikke, hvis den dårligere retsstilling har været tilsigtet og i øvrigt ikke strider mod databeskyttelsesdirektivet.

Det følger desuden af lovens § 2, stk. 2, at loven ikke finder anvendelse, hvis anvendelsen vil være i strid med informations- og ytringsfriheden, jf. Den Europæiske Menneskerettighedskonventions artikel 10.

Persondataloven gælder ikke for behandlinger, som en fysisk person foretager med henblik på udøvelse af aktiviteter af rent privat karakter, jf. lovens § 2, stk. 3.

Udtrykket "rent privat karakter" dækker over forskellige typer af behandlinger, som privatpersoner foretager i forbindelse med udøvelse af personlige eller familiemæssige aktiviteter. Der skal være tale om sædvanlige og legitime private aktiviteter, således at bestemmelsen ikke anvendes til at omgå reglerne for lovlig behandling. De aktiviteter, der

efter bestemmelsen undtages fra lovens område, kan være reguleret i anden lovgivning, herunder bl.a. i straffelovens kapitel 27 om freds- og ærekrænkelser.

Lovens § 2, stk. 4, indebærer, at persondatalovens regler om den registreredes rettigheder kun i begrænset omfang finder anvendelse på behandlinger, der foretages for domstolene, politiet og anklagemyndigheden inden for det strafferetlige område.

Persondataloven finder ikke anvendelse på behandling af oplysninger, der foretages for Folketinget og institutioner med tilknytning dertil, jf. § 2, stk. 5.

Reglerne i persondatalovens § 2, stk. 6-10, indebærer endvidere, at mediernes behandlinger af personoplysninger i vidt omfang er undtaget fra lovens område.

Endelig gælder persondataloven ikke for behandlinger, der udføres for politiets og forsvarets efterretningstjenester, jf. § 2, stk. 11.

2.1.1.2. Lovens geografiske område

Persondataloven gælder for behandling af oplysninger, som udføres for en dataansvarlig[6], der er etableret[7] i Danmark, hvis aktiviteterne finder sted inden for Det Europæiske Fællesskabs område, jf. § 4, stk. 1. Det bemærkes, at Færøerne og Grønland ikke anses for dansk område efter bestemmelsen, men for tredjelande[8].

Uden for bestemmelsen falder de tilfælde, hvor en dataansvarlig, som er etableret uden for dansk område, f.eks. i en anden medlemsstat, udøver aktiviteter på dansk område. Dog gælder lovens sikkerhedsregler for behandlinger, som foretages af databehandlere[9] i Danmark, uanset behandlingen i øvrigt er undergivet en anden medlemsstats lovgivning, jf. § 41, stk. 3, 2. pkt., der omtales nærmere under punkt 2.1.2.1. Endvidere gælder lovens regler om Datatilsynets jurisdiktionskompetence i relation til sådanne behandlinger, jf. § 64, stk. 1. Tilsynets kompetence udøves i så fald på baggrund af fremmed ret, jf. det under punkt 2.4.1.5 anførte.

---

[6] Ved en dataansvarlig forstås ifølge persondatalovens § 3, nr. 4, 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.

[7] Etablering i bestemmelsens forstand foreligger, når der er tale om faktisk udøvelse af aktiviteter gennem en mere permanent struktur. Den pågældende strukturs retlige form er uden betydning. Omfattet vil således kunne være aktiviteter, der udøves af såvel filialer som datterselskaber med status som juridisk person.

[8] Et tredjeland er en stat, som ikke indgår i Det Europæiske Fællesskab, og som ikke har gennemført aftaler, der er indgået med Det Europæiske Fællesskab, og som indeholder regler svarende til direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, jf. persondatalovens § 3, nr. 9.

[9] Ved en databehandler forstås ifølge persondatalovens § 3, nr. 5, den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne.

Hvis en dataansvarlig er etableret på dansk område, følger det af § 4, stk. 1, at den dataansvarliges behandlinger vil være omfattet af lovens regulering, uanset om de aktiviteter, som behandlingerne knytter sig til, udøves på dansk område eller ej. Dette gælder dog kun, hvis der er tale om aktiviteter, som den dataansvarlige udøver inden for Det Europæiske Fællesskabs område.

En dataansvarlig, der er etableret i Danmark, og som foretager behandling af oplysninger i et tredjeland, uden at behandlingen har nogen tilknytning til Det Europæiske Fællesskabs område, vil således ikke være omfattet af lovens regulering. Derimod vil den behandling af oplysninger, som en dataansvarlig, der er etableret i Danmark, overlader til en databehandler i et tredjeland at foretage, være omfattet af lovens anvendelsesområde. En betingelse er dog, at databehandlingen har tilknytning til aktiviteter på Det Europæiske Fællesskabs område.

Er en dataansvarlig på samme tid etableret i Danmark og i en anden medlemsstat, finder lovens regler begrænset anvendelse. Hvis et selskab, som er etableret i en anden medlemsstat, etablerer en filial i Danmark, vil lovens regler kun finde anvendelse på denne filials aktiviteter. Det gælder dog kun i det omfang aktiviteterne finder sted inden for Fællesskabets område, jf. herved § 4, stk. 1. Den pågældende filial skal i givet fald opfylde lovens regler.

Persondataloven finder ifølge § 4, stk. 3, også anvendelse, hvis den dataansvarlige er etableret i et tredjeland, og behandlingen af oplysninger sker under benyttelse af hjælpemidler, der befinder sig i Danmark, medmindre hjælpemidlerne kun benyttes med henblik på forsendelse af oplysninger gennem Det Europæiske Fællesskabs område. Loven finder endvidere anvendelse, hvis indsamling af oplysninger i Danmark sker med henblik på behandling i et tredjeland.

I de tilfælde, hvor der anvendes hjælpemidler her i landet, skal den dataansvarlige udpege en repræsentant, som er etableret i Danmark, jf. § 4, stk. 4, og underrette Datatilsynet om, hvem der er udpeget som repræsentant. Som eksempel på et hjælpemiddel er i forarbejderne til loven nævnt teknisk udstyr. Det er uden betydning, om det er edb-baseret eller ej.

Lovens § 4, stk. 3, indebærer, at hvis en dataansvarlig, der er etableret i et tredjeland, benytter et edb-servicebureau eller en databehandler i Danmark, gælder persondataloven. Persondataloven vil dog kun gælde for den faktiske behandling, der finder sted her i landet.

2.1.2. Persondatalovens bestemmelser om behandlingssikkerhed

Persondatalovens kapitel 11 (§§ 41-42) indeholder bestemmelser om såkaldt behandlingssikkerhed, det vil sige krav til, hvordan personoplysninger skal beskyttes mod uvedkommendes adgang, misbrug eller anden behandling i strid med loven.

I tilknytning til reglerne i kapitel 11 om behandlingssikkerhed har Justitsministeriet i medfør af § 41, stk. 5, udstedt bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles af den offentlige forvaltning[10] (**sikkerhedsbekendtgørelsen**) og bekendtgørelse nr. 535 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for domstolene. Sidstnævnte bekendtgørelse omtales ikke yderligere i nærværende rapport.

Der kan endvidere i forbindelse med konkrete behandlinger af personoplysninger fastsættes vilkår om bl.a. sikkerhed. Det følger således af lovens § 9, stk. 3, at der kan fastsættes vilkår for behandlingen af oplysninger, der sker med henblik på at føre retsinformationssystemer, ligesom det følger af § 50, stk. 5, at Datatilsynet over for private dataansvarlige i visse tilfælde kan fastsætte vilkår til beskyttelse af de registreredes privatliv ved behandling af følsomme oplysninger, behandling af oplysninger i forbindelse med førelse af advarselsregister/spærreliste, kreditoplysningsbureau, stillingsbesættende virksomhed og retsinformationssystemer samt ved overførsel af oplysninger til tredjelande. Datatilsynet har udnyttet denne mulighed til at fastsætte vilkår, herunder vilkår om datasikkerhed.

2.1.2.1. Persondatalovens § 41

Det følger af § 41, stk. 1, at personer, virksomheder mv., der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, kun må behandle disse efter instruks fra den dataansvarlige, medmindre andet følger af lov eller bestemmelser fastsat i henhold til lov. Bestemmelsen gælder også for en eventuel databehandler[11].

Der gælder ikke særlige formkrav til instrukserne. En instruks kan efter omstændighederne følge af en bestemt stillingsbetegnelse eller af det forhold, at den dataansvarlige autoriserer en ansat eller andre til at have adgang til bestemte oplysninger.

Kravet om, at vedkommende person mv. kun må behandle oplysninger i overensstemmelse med instruks fra den dataansvarlige, indebærer bl.a., at personen mv. ikke må behandle oplysninger til andre formål end dem, som den dataansvarlige har fastsat – herunder ikke til egne formål – samt at vedkommende ikke må behandle oplysninger efter

[10] Ved bekendtgørelse nr. 201 af 22. marts 2001 er bekendtgørelsens § 2, stk. 2, ændret.

instruks fra andre end den dataansvarlige. Dette gælder dog ikke, hvis andet følger af lovgivningen.

En databehandler, f.eks. et edb-servicebureau, må ikke 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.

De overordnede krav til den dataansvarliges behandlingssikkerhed fremgår af § 41, stk. 3, 1. pkt., hvoraf følger, at 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.

Det forudsættes i databeskyttelsesdirektivets artikel 17, stk. 2, at foranstaltningerne under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse, vil tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes.

Datatilsynet har givet udtryk for, at pligten til at træffe sikkerhedsforanstaltninger efter persondataloven er ufravigelig og ikke bortfalder, selv om den registrerede har givet sit samtykke hertil.[12]

Det følger af § 41, stk. 3, 2. pkt., at pligten i medfør af 1. pkt. gælder tilsvarende for databehandlere. Databehandlerens pligt er således ikke begrænset til den aftale, der er indgået mellem den dataansvarlige og databehandleren, men databehandleren har en *selvstændig pligt* til at sørge for, at kravene i § 41, stk. 3, bliver overholdt.

Databehandlerens forpligtelser gælder, uanset om der er tale om en databehandler, der foretager behandling af oplysninger for en dataansvarlig, der er etableret i Danmark, eller en dataansvarlig uden for Danmark, herunder i en anden medlemsstat. Hvis databehandleren udøver sin virksomhed på dansk område, gælder reglen om behandlingssikkerhed.

Dette indebærer, at de særlige sikkerhedsbestemmelser for *databehandlere*, som er fastsat i en EU-medlemsstat, gælder for databehandlere, som er etableret i det pågældende land, uanset om vedkommende databehandler udfører behandling for dataansvarlige i andre medlemsstater. Omvendt vil de særlige sikkerhedsbestemmelser for *databehandlere*, som er fastsat i den medlemsstat, hvor den dataansvarlige er etableret, ikke gælde for en sådan behandling, hvis databehandleren er etableret i en anden medlemsstat. Der-

[12] Jf. Datatilsynets årsberetning 2005, side 69 f.

imod skal den *dataansvarlige* iagttage de sikkerhedsbestemmelser og de behandlingsregler, regler om rettigheder for den registrerede mv., som er gældende i den medlemsstat, hvor den dataansvarlige er etableret, uanset om databehandleren er etableret i en anden medlemsstat.

Lovens § 41, stk. 4, indeholder den såkaldte "krigsregel", hvorefter der for så vidt angår 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.

Bestemmelsen omfatter behandlinger af oplysninger, som en besættelsesmagt eller en magt, der har erobret en del af landet, vil have særlig interesse i bl.a. for dermed hurtigt og effektivt at kunne overtage den almindelige administration.

Reglen indebærer ikke, at de omtalte oplysninger nødvendigvis skal bortskaffes eller destrueres i tilfælde af krig eller lignende forhold. Bestemmelsen sikrer blot, at der lovligt vil kunne træffes beslutning om destruktion mv., hvis det skulle vise sig nødvendigt. Det påhviler den dataansvarlige at træffe de foranstaltninger, som muliggør destruktion mv.

Reglen i stk. 4 indebærer, at ikke alle behandlinger – offentlige eller private – vil kunne udføres af en databehandler i et andet EU-land, hvilket ellers er lovens hovedregel. Det antages således, at f.eks., at Det Centrale Kriminalregister og Det Centrale Personregister ikke må føres i udlandet.

Bestemmelsen i § 41, stk. 5, indeholder en bemyndigelse for justitsministeren til at fastsætte nærmere regler om de i stk. 3 anførte sikkerhedsforanstaltninger. Bemyndigelsen er som anført under punkt 2.1.2 benyttet til bl.a. at udstede sikkerhedsbekendtgørelsen, som vedrører sikkerhedsforanstaltninger til beskyttelse af personoplysninger, der behandles for den offentlige forvaltning.

I tilknytning til sikkerhedsbekendtgørelsen har Datatilsynet udstedt sikkerhedsvejledningen[13], der nærmere beskriver, hvordan kravene i bekendtgørelsen vil kunne opfyldes.

2.1.2.2. Datasikkerhed i den offentlige forvaltning

For så vidt angår fastlæggelsen af kravene til datasikkerhed i den offentlige forvaltning må der skelnes mellem behandling af oplysninger i manuelle registre og behandling af oplysninger, der foretages helt eller delvis ved hjælp af elektronisk databehandling, idet

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

sikkerhedsbekendtgørelsen alene finder anvendelse på sidstnævnte behandlingsform, jf. bekendtgørelsens § 1.

Kravene til behandling af oplysninger i manuelle registre følger således alene af bestemmelsen i persondatalovens § 41, stk. 3.

Sikkerhedsbekendtgørelsen stiller bl.a. krav om, at den dataansvarlige myndighed fastsætter nærmere interne bestemmelser – der skal gennemgås mindst én gang om året – om sikkerhedsforanstaltninger i myndigheden til uddybning af de regler, som fremgår af bekendtgørelsen, jf. § 5.

Af bekendtgørelsens § 5 følger også, at der skal fastsættes retningslinjer for myndighedens tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat af myndigheden.

Det følger af § 8, at der på steder, hvor der foretages behandling af personoplysninger, skal træffes forholdsregler med henblik på at forhindre uvedkommendes adgang til oplysningerne.

Efter § 9 er det et krav, at den dataansvarlige myndighed i forbindelse med reparation og service af dataudstyr, samt ved salg og kassation af anvendte datamedier skal træffe de fornødne foranstaltninger for at sikre, at uvedkommende ikke får adgang til lagrede oplysninger.

Efter § 11, stk. 1, må kun personer, som autoriseres hertil, have adgang til de personoplysninger, der behandles. Der må kun autoriseres personer, som er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for, jf. § 11, stk. 2.

Den dataansvarlige myndighed skal, jf. § 12, træffe foranstaltninger for at sikre, at kun autoriserede brugere kan få adgang, og at disse kun kan få adgang til de personoplysninger og anvendelser, som de er autoriserede til.

Såfremt der etableres eksterne kommunikationsforbindelser, må disse kun etableres, hvis der træffes særlige foranstaltninger for at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger, jf. § 14. Det indebærer ifølge Datatilsynets sikkerhedsvejledning bl.a., at der ved transmission af fortrolige og følsomme personoplysninger over åbne net (f.eks. internettet) skal foretages kryptering.

Behandlinger af personoplysninger der er anmeldelsespligtige[14], skal ske under iagttagelse af de supplerende sikkerhedsbestemmelser i sikkerhedsbekendtgørelsens kapitel 3 (§§ 15-19).

Det følger af § 16, at autorisationer skal angive, i hvilket omfang brugeren må forespørge, inddatere eller slette personoplysninger, og mindst hver halve år skal det, jf. § 17, kontrolleres, om de autoriserede personer fortsat opfylder betingelserne for de tildelte autorisationer.

Der skal endvidere foretages registrering med alle afviste adgangsforsøg, og hvis der inden for en fastsat periode er registreret et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg fra samme arbejdsstation eller med samme brugeridentifikation, skal der blokeres for yderligere forsøg, jf. § 18.

Bekendtgørelsens § 19 fastsætter de nærmere regler for, hvornår det skal foretages logning. Efter § 19, stk. 1, er det som udgangspunkt et krav, at der skal foretages logning af alle anvendelser af personoplysninger, og at loggen skal opbevares i seks måneder.

2.1.2.3. Datasikkerhed i den private sektor

Der er ikke fastsat uddybende regler for datasikkerheden i den private sektor, hvorfor det er bestemmelsen i persondatalovens § 41, stk. 3, som spørgsmål herom må afgøres efter.

Datatilsynet har imidlertid udtalt, at det er tilsynets opfattelse, at § 41, stk. 3, medfører, at der som udgangspunkt må stilles samme krav til datasikkerheden i den private sektor som i den offentlige forvaltning[15]. Tilsynet anbefaler derfor generelt, at private dataansvarlige i videst muligt omfang tilrettelægger deres sikkerhedsforanstaltninger i overensstemmelse med sikkerhedsbekendtgørelsen.

Der forekommer fravigelser fra dette udgangspunkt. Et eksempel er de divergerende krav til datasikkerhed ved transmission af oplysninger over internettet.

Private dataansvarlige skal således ifølge Datatilsynet kun foretage kryptering ved overførsel af personnumre og følsomme oplysninger via hjemmesider og i de tilfælde, hvor behandlingen af personoplysninger i den private sektor sker efter tilladelse med vilkår om konkrete sikkerhedsforanstaltninger ved transmission over internettet. I en række

[14] Reglerne om anmeldelse af behandlinger, der foretages for den offentlige forvaltning, fremgår af persondatalovens kapitel 12 og bekendtgørelse nr. 529 af 15. juni 2000 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning. Reglerne er kort omtalt under punkt 2.4.1.8, men gennemgås ikke herudover nærmere i denne rapport.
[15] Jf. Datatilsynets årsberetning 2001, side 68 f.

andre situationer anbefaler Datatilsynet, at personoplysninger beskyttes, når de overføres via internettet. Datatilsynets vilkår om datasikkerhed omtales under punkt 2.1.2.4.

Derimod skal offentlige myndigheder foretage kryptering ved enhver transmission af fortrolige og følsomme oplysninger via internettet. Kravene til den offentlige sektor gælder uanset, hvordan transmissionen sker.

Datatilsynets hjemmesidetekst om krav og anbefalinger i forbindelse med overførsel af personoplysninger via internettet i den private sektor vedlægges som **bilag 1**.

2.1.2.4. Vilkår om datasikkerhed

Persondatalovens § 9 fastsætter de nærmere regler om behandling af oplysninger med henblik på at føre et retsinformationssystem. Af § 9, stk. 3, fremgår, at tilsynsmyndigheden kan meddele nærmere vilkår for behandlingen af oplysninger. Vilkårene fastsættes i forbindelse med den dataansvarliges anmeldelse til Datatilsynet og tilsynets efterfølgende udtalelse, jf. § 45, stk. 1, nr. 2 (hvis den dataansvarlige er en offentlig myndighed), eller tilladelse, jf. § 50, stk. 1, nr. 5 (hvis den dataansvarlige er en privat virksomhed mv.).

Det følger af § 50, stk. 1, at Datatilsynets tilladelse skal indhentes, før der iværksættes en behandling af oplysninger, som er omfattet af private dataansvarliges anmeldelsespligt i § 48, når behandlingen omfatter følsomme oplysninger (§ 50, stk. 1, nr. 1), behandlingen sker med henblik på at føre et advarselsregister (nr. 2), behandlingen sker med henblik på at drive virksomhed som kreditoplysningsbureau (nr. 3), behandlingens sker med henblik på at drive stillingsbesættende virksomhed (nr. 4), eller behandlingen sker med henblik på at føre retsinformationssystemer (nr. 5).

Datatilsynets tilladelse skal ifølge § 50, stk. 2, endvidere indhentes ved overførsel af oplysninger som nævnt i § 50, stk. 1, til tredjelande i medfør af § 27, stk. 1, og stk. 3, nr. 2-4.

Bestemmelsen i § 50, stk. 3, indeholder en bemyndigelse for justitsministeren til at fastsætte undtagelser fra bestemmelserne i § 50, stk. 1, nr. 1, og stk. 2. Bestemmelsen er benyttet til at fastsætte bekendtgørelse nr. 534 af 15. juni 2000 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for en privat dataansvarlig[16] (undtagelsesbekendtgørelsen). Undtagelsesbekendtgørelsen fastsætter alene undtagelser fra bestemmelsen i § 50, stk. 1, nr. 1.

[16] Ved bekendtgørelse nr. 202 af 22. marts 2001 er § 2, stk. 3, indsat i bekendtgørelsen, og ved bekendtgørelse nr. 410 af 9. maj 2012 er § 2, stk. 3, ændret.

Justitsministeren kan endvidere fastsætte regler om, at der forinden iværksættelse af andre anmeldelsespligtige behandlinger end de i § 50, stk. 1 og 2, nævnte skal indhentes tilladelse fra tilsynet, jf. § 50, stk. 4. Denne bemyndigelse er ikke udnyttet.

Det følger af § 50, stk. 5, at Datatilsynet i forbindelse med meddelelse af tilladelse efter stk. 1, 2 eller 4 kan fastsætte nærmere vilkår for udførelsen af behandlingerne til beskyttelse af de registreredes privatliv, jf. § 50, stk. 5.

Fastsættelsen af vilkår sker principielt altid på grundlag af en konkret vurdering i den enkelte sag. I praksis har Datatilsynet dog på en række områder fastsat standardvilkår, der om nødvendigt kan tilpasses den dataansvarlige. Standardvilkårene vil typisk omfatte et eller flere vilkår om datasikkerhed.

Datatilsynet har fastsat standardvilkår for (vedlægges samlet som **bilag 2**):

- private forskningsprojekter – vilkårene vedlægges i bilag 2
- privathospitaler – et eksempel på en tilladelse med vilkår vedlægges i bilag 2
- advarselsregistre – et eksempel på en tilladelse med vilkår vedlægges i bilag 2
- spærrelister – et eksempel på en tilladelse med vilkår vedlægges i bilag 2
- kreditoplysningsbureauer – et eksempel på en tilladelse med vilkår vedlægges i bilag 2
- retsinformationssystemer – vilkårene vedlægges i bilag 2

I forhold til private forskningsprojekter vil der således typisk blive fastsat bl.a. følgende vilkår for så vidt angår elektroniske behandlede oplysninger:

- ”Identifikationsoplysninger skal krypteres eller erstattes af et kodenummer el. lign. Alternativt kan alle oplysninger lagres krypteret. Krypteringsnøgle, kodenøgle mv. skal opbevares forsvarligt og adskilt fra personoplysningerne.
- Adgangen til projektdata må kun finde sted ved benyttelse af et fortroligt password. Password skal udskiftes mindst én gang om året, og når forholdene tilsiger det.
- Ved overførsel af personhenførbare oplysninger via Internet eller andet eksternt netværk skal der træffes de fornødne sikkerhedsforanstaltninger mod, at oplysningerne kommer til uvedkommendes kendskab. Oplysningerne skal som minimum være forsvarligt krypteret under hele transmissionen. Ved anvendelse af interne net skal det sikres, at uvedkommende ikke kan få adgang til oplysningerne.
- Udtagelige lagringsmedier, sikkerhedskopier af data m.v. skal opbevares forsvarligt aflåst og således, at uvedkommende ikke kan få adgang til oplysningerne.”

For så vidt angår manuelt behandlede oplysninger, vil der typisk blive fastsat følgende vilkår i forhold til private forskningsprojekter:

- ”Manuelt projektmateriale, udskrifter, fejl- og kontrollister, m.v., der direkte eller indirekte kan henføres til bestemte personer, skal opbevares forsvarligt aflåst og på en sådan måde, at uvedkommende ikke kan gøre sig bekendt med indholdet.”

Endvidere vil der i forhold til private forskningsprojekter, hvor der gøres brug af en databehandler, typisk blive fastsat følgende vilkår:

- ”Datatilsynets vilkår gælder også ved behandling hos databehandler.
- Ved behandling hos databehandler skal der indgås en skriftlig aftale herom mellem den dataansvarlige og databehandleren. Det skal fremgå af aftalen, at databehandleren alene handler efter instruks fra den dataansvarlige, og at oplysninger ikke må anvendes til databehandlerens egne formål. Databehandleren skal desuden give den dataansvarlige tilstrækkelige oplysninger til, at denne til enhver tid kan sikre sig, at Datatilsynets vilkår kan overholdes, og at de bliver overholdt.
- Hvis databehandleren er etableret i en anden medlemsstat, skal det desuden fremgå af aftalen, at de yderligere bestemmelser om sikkerhedsforanstaltninger for databehandlere, som eventuelt er fastsat i den medlemsstat, hvor databehandleren er etableret, også er gældende for databehandleren.”

I forhold til privathospitaler vil der typisk blive fastsat vilkår om, at behandling af personoplysninger skal ske under iagttagelse af en række sikkerhedsregler, som i vidt omfang svarer til sikkerhedsbekendtgørelsens regler.

I forhold til advarselsregistre vil der typisk blive fastsat følgende vilkår om datasikkerhed:

- ”Oplysningerne skal ajourføres løbende. Hvis der udsendes advarselslister i papirform, skal disse udsendes mindst hver 3. måned. Straks efter modtagelsen, skal medlemmet/deltageren i ordningen destruere tidligere modtagne lister el. lign., hvilket skal angives af [X] i forbindelse med udsendelsen. Kravet om destruktion af tidligere lister gælder også lister i elektronisk form, der er hentet fra en hjemmeside, eller som medlemmet/deltageren i ordningen har modtaget via e-post, CD-rom eller diskette.
- Der skal hos [X] og medlemmerne/deltagerne i ordningen træffes de fornødne sikkerhedsforanstaltninger til sikring af, at oplysninger i registeret ikke misbruges eller kommer til uvedkommendes kendskab.
- Hvis der anvendes advarselslister i papirform, skal disse opbevares aflåst, når de ikke benyttes. Det samme gælder lister i elektronisk form, der er hentet fra en hjemmeside, eller som deltageren i ordningen har modtaget via e-post, CD-rom eller diskette.
- Ved indberetning eller videregivelse via en hjemmeside på internettet eller ved fremsendelse af indberetninger eller advarselslister ved brug af e-post skal der anvendes en forsvarlig kryptering.
- Hvis der gives brugerne af listen adgang til oplysningerne via en hjemmeside, må dette alene ske efter indtastning af bruger id og adgangskode (password). [X] skal være i besiddelse af oplysninger om, hvem der har fået tildelt adgang, således at forpligtelsen efter vilkår [Y] til at foretage berigtigelse kan efterleves.
- Der må ikke videregives oplysninger fra advarselslisten telefonisk.”

I forhold til spærrelister vil der typisk blive fastsat bl.a. følgende vilkår om datasikkerhed:

- "Oplysningerne på spærrelisten skal ajourføres løbende.
- Der skal hos [X] og betalingsmodtagere træffes de fornødne sikkerhedsforanstaltninger til sikring af, at oplysninger på spærrelisten ikke misbruges eller kommer til uvedkommendes kendskab."

I forhold til kreditoplysningsbureauer vil der typisk blive fastsat bl.a. følgende vilkår om datasikkerhed:

- "Der skal hos [X] og bureauets abonnenter træffes de fornødne sikkerhedsforanstaltninger til sikring af, at oplysninger i registeret ikke misbruges eller kommer til uvedkommendes kendskab
- Fremsendelse af oplysninger over det åbne internet må alene ske i forsvarlig krypteret form.
- Hvis der gives bureauets abonnenter adgang til oplysningerne via en hjemmeside, skal der endvidere etableres en ordning, således at der kun gives adgang til oplysningerne efter indtastning af en adgangskode (password). Hvis oplysningerne gøres tilgængelige over det åbne internet, skal oplysningerne sendes i forsvarlig krypteret form.

Datatilsynet har også fastsat standardvilkår for sikkerhed vedrørende personaleadministration og klientjournaler.

Datatilsynet har endvidere fastsat standardvilkår for stillingsbesættende virksomhed. Disse vedlægges ikke, da de ikke indeholder vilkår om datasikkerhed.

2.1.2.5. Persondatalovens § 42

Det følger af § 42, stk. 1, at den dataansvarlige – når denne overlader en behandling af oplysninger til en databehandler – skal sikre sig, at databehandleren kan træffe de i § 41, stk. 3-5, nævnte tekniske og organisatoriske foranstaltninger, og at den dataansvarlige skal påse, at dette sker.

Den dataansvarlige skal således aktivt sikre, at de krævede sikkerhedsforanstaltninger overholdes hos databehandleren. Den dataansvarlige kan vælge selv at udføre kontrollen med databehandleren, men det kan også være relevant at indhente en årlig revisionserklæring fra en uafhængig tredjepart.

Gennemførelsen af en behandling af oplysninger ved en databehandler skal ske i henhold til en skriftlig aftale parterne imellem, jf. § 42, stk. 2, 1. pkt. Det skal fremgå af aftalen, at databehandleren alene handler efter instruks fra den dataansvarlige, og at reglerne i § 41, stk. 3-5, ligeledes gælder for behandlingen ved databehandleren.

Er den dataansvarlige en offentlig myndighed, følger det af sikkerhedsbekendtgørelsens § 7, stk. 1, 1. pkt., at det skal fremgå af den skriftlige databehandleraftale, at reglerne i sikkerhedsbekendtgørelsen ligeledes gælder for behandlingen ved databehandleren.

Hvis databehandleren er etableret i en anden medlemsstat, skal det fremgå af aftalen, at de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den medlemsstat, hvor databehandleren er etableret, gælder for denne, jf. § 42, stk. 2, 3. pkt.

2.1.3. Persondatalovens behandlingsregler

I persondatalovens kapitel 4 (§§ 5-14) er fastsat regler om, i hvilket omfang behandling af personoplysninger må finde sted. Bestemmelserne har til formål at yde den registrerede en beskyttelse i vid forstand.

I § 5 er fastsat en række grundlæggende principper for den dataansvarliges behandling af oplysninger. Disse principper skal ses i sammenhæng med bestemmelserne i §§ 6-13, hvori de nærmere betingelser for behandling af oplysninger er fastsat. I § 14 er fastsat regler om arkivering af oplysninger, der er omfattet af loven.

I de følgende afsnit gennemgås § 5 og bestemmelsens betydning for fastlæggelsen af kravene til datasikkerhed, ligesom de grundlæggende betingelser for behandling af oplysninger omtales.

2.1.3.1. Grundlæggende principper for behandling af personoplysninger

Som anført ovenfor indeholder § 5 en række grundlæggende principper for den dataansvarliges behandling af oplysninger. Disse krav skal altid være opfyldt.

Af § 5, stk. 1, følger, at oplysninger skal behandles i overensstemmelse med god databehandlingsskik. Det vil sige, at behandlingen skal være rimelig og lovlig. Heri ligger navnlig, at den dataansvarlige nøje skal overholde reglerne i loven, såvel i ånd som bogstav, og ikke må forsøge at omgå reglerne.

Af persondatalovens § 5, stk. 2, følger, at indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål, og at senere behandling ikke må være uforenelig med disse formål (*finalité*-princippet).

Det følger endvidere af § 5, stk. 3, at oplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.

Af lovens § 5, stk. 4, følger, at behandling af oplysninger skal tilrettelægges således, at der foretages fornøden ajourføring af oplysningerne. Der skal endvidere foretages den fornødne kontrol for at sikre, at der ikke behandles urigtige eller vildledende oplysninger. Oplysninger, der viser sig urigtige eller vildledende, skal snarest muligt slettes eller berigtiges.

Endelig følger det af bestemmelsens stk. 5, at indsamlede oplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.

De grundlæggende principper har betydning for behandlingen af oplysninger *inden for* den enkelte offentlige myndighed eller private virksomhed mv., idet den dataansvarlige skal tilrettelægge sin behandling således, at den er i overensstemmelse med § 5 og § 41, stk. 3 (samt bestemmelserne i sikkerhedsbekendtgørelsen for så vidt angår den offentlige sektor).

Som eksempel herpå kan nævnes, at Datatilsynet i sit høringssvar[17] vedrørende Strukturkommissionens betænkning nr. 1434/2004 har påpeget, at en generel adgang til alle borgerrelaterede oplysninger i kommunale servicecentre efter tilsynets opfattelse er meget vidtgående og vanskelig at forene med § 5 og de generelle krav om datasikkerhed i lovens § 41, stk. 3, som bl.a. er udmøntet i sikkerhedsbekendtgørelsens § 11. Høringssvaret vedlægges som **bilag 3**.

§ 5 har ligeledes betydning i tilfælde, hvor der har været brud på datasikkerheden. Hvis oplysninger er kommet til uvedkommendes kendskab eller har været i risiko herfor, er det således Datatilsynets opfattelse, at det følger af kravet om god databehandlingsskik i § 5, stk. 1, at den dataansvarlige bør reagere med henblik på at begrænse skaden.

Afhængig af de konkrete omstændigheder kan det være påkrævet, at den dataansvarlige tager skridt til:

1. at påse, at data bliver slettet eller eventuelt afhentet eller returneret fra uberettigede modtagere,
2. at sørge for, at data slettes fra internettet, herunder fra søgemaskiner,
3. at sørge for hurtig underretning af de berørte personer,
4. at det langsigtet sikres, at situationen ikke gentager sig, f.eks. ved at interne retningslinjer og forretningsgange gennemgås, ved bedre instruktion af medarbejdere og/eller ved systemteknisk understøttelse af relevante forretningsgange i organisationen.

[17] Brev af 7. april 2004 til Indenrigs- og Sundhedsministeriet, Datatilsynets j.nr. 2004-122-0103.

2.1.3.2. Betingelser for behandling af personoplysninger

I lovens § 6, stk. 1, fastsættes de generelle betingelser for, hvornår behandling af oplysninger må finde sted. Bestemmelsen gælder som udgangspunkt for enhver behandling af oplysninger, der er omfattet af loven. Lovligheden af visse særlige former for behandlinger skal dog afgøres efter § 6, stk. 2-4, §§ 7-13 eller efter reglerne i lovens kapitel 5-7[18].

Anvendelsesområdet for § 6 omfatter således i praksis almindelige, ikke-følsomme oplysninger, det vil sige alle andre oplysninger end oplysninger om rent private forhold, jf. §§ 7-8.

En del af de oplysninger, der er omfattet af § 6, vil være fortrolige, mens andre ikke kan betegnes som fortrolige. I modsætning hertil anses oplysninger, der er omfattet af §§ 7-8, for såvel følsomme som fortrolige.

Af § 6, stk. 1, følger, at behandling af personoplysninger kun må finde sted, hvis en af de i nr. 1-7 angivne betingelser er opfyldt. Fælles for disse betingelseer – når bortses fra samtykkereglen i nr. 1 – at behandling kun kan ske, hvis den er *nødvendig* af hensyn til en række nærmere angivne interesser.

Efter § 7, stk. 1, må der som udgangspunkt ikke behandles oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold.

I § 7, stk. 2-7, angives de nærmere betingelser for, hvornår der alligevel må behandles følsomme oplysninger af den nævnte karakter. Af § 7, stk. 8, fremgår, at der for den offentlige forvaltning ikke må føres edb-registre med oplysninger om politiske forhold, som ikke er offentligt tilgængelige.

Det fremgår af bemærkningerne til § 7, at det med bestemmelsen tilsigtes at sikre et højt beskyttelsesniveau i forhold til den enkelte borger. Det indebærer, at behandlingsreglerne i bestemmelsens stk. 2-7 i videst muligt omfang forudsættes administreret på den måde, at der ikke uden samtykke registreres og videregives personoplysninger i videre udstrækning end efter den tidligere registerlovgivning.

§ 8 vedrører behandlingen af oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i § 7, stk. 1 nævnte.

---

[18] Som anført under punkt 2.1.1.1 vedrørende persondatalovens § 2, stk. 1, kan lovens regler om behandling af personoplysninger endvidere være fraveget ved regler i anden lovgivning.

Sådanne oplysninger må som udgangspunkt ikke behandles for den offentlige forvaltning, medmindre det er nødvendigt for varetagelsen af myndighedens opgaver, jf. § 8, stk. 1. § 8, stk. 2 og 3, angiver de nærmere betingelser for, hvornår en offentlige dataansvarlig kan videregive oplysninger omfattet af § 8.

Private må kun behandle sådanne andre følsomme personoplysninger, hvis den registrerede har givet sit udtrykkelige samtykke hertil, eller hvis det er nødvendigt til varetagelse af en berettiget interesse, og denne interesse klart overstiger hensynet til den registrerede, jf. § 8, stk. 4. § 8, stk. 5 angiver de nærmere betingelser for, hvornår en privat dataansvarlig kan videregive § 8-oplysninger.

For så vidt angår behandlingen af oplysninger om personnummer – der er en ikke-følsom, men fortrolig personoplysning – følger det af § 11, stk. 1, at offentlige myndigheder kan behandle oplysninger herom med henblik på en entydig identifikation eller som journalnummer.

Private må som udgangspunkt behandle oplysninger om personnummer, når det følger af lov eller bestemmelser fastsat i henhold til lov, eller den registrerede har givet sit udtrykkelige samtykke hertil, jf. § 11, stk. 2. nr. 1 og 2. Af § 11, stk. 2, nr. 3, og stk. 3, fremgår yderligere betingelser for, hvornår private kan behandle, herunder videregive, oplysninger om personnummer.

Som det fremgår, er der – afhængig af oplysningernes karakter – ganske betydelige forskelle på, hvor restriktive betingelser der gælder for behandling af personoplysninger, ligesom der i nogle tilfælde gælder forskellige betingelser afhængig af, om den dataansvarlige er en offentlig myndighed eller en privat virksomhed mv.

2.2. Regler om beskyttelse af personoplysninger på det finansielle område

2.2.1. Generelt om den finansielle lovgivning

Et grundlæggende formål med den finansielle lovgivning er at sikre den finansielle stabilitet. Derfor indeholder lovgivningen en række krav til finansielle virksomheder[19], der skal sikre, at virksomhederne drives på en forsvarlig måde, så kunderne kan have tiltro til, at deres midler bliver behandlet forsvarligt, og så virksomhederne ikke eksponeres for at lide tab som følge af misbrug og kriminalitet. Den finansielle lovgivnings krav til it-sikkerhed skal ses som udtryk herfor.

[19] Finansielle virksomheder er pengeinstitutter, forsikringsselskaber, realkreditinstitutter, fondsmæglerselskaber og investeringsforeningsselskaber.

Fokus for reglerne om beskyttelse af kundedata i den finansielle lovgivning er således at sikre, at der kun sker de transaktioner med kundernes midler, som kunderne ønsker, og som er aftalt med virksomhederne. Reglerne er udformet med henblik på at sikre, at de betalingsdata, der befinder sig i de finansielle virksomheder, og som udveksles mellem virksomhederne, er beskyttet imod at gå tabt, blive forvansket, ændret eller misbrugt til uretmæssigt at flytte eller fjerne midler. Udgangspunktet for den finansielle lovgivning er således fortrinsvis i økonomisk forstand at søge at sikre kundernes midler, men heri ligger også et behov for at sikre ægtheden af data, og at de ikke kan tilgås eller manipuleres af uvedkommende.

Dette afspejles også i det tilsyn med finansielle virksomheders it-sikkerhed, som Finanstilsynet udøver, og som alene er rettet mod de finansielle virksomheder og datacentraler mv. Finanstilsynet er således ikke en klageinstans i forhold til offentligheden. Hvis tilsynet modtager generelle klager over manglende datasikkerhed, vil tilsynet på grund af den skærpede tavshedspligt, som tilsynsarbejdet er underlagt, være afskåret fra at oplyse klageren om, hvorvidt klagen giver Finanstilsynet anledning til at tage en sag op, og hvilke tilsynsreaktioner oplysningerne i givet fald giver anledning til.

Den finansielle lovgivning indeholder tillige regler om finansielle virksomheders tavshedspligt, der har til formål at beskytte kunder imod, at ansatte i finansielle virksomheder uberettiget videregiver deres fortrolige oplysninger. Disse regler, der er klassiske tavshedspligtsregler, somikke er særligt knyttet til it-sikkerhed, forbyder ansatte i finansielle virksomheder og andre personer med tilknytning til virksomheden, herunder ledelsesmedlemmer, revisorer mv., uberettiget at videregive fortrolige oplysninger om kunder i virksomheden. Modtager Finanstilsynet en konkret klage over en uberettiget videregivelse, har tilsynet mulighed for at tildele klageren visse partsrettigheder og orientere vedkommende om eventuelle tilsynsreaktioner som følge af klagen.

2.2.2. Lov om finansiel virksomhed

2.2.2.1. Regler om it-sikkerhed og databehandling for pengeinstitutter

Lov om finansiel virksomhed[20] stiller i § 71 krav om, at en finansiel virksomhed, herunder et pengeinstitut, skal have effektive former for virksomhedsstyring, herunder betryggende kontrol- og sikringsforanstaltninger.

Disse krav er udmøntet i bekendtgørelse nr. 1321 af 25. november 2015 om ledelse og styring af pengeinstitutter m.fl., herunder i bekendtgørelsens bilag 5 om it-sikkerhed. Ifølge bekendtgørelsen skal virksomhedens bestyrelse fastsætte en it-sikkerhedspolitik, der ud fra den ønskede risikoprofil på it-området skal indeholde en overordnet stillingtagen til alle væsentlige forhold vedrørende it-sikkerheden. Hvad der er væsentligt, af-

[20] Lovbekendtgørelse nr. 182 af 18. februar 2015 med senere ændringer.

hænger bl.a. af virksomhedens størrelse samt omfanget og kompleksiteten af virksomhedens it-anvendelse. Væsentlige forhold omfatter bl.a. beskyttelse af systemer, data, maskinel og kommunikationsveje, funktionsadskillelse samt kontrol og rapportering.

Mere konkret, når der ses på eksempelvis området rettighedstildeling, adgangsstyring og logiske adgangskontroller, vil følgende være emner på en inspektion foretaget af Finanstilsynet:

- Periodisk revurdering af tildelte rettigheder, herunder vurdering af funktionsadskillelse/kompenserende kontroller ved tildeling af rettigheder.
- Funktionsadskillelse mellem udviklings-, test- og driftsmiljø. Politik for eksterne adgange til kritiske systemer. Udvidet adgang, systemadministratoradgange, adgang til kritiske data, konfigurationsfiler, logs, backup/produktionsdata mv. (risikovurderinger).
- Anvendelse af nødbrugere og midlertidige udvidede rettigheder og adgange.

Virksomhedens direktion er ansvarlig for, at it-sikkerhedspolitikken efterleves og uddybes i procedurer, herunder at funktionsadskillelsen bliver overvåget, at systemer og data klassificeres og prioriteres, at der sker adgangskontrol til systemer og data, samt at der udarbejdes en it-beredskabsplan.

Det følger endvidere af bekendtgørelsen, at pengeinstituttet m.fl. skal have metoder og procedurer, der er egnede til at opdage og mindske risikoen for virksomhedens manglende overholdelse af den for virksomheden gældende lovgivning, markedsstandarder eller interne regelsæt. Desuden skal virksomheden have en *compliance*-funktion, der fungerer uafhængigt, og som har til opgave at føre kontrol med virksomhedens overholdelse af lovgivning, markedsstandarder eller interne regelsæt.

Et pengeinstitut kan outsource opgaver, herunder databehandling.

Hvis et pengeinstitut outsourcer opgaver, skal instituttet sikre, at den virksomhed, opgaven outsources til, har betryggende sikkerheds- og kontrolprocedurer, og instituttet skal føre kontrol med, at outsourcing-virksomheden følger disse procedurer. Outsourcing af væsentlige opgaver skal meddeles Finanstilsynet.

2.2.2.2. Regler om it-sikkerhed og databehandling for fællesejede datacentraler

Fællesejede datacentraler[21] er reguleret af § 343 q i lov om finansiel virksomhed. Det følger af bestemmelsen, at en datacentral skal opfylde de samme krav til datasikkerhed, som gælder for finansielle virksomheder efter lovens § 71, jf. ovenfor.

En fællesejet datacentral er derudover underlagt bekendtgørelse om systemrevisionens gennemførelse i fælles datacentraler. Ved systemrevision forstås i henhold til denne bekendtgørelse intern og ekstern revision af, at de generelle it-kontroller, det vil sige styringen af den grundlæggende it-sikkerhed, men ikke sikkerheden i specifikke it-systemer, er og fungerer betryggende.
I bekendtgørelsen stilles der krav til den eksterne og interne systemrevision, den eksterne og interne systemrevisions protokol samt til erklæringer om system-, data- og driftssikkerheden i henhold til bekendtgørelsen. Revisionen skal blandt andet påse, om kravet om betryggende kontrol- og sikringsforanstaltninger tilgodeses i tilstrækkeligt omfang ved udvikling, vedligeholdelse og drift af datacentralens systemer, som har relation til de tilsluttede virksomheder, og om datacentralens forretningsgange, som har relation til de tilsluttede virksomheder, er tilrettelagt og fungerer på betryggende vis.

Reglerne for fælles datacentraler gælder også for datacentraler, der udfører både væsentlig it-drift og it-udvikling for den fælles betalingsinfrastruktur, jf. lov om finansiel virksomhed § 343 q, stk. 2.

2.2.2.3. Regler om videregivelse af fortrolige kundeoplysninger

Kapitel 9 i lov om finansiel virksomhed indeholder regler om finansielle virksomheders videregivelse og udnyttelse af fortrolige oplysninger.

Hovedbestemmelsen om videregivelse og udnyttelse af fortrolige oplysninger findes i § 117 og angiver, at ansatte og andre personer tilknyttet finansielle virksomheder ikke uberettiget må udnytte eller videregive fortrolige oplysninger, som de bliver bekendt med under udøvelsen af deres hverv.

Det fremgår af forarbejderne til bestemmelsen, at den – foruden at beskytte mod udlevering af fortrolige oplysninger om den finansielle virksomhed selv – også beskytter virksomhedens kunder mod uberettiget videregivelse eller udnyttelse af fortrolige oplysninger.

[21] Ved fælles datacentraler forstås ifølge § 343 q, stk. 1, virksomheder, hvis væsentligste aktiviteter omfatter it-drifts- eller -udviklingsopgaver for flere finansielle virksomheder, finansielle holdingvirksomheder eller sådanne virksomheders dattervirksomheder, og som overvejende er ejet af 1) en eller flere finansielle virksomheder, finansielle holdingvirksomheder eller sådanne virksomheders dattervirksomheder i forening eller 2) en eller flere foreninger, hvis medlemmer overvejende er finansielle virksomheder, finansielle holdingvirksomheder eller sådanne virksomheders dattervirksomheder.

Begrebet fortrolige oplysninger skal forstås bredt og omfatter alle oplysninger, som ikke er offentligt tilgængelige, herunder oplysninger om hvem der er kunder i en finansiel virksomhed og oplysninger om deres transaktioner.

Forbuddet mod videregivelse er begrænset til "uberettiget videregivelse". Ved vurderingen af, om en videregivelse er berettiget, skal der foretages en konkret afvejning af den finansielle virksomheds interesse i at kunne videregive oplysninger over for kundens berettigede forventning om, at oplysninger hemmeligholdes. Dette indebærer, at en finansiel virksomhed f.eks. har mulighed for at videregive fortrolige kundeoplysninger i forbindelse med outsourcing af opgaver, hvis en interesseafvejning fører til, at virksomhedens interesse i at kunne foretage en outsourcing overstiger kundernes forventning om hemmeligholdelse.

Videregives kundeoplysninger f.eks. som led i outsourcing, følger tavshedspligten oplysningerne efter, jf. § 117, stk. 2. Det indebærer, at personer, som de fortrolige oplysninger videregives til, vil være bundet af den samme tavshedspligt som gælder efter § 117, stk. 1.

Dette indebærer eksempelvis, at hvis et pengeinstitut videregiver fortrolige kundeoplysninger til en fællesejet datacentral, der løser opgaver for pengeinstituttet, vil de kundedata, som videregives, fortsat være beskyttet mod uberettiget videregivelse fra ansatte i datacentralen.

Reglerne i kapitel 9 træder i stedet for behandlingsreglerne i persondatalovens §§ 6-8, jf. punkt 2.1.1.1.

2.2.2.4. Whistleblowerordninger

I forbindelse med implementeringen af kapitalkravsdirektivet i dansk ret er der i lov om finansielle virksomheder § 75 a indført regler om, at alle finansielle virksomheder og betalingsinstitutter skal etablere whistleblowerordninger, så medarbejdere i virksomheden via en særlig, uafhængig og selvstændig kanal kan indberette overtrædelser eller potentielle overtrædelser af den finansielle lovgivning, herunder også af reglerne om, at virksomheden skal have et tilstrækkeligt it-sikkerheds- og kontrolniveau. Indberetningen sker til virksomheden selv med henblik på, at den kan rette op på de fejl eller svagheder, som kommer til dens kendskab. Finanstilsynet har samtidig indført en ordning, så man har mulighed for anonymt at orientere tilsynet om forhold, som tilsynet bør være opmærksomt på i forhold til de relevante virksomheder under tilsyn.

2.2.3. Lov om betalingstjenester og elektroniske penge

2.2.3.1. Lov om betalingstjenester og elektroniske penge (betalingstjenesteloven)[22] regulerer de virksomheder, som udfører betalingstjenester. Eksempler på betalingstjenester er blandt andet gennemførelse af betalingstransaktioner, herunder overførsel af midler til en betalingskonto, gennemførelse af betalingstransaktioner via et kreditkort, og udstedelse og indløsning af betalingsinstrumenter, f.eks. betalingskort.

Desuden indeholder loven de regulatoriske krav til virksomheder, der udfører betalingstjenester, og som ikke er pengeinstitutter omfattet af lov om finansiel virksomhed. Sådanne virksomheder er betalingsinstitutter og skal have tilladelse efter § 7 i betalingstjenesteloven.

En betingelse for at opnå og bevare en tilladelse som betalingsinstitut er, at virksomhedens forretningsgange, administrative forhold, organisation, regnskabsmæssige procedurer, revisionsmæssige foranstaltninger og kontrol- og sikkerhedsmæssige foranstaltninger er forsvarlige.

Desuden foreskriver lovens § 19, at et betalingsinstitut bl.a. skal have fyldestgørende interne kontrolprocedurer og betryggende kontrol- og sikkerhedsforanstaltninger på it-området. Kravet om betryggende it-forhold er analogt til kravene efter ledelsesbekendtgørelsen udstedt i medfør af lov om finansiel virksomhed § 71. Finanstilsynet vil derfor vurdere it-sikkerheden i sådanne institutter på samme måde som i finansielle virksomheder og fælles datacentraler.

Hvis et betalingsinstitut outsourcer opgaver, skal virksomheden sikre, at den virksomhed, opgaven outsources til, har betryggende sikkerheds- og kontrolprocedurer, herunder på it-området, og betalingsinstituttet skal føre kontrol med, at outsourcing-virksomheden følger disse.

Finanstilsynet skal endvidere give tilladelse til outsourcing af væsentlige opgaver. Det er i den forbindelse sædvanligt, at Finanstilsynet knytter betingelser til tilladelsen, særligt i form af *governance*-krav til styring og kontrol.

En outsourcende virksomhed skal føre løbende kontrol med, at leverandøren lever op til forpligtelserne i henhold til kontrakten. Når outsourcing vedrører it-funktioner, skal den outsourcende virksomhed have procedurer og retningslinjer til sikring af, at leverandøren overholder de relevante dele af outsourcers it-sikkerhedspolitik og sikkerhedsregler, og der skal aftales procedurer med leverandøren om, at outsourcer regelmæssigt kan kontrollere dette.

[22] Lovbekendtgørelse nr. 613 af 24. april 2015 med senere ændringer.

Der er endvidere krav om, at leverandøren forpligtes til at give Finanstilsynet, outsourcer og dennes revision alle nødvendige oplysninger om de outsourcede opgaver, ligesom Finanstilsynet mod behørig legitimation skal have adgang til leverandøren vedrørende den outsourcede aktivitet.

2.2.3.2. Betalingstjenestelovens § 85 indeholder regler om behandling af personoplysninger, herunder transaktionsdata.

Det følger af § 85, at der kun må ske behandling af oplysninger om, hvor betalere har anvendt deres betalingsinstrument, og hvad de har købt, når det er nødvendigt til gennemførelse eller korrektion af betalingstransaktioner, eller når det på anden saglig måde er nødvendigt. Bestemmelsen har følgende ordlyd:

> *"**§ 85.** Lov om behandling af personoplysninger finder anvendelse med de ændringer, der følger af stk. 2-6.*
> *Stk. 2. Betalerens udbyder skal sikre, at betalerens cpr-nummer på et betalingsinstrument ikke kan aflæses fysisk eller elektronisk af andre end betalerens udbyder.*
> *Stk. 3. Der må kun ske behandling af oplysninger om, hvor betalerne har anvendt deres betalingsinstrumenter, og hvad de har købt, når det*
> *1) er nødvendigt til gennemførelse eller korrektion af betalingstransaktioner eller andre funktioner, som betalerens udbyder har knyttet til betalingsinstrumentet,*
> *2) er nødvendigt til retshåndhævelse eller for at hindre misbrug eller*
> *3) er hjemlet ved anden lovgivning.*
> *Stk. 4. Der må endvidere ske behandling af oplysninger om, hvor betalerne har anvendt deres betalingsinstrumenter, når*
> *1) det er nødvendigt for betalerens udbyders rådgivning af en betaler med henblik på en hensigtsmæssig anvendelse af betalingsinstrumenter, og når de oplysninger, der frembringes, alene angår, hvilke typer betalingstransaktioner betaleren foretager, eller*
> *2) behandlingen er nødvendig for udstederens tilpasning af betalingssystemer, således at disse er sikre, effektive og tidssvarende og der ikke frembringes oplysninger på enkeltbrugerniveau.*
> *Stk. 5. Økonomi- og erhvervsministeren kan bestemme, at stk. 3 fraviges i forskningsøjemed.*
> *Stk. 6. Økonomi- og erhvervsministeren kan efter indhentet udtalelse fra Datatilsynet fastsætte regler om behandling i udlandet af de i stk. 3 nævnte oplysninger."*

Betalingstjenestelovens § 85 finder som udgangspunkt anvendelse på både udbydere af betalingstjenester og på andre virksomheder. Undtaget herfra er § 85, stk. 2, der kun finder anvendelse på udbydere af betalingstjenester.

Betalingstjenestelovens § 85 finder anvendelse på alle de betalingsinstrumenter, der er omfattet af loven, f.eks. et betalingskort eller en adgangskode til en netbank, og indehol-

der en udtømmende angivelse af, til hvilke formål der kan ske behandling af oplysninger om, hvor betalerne har anvendt deres betalingsinstrumenter, og hvad de har købt.

Betalingstjenestelovens § 85 omfatter som udgangspunkt behandling af oplysninger om både fysiske og juridiske personer, der optræder som betalere. Bestemmelsen er præceptiv i forbrugerforhold, jf. lovens § 5, stk. 1 og 2, modsætningsvis, hvilket betyder, at forbrugere ikke kan give samtykke til behandling af oplysninger, der er omfattet af § 85, med henblik på andre formål end dem, der er nævnt i § 85. Bestemmelsen kan fraviges ved aftale i erhvervsmæssige kundeforhold.

Formålet med bestemmelsen er at sikre, at oplysninger om hvor betalingsinstrumenterne har været anvendt, og hvad der er købt, ikke benyttes til uvedkommende formål eller i integritetskrænkende øjemed, idet oplysningerne kan være meget følsomme. Oplysningerne må således ikke benyttes til for eksempel opstilling af forbrugsprofiler eller kortlægning af brugernes forbrugsmønstre. Sådanne oplysninger vil kunne danne grundlag for den erhvervsdrivendes egen markedsføring eller vil kunne sælges eller videregives til andre erhvervsdrivende med henblik på f.eks. markedsføring, kreditvurdering eller risikovurdering i forbindelse med tegning af forsikringer.

Betalingstjenestelovens § 85, stk. 1, præciserer, at persondataloven også gælder for den behandling af persondata, som finder sted i forbindelse med brug af betalingstjenester. Det antages i teorien, at betalingstjenestelovens § 85 er mere restriktiv end persondataloven.

Ud over persondataloven supplerer også markedsføringsloven[23] betalingstjenestelovens § 85 for så vidt angår anvendelse af oplysninger til markedsføringsmæssige formål.

Hertil kommer, at kapitel 9 i lov om finansiel virksomhed om videregivelse af fortrolige oplysninger, herunder tavshedspligtsbestemmelsen i § 117, finder anvendelse for de virksomheder, der er omfattet af lov om finansiel virksomhed, og som udbyder betalingstjenester, jf. herom punkt 2.2.2.3 ovenfor.

Betalingstjenestelovens § 85, stk. 3, slår fast, at der kun må behandles oplysninger om, hvor en betaler har anvendt sit betalingsinstrument, og hvad han har købt, når det er nødvendigt enten for at gennemføre eller korrigere betalingstransaktioner eller andre funktioner, som betalerens udbyder har knyttet til betalingsinstrumentet, eller nødvendigt på grund af retshåndhævelse eller for at hindre misbrug. Derudover vil behandlingen af oplysninger være lovlig, hvis den har hjemmel i anden lovgivning.

[23] Lovbekendtgørelse nr. 1216 af 25. september 2013 om markedsføring.

Derudover må der efter betalingstjenestelovens § 85, stk. 4, ske behandling af oplysninger om, hvor betaleren har brugt sit kort, når det er nødvendigt for rådgivning af betaleren for hensigtsmæssig anvendelse af betalingsmidler, eller hvor det er nødvendigt for udstederen for at tilpasse betalingssystemer under forudsætning af, at der ikke frembringes oplysninger på enkeltbrugerniveau.

Udtrykket "behandling" svarer til sprogbrugen og definitionen i persondataloven og dækker over "enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for", jf. persondatalovens § 3, nr. 2. Det antages, at begrebet "behandling" ikke blot omfatter registrering, opbevaring, videregivelse og samkøring af oplysninger, men enhver form for håndtering af oplysninger.[24]

Betalingstjenestelovens § 85, stk. 2–6, vedrører kun behandling af oplysninger om betalere, f.eks. brugere af betalingskort. Eventuel behandling af oplysninger om betalingsmodtagere (f.eks. forretninger, der modtager betaling med et betalingskort) er derimod alene underlagt den almindelige databeskyttelseslovgivning, markedsføringsloven, lov om finansiel virksomhed mv.

2.3. Andre relevante regler om beskyttelse af personoplysninger

2.3.1. Regler om beskyttelse af personoplysninger på sundhedsområdet

2.3.1.1. Generelt om lovgivningen på sundhedsområdet

I sundhedsvæsenet behandles en række følsomme oplysninger om borgernes helbred og sygdomme. Både i forbindelse med den primære patientbehandling og til sekundære formål såsom kvalitetssikring af behandlingen, forskning i nye behandlingsformer samt analyser af f.eks. af forbruget af sundhedsydelser og ventetider til undersøgelse og behandling.

Samtidig ændres behandlingsformerne, og en større og større del af patientens behandling sker nu i et samarbejde mellem sygehuse, egen læge, kommunen og andre. Derfor bliver behovet for at kunne dele data også større. Borgerne har en forventning om, at den sundhedsperson, der skal behandle dem, har de nødvendige oplysninger til rådighed, og kan ikke forstå, hvis de bliver spurgt om de samme oplysninger flere gange. Hertil kommer, at manglende adgang til nødvendige oplysninger kan forsinke behandlingen eller føre til fejlbehandling.

Derfor skal der i sundhedsvæsenet ske en konstant afvejning mellem behovet for patientsikkerhed og informationssikkerhed. Relevante data skal være til rådighed for det

[24] Jf. Lov om behandling af personoplysninger med kommentarer (Henrik Waaben og Kristian Korfits Nielsen, 3. udgave, 2015), s. 145-146.

relevante personale, når det er nødvendigt. Samtidig skal borgerne føle sig trygge og opleve sikkerhed om dataanvendelsen i sundhedsvæsenet.

Tidligere var antallet af medarbejdere, der havde adgang til elektroniske patientoplysninger meget mindre, og de havde typisk kun adgang til data inden for f.eks. eget sygehus eller område. Efterhånden er der etableret flere fælles nationale løsninger, og data deles i stigende grad på tværs af sundhedsvæsenet og mellem forskellige sektorer. Dette skyldes et øget behov for at kunne tilgå informationerne, uanset deres oprindelse eller fysiske placering, da patienten bevæger sig rundt i sundhedsvæsenet og på tværs af sektorer.

Patientoplysninger anvendes ikke kun i den primære patientbehandling, men også til forskning, administrative formål og til kvalitetssikring, både på lokalt og nationalt niveau. I mange tilfælde sker dette ved at etablere særskilte databaser, f.eks. de regionale og nationale kvalitetsdatabaser samt datavarehuse, hvor data bliver struktureret på en måde, som tilgodeser statistiske og forskningsmæssige formål.

For sundhedsdata gælder de almindelige regler i persondataloven om it-sikkerhed, men der er herudover fastsat regler i andre love, f.eks. sundhedsloven[25], om videregivelse og indberetning af oplysninger.

2.3.1.2. Regler om databehandling i forbindelse med den primære patientbehandling i sundhedsvæsenet

Databehandling i forbindelse med den primære patientbehandling skal sikre, at sundhedspersoner har de relevante oplysninger til rådighed om patienten i behandlingssituationen.

Persondatalovens krav om, at ansatte kun må have adgang til oplysninger, som de har behov for i forbindelse med løsningen af deres arbejdsopgaver, suppleres af bestemmelserne i sundhedsloven om, at adgangen skal være bestemt af, at der findes en eksisterende behandlingsrelation og af patientens ret til i visse tilfælde at frabede sig videregivelse eller elektronisk indhentning af deres patientoplysninger.

Sundhedslovens bestemmelser om videregivelse, indhentning af og adgang til oplysninger findes dels i sundhedslovens kapitel 9 om tavshedspligt, videregivelse og indhentning af helbredsoplysninger mv., dels i specifikke bestemmelser om konkrete registre/systemer, f.eks. §§ 156, 157 og 157 a om henholdsvis det Centrale Tilskudsregister, det Fælles Medicinkort og det Danske Vaccinationsregister.

[25] Lovbekendtgørelse nr. 1202 af 14. november 2014 med senere ændringer.

Databehandling sker i sundhedssektoren også til sekundære formål, det vil sige som led i andet end den direkte behandling. Formålet hermed er dels at sikre grundlaget for administrationen af sundhedsvæsenet (afregning, kvalitetssikring mv.), dels at give mulighed for registerforskning og statistisk bearbejdning og analyse til gavn for patienterne og samfundet.

Fælles for databehandlingerne er, at det er relevant at behandle store mængder personhenførbare oplysninger for at generere resultater, der ikke er personhenførbare. Nedenfor er det generelle regelsæt nærmere gennemgået.

2.3.1.2.1. Videregivelse af helbredsoplysninger mv. i forbindelse med og efter behandling af patienter

Det følger af sundhedslovens § 41, stk. 2, at sundhedspersoner til andre sundhedspersoner kan videregive oplysninger om patientens helbredsforhold, øvrige rent private forhold og andre fortrolige oplysninger i forbindelse med behandling af patienten eller behandling af andre patienter uden patientens samtykke, når:

1) det er nødvendigt af hensyn til et aktuelt behandlingsforløb for patienten, og videregivelsen sker under hensyntagen til patientens interesse og behov,
2) videregivelsen omfatter et udskrivningsbrev fra en læge, der er ansat i sygehusvæsenet, til patientens alment praktiserende læge eller den praktiserende speciallæge, der har henvist patienten til sygehusbehandling,
3) videregivelsen omfatter et udskrivningsbrev fra en læge, der er ansat på privatejet sygehus, klinik m.v., til de i nr. 2 nævnte læger, når behandlingen er ydet efter aftale med et regionsråd eller en kommunalbestyrelse i henhold til denne lov,
4) videregivelsen er nødvendig til berettiget varetagelse af en åbenbar almen interesse eller af væsentlige hensyn til patienten, herunder en patient, der ikke selv kan varetage sine interesser, sundhedspersonen eller andre,
5) videregivelsen sker til patientens alment praktiserende læge fra en læge, der virker som stedfortræder for denne,
6) videregivelsen sker til en læge, tandlæge eller jordemoder om en patient, som modtageren tidligere har deltaget i behandlingen af, når
    a) videregivelsen er nødvendig og relevant til brug for evaluering af modtagerens egen indsats i behandlingen eller som dokumentation for erhvervede kvalifikationer i et uddannelsesforløb og
    b) videregivelsen sker under hensyntagen til patientens interesse og behov, eller
7) videregivelsen sker til en studerende, der som led i en sundhedsvidenskabelig eller sundhedsfaglig uddannelse deltager i behandlingen af en patient uden at være medhjælp, når

a) videregivelsen er nødvendig for den studerendes forståelse af behandlingssituationen eller evaluering af den studerendes deltagelse i behandlingssituationen og
b) videregivelsen sker under hensyntagen til patientens interesse og behov.

Det følger endvidere af sundhedslovens § 41, stk. 1, at videregivelse af helbredsoplysninger mv. i forbindelse med behandling af patienten eller behandling af andre patienter kan ske til andre sundhedspersoner med patientens samtykke. Samtykket kan være mundtligt eller skriftligt. Samtykket kan afgives til den sundhedsperson, der videregiver oplysninger, eller til den sundhedsperson, der modtager oplysninger. Samtykket skal indføres i patientjournalen.

Den sundhedsperson, der er i besiddelse af en fortrolig oplysning, afgør, hvorvidt videregivelse efter de nævnte bestemmelser er berettiget.

Patienten kan ifølge § 41, stk. 3, frabede sig, at oplysninger videregives efter stk. 2, nr. 1-3, 6 og 7. Frabedelse af videregivelse skal dokumenteres på samme måde som et samtykke.

2.3.1.2.2. Indhentning af elektroniske helbredsoplysninger mv. i forbindelse med behandling af patienter

Det følger af sundhedslovens § 42 a, stk. 1, at læger, tandlæger, jordemødre, sygeplejersker, sundhedsplejersker, social- og sundhedsassistenter, radiografer og ambulancebehandlere med særlig kompetence ved opslag i elektroniske systemer i fornødent omfang kan indhente oplysninger om en patients helbredsforhold, øvrige rent private forhold og andre fortrolige oplysninger, når det er nødvendigt i forbindelse med aktuel behandling af patienten. Sundheds- og ældreministeren kan fastsætte regler om, at andre sundhedspersoner, der som led i deres virksomhed deltager i behandling af patienter, kan indhente oplysninger efter samme regler. Hjemlen er benyttet til at give kiropraktorer adgang til indhentning af helbredsoplysninger når det er nødvendigt i forbindelse med aktuel behandling af patienten, jf. bekendtgørelse om kiropraktorers adgang til indhentning af helbredsoplysninger mv. i elektroniske systemer[26].

Ovennævnte sundhedspersoner kan endvidere indhente oplysninger efter den såkaldte "værdispringsregel" i § 42 a, stk. 5, hvis indhentningen er nødvendig til berettiget varetagelse af en åbenbar almen interesse eller af væsentlige hensyn til patienten, herunder en patient, der ikke kan varetage sine interesser, sundhedspersonen eller andre patienter.

[26] Jf. bekendtgørelse nr. 13 af 11. januar 2013 om kiropraktorers adgang til indhentning af helbredsoplysninger m.v. i elektroniske systemer.

Andre sundhedspersoner end de ovennævnte kan ifølge § 42 a, stk. 2, ved opslag i elektroniske systemer, hvori adgangen for den pågældende sundhedsperson teknisk er begrænset til de patienter, der er i behandling på samme behandlingsenhed, som den pågældende sundhedsperson er tilknyttet, i fornødent omfang indhente oplysninger om aktuel behandling, når det er nødvendigt i forbindelse med aktuel behandling af patienten.

En læge, tandlæge eller jordemoder kan ifølge § 42 a, stk. 6, endvidere indhente oplysninger som nævnt i stk. 1 om patienter, som modtageren tidligere har deltaget i behandlingen af, hvis indhentningen er nødvendig og relevant til brug for evaluering af modtagerens egen indsats i behandlingen eller som dokumentation for erhvervede kvalifikationer i et uddannelsesforløb og indhentningen sker under hensyntagen til patientens interesse og behov. Indhentningen må kun ske i umiddelbar forlængelse af behandlingsforløbet og senest 6 måneder efter den indhentende læges, tandlæges eller jordemoders afslutning af behandlingen eller viderehenvisning af patienten, medmindre indhentningen er påkrævet som led i speciallæge- eller specialtandlægeuddannelsen.

Sundhedspersoner kan endvidere med patientens samtykke ved opslag i elektroniske systemer indhente oplysninger i forbindelse med behandling af patienter. Patienten kan frabede sig, at en sundhedsperson indhenter oplysninger, dog ikke indhentelse i medfør af den såkaldte "værdispringsregel", jf. ovenfor. Samtykket eller tilkendegivelse om frabedelse af indhentning af oplysninger kan være mundtligt eller skriftligt. Samtykket eller tilkendegivelsen skal meddeles til den sundhedsperson, som indhenter oplysningerne, eller under hvis ansvar oplysningerne indhentes. Samtykket eller tilkendegivelsen skal indføres i patientjournalen, jf. sundhedslovens § 42 b.

Det følger af § 42 a, stk. 10, at en sundhedsperson under dennes ansvar kan lade sekretærer yde teknisk bistand til opslag i oplysninger, som den pågældende sundhedsperson selv har adgang til.

2.3.1.2.3. Videregivelse af helbredsoplysninger mv. til andre formål

Det følger af sundhedslovens § 43, stk. 1, at sundhedspersoner med patientens samtykke til andre formål end behandling kan videregive oplysninger om patientens helbredsforhold, øvrige rent private forhold og andre fortrolige oplysninger til sundhedspersoner, myndigheder, organisationer, private personer m.fl. Samtykket skal være skriftligt. Kravet om skriftlighed kan dog fraviges, når sagens karakter eller omstændighederne i øvrigt taler derfor. Samtykket skal indføres i patientjournalen. Samtykket bortfalder senest 1 år efter, at det er givet.

Videregivelse af oplysninger til andre formål kan ifølge § 43, stk. 2, ske uden patientens samtykke ske, når

1. det følger af lov eller bestemmelser fastsat i henhold til lov, at oplysningen skal videregives og oplysningen må antages at have væsentlig betydning for den modtagende myndigheds sagsbehandling,
2. videregivelsen er nødvendig for berettiget varetagelse af en åbenbar almen interesse eller af væsentlige hensyn til patienten, sundhedspersonen eller andre, eller
3. videregivelsen er nødvendig for, at en myndighed kan gennemføre tilsyns- og kontrolopgaver.

Hvis der videregives oplysninger efter bestemmelsen i § 43, stk. 2, nr. 2, skal den, oplysningen angår, snarest muligt herefter orienteres om videregivelsen og formålet hermed, medmindre orientering kan udelades efter anden lovgivning eller af hensyn til offentlige eller private interesser svarende til dem, der beskyttes i denne lovgivning, jf. § 43, stk. 4.

2.3.1.2.4. Videregivelse af helbredsoplysninger til pårørende og læge vedrørende afdøde patienter

Det følger af sundhedslovens § 45, at en sundhedsperson efter anmodning kan og skal videregive oplysninger om en afdød patients sygdomsforløb, dødsårsag og dødsmåde til afdødes nærmeste pårørende, afdødes alment praktiserende læge og den læge, der havde afdøde i behandling, såfremt det ikke må antages at stride mod afdødes ønske og hensynet til afdøde, eller andre private interesser ikke taler afgørende herimod.

2.3.1.2.5. Videregivelse af helbredsoplysninger til særlige formål (forskning, statistik mv.)

Det følger af sundhedslovens § 46, stk. 1, at oplysninger om enkeltpersoners helbredsforhold, øvrige rent private forhold og andre fortrolige oplysninger fra patientjournaler mv. kan videregives til en forsker til brug for et konkret sundhedsvidenskabeligt forskningsprojekt, såfremt der er meddelt tilladelse til projektet efter lov om et videnskabsetisk komitésystem og behandling af biomedicinske forskningsprojekter (nu lov om videnskabsetisk behandling af sundhedsvidenskabelige forskningsprojekter).

Oplysningerne kan, når et forskningsprojekt ikke er omfattet af lov om videnskabsetisk behandling af sundhedsvidenskabelige forskningsprojekter, endvidere videregives til en forsker til brug ved et konkret forskningsprojekt af væsentlig samfundsmæssig interesse efter godkendelse af Sundhedsstyrelsen, som fastsætter vilkår for videregivelsen, jf. § 46, stk. 2.

Det følger i den forbindelse af § 46, stk. 3, at der kun må ske efterfølgende henvendelse til enkeltpersoner, i det omfang de sundhedspersoner, der har behandlet de pågældende, giver tilladelse hertil.

Oplysninger som nævnt i § 46 kan videregives til brug for statistik eller planlægning efter godkendelse af Sundhedsstyrelsen, som fastsætter vilkår for oplysningernes anvendelse mv., jf. § 47, stk. 1. Videregivelse af oplysninger kan dog ske uden godkendelse af Sundhedsstyrelsen, når det følger af lov, at oplysningerne skal videregives, jf. § 47, stk. 2.

Oplysninger, der er indhentet til brug for forskning, statistik eller planlægning, må ikke senere behandles i andet end statistisk eller videnskabeligt øjemed, jf. § 48, stk. 1. Offentliggørelse af oplysninger må kun ske i en form, hvori oplysningerne ikke kan henføres til enkeltpersoner, jf. § 48, stk. 2.

2.3.1.2.6. Særlige regler om adgang til nationale registre

Som nævnt ovenfor er der fastsat særlige regler for adgang til det Centrale Tilskudsregister (CTR), det Fælles Medicinkort (FMK) og det Danske Vaccinationsregister (DDV) i sundhedslovens §§ 156, 157 og 157 a.

Det Centrale Tilskudsregister indeholder oplysninger, der er nødvendige for beregning af lægemiddeltilskud, når patienterne køber medicin på apotek, jf. sundhedslovens § 156.

I bekendtgørelse om det Centrale Tilskudsregister (CTR)[27] er der fastsat regler om, at apotekere og apotekspersonale har adgang til oplysningerne i forbindelse med beregning af tilskud, kommunalt helbredstillæg og egenbetaling i forbindelse med udlevering af lægemidler, samt til information af patienten. Læger har adgang til oplysningerne, når lægen har patienten i aktuel behandling, og Sundhedsstyrelsen har adgang til oplysningerne i forbindelse med sikring af registerets drift og datakvalitet.

Det Fælles Medicinkort (FMK) er reguleret i sundhedslovens § 157 om Statens Serum Instituts elektroniske registrering af borgernes medicinoplysninger. Dataansvaret for FMK blev tidligere varetaget af Lægemiddelstyrelsen, men i forbindelse med ressortomlægningen i 2012 er ansvaret overgået til Statens Serum Institut, og ved ressortomlægning i 2015 er ansvaret overgået til Sundhedsdatastyrelsen. Det Danske Vaccinationsregister er reguleret i sundhedslovens § 157 a. Statens Serum Institut er dataansvarlig.

[27] Bekendtgørelse nr. 1449 af 4. december 2015.

I bekendtgørelsen om FMK og DDV (bekendtgørelse om adgang til og registrering mv. af lægemiddel- og vaccinationsoplysninger[28]) er der fastsat regler om, at sundhedspersonale har adgang til lægemiddel- og vaccinationsoplysninger i forbindelse med aktuel behandling af patienten, at Sundhedsstyrelsen har adgang til sådanne oplysninger i forbindelse med behandling af sager om bivirkningsindberetninger, at Sundhedsdatastyrelsen hhv Statens Serum Institut har adgang til oplysningerne som data-/systemansvarlig, og at borgeren har adgang til oplysninger, som er registreret om vedkommende selv.

2.3.1.3. Regler om tavshedspligt

Tavshedspligt og fortrolighed er to grundlæggende principper i dansk sundhedsret.

Tavshedspligten følger af sundhedslovens § 40, hvorefter en patient har krav på, at sundhedspersoner iagttager tavshed om, hvad de under udøvelsen af deres erhverv erfarer eller får formodning om angående helbredsforhold, øvrige rent private forhold og andre fortrolige oplysninger, jf. dog reglerne om videregivelse og indhentelse af oplysninger. Tavshedspligten gælder også for studerende, der som led i en sundhedsvidenskabelig eller sundhedsfaglig uddannelse deltager i behandlingen af en patient uden at være medhjælp.

Derudover finder de almindelige bestemmelser om tavshedspligt for den offentlige forvaltning anvendelse, herunder forvaltningslovens § 27 og straffelovens §§ 152-152 f.

2.3.2. Straffelovens regler om freds- og ærekrænkelser

Straffelovens kapitel 27 indeholder bestemmelser om freds- og ærekrænkelser.

Det er efter straffelovens § 263, stk. 2, strafbart uberettiget at skaffe sig adgang til en andens oplysninger, der er bestemt til at bruges i et informationssystem.

Det fremgår af § 264 c, at § 263 tilsvarende finder anvendelse på den, der uden at have medvirket til gerningen skaffer sig eller uberettiget udnytter oplysninger, som er fremkommet ved overtrædelsen.

Herudover er det efter § 264 d strafbart uberettiget at videregive meddelelser eller billeder vedrørende en andens private forhold eller i øvrigt billeder af den pågældende under omstændigheder, der åbenbart kan forlanges unddraget offentligheden.

[28] Bekendtgørelse nr. 460 af 8. maj 2014.

2.4. Tilsynet med overholdelse af reglerne

2.4.1. Datatilsynet

Persondatalovens kapitel 16 (§§ 55-66) omhandler Datatilsynet, og reglerne i dette kapitel beskriver tilsynets organisation samt tilsyns- og inspektionskompetence. I det følgende omtales de bestemmelser i kapitlet, der er relevante i den aktuelle sammenhæng.

2.4.1.1. Generelt om tilsynet med persondataloven

Ifølge persondatalovens § 55 fører Datatilsynet tilsyn med enhver behandling, der omfattes af loven, jf. herved reglerne i lovens kapitel 1 og 3.

Tilsynet med behandling af personoplysninger, der foretages for domstolene, føres dog af Domstolsstyrelsen og de overordnede retter, jf. lovens kapitel 17.

Endvidere kan det i lovgivningen være bestemt, at tilsynet inden for andre lovgivningsområder hører under andre myndigheder.

Som eksempel herpå kan nævnes, at Forbrugerombudsmanden i medfør af betalingstjenestelovens § 97 bl.a. fører tilsyn med visse behandlinger af oplysninger i forbindelse med brug af betalingsinstrumenter, jf. herom punkt 2.4.3 nedenfor.

2.4.1.2. Datatilsynets tilsynsbeføjelse

Datatilsynet påser af egen drift eller efter klage fra en registreret, at behandlingen af oplysninger finder sted i overensstemmelse med persondataloven og regler udstedt i medfør af loven, jf. lovens § 58, stk. 1.

Enhver registreret person eller virksomhed mv., som er beskyttet af persondataloven, kan i overensstemmelse med det almindelige forvaltningsretlige partsbegreb klage til Datatilsynet over en behandling, som vedkommende føler sig forurettet af. Som udgangspunkt vil Datatilsynets behandling af en klage dog være betinget af, at eventuelle klagemuligheder inden for det konkrete sagsområde er udtømt.

Herudover kan Datatilsynet tage sager op af egen drift, hvis tilsynet finder anledning hertil. Tredjemand har ikke en ret til at klage til Datatilsynet med den følge, at tilsynet *skal* behandle sagen, men tilsynet kan og vil i sådanne tilfælde tage sagen op af egen drift, hvis der vurderes at være anledning dertil.

2.4.1.3. Oplysningspligt over for Datatilsynet

Det følger af lovens § 62, stk. 1, at Datatilsynet kan kræve enhver oplysning, der er af betydning for tilsynets virksomhed, herunder til afgørelse af, om et forhold falder ind under lovens bestemmelser.

Undladelse af at efterkomme Datatilsynets krav om oplysninger er strafsanktioneret, jf. § 70, stk. 1, nr. 3.

Private dataansvarliges behandling af oplysninger i strid med loven er i meget vidt omfang strafsanktioneret, jf. § 70. Oplysningspligten over for Datatilsynet er derfor undergivet de begrænsninger, der følger af retssikkerhedslovens[29] § 1, stk. 3, jf. § 10, om retten til ikke at inkriminere sig selv.

2.4.1.4. Datatilsynets inspektionsadgang

Det følger af 62, stk. 2, at Datatilsynets medlemmer og personale til enhver tid – mod behørig legitimation – uden retskendelse har adgang til alle lokaler, hvorfra en behandling af oplysninger, som foretages for den offentlige forvaltning, administreres, eller hvorfra der er adgang til de oplysninger, som behandles, samt til lokaler, hvor oplysningerne eller tekniske hjælpemidler opbevares eller anvendes.

Bestemmelsen finder anvendelse i forhold til behandlinger af oplysninger, der foretages *for den offentlige forvaltning*, og gælder dermed også, hvis behandlingen foretages af en privat databehandler på en dataansvarlig myndigheds vegne. Tilsynets inspektionsadgang gælder også i de tilfælde, hvor en offentlig myndighed har etableret hjemmearbejdspladser, hvorfra der behandles oplysninger, der er omfattet af loven.

Det er en forudsætning, at Datatilsynet har mulighed for selv at gøre sig bekendt med behandlede oplysninger efter at have fået adgang til lokaler, hvorfra der er adgang til oplysningerne. Datatilsynets medarbejdere vil derfor i forbindelse med en inspektion selv kunne foretage opslag i et register og foretage udskrivning af oplysninger. I praksis gennemføres inspektioner dog i tæt samarbejde med medarbejdere fra den pågældende offentlige myndighed.

Datatilsynet har ret til at gennemføre sine inspektioner uanmeldt, men i praksis varsles langt de fleste inspektioner i forvejen for at sikre, at de relevante medarbejdere er til stede.

Inspektionerne er omfattet af begrebet "husundersøgelser" i retssikkerhedslovens § 1, stk. 1, nr. 1, og denne lovs kapitel 2 og 3 finder dermed anvendelse.

Det følger af § 62, stk. 3, at bestemmelsen i stk. 2 tilsvarende gælder for behandlinger, som foretages *for private dataansvarlige*. Datatilsynets inspektionskompetence over for

[29] Lov nr. 442 af 9. juni 2004 om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter med senere ændringer.

den private sektor er dog begrænset til de typer af behandlinger, der er undergivet et krav om forudgående tilladelse efter reglerne i § 50, eller som foretages for private dataansvarlige i forbindelse med tv-overvågning.

Endelig gælder bestemmelsen i stk. 2 for så vidt angår den behandling, der udføres af databehandlere som nævnt i § 53 (edb-servicebureauer), jf. § 62, stk. 4.

2.4.1.5. Datatilsynets samarbejde med udenlandske tilsynsmyndigheder

Det følger af § 64, stk.1, at Datatilsynet af egen drift eller efter anmodning fra en anden medlemsstat kan påse, at en behandling af oplysninger, som finder sted i Danmark, er lovlig, uanset at den pågældende behandling er undergivet en anden medlemsstats lovgivning.

Datatilsynet vil kunne kræve oplysninger af en eventuel databehandler, som er etableret i Danmark, eller af en repræsentant for en dataansvarlig, som befinder sig i Danmark, ligesom tilsynet efter omstændighederne vil kunne udføre inspektioner, jf. det under punkt 2.4.1.3 og punkt 2.4.1.4 anførte.

Herudover har Datatilsynet kompetence til at realitetsbehandle og afgøre sagen efter den pågældende medlemsstats materielle lovgivning. Dette må forventes at ske på grundlag af oplysninger fra tilsynsmyndigheden i den pågældende medlemsstat.

Endelig kan Datatilsynet meddele forbud eller påbud til en databehandler eller en repræsentant for den dataansvarlige, såfremt disse befinder sig i Danmark.

Uanset ordlyden af § 64, stk. 1, forudsættes det, at tilsynsmyndighederne i medlemsstaterne samarbejder i det omfang, det er nødvendigt for at opfylde deres pligter.

Datatilsynet kan videregive oplysninger til tilsynsmyndigheder i andre medlemsstater i det omfang, det er nødvendigt for at påse overholdelsen af bestemmelserne i persondataloven eller den pågældende medlemsstats databeskyttelseslovgivning, jf. § 64, stk. 2.

2.4.1.6. Datatilsynets beføjelser over for den dataansvarlige

2.4.1.6.1. Private dataansvarlige

Persondatalovens § 59, stk. 1-3, regulerer Datatilsynets beføjelser til at meddele forbud og påbud over for private dataansvarlige. Det følger således af stk. 3, at Datatilsynet kan påbyde en privat dataansvarlig at træffe bestemte tekniske og organisatoriske sikkerhedsforanstaltninger mod, at der behandles oplysninger, som ikke må behandles, 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.

Bestemmelsen i stk. 3 skal ses i sammenhæng med § 41, stk. 3, om, at der skal træffes fornødne tekniske og organisatoriske sikkerhedsforanstaltninger.

I medfør af § 59, stk. 4, kan Datatilsynet i særlige tilfælde meddele databehandlere påbud eller forbud, jf. stk. 1-3.

Bestemmelsen i stk. 4 medfører, at Datatilsynet vil kunne meddele en databehandler påbud eller forbud, jf. stk. 1-3. Dette kan være relevant, såfremt det ikke er muligt for tilsynet at meddele den dataansvarlige de nødvendige påbud eller forbud, f.eks. fordi det ikke er muligt at komme i kontakt med den dataansvarlige, eller hvis den dataansvarlige ikke ønsker at efterleve en afgørelse, som er truffet af tilsynet i henhold til stk. 1-3. Det er en forudsætning, at der ikke umiddelbart er udsigt til, at tilsynet kan meddele den dataansvarlige sin afgørelse efter stk. 1-3 eller til, at den dataansvarlige efterlever tilsynets afgørelse, såfremt denne allerede er truffet og meddelt den dataansvarlige. Det er endvidere en forudsætning, at den fortsatte behandling er til skade for den registrerede eller for andre, f.eks. fordi der foregår en ulovlig videregivelse eller anden udbredelse af personoplysninger.

2.4.1.6.2. Offentlige dataansvarlige

Datatilsynet har efter bestemmelsen i § 60, stk. 1, kun afgørelseskompetence med bindende virkning over for andre myndigheder i sager vedrørende § 7, stk. 7, § 9, stk. 3, § 10, stk. 3, § 13, stk. 1, § 27, stk. 4, §§ 28-31, § 32, stk. 1, 2 og 4, §§ 33-37, § 39 samt § 58, stk. 2. I andre situationer har tilsynet alene kompetence til at afgive uforbindende udtalelser, jf. stk. 2.

Tilsynet har således som udgangspunkt alene en udtalelsesret over for offentlige myndigheder.

I sager, hvor Datatilsynet alene har en udtalelseret, og hvor tilsynet ikke kan tiltræde udførelsen af en behandling af oplysninger, der foretages for en underordnet myndighed eller en regional eller kommunal myndighed, kan sagen for så vidt angår behandlinger der udføres for en underordnet myndighed, forelægges for vedkommende minister, og med hensyn til behandlinger der udføres for en kommunal myndighed, økonomi- og indenrigsministeren, jf. § 47.

2.4.1.7. Datatilsynets inspektionsvirksomhed

Datatilsynet har i 2013 udarbejdet en inspektionsstrategi, som fastlægger overordnede rammer, mål og principper for tilsynets inspektionsindsats i årene 2013-2015. Strategien suppleres af diverse vejledninger og hjælpeværktøjer. Strategien skal bl.a. sikre størst mulig effekt af tilsynets inspektioner.

Strategien har resulteret i ti konkrete initiativer. Ét af initiativerne er, at Datatilsynet har udvalgt seks kategorier af virksomheder, myndigheder og databehandlinger, hvor der er særligt behov for regelmæssigt tilsyn. Inspektionerne vil som følge deraf primært ske inden for følgende kategorier: lokale politiembeder og Rigspolitiet, kommuner, sygehuse og sundhedsdatabaser, kreditoplysningsbureauer og advarselsregistre, privat og offentlig forskning samt tv-overvågning.

Valget af disse fokuspunkter udelukker ikke, at der foretages inspektioner i andre kategorier.

Blandt strategiens øvrige initiativer indgår bl.a. følgende:

- Datatilsynet vil påtale alle væsentlige brud på persondataloven, udtale kritik eller beklagelse samt stille krav om, at forholdene bringes i orden.
- Datatilsynet vil følge op på, at de påtalte forhold bringes i orden.
- Datatilsynet vil udnytte den viden, som tilsynet indsamler via inspektionerne.
- Datatilsynet vil tilstræbe høj grad af transparens omkring tilsynets praksis og tilsynsaktiviteter.

Datatilsynet har i perioden fra tilsynets oprettelse i 2000 gennemført følgende antal tilsynsbesøg:

År:	Antal inspektioner:
2000:	23
2001:	76
2002:	116
2003:	71
2004:	68
2005:	61
2006:	63
2007:	66
2008:	94
2009:	83
2010:	64

2011: 54
2012: 43 (hertil kommer 2 skriftlige inspektioner og 21 online-undersøgelser)
2013: 46 (hertil kommer 1 skriftlig inspektion og 15 online-undersøgelser)
2014: 48 (hertil kommer 20 online-undersøgelser)
2015: 32 (hertil kommer 10 skriftlige inspektioner og 27 online-undersøgelser)

Datatilsynet har primo 2016 oprettet en ny tilsynsenhed. Den nye tilsynsenhed får ansvaret for alle Datatilsynets planlagte tilsyn samt Datatilsynets ad hoc tilsyn vedrørende brud på persondatalovens sikkerhedskrav.

Ved udvælgelse af emner for planlagte tilsyn skal der ifølge Datatilsynets tilsynsstrategi for 2016-2018 navnlig fokuseres på behandlinger af personoplysninger, som på grund af deres omfang eller formål kan indebære en særlig risiko for at krænke de registreredes ret til databeskyttelse og privatliv, samt på behandlinger, som indebærer brug af ny teknologi.

Ved udvælgelsen af såvel emner som de dataansvarlige, der skal indgå i de planlagte tilsyn, tager Datatilsynet bl.a. i betragtning, om der på et område er fremkommet oplysninger – herunder ved henvendelser fra borgere eller via medieomtale – der kunne tyde på et særligt behov for tilsyn. Datatilsynets tilsynsenhed fokuserer i 2016 på udvalgte emner hos en række dataansvarlige.

Kontrol af følgende emner vil gå igen på 30 tilsyn overfor offentlige myndigheder:
• Uddybende sikkerhedsregler,
• myndighedens eget tilsyn,
• databehandleraftaler, og
• myndighedens egen kontrol med databehandlere.

Hos 20 private dataansvarlige vil følgende emner gå igen:
• Iagttagelse af Datatilsynets vilkår,
• databehandleraftaler, og
• virksomhedens egen kontrol med databehandlere.

På alle tilsyn vil der blive anvendt oplysningsindsamling ved hjælp af spørgeskema.

Overfor mindst 5 dataansvarlige vil Datatilsynet endvidere følge op med egentlige tilsynsbesøg.

2.4.1.8. Anmeldelsesordningerne

Som det fremgår under punkt 2.1.2.2 (vedrørende rækkevidden af sikkerhedsbekendtgørelsens kapitel 3), punkt 2.1.2.4 (vedrørende muligheden for at fastsætte vilkår om datasikkerhed) og punkt 2.4.1.4 (vedrørende Datatilsynets inspektionskompetence over for private dataansvarlige) er visse datasikkerhedsmæssige tiltag afhængige af, om behandlingen af oplysninger er omfattet af anmeldelsesordningerne[30].

Udgangspunktet for anmeldelsesordningerne er, at alle behandlinger skal anmeldes forudgående til Datatilsynet. Desuden skal visse behandlinger tillige kontrolleres inden iværksættelsen. Kravet om kontrol kommer med hensyn til de offentlige dataansvarlige til udtryk i et krav om *forudgående udtalelse*, mens der for private dataansvarlige er etableret en *tilladelsesordning*. Mange typer af behandlinger, hvor det i betragtning af de behandlede oplysninger ikke er sandsynligt, at registreredes rettigheder krænkes, er fritaget fra anmeldelse.

Reglerne om anmeldelse af behandlinger og de tilhørende regler om offentlig tilgængelighed af behandlinger af oplysninger tjener en række formål, først og fremmest *gennemsigtighed* og *kontrol*: Det sikres, at en behandlings formål samt dens vigtigste karakteristika gøres offentligt kendt med henblik på kontrol af behandlingens overensstemmelse med loven. Herved tilvejebringes gennemskuelighed for borgerne, hvilket styrker borgernes muligheder for at gøres deres rettigheder ifølge loven gældende. Hertil kommer hensynet til at sikre, at vedkommende tilsynsmyndighed får det fornødne indseende med, hvilke typer behandlinger der foretages for offentlige eller private dataansvarlige, såvel konkret som i almindelighed. Herved styrkes tilsynsmyndighedens muligheder for at føre et effektivt tilsyn.

Bestemmelserne om anmeldelse har deres baggrund i databeskyttelsesdirektivets artikel 18-20, og reglerne om behandlingernes offentlige tilgængelighed har baggrund i direktivets artikel 21.

Databeskyttelsesdirektivets artikel 18 giver endvidere mulighed for at forenkle anmeldelsesordningen eller helt at fritage for anmeldelse, hvis medlemsstaten etablerer en ordning, hvorefter den dataansvarlige udpeger en databeskyttelsesansvarlig, som bl.a. har til opgave i fuld uafhængighed at sikre den interne anvendelse af de nationale bestemmelser, der er truffet i medfør af databeskyttelsesdirektivet, for på den måde at sikre, at det ikke er sandsynligt, at de registreredes rettigheder og frihedsrettigheder vil kunne krænkes som følge af behandlingen.

[30] Anmeldelsesordningerne og de tilhørende regler om offentlig tilgængelighed af behandlinger af oplysninger er reguleret af persondatalovens kapitel 12-15.

Denne del af direktivet er ikke implementeret i Danmark. Dette er imidlertid tilfældet i Sverige, Tyskland og Norge (direktivet gælder også for EØS-landene, jf. EØS-komiteens beslutning nr. 83/1999 af 25. juni 1999), som alle synes at have gode erfaringer med, at de dataansvarlige udpeger interne databeskyttelsesansvarlige.

Muligheden for at udpege databeskyttelsesansvarlige indgår også i den nye databeskyttelsesforordning.

2.4.2. Finanstilsynet

2.4.2.1. Generelt om Finanstilsynets tilsyn med it-sikkerhed og databehandling

Et hovedformål med den finansielle lovgivning er at sikre den finansielle stabilitet og tillid til de finansielle virksomheder og markeder. Med afsæt heri indeholder lovgivningen en række krav til finansielle virksomheder, der skal sikre, at virksomhederne drives på en forsvarlig måde, så kunderne kan have tiltro til, at deres midler bliver behandlet forsvarligt, og virksomhederne ikke lider tab som følge af misbrug og kriminalitet. Den finansielle lovgivnings krav til it-sikkerhed skal ligeledes ses på denne baggrund. Finanstilsynet fører et tilsvarende tilsyn med it-sikkerheden i betalingsinstitutter efter lov om betalingstjenester.

Kravene til it-sikkerhed tilgodeser således flere forskellige hensyn, der med udgangspunkt i den konkrete virksomhed bl.a. har afsæt i:

- Fortrolighed: Sikrer at data opbevares betryggende, ikke kan tilgås af uvedkommende, er sikret mod interne og eksterne trusler mv.
- Integritet: Sikrer ægtheden af data, at data ikke kan manipuleres eller ændres mv.
- Tilgængelighed: Sikrer at tjenester og systemer er tilgængelige, driftsstabile mv.

It-sikkerhed skal ses i virksomhedens konkrete kontekst, herunder virksomhedens størrelse, kompleksitet og forretningsmodel. It-sikkerhed tjener således flere formål fra beskyttelse af systemer og data til sikker og stabil drift mv.

Finanstilsynets it-tilsyn angår bl.a. en vurdering af, om virksomheden, ud fra Finanstilsynets risikobetragtning, virksomhedens egne målsætninger og risikovurderinger mv., har forholdt sig til alle relevante it-sikkerhedsforhold og ud fra dette har etableret betryggende kontrol- og sikringsforanstaltninger på it-området.

Finanstilsynet fører bl.a. tilsyn med overholdelse af de krav om betryggende kontrol- og sikringsforanstaltninger på it-området, der følger af lov om finansiel virksomhed § 71,

stk. 1, nr. 8, og som er uddybende beskrevet i bilag 5 til den bekendtgørelse, der er udstedt i medfør af § 71, stk. 2, jf. herom punkt 2.2.2.1 ovenfor.

Som led heri førte Finanstilsynet frem til 2012 også et indirekte tilsyn med fællesejede datacentraler, som håndterer en betydelig del af de finansielle virksomheders it-anvendelse. I 2012 blev tilsynets beføjelser udvidet til også at omfatte mere direkte tilsynsopgaver i forhold til fællesejede datacentraler. Finanstilsynet fik herunder mulighed for at foretage inspektioner og give påbud til datacentralerne.

Tilsynet er baseret på, at lovændringen alene medfører, at fælles datacentraler bliver omfattet af samme regler om betryggende kontrol- og sikringsforanstaltninger på it-området som finansielle virksomheder såsom banker, forsikringsselskaber, pensionskasser og realkreditinstitutter mv., jf. herved følgende formulering fra det bagvedliggende lovforslag[31]:

> "*Med lovforslaget vil Finanstilsynet få mulighed for at kræve ændringer i it-sikkerheden i de fælles datacentraler, ligesom Finanstilsynet vil få mulighed for at gribe ind, hvis outsourcingen fra de fælles datacentraler ikke lever op til kravene i outsourcingbekendtgørelsen. For at ligestille datacentralerne med de finansielle virksomheder, foreslås tillige, at Finanstilsynet imod behørig legitimation og uden retskendelse kan få adgang til en datacentral.*"

Finanstilsynet fik i forbindelse med lovændringen tilført yderligere ét årsværk til it-tilsynet. Finanstilsynet har herefter i alt 3 årsværk, som varetager tilsynet med, at finansielle virksomheder og datacentraler mv. overholder lovens krav om betryggende kontrol- og sikringsforanstaltninger på it-området.

I det omfang datacentralerne lader opgaver udføre hos underleverandører, finder lov om finansiel virksomheds regler om outsourcing tilsvarende anvendelse for datacentraler, og Finanstilsynets tilsyn omfatter outsourcingen.

Finanstilsynet fører som udgangspunkt tilsyn med den generelle it-anvendelse hos finansielle virksomheder og fælles datacentraler mv. Herved forstås styringen af den grundlæggende it-sikkerhed i forlængelse af ledelsens strategier, risikovurderinger og heraf afledte politikker og kontroller mv., men typisk ikke en gennemgang af funktionerne i specifikke it-systemer.

Finanstilsynets metode tager afsæt i en risikobaseret tilgang. Opgaven tilskæres i planlægningsfasen med afsæt i den konkrete risikovurdering og systemisk vigtighed. Der vil herunder eksempelvis blive foretaget en gennemgang af it-sikkerhedsstyring, adgang til

[31] Lovforslag nr. L 59 af 14. december 2011.

systemer og data, it-drift og -udvikling, logisk sikkerhed (som eksempelvis password, logning og kryptering af data), it-organisationen mv.

2.4.2.2. Oplysningspligt over for Finanstilsynet

Finanstilsynet kan efter lov om finansiel virksomhed § 347 og lov om betalingstjenester § 86 kræve alle oplysninger, som tilsynet skønner nødvendige for tilsynsvirksomheden.

Undlader en finansiel virksomheds bestyrelse, direktion m.v. at efterkomme de pligter, som påhviler dem i medfør af loven, kan Finanstilsynet som tvangsmiddel pålægge dem daglige eller ugentlige bøder.

Undlader et betalingsinstitut at efterkomme Finanstilsynets krav om oplysninger, kan virksomheden straffes med bøde i medfør af lovens § 107, stk. 3. I det omfang der indhentes oplysninger, der kan føre til strafferetlig forfølgning, er oplysningspligten over for Finanstilsynet dog undergivet de begrænsninger, der følger af retssikkerhedslovens[32] § 1, stk. 3, jf. § 10, om retten til ikke at inkriminere sig selv.

2.4.2.3 Finanstilsynets inspektionsadgang

Finanstilsynet har – i lighed med Datatilsynet – til enhver tid og mod behørig legitimation uden retskendelse adgang til virksomheder under tilsyn og til virksomheder, hvortil der er outsourcet opgaver, med henblik på indhentelse af oplysninger, herunder ved inspektioner. Dette følger af henholdsvis lov om finansiel virksomhed § 347, stk. 2, og lov om betalingstjenester § 87, stk. 4.

Desuden har tilsynet i henhold til § 346, stk. 1, en eksplicit forpligtelse til at undersøge finansielle virksomheders og fællesejede datacentralers forhold.

Der føres i udgangspunktet ikke målrettet tilsyn med anvendelse af specifikke systemer, som der kan være hundredvis af i større virksomheder.

Finanstilsynet modtager løbende indberetninger fra de finansielle virksomheder og datacentraler mv., som behandles og vurderes løbende. Herudover foretages der også inspektioner på stedet hos disse.

Turnusfrekvens for inspektioner bliver generelt fastsat på baggrund af en vurdering af den pågældende virksomheds størrelse og betydning for den finansielle sektor og den finansielle stabilitet. Som udgangspunkt vil eksempelvis fælles datacentraler have en 4-

[32] Lov nr. 442 af 9. juni 2004 om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter med senere ændringer.

årig inspektionsfrekvens på it-inspektioner. Der omprioriteres løbende ved indikation på behov herfor.

Fælles datacentraler er underlagt krav om ekstern systemrevision, som blandt andet skal påse, at betryggende kontrol- og sikringsforanstaltninger tilgodeses i tilstrækkeligt omfang ved udvikling, vedligeholdelse og drift af datacentralens systemer, og at forretningsgange er tilrettelagt og fungerer betryggende. Der skal føres et særskilt systemrevisionsprotokollat til datacentralens bestyrelse herom. Har datacentralen tillige en intern systemrevision, kan den eksterne systemrevision aftale, at visse erklæringer alene fremgår af den interne systemrevisions protokollat. Finanstilsynet modtager disse protokollater på samme vis som andre revisionsprotokollater, der således indgår i Finanstilsynets grundlag for planlægning af tilsynsindsatsen.

Det bemærkes, at systemrevisionen skal påse, at Finanstilsynet straks modtager meddelelse, bl.a. hvis den må formode, at datacentralens samlede system-, data- og driftssikkerhed på centrale områder ikke er betryggende.

For nogle virksomhedstyper gennemføres der også årlige møder med virksomhedernes ledelser med en bred dagsorden. Hvis løbende indberetninger eller andre oplysninger indikerer et ændret risikobillede af den enkelte virksomhed, vil ændret turnusfrekvens for den pågældende virksomhed blive overvejet.

Finanstilsynets it-inspektører har fra 2008 til medio 2016 foretaget i alt 38 it-inspektioner hos større kreditinstitutter, forsikringsselskaber, fælles datacentraler mv.

Herudover er der foretaget mindre omfattende gennemgang af it-området på andre inspektioner i særligt mindre betydende virksomheder ved øvrige undersøgere, i nogle tilfælde dog med bistand fra it-inspektørerne.

Som en del af it-tilsynet følger Finanstilsynet også straks op på væsentlige it-hændelser.

Opfølgningen består hovedsageligt i en indledende orientering til Finanstilsynet om det passerede, og de tiltag der iværksættes i anledning heraf. Hurtigst muligt efter modtager Finanstilsynet en nærmere redegørelse om samme. Finanstilsynet vurderer på den baggrund, om de igangsatte tiltag skønnes relevante og tilstrækkelige, eller om der skal kræves yderligere opfølgning, herunder en eventuel målrettet inspektion fra tilsynets side.

Finanstilsynet har ved årsskiftet 2013/14 fremsendt en vejledning om indberetning i forbindelse med opfølgning til de største finansielle virksomheder og datacentraler mv.

2.4.2.4. Finanstilsynets beføjelser

Hvis en finansiel virksomhed, en fællesejet datacentral eller et betalingsinstitut ikke har levet eller ikke lever op til kravene om at have en betryggende it-sikkerhed, vil Finanstilsynet enten som led i en inspektion eller i forbindelse med behandling af konkrete sager have en række reaktionsmuligheder til rådighed:

1) Påtaler: Finanstilsynet anvender en påtale, hvis der konstateres en lovovertrædelse, der ikke længere består. Situationen foreligger både, hvor lovovertrædelsen vedrører en situation af midlertidig karakter, der nu er afsluttet, samt hvor virksomheden af egen drift har bragt forholdet i orden.

2) Påbud: Et påbud anvendes i de situationer, hvor Finanstilsynet påbyder en bestemt adfærd eller handling fremover. Det kan både være, fordi en virksomhed handler på en lovstridig måde, eller fordi virksomheden undlader at handle, hvor handling er påkrævet.

3) Risikooplysninger: Hvis Finanstilsynet vurderer, at der er behov for at henlede en virksomheds opmærksomhed på, at virksomheden har en væsentlig forøget risiko på et område, f.eks. i forhold til it-sikkerhed eller uholdbare elementer i forretningsmodellen, uden der foreligger en lovovertrædelse, kan der anvendes risikooplysninger. Selvom der ikke eksisterer en eksplicit hjemmel til at give en risikooplysning, anses det at ligge i selve Finanstilsynets virksomhed, at tilsynet har mulighed for at påpege forhold, hvor en finansiel virksomhed udsætter sig selv for en forhøjet risiko. Finanstilsynet vil som hovedregel følge op på, hvordan virksomheden har forholdt sig til risikooplysningen.

Hjemlen til at give påtaler og påbud følger af tilsynets generelle adgang og pligt til at påse overholdelsen af lovgivningen efter § 344 i lov om finansiel virksomhed. Et påbud vil indeholde en rimelig frist til opfyldelse, normalt inden for et par måneder efter, at påbuddet er meddelt virksomheden skriftligt. Senest ved udløbet af denne frist skal virksomheden sende en erklæring til Finanstilsynet om, at forholdet nu er bragt i orden. Herefter kan kontrollen enten udføres af Finanstilsynet selv eller af en revisor, eventuelt i den førstkommende revisionsprotokol.

Da der er tale om et risikobaseret tilsyn, skal karakteren af opfølgningen af det enkelte påbud afspejle dette. Mindre alvorlige påbud kan opfølges ved virksomhedens revision. Mere alvorlige forhold vil Finanstilsynet sædvanligvis følge op på inden for en kortere tidshorisont. Der henvises i øvrigt til punkt 2.5.2 nedenfor.

2.4.2.5. Tilsyn med reglerne om videregivelse af fortrolige kundeoplysninger

Finanstilsynet fører ikke et systematisk tilsyn med overholdelsen af reglerne om videregivelse af fortrolige kundeoplysninger, eksempelvis i form af målrettede inspektioner, men behandler sager på baggrund af henvendelser fra kunder eller fra finansielle virksomheder, typisk i form af forespørgsler om, hvorvidt en videregivelse i en konkret situation vil være berettiget.

Finanstilsynet har i behandlingen af sager vedrørende uberettiget videregivelse de samme tilsynsbeføjelser, som gælder for Finanstilsynets tilsyn med it-sikkerhed, jf. herom punkt 2.4.2.2-2.4.2.4 ovenfor.

Finanstilsynet har således i forbindelse med behandling af sager om uberettiget videregivelse af fortrolige oplysninger mulighed for at kræve alle nødvendige oplysninger til belysning af sagen, ligesom tilsynet kan give en virksomhed en påtale og/eller påbyde den at træffe foranstaltninger, der er nødvendige for at sikre den fremtidige overholdelse af tavshedspligten. Endvidere er bestemmelsen i § 117 strafbelagt, hvorfor tilsynet tillige har mulighed for at politianmelde eventuelle overtrædelser. Dette gælder både i forhold til virksomheden og de personer som konkret måtte have overtrådt tavshedspligten.

§ 355 i lov om finansiel virksomhed angiver specifikt, hvem der er parter i forhold til Finanstilsynet. Sædvanligvis er kunder i finansielle virksomheder ikke omfattet af partsbegrebet. Finanstilsynet har dog – når tilsynet tager en sag op om videregivelse af fortrolige oplysninger – mulighed for efter § 355, stk. 6, at tildele visse partsbeføjelser til andre fysiske og juridiske personer, herunder til kunder i finansielle virksomheder, for så vidt angår den del af sagen, som har en direkte og væsentlig betydning for den pågældende.

2.4.3. Forbrugerombudsmanden

Det er som udgangspunkt Finanstilsynet, der fører tilsyn med overholdelsen af betalingstjenestelovens regler, jf. lovens § 86, stk. 1.

Af betalingstjenestelovens § 97, stk. 1, følger imidlertid, at Forbrugerombudsmanden er tilsynsmyndighed for så vidt angår udbydere af betalingstjenester, som gennemføres med betalingsinstrumenter, f.eks. et betalingskort, jf. § 6, nr. 9, udbydere af betalingstjenester som er omfattet af lovens bilag 1, nr. 7, samt betalingsmodtagere og andre.

Det er også omtalt i forarbejderne[33] til betalingstjenestelovens § 86, at der således er to myndigheder, der fører tilsyn med de samme bestemmelsers anvendelse på forskellige typer af betalingstjenester, og at dette forudsætter en koordinering af tilsynet. Denne

[33] Lovforslag nr. L 119 af 28. januar 2009, jf. Folketingstidende 2008-09, Tillæg A, s. 3576.

konstruktion blev indført med betalingstjenesteloven i 2009. Efter den tidligere betalingsmiddellov lå tilsynet hos Forbrugerombudsmanden alene.

Det er Forbrugerombudsmanden, der skal føre tilsyn med de af lovens regler, der vedrører en udbyders adfærd i forbindelse med udbud af betalingstjenester, der gennemføres ved hjælp af betalingsinstrumenter, for eksempel betalingskort og netbanker.

Ved en lovændring i 2014[34] blev betalingstjenestelovens § 97 præciseret således, at Forbrugerombudsmanden også kan håndhæve de i § 97 nævnte bestemmelser i forhold til "betalingsmodtagere og andre" og ikke kun udbyderne. Ændringen bringer Forbrugerombudsmandens tilsynskompetence i overensstemmelse med, hvad der var gældende efter den tidligere betalingsmiddellov, og hvad der også var tiltænkt med betalingstjenesteloven.

Forbrugerombudsmanden kan i forbindelse med sit tilsyn kræve alle oplysninger, som findes nødvendige for Forbrugerombudsmandens virksomhed, herunder til afgørelse af, om et forhold falder ind under lovens bestemmelser, jf. betalingstjenestelovens § 97, stk. 2. Undladelse af at meddele afkrævede oplysninger kan straffes med bøde, jf. betalingstjenestelovens § 107, stk. 4.

Såfremt en ændring af forhold, der strider mod de i betalingstjenestelovens § 97, stk. 1, opregnede bestemmelser, herunder § 85, ikke kan ske ved forhandling, kan Forbrugerombudsmanden udstede påbud herom. Påbuddet kan forlanges indbragt for domstolene af den, som påbuddet retter sig imod. Anmodning skal fremsættes skriftligt over for Forbrugerombudsmanden senest fire uger efter, at påbuddet er meddelt, hvorefter Forbrugerombudsmanden skal indbringe sagen for domstolene inden en uge, jf. betalingstjenestelovens § 97, stk. 3. Denne bestemmelse svarer til markedsføringslovens § 27, stk. 3. Overtrædelse af et påbud udstedt i medfør af betalingstjenestelovens § 97, stk. 3, er strafbelagt, jf. lovens § 107, stk. 4.

Retten kan bestemme, at indbringelse af et påbud for domstolene har opsættende virkning, jf. betalingstjenestelovens § 97, stk. 4.

Forbrugerombudsmandens afgørelser efter betalingstjenesteloven kan ikke indbringes for anden administrativ myndighed, jf. lovens § 97, stk. 5.

Ved overtrædelse af de i betalingstjenestelovens § 97, stk. 1, opregnede bestemmelser, herunder § 85, kan Forbrugerombudsmanden anlægge sag om forbud, påbud, erstatning og tilbagesøgning af uretmæssigt opkrævede beløb, jf. lovens § 97, stk. 6. Forbrugerom-

[34] Lov nr. 403 af 28. april 2014 om ændring af lov om finansiel virksomhed m.fl.

budsmanden kan tillige udpeges som gruppererepræsentant efter reglerne i retsplejelovens kapitel 23 a. Bestemmelsen er en pendant til § 348 i lov om finansiel virksomhed.

Ifølge betalingstjenestelovens § 97, stk. 7, varetager Datatilsynet efter bestemmelserne i persondatalovens § 64 samarbejdet med udenlandske myndigheder i samråd med Forbrugerombudsmanden.

Da markedsføringsloven supplerer anden lovgivning, kan Forbrugerombudsmanden som led i sit tilsyn anvende markedsføringsloven, medmindre andet følger af lovgivningen. Forbrugerombudsmandens tilsyn udføres i øvrigt efter reglerne i markedsføringsloven, herunder bekendtgørelse om Forbrugerombudsmandens virksomhed[35]. Af bekendtgørelsen fremgår det blandt andet, at Forbrugerombudsmanden ikke er forpligtet til at behandle klager, men har adgang til at prioritere hvilke klager, han eller hun vil behandle.

I 2006 blev der i markedsføringslovens § 22 a indført en hjemmel til, at Forbrugerombudsmanden kan foretage kontrolundersøgelser hos private eller offentlige virksomheder. Bestemmelsen gælder dog kun for behandlingen af klager, som Forbrugerombudsmanden modtager fra håndhævelsesmyndigheder i andre EU-lande efter forordning 2006/2004 om forbrugerbeskyttelsessamarbejde, det såkaldte CPC-samarbejde.

Forbrugerombudsmanden har ikke herudover hjemmel til at foretage inspektioner hos erhvervsdrivende.

2.4.3.1. Praksis vedrørende Forbrugerombudsmandens tilsyn

Forbrugerombudsmanden har taget stilling til netbankers brug af kundeoplysninger til dannelse af generelle oversigter over udgifter og indtægter i forhold til betalingstjenestelovens § 85. Forbrugerombudsmandens vurderede, at der ved dannelsen af oversigter i netbanken sker en behandling af data om, hvor brugerne har anvendt deres betalingsinstrumenter, som ligger ud over, hvad der er nødvendigt til gennemførelse eller korrektion af betalingstransaktionerne. Forbrugerombudsmanden udtalte derfor, at den omhandlede behandling af data ikke er i overensstemmelse med betalingstjenestelovens § 85, stk. 3. Forbrugerombudsmanden lagde vægt på, at det ikke i sig selv er afgørende, at kun betaleren har adgang til de pågældende oversigter, og at oversigterne ikke kan læses eller bruges af bankens medarbejdere og derfor heller ikke benyttes i markedsføringen, da der er tale om en offentligretlig regel, som ikke kan fraviges ved et samtykke fra forbrugeren. Bankerne tilkendegav i lyset af denne udtalelse, at bankerne ville søge erhvervs- og vækstministeren om en dispensation, jf. betalingstjenestelovens § 1, stk. 3.

[35] Bekendtgørelse nr. 1249 af 25. november 2014 om regler for Forbrugerombudsmandens virksomhed.

Finanstilsynet meddelte efter bemyndigelse fra erhvervs- og vækstministeren d. 25. april 2014 dispensation til denne form for databehandling under følgende betingelser:

- Betaler kan frabede sig behandlingen.
- Behandlingen kun sker, når en betaler, der ønsker et betalingsoverblik, logger på sin netbank eller mobile platform, og den datasammenstilling, der er fortaget, ophører, når betaler logger af, så der ikke gemmes oplysninger om kundens anvendelse af betalingsinstrumentet, efter at betaler har logget af.
- Ansatte i instituttet, bortset fra enkelte driftsmedarbejdere, har ikke adgang til oplysninger om, hvor en betaler har anvendt sit betalingsinstrument, og må ikke opfordre betaler til at overlade oplysningerne til sig, herunder særlig ikke i forbindelse med rådgivning eller kreditgivning.
- It-sikkerheden i forbindelse med behandlingen skal leve op til samme standarder for it-sikkerhed som pengeinstituttets øvrige it-systemer.

Derudover kan nævnes en sag, hvor Forbrugerombudsmanden i forbindelse med en erhvervsdrivendes anmodning om forhåndsbesked har vurderet lovligheden af et loyalitets-/rabatkoncept i relation til betalingstjenestelovens § 85. Forbrugerombudsmanden tilkendegav, at loyalitets-/rabatkonceptet måtte anses at være lovligt efter betalingstjenestelovens § 85, da oplysninger om, hvor betalerne havde anvendt deres betalingsinstrumenter, og hvad de havde købt, alene anvendes i et rabatkoncept, hvor rabatten ydes efter en generel, forud fastlagt rabatstruktur, og ikke er baseret på en segmentering ud fra kundes konkrete købsdata. Forbrugerombudsmanden lagde endvidere til grund, at eventuelle markedsføringstiltag, herunder ad hoc tilbud, alene er baseret på en segmentering på baggrund af data oplyst af kunden i forbindelse med selve tilmeldingen til konceptet, ikke ud fra kundes konkrete købsdata. Forbrugerombudsmanden lagde ved sin vurdering vægt på, at det følger af forarbejderne, at en rabatordning er nævnt som en funktion, som lovligt kan knyttes til et betalingsinstrument, når brugeren anvender betalingsfunktionen.

Forbrugerombudsmanden har ikke på nuværende tidspunkt af egen drift taget sager op med henblik på undersøgelse af overholdelse af lovens § 85.

2.4.4. Tilsyn med reglerne om tavshedspligt mv. i sundhedsvæsenet

Det følger af lov om klage- og erstatningsadgang inden for sundhedsvæsenet[36], at Styrelsen for Patientsikkerhed behandler klager over sundhedsvæsenets sundhedsfaglige virksomhed (klager over behandlingssteder/forløbsklager) og forhold omfattet bl.a. af sundhedslovens kapitel 9 om tavshedspligt, indhentelse og videregivelse af oplysninger. Styrelsen for Patientsikkerhed træffer afgørelse om, hvorvidt den sundhedsfaglige virk-

[36] Lovbekendtgørelse nr. 1113 af 7. november 2011 med senere ændringer.

somhed har været kritisabel, eller om sundhedsvæsenet har handlet i strid med lovgivningens regler.

Sundhedsvæsenets Disciplinærnævn behandler tilsvarende klager over sundhedsfaglig virksomhed (klager over konkrete sundhedspersoner). Sundhedsvæsenets Disciplinærnævn afgiver udtalelse om, hvorvidt sundhedspersonens sundhedsfaglige virksomhed har været kritisabel, eller om sundhedspersonen har handlet i strid med bl.a. sundhedslovens kapitel 9. Nævnet kan udtale kritik med indskærpelse eller søge iværksat sanktioner. Sidstnævnte reaktionsmulighed vedrører bl.a. tilfælde, hvor sagen efter nævnets opfattelse giver grundlag for berettiget mistanke om, at sundhedspersonen kan have gjort sig skyldig i grovere eller gentagen skødesløshed, og hvor Disciplinærnævnet på den baggrund kan anmode anklagemyndigheden om at overveje at rejse tiltale.

Herudover behandler Sundhedsdatastyrelsen klager over uberettiget adgang til data, hvor instituttet er dataansvarlig, bl.a. i forhold til det Fælles Medicinkort, jf. sundhedslovens § 157. Instituttet foretager også af egen drift stikprøvevis opfølgning på logs for at afdække eventuelt misbrug. I tilfælde, hvor Statens Serum Institut vurderer, at en adgang har været uberettiget, foretager instituttet politianmeldelse.

2.5. Straffebestemmelser mv.

2.5.1. Straffebestemmelser mv. i persondataloven

Persondatalovens sanktionsmuligheder – erstatning, straf og rettighedsfrakendelse – beskrives i lovens kapitel 18 (§§ 69-71).

2.5.1.1. Erstatning

Det følger af persondatalovens § 69, at den dataansvarlige skal erstatte skade, der er forvoldt ved behandling i strid med bestemmelserne i persondataloven, medmindre det godtgøres, at skaden ikke kunne have været afværget ved den agtpågivenhed og omhu, der må kræves i forbindelse med behandling af oplysninger.

Bestemmelsen fastlægger et præsumptionsansvar for den dataansvarlige, men indebærer i øvrigt ikke ændringer i dansk rets almindelige erstatningsretlige regler, herunder reglerne om kausalitet, adækvans mv., som fortsat finder anvendelse i bedømmelsen af, om den dataansvarlige i forbindelse med behandling af oplysninger har pådraget sig et erstatningsansvar over for den registrerede.

Godtgørelse for tort i anledning af en krænkelse af lovens regler om beskyttelse af den registreredes personlige integritet, der ikke medfører formuetab, kan alene kræves i det omfang, lovgivningen i øvrigt giver adgang hertil – det vil i praksis sige i medfør af erstatningsansvarslovens § 26.

Erstatningskrav efter § 69 skal indbringes for domstolene og vil ikke kunne forelægges Datatilsynet.

2.5.1.2. Straf

Med mindre højere straf er forskyldt efter den øvrige lovgivning, er persondatalovens strafferamme, jf. § 70, bøde eller fængsel i indtil fire måneder.

Det følger af § 70, stk. 1, at medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 4 måneder den, der i forbindelse med en behandling, som udføres for private:

1) Overtræder bl.a. § 5, stk. 2-5, § 41, stk. 1 og 3, § 42, § 50, stk. 1 og 2, og § 53,
2) Undlader at efterkomme Datatilsynets afgørelse efter bl.a. § 5, stk. 1, og § 50, stk. 2,
3) Undlader at efterkomme Datatilsynets krav efter § 62, stk. 1,
4) Hindrer Datatilsynet i at få adgang efter § 62, stk. 3 og 4,
5) Tilsidesætter vilkår som nævnt i bl.a. § 9, stk. 3, og § 50, stk. 5, eller
6) Undlader at efterkomme et forbud eller påbud, der er meddelt i henhold til § 59 eller i henhold til regler udstedt i medfør af loven.

I straffedomme over private vil der endvidere kunne pålægges fortløbende tvangsbøder med henblik på at gennemtvinge en forpligtelse, der påhviler dataansvarlige eller databehandlere. Forpligtelsen følger direkte af lovgivningen (persondataloven eller bekendtgørelser udstedt i henhold hertil) eller af et forbud eller påbud meddelt af Datatilsynet i henhold til persondatalovgivningen. Hjemlen til at pålægge tvangsbøder følger af retsplejelovens § 997, stk. 3.

Ligeledes kan den, der i forbindelse med en behandling, som udføres for offentlige myndigheder, overtræder § 41, stk. 3, eller § 53 eller tilsidesætter vilkår som nævnt i f.eks. § 9, stk. 3, straffes med bøde eller fængsel indtil 4 måneder, jf. § 70, stk. 2.

Strafansvar vil endvidere efter omstændighederne kunne pålægges i medfør af bestemmelser i straffelovens kapitel 16 om forbrydelse i offentlig tjeneste eller hverv mv. Endelig vil der kunne skrides disciplinærretligt ind over for offentlige ansattes tilsidesættelse af persondatalovgivningen.

Efter § 70, stk. 3, kan der pålægges straf i forbindelse med behandlinger, som er omfattet af en anden medlemsstats lovgivning, men som Datatilsynet efter § 64, stk. 1, påser lovligheden af. Med bestemmelsen sikres det, at der vil kunne pålægges databehandlere

strafansvar, hvis de ikke efterlever Datatilsynets forbud eller påbud efter § 59, hvis de ikke opfylder tilsynets krav efter § 62, stk. 1, eller hvis de hindrer tilsynet i at udføre inspektioner, jf. § 62, stk. 3 og 4.

Endelig kan selskaber (juridiske personer) pålægges strafansvar efter reglerne i straffelovens 5. kapitel, jf. § 70, stk. 5.

2.5.1.2.1. Praksis vedrørende overtrædelse af persondataloven
Datatilsynet har oplyst, at tilsynet har en intern oversigt over sager, der har ført til bødevedtagelse eller dom. Oversigten vedrører dels sager, hvor Datatilsynet har indgivet politianmeldelse, dels andre sager, som tilsynet har fået kendskab til.

Oversigten indeholder en bred vifte af overtrædelser af persondataloven, men henset til kortlægningens formål har Datatilsynet særligt fremhævet følgende overtrædelser:

1) Opslag i RKI-registeret
Datatilsynet har oplyst at have kendskab til flere bødevedtagelser og en enkelt dom vedrørende uberettigede opslag i kreditoplysningsbureauet Experian A/S' register over dårlige betalere – det såkaldte RKI-register. Der var tale om overtrædelse af persondatalovens § 5, stk. 2, og § 6, stk. 1. En af sagerne vedrørte tre journalisters opslag i RKI-registret via deres arbejdsgivers – en avis – RKI-abonnement og efterfølgende videregivelse af oplysningerne i forbindelse med udgivelse af artikler vedrørende et medlem af Folketinget. Uberettigede opslag i RKI-registret takseres normalt til en bøde på 5.000 kroner, men i den nævnte sag vedtog den ene af de tre journalister et bødeforelæg på 10.000 kroner.

2) Opslag i Det Central Motorregister (CRM)
Datatilsynet har oplyst at have kendskab til én sag, hvor en ansat i et forsikringsselskab på sin arbejdsplads ved opslag i CRM indsamlede personoplysninger om seks køretøjers ejerforhold og efterfølgende videregav oplysningerne til personer med tilhørsforhold til bandemiljøet. Der var tale om overtrædelse af persondatalovens § 5, stk. 2, og § 6, stk. 1. Der blev i sagen vedtaget et bødeforelæg på 5.000 kroner.

3) Opslag i Det Centrale Personregister (CPR)
Datatilsynet har oplyst at have kendskab til, at Østre Landsret i 2012 stadfæstede Retten i Glostrups dom på 30 dages ubetinget fængsel til en byrådspolitiker for misbrug af sit hverv som borgmester ved at pålægge en ansat i kommunen at indhente oplysninger af personlig og fortrolige karakter med henblik på fremme borgmesterens karriere ved at skade et andet byrådsmedlems omdømme. Borgmesteren blev ligeledes dømt for at have videregivet oplysningerne til tredjemand. Der var tale om overtrædelse af straffe-

lovens § 152, stk. 2, jf. stk. 1, og § 155, 1. og 2. pkt. Anklagemyndigheden frafaldt som led i sin anke den subsidiære tiltale for overtrædelse af persondatalovens § 6.

4) Sikkerhedsbrister
Datatilsynet har oplyst at have kendskab til to bødevedtagelser og en dom i sager, hvor butikker har videresolgt computere med harddiske indeholdende oplysninger om tidligere ejere. I disse sager var der tale om overtrædelse af persondatalovens § 41, stk. 3, idet der ikke var truffet de fornødne tekniske og organisatoriske foranstaltninger mod, at oplysninger kom til uvedkommendes kendskab. I den ældste sag blev der afsagt dom mod en detailhandelskæde lydende på betaling af en bøde på 3.000 kr., og i den næstældste sag blev der vedtaget et bødeforelæg på 5.000 kr. I den nyeste sag blev der vedtaget et bødeforelæg på 15.000 kr. til detailhandelskæden i den førstnævnte sag, idet der var tale om et gentagelsestilfælde.

I sager, hvor offentligt ansatte har misbrugt deres adgang til personoplysninger og uberettiget har videregivet oplysninger til uvedkommende, er det Datatilsynets opfattelse, at et sådant misbrug bør imødegås med følelige disciplinære foranstaltninger. Tilsynet har i den forbindelse henvist til sin udtalelse af 28. juni 2001 til Holstebro Kommune vedrørende videregivelse af personoplysninger fra et kommunalt register til en avis[37]. Udtalelsen vedlægges som **bilag 4**.

2.5.1.3. Rettighedsfrakendelse
Ifølge persondatalovens § 71, 1. pkt., kan den, der driver eller er beskæftiget med virksomhed som nævnt i § 50, stk. 1, nr. 2-5 (advarselsregister/spærreliste, kreditoplysningsbureau, stillingsbesættende virksomhed og retsinformationssystem), eller § 53 (edb-servicebureau), ved dom for strafbart forhold frakendes retten hertil, såfremt det udviste forhold begrunder en nærliggende fare for misbrug.

Straffelovens bestemmelser om tidsmæssig begrænsning af frakendelsen af retten og om umiddelbar udelukkelse af denne under sagens behandling mv. finder tillige anvendelse, jf. henvisningen til straffelovens § 79, stk. 3 og 4, i § 71, 2. pkt.

2.5.2. Straffebestemmelser mv. på det finansielle område
2.5.2.1. Lov om finansiel virksomhed
Finanstilsynets tilsynsbeføjelser er nærmere beskrevet under punkt 2.4.2 ovenfor, herunder muligheden for at give virksomheder påbud, der er nødvendige for efterlevelse af reglerne i lov om finansiel virksomhed. Hvis en virksomhed omfattet af lov om finansiel virksomhed undlader at efterleve et påbud fra Finanstilsynet, kan den straffes med bøde jf. § 374, stk. 5, i lov om finansiel virksomhed.

[37] Datatilsynets j.nr. 2000-632-0002.

Finanstilsynets tilsyn med finansielle virksomheder og fællesejede datacentraler efter lov om finansiel virksomhed er generelt omfattet af en skærpet tavshedspligt, jf. lov om finansiel virksomhed § 354. Imidlertid indeholder loven en række bestemmelser, der sikrer offentligheden informationer om tilsynet.

Det følger af § 354 a, at afgørelser og politianmeldelser, der har været behandlet af Finanstilsynets bestyrelse, og som dermed er af principiel eller vidtrækkende karakter, som alt overvejende hovedregel skal offentliggøres med angivelse af virksomhedens navn.

Efter hver inspektion i en finansiel virksomhed udarbejder Finanstilsynet en redegørelse, som virksomheden er forpligtet til at offentliggøre. Redegørelsen skal give offentligheden – herunder eksisterende og potentielle kunder, journalister og investorer – bedre indsigt i virksomhedens risikoprofil. Redegørelsens indhold skal være sammenfaldende med de hovedbudskaber, som Finanstilsynet giver til virksomheden, herunder de væsentligste tilsynsreaktioner. Redegørelsen indeholder både de centrale påbud, påtaler og risikooplysninger, som Finanstilsynet giver i forbindelse med inspektionerne og en sammenfattende risikovurdering af virksomheden.

Pr. 1. januar 2015 skal også fællesejede datacentraler offentliggøre sine inspektionsrapporter.

Overtrædelser af bestemmelsen om tavshedspligt i § 117 i lov om finansiel virksomhed straffes jf. lovens § 373, stk. 1, med bøde eller fængsel i 4 måneder, medmindre højere straf er forskyldt efter anden lovgivning. Der kan efter § 373, stk. 5, pålægges selskaber mv. strafansvar. Dette indebærer, at en finansiel virksomhed eller en ansat i en finansiel virksomhed, som uberettiget udnytter eller videregiver fortrolige oplysninger, herunder oplysninger om virksomhedens kunder, kan ifalde straf.

Da tavshedspligten efter § 117, stk. 2, følger oplysningerne, vil det tillige være muligt at strafforfølge en person eller virksomhed, som har fået videregivet oplysningerne, for eksempel i forbindelse med en finansiel virksomheds outsourcing af opgaver, herunder outsourcing af databehandlingsopgaver, og som uberettiget videregiver sådanne oplysninger.

Der findes ikke egentlig domspraksis på området, men der er i 2013 vedtaget et udenretligt bødeforlæg på 25.000 kr. af en person, der uberettiget havde udnyttet visse fortrolige oplysninger om et pengeinstitut.

2.5.2.2. Lov om betalingstjenester og elektroniske penge

Overtrædelse af betalingstjenestelovens § 85, stk. 2-4, straffes med bøde, jf. lovens § 107, stk. 2. Forbrugerombudsmanden er ikke bekendt med, at der har været rejst straffesager om overtrædelse af betalingstjenestelovens § 85 eller tilsvarende bestemmelser i tidligere love. Lovens forarbejder giver i øvrigt ikke anvisninger om strafniveauet for overtrædelse af bestemmelsen.

Finanstilsynet har i tilsynet med betalingsinstitutter de samme sanktionsmuligheder, som tilsynet kan anvende i forhold til finansielle virksomheder og fællesejede datacentraler. Det vil sige, at tilsynet som led i sin tilsynsvirksomhed efter betalingstjenestelovens § 86 kan anvende påtaler, påbud og risikooplysninger, hvis Finanstilsynet i forbindelse med en inspektion eller behandlingen af konkrete tilsynssager konstaterer, at virksomheden ikke lever op til/har opfyldt lovens krav om en betryggende it-sikkerhed.

Hvis et betalingsinstitut ikke efterkommer et påbud, f.eks. om at indføre konkrete sikkerhedsprocedurer, kan virksomheden straffes med bøde, jf. betalingstjenestelovens § 107, stk. 3.

Tilsynet med betalingsinstitutter er ligesom tilsynet med finansielle virksomheder og fællesejede datacentraler generelt omfattet af en skærpet tavshedspligt, jf. lovens § 92.

Dog skal afgørelser og politianmeldelser, der har været behandlet af Finanstilsynets bestyrelse, og som dermed er af principiel eller vidtrækkende karakter, offentliggøres efter reglerne i lov om finansiel virksomhed.

Ligeledes skal Finanstilsynet i forbindelse med inspektioner udarbejde en inspektionsredegørelse efter samme regler, som gælder efter lov om finansiel virksomhed, og som skal offentliggøres af det undersøgte betalingsinstitut.

2.5.3. Straffebestemmelser i anden relevant lovgivning

2.5.3.1. Straffebestemmelser mv. i sundhedsloven

2.5.3.1.1. Overtrædelse af sundhedslovens bestemmelser om indhentning og videregivelse af oplysninger er strafbelagt, jf. lovens § 271. Strafbelagt er ifølge denne bestemmelse:

1) Videregivelse af oplysninger i strid med § 41, stk. 1-3, § 43, stk. 1 og 2, og § 45,
2) Indhentelse af oplysninger i strid med § 42 a, stk. 1-10,
3) Uberettiget udnyttelse af oplysninger omfattet af § 41, stk. 1, eller

4) Indhentelse, videregivelse eller udnyttelse oplysninger i strid med § 157, stk. 2-4, 6 eller 11, eller § 157 a, stk. 2 eller 3, eller i strid med regler fastsat i medfør af § 157, stk. 5, eller § 157 a, stk. 4.

På samme måde straffes andre end de personer, der er nævnt i §§ 41, 42 a, 43, 45, 157 og 157 a, ved uberettiget indhentning, videregivelse eller udnyttelse af oplysninger omfattet af disse bestemmelser. Sanktionsmuligheden retter sig primært mod personer, der ikke har en berettiget adgang til systemerne, men som desuagtet bliver bekendt med oplysninger.

Strafferammen i sundhedslovens § 271 er bøde eller fængsel indtil 4 måneder.

Det følger herudover af § 16, stk. 1, i bekendtgørelse nr. 460 af 8. maj 2014 om adgang til og registrering af lægemiddel- og vaccinationsoplysninger, at medmindre højere straf er forskyldt efter anden lovgivning, straffes med bøde den, der uberettiget indhenter, overfører, videregiver eller undlader at indberette lægemiddel- og vaccinationsoplysninger i strid med bekendtgørelsens §§ 6-11.

Herudover vil en uberettiget indhentelse eller videregivelse af patientoplysninger kunne få ansættelsesretlige konsekvenser, ligesom overtrædelse af regelsættet kan indbringes for Styrelsen for Patientsikkerhed og Sundhedsvæsenets Disciplinærnævn.

Endelig kan der meddeles et fagligt påbud til en autoriseret sundhedsperson om ændring af dennes virksomhed, hvis styrelsen finder, at sundhedspersonen har udvist alvorlig eller gentagen kritisabel faglig virksomhed. På baggrund af en sådan indskærpelse kan en sundhedsperson fratages autorisationen, hvis vedkommende ikke efterkommer et sådant påbud, jf. autorisationslovens[38] § 7.

Styrelsen for Patientsikkerhed kan i en række tilfælde midlertidigt fratage en sundhedsperson autorisationen helt eller delvist, jf. autorisationslovens § 8. Midlertidig fratagelse af autorisationen kan ske i påtrængende tilfælde, hvor den fortsatte virksomhed skønnes at frembyde overhængende fare. Midlertidig indskrænkelse af retten til virksomhedsudøvelse kan ske i påtrængende tilfælde, hvor der er begrundet mistanke om, at en autoriseret sundhedsperson er til fare for patientsikkerheden på et eller flere faglige områder, mens mistanken undersøges.

2.5.3.1.2. Praksis vedrørende overtrædelse af lovgivningen på sundhedsområdet

[38] Lovbekendtgørelse nr. 877 af 4. august 2011 om autorisation af sundhedspersoner og om sundhedsfaglig virksomhed med senere ændringer.

I konkrete tilfælde er der sket afskedigelser begrundet i uberettiget adgang til oplysninger. Der kendes ikke til eksempler på, at en sundhedsperson er blevet frataget sin autorisation som følge af uberettiget indhentelse eller videregivelse af oplysninger.

For så vidt angår uberettiget adgang til det Fælles Medicinkort, jf. sundhedslovens § 157, modtog Sundhedsdatastyrelsen i 2015 ca. 60 henvendelser om potentielle uberettigede opslag. Af disse sager førte ca. 20 til politianmeldelse på baggrund af uberettiget adgang. Sagerne er typisk endt med vedtagelse af bødeforelæg i størrelsesordenen 4.000 kr.

Sagerne opdages oftest som følge af, at en borger retter henvendelse til Sundhedsdatastyrelsen på baggrund af logoplysninger udstillet i "Min Log" på Sundhed.dk. Sager om uberettiget adgang falder typisk i to kategorier:

- Sager, hvor den pågældende kliniker ikke har været opmærksom på regelsættet, har fejlanvendt sit system eller lignende, og
- sager, hvor der er en personlig relation mellem klinikeren, og den borger der foretages opslag på.

Herudover er der eksempler på sager, hvor borgeres CPR-numre er blevet misbrugt af andre til at få udstedt recepter og udleveret medicin, idet én person har udgivet sig for at være en anden ("identitetstyveri"). I sådanne sager er der typisk tale om, at "identitetstyven", ved at udgive sig for at være en anden, formår at få en læge til at tilgå den anden persons data og f.eks. udstede recepter til sig, hvorefter apoteket tilgår den anden persons data i forbindelse med udleveringen.

I denne type sager sker der en udredning og en berigtigelse af registrerede oplysninger, der fejlagtigt er blevet registreret. Der sker ikke politianmeldelse af de involverede sundhedspersoner, da de har befundet sig i en faktisk vildfarelse om at have den pågældende person i aktuel behandling, men "identitetstyven" vil kunne blive straffet i medfør af straffeloven eller anden lovgivning.

2.5.3.2. Straffelovens bestemmelser om freds- og ærekrænkelser

Overtrædelse af straffelovens § 263, stk. 2, straffes ifølge bestemmelsen med bøde eller fængsel indtil 1 år og 6 måneder.

Overtrædelse af straffelovens § 264 d straffes ifølge bestemmelsen med bøde eller fængsel indtil 6 måneder.

3. Beskyttelse af personoplysninger på sundhedsområdet

Som nævnt under punkt 1.1.1 ovenfor, blev der i forlængelse af afsløringerne om Se og Hørs overvågning af en række kongelige og kendte personers brug af kreditkort bragt historier i medierne om, at også ansatte hos bl.a. Rigshospitalet havde forsynet Se og Hør med oplysninger om kongelige og kendte personer.

På den baggrund omtales beskyttelse af personoplysninger på sundhedsområdet i det følgende.

3.1. Kortlægning af eksisterende niveau

3.1.1. Sundheds- og Ældreministeriet har lavet en kortlægning af koncernens arbejde med datasikkerhed.

Kortlægningen omfatter Statens Serum Institut (herunder National Sundheds-IT (nu Sundhedsdatastyrelsen)), Sundhedsstyrelsen, Patientombuddet (nu Styrelsen for Patientsikkerhed), departementet og MedCom, og tager udgangspunkt i følgende emner: Adgang til persondata, kriterier for adgang, logning, fysisk lagring af data, øvrige relevante sikkerhedsprocedurer, eksempler på misbrug, planlagte forbedringer af sikkerhedsniveauet og ansvar for overholdelse af sikkerhedsprocedure.

Overordnet viser gennemgangen, at der sker logning på alle relevante it-systemer af klinikeradgang. Der er konstateret ét tilfælde af misbrug som medførte afskedigelse. Som led i koncernstrategi for it-sikkerhed indføres logning på alle systemer, herunder på administrator-niveau.

3.1.2. It-sikkerhed i koncern it-strategien

Sundheds- og Ældreministeriet har i sin koncern it-strategi for 2013-2016 fokus på it-sikkerhed. Sundheds- og Ældreministeriet har igangsat initiativer, som skal sikre, at hele koncernen kan opfylde statens krav til informationssikkerhed gennem efterlevelse af gældende love og regler samt relevante standarder, herunder ISO/IEC 27001 – en standard, der indeholder krav til, hvorledes et informationssikkerhedsledelsessystem skal implementeres og vedligeholdes.

3.1.3. It-sikkerhed i praksis

Statens Serum Institut (National Sundheds-IT)

National Sundheds-IT (nu Sundhedsdatastyrelsen) har ikke konstateret konkrete tilfælde af intern misbrug, hverken i deres egne systemer eller i de systemer, de drifter for de andre styrelser.

Klinikernes datahåndtering logges i overensstemmelse med sikkerhedsbekendtgørelsens krav, og der er etableret en række sikkerhedstiltag hos Sundhedsdatastyrelsen og leverandører, herunder vedrørende logning og begrænsninger på fysisk adgang. For så vidt angår Fælles Medicinkort og dets forgænger, Medicinprofilen, konstateredes der frem til 2014 i alt ca. 5 tilfælde årligt, hvor uberettiget adgang førte til politianmeldelse. I 2015 steg antallet af henvendelser, bl.a. på baggrund af en informationskampagne overfor borgerne om mulighed for at kontrollere adgangen til egne data, og der var ca. 20 tilfælde af politianmeldelse.

I forbindelse med koncernens fælles IT-strategi vurderes mulighederne for at konsolidere brugeradministrationen, så der opnås en større sikkerhed i administrationen af adgangsrettigheder. Der er konkret planlagt etablering af systematisk overvågning og logning af systemadministratorer med udvidede rettigheder.

Sundhedsstyrelsen og nu Lægemiddelstyrelsen
Sundhedsstyrelsen har ikke konstateret konkrete tilfælde af misbrug. Styrelsen har udarbejdet særlige retningslinjer og procedure for tildeling af brugeradgange for både styrelsens egne medarbejderne samt for Sundhedsdatastyrelsen og KMD, som drifter Sundhedsstyrelsens og Lægemiddelstyrelsens it-systemer. Der foretages logning på alle systemer hos KMD, og der er ved at blive udarbejdet en instruks for regelmæssig log-gennemgang.

Langt de fleste af Sundhedsstyrelsens systemer er enten kun tilgængelige for et meget lille antal medarbejdere, eller også er der mulighed for i hvert enkelt system at niveaudele rettighederne, således at medarbejderne kun har adgang til deres eget fagområde/relevante data i systemet.

Patientombuddet (nu Styrelsen for Patientsikkerhed)
Patientombuddet har ikke konstateret konkrete tilfælde af misbrug. Der sker logning i alle it-systemer hos Patientombuddet, enten af Patientombuddet eget system, eller af den part som drifter systemet. Der er i dag ikke etableret faste kontroller eller stikprøver af loggene, men det forventes indført i forlængelse af koncern it-strategiens fokus på datasikkerhed.

MedCom[39]
For et af MedCom's systemer har der været en enkelt episode, hvor der har været konstateret misbrug, hvilket resulterede i afskedigelse af den pågældende medarbejder.

[39] MedCom blev stiftet i 1994 og er en non-profit organisation, ejet og finansieret af Sundheds- og Ældreministeriet, Danske Regioner og Kommunernes Landsforening. Formålet med etableringen af MedCom var at standardisere og digitalisere de hyppigst forekommende kommunikationsstrømme mellem praktiserende læger, sygehuse og kommuner.

Endvidere har der været episoder, hvor sundhedsfaglige personer har kigget i egen journal, hvilket har medført advarsler.

Der sker logning for alle MedComs it-systemer, og for de systemer, som leverer oplysninger til Sundhedsjournalen, er alle logninger endvidere tilgængelige i MinLog på sundhed.dk, så borgeren kan følge med i, hvem der har kigget i journalen.

3.2. Teknisk understøttelse af datasikkerhed på sundhedsområdet

MinLog

På www.sundhed.dk kan borgerne se oplysninger om, hvem der har haft adgang til deres oplysninger i eJournal, sundhedsjournal eller det Fælles Medicinkort og på den baggrund selv tage affære, hvis de mener, at der er nogen, der uretmæssigt har tilgået oplysninger om dem.

Opfølgning på log

Der gælder efter sikkerhedsbekendtgørelsen i visse tilfælde krav om logning, jf. punkt 2.1.2.2 ovenfor. Loggen skal som udgangspunkt opbevares i 6 måneder, så den kan bruges, hvis man har mistanke om misbrug. Myndigheder med et særligt behov kan opbevare loggen i op til 5 år. For så vidt angår det Fælles Medicinkort og det Danske Vaccinationsregister har de dataansvarlige myndigheder vurderet, at der er et særligt behov for at opbevare data i to år, svarende til den strafferetlige forældelsesfrist for uberettigede opslag. Opbevaringen af logoplysninger i to år er anmeldt til Datatilsynet.

Som dataansvarlig bør der etableres en proaktiv opfølgning på logdata mhp. at identificere anomalier og uberettigede adgange. Det er derfor nødvendigt at opstille regler for, hvad der udgør normal og atypisk adfærd.

Mængden af transaktioner til fælles nationale services og på tværs i sundhedsvæsenet er i en markant stigning, hvilket øget behovet for en automatiseret opfølgning. Derfor har man etableret en såkaldt ”behandlingsrelationsservice”, der kan benyttes til at identificere transaktioner, hvor der ikke er tvivl om berettigelsen af et opslag. Dermed kan en opfølgning koncentrere sig om atypiske opslag.

Behandlingsrelationsservice sammenstiller datakilder for at vurdere, om der har været en behandlingsrelation mellem sundhedspersonen og patienten, f.eks. at der er sket afregning for en konsultation. Hermed kan man reducere mængden af transaktioner, der skal behandles manuelt.

Fortsat fokus på sikkerhedsarbejde

Af Økonomiaftalen for 2015 fremgår det, at adgang til data er afgørende for en god, effektiv og sammenhængende behandling af borgerne. Regeringen, KL og Danske Regioner er enige om, at arbejdet med data- og it-sikkerhed skal styrkes yderligere med henblik på at sikre fortrolighed om personoplysninger og et højt sikkerhedsniveau i den digitale infrastruktur og i brug af sundhedsdata.

4. Undersøgelser af beskyttelsesniveauet i Se og Hør-sagen

4.1. I lyset af afsløringerne om Se og Hørs overvågning af kendte og kongelige gennemførte Nets en intern undersøgelse af de faktiske forhold. Det fremgår af en redegørelse fra oktober 2014 udarbejdet til arbejdsgruppen (vedlagt som **bilag 5**).

Den interne undersøgelse viste bl.a., hvordan den omtalte IBM-operatør i perioden fra 2008 til 2012 lykkedes med at lække oplysninger om kendte og kongelige til Se og Hør. Det skete ifølge Nets for det første ved at foretage forespørgsler om transaktioner på et givent betalingskort, som IBM-operatørens jobfunktion gav mulighed for, til at spore udvalgte personer. For det andet benyttede IBM-operatøren sig af muligheden for at nulstille adgangskoden for medarbejdere i Nets' kundeservice, hvilket var muligt i dennes jobfunktion uden for normal arbejdstid. Hermed kunne IBM-operatøren midlertidigt (om aftenen, i ferier mv.) overtage medarbejderens identitet og på denne måde tilgå oplysninger, som IBM-operatøren ellers var afskåret fra. Nets skriver i redegørelsen, at det ikke længere er muligt for IBM-operatører hos Nets at foretage søgninger i transaktioner eller at nulstille adgangskoder.

Nets oplyser derudover, at der som opfølgning på Se og Hør-sagen er taget en række initiativer:

> "Nets har således udvidet adfærdsmonitoreringen og omfanget af stikprøvekontroller, ligesom der er foretaget en ekstraordinær gennemgang og indsnævring af brugeradgange til et absolut minimum. Alle ansættelseskontrakter er desuden blevet opdateret med skærpning og tydeliggørelse af konsekvenser ved overtrædelser. Alle ansatte i Nets har derudover modtaget ekstraordinær sikkerhedsundervisning. Der er endvidere oprettet en ekstern whistleblower-hotline for ansatte, der måtte få mistanke om misbrug."

Finanstilsynet var over årsskiftet 2014/2015 på en ordinær og planlagt funktionsundersøgelse på it-området hos Nets. Finanstilsynets inspektion gav som følge af de konstaterede svagheder anledning til seks påbud. De seks påbud er relateret til it-sikkerhed- og risikostyring, herunder styrkelse af it-sikkerhedsorganisationen med klart definerede roller og ansvar for organisering af it-arbejdet, outsourcing, adgang til systemer og data samt sikring af tilstrækkeligt fokus på at udbedre svagheder konstateret af systemrevisionen.

Finanstilsynet bemærkede dog samtidig, at der allerede var igangsat flere initiativer til at styrke it-sikkerheden i Nets, jf. følgende fra den offentlige redegørelse om it-inspektionen i Nets (vedlagt som **bilag 6**):

> "Finanstilsynet har konstateret, at Nets har igangsat flere væsentlige forbedringstiltag, der fremadrettet skal styrke Nets` generelle it-sikkerhedsstyring, og i forlængelse heraf er det Finanstilsynets vurdering, at de planlagte forbedringstiltag, hvis tilstrækkeligt implementeret, herunder med fastholdt ledelsesmæssigt fokus og prioritering, vil imødekomme Finanstilsynets påbud".

Nets har i marts 2016 udarbejdet en opdateret redegørelse til arbejdsgruppen (vedlagt som **bilag 7**). Her oplyser Nets, at man siden Finanstilsynets inspektion har arbejdet på at imødegå påbuddene samt på generelt at højne niveauet for it-sikkerhed og it-risikostyring:

> "Umiddelbart efter IT-inspektionen nedsatte Nets en intern task force med fuld støtte og bevågenhed hos koncernledelsen, der skal sikre, at Nets imødegår påbuddene. Alene i 2015 og 2016 investerer Nets et trecifret millionbeløb i udbygning af sikkerhedsorganisationen med henblik på at styrke sikkerheden på en måde, der ikke blot imødegår påbuddene, men også sikrer, at Nets fremadrettet vil have en IT-sikkerhedsorganisation, der afspejler det højst mulige niveau for risikostyring og informationssikkerhed. Hvor Nets' afdeling for IT-sikkerhed i 2014 bestod af 10 personer, består den i dag af 40 interne og 15 eksterne konsulenter, der udelukkende beskæftiger sig med opgave som logning og monitorering af transaktioner, løbende trusselsopsamling, statistiske beregninger af trusselsscenarier, gennemførelse af prøvecases og screeninger af kommende medarbejdere.
>
> Nets' interne systemrevision monitorerer løbende arbejdet med at imødegå påbuddene og implementere Nets' nye og forbedrede IT-sikkerhedsorganisation. Nets vil inden årets udgang have imødekommet samtlige påbud og anmodninger fra Finanstilsynet, samtidig med Nets implementerer det højst mulige niveau for risikostyring og informationssikkerhed, som man kan forvente af en virksomhed, der bl.a. arbejder med digitale betalinger."

Finanstilsynet foretager rutinemæssigt opfølgende undersøgelser i virksomheder, hvor der er fundet svagheder eller lignende af en karakter, som det har været tilfældet med Nets. En ny inspektion i Nets er således også planlagt.

4.2. Som nævnt under punkt 1.1.1 ovenfor, indledte Københavns Vestegns Politi den 28. april 2014 en efterforskning i sagen om Se og Hørs overvågning af en række kongelige og kendte personers brug af kreditkort. Der verserer på den baggrund en straffesag ved Retten i Glostrup, og der er forhåndsberammet retsmøder i sagen i efteråret 2016.

4.3. I forhold til de undersøgelser, som Datatilsynet som nævnt under punkt 1.1.1 ovenfor har iværksat, kan følgende oplyses:

Se og Hør

Datatilsynet blev via presseomtale i april 2014 bekendt med, at Se og Hør angiveligt systematisk havde indsamlet og brugt oplysninger fra Nets (tidligere PBS) om kendte danskeres brug af kreditkort. Datatilsynet anmodede Se og Hør om en redegørelse til brug for tilsynets overvejelser om, i hvilket omfang der kunne være tale om behandling af oplysninger i strid med persondataloven. I den forbindelse bemærkede Datatilsynet, at Se og Hør ikke sås at have anmeldt en redaktionel informationsdatabase til tilsynet efter § 3 i lov om massemediers informationsdatabaser.

Datatilsynets henvendelse blev i juli 2014 besvaret af Aller Media A/S' advokat, der bl.a. henviste til, at Aller Media A/S var blevet sigtet af politiet og derfor ikke ønskede at udtale sig til Datatilsynet.

På grund af forbuddet mod selvinkriminering i retssikkerhedslovens[40] § 10 havde Datatilsynet ikke mulighed for – som det ellers er tilfældet – at afkræve Aller Media A/S de oplysninger, som var nødvendige til sagens behandling.

Datatilsynet sendte på den baggrund sagen til Københavns Vestegns Politi med anmodning om, at spørgsmålet om eventuel overtrædelse af persondataloven blev inddraget i politiets sag mod Aller Media A/S.

I den forbindelse gjorde Datatilsynet opmærksom på, at det følger af persondatalovens § 2, stk. 6, at loven ikke finder anvendelse på behandlinger, der er omfattet af lov om massemediers informationsdatabaser. Datatilsynet anførte endvidere, at det efter tilsynets opfattelse er en forudsætning for, at en behandling er undtaget fra persondatalovens regler, at informationsdatabasen er anmeldt til Datatilsynet, jf. lov om massemediers informationsdatabaser § 3, stk. 1.

Den 18. marts 2015 oplyste Københavns Vestegns Politi over for Datatilsynet, at politikredsen ikke foretog sig yderligere i anledning af tilsynets henvendelse. Politikredsen henviste til, at Aller Media A/S havde oplyst, at selskabet - efter at have anmeldt Se og Hørs redaktionelle informationsdatabaser til Datatilsynet i september 2014 - var af den opfattelse, at de behandlinger, som måtte have fundet sted hos Se og Hør, er undtaget fra persondatalovens anvendelsesområde, jf. lovens § 2, stk. 6.

Ved brev af 20. maj 2015 til Københavns Vestegns Politi anførte Datatilsynet, at Aller Media A/S på tidspunktet for den eventuelle behandling af oplysninger fra Nets ikke havde foretaget anmeldelse af en redaktionel informationsdatabase til Datatilsynet. Det

[40] Lov nr. 442 af 9. juni 2004 om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter med senere ændringer.

er på den baggrund Datatilsynets opfattelse, at den behandling af personoplysninger, der skete hos Se og Hør forud for anmeldelsen af (bl.a.) Se og Hørs redaktionelle informationsdatabase, var omfattet af persondatalovens regler.

Datatilsynet indgav samtidig politianmeldelse mod Aller Media A/S for overtrædelse af persondatalovens § 6, stk. 1, og § 5, stk. 2, jf. § 70, stk. 1, nr. 1, ved over en længere periode at have indsamlet og gjort brug af oplysninger fra Nets (tidligere PBS) om kendte danskeres brug af kreditkort.

Rigshospitalet
Datatilsynet anmodede i maj 2014 Region Hovedstaden om en udtalelse, idet tilsynet via presseomtale var blevet bekendt med, at Se og Hør fra medarbejdere på Rigshospitalet angiveligt havde modtaget oplysninger om kendte personers scanninger på hospitalet.

Region Hovedstaden oplyste i maj 2014 bl.a., at chefredaktøren for Se og Hør telefonisk havde oplyst til den lægelige direktør for Rigshospitalet, at Se og Hør ikke havde udbetalt penge til ansatte fra Rigshospitalet for oplysninger, og at ingen ansatte fra Rigshospitalet havde leveret oplysninger til Se og Hør.

Datatilsynet foretog herefter i august 2014 en inspektion på Rigshospitalet. Inspektionen tog udgangspunkt i sikkerhedsmæssige spørgsmål omkring de oplysninger og it-systemer, der kunne være relevante i den aktuelle sag om muligt misbrug af oplysninger om kendte personers scanninger.

I forlængelse af inspektion anmodede Datatilsynet i december 2014 Region Hovedstaden – som dataansvarlig for Rigshospitalets behandling af personoplysninger – om supplerende oplysninger vedrørende to af de i sagen omhandlede elektroniske systemer. Region Hovedstaden besvarede Datatilsynets henvendelse den 15. januar 2015.

Region Hovedstadens svar rejste efter Datatilsynets opfattelse problemstillinger, som tilsynet fandt mest hensigtsmæssigt at behandle separat. Datatilsynet anmodede derfor i juni 2015 Region Hovedstaden om at besvare en række spørgsmål, særligt vedrørende medarbejderes brugeradgange til personoplysninger på regionens hospitaler. Datatilsynet meddelte samtidig, at regionens svar også vil kunne indgå i Datatilsynets sag om muligt læk af patientoplysninger, herunder tilsynets inspektionssag.

Region Hovedstaden har i brev af 28. august 2015 besvaret Datatilsynets seneste spørgsmål. Datatilsynet forventer umiddelbart at kunne træffe afgørelse i sagerne medio 2016.

SAS og Naviair

Datatilsynet anmodede i maj 2014 SAS om en udtalelse i anledning af, at tilsynet via presseomtale var blevet bekendt med, at Se og Hør fra medarbejdere i SAS angiveligt havde modtaget oplysninger fra SAS' it-systemer om kendte personers flyrejser.

SAS afgav i breve af 20. maj og 8. september 2014 oplysninger til sagen.

Sideløbende besluttede datatilsynsmyndighederne i Norge, Island, Finland og Danmark i foråret 2015 som led i et nordisk samarbejde at gennemføre inspektioner af flere nordiske flyselskaber. Datatilsynet gennemførte i den forbindelse en inspektion af SAS' behandling af personoplysninger.

Datatilsynet anmodede i første omgang skriftligt SAS om at besvare en række spørgsmål om selskabets behandling af kundeoplysninger. På baggrund af svaret fra SAS besluttede Datatilsynet at gennemføre en fysisk inspektion hos SAS. Inspektionen blev foretaget den 25. juni 2015.

Ved e-mail af 21. august 2015 afgav SAS bemærkninger til Datatilsynets udkast til inspektionsreferat. Datatilsynet forventer at træffe afgørelse i august eller september 2016.

Datatilsynet har i øvrigt fra Trafik- og Byggestyrelsen bl.a. modtaget en redegørelse fra Naviair. Redegørelsen gav ikke Datatilsynet anledning til at indlede en undersøgelse af forholdene hos Naviair. Datatilsynet måtte på baggrund af det oplyste lægge til grund, at der var tale om et enkeltstående tilfælde, som virksomheden effektivt havde taget hånd om.

5. Regeringens arbejde med informationssikkerhed

Finansministeriet har ansvaret for informationssikkerhed og privatlivsbeskyttelse i den offentlige sektor. Dette indebærer ansvaret for:

- National strategi for cyber- og informationssikkerhed i samarbejde med Center for Cybersikkerhed.
- Implementering af den internationale sikkerhedsstandard ISO27001 i statslige institutioner.
- Ny digitaliseringsstrategi 2016-20 med fokus på bl.a. informationssikkerhed.
- Statens informationssikkerhedsforum (SISF) for statslige informationssikkerhedskoordinatorer.
- De fællesoffentlige login-sikkerhedsløsninger, NemLogin og NemID.

I det følgende omtales regeringens arbejde på disse områder kort.

5.1. Strategi for cyber- og informationssikkerhed

For at styrke og professionalisere arbejdet med cyber- og informationssikkerhed i staten nedsatte den daværende regering i foråret 2014 en tværministeriel arbejdsgruppe med det opdrag at udarbejde en strategi for cyber- og informationssikkerhed.

Den stigende digitalisering indebærer en øget koncentration af oplysninger og centrale it-systemer, og den øgede anvendelse af digitale løsninger indebærer et øget behov for, at myndighederne har stort fokus på at styrke deres arbejde på cyber- og informationssikkerhedsområdet. Endvidere er der behov for fokus på tværgående koordinering, så det sikres, at de informationer og systemer, der indgår i den digitale infrastruktur, er beskyttet på bedst mulig vis.

På den baggrund lancerede den daværende regering i december 2014 en national strategi for cyber- og informationssikkerhed.

Strategien er målrettet de statslige myndigheder, men indeholder også en indsats rettet mod virksomheder på energiområdet og teleområdet med infrastruktur af væsentlig samfundsmæssig betydning.

De overordnede målsætninger for regeringens arbejde med at styrke cyber- og informationssikkerhedsarbejdet er:

- Borgere og virksomheder skal have tillid til, at cyber- og informationssikkerheden i staten og blandt leverandører af samfundsmæssig væsentlig infrastruktur håndteres professionelt og betryggende. Indsatsen for at styrke cyber- og informationssikkerheden skal samtidig muliggøre en brugervenlig og effektiv udnyttelse af nye teknologiske muligheder.
- Der skal ske en styrket beskyttelse af vigtige samfundsfunktioner og af den nationale sikkerhed mod cyberangreb.

Derudover beskriver strategien en klar ansvarsfordeling mellem myndighederne på cyber- og informationssikkerhedsområdet og danner således grundlag for en styrket koordinering af aktiviteterne på området. Strategien skal sikre, at den offentlige sektor kan agere aktivt i forhold til nye muligheder og trusler, således at digitaliseringens potentialer kan udnyttes uden uacceptable sikkerhedsrisici.

Til at understøtte målsætningen har regeringen udpeget seks strategiske indsatsområder, der skal løfte samfundets cyber- og informationssikkerhed. Disse er:

1. Stærkt it-tilsyn og professionalisering
2. Klare krav til leverandører
3. Styrket cybersikkerhed og mere viden på området
4. Robust infrastruktur i energisektoren og telesektoren
5. Danmark som stærk international medspiller
6. Stærk efterforskning og klar information til borgere, virksomheder og myndigheder

Under disse indsatsområder er der 27 initiativer, herunder på det styringsmæssige område udvikling af et fælles koncept for it-tilsynet i staten, krav om efterlevelse af sikkerhedsstandarden ISO27001, obligatoriske, privatlivsrelaterede og sikkerhedsmæssige risikovurderinger i it-projekter til over 10 mio. kr. samt opfølgning på den sikkerhedsmæssige leverandørstyring. Med dette adresserer strategien, at myndighederne fremadrettet skal professionalisere deres sikkerhedsledelse og skærpe deres fokus på sikring af data, herunder borgernes følsomme personoplysninger, gennem bedre leverandørstyring og privatlivsvurderinger.

Endelig skal der sikres en bedre fællesoffentlig koordinering, videndeling og hændelseshåndtering mellem statslige myndigheder, ligesom der skal gennemføres en informationsindsats målrettet borger og virksomheder i Danmark.

5.2. ISO27001 – en international standard til styring af informationssikkerhed

Den internationale informationssikkerhedsstandard ISO27001 skal som følge af den nationale cyber- og informationssikkerhedstrategi være implementeret i statslige myndigheder primo 2016. Standarden stiller en række krav til styring af arbejdet med informationssikkerhed, herunder at arbejdet er risikobaseret og forankret i topledelsen. Dette indebærer, at ledelsen gennem en risikovurdering gøres bekendt med organisationens risici. Derudfra kan ledelsen prioritere ressourcerne og igangsætte initiativer for at sikre, at organisationen ikke udsætter sig for større risici, end det kan accepteres.

Arbejdet med informationssikkerhed i en organisation handler grundlæggende om at sikre organisationens samlede informationsaktivers *fortrolighed, tilgængelighed og integritet*. Med informationsaktiver forstås informationer og data, som organisationen bruger i sin drift, f.eks. notater, korrespondance, arbejdsdokumenter, kalenderaftaler, forretningsdokumenter, og som kan indgå i et journalsystem, e-mailsystem, papirbaseret arkiv, en selvbetjeningsløsning mv.

Implementering af ISO27001 i en organisation medfører, at der skal opbygges et ledelsessystem, der betoner en ledelsesforankret, forretningsorienteret og risikobaseret tilgang til beskyttelse af organisationens informationer. Ledelsessystemet for informa-

tionssikkerhed, det såkaldte *Information Security Management System* (ISMS), beskriver, de processer og aktiviteter som organisationen skal implementere i sit ledelsessystem for at strukturere, implementere, vedligeholde og forbedre et passende informationssikkerhedsniveau.

Et ledelsessystem for informationssikkerhed består således af alle de politikker, procedurer, retningslinjer og tilhørende ressourcer og aktiviteter, som organisationen administrerer for at beskytte sine informationsaktiver. Alt sammen elementer, der understøtter organisationen i at nå sine mål. ISO-standarden er på den måde et relevant ledelsessystem at anvende for organisationer, der har behov for en systematiseret tilgang til at vurdere informationsaktivernes betydning for organisationen.

Ledelsessystemet tager udgangspunkt i en særlig metode til kvalitetssikring og strukturering af alle processer. Med det opnår institutionerne at etablere et systematiseret fokus på institutionernes informationsaktiver og -processer og en vurdering af den forretningsorienterede betydning.

Implementering af ISO-standarden anviser således muligheden for ledelsen til at etablere den nødvendige viden om organisationens risikobillede til at kunne igangsætte de beslutninger og den indsats, der giver størst sikkerhed i forhold til ressourceforbruget. Dermed styrkes forudsætningerne for, at niveauet for informationssikkerhed og robustheden over for cyberangreb kan øges ud fra en prioritering af ressourcerne. Med efterlevelse af sikkerhedsstandarden er der mulighed for, at sikkerhedsarbejdet håndteres i faste rammer i myndigheden og bliver tænkt ind i alle sammenhænge. Målet er, at myndigheden derved bliver bedre til f.eks. at opdage sårbarheder, sådan at der forhåbentlig vil komme færre konkrete sikkerhedshændelser, hvor borgerne data udstilles.

For at støtte arbejdet med sikkerhedsdagsordenen har Digitaliseringsstyrelsen publiceret en række vejledninger om implementering af standarden.

5.3. Ny digitaliseringsstrategi

Kommunerne, regionerne og staten har i maj 2016 lanceret en ny fællesoffentlig digitaliseringsstrategi, som skal sikre, at den offentlige sektor frem mod 2020 tilbyder en tilgængelig, hurtig og sammenhængende offentlig service, der er omkostningseffektiv og understøtter vækst og produktivitet i virksomhederne. Digitaliseringsstrategien tager afsæt i de resultater, der allerede nu er opnået med den nuværende digitaliseringsstrategi for 2011-2015. Strategien sætter et højt ambitionsniveau for digitalisering af den offentlige sektor og understøtter, at borgere og virksomheder for alvor er rykket over på de offentlige digitale kanaler.

I den fællesoffentlige digitaliseringsstrategi indgår informationssikkerhed med betydelig vægt. Baggrunden for dette fokus er bl.a., at kravene til sikkerhed er øget i takt med koncentrationen af data i centrale it-systemer. Dette nødvendiggør, at det offentlige sørger for, at sikkerheden i deres håndtering af borgere og virksomheders oplysninger har et passende niveau, således at borgere og virksomheder kan have tillid til, at det offentlige behandler deres data forsvarligt.

5.4. Statens informationssikkerhedsforum

Statens informationssikkerhedsforum (SISF) består af sikkerhedskoordinatorer i statslige myndigheder. Forummet samles til fire møder og fire workshops om året med henblik på at sikre fælles læring og erfaringsudveksling mellem koordinatorerne.

Forummet sikrer, at sikkerhedskoordinatorerne kan drøfte forskellige aspekter af sikkerhedsarbejdet med ligesindede såsom etablering af sikkerhedskultur, sikring af ledelsesinvolvering, processer til risikovurdering, håndtering af hændelser og *awareness*. Med forummet er der etableret et stærkt netværk blandt fagpersoner, hvis fælles læring og dialog medvirker til et øget fokus på sikkerhedsdagsordenen og et højere sikkerhedsniveau i statens institutioner.

5.5. Andre initiativer

Den tidligere regering traf samtidig med iværksættelse af arbejdet med en national strategi for cyber- og informationssikkerhed beslutning om at igangsætte en række initiativer for at styrke cybersikkerheden i staten umiddelbart. Tiltagene skulle styrke forebyggelsen af hackerangreb og dermed forhindre eller reducere en væsentlig del af de målrettede angreb fra internettet. Blandt tiltagene var en positivliste af godkendte programmer, sikkerhedsopdatering af programmer, begrænsning af brugeradgang med særlige administrator-privilegier, logning mv. – tiltag som kan forbedre sikkerheden hos myndighederne.

Som netsikkerhedstjeneste udsender Center for Cybersikkerhed varsler om potentielle cyberangreb og assisterer andre myndigheder med at klarlægge forløbet ved større cyberangreb på samfundsvigtig informations- og kommunikations-infrastruktur og med afhjælpning af konsekvenserne af angrebet. Et eksempel er håndteringen af det sikkerhedsbrud, der fandt sted hos CSC i 2013, hvor Center for Cybersikkerhed i samarbejde med henholdsvis Justitsministeriet og Finansministeriet har spillet en væsentlig rolle. Regeringen har i forlængelse af sikkerhedsbruddet hos CSC udarbejdet to afsluttende rapporter. Formålet med rapporterne har været at sikre både en fyldestgørende undersøgelse af sikkerhedsbruddet samt at give en række konkrete anbefalinger til styrkelse af danske myndigheders it-sikkerhed.

Endelig udarbejdede Digitaliseringsstyrelsen i samarbejde med Center for Cybersikkerhed på baggrund af CSC-sagen rapporten 'Styrkelse af sikkerheden i statens outsourcede it-drift' i august 2014. Rapporten indeholder en række fremadrettede anbefalinger til statslige myndigheder vedrørende sikring af outsourcet it-drift. Anbefalingerne skal styrke informationssikkerheden i de statslige myndigheders outsourcede it.

Formålet med rapportens anbefalinger er at understøtte en styrkelse af såvel sikkerheden i de outsourcede statslige løsninger samt myndighedernes kontrol hermed. Rapporten og dens anbefalinger danner baggrund for, at statslige myndigheder i højere grad kan agere kompetent, rettidigt og – i passende omfang – koordineret i forhold til it-sikkerheden i nye og eksisterende outsourcede løsninger. Rapporten anbefaler bl.a. højere grad af dialog med leverandørerne om, hvordan den ønskede sikkerhed i de leverede ydelser opnås, og at myndighedernes risikovurdering og risikoledelse tager udgangspunkt i et opdateret trusselsbillede både ved nyudvikling, drift og videreudvikling af it-løsninger.

6. Arbejdsgruppens overvejelser

Som det fremgår under punkt 2 ovenfor, gælder der i dag i vidt omfang regler om, hvordan personoplysninger, herunder oplysninger om hvor betalere har anvendt deres betalingsinstrument, skal beskyttes mod uvedkommendes adgang mv. Som det endvidere fremgår, føres der af en række myndigheder – Datatilsynet, Finanstilsynet og Forbrugerombudsmanden – tilsyn med, at disse regler overholdes, og myndighederne har i den forbindelse en række tilsynsbeføjelser. I tilfælde af, at reglerne ikke overholdes, har de pågældende myndigheder en række reaktionsmuligheder, ligesom manglende overholdelse af reglerne kan sanktioneres med straf mv.

Afsløringerne om Se og Hørs overvågning rejser naturligt nok det spørgsmål, om de regler, der gælder i dag, og det tilsyn, der føres i dag, er godt nok til at sikre en effektiv beskyttelse af personoplysninger.

Afsløringerne om Se og Hørs overvågning må – ud fra det kendskab hertil, arbejdsgruppen har til sagen, bl.a. fra politiet, fra Nets' redegørelse til arbejdsgruppen og fra Finanstilsynets redegørelse om it-inspektion i Nets (jf. punkt 4 ovenfor) – efter arbejdsgruppens opfattelse anses som udtryk for, at enkeltpersoner i strid med gældende regler har misbrugt oplysninger, de som led i deres arbejde har været nødt til at have adgang til. Sådanne former for misbrug vil efter arbejdsgruppens opfattelse aldrig helt kunne forhindres. Det, man imidlertid kan overveje, er, om der kan gøres mere for at forhindre sådanne former for misbrug, f.eks. ved at højne sikkerhedsniveauet for beskyttelse af borgernes oplysninger.

Arbejdsgruppen har på den baggrund overvejet, om den beskyttelse af oplysninger, som efter de gældende regler er påkrævet, i tilstrækkeligt omfang sikrer mod misbrug. Arbejdsgruppen har i den forbindelse fokuseret på følgende to it-sikkerhedsmæssige spørgsmål: spørgsmålet om *adgang* til oplysninger og spørgsmålet om *sporing (logning)* af foretagne behandlinger af oplysninger.

Arbejdsgruppen har desuden overvejet, om der er anledning til at gøre mere for at sikre, at de til enhver tid gældende regler efterleves. Manglende efterlevelse af reglerne kan efter arbejdsgruppens opfattelse både skyldes, at dem, reglerne er rettet imod, ikke i tilstrækkeligt omfang er bekendt med indholdet heraf, eller at de sanktioner, som er forbundet med manglende efterlevelse af reglerne, ikke i tilstrækkelig grad motiverer til efterlevelse af reglerne.

Arbejdsgruppen har herudover overvejet, om der er behov for at ændre på det tilsyn, der føres med reglerne på området – både i forhold til beføjelser og reaktionsmuligheder - samt i forhold til grænsedragningen mellem tilsynsmyndighederne på området.

Arbejdsgruppen har i sine overvejelser taget udgangspunkt i, at der bør være balance mellem på den ene side de krav, der stilles til sikkerhedsniveauet for beskyttelse af oplysninger, og på den anden side behovet for, at virksomheder og myndigheder kan løse deres opgaver effektivt. Det er således på den ene side arbejdsgruppens opfattelse, at beskyttelse af oplysninger om borgernes elektroniske betalinger mv. skal prioriteres, og at beskyttelsesniveauet bør være så højt som muligt. På den anden side er arbejdsgruppen opmærksom på den hindring, som unødigt høje krav til it-sikkerhed mv. kan være for virksomheders og myndigheders løsning af deres opgaver.

Arbejdsgruppen har i sine overvejelser desuden taget udgangspunkt i, at persondatalovens regler, jf. punkt 2.1. ovenfor, i vidt omfang er baseret på og gennemfører EU's databeskyttelsesdirektiv. Direktivets bestemmelser om, hvornår der må ske behandling af personoplysninger, og om, hvordan personoplysninger skal beskyttes, indebærer således visse begrænsninger i adgangen til at fastsætte nationale regler om behandling af personoplysninger.

Det er herudover indgået i arbejdsgruppens overvejelser, at en ny databeskyttelsesforordning, som skal erstatte det gældende databeskyttelsesdirektiv fra 1995, blev vedtaget i april 2016 og skal anvendes fra den 25. maj 2018, jf. forordning nr. 679 af 27. april 2016. En forordning gælder direkte i medlemsstaterne[41], og danske myndigheder, virksomheder og borgere har således pligt til at rette sig efter en forordning. Eventuelle nye krav på nationalt niveau til beskyttelse af personoplysninger kan således meget vel vise

[41] Jf. EUF-Traktatens artikel 288.

sig at skulle ændres, når databeskyttelsesdirektivet bliver erstattet af den nye databeskyttelsesforordning.

Endelig er det indgået i arbejdsgruppens overvejelser, at justitsministeren senest i forbindelse med behandlingen af beslutningsforslag nr. B 140 om datasikkerhed har tilkendegivet, at den under punkt 1.1.1 ovenfor nævnte politiske drøftelse også vil omfatte udarbejdelsen af en samlet strategi til sikring af danskernes personoplysninger.

6.1. Behov for ændring af reglerne om behandlingssikkerhed (it-sikkerhed)

6.1.1. Generelt

Som det fremgår af punkt 2.1.2, 2.2.2.1 og 2.2.2.2 ovenfor, gælder der i vidt omfang regler om, hvordan personoplysninger, herunder oplysninger om, hvor betalere har anvendt deres betalingsinstrument, skal beskyttes mod uvedkommendes adgang mv. Disse regler sikrer efter arbejdsgruppens opfattelse en god beskyttelse af personoplysninger.

Det er som nævnt ovenfor desuden arbejdsgruppens opfattelse, at afsløringerne om Se og Hørs overvågning må anses som udtryk for, at enkeltpersoner – i strid med gældende regler – har misbrugt oplysninger, de som led i deres arbejde har været nødt til at have adgang til. Sådanne former for misbrug vil aldrig helt kunne forhindres, og sagen giver efter arbejdsgruppens opfattelse ikke i sig selv anledning til at ændre de gældende generelle regler om behandlingssikkerhed (it-sikkerhed), jf. punkt 6.1.2-6.1.4 nedenfor.

I forhold til spørgsmålet om, at der ud fra en generel betragtning kan siges at være behov for at ændre de gældende regler om behandlingssikkerhed, bemærkes, at der som nævnt er vedtaget en ny databeskyttelsesforordning. Denne forordning indeholder nye regler om behandlingssikkerhed. En forordning vil som nævnt være umiddelbart gældende i medlemsstaterne. På den baggrund må en eventuel ændring af i hvert fald persondatalovens regler om behandlingssikkerhed på nuværende tidspunkt anses for uhensigtsmæssig. Det vil således kunne medføre betydelige udgifter for virksomheder mv., hvis de flere gange i løbet af kortere tid vil skulle ændre de sikkerhedsforanstaltninger, der er truffet for at leve op til de gældende regler på området.

Arbejdsgruppens nærmere overvejelser om behovet for at ændre reglerne om behandlingssikkerhed følger af punkt 6.1.2-6.1.5 nedenfor.

6.1.2. Uddybende regler om behandlingssikkerhed for den private sektor

Som nævnt under punkt 2.1.2 ovenfor er der i medfør af persondatalovens § 41, stk. 5, fastsat uddybende regler om behandlingssikkerhed for den offentlige sektor i sikkerhedsbekendtgørelsen. I tilknytning hertil har Datatilsynet udstedt sikkerhedsvejledningen, der nærmere beskriver, hvordan kravene i bekendtgørelsen vil kunne opfyldes.

Som nævnt under punkt 2.1.2.3 ovenfor, er der ikke fastsat sådanne uddybende regler om behandlingssikkerhed for den private sektor, hvorfor det er bestemmelsen i persondatalovens § 41, stk. 3, som spørgsmål herom må afgøres efter.

Det fremgår af bemærkningerne til bestemmelsen i persondatalovens § 41, stk. 5, at det var hensigten ved lovens ikrafttræden at udstede en bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for *den offentlige forvaltning* helt eller delvis ved hjælp af elektronisk databehandling. Endvidere var det forudsat, at der skulle udstedes en tilsvarende bekendtgørelse for *domstolene*. Derimod var det ikke en forudsætning, at der (straks) ved lovens ikrafttræden skulle fastsættes nærmere regler om behandlingssikkerheden i *den private sektor*.

Arbejdsgruppen har overvejet, om der på nuværende tidspunkt i medfør af persondatalovens § 41, stk. 5, bør fastsættes nærmere regler om behandlingssikkerhed for den private sektor.

Som nævnt under punkt 2.1.2.3 er det Datatilsynets opfattelse, at bestemmelsen i persondatalovens § 41, stk. 3, medfører, at der som udgangspunkt må stilles samme krav til datasikkerheden i den private sektor som i den offentlige forvaltning, og tilsynet anbefaler generelt, at private dataansvarlige i videst muligt omfang tilrettelægger deres sikkerhedsforanstaltninger i overensstemmelse med sikkerhedsbekendtgørelsen.

Efter arbejdsgruppens opfattelse vil de tilfælde af misbrug, som afsløringerne om Se og Hørs overvågning har afdækket, næppe kunne være undgået ved, at der blev fastsat nærmere regler om behandlingssikkerhed for den private sektor. Som det fremgår af punkt 4 ovenfor, har eksempelvis Nets således i vidt omfang tilrettelagt sin it-sikkerhed i overensstemmelse med kravene i den sikkerhedsbekendtgørelse, der gælder for den offentlige sektor, herunder ved at foretage logning, indsnævre brugeradgange, undervise ansatte i sikkerhed, foretage intern og ekstern auditering samt løbende tilpasse kontrol- og sikkerhedsforanstaltninger i takt med behovet herfor.

Hertil kommer, at det i lyset af den nye databeskyttelsesforordning som nævnt vil være uhensigtsmæssigt at fastsætte nærmere regler om behandlingssikkerhed på nuværende tidspunkt.

Det er på den baggrund arbejdsgruppens opfattelse, at der ikke i medfør af persondatalovens § 41, stk. 5, bør fastsættes nærmere regler om behandlingssikkerhed for den private sektor.

6.1.3. Efterlevelse af ISO27001 i den private sektor

Som nævnt under punkt 5.2 ovenfor, blev alle statslige myndigheder forpligtede til at implementere den internationale informationssikkerhedsstandard ISO27001 primo 2016.

Arbejdsgruppen har overvejet, om det også bør gøres obligatorisk for private virksomheder, organisationer mv. at følge denne informationssikkerhedsstandard.

Som det fremgår af punkt 5.2 ovenfor, er informationssikkerhedsstandarden ISO27001 risikobaseret, hvilket betyder, at indsatsen primært skal fokuseres på områder, hvor der er høj risiko. I forbindelse med anvendelse af eksterne leverandører skal statslige myndigheder vurdere, om en potentiel leverandør kan træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger til at beskytte data. Som en del af dette skal kunden undersøge, om leverandøren kan opfylde de sikkerhedsmæssige krav, som kunden har defineret på grundlag af gennemførte it-risikovurderinger, herunder hvorledes leverandøren har organiseret sit sikkerhedsarbejde, eksempelvis om leverandøren har implementeret sikkerhedsstandarden ISO27001 eller arbejder på tilsvarende vis efter andre anerkendte standarder.

Efter arbejdsgruppens opfattelse vil de tilfælde af misbrug, som afsløringerne om Se og Hørs overvågning har afdækket, næppe kunne være undgået ved, at Nets eller andre implicerede var forpligtet til at efterleve sikkerhedsstandarden ISO27001.

Endvidere vurderer arbejdsgruppen, at det umiddelbart vil blive særdeles omkostningstungt, hvis alle danske virksomheder og organisationer forpligtes til at anvende sikkerhedsstandarden ISO27001. Der er stor sandsynlighed for, at krav om anvendelse af sikkerhedsstandarden for alle virksomheder og organisationer vil blive anset som en uproportional administrativ byrde, særligt af virksomheder og organisationer, hvis it-anvendelse ikke er forbundet med en høj risiko for misbrug af personoplysninger.

Det er på den baggrund arbejdsgruppens opfattelse, at sikkerhedsstandarden ISO27001 ikke bør gøres obligatorisk for private virksomheder og organisationer i Danmark. Det er dog arbejdsgruppens generelle anbefaling, at private virksomheder og organisationer implementerer sikkerhedsstandarden i situationer, hvor virksomheden eller organisationen ud fra en risikobaseret tilgang vurderer, at det vil understøtte deres sikkerhedsarbejde på konstruktiv vis.

6.1.4. Indførelse af ordning med databeskyttelsesansvarlige

Som anført under punkt 2.4.1.8 ovenfor giver databeskyttelsesdirektivets artikel 18 mulighed for at forenkle anmeldelsesordningen eller helt at fritage for anmeldelse, hvis

medlemsstaten etablerer en ordning, hvorefter den dataansvarlige udpeger en databeskyttelsesansvarlig, som bl.a. har til opgave i fuld uafhængighed at sikre den interne anvendelse af de nationale bestemmelser, der er truffet i medfør af databeskyttelsesdirektivet, for på den måde at sikre, at det ikke er sandsynligt, at de registreredes rettigheder og frihedsrettigheder vil kunne krænkes som følge af behandlingen.

Muligheden for at forenkle anmeldelsesordningen og gøre brug af en ordning, hvorefter den dataansvarlige udpeger en databeskyttelsesansvarlig, er ikke implementeret i Danmark. Arbejdsgruppen er imidlertid bekendt med, at dette er tilfældet i Sverige, Tyskland og Norge (direktivet gælder også for EØS-landene, jf. EØS-komitéens beslutning nr. 83/1999 af 25. juni 1999).

Arbejdsgruppen har på den baggrund overvejet, om indførelse af en ordning med databeskyttelsesansvarlige, eventuelt kombineret med en forenkling af anmeldelsesordningen, vil kunne føre til øget beskyttelse af personoplysninger.

Om muligheden for at indføre en sådan ordning er anført følgende i Registerudvalgets betænkning nr. 1345/1997 om behandling af personoplysninger, der danner baggrund for persondataloven, s. 336-337:

> ”Den i [persondatadirektivets] artikel 18, stk. 2, 2. pind, skitserede mulighed for undtagelse er ikke anvendt. Undtagelsesbestemmelsen forudsætter udpegelsen af en person med ansvar for beskyttelse af personoplysninger. Den udpegede person skal bl.a. have til opgave i fuld uafhængighed at sikre den interne anvendelse af de nationale bestemmelser, der er truffet i medfør af direktivet. Endvidere skal vedkommende have til opgave at føre et register over de behandlinger, der gennemføres af den dataansvarlige, og som omfatter de i artikel 21, stk. 1, omhandlede oplysninger. Der findes ingen tilsvarende konstruktion i den nugældende registerlovgivning. I den føderale tyske databeskyttelseslov er der i dag regler om udpegning af en uafhængig ”databeskyttelsesofficer” i virksomheder m.v. med over et vist antal ansatte. Denne ”officer” skal føre et vist tilsyn med overholdelsen af lovgivningen på området samt føre en fortegnelse over de behandlinger, som finder sted i den pågældende virksomhed.
>
> Indførelsen af en sådan ordning vil rejse en række problemstillinger af ansættelsesretlig og ledelsesmæssig karakter, navnlig som følge af kravet om at den pågældende person skal fungere i fuld uafhængighed. F.eks. vil der kunne opstå problemer i tilfælde af uenighed mellem ledelsen i en myndighed eller virksomhed og den pågældende person, ligesom der også i det daglige samarbejde vil kunne opstå problemer. Udvalget er endvidere af den opfattelse, at et krav om udpegelse af en person, som har ansvaret for at påse overholdelsen af reglerne i lovudkastet, vil pålægge virksomhederne en stor byrde. Hertil kommer, at udvalget finder det væsentligt, at tilsynet føres centralt af instanser med en særlig ekspertise på området samt erfaringer med behandlinger, som foretages for *alle* typer af virksomheder, hvorved det sikres, at praksisdannelsen bliver ensartet og sammenhængende. Ordningen er under alle omstændigheder heller ikke egnet til at finde anvendelse i mindre virksomheder, institutioner m.v. På denne baggrund har udvalget ikke foreslået indførelsen af en sådan ordning.”

Henset til det i betænkningen anførte om baggrunden for ikke at indføre en sådan ordning i Danmark og til, at der er vedtaget en ny databeskyttelsesforordning, som vil indeholde nye regler om behandlingssikkerhed, herunder krav om brug af databeskyttelsesansvarlige i visse situationer, er det arbejdsgruppens opfattelse, at der ikke på nuværende tidspunkt bør indføres en ordning med databeskyttelsesansvarlige.

Det bemærkes i den forbindelse dog, at det følger af artikel 37 i den nye databeskyttelsesforordning, at den dataansvarlige og databehandleren altid skal udpege en databeskyttelsesrådgiver, når a) behandling foretages af en offentlig myndighed eller et offentligt organ, undtagen domstole, der handler i deres egenskab af domstol, b) den dataansvarliges eller databehandlerens kerneaktiviteter består af behandlingsaktiviteter, der i medfør af deres karakter, omfang og/eller formål kræver regelmæssig og systematisk overvågning af registrerede i stort omfang, eller c) den dataansvarliges eller databehandlerens kerneaktiviteter består af behandling i stort omfang af særlige kategorier af oplysninger, jf. artikel 9, og oplysninger vedrørende straffedomme og straffelovsovertrædelser, jf. artikel 10.

6.1.5. Særligt om det finansielle område

6.1.5.1. Generelt

Som nævnt under punkt 2.2.2 og 2.4.2 ovenfor er finansielle virksomheder, der håndterer fortrolige betalingsdata, alle underlagt regulering med krav til virksomhedernes indretning og kontrolsystemer og et løbende tilsyn. Der er over de seneste 6-7 år sket en række opstramninger af reglerne på området, og den finansielle lovgivning komplementerer samtidig de almindelige regler om beskyttelse af personoplysninger i persondataloven.

Herudover har Nets som beskrevet under punkt 4 taget en række initiativer til at styrke datasikkerheden i forlængelse af Se og Hør-sagen. Disse forbedringstiltag vurderes, såfremt de bliver tilstrækkeligt implementeret og forankrede, fremadrettet at kunne styrke Nets' generelle it-sikkerhedsstyring, hvor der i forbindelse med Finanstilsynets inspektion blev konstateret væsentlige svagheder på flere områder, jf. punkt 4 ovenfor.

Ydermere har bankernes interesseorganisation, Finansrådet, vedtaget fælles retningslinjer vedrørende beskyttelse af fortrolige kundeoplysninger. Retningslinjerne vedrører henholdsvis 1) håndtering af adgangskontrol og logning for medarbejdere med adgang til fortrolige kundedata samt 2) sikring af medarbejdernes viden om behandling af fortrolige oplysninger, jf. **bilag 8**.

For så vidt angår adgangskontrol lægges der med retningslinjerne op til, at der skal være et arbejdsbetinget behov for at kunne opnå adgang til fortrolige kundeoplysninger, og at der bør være en risikovurdering forbundet hermed samt en løbende vurdering af, om de oprindelige kriterier for at tildele rettighed fortsat er aktuelle. Derudover lægges op til, at der bør ske en logning af anvendelsen af adgangen til kundeoplysninger for at kunne dokumentere, hvem der har foretaget opslag, registreringer og transaktioner, og på hvilke kunder.

For så vidt angår medarbejdernes viden om behandling af fortrolige oplysninger lægges der med retningslinjerne op til, at medarbejdere og eksterne konsulenter bør underskrive en tavshedserklæring, inden de får adgang til fortrolige oplysninger og i denne forbindelse oplyses om gældende regler på området og konsekvenserne ved overtrædelse. Derudover lægges op til, at der skal ske en løbende indsats for at styrke relevante medarbejderes viden. Finansrådet vil ét år efter vedtagelse af retninglinjerne følge op på disse awareness-indsatser.

Arbejdsgruppen anerkender sektorens indførelse af fælles retningslinjer og vurderer, at disse vil kunne højne sektorens fokus på behovet for løbende at styrke og udbygge god it-adfærd og vil kunne sikre, at branchen selv tager ansvar for kontinuerligt at følge de højeste standarder for it-sikkerhed.

Set i lyset af ovenstående har arbejdsgruppen ikke umiddelbart identificeret områder, hvor der er et åbenbart behov for at foretage nye gennemgribende reguleringsmæssige tiltag over for finansielle virksomheder. Det vurderes dog, at der med fordel kan foretages visse præciseringer af den gældende lovgivning på udvalgte områder.

6.1.5.2. Præcisering af krav til indretning og kontrol af it-systemer

Som beskrevet under punkt 2.2.2.1 ovenfor indeholder lovgivningen i dag generelle regler i forhold til finansielle virksomheders ledelse og styring, herunder i forhold til indretning, kontrol og styring af it-systemer. I dag er reglerne i bekendtgørelsen om ledelse og styring af pengeinstitutter m.fl. relativt generelt formuleret, og Finanstilsynet kan konstatere, at der i virksomhederne i dag ofte er vide muligheder for at tildele rettigheder og adgang til data mv. og for svage kontroller og risikostyring, hvilket også er illustreret af Se og Hør-sagen, jf. bl.a. Finanstilsynets redegørelse på baggrund af inspektionen hos Nets (bilag 6).

Arbejdsgruppen har overvejet, om der er behov for yderligere at præcisere bekendtgørelsens krav til indretning, styring og kontrol af it-systemer med særlig fokus på rettighedstildelinger og kontroller, således at det bliver klarere for virksomhederne, hvad der anses for at være en hensigtsmæssig eller tilstrækkelig praksis på disse områder. Der

kan dermed opnås et større fokus i virksomhederne på netop de områder, hvor Finanstilsynet har konstateret, at der ofte kan være udfordringer.

En yderligere præcisering af bekendtgørelsens krav forventes ikke i sig selv at medføre øgede administrative byrder for virksomhederne, da ændringen blot vil tydeliggøre for virksomhederne, hvilke krav der allerede gælder i dag.

Arbejdsgruppen foreslår på den baggrund en yderligere præcisering af bekendtgørelsens krav til indretning, styring og kontrol af it-systemer med særlig fokus på rettighedstildelinger og kontroller.

En præcisering kan bl.a. omfatte Finanstilsynets forventninger til virksomhedens overblik over kombinationer af rettigheder, der tilsammen kan omgå den organisatoriske funktionsadskillelse, logning af rettighedstildeling og rettighedsanvendelse, nulstilling af kodeord, nødbrugeradgange, særlig kontrol af tildelte rettigheder, når ansatte skifter arbejdsområde internt i virksomheden samt leverandørers og konsulenters adgange til systemer og rettigheder i disse.

6.2. Behov for skærpelse af straffen for overtrædelse af persondataloven og anden relevant lovgivning?

6.2.1. Strafferammen for overtrædelse af persondataloven er bøde eller fængsel indtil fire måneder, jf. punkt 2.5.1.2 ovenfor. Som det fremgår af punkt 2.5.1.2.1 ovenfor, har man i retspraksis lagt sig fast på et relativt beskedent niveau hvad angår den straf, der udmåles for overtrædelse af relevante regler i persondataloven, der sædvanlig lyder på en bøde på 5.000 kr., men dog har varieret fra 3.000 til 15.000 kr.

Overtrædelse af bestemmelsen om tavshedspligt i § 117 i lov om finansiel virksomhed kan ligeledes straffes med bøde eller fængsel indtil fire måneder. Som nævnt under punkt 2.5.2.1 ovenfor er der indtil videre vedtaget én bøde på 25.000 kr. for overtrædelse af bestemmelsen.

Virksomheder, som ikke efterlever et påbud fra Finanstilsynet givet efter lov om finansiel virksomhed om f.eks. at styrke it-sikkerheden straffes med bøde, jf. ligeledes punkt 2.5.2.1 ovenfor.

Manglende efterlevelse af et påbud fra Finanstilsynet givet efter betalingstjenesteloven om f.eks. at indføre konkrete sikkerhedsprocedurer kan ligeledes straffes med bøde, jf. punkt 2.5.2.2 ovenfor.

Betalingsinstitutter, der overtræder betalingstjenestelovens § 85 er straffes som nævnt under punkt 2.5.2.2 ovenfor med bøde.

6.2.2. Det er arbejdsgruppens opfattelse, at strafferammen for overtrædelse af de omtalte regler om beskyttelse af oplysninger om borgernes elektroniske betalinger mv. må anses for passende.

Det strafniveau, man i praksis har lagt sig fast på for overtrædelse af persondatalovens regler, er imidlertid relativt beskedent. Muligheden for at idømme fængselsstraf for overtrædelse af persondatalovens regler ses i øvrigt aldrig at være udnyttet.

Arbejdsgruppen har på den baggrund overvejet, om der er behov for at skærpe straffen for overtrædelse af persondataloven.

Det er arbejdsgruppens opfattelse, at straffen for overtrædelse af persondatalovens regler bør afspejle disse lovovertrædelsers grovhed og indgribende betydning for de personer, oplysningerne vedrører. Der er således tale om krænkelser af privatlivets fred i form af misbrug af personoplysninger, som bl.a. kan have betydning for de omhandlede personers velfærd og omdømme.

Hertil kommer, at sådan, som vores samfund er indrettet i dag, er der i vidt omfang behov for, at store mængder personoplysninger, herunder følsomme personoplysninger, kan tilgås af ansatte hos virksomheder og myndigheder. Denne adgang til personoplysninger må naturligvis ske under den forudsætning, at oplysningerne behandles med den fornødne omhu og ikke misbruges. Det styrker efter arbejdsgruppens opfattelse behovet for, at de sanktioner, som kan være forbundet med manglende efterlevelse af reglerne, i tilstrækkelig grad motiverer til efterlevelse af reglerne.

Arbejdsgruppen finder på den baggrund, at der er behov for en skærpelse af bødestraffen for overtrædelse af persondataloven.

Den nærmere fastlæggelse af bødeniveauet må efter arbejdsgruppens opfattelse bero på en række overvejelser, herunder om lovovertrædelsens karakter og grovhed, de misbrugte oplysningers karakter og mængde samt lovovertrædelsens betydning for de(n) berørte person(er).

I den nye databeskyttelsesforordning indgår der imidlertid bestemmelser om, at de nationale tilsynsmyndigheder skal have mulighed for at udstede administrative bøder, og om størrelsen af disse bøder, jf. forordningens artikel 83. Det taler efter arbejdsgruppens

opfattelse imod, at bødeniveauet for overtrædelse af persondataloven ændres på nuværende tidspunkt.

Der opereres i forordningen med et bødeniveau på op til 20.000.000 euro eller 4 % af årlig global omsætning. En ordning med *administrative* bøder giver anledning til grundlovsmæssige betænkeligheder for Danmark, idet en sådan ordning vil indebære et brud med det grundlæggende princip om, at straf alene kan idømmes af domstolene. Der er på den baggrund i forordningens artikel 83, stk. 9, tilføjet en bestemmelse, som giver mulighed for at implementere bestemmelserne om administrative bøder i det nationale *strafferetlige* system. De bøder, som fastlægges i det strafferetlige system, skal dog have en virkning, som svarer til virkningen af de administrative bøder, og skal være effektive, proportionale og afskrækkende.

6.2.3. Arbejdsgruppen har overvejet, om der er behov for skærpede sanktioner ved overtrædelser af den finansielle lovgivning.

Arbejdsgruppen bemærker hertil, at der har været nedsat et udvalg i regi af Erhvervs- og Vækstministeriet, der netop har set på sanktionsniveauet på det finansielle område. Udvalget afsluttede sit arbejde i [juni] 2016. Udvalget har vurderet, at der er behov for en skærpelse af bødeniveauet for overtrædelse af lov om finansiel virksomhed og anbefaler i sin betænkning, at der fremadrettet skal kunne tildeles bøder til virksomheder på op til 50 millioner kroner og til fysiske personer på op til 2 gange en månedsløn. Udvalget vurderer, at der herved skabes en bedre sammenhæng mellem strafudmålingen og dels grovheden af overtrædelsen, dels størrelsen af den finansielle virksomhed, der har begået overtrædelsen.

Der er tale om en væsentlig forhøjelse af bødeniveauet, der som nævnt ovenfor, i dag ligger på omkring 25.000 – 30.000 kroner for virksomheder for en førstegangsovertrædelse.

Erhvervs- og vækstministeren har annonceret, at der vil blive fremsat det nødvendige lovforslag til gennemførsel af udvalgets anbefalinger i næste folketingssamling.

6.3. Behov for styrkelse af tilsynsbeføjelser og reaktionsmuligheder for tilsynsmyndigheder?

De myndigheder, som fører tilsyn med overholdelsen af reglerne om, hvordan personoplysninger, herunder oplysninger om, hvor betalere har anvendt deres betalingsinstrument, skal beskyttes mod uvedkommendes adgang mv., har som beskrevet under punkt 2.4 ovenfor en række beføjelser og reaktionsmuligheder.

Datatilsynet har således bl.a. mulighed for at kræve oplysninger af betydning for dets virksomhed, at få adgang til lokaler uden retskendelse og at meddele forbud og påbud til private dataansvarlige, herunder om iværksættelse af bestemte sikkerhedsforanstaltninger. Hertil kommer, at Datatilsynet i sager, hvor der er begået en strafbar overtrædelse af persondataloven, har mulighed for at foretage politianmeldelse.

Finanstilsynet har bl.a. mulighed for at kræve oplysninger af betydning for dets virksomhed, at få adgang til lokaler uden retskendelse, at påtale forhold, at meddele påbud og at anvende såkaldte risikooplysninger. Hertil kommer, at Finanstilsynet i sager, hvor der er begået en strafbar overtrædelse af lov om finansiel virksomhed, har mulighed for at foretage politianmeldelse.

Forbrugerombudsmanden har bl.a. mulighed for at kræve oplysninger af betydning for ombudsmandens virksomhed, udstede påbud samt anlægge sag om forbud, påbud og erstatning, ligesom ombudsmanden kan udpeges som grupperepræsentant i et gruppesøgsmål.

På sundhedsområdet er der mulighed for at klage til Styrelsen for Patientsikkerhed, Sundhedsvæsenets Disciplinærnævn og Sundhedsdatastyrelsen over manglende overholdelse af reglerne på området. Disse myndigheder vil bl.a. kunne udtale kritik og foretage politianmeldelse i tilfælde af, at lovgivningen på området ikke overholdes.

Efter arbejdsgruppens opfattelse vil de tilfælde af misbrug, som afsløringerne om Se og Hørs overvågning har afdækket, næppe kunne være undgået ved, at de myndigheder, som fører tilsyn med overholdelsen af reglerne på området, havde haft yderligere tilsynsbeføjelser og reaktionsmuligheder. Det er således arbejdsgruppens opfattelse, at muligheden for at afdække misbrug af personoplysninger, som begås af enkeltpersoner i det skjulte, næppe vil blive nævneværdigt forøget ved, at tilsynsmyndighederne tildeles flere beføjelser og reaktionsmuligheder. Arbejdsgruppen henviser herved til, at sådanne beføjelser og reaktionsmuligheder i højere grad må antages at hjælpe til at *afdække* misbrug af personoplysninger og i mindre grad til at *forebygge* sådan misbrug.

Hertil kommer, at det i lyset af, at den nye databeskyttelsesforordning, må anses for uhensigtsmæssigt at fastsætte nye regler om tilsynsbeføjelser og reaktionsmuligheder på nuværende tidspunkt.

Det er på den baggrund arbejdsgruppens opfattelse, at der ikke er behov for eller i øvrigt bør foretages en styrkelse af tilsynsbeføjelser og reaktionsmuligheder for tilsynsmyndighederne på området på nuværende tidspunkt.

6.4. Behov for ændring af grænsedragningen mellem tilsynsmyndighedernes kompetencer?

Beskyttelsen af persondata er i dag omfattet af regler i flere forskellige love (bl.a. persondataloven, lov om finansiel virksomhed og lov om betalingstjenester) og under tilsyn af flere myndigheder (bl.a. Datatilsynet, Finanstilsynet og Forbrugerombudsmanden). Det er ikke i alle tilfælde en klar afgræsning mellem myndighedernes kompetencer. Samtidig findes der i dag ikke et formaliseret samarbejde mellem de tre myndigheder, og koordinering og håndteringen af klager sker således på ad hoc-basis.

Arbejdsgruppen har noteret sig, at lov om betalingstjenester og elektroniske penge vil skulle revideres som følge af vedtagelsen af det reviderede betalingstjenestedirektiv i EU.

Arbejdsgruppen anbefaler, at det – i forbindelse med den forestående revision af lov om betalingstjenester og tilpasningen af dansk lovgivning som følge af den nye databeskyttelsesforordning – overvejes, hvordan man bedst fastlægger et klart og entydigt tilsyn på hele det finansielle område og sikre en klar grænsedragning mellem de relevante myndigheders kompetencer.

Spørgsmålet om ændring af grænsedragningen mellem tilsynsmyndighedernes kompetencer kan i øvrigt efter arbejdsgruppens opfattelse passende indgå som et element i den under punkt 5 ovenfor omtalte samlede strategi til sikring af danskernes personoplysninger.

6.5. Behov for øvrige ændringer?

6.5.1. Indberetningspligt for finansielle virksomheder i forbindelse med videregivelse af oplysninger

I foråret 2014 solgte de danske banker Nets til ATP og to amerikanske kapitalfonde. I den forbindelse blev der fra politisk side fremført en del bekymringer, bl.a. hvorvidt Nets som følge af den amerikanske lovgivning, som de to amerikanske kapitalfonde er underlagt, potentielt kan blive tvunget til at udlevere persondata om danske statsborgere til de amerikanske myndigheder.

I forhold til dansk lovgivning vil en videregivelse af oplysninger fra virksomheder, der er etableret i Danmark, til udenlandske myndigheder skulle ske inden for rammerne af persondataloven. Persondataloven sondrer mellem videregivelse af personoplysninger inden for EU og videregivelse af personoplysninger til tredjelande (fx USA). Der stilles efter loven strengere krav til den sidstnævnte. Dette kan ske, enten hvis der er tale om et tredjeland, som sikrer et "tilstrækkeligt beskyttelsesniveau", eller – hvis dette ikke er tilfældet – i en række nærmere angivne tilfælde, jf. persondatalovens § 27, stk. 3, eller

hvis Datatilsynets tilladelse til overførslen foreligger. Det bemærkes, at der i 2012 er foretaget en ændring af persondataloven, hvorved det er gjort muligt uden tilladelse fra Datatilsynet at overføre personoplysninger til tredjelande på grundlag af kontrakter, der er i overensstemmelse med standardkontraktbestemmelser, som er godkendt af Kommissionen.

Det kan imidlertid ikke afvises, at udenlandsk ejede virksomheder etableret i Danmark vil kunne stå i et dilemma imellem overholdelsen af lovgivning i landet, hvor moderselskabet er etableret, og persondataloven. F.eks. kan man forestille sig en situation, hvor en virksomhed efter amerikansk lov vil være forpligtet til at udlevere oplysninger til de amerikanske myndigheder, men hvor en sådan udlevering samtidig vil være i strid med persondataloven.

For at imødegå problemstillingen om, at udenlandsk ejede virksomheder kan blive klemt imellem dansk lovgivning og et andet lands lovgivning (f.eks. amerikansk), har arbejdsgruppen overvejet at etablere en hjemmel, der pålægger dansk etablerede (men udenlandsk ejede) finansielle virksomheder, betalingsinstitutter samt fællesejede datacentraler at indberette til Finanstilsynet, såfremt udenlandske myndigheder pålægger virksomheden, f.eks. fordi den er datterselskab til en udenlandsk virksomhed, at udlevere personoplysninger til den udenlandske myndighed. Gældende dansk lovgivning indeholder ikke hjemmel til, at Finanstilsynet kan kræve, at virksomhederne informerer Finanstilsynet herom.

Formålet med at skabe hjemmel til en sådan indberetningspligt vil være at give de danske myndigheder viden om tilfælde, hvor danske virksomheder anmodes om at videregive personoplysninger til udenlandske myndigheder.

En sådan lovbestemt indberetningspligt må ske med respekt for forbuddet mod selvinkriminering, som følger af retssikkerhedslovens § 10. Forbuddet mod selvinkriminering indebærer, at virksomheder ikke vil have pligt til at oplyse om en konkret videregivelse af oplysninger til udenlandske myndigheder, hvis der er mistanke om, at virksomheden har begået en (strafsanktioneret) lovovertrædelse.

Selve den omstændighed, at en virksomhed etableret i Danmark er blevet anmodet om at udlevere oplysninger til en udenlandsk myndighed, vil imidlertid formentlig sjældent i sig selv indebære, at der foreligger en konkret mistanke om, at den pågældende virksomhed har begået en (strafsanktioneret) lovovertrædelse. Et eventuelt krav om, at virksomhederne skal oplyse til de danske myndigheder, såfremt de er blevet anmodet om at udlevere oplysninger til en udenlandsk myndighed, vurderes på den baggrund at kunne etableres uden generelt at indebære selvinkriminering.

Det bemærkes dog, at de eksisterende regler om udlevering af data til tredjelande er fastlagt ud fra nøje overvejelser om behovet for at give myndighederne indseende i forhold til behandling af personoplysninger, herunder overførsler af personoplysninger i et tredjeland. Det er derfor uklart, hvor effektiv en sådan indberetningspligt til Finanstilsynet vil være.

Der er således usikkerhed omkring effektiviteten af at indføre indberetningspligten. Dette bør undersøges nærmere. Arbejdsgruppen anbefaler derfor, at regeringen som opfølgning på rapporten undersøger fordele og ulemper ved at etablere en indberetningspligt for dansk etablerede (men udenlandsk ejede) finansielle virksomheder, betalingsinstitutter samt fællesejede datacentraler om at indberette til Finanstilsynet, såfremt udenlandske myndigheder pålægger virksomheden at udlevere personoplysninger.

6.5.2. Øget bevilling til Datatilsynet

Arbejdsgruppen har noteret sig, at justitsministeren i forbindelse med 1. behandlingen den 17. maj 2016 af beslutningsforslag B 148 om datasikkerhed oplyste, at regeringen lægger op til at styrke Datatilsynet i 2016 og med ca. 2 mio. kr. årligt fra 2017 og frem, hvilket svarer til en bevillingsforøgelse på ca. 10 %. Justitsministeren oplyste derudover, at spørgsmålet om tilsynets ressourcer løbende vil blive overvejet i forbindelse med arbejdet med databeskyttelsesforordningen.

6.5.3. Øget bevilling til Finanstilsynet

Finanstilsynet har i dag 3 it-inspektør stillinger til it-tilsynet med alle finansielle virksomheder. På denne baggrund udføres der for tiden 7-8 planlagte it-inspektioner årligt af finansielle virksomheder mv. Tillige udføres mange forskelligartede ad hoc-opgaver eksempelvis i forbindelse med tilladelser og internationalt arbejde.

Arbejdsgruppen har overvejet, om der er behov for at styrke Finanstilsynets tilsyn med it-sikkerhed. De tilførte årsværk kan blandt andet anvendes til både hyppigere inspektioner af virksomheder, som er væsentlige for den finansielle it-sikkerhed, samt flere gennemførte it-inspektioner om året generelt. Idet it-området er et stadig mere betydningsfuldt område i konstant forandring, vil tilførsel af ekstra årsværk også bidrage til det voksende arbejde med at opdatere og yderligere udfolde de nuværende regler mv.

På den baggrund anbefaler arbejdsgruppen at styrke Finanstilsynets tilsyn med it-sikkerhed med 1-2 årsværk.

7. Bilag

En liste over rapportens bilag følger her:

- Bilag 1: Datatilsynets krav og anbefalinger i forbindelse med overførsel af personoplysninger via internettet i den private sektor.

- Bilag 2: Datatilsynets standardvilkår vedr. private forskningsprojekter, privathospitaler mv.

- Bilag 3: Datatilsynets høringssvar af 7. april 2004 vedr. Strukturkommissionens betænkning (Datatilsynets j.nr. 2004-122-0103).

- Bilag 4: Datatilsynets udtalelse af 28. juni 2001 til Holstebro Kommune vedr. videregivelse af personoplysninger fra et kommunalt register til en avis (Datatilsynets j.nr. 2000-632-0002).

- Bilag 5: Nets' redegørelse fra oktober 2014 til arbejdsgruppen.

- Bilag 6: Finanstilsynets redegørelse om it-inspektionen i Nets.

- Bilag 7: Nets' opdaterede redegørelse fra marts 2016 til arbejdsgruppen.

- Bilag 8: Finansrådets fælles retningslinjer vedrørende beskyttelse af fortrolige kundeoplysninger.