

Dansk persondataret



BENT OLE GRAM MORTENSEN (RED.)

Dansk persondataret

ExTuto
PUBLISHING
www.extuto.com

Bent Ole Gram Mortensen (red.), Carina Risvig Hamer, Daniel Hartfield-Traun, Lisa Hjerrild, Kent Kristensen, Jesper Kruse Markvart, Helene Arensbak Mørk, Jesper Løffler Nielsen, Ayo Næsborg-Andersen, Sten Schaumburg-Müller, Christian Højer Schjøler, Peter Starup, Jøren Ullits & Frederik Waage

Dansk persondataret

Første udgave, første oplag

Denne bog er udgivet i januar 2020 af EX TUTO PUBLISHING A/S. Grafisk tilrettelæggelse og sats af MERE.INFO A/S, som har anvendt LibreOffice/Linux samt skrifterne Baskerville Original og Cronos designet af henholdsvis FRANTIŠEK ŠTORM i 2000 og ROBERT SLIMBACH i 1996. JAN TRZASKOWSKI har stået for forlagsredaktion og TOVE MØGELVANG-HANSEN har været ansvarlig for korrekturlæsning. Bogen er trykt på Munken Pure 100 g/m² af NARAYANA PRESS, der ligger på Gyllingnæs syd for Odder. Indbindingen er udført af BUCHBINDEREI S.R. BÜGE GMBH i Celle. Bogen er fagfællebedømt.

Ex Tuto A/S er medlem af Forening for Boghaandværk, og vi støtter bæredygtig skovforvaltning ved at anvende FSC-certificeret papir.

Copyright © 2020 the editor and the authors

Printed in Denmark 2020

ISBN 978-87-420-0033-5

Ex Tuto Publishing A/S

Toldbodgade 55, 1.

DK-1253 København K

www.extuto.com



Udgivet med støtte fra

dreyersfond

Kapitelloversigt

DEL I: GENERELLE SPØRGSMÅL	1
1. Fra registerlov til databeskyttelsesforordning <i>Bent Ole Gram Mortensen</i>	3
2. Den centrale lovgivning på databeskyttelsesområdet <i>Peter Starup</i>	19
3. Hvornår er der tale om en personoplysning, og hvornår er det behandling af en sådan? <i>Sten Schaumburg-Müller</i>	29
4. Nærmere om persondatarettens dækning <i>Sten Schaumburg-Müller</i>	41
5. De overordnede principper for databehandling <i>Ayo Næsborg-Andersen</i>	55
6. Oplysningskategorier og behandlingsbetingelser <i>Sten Schaumburg-Müller</i>	75
7. Ytrings- og informationsfrihed <i>Sten Schaumburg-Müller</i>	117
8. Personbilleder <i>Sten Schaumburg-Müller</i>	127
9. Ansvarlighed og dokumentation <i>Jesper Løffler Nielsen & Helene Arensbak Mørk</i>	169
10. Ansvarssubjekter og aftaleregulering <i>Jesper Løffler Nielsen & Helene Arensbak Mørk</i>	177

11. Databeskyttelsesrådgiveren	191
<i>Lisa Hjerrild</i>	
12. Krav om konsekvensanalyse	203
<i>Lisa Hjerrild</i>	
13. De registreredes rettigheder	213
<i>Jøren Ullits, Ayo Næsborg-Andersen & Kent Kristensen</i>	
14. Sikkerhed og håndtering af databrud	229
<i>Daniel Hartfield-Traun</i>	
15. Tredjelandsoverførsler	255
<i>Jesper Løffler Nielsen & Helene Arensbak Mørk</i>	
16. Tilsynsmyndigheder og sanktioner	269
<i>Carina Risvig Hamer</i>	
DEL II: UDVALGTE RETSOMRÅDER	281
17. Persondatarettens anvendelse på forskningsprojekter	283
<i>Kent Kristensen & Jøren Ullits</i>	
18. Statistik	301
<i>Ayo Næsborg-Andersen</i>	
19. Behandlingen af personoplysninger ved domstolene	309
<i>Frederik Waage</i>	
20. Persondatabehandling i journalistisk øjemed	321
<i>Jøren Ullits & Sten Schaumburg-Müller</i>	
21. Kunstnerisk, litterær og akademisk virksomhed	343
<i>Sten Schaumburg-Müller</i>	
22. Markedsføring og personoplysninger	349
<i>Bent Ole Gram Mortensen</i>	
23. Forsyningsvirksomheder	367
<i>Bent Ole Gram Mortensen & Lisa Hjerrild</i>	
24. Geodata	377
<i>Lisa Hjerrild</i>	

25. Konkurrenceret	385
<i>Peter Starup & Jesper Kruse Markvart</i>	
26. Sundhedslovens behandlingsregler	429
<i>Kent Kristensen & Jøren Ullits</i>	
27. Forvaltningens samkøring af borgerdata	443
<i>Jøren Ullits</i>	
28. HR og persondataret	453
<i>Christian Højer Schjøler</i>	
Bibliografi	481
Stikordsregister	495

Tilsynsmyndigheder og sanktioner

Carina Risvig Hamer

16.1. Indledning

En væsentlig årsag til, at regler overholdes, er ofte risikoen for sanktioner. Ved risikoen for f.eks. straf og bøder vil man ofte være mere omhyggelig med at sikre, at regler overholdes for derved at undgå sanktioner. I den juridiske sprogbrug taler vi om, at der skal være en effektiv håndhævelse af regler. I den forbindelse er det vigtigt, at sanktionerne har en tilstrækkeligt afskrækkende effekt, og at der reelt er en nærliggende risiko for, at de kommer i spil.

I databeskyttelsesretten blev der med databeskyttelsesforordningen (GDPR) indført mulighed for at udstede store bøder af en størrelsesorden på op til 20 mio. euro eller 4 % af den globale omsætning. Et beløb der var med til at åbne øjnene for de nye regler, særligt i lyset af, at størrelsen på bøder for overtrædelse af den daværende persondatalov lå på under 10.000 kr. Overholdelse af databeskyttelsesreglerne har dermed fået større fokus i lyset af de strengere sanktionsmuligheder, og generelt er fokus omkring håndhævelse af reglerne blevet øget. Bødens størrelse var i sig selv en af årsagerne til den store opmærksomhed, reglerne i forordningen fik ved indførelse i maj 2018, men også

muligheden for fængselsstraf er en skærpelse af sanktionsmulighederne.

Det fremgår af Charterets artikel 8, at overholdelse af reglerne om beskyttelse af personoplysninger er underlagt en uafhængig myndigheds kontrol. I Danmark er det Datatilsynet, der fører tilsyn med, at reglerne overholdes,¹ og udover muligheden for bøder kan Datatilsynet bl.a. også udstede påbud. Datatilsynet kan dog ikke selv udstede administrative bøder eller pålægge straf, hvorfor der er tale om en særlig proces, når bøder og straf kommer i spil (se herom nedenfor afsnit 16.5.1.2).

Dette kapitel ser først nærmere på Datatilsynets rolle (afsnit 16.2). Dernæst behandles tilsynet med databeskyttelsesreglerne (afsnit 16.3). Afsnit 16.4 behandler Datatilsynets samarbejde med andre datatilsyn og endeligt ses der nærmere på de mulige sanktioner for overtrædelse af databeskyttelsesreglerne (afsnit 16.5).

16.2. Datatilsynets rolle

Datatilsynet fører tilsyn med, at myndigheder, virksomheder og andre dataansvarlige og databehandlere overholder databeskyttelsesreglerne. Reglerne om Datatilsynets opgaver og kompetencer findes i databeskyttelseslovens kapitel V (§§ 27-36). Datatilsynet er en uafhængig myndighed, der kan træffe afgørelser om, hvorvidt databeskyttelsesreglerne er overholdt. Ud over funktionen som tilsynsmyndighed varetager Datatilsynet også en række andre opgaver som f.eks. at kommentere på lovgivning,² give tilladelser til visse typer af behandling, udar-

-
1. Dog er det Domstolsstyrelsen, der fører tilsyn med behandling af oplysninger, der foretages for domstolene, når disse ikke handler i deres egenskab af domstol, jf. databeskyttelseslovens § 37.
 2. Jf. Databeskyttelseslovens § 28. Datatilsynet behandler årligt ca. 4-500 høringer over udkast til lovforslag, bekendtgørelser og andre generelle forskrifter. Når omfanget af materialet er meget stort, anmoder Datatilsynet den hørende myndighed om at pege på de dele af udkastet, som angår databeskyttelsesretlige forhold. Det betyder, at der kan være forhold, der ikke bliver bemærket, hvilket var tilfældet ved en lov på beskæftigelsesområdet i 2019, der medførte, at Datatilsynet så på sagen på ny. Se herom pressemeddelelsen om sagen <<https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/maj/datatilsynet-ser-paa-beskaeftigelseslov-igen/>> (besøgt maj 2019).

bejde vejledninger, og tilsynet svarer derudover på et stort antal henvendelser om reglerne både skriftligt og telefonisk.

Datatilsynet består af et råd og et sekretariat, der ledes af en direktør. Datarådet er nedsat af justitsministeren og består af 8 personer: en formand og 7 andre medlemmer (p.t. består Datarådet af 2 kvinder og 6 mænd). Datarådet træffer primært afgørelser i konkrete sager af principiel karakter. Det er formanden for rådet, der i samarbejde med sekretariatet forbereder sagernes forelæggelse for rådet og leder rådets møder.

Det er muligt at indgive en klage til Datatilsynet over behandlingen af personoplysninger.³ De fleste af Datatilsynets afgørelser kan findes på tilsynets hjemmeside.⁴ Datatilsynets afgørelser kan ikke indbringes for anden administrativ myndighed, men afgørelserne kan indbringes for domstolene.⁵ Herudover er tilsynets virksomhed undergivet Folketingets Ombudsmands kompetence.

Dataansvarlige skal anmelde brud på persondatasikkerheden til Datatilsynet (se herom i kapitel 10). Anmeldelsen skal ske uden unødigt forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet. Det er vigtigt, at man lærer af sine fejl, og derfor er det vigtigt, at der sker anmeldelse til Datatilsynet, så der kan rettes op på det. Af samme årsag vil manglende anmeldelse blive straffet hårdere. I 2018 behandlede Datatilsynet 2.722 sager om brud på persondatasikkerheden.⁶

Endeligt kan det bemærkes, at Datatilsynet skal udarbejde en årlig rapport jf. forordningen artikel 59.⁷

16.3. Tilsyn med overholdes af databeskyttelsesreglerne

En tilsynsmyndighed fører som nævnt tilsyn med, at regler overholdes. I Danmark er det Datatilsynet, der fører tilsyn med, at databeskyttelses-

3. Se herom Datatilsynets hjemmeside: <<https://www.datatilsynet.dk/generelt-om-databeskyttelse/klage-til-datatilsynet/>> (besøgt maj 2019).

4. Afgørelserne kan findes på <<https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/>> (besøgt maj 2019).

5. Jf. databeskyttelseslovens § 30, stk. 1 samt lovens § 39, stk. 2.

6. Jf. Datatilsynet 2018, s. 11.

7. Ibid.

reglerne overholdes. Datatilsynet udfører både planlagte tilsyn og ad hoc tilsyn.

Angående de planlagte tilsyn udarbejder Datatilsynet årligt en oversigt over kommende tilsyn og hvilke emner, der vil være genstand for tilsyn. I første halvår af 2019 var følgende temaer i fokus:

- Brud på persondatasikkerheden hos offentlige myndigheder og private virksomheder
- Databeskyttelsesrådgiverfunktionen hos kommunerne
- Kryptering af e-mails hos private virksomheder
- Autorisation af medarbejdere hos kommunerne
- Den registreredes indsigtsret hos offentlige myndigheder og private virksomheder
- Brug (og genbrug) af data i den kommunale forvaltning
- Aggregering og sammenstilling af data til brug for videresalg hos private virksomheder⁸

Ad hoc tilsyn vil oftest være sager, som tilsynet selv bliver opmærksomme på eller får tip om udefra, og hvor forholdet er så alvorligt, at Datatilsynet finder det nødvendigt at gribe ind.

Når Datatilsynet fører tilsyn, kan tilsynet, jf. databeskyttelseslovens § 29 kræve “[...] enhver oplysning, der er af betydning for dets virksomhed, herunder til afgørelse af, om et forhold falder ind under databeskyttelsesforordningens og lovens bestemmelser.” Ofte vil Datatilsynet fremsende spørgeskemaer, som skal besvares inden for en given frist, men Datatilsynet har også mulighed for – uden retskendelse – at få adgang til lokaler (herunder måske særligt computere), hvorfra en behandling af personoplysninger foretages, jf. databeskyttelseslovens § 29, stk. 2. Ofte vil spørgeskemaer blive suppleret af et fysisk besøg fra tilsynet.

Når Datatilsynet er på fysisk besøg, finder reglerne i retssikkerhedsloven anvendelse i forbindelse med Datatilsynets tilsyn.⁹ Det

8. Datatilsynet 2019d.

9. Se særligt retssikkerhedslovens §§ 9 og 10. En vejledning om reglerne kan findes på <https://www.retsinformation.dk/Forms/R0710.aspx?id=1959> (besøgt maj 2019).

betyder, at hvis der foreligger en konkret mistanke om et strafbart forhold, skal Datatilsynet oplyse om muligheden for ikke at udtale sig. Uanset, at der er tale om oplysninger, der efter retssikkerhedsloven ikke er pligt til at afgive, kan den pågældende, jf. retssikkerhedslovens § 10, stk. 3, 2. pkt., meddele samtykke til, at oplysninger indhentes/afgives. Et samtykke skal gives på skriftligt, frivilligt, specifikt og informeret grundlag og kan til enhver tid tilbagekaldes.

16.4. Samarbejde med EU tilsynsmyndigheder i andre medlemsstater

Datatilsynet er medlem af Det Europæiske Databeskyttelsesråd (tidligere Artikel 29-Gruppen).¹⁰ Rådet består af repræsentanter for medlemsstaternes tilsynsmyndigheder og kan i visse sager træffe afgørelser, der er bindende for medlemsstaterne. Hvert lands tilsynsmyndighed har 1 stemme, og afgørelser træffes efter simpelt flertal. Et lille land som Danmark har således lige så stor indflydelse på samarbejdet som et større EU-land.¹¹ Også EU-Kommissionen deltager i samarbejdet uden dog at have stemmeret, men har bl.a. mulighed for at fremsætte anmodninger. Af GDPR artikel 70 fremgår en længere liste af opgaver for Databeskyttelsesrådet, herunder bl.a. at føre tilsyn, udarbejde retningslinjer og vejledningsvirksomhed samt rådgivning af Kommissionen.

Et af formålene med et samlet europæisk råd er at sikre, at der sker en ensartet praksis på området i de forskellige medlemsstater.¹² Dette er ikke helt uproblematisk set i lyset af, at selv om der er tale om en forordning, er reglerne ikke fuldt ud identiske i alle medlemsstater. Der vil således være tilfælde, hvor et forhold er tilladt i en medlemsstat, mens det ikke er tilladt i andre. En sammenhængsmekanisme fremgår

10. Databeskyttelseslovens § 27, stk. 9, angiver "Datatilsynet repræsenterer tilsynsmyndighederne i Det Europæiske Databeskyttelsesråd i overensstemmelse med databeskyttelsesforordningens kapitel VII, afdeling 1 og 2." Om Det Europæiske Databeskyttelsesråds rolle og funktioner se også Blume 2018a, s. 202-204. Se desuden Rådets hjemmeside: <https://edpb.europa.eu/edpb_en> (besøgt maj 2019).

11. Det danske Datatilsyn deltager også i et nordisk samarbejdet, hvor de senest har vedtaget *Stockholm-erklæring*, se nærmere på Datatilsynets hjemmeside.

12. Artikel 60-62 fastsætter den nærmere fremgangsmåde for samarbejdet mellem tilsynene.

af forordningens artikel 63, der angiver “Med henblik på at bidrage til en ensartet anvendelse af denne forordning i hele Unionen samarbejder tilsynsmyndighederne med hinanden og, hvis det er relevant, med Kommissionen gennem den sammenhængsmekanisme, der er omhandlet i denne afdeling.”

Tilsyn med grænseoverskridende behandlingsaktiviteter, der involverer statsborgere fra mere end et EU-land, ledes af én tilsynsmyndighed alene. Dette kaldes for *one-stop-shop princippet*. Som udgangspunkt er den tilsynsmyndighed, hvor den pågældende organisation har sit hovedkontor, den ledende tilsynsvirksomhed.¹³ Datatilsynet kan videregive oplysninger til tilsynsmyndigheder i andre medlemsstater i det omfang, det er nødvendigt for at påse overholdelsen af databeskyttelsesreglerne, jf. lovens § 32, stk. 2.

16.5. Ansvar og sanktioner

Effektivitetsprincippet¹⁴ kræver, at medlemsstaternes regler ikke er udformet på en sådan måde, at det i praksis er umuligt eller forholdsvis vanskeligt at udøve de rettigheder, der følger af EU-retten, og at håndhævelsen af EU-reglerne således sikrer en effektiv beskyttelse af de EU-retlige rettigheder. Princippet sikrer dermed en effektiv beskyttelse af de rettigheder, der følger af databeskyttelsesreglerne, samt en effektiv håndhævelse heraf. En vigtig brik i den effektive håndhævelse er forordningens tiltag om større bøder. Hvorvidt regler efterleves, afhænger ofte af, om håndhævelsen af reglerne er effektiv. For at sikre en stærk og sammenhængende databeskyttelsesramme i EU er det vigtigt, at det understøttes af en effektiv håndhævelse.¹⁵

Historisk set har der været forskellige beskyttelsesniveauer i EU (direktivet gav muligheder for særskilt implementering), men med for-

13. Hovedreglen er ikke uden undtagelser, se herom Artikel 29-Gruppen WP 244 rev.01.

14. Det EU-retlige effektivitetsprincip kan udledes af artikel 4 TEU, hvorefter medlemsstaterne ikke må modarbejde virkeliggørelsen af Unionens formål sammenholdt med artikel 19 TEU, hvorefter medlemsstaterne “[...] tilvejebringer den nødvendige adgang til domstolsprøvelse for at sikre en effektiv retsbeskyttelse på de områder, der er omfattet af EU-retten [...]”. Princippet er yderligere udviklet og anerkendt af EU-Domstolen som et af EU-rettens generelle principper.

15. Se forordningens præambel nr. 7.

ordningen skete der en samlet harmonisering (ensretning), således at beskyttelsesniveauet er ens i medlemsstaterne. I forordningens artikel 83, stk. 4-6, følger en detaljeret EU-regulering af, hvilke handlinger og undladelser der skal være strafbare.

Udover udstedelse af bøder (se herom afsnit 16.5.1) kan også fængselsstraf (afsnit 16.5.2) og erstatning (afsnit 16.5.3) komme i spil.

16.5.1. Bøder

16.5.1.1. Bødestørrelsen

Niveauet af bødestørrelsen fremgår direkte af forordningen. Det betyder, at den enkelte medlemsstat ikke kan vælge at fastsætte et lavere eller højere bødeniveau. Bøder skal være effektive, stå i rimeligt forhold til overtrædelserne og have afskrækkende virkning. Bødestørrelsen afhænger af, hvilke regler der er overtrådt. De væsentligste overtrædelser af databeskyttelsesreglerne kan straffes med bøder op til 20.000.000 EUR eller op til 4 % af en virksomheds samlede globale årlige omsætning i det foregående regnskabsår, såfremt dette beløb er højere end de 20.000.000 EUR, jf. artikel 83, stk. 5. Det drejer sig bl.a. om overtrædelser af de grundlæggende principper for behandling af persondata, herunder betingelserne for samtykke, eller hvis en registrets rettigheder, jf. artikel 12-22 ikke er overholdt.¹⁶

Andre overtrædelser af databeskyttelsesreglerne kan straffes med bøder op til 10.000.000 EUR eller op til 2 % af en virksomheds samlede globale årlige omsætning i det foregående regnskabsår, såfremt dette beløb er højere end de 10.000.000 EUR, jf. artikel 83, stk. 4.

16. Artikel 83, stk. 5, lister følgende overtrædelser, der kan føre til, at det højeste bødeniveau skal anvendes "(a) de grundlæggende principper for behandling, herunder betingelserne for samtykke, i artikel 5, 6, 7 og 9, (b) de registreredes rettigheder i henhold til artikel 12-22, (c), overførsel af personoplysninger til en modtager i et tredjeland eller en international organisation i henhold til artikel 44-49, (d) eventuelle forpligtigelser i medfør af medlemsstaternes nationale ret vedtaget i henhold til kapitel IX, (e) manglende overholdelse af et påbud eller en midlertidig eller definitiv begrænsning af behandling eller tilsynsmyndighedens suspension af overførsel af oplysninger i henhold til artikel 58, stk. 2, eller manglende adgang i strid med artikel 58, stk. 1."

Denne type overtrædelser vedrører bl.a. den dataansvarliges og databehandlerens forpligtelser i henhold til artikel 8, 11, 25-39 og 42 og 43.¹⁷

I Danmark har man valgt at indføre et lavere bødeniveau for det offentlige. Det er et generelt princip, at staten, regioner og kommuner alene kan straffes for overtrædelser, der begås ved udøvelse af virksomhed, der svarer til eller kan sidestilles med virksomhed udøvet af private, jf. straffelovens § 27, stk. 2. Af de almindelige bemærkninger til lovforslaget (L68) sektion 2.8.3.8 fremgår: “For overtrædelser omfattet af forordningens artikel 83, stk. 5 og 6 (lovforslagets § 41, stk. 1, nr. 4-6, og stk. 2, nr. 2-5, samt nr. 1 for så vidt angår §§ 5-13, 20 og 21), forudsættes et bødeloft på 4 % af driftsbevillingen, dog maksimalt 16 mio. kroner.” Det offentlige kan altså max pålægges en bøde på 16 mio. kroner. Oprindeligt var det ikke tanken, at det skulle være muligt for det offentlige at blive pålagt bøder, og af høringsudkastet fremgik bl.a., at “[stillingtagen til sanktions-spørgsmålet i forhold til offentlige myndigheder udestår]”, hvilket resulterede i en større debat omkring spørgsmålet af bøder. Et af argumenterne for ikke at pålægge det offentlige bøder er bl.a. konstruktionen om, at det offentlige er alle, og at bøder blot indbetales af det offentlige selv.¹⁸ Ikke desto mindre er der skabt et (næsten) lige system mellem overtrædelser af det offentlige med overtrædelser foretaget af det private.

Uanset, at der kan pålægges ganske store bøder, er der også elementer, der kan pege i retningen af, at en mindre bøde skal anvendes. Således vil overholdelse af princippet om ansvarlighed bl.a. kunne være med til at reducere bødens størrelse. Andre elementer, der kan indgå i vurdering, fremgår bl.a. af præambelbetragtning 148, der angiver “Der bør dog tages behørigt hensyn til overtrædelsens karakter, alvor og varighed, overtrædelsens eventuelle forsætlige karakter, foranstaltninger, der er truffet for at begrænse den forvoldte skade, graden af ansvar eller eventuelle relevante tidligere overtrædelser, måden, hvorpå tilsynsmyndigheden fik kendskab til overtrædelsen, overholdelse af for-

17. Artikel 83, stk. 4, lister følgende overtrædelser, der kan føre til at det lavere bødeniveau skal anvendes: “(a) den dataansvarliges og databehandlerens forpligtelser i henhold til artikel 8, 11, 25-39 og 42 og 43; (b) certificeringsorganets forpligtelser i henhold til artikel 42 og 43; (c) kontrolorganets forpligtelser i henhold til artikel 41, stk. 4.”

18. Se bl.a. Mortensen 2017.

anstaltninger truffet over for den dataansvarlige eller databehandleren, overholdelse af en adfærdskodeks samt andre skærpene eller formildende faktorer.”

Ved visse mindre overtrædelser, eller hvis den bøde, der kunne blive pålagt, ville udgøre en uforholdsmæssigt stor byrde for en fysisk person, kan der udstedes en irrettesættelse i stedet for en bøde (præambelbetragtning 148).

Vi mangler fortsat praksis på bødestørrelserne. Datatilsynet har politianmeldt Taxa 4x35 og indstillet selskabet til en bøde på 1,2 mio. kr. for en overtrædelse af reglerne i databeskyttelsesforordningen.¹⁹ Sagen omhandler det forhold, at Taxa 4x35 ikke slettede kundernes telefonnumre efter 2 år, men alene kundernes navne. Det betød, at det var muligt at hente oplysninger om kundernes taxature (herunder opsamlings- og afleveringsadresser), og disse oplysninger kunne henføres til en fysisk person via telefonnummeret, som først blev slettet efter fem år. Datatilsynet har vurderet, at “[...] man imidlertid ikke [kan] fastsætte en slettefrist, som er tre år længere end nødvendigt, blot fordi virksomhedens system gør det besværligt at efterleve reglerne i databeskyttelsesforordningen.” Derfor indstillede Datatilsynet til en bøde i sagen og lagde i den forbindelse særligt vægt på, at der var tale om meget store mængder personoplysninger, der er blevet gemt uden et sagligt formål. I en anden sag har Datatilsynet politianmeldt ID design NS og indstillet virksomheden til en bøde på 1,5 mio. kr. for manglende sletning af oplysninger.²⁰

16.5.1.2. Processen for tildeling af bøder

Ifølge forordningen er det administrative bøder, der skal anvendes ved overtrædelser af reglerne. Af forordningens præambelbetragtning 148 fremgår i den forbindelse, at “pålægelse af sanktioner, herunder administrative bøder, bør være omfattet af fornødne proceduremæssige garantier i overensstemmelse med de generelle principper i EU-retten og chartret, herunder effektiv retsbeskyttelse og en retfærdig procedure.” Med andre ord skal det være muligt for den, der bliver pålagt en bøde, at blive hørt og sikre, at proceduren er retfærdig. I Danmark

19. Se Datatilsynet 2019b.

20. Se nyhed fra Datatilsynet fra 11. juni 2019.

betyder det, at bøder ikke hører til i det administrative system (dvs. ved forvaltningen), men i stedet hører til hos domstolene. I Lovforslaget afsnit 2.8.3.6 fremgår “Indførelsen af administrative bøder giver i dansk ret betænkeligheder i forhold til grundloven. I dansk retspleje er det et grundlæggende princip, at bøder, der har karakter af strafferetlig sanktion, kun kan idømmes ved domstolene og i strafferetsplejens former, der sikrer den sigtede en effektiv beskyttelse. Datatilsynet bør dermed ikke få beføjelse til at fastsætte administrative bøder, som har karakter af en strafferetlig sanktion, men er henvist til at indgive politianmeldelse, såfremt tilsynet konstaterer overtrædelser af persondataloven. Datatilsynet kan dog få mulighed for at udstede bødeforelæg i egnede sager, jf. herom afsnit 2.8.3.9.”

I de fleste europæiske lande kan de nationale datatilsyn selv udstede administrative bøder, men reglerne er anderledes i Estland og Danmark.²¹ I Danmark kan Datatilsynet ikke pålægge bøder direkte, men det er overladt til domstolene. Datatilsynet har dog fået tillagt mulighed for at udstede et bødeforlæg, som virksomhederne så kan vælge at acceptere. Accepteres bødeforlægget ikke, skal sagen for domstolene. Denne mulighed er dog ikke aktuel endnu, da domstolene først skal have fastlagt bødeniveauet for overtrædelserne. Det fremgår af loven, at i de tilfælde, hvor det skønnes, at overtrædelse af databeskyttelsesreglerne ikke kan føre til højere straf end bøde, kan Datatilsynet, jf. § 42, stk. 1, “[...] i et bødeforelæg tilkendegive, at sagen kan afgøres uden retssag, hvis den, der har begået overtrædelserne, erklærer sig skyldig i overtrædelserne og erklærer sig rede til [...], at betale en i bødeforelægget angivet bøde.” Betales bøden, bortfalder videre forfølgning jf. § 42, stk. 3.

21. At det er muligt at unnlade administrative bøder, fremgår af artikel 83, stk. 9, “Hvis en medlemsstats retssystem ikke giver mulighed for at pålægge administrative bøder, kan denne artikel anvendes på en sådan måde, at den kompetente tilsynsmyndighed tager skridt til bøder, og de kompetente nationale domstole pålægger dem, idet det sikres, at disse retsmidler er effektive, og at deres virkning svarer til virkningen af administrative bøder, som pålægges af tilsynsmyndighederne. Bøder skal under alle omstændigheder være effektive, stå i rimeligt forhold til overtrædelserne og have afskrækkende virkning. De pågældende medlemsstater giver Kommissionen meddelelse om bestemmelserne i deres love, som de vedtager i henhold til dette stykke, senest den 25. maj 2018 og underretter den straks om alle senere ændringslove eller ændringer, der berører dem.”

Af lovforslaget afsnit 2.8.3.7. fremgår baggrunden, nemlig: “Med denne fremgangsmåde finder Justitsministeriet, at Datatilsynet som forudsat i forordningen har mulighed for at tage skridt til idømmelse af bøder ved, at tilsynet på grundlag af de konstaterede overtrædelser af forordningens bestemmelser overvejer, hvorvidt der kan idømmes bøde og i så fald dennes størrelse. Såfremt Datatilsynet i en konkret sag vurderer, at der kan idømmes en bøde for de pågældende overtrædelser, indgiver tilsynet politianmeldelse sammen med en redegørelse for tilsynsmyndighedens vurdering, herunder niveauet for bøden.”

16.5.2. Fængselsstraf

Udover muligheden for bøde kan overtrædelser af databeskyttelsesreglerne også straffes med fængsel indtil 6 måneder. Af lovforslaget afsnit 2.8.3.7. fremgår “Strafferammen på bøde eller fængsel indtil 6 måneder er inspireret af straffelovens § 264 d om uberettiget videregivelse af meddelelser eller billeder vedrørende en andens private forhold eller i øvrigt billeder af den pågældende under omstændigheder, der åbenbart kan forlanges unddraget offentligheden.” Endvidere fremgår det om behovet for at anvende fængselsstraf, at “Der vil være grundlag for, at straffen stiger til fængsel i tilfælde, hvor der f.eks. sker en forsætlig offentliggørelse af særligt beskyttelsesværdige oplysninger, såsom følsomme oplysninger, i et meget betydeligt omfang.”

16.5.3. Godtgørelse og erstatning

I de tilfælde, hvor der er sket en overtrædelse af databeskyttelsesreglerne, kan der som behandlet ovenfor afsnit 16.5.1 og 16.5.2, pålægges en bøde og endda fængselsstraf. Ofte vil den person, hvis persondata er involveret i den uretmæssige behandling af personoplysningerne, ikke have nogen særlig interesse i, at der pålægges en bøde. I disse tilfælde vil den pågældende ikke opnå nogen form for kompensation for overtrædelsen.

Det fremgår af Databeskyttelseslovens § 40, at “Enhver person, som har lidt materiel eller immateriel skade som følge af en ulovlig behandlingsaktivitet eller enhver anden behandling i strid med denne lov og databeskyttelsesforordningen, har ret til erstatning efter databeskyttelsesforordningens artikel 82”. Muligheden for at få erstatning

afhænger af dansk rets almindelige principper om erstatning, hvilket indebærer et krav om, at der skal være sket et økonomisk tab, hvilket i praksis kan være svært at opgøre.

Godtgørelse kan muligvis også søges efter erstatningsansvarslovens § 26 om tort.