Udskriftsdato: 7. januar 2026

CIR1H nr 10140 af 12/08/2022 (Gældende)

Rigsadvokatmeddelelsen, afsnittet: Databeskyttelse - Straffesager

Ministerium: Justitsministeriet	Journalnummer: CMS VB 9324

Rigsadvokatmeddelelsen, afsnittet: Databeskyttelse - Straffesager

1. Overblik og tjekliste

Politiet skal under efterforskningen være særligt opmærksom på:
- I relevant omfang at foretage en indledende bevissikring, se nærmere under pkt. 3.4 og 3.5.
  - Hvor sagen er af kompleks eller hastende karakter, kan der være behov for specifik og/eller hurtig bevissikring, som tilsiger et nærmere samarbejde mellem Datatilsynet og politiet. Se nærmere under pkt. 3.4.3.
- Muligheden for at indhente en foreløbig udtalelse om overtrædelsens strafværdighed fra Datatilsynet, hvis politikredsen efter modtagelsen af en anmeldelse direkte fra en borger eller virksomhed mv. vurderer, at det er uklart, om der foreligger en overtrædelse, der bør undergives strafforfølgning. Se nærmere under pkt. 3.5.1.1.

Anklagemyndigheden skal være særligt opmærksom på:
- At Datatilsynet generelt skal høres i alle sager om **overtrædelse af databeskyttelsesreglerne**, inden der træffes afgørelse om tiltalespørgsmålet. Se nærmere under pkt. 3.5.2.1. Datatilsynet skal endvidere inddrages ved spørgsmålet om eventuel anke og skal orienteres om og have kopi af alle endelige afgørelser. Se nærmere under pkt. 6.1.
- At der gælder særlige retningslinjer for behandlingen af sager om **overtrædelse af databeskyttelsesreglerne** der bl.a. medfører, at
  - politikredsen skal forelægge tiltalespørgsmålet (herunder strafpåstanden) for statsadvokaten i alle sager om overtrædelse af databeskyttelsesreglerne. Se nærmere under pkt. 3.7.
  - sagerne ikke må afgøres med bødeforelæg, før sanktionsniveauet er tilstrækkelig afklaret i retspraksis.
  - sager, hvor anklagemyndigheden ikke har fået medhold i tiltalen og/eller strafpåstanden, skal forelægges for statsadvokaten, inden ankefristens udløb. Se nærmere under pkt. 6.2.
  - endelige domme skal indberettes til Rigsadvokaten, herunder med henblik på optagelse i Vidensbasen. Se nærmere under pkt. 6.3.

- At sager om **overtrædelse af tv-overvågningslovens § 4 c**, skal behandles efter særlige retningslinjer bl.a. med henblik på at sikre, at evt. bødeudmåling i sagerne sker under iagttagelse af bødeniveauet for overtrædelse af databeskyttelsesforordningen og databeskyttelsesloven. Retningslinjerne er nærmere beskrevet under pkt. 3.9., pkt. 6.1. og pkt. 6.2.

  Retningslinjerne indebærer bl.a., at:

  - sagerne – på samme måde som sager om overtrædelse af databeskyttelsesreglerne – skal forelægges for både Datatilsynet og statsadvokaten. Det indebærer bl.a. at Datatilsynet skal høres, inden der træffes afgørelse om tiltalespørgsmålet, og at politikredsen skal forelægge tiltalespørgsmålet (herunder strafpåstanden) for statsadvokaten. Se nærmere under pkt. 3.9.1.

  - sagerne ikke må afgøres med bødeforelæg, før sanktionsniveauet er tilstrækkelig afklaret i retspraksis.

- sager, hvor anklagermyndigheden ikke har fået medhold i tiltalen og/eller strafpåstanden, skal forelægges for statsadvokaten og for Datatilsynet, inden ankefristens udløb. Se nærmere under pkt. 6.1. og pkt. 6.2.

- At sager om **overtrædelser (af f.eks. straffeloven, sundhedsloven eller anden særlovgivning) med databeskyttelsesretlige elementer**, hvori der vil blive nedlagt påstand om bødestraf, skal behandles efter særlige retningslinjer bl.a. med henblik på at sikre, at bødeudmålingen i sagerne i relevant omfang sker under iagttagelse af bødeniveauet for overtrædelse af databeskyttelsesforordningen og databeskyttelsesloven. Retningslinjerne er nærmere beskrevet under pkt. 3.10.

  Retningslinjerne indebærer bl.a., at

  - politikredsen i alle sager skal forelægge tiltalespørgsmålet (herunder bødepåstanden) for statsadvokaten. Se nærmere under pkt. 3.10.4.

  I sager, hvor der vil blive nedlagt påstand om bødestraf udmålt under iagttagelse af bødeniveauet for overtrædelse af databeskyttelsesforordningen og databeskyttelsesloven, indebærer retningslinjerne endvidere, at

  - statsadvokaterne indtil videre skal drøfte bødepåstanden med Datatilsynet i forbindelse med forelæggelsen. Se nærmere under pkt. 3.10.4.

  - sagerne ikke må afgøres med bødeforelæg, før sanktionsniveauet er tilstrækkelig afklaret i retspraksis.

  - sager, hvor anklagemyndigheden ikke har fået medhold i tiltalen og/eller strafpåstanden, skal forelægges for statsadvokaten, inden ankefristens udløb. Se nærmere under pkt. 3.10.4. og pkt. 6.2.

  - det generelle notat om "Overtrædelser af straffeloven og andre særregler med databeskyttelsesretlige elementer", Datatilsynets "Bødevejledning – Udmåling af bøder til fysiske personer" og "Notat om Datatilsynets behandling af sager om såkaldt registermisbrug, mv." skal i relevant omfang bilageres ind på alle sager. Se nærmere under pkt. 3.10.5.

- At **visse sager om overtrædelser med databeskyttelsesretlige elementer kan være undtaget fra retningslinjerne**, hvis der i forarbejderne til loven er angivet et klart udgangspunkt for bødeniveauet, hvilket der bl.a. er i forarbejderne til straffelovens § 264 e om identitetstyveri. Se nærmere under pkt. 3.10.9.

2. Politiets efterforskning og sagsbehandling

Se pkt. 3 om sagsbehandling og forberedelse.

3. Sagsbehandling og forberedelse

3.1. Datatilsynets rolle

Datatilsynet er den centrale uafhængige myndighed, der fører tilsyn med, at reglerne om databeskyttelse bliver overholdt, herunder reglerne i databeskyttelsesforordningen, databeskyttelsesloven, retshåndhævelsesloven og dele af TV-overvågningsloven. Der henvises til Datatilsynets hjemmeside www.datatilsynet.dk.

Borgere mv. kan klage over eller indberette en overtrædelse af de databeskyttelsesretlige regler til Datatilsynet, men kan også vælge at anmelde et forhold direkte til politiet.

Når der klages over eller indberettes en overtrædelse til Datatilsynet, og tilsynet vurderer, at overtrædelsen er af en sådan karakter, at den bør undergives strafforfølgning, kan Datatilsynet indgive en politianmeldelse.

Der henvises til pkt. 3.2., pkt. 3.4. og pkt. 3.5. for nærmere om Datatilsynets bistand i forbindelse med efterforskningen og forberedelsen.

3.2. Bistand under sagsbehandlingen

3.2.1. Kontaktpersoner hos Datatilsynet, Rigspolitiet og Rigsadvokaten

Der er udpeget kontaktpersoner på databeskyttelsesområdet i Datatilsynet, Rigspolitiets Databeskyttelsesenhed og Rigsadvokatens Databeskyttelsesenhed. Kontaktpersonerne kan kontaktes på tværs af de respektive myndigheder med henblik på afklaring af spørgsmål af databeskyttelsesretlig karakter, der kan opstå under sagsbehandlingen, og som ikke kan afklares ved inddragelse af den lokale anklagemyndighed eller i samarbejde med statsadvokaten. Listen over kontaktpersoner findes på anklagemyndighedens Vidensbase.

Rigspolitiets Databeskyttelsesenhed fungerer som kontaktpunkt under sagernes efterforskning.

Rigsadvokatens Databeskyttelsesenhed fungerer som kontaktpunkt, når sagerne er overgivet til anklagemyndigheden.

Datatilsynet sender en kopi af alle tilsynets politianmeldelser vedrørende overtrædelse af databeskyttelsesreglerne til Rigspolitiets Databeskyttelsesenhed og Rigsadvokatens Databeskyttelsesenhed til orientering.

3.2.2. Rigsadvokatens bistand i sager vedr. grænseoverskridende kriminalitet

Sager om overtrædelse af databeskyttelsesreglerne kan – f.eks. når det drejer sig om ulovlig offentliggørelse af personoplysninger på udenlandske hjemmesider eller sociale medier – have international karakter. Som i andre sager om grænseoverskridende kriminalitet kan det derfor være relevant at overveje behovet for international retshjælp. Spørgsmål vedrørende international retshjælp kan rettes til International Enhed hos Rigsadvokaten.

Der henvises til Rigsadvokatmeddelelsens afsnit om International retshjælp og om Indhentelse af elektroniske beviser fra internationale internetserviceudbydere (Facebook, Google mv.).

I de tilfælde, hvor det overvejes at inddrage Datatilsynet, skal det bemærkes, at sager mod virksomheder, der opererer i flere lande, skal håndteres af tilsynsmyndigheden i det EU-land, hvor virksomheden har sit europæiske hovedkontor, jf. forordningens artikel 55.

Der henvises til https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/internationalt-/danmark-eu-og-resten-af-verden/internationale-virksomheder

3.2.3. Bistand fra National enhed for Særlig Kriminalitet (NSK) – Nationalt Cyber Crime Center (NC3)

I konkrete sager kan National enhed for Særlig Kriminalitet (NSK) – Nationalt Cyber Crime Center (NC3) bistå Datatilsynet og politikredsene under efterforskningen, herunder i forbindelse med bevissikring, gennemgang af beslaglagte datamedier mv.

3.3. Særlige retningslinjer

Rigsadvokaten har fastsat særlige retningslinjer for behandlingen af sager om overtrædelse af databeskyttelsesforordningen og databeskyttelsesloven.

Retningslinjerne indebærer blandt andet, at:

- politikredsen skal forelægge tiltalespørgsmålet (herunder strafpåstanden) for statsadvokaten i alle sager om overtrædelse af databeskyttelsesreglerne, se nærmere nedenfor under pkt. 3.4.3 og pkt. 3.7.,
  - sager, hvor politikredsen vurderer, at der kan ske henlæggelse eller påtaleopgivelse efter retsplejelovens §§ 749 eller 721, skal dog ikke forelægges for statsadvokaten, hvis beslutningen herom er i overensstemmelse med udtalelsen fra Datatilsynet, jf. nedenfor pkt. 3.5.1.1, eller hvis der undtagelsesvist ikke har været grundlag for at høre Datatilsynet, jf. nedenfor pkt. 3.5.1.
- sager om overtrædelse af databeskyttelsesreglerne ikke må afgøres med bødeforelæg, før sanktionsniveauet er tilstrækkelig afklaret i retspraksis, og
- politikredsen skal forelægge alle domme, hvor anklagemyndigheden ikke har fået fuldt medhold (herunder i strafpåstanden), for statsadvokaten, inden ankefristens udløb, se nærmere nedenfor pkt. 6.

3.4. Sager, som er anmeldt af Datatilsynet

3.4.1. Datatilsynets politianmeldelse med henblik på tiltalerejsning

Datatilsynet indgiver politianmeldelse med henblik på tiltalerejsning, hvis tilsynet i en konkret sag vurderer, at sagen er fuldt oplyst, og at den pågældende overtrædelse bør undergives strafforfølgning. Politianmeldelsen ledsages af en redegørelse for Datatilsynets vurdering af sagen, herunder bødeniveauet.

Sagsbehandleren hos Datatilsynet står til rådighed for spørgsmål til sagen fra politikredsen.

Hvis anklagemyndigheden er uenig i Datatilsynets vurdering, følges retningslinjerne i Rigsadvokat-meddelelsens afsnit "Samarbejdet med særmyndigheder i særlovssager".

Anklagemyndigheden skal orientere Datatilsynet ved tiltalerejsning.

3.4.1.1. Nye oplysninger i sagen

Hvis der efter politianmeldelsen fremkommer væsentlige nye oplysninger i sagen, f.eks. at sigtede er tidligere straffet af betydning for sagen, som det ikke kan antages, at Datatilsynet var bekendt med på tidspunktet for politianmeldelsen, skal Datatilsynet have lejlighed til at afgive en supplerende udtalelse på baggrund af de nye oplysninger.

3.4.2. Datatilsynets politianmeldelse med anmodning om yderligere efterforskning

Når Datatilsynet indgiver politianmeldelse med henblik på yderligere efterforskning, afventer Datatilsynet politiets afslutning af efterforskningen og anklagemyndighedens forelæggelse af sagen med henblik på Datatilsynets vurdering af tiltalespørgsmålet, herunder en indstilling om sanktionsspørgsmålet, se nærmere pkt. 3.5.2.

3.4.2.1. Datatilsynets politianmeldelse ved sager af særlig kompleks eller hastende karakter

I særlige tilfælde, hvor sagen er af kompleks eller hastende karakter, kan der være behov for mere specifik og/eller hurtig bevissikring, som tilsiger et nærmere samarbejde mellem Datatilsynet og politiet.

Når Datatilsynet har indgivet en politianmeldelse med anmodning om assistance til bevissikring i en kompleks og/eller hastende sag, skal sagsbehandleren hos henholdsvis Datatilsynet og i politikredsen hurtigst muligt herefter indgå i en dialog med henblik på afklaring af sagens videre forløb. Hvis det vurderes relevant, skal en anklager fra den relevante politikreds inddrages i dialogen.

Dialogen skal som udgangspunkt omfatte en drøftelse af:

- Identifikation af eventuelle straffeprocessuelle og/eller databeskyttelsesretlige problemstillinger,
- Sagens videre forløb og
- Bevissikring, herunder rollefordelingen mellem politiet og Datatilsynet.

Dialogen skal initieres af den relevante sagsbehandler i politikredsen. Forinden politiet retter henvendelse til sagsbehandleren i Datatilsynet, skal det være klarlagt, hvorvidt det i den konkrete sag vil være relevant at inddrage en anklager.

3.5. Sager, som ikke er anmeldt af Datatilsynet

3.5.1. Overtrædelser, hvis strafværdighed er tvivlsom

Hvis politikredsen efter modtagelsen af en anmeldelse fra en borger eller virksomhed mv. vurderer, at det er uklart, om der foreligger en overtrædelse, der bør undergives strafforfølgning, skal politikredsen overveje, om der allerede i forbindelse med efterforskningen skal indhentes en foreløbig udtalelse om overtrædelsens strafværdighed fra Datatilsynet, medmindre anmeldelsen på det foreliggende grundlag kan afvises som åbenbart grundløs, jf. retsplejelovens § 749.

3.5.1.1. Datatilsynets foreløbige udtalelse om en overtrædelses strafværdighed

På baggrund af den foreløbige udtalelse fra Datatilsynet kan det afklares, hvorvidt overtrædelsen efter tilsynets opfattelse har en alvor, der tilsiger en strafferetlig behandling af sagen.

Ved eventuelle tvivlsspørgsmål af databeskyttelsesretlig karakter kan Datatilsynets kontaktpersoner kontaktes telefonisk forud for sagens forelæggelse, se nærmere ovenfor pkt. 3.2.1.

3.5.1.1.1. Indhold af forelæggelsen

En sag, der forelægges for Datatilsynet til en foreløbig udtalelse om en overtrædelses strafværdighed, skal som udgangspunkt indeholde mindst følgende oplysninger:

- En beskrivelse af handlingen/undladelsen.
  - Hvis der er tale om en offentliggørelse af personoplysninger på sociale medier, skal der vedlægges oplysninger om den profil, hvorfra offentliggørelsen er sket. Det skal bl.a. oplyses, hvorvidt der er tale om en åben/lukket profil eller gruppe og hvor mange personer, der umiddelbart har/har haft adgang til de pågældende personoplysninger.
- Hvilke personoplysninger der er tale om. Se nærmere om de forskellige typer af personoplysninger under pkt. 4.1.2.
- Angivelse af dato hhv. tidsperiode.
- Evt. angivelse af antallet af berørte registrerede.
- Anmelders forklaring, medmindre sagen er tilstrækkelig oplyst til, at Datatilsynet kan afgive en foreløbig udtalelse om overtrædelsens strafværdighed.

Politikredsen skal i forbindelse med oversendelsen til Datatilsynet anonymisere personoplysninger, som åbenbart ikke er relevante for sagens behandling.

Det bemærkes, at ordningen vedrørende Datatilsynets foreløbige udtalelse om en overtrædelses strafværdighed ikke bør anvendes til at afklare andre spørgsmål omkring efterforskningen mv. Sådanne spørgsmål bør i første omgang søges afklaret i politikredsen, herunder ved inddragelse af den lokale anklagemyndighed, ligesom statsadvokaten kan kontaktes efter behov.

3.5.1.1.2. Hvis Datatilsynet vurderer, at der er tale om et strafværdigt forhold

Hvis Datatilsynet foreløbigt vurderer, at der er tale om et strafværdigt forhold, skal sagen sendes til videre efterforskning i politikredsen. Herefter følges fremgangsmåden som anført under pkt. 3.5.2.

3.5.1.1.3. Hvis Datatilsynet vurderer, at der ikke er tale om et strafværdigt forhold

Hvis Datatilsynet vurderer, at der er tale om et forhold, der af Datatilsynet ville blive afvist eller sanktioneret med tilsynets korrigerende beføjelser efter databeskyttelsesforordningens artikel 58 (f.eks. et påbud), kan politikredsen vurdere spørgsmålet om eventuel henlæggelse eller påtaleopgivelse efter retsplejelovens §§ 749 eller 721.

Ved en eventuel henlæggelse eller påtaleopgivelse skal det overvejes, om henlæggelsen/påtaleopgivelsen, ud over den almindelige klagevejledning efter retsplejeloven, skal ledsages af en vejledning om, at

borgeren mv. har mulighed for at klage over en behandling af sine personoplysninger til Datatilsynet, jf. den generelle vejledningspligt efter forvaltningslovens § 7.

3.5.2. Utvivlsomt strafværdige overtrædelser

Når politikredsen modtager en anmeldelse fra en borger eller virksomhed mv., og det må lægges til grund, at der er tale om en overtrædelse af en sådan karakter, at den bør undergives strafforfølgning, skal politiet foretage den nødvendige og tilstrækkelige efterforskning i sagen, f.eks. ved indhentelse af nærmere oplysninger om de faktiske forhold, afhøringer mv.

Ved eventuelle tvivlsspørgsmål af databeskyttelsesretlig karakter, der opstår under efterforskningen og/ eller sagsbehandlingen af utvivlsomt strafværdige overtrædelser, kan politikredsen som udgangspunkt kontakte Rigspolitiets Databeskyttelsesenhed for nærmere vejledning. Se nærmere om kontaktpersoner ovenfor pkt. 3.2.1.

3.5.2.1. Forelæggelse for Datatilsynet

Datatilsynet skal høres, inden der træffes afgørelse om tiltalespørgsmålet. Høringssvaret fra Datatilsynet skal tillægges vægt ved vurderingen af sagen. Det fremgår af forarbejderne til databeskyttelsesloven (L 68 af 25. oktober 2017, de alm. bemærkninger pkt. 2.8.3.7).

Udtalelsen fra Datatilsynet vil, ligesom i sager som anmeldes af Datatilsynet, jf. pkt. 3.4, indeholde tilsynets vurdering af tiltalespørgsmålet, herunder en indstilling om sanktionsspørgsmålet. Datatilsynets udtalelse om sanktionsspørgsmålet omfatter også – i det omfang det er muligt – en redegørelse om sanktionsniveauet i andre EU-medlemslande.

3.5.2.1.1. Indhold af forelæggelsen

En sag, der forelægges for Datatilsynet, skal som udgangspunkt indeholde mindst følgende oplysninger:

- Beskrivelse af handlingen/undladelsen.
  - Hvis der er tale om en offentliggørelse af personoplysninger på sociale medier, skal der vedlægges oplysninger om den profil, hvorfra offentliggørelsen er sket. Det skal bl.a. oplyses, hvorvidt der er tale om en åben/lukket profil eller gruppe, og hvor mange personer der umiddelbart har/har haft adgang til de pågældende personoplysninger.
- Hvilke personoplysninger der er tale om. Se nærmere om de forskellige typer af personoplysninger under pkt. 4.1.2.
- Angivelse af dato hhv. tidsperiode.
- Evt. angivelse af antallet af berørte registrerede.
- Dokumentation for den pågældende behandling af personoplysninger.
  - Hvis der er tale om omfattende materiale, skal der så vidt muligt henvises til det konkrete forhold i materialet ved angivelse af sidetal mv.
- Anmelders og anmeldtes forklaring.

Anklagemyndigheden skal være opmærksom på, om den sigtede er tidligere straffet af betydning for sagen. Hvis den sigtede tidligere er straffet af betydning for sagen, skal det oplyses til Datatilsynet i det omfang, det må antages at have betydning for Datatilsynets vurdering af sanktionsspørgsmålet.

Anklagemyndigheden skal i forbindelse med oversendelsen anonymisere personoplysninger, som åbenbart ikke er relevante for sagens behandling.

3.6. Overtrædelser, som anmeldes til begge myndigheder

Hvis det fremgår, at en anmeldelse/henvendelse både er sendt til Datatilsynet og til politiet, skal politikredsen som udgangspunkt afvente Datatilsynets afgørelse. Politikredsen kan i den forbindelse kontakte Datatilsynet og gøre tilsynet opmærksom herpå.

Når Datatilsynet har truffet afgørelse, skal politikredsen viderebehandle sagen i overensstemmelse med retningslinjerne i dette afsnit af Rigsadvokatmeddelelsen.

3.7. Forelæggelse for statsadvokaturen

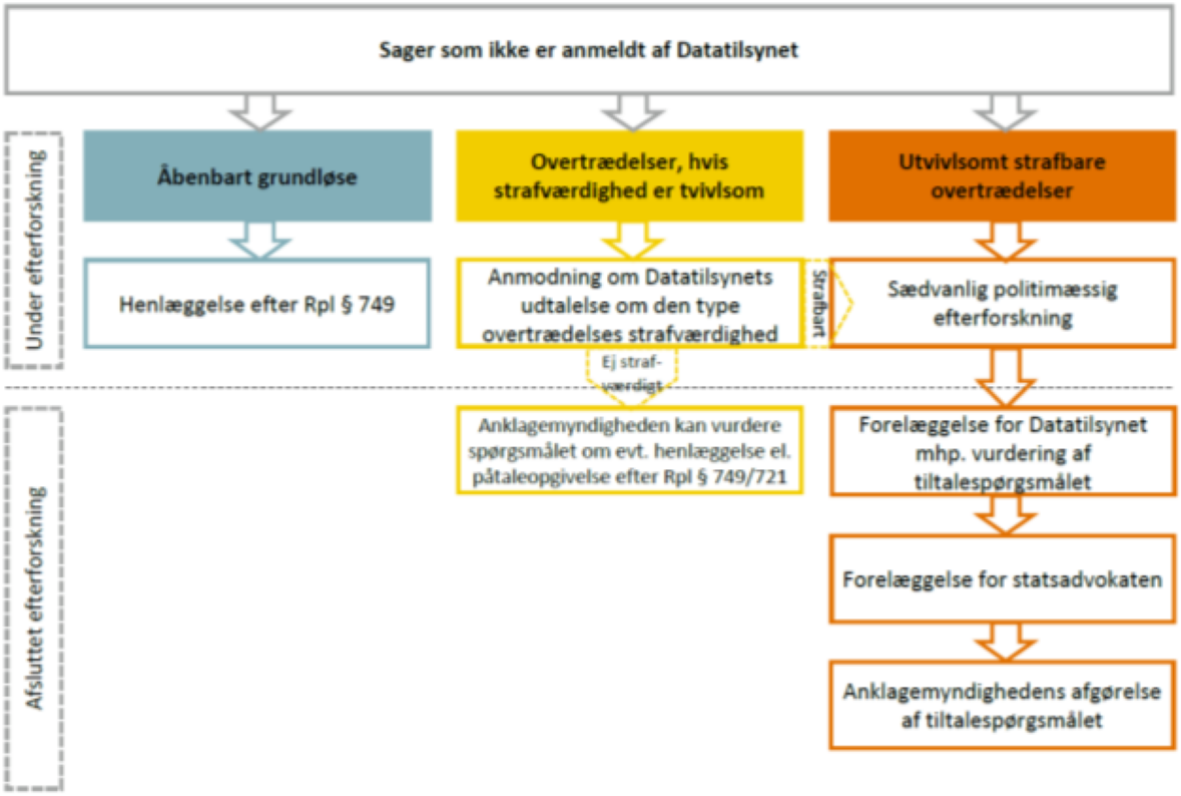
Politikredsen skal forelægge tiltalespørgsmålet (herunder strafpåstanden) for statsadvokaten i alle sager om overtrædelse af de databeskyttelsesretlige regler.

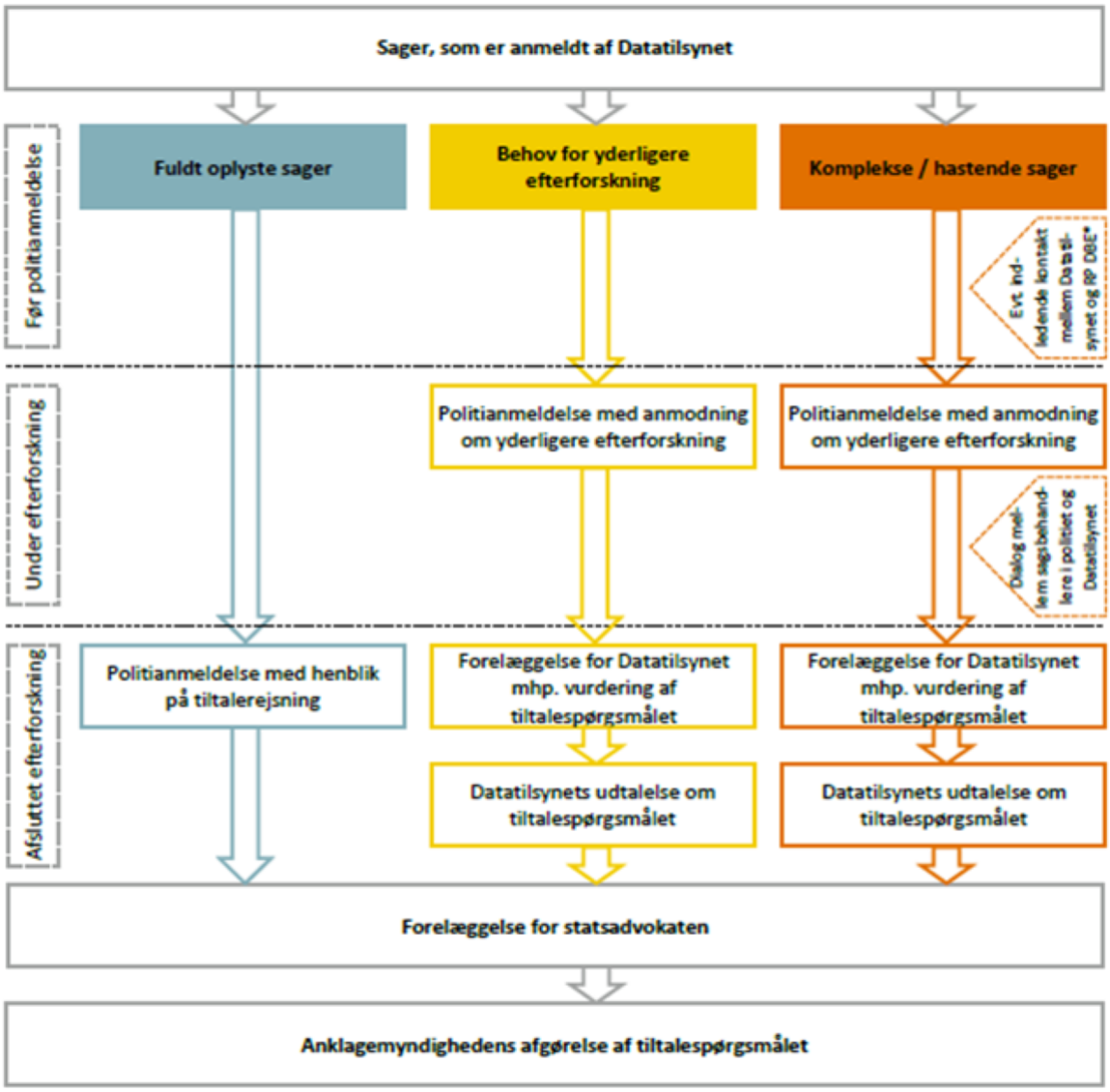
Sager, hvor politikredsen vurderer, at der kan ske henlæggelse eller påtaleopgivelse efter retsplejelovens §§ 749 eller 721 skal dog ikke forelægges for statsadvokaten, hvis beslutningen herom er i overensstemmelse med den foreløbige udtalelse fra Datatilsynet, jf. ovenfor pkt. 3.5.1.1., eller hvis der undtagelsesvist ikke har været grundlag for at høre Datatilsynet, jf. ovenfor pkt. 3.5.1.

Forud for forelæggelsen for statsadvokaten skal politikredsen høre Datatilsynet, inden der træffes afgørelse om tiltalespørgsmålet, jf. ovenfor pkt. 3.5.2.1. I tilfælde af uenighed mellem anklagemyndigheden og Datatilsynet følges retningslinjerne i Rigsadvokatmeddelelsens afsnit om Samarbejdet med særmyndigheder i særlovssager.

Anklagemyndigheden skal orientere Datatilsynet ved tiltalerejsning.

3.8. Oversigt over sagsgangen i sager om overtrædelse af de databeskyttelsesretlige regler





* Rigspolitiets Databeskyttelsesenhed

3.9. Særligt om sagsbehandling og forberedelse af sager om overtrædelse af tv-overvågningslovens § 4 c

Som følge af de nye regler i databeskyttelsesforordningen og databeskyttelsesloven blev tv-overvågningsloven ændret den 23. maj 2018. Formålet med lovændringen var bl.a. at videreføre den tidligere gældende persondatalovs §§ 26 a og 26 d om behandling af personoplysninger i forbindelse med tv-overvågning. For en nærmere gennemgang af de mest relevante regler i tv-overvågningsloven henvises til pkt. 4.4. nedenfor.

3.9.1. Forelæggelse for Datatilsynet og statsadvokaterne

Datatilsynet fører tilsyn med enhver behandling af personoplysninger omfattet af tv-overvågningslovens §§ 4 c og 4 d, jf. lovens § 4 e.

Det fremgår af lovforslagets (lovforslag nr. 205 af 21. marts 2018 om ændring af lov om tv-overvågning og lov om retshåndhævende myndigheders behandling af personoplysninger) specielle bemærkninger til §

4 e, at der med § 4 e er sket en videreførelse af den indtil da gældende retstilstand, hvorefter Datatilsynet førte tilsyn med behandling af personoplysninger omfattet af reglerne i persondatalovens §§ 26 a og 26 d. Med lovændringen skal Datatilsynet således fortsat føre tilsyn med overholdelsen af reglerne om behandling af personoplysninger i forbindelse med tv-overvågning i kriminalitetsforebyggende øjemed. Efter bestemmelsen har Datatilsynet kompetence i relation til enhver behandling af personoplysninger, som omfattes af lovens § 4 c.

Sager om overtrædelse af tv-overvågningslovens § 4 c skal på den baggrund, på samme måde som sager om overtrædelse af databeskyttelsesreglerne, behandles efter retningslinjerne om forelæggelse for både Datatilsynet og statsadvokaten, der fremgår af pkt. 3.5.2.1. og pkt. 3.7. ovenfor.

Det indebærer bl.a.:

- at Datatilsynet skal høres, inden der træffes afgørelse om tiltalespørgsmålet,
- at tilsynets udtalelse bl.a. vil indeholde en udtalelse om sanktionsniveauet, og
- at tiltalespørgsmålet (herunder strafpåstanden) skal forelægges for statsadvokaten.

Sager, hvor anklagermyndigheden ikke har fået medhold i tiltalen og/eller strafpåstanden, skal forelægges for statsadvokaten og for Datatilsynet, inden ankefristens udløb. Se nærmere under pkt. 6.1. og 6.2.

Datatilsynet er ikke tilsynsmyndighed i forhold til de øvrige bestemmelser i tv-overvågningsloven.

3.9.2. Særligt om tiltalerejsning

I sager om den dataansvarliges overtrædelse af tv-overvågningslovens § 4 c skal der ved tiltalerejsning som udgangspunkt alene henvises til tv-overvågningslovens regler og ikke tillige reglerne i databeskyttelsesforordningen eller databeskyttelsesloven.

Sagerne må ikke afgøres med bødeforelæg, før bødeniveauet er tilstrækkelig afklaret i retspraksis.

3.10. Særligt om sagsbehandling og forberedelse af sager om overtrædelser med databeskyttelsesretlige elementer

Alle sager om overtrædelser med databeskyttelsesretlige elementer, dvs. overtrædelser, hvor gerningsindholdet også falder inden for forordningens og databeskyttelseslovens anvendelsesområde, hvori der vil blive nedlagt påstand om bødestraf, skal behandles i overensstemmelse med indeværende retningslinjer med henblik på at sikre, at bødeudmålingen i relevant omfang sker under iagttagelse af bødeniveauet for overtrædelser af databeskyttelsesforordningen og databeskyttelsesloven. For en nærmere gennemgang af begrebet "overtrædelser med databeskyttelsesretlige elementer" og baggrunden for de særlige retningslinjer, som trådte i kraft den 27. september 2021, henvises til pkt. 4.5. nedenfor.

3.10.1. Afgrænsning af relevante overtrædelser, herunder i straffeloven og sundhedsloven

Straffeloven indeholder en række bestemmelser med databeskyttelsesretlige elementer, dvs. bestemmelser, hvor gerningsindholdet ofte også vil være omfattet af databeskyttelsesreglerne. Som eksempel på sådanne bestemmelser kan nævnes straffelovens §§ 152-152f om tavshedspligt, § 155 om stillingsmisbrug (typisk i form af registermisbrug), § 232 om blufærdighedskrænkelse, § 263, stk. 1, nr. 3, om aflytning og lydoptagelser, "hackerbestemmelsen" i § 263, stk. 1, § 264 a om uberettiget billedoptagelse af personer, § 264 d om uberettiget videregivelse af billeder mv. og § 264 e om identitetsmisbrug.

Derudover indeholder sundhedsloven en række bestemmelser med databeskyttelsesretlige elementer. Som eksempel på sådanne bestemmelser i sundhedsloven kan nævnes reglerne om tavshedspligt i § 40, reglerne om videregivelse af helbredsoplysninger i § 41, § 43 og § 45 samt reglerne om indsamling af oplysninger, herunder ved registeropslag, i § 42 a, § 42 d og § 46.

Datatilsynet har i samarbejde med Rigsadvokaten udarbejdet et generelt notat, hvori der dels redegøres for, hvornår de databeskyttelsesretlige regler finder anvendelse, dels opremses eksempler på situationer, der både vil udgøre en overtrædelse af straffeloven mv. og af de databeskyttelsesretlige regler. Notatet findes på Vidensbasen og er desuden beskrevet nærmere under pkt. 3.10.5. Notatet skal – som beskrevet under pkt. 3.10.5. – bilageres ind i alle sager om overtrædelser med databeskyttelsesretlige elementer, hvori der vil blive nedlagt påstand om bødestraf udmålt under iagttagelse af bødeniveauet for overtrædelse af databeskyttelsesforordningen og databeskyttelsesloven.

Det bemærkes, at ovennævnte eksempler på overtrædelser med databeskyttelsesretlige elementer – og gennemgangen i det generelle notat – ikke er udtømmende.

3.10.2. Samspillet mellem overtrædelser med databeskyttelsesretlige elementer og de databeskyttelsesretlige regler - tiltalerejsning

Det er Rigsadvokatens opfattelse, at der i sager om handlinger (eller undladelser), der udgør en overtrædelse af både straffeloven og de databeskyttelsesretlige regler, som udgangspunkt alene skal rejses tiltale efter straffeloven, medmindre der er tvivl om bevisvurderingen og/eller forsætsgraden i forhold til straffelovsovertrædelsen. Tilsvarende må antages at gælde for andre overtrædelser med databeskyttelsesretlige elementer (f.eks. i sundhedsloven). Dette er i overensstemmelse med almindelige strafferetlige principper om absorption mv., ligesom det også kan siges at følge af databeskyttelseslovens § 1, stk. 3, hvorefter særregler om behandling af personoplysninger går forud for reglerne i databeskyttelsesloven.

Hvis der imidlertid er tvivl om, hvorvidt der kan ske domfældelse efter straffeloven eller speciallovgivning som f.eks. sundhedsloven (f.eks. fordi det er tvivlsomt, om gerningsindholdet er opfyldt, eller der for så vidt angår straffeloven alene foreligger uagtsomhed), bør der som udgangspunkt rejses en subsidiær tiltale for overtrædelse af de databeskyttelsesretlige regler, hvis det vurderes, at forholdet kan føre til et strafansvar efter disse regler.

Inden sager om overtrædelser med databeskyttelsesretlige elementer eventuelt henlægges eller påtaleopgives, skal det således altid overvejes, om der i stedet er grundlag for at gøre et strafansvar gældende efter de databeskyttelsesretlige regler (f.eks. pga. lavere tilregnelseskrav).

Uanset hvilket regelsæt anklagemyndigheden rejser tiltale efter, skal anklageren være opmærksom på, at overtrædelser med databeskyttelsesretlige elementer vil blive grebet af den længere forældelsesfrist i databeskyttelsesloven, når et forhold indebærer overtrædelse af begge regelsæt. Der henvises i den forbindelse til pkt. 5.1.3.

3.10.3. Inddragelse af Datatilsynet

Inden der rejses (eventuelt subsidiær) tiltale for overtrædelse af de databeskyttelsesretlige regler, skal der altid indhentes en udtalelse fra Datatilsynet, hvori tilsynet bl.a. udtaler sig om sanktionsspørgsmålet. Der

henvises i den forbindelse til pkt. 3.5. for en nærmere gennemgang af forelæggelsesordningen, herunder pkt. 3.5.2.1.1. om indholdet af forelæggelsen.

Sager, der omhandler overtrædelser med databeskyttelsesretlige elementer, hvori der ikke også rejses (principal eller subsidiær) tiltale for overtrædelse af de databeskyttelsesretlige regler, skal derimod ikke forelægges for Datatilsynet. Se dog nærmere om disse sagers behandling nedenfor under pkt. 3.10.4. vedrørende bl.a. inddragelse af statsadvokaterne og pkt. 3.10.5. om notatet om " Overtrædelser af straffeloven og andre særregler med databeskyttelsesretlige elementer", "Bødevejledning - Udmåling af bøder til fysiske personer"" og "Notat om Datatilsynets behandling af sager om såkaldt registermisbrug, mv.".

Inden sager om overtrædelser med databeskyttelsesretlige elementer eventuelt henlægges eller påtaleopgives, skal det altid overvejes, om der i stedet er grundlag for at gøre et strafansvar gældende efter de databeskyttelsesretlige regler (f.eks. pga. lavere tilregnelseskrav).

Sager om overtrædelser med databeskyttelsesretlige elementer kan kun henlægges eller påtaleopgives uden inddragelse af Datatilsynet, hvis sagen ikke kan eller skal rejses efter de databeskyttelsesretlige regler. Hvis der er tvivl om, hvorvidt sagen vil kunne føre til en dom for overtrædelse af de databeskyttelsesretlige regler, skal sagen forelægges for Datatilsynet. Se nærmere herom under pkt. 3.5., herunder pkt. 3.5.1.1. om Datatilsynets foreløbige udtalelse om en overtrædelses strafværdighed.

3.10.4. Inddragelse af statsadvokaten

I alle sager om overtrædelser med databeskyttelsesretlige elementer, hvori der vil blive nedlagt påstand om bødestraf, skal politikredsen forelægge tiltalespørgsmålet (herunder sanktionspåstanden) for statsadvokaten. Se nærmere om overgangsordningen, herunder særligt i forhold til bødeniveauet under pkt. 3.10.6.

I alle sager om overtrædelser med databeskyttelsesretlige elementer, hvori anklagemyndigheden vurderer, at der bør nedlægges påstand om en bøde udmålt under iagttagelse af bødeniveauet for overtrædelser af databeskyttelsesforordningen og databeskyttelsesloven, skal statsadvokaterne i forbindelse med stillingtagen til tiltalespørgsmålet drøfte bødepåstanden med Datatilsynet. Drøftelsen med Datatilsynet er som udgangspunkt ikke en egentlig forelæggelse og kan efter omstændighederne ske telefonisk.

Disse sager må ikke afgøres med bødeforelæg, før bødeniveauet er tilstrækkelig afklaret i retspraksis.

I sager, hvor gerningstidspunktet ligger forud for retningslinjernes ikrafttræden den 27. september 2021, og hvor anklagemyndigheden vurderer, at der bør nedlægges påstand om en bøde udmålt med udgangspunkt i bødeniveauet på tidspunktet for overtrædelsen, skal statsadvokaterne derimod ikke drøfte bødepåstanden med Datatilsynet. Disse sager må endvidere gerne afgøres med bødeforelæg, hvis der i øvrigt er grundlag for det.

Hvis politikredsen påtænker at henlægge eller påtaleopgive en sag, skal det overvejes, om der i stedet er grundlag for at gøre et strafansvar gældende efter de databeskyttelsesretlige regler (f.eks. pga. lavere tilregnelseskrav), jf. ovenfor pkt. 3.10.3.

Sager, hvor anklagemyndigheden har nedlagt påstand om bødestraf udmålt under iagttagelse af bødeniveauet for overtrædelser af databeskyttelsesforordningen og databeskyttelsesloven, men ikke har fået fuldt ud medhold i tiltalen og/eller sanktionspåstanden, skal forelægges for statsadvokaten, inden ankefristens udløb.

3.10.5. Det generelle notat om "Overtrædelser af straffeloven og andre særregler med databeskyttelsesretlige elementer", "Bødevejledning - Udmåling af bøder til fysiske personer" og "Notat om Datatilsynets behandling af sager om såkaldt registermisbrug, mv."

Der er udarbejdet to notater og en vejledning, der har særlig relevans for sager om overtrædelser med databeskyttelsesretlige elementer, hvori der vil blive nedlagt påstand om bødestraf (pkt. 3.10.1.). Det drejer sig om det generelle notat "Overtrædelser af straffeloven og andre særregler med databeskyttelsesretlige elementer", om "Bødevejledning – Udmåling af bøder til fysiske personer" og om "Notat om Datatilsynets behandling af sager om såkaldt registermisbrug, mv.". Dokumenterne skal i relevant omfang bilageres ind på alle sager om overtrædelser med databeskyttelsesretlige elementer, hvori der vil blive nedlagt påstand om bødestraf udmålt under iagttagelse af bødeniveauet for overtrædelser af databeskyttelsesforordningen og databeskyttelsesloven, med henblik på at sikre, at der ved bødeudmålingen tages hensyn til bødeniveauet på det databeskyttelsesretlige område.

Det generelle notat indeholder bl.a. en gennemgang af databeskyttelsesforordningens materielle anvendelsesområde, en gennemgang af de mest centrale begreber og konkrete eksempler på handlinger (eller undladelser), der dels udgør overtrædelser af straffeloven mv., dels udgør overtrædelser af de databeskyttelsesretlige regler. Notatet skal bilageres ind på alle sager om overtrædelser med databeskyttelsesretlige elementer, hvori der vil blive nedlagt påstand om bødestraf udmålt under iagttagelse af bødeniveauet for overtrædelser af databeskyttelsesforordningen og databeskyttelsesloven.

Det er hensigten, at det på baggrund af det generelle notat – og uden indhentelse af en udtalelse fra Datatilsynet i de konkrete sager – skal vurderes, om en given overtrædelse med databeskyttelsesretlige elementer ligeledes er omfattet af de databeskyttelsesretlige regler.

Når det er lagt fast, at en overtrædelse er omfattet af de databeskyttelsesretlige regler, er det endvidere hensigten, at anklagemyndigheden på baggrund af enten "Notat om Datatilsynets behandling af sager om såkaldt registermisbrug, mv." (for så vidt angår sager om registermisbrug) eller Datatilsynets "Bødevejledning - Udmåling af bøder til fysiske personer" (for så vidt angår alle andre sager om overtrædelser med databeskyttelsesretlige elementer end sagerne om registermisbrug) skal kunne fastlægge et bødeniveau for overtrædelsen under iagttagelse af bødeniveauet for overtrædelser af databeskyttelsesforordningen og databeskyttelsesloven. På denne måde skal det sikres, at der ikke udmåles en lavere bøde for overtrædelsen end bødeniveauet for tilsvarende overtrædelser af forordningen, ligesom bødeniveauet for overtrædelsen ikke må overskride grænserne for bødeniveauet i forordningens artikel 83.

Der henvises i den forbindelse til pkt. 3.10.4. om inddragelse af statsadvokaten.

3.10.6. Overgangsordning i relation til sager om overtrædelser med databeskyttelsesretlige elementer

Ovenstående retningslinjer for håndtering af sager om overtrædelser med databeskyttelsesretlige elementer finder anvendelse på alle sager om overtrædelser med databeskyttelsesretlige elementer, hvori der vil blive nedlagt påstand om bødestraf, jf. dog nedenfor i relation til bødeniveau mv.

Det indebærer, at der i alle tilfælde skal ske en forelæggelse af sagen for statsadvokaten, som nærmere beskrevet under pkt. 3.10.4., med henblik på bl.a. stillingtagen til bødepåstanden.

Det er i den forbindelse udgangspunktet, at bødepåstanden skal fastsættes under iagttagelse af bødeniveauet for overtrædelse af databeskyttelsesforordningen og databeskyttelsesloven. Dette udgangspunkt gælder undtagelsesfrit for så vidt angår sager, hvor gerningstidspunktet ligger efter retningslinjernes ikrafttræden den 27. september 2021.

I sager, hvor gerningstidspunktet ligger forud for retningslinjernes ikrafttræden den 27. september 2021, kan der dog ved fastlæggelsen af bødeniveauet efter en konkret vurdering – og under sædvanlig inddragelse af skærpende og formildende omstændigheder – i stedet lægges vægt på bødeniveauet på tidspunktet for overtrædelsen, f.eks. hvis en række tilsvarende sager er afgjort på baggrund af dette bødeniveau.

Hvis der er tale om en sag, hvor bødeniveauet skal udmåles under iagttagelse af bødeniveauet for overtrædelse af databeskyttelsesforordningen og databeskyttelsesloven, indebærer retningslinjerne – ud over pligten til at forelægge sagen for statsadvokaten – bl.a. følgende:

- at statsadvokaterne skal drøfte bødepåstanden med Datatilsynet i forbindelse med kredsens forelæggelse af sagen, som anført under pkt. 3.10.4.
- at sagerne ikke må afgøres med bødeforelæg, som anført under pkt. 3.10.4., og
- at det generelle notat "Overtrædelser af straffeloven og andre særregler med databeskyttelsesretlige elementer" og Datatilsynets "Bødevejledning – Udmåling af bøder til fysiske personer" skal bilageres ind på sagerne, som beskrevet under pkt. 3.10.5.

Hvis det derimod efter en konkret vurdering besluttes, at der skal nedlægges påstand om en bøde udmålt med udgangspunkt i bødeniveauet på tidspunktet for overtrædelsen gælder der – ud over pligten til at forelægge sagen for statsadvokaten – ikke yderligere særlige retningslinjer for sagsbehandlingen. Det betyder:

- at bødepåstanden ikke skal drøftes med Datatilsynet
- at sagerne godt kan afgøres med bødeforelæg (hvis der i øvrigt er grundlag for det)
- at det generelle notat "Overtrædelser af straffeloven og andre særregler med databeskyttelsesretlige elementer" og Datatilsynets "Bødevejledning – Udmåling af bøder til fysiske personer" ikke skal bilageres ind på sagerne

Uanset ovenstående bemærkes det desuden, at det af visse straffebestemmelser i særlovgivningen fremgår, at overtrædelse af givne bestemmelser straffes efter særlovens regler, medmindre højere straf er forskyldt efter anden lovgivning. Ved sådanne formuleringer bør det overvejes, om højere straf er forskyldt efter de databeskyttelsesretlige regler med den konsekvens, at sagen bør rejses efter de databeskyttelsesretlige regler, uanset at gerningstidspunktet ligger forud for offentliggørelsen af indeværende opdaterede afsnit i rigsadvokatmeddelelsen.

3.10.7. Oversigt over sagsgangen i sager om overtrædelser med databeskyttelsesretlige elementer

Straf	Straf	Straf
Frihedsstraf efter straffeloven eller speciallovgivningen	*Bødestraf* efter straffeloven eller speciallovgivningenog	*Bødestraf* efter straffeloven eller speciallovgivningen
Tiltale *Ingen* subsidiær tiltale for overtrædelse af de databeskyttelsesretlige regler	Tiltale *Ingen* subsidiær tiltale for overtrædelse af de databeskyttelsesretlige regler	Tiltale *Subsidiær* tiltale for overtrædelse af de databeskyttelsesretlige regler
Særlige retningslinjer? Sagen *er ikke* omfattet af de særlige retningslinjer i dette afsnit af Rigsadvokatmeddelelsen	Særlige retningslinjer? Sagen *er* omfattet af de særlige retningslinjer i dette afsnit af Rigsadvokatmeddelelsen, jf. pkt. 3.10.	Særlige retningslinjer? Sagen *er* omfattet af de særlige retningslinjer i dette afsnit af Rigsadvokatmeddelelsen, jf. pkt. 3.10. og 3.3.-3.7.
	Bødeniveau Det databeskyttelsesretlige område	Bødeniveau Det databeskyttelsesretlige område
Forelægges SA? Nej	Forelægges SA? Ja	Forelægges SA? Ja
Inddragelse af Datatilsynet? Nej	Inddragelse af Datatilsynet? Ja *(evt. drøftelse af bødepåstanden)*	Inddragelse af Datatilsynet? Ja *(evt. drøftelse af bødepåstanden og udtalelse fsa. den subsidiære tiltale)*

3.10.8. Procedure

Rigsadvokaten har udarbejdet et notat til eventuel brug for anklagerens procedure om bødeudmålingen i sager om overtrædelser med databeskyttelsesretlige elementer, hvori anklageren vil nedlægge påstand om bødeudmåling under iagttagelse af bødeniveauet for overtrædelser af databeskyttelsesforordningen og databeskyttelsesloven. Notatet ligger på den interne del af anklagemyndighedens Vidensbase.

3.10.9. Undtagelser fra retningslinjerne for behandling af sager om overtrædelser med databeskyttelsesretlige elementer

Danmark er EU-retligt forpligtet til at sikre, at udmålingen af straf for overtrædelse af bestemmelser med databeskyttelsesretlige elementer – i det omfang forholdet falder inden for forordningens og databeskyttelseslovens anvendelsesområde – sker under iagttagelse af strafniveauet for overtrædelser af databeskyttelsesforordningen og databeskyttelsesloven. Det betyder, at evt. udmålte bøder ikke må være lavere, når de er udmålt efter straffeloven, end de ville have været, hvis de havde været udmålt efter databeskyttelsesreglerne.

Alle sager om overtrædelser med databeskyttelsesretlige elementer, hvori der vil blive nedlagt påstand om bødestraf, skal derfor behandles i overensstemmelse med de retningslinjer, der fremgår ovenfor af pkt. 3.10., jf. dog undtagelsen nedenfor om **sager, hvor bødeniveauet er angivet i forarbejderne**.

Hvis der er angivet et klart udgangspunkt for bødeniveauet i forarbejderne til loven, som det for eksempel er tilfældet i forarbejderne til bestemmelsen om identitetsmisbrug i straffelovens § 264 e, og forholdet vurderes at være omfattet af udgangspunktet (dvs. som altovervejende udgangspunkt førstegangstilfælde, hvor der foreligger en enkelt overtrædelse) kan sagen afgøres med bødeforelæg uden iagttagelse af ovenstående retningslinjer for behandling af sager om overtrædelser med databeskyttelsesretlige elementer.

Retningslinjerne for behandling af sager identitetstyveri efter straffelovens § 264 e er beskrevet nærmere i Rigsadvokatmeddelelsens afsnit om Freds- og ærekrænkelser (§§ 263-275 a).

4. Jura

4.1. Generelt om databeskyttelse

4.1.1. Oversigt over grundlæggende begreber i databeskyttelsesretten

4.1.1.1. Personoplysning

En ”personoplysning” er enhver form for information om en identificeret eller identificerbar fysisk person eller en enkeltmandsejet virksomhed, jf. databeskyttelsesforordningens artikel 4, nr. 1.

Begrebet personoplysning omfatter bl.a. personnumre, registreringsnumre, billeder, lyd/stemme, fingeraftryk og genetiske kendetegn mv. En oplysning er ”personhenførbar”, når det i praksis er muligt at identificere en person ud fra oplysningen eller i kombination med andre oplysninger. Også de tilfælde hvor det alene for den indviede vil være muligt at forstå, hvem en oplysning vedrører, er omfattet af definitionen, og det er uden betydning, om identifikationsoplysningerne er alment kendte eller umiddelbart tilgængelige.

Der gælder forskellige betingelser og procedurer for behandling af personoplysninger afhængig af oplysningernes karakter, se nærmere nedenfor under pkt. 4.1.2. om de forskellige typer af personoplysninger.

4.1.1.2. Behandling

Databeskyttelsesreglerne finder anvendelse, når der sker en "behandling" af personoplysninger. Begrebet ”behandling” omfatter enhver form for håndtering af oplysninger, f.eks. indsamling, registrering, systematisering, opbevaring, tilpasning, søgning, brug, videregivelse (herunder offentliggørelse), formidling og sletning, jf. definitionen i forordningens artikel 4, nr. 2.

Finder blot én af de i forordningens artikel 4, nr. 2, nævnte former for håndtering af personoplysninger sted, vil der være tale om en behandling, som er omfattet af databeskyttelsesreglerne.

4.1.1.3. Den registrerede

”Den registrerede” er den person, oplysningerne vedrører. Den registrerede har forskellige rettigheder i relation til behandlingen af oplysningerne, herunder ret til at få besked om, at der behandles oplys-

ninger om vedkommende (oplysningspligt), ret til at få adgang til og information om oplysninger om vedkommende selv (indsigtsret) og ret til – i visse situationer – at få oplysninger rettet eller slettet.

Se Datatilsynets vejledning om de registreredes rettigheder for en nærmere beskrivelse. Vejledningen findes på Datatilsynets hjemmeside.

4.1.1.4. Den dataansvarlige og databehandleren

I databeskyttelsesretten sondres der mellem "dataansvarlige" og "databehandlere". Der gælder forskellige forpligtelser efter de databeskyttelsesretlige regler alt efter, om der er tale om en dataansvarlig eller en databehandler. Afgrænsningen kan i visse tilfælde give anledning til tvivl.

Det er som udgangspunkt den "dataansvarlige", som har ansvaret for, at en behandling af personoplysninger lever op til de databeskyttelsesretlige regler. En dataansvarlig er en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger, jf. definitionen i forordningens artikel 4, nr. 7.

En "databehandler" er en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne, jf. definitionen i forordningens artikel 4, nr. 8.

Både den dataansvarlige og eventuelle databehandlere kan ifalde strafansvar for overtrædelse af databeskyttelsesreglerne.

Se Datatilsynets og Justitsministeriets vejledning om dataansvarlige og databehandlere for nærmere vedrørende afgrænsningen mellem at være dataansvarlig og databehandler. Vejledningen findes på Datatilsynets hjemmeside.

4.1.2. Kategorier af personoplysninger

Der gælder forskellige betingelser og sikkerhedskrav mv. ved behandling af personoplysninger afhængigt af oplysningernes karakter. Personoplysninger inddeles således i forskellige kategorier:

1) Almindelige personoplysninger, jf. forordningens artikel 6.
2) Særlige kategorier af personoplysninger (følsomme personoplysninger), jf. forordningens artikel 9.
3) Herudover findes der regler i databeskyttelsesloven, der særligt regulerer behandling af oplysninger om straffedomme og lovovertrædelser (strafbare forhold), jf. databeskyttelseslovens § 8, og behandling af oplysninger om personnummer, jf. databeskyttelseslovens § 11.

Ad 1) Artikel 6 er en opsamlingsbestemmelse, og enhver personoplysning, der ikke er omfattet af den udtømmende opremsning af særlige kategorier af personoplysninger i artikel 9 eller af særlovgivning (f.eks. databeskyttelsesloven) er omfattet af artikel 6.

Ad 2) Særlige kategorier af personoplysninger, også kaldet følsomme personoplysninger, er udtømmende oplistet i forordningens artikel 9. Følsomme personoplysninger er oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt

behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Ad 3) Databeskyttelseslovens § 8 indeholder regler om offentlige myndigheders og privates behandling af oplysninger om strafbare forhold.

Databeskyttelseslovens § 11 indeholder regler om offentlige myndigheders og privates behandling af oplysninger om personnummer.

Se i øvrigt Datatilsynets hjemmeside www.datatilsynet.dk for en nærmere beskrivelse af reglernes indhold.

4.1.3. Oversigt over grundlæggende regler

De databeskyttelsesretlige regler indeholder bl.a.:

- Regler for, hvornår der må behandles personoplysninger, også kaldet behandlingsgrundlag, jf. forordningens artikel 6-10 og databeskyttelseslovens kapitel 3.
  - Se nærmere om begrebet "behandling" ovenfor under pkt. 4.1.1.2.
- Regler om grundlæggende principper for behandling af personoplysninger, jf. forordningens artikel 5.
  - Disse principper skal altid være opfyldt ved enhver behandling af personoplysninger.
- Regler om generelle forpligtelser for den dataansvarlige og databehandleren, jf. forordningens kapitel IV.
  - Se nærmere om begreberne "dataansvarlig" og "databehandler" ovenfor under pkt. 4.1.1.4.
- Regler om den registreredes rettigheder, jf. forordningens kapitel III og artikel 34 samt databeskyttelseslovens §§ 22-23.
  - Se nærmere om begrebet "den registrerede" ovenfor under pkt. 4.1.1.3.
- Regler om behandlingssikkerhed, jf. forordningens artikel 32.
- Regler om overførsel af personoplysninger til tredjelande eller internationale organisationer, jf. forordningens kapitel V.

4.2. Databeskyttelsesforordningen og databeskyttelsesloven

Den 25. maj 2018 blev persondataloven afløst af databeskyttelsesforordningen, der suppleres af databeskyttelsesloven og anden national særregulering.

Databeskyttelsesforordningen har direkte virkning i Danmark, hvilket bl.a. betyder, at forordningen har samme virkning som en lov i Danmark.

For så vidt angår anvendelsesområdet, svarer dette i vidt omfang til persondatalovens anvendelsesområde. Materielt gælder reglerne således bl.a. som udgangspunkt for al automatisk (dvs. elektronisk) behandling af personoplysninger, der foretages af offentlige myndigheder og private virksomheder, foreninger mv. Se nærmere om reglernes materielle og geografiske anvendelsesområde nedenfor under pkt. 4.2.1.

4.2.1. Materielt og territorialt anvendelsesområde

Databeskyttelsesforordningen finder anvendelse på behandling af personoplysninger, jf. forordningens artikel 2, nr. 1, første led. En personoplysning er enhver form for information om en identificeret eller identificerbar fysisk person eller en enkeltmandsejet virksomhed, jf. databeskyttelsesforordningens artikel 4, nr. 1. Se nærmere om begrebet "personoplysning" ovenfor under pkt. 4.1.1.1.

Det er desuden en forudsætning for reglernes anvendelse, at behandlingen af personoplysningerne foretages helt eller delvist ved hjælp af automatisk databehandling, eller at oplysningerne er eller vil blive indeholdt i et register, jf. forordningens artikel 2, stk. 1, andet led. Begrebet "automatisk databehandling" er sammenfaldende med "elektronisk databehandling", som blev anvendt i det tidligere gældende databeskyttelsesdirektiv og persondataloven. Se nærmere om begrebet "behandling" ovenfor under pkt. 4.1.1.2.

Databeskyttelsesforordningens regler gælder ikke for en fysisk persons behandling af oplysninger under en rent personlig eller familiemæssig aktivitet og uden forbindelse med en erhvervsmæssig eller kommerciel aktivitet. Personlige eller familiemæssige aktiviteter kan bl.a. omfatte sociale netværksaktiviteter og onlineaktiviteter, der udøves som led i sådanne aktiviteter.

Ved vurderingen af, om en privat persons offentliggørelse af personoplysninger på internettet kan anses for at være sket i rent private sammenhænge – og dermed falder uden for databeskyttelsesreglernes anvendelsesområde – skal der foretages en konkret helhedsvurdering af offentliggørelsen, herunder om aktiviteten kan anses for at være legitim, ligesom der også kan lægges vægt på, om der er tale om en aktivitet, der anses for sædvanlig i den konkrete sammenhæng. I den forbindelse kan bl.a. inddrages karakteren af de offentliggjorte oplysninger, konteksten, hvori oplysningerne er offentliggjort og formålet med offentliggørelsen. Det kan også indgå i vurderingen, om behandlingen er uden forbindelse med erhvervsmæssig eller kommerciel aktivitet.

Databeskyttelsesforordningen finder endvidere ikke anvendelse, hvis det vil være i strid med ytringsfriheden i artikel 10 i Den Europæiske Menneskerettighedskonvention, eller artikel 11 i Den Europæiske Unions Charter om Grundlæggende Rettigheder, jf. databeskyttelseslovens § 3.

Forordningen er umiddelbart gældende i hver EU-medlemsstat og finder anvendelse på behandling af personoplysninger, som foretages som led i aktiviteter, der udføres for en dataansvarlig eller en databehandler, som er etableret i EU. Dette gælder, uanset om behandlingen finder sted i EU eller ej, jf. forordningens artikel 3, nr. 1. Se nærmere om begreberne "dataansvarlig" og "databehandler" ovenfor pkt. 4.1.1.4.

Forordningen finder også anvendelse på behandling af personoplysninger om registrerede, der er i EU, og som foretages af en dataansvarlig eller databehandler, der *ikke* er etableret i EU. Dette gælder dog kun, hvis behandlingsaktiviteterne vedrører udbud af varer eller tjenester til sådanne registrerede i EU, uanset om betaling fra den registrerede er påkrævet, eller hvis aktiviteten vedrører overvågning af sådanne registreredes adfærd, såfremt deres adfærd finder sted i EU, jf. forordningens artikel 3, nr. 2.

I langt de fleste tilfælde vil en behandling af personoplysninger, som foregår i Danmark, være omfattet af den danske lovgivning, dvs. forordningen, databeskyttelsesloven og eventuelle relevante danske særregler. Men der kan være situationer, hvor den dataansvarlige er etableret i et andet EU-land. I så fald vil det ud over forordningen være lovgivningen i dette land, der gælder.

Se forordningens artikel 2 og 3 samt databeskyttelseslovens §§ 1-4 for nærmere vedrørende reglernes anvendelsesområde. Se endvidere nærmere om de grundlæggende begreber ovenfor under pkt. 4.1.1.

4.3. Retshåndhævelsesloven

Parallelt med databeskyttelsesforordningen og databeskyttelsesloven gælder retshåndhævelsesloven, der trådte i kraft den 30. april 2017. Retshåndhævelsesloven gælder for politiets, anklagemyndighedens, herunder den militære anklagemyndigheds, kriminalforsorgens, Den Uafhængige Politiklagemyndigheds og domstolenes behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og for anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register, når behandlingen foretages med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder for at beskytte mod eller forebygge trusler mod den offentlige sikkerhed, jf. retshåndhævelseslovens § 1.

Retshåndhævelsesloven finder først og fremmest anvendelse på den behandling af personoplysninger, som finder sted i forbindelse med de kompetente myndigheders aktiviteter inden for strafferetsplejen.

Loven omfatter i øvrigt det område, der tidligere var omfattet af begrebet "det strafferetlige område", jf. persondatalovens § 2, stk. 4. Dette begreb blev i praksis defineret bredt og omfattede i hvert fald kerneområdet af domstolenes samt politiets og anklagemyndighedens virksomhed inden for strafferetsplejen, dvs. behandling af sager, som er under efterforskning, eller hvor der tages stilling til strafansvar og strafudmåling. Ud over dette kerneområde er det i praksis fastlagt under persondataloven, at også politiets og anklagemyndighedens aktiviteter af mere generel karakter på det strafferetlige område kan være omfattet af begrebet. Retshåndhævelsesloven finder også anvendelse for langt hovedparten af politiets øvrige virksomhed, herunder ordenshåndhævelse, kriminalitetsforebyggelse og på områder, hvor politiet kan forventes at gennemføre tvangsindgreb og foretage magtanvendelse.

Det bemærkes, at databeskyttelsesforordningens/databeskyttelseslovens og retshåndhævelseslovens anvendelsesområder er gensidigt udelukkende. En behandling af personoplysninger kan således ikke være omfattet af både retshåndhævelsesloven og databeskyttelsesforordningen/databeskyttelsesloven.

4.4. Tv-overvågningsloven

Som følge af de nye regler i databeskyttelsesforordningen og databeskyttelsesloven blev tv-overvågningsloven ændret den 23. maj 2018. Formålet med lovændringen var bl.a. at videreføre den tidligere gældende persondatalovs §§ 26 a og 26 d om behandling af personoplysninger i forbindelse med tv-overvågning.

4.4.1. Den dataansvarliges videregivelse af optagelser foretaget i forbindelse med tv-overvågning i kriminalitetsforebyggende øjemed, jf. tv-overvågningslovens § 4 c

Ved ændringen af tv-overvågningsloven i 2018 blev § 4 c indsat i loven. Af bestemmelsens stk. 1, fremgår det, at billed- og lydoptagelser med personoplysninger, der optages i forbindelse med tv-overvågning i kriminalitetsforebyggende øjemed, kun må videregives, hvis

1) den registrerede har givet sit udtrykkelige samtykke,
2) videregivelsen følger af lov, eller
3) videregivelsen sker til politiet i kriminalitetsopklarende øjemed.

Efter bestemmelsens stk. 2, må en erhvervsdrivende dog videregive billed- og lydoptagelser, der er optaget i forbindelse med tv-overvågning, internt i organisationen eller til andre erhvervsdrivende i kriminalitetsforebyggende øjemed, hvis betingelserne herfor er opfyldt, jf. bestemmelsens stk. 2, nr. 1 – 4.

Optagelserne som nævnt i stk. 1, skal som udgangspunkt slettes senest 30 dage efter, at optagelserne er foretaget, jf. bestemmelsens stk. 4, medmindre opbevaring i et længere tidsrum er nødvendigt af hensyn til den dataansvarliges behandling af en konkret tvist eller behandling af oplysningerne i kriminalitetsforebyggende øjemed efter stk. 2, jf. bestemmelsens stk. 5.

4.4.2. Straf for uberettiget videregivelse af optagelser omfattet af tv-overvågningsloven § 4 c, jf. lovens § 5, stk. 2.

Ved ændringen af tv-overvågningslovens i 2018 blev § 5, stk.2, ligeledes indsat i loven. Bestemmelsen foreskriver, at medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 6 måneder den, der i forbindelse med en behandling som udføres for private, overtræder lovens § 4 c.

Med henblik på at afstemme tv-overvågningsloven med databeskyttelsesforordningen og databeskyttelsesloven blev det med lovændringen forudsat, at bødeniveauet skulle forhøjes væsentligt i forhold til det dagældende bødeniveau efter persondataloven, ligesom der blev indført en strafferamme på fængsel i indtil 6 måneder i stedet for de dagældende 4 måneder. Det fremgår af lovforslagets (lovforslag nr. 205 af 21. marts 2018 om ændring af lov om tv-overvågning og lov om retshåndhævende myndigheders behandling af personoplysninger) specielle bemærkninger til § 5, stk. 2, at udmåling af straf efter bestemmelsen således skal ske forholdsmæssigt i forhold til strafniveauet for overtrædelser af databeskyttelsesforordningen og databeskyttelsesloven. Politikredsen skal derfor være opmærksom på, at der er sket en skærpelse af strafniveauet i forhold til tidligere, hvor videregivelse af optagelser fra tv-overvågning optaget i kriminalitetsforebyggende øjemed var reguleret af persondataloven. Der henvises nærmere til pkt. 5 om straf og andre retsfølger.

4.5. Overtrædelser med databeskyttelsesretlige elementer

Begrebet "overtrædelser med databeskyttelsesretligt elementer" dækker – når det anvendes i Rigsadvokatmeddelelsen – alle overtrædelser af straffeloven og speciallovgivningen (herunder sundhedsloven) med databeskyttelsesretlige elementer, dvs. overtrædelser, hvor gerningsindholdet også falder inden for databeskyttelsesforordningens og databeskyttelseslovens anvendelsesområde.

Hvis gerningsindholdet omvendt falder uden for forordningens og databeskyttelseslovens anvendelsesområde – f.eks. fordi der ikke er tale om automatisk databehandling mv., jf. databeskyttelsesforordningens artikel 2, stk. 1, og databeskyttelseslovens § 1, stk. 2 – gælder retningslinjerne ikke, uanset at der måtte være tale om overtrædelse af en af de bestemmelser, der er opremset ovenfor under pkt. 3.10.1. og i det generelle notat "Overtrædelser af straffeloven og andre særregler med databeskyttelsesretlige elementer".

Se nærmere om databeskyttelsesforordningens og databeskyttelseslovens materielle og territoriale anvendelsesområde ovenfor under pkt. 4.2.1., og om afgrænsningen af relevante straffebestemmelser og om det generelle notat ovenfor under pkt. 3.10.1.

4.5.1. Danmarks EU-retlige forpligtigelser

Databeskyttelsesforordningens artikel 83 og 84 indeholder bestemmelser om pålæggelse af bøder og andre sanktioner for overtrædelse af forordningen. Bestemmelserne suppleres af databeskyttelsesloven.

Det fremgår af bestemmelserne, at sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Det fremgår af betænkning nr. 1565/2017 om databeskyttelsesforordningen, at man i medfør af artikel 84 nationalt kan indføre og opretholde bestemmelser i særlovgivningen, der straffes med andre sanktioner, herunder bøde- og fængselsstraf. Sådanne sanktioner må dog antages at skulle fastsættes forholdsmæssigt i forhold til bødeniveauet i forordningens artikel 83 for herved at sikre en virkning svarende til forordningens.

Straffeloven og til dels også speciallovgivningen (f.eks. sundhedsloven) indeholder en række bestemmelser med databeskyttelsesretlige elementer, dvs. bestemmelser, hvor gerningsindholdet ofte også vil være omfattet af databeskyttelsesreglerne. Sådanne overtrædelser med databeskyttelsesretlige elementer må anses for nationale særregler, der kan opretholdes i medfør af forordningens artikel 84.

Visse af straffelovsbestemmelserne med databeskyttelsesretlige elementer blev revideret i 2018 i forbindelse med en revision af straffelovens kapitel om freds- og ærekrænkelser (Lov nr. 1719 af 27. december 2018 om ændring af straffeloven, retsplejeloven, lov om erstatningsansvar og medieansvarsloven (Freds- og ærekrænkelser m.v.)). I den forbindelse blev det i forarbejderne til lovændringen (Lovforslag nr. L 20 af 3. oktober 2018 til lov om ændring straffeloven, retsplejeloven, erstatningsansvarsloven og mediaansvarsloven (freds- og ærekrænkelser m.v.), de almindelige bemærkninger, punkt 3 om forholdet til databeskyttelsesforordningen og databeskyttelsesloven) anført, at udmåling af straf for overtrædelser af de specifikke bestemmelser i lovforslaget, der tilpasser anvendelsen af forordningen, i det omfang forholdet falder inden for forordningens og databeskyttelseslovens anvendelsesområde, skal ske under iagttagelse af strafniveauet for overtrædelser af databeskyttelsesforordningen og databeskyttelsesloven.

Det fremgår videre af bemærkningerne, at det efter Justitsministeriets vurdering eksempelvis indebærer, at bødeniveauet for overtrædelser af specifikke bestemmelser, der tilpasser anvendelsen af forordningen, ikke må være lavere end bødeniveauet for tilsvarende overtrædelser af forordningen, ligesom bødeniveauet ikke må overskride grænserne for bødeniveauet i forordningens artikel 83.

Da det imidlertid ikke er alle straffelovens bestemmelser med databeskyttelsesretlige elementer, der er omfattet af ovennævnte lovforslag og lovbemærkningerne om skærpelse af bøderne, vil der være nogle straffelovsbestemmelser med databeskyttelsesretlige elementer, hvor der ikke i lovforarbejderne er taget direkte stilling til strafudmålingen i relation til de databeskyttelsesretlige regler. Tilsvarende gør sig gældende i forhold til eksempelvis sundhedslovens bestemmelser med databeskyttelsesretlige elementer, idet der ikke i lovforarbejderne til sundhedsloven er taget stilling til strafudmålingen i relation til de databeskyttelsesretlige regler.

Fælles for alle overtrædelser med databeskyttelsesretlige elementer (i såvel straffeloven som i speciallovgivningen) er dog, at Danmark er forpligtet efter EU-retten til at sikre, at udmålingen af straf for overtrædelse af de pågældende bestemmelser – i det omfang forholdet falder inden for forordningens og

databeskyttelseslovens anvendelsesområde – skal ske under iagttagelse af strafniveauet for overtrædelser af databeskyttelsesforordningen og databeskyttelsesloven.

5. Straf og andre retsfølger

5.1. Generelt om sanktionsspørgsmålet i sager om overtrædelse af databeskyttelsesreglerne

Et af hovedformålene med databeskyttelsesforordningen er at styrke og harmonisere EU-landenes sanktionsmuligheder ved overtrædelse af databeskyttelsesreglerne.

Tidligere blev overtrædelser af persondataloven typisk straffet med bøder på mellem 2.000 og 25.000 kr. afhængigt af karakteren af de pågældende overtrædelser.

Forordningens artikel 83 indeholder de generelle betingelser for udstedelse af administrative bøder for overtrædelse af forordningens bestemmelser.

Det fremgår af artikel 83, stk. 1, at bøden i hver enkelt sag skal være effektiv, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

I artikel 83, stk. 2, er derefter beskrevet en række momenter, som skal indgå, når der skal træffes afgørelse om sanktionsspørgsmålet for overtrædelser af forordningen, herunder om hvorvidt der skal pålægges en administrativ bøde og om den administrative bødes størrelse. Det nærmere indhold af artikel 83, stk. 2, er beskrevet nedenfor i pkt. 5.1.2.

For så vidt angår strafniveauet for overtrædelser af flere bestemmelser i forordningen fremgår det af forordningens artikel 83, stk. 3, at hvis en dataansvarlig eller en databehandler forsætligt eller uagtsomt i forbindelse med de samme eller forbundne behandlingsaktiviteter overtræder flere bestemmelser i forordningen, må bødens samlede størrelse ikke overstige beløbet for den alvorligste overtrædelse.

Forordningens artikel 83, stk. 4 og 5, indeholder derefter en inddeling af de mulige overtrædelser af forordningen i to kategorier baseret på overtrædelsernes karakter samt fastsætter et bødemaksimum for hver af de to kategorier.

Det fremgår således af forordningens artikel 83, stk. 4, at overtrædelse af en række nærmere angivne bestemmelser straffes med bøder på op til 10.000.000 euro, eller hvis det drejer sig om en virksomhed, med op til 2 % af dens samlede globale årlige omsætning i det foregående regnskabsår, hvis det beløb er højere.

Endvidere fremgår det af forordningens artikel 83, stk. 5 og 6, at overtrædelse af de øvrige bestemmelser samt manglende overholdelse af et påbud fra Datatilsynet straffes med bøder på op til 20.000.000 euro, eller hvis det drejer sig om en virksomhed, med op til 4 % af dens samlede globale årlige omsætning i det foregående regnskabsår, hvis det beløb er højere.

Se nærmere om strafudmåling i relation til hhv. juridiske personer under pkt. 5.2., fysiske personer under pkt. 5.3. og offentlige myndigheder under pkt. 5.4.

Det fremgår af databeskyttelseslovens § 41, stk. 1-2, at straffen for overtrædelse af de databeskyttelsesretlige regler er bøde eller fængsel indtil 6 måneder. Det fremgår desuden af databeskyttelseslovens § 41, stk. 3, at databeskyttelsesforordningens artikel 83, stk. 2, skal følges ved pålæggelse af straf efter lovens § 41, stk. 1 og 2. Straffelovens kapitel 10 om straffens fastsættelse finder i øvrigt anvendelse.

Reglerne i databeskyttelsesforordningen og databeskyttelsesloven lægger således op til en markant forøgelse af bødeniveauet i forhold til, hvad overtrædelser af persondataloven blev takseret til. Tidligere retspraksis kan derfor kun i meget begrænset omfang tillægges betydning ved afgørelse af sanktionsspørgsmålet efter de nuværende regler, mens såvel doms- som administrativ praksis fra andre EU-lande fremadrettet vil få øget betydning.

Det fremgår af forarbejderne til databeskyttelsesloven (Lovforslag nr. L 68 af 25. oktober 2017, de almindelige bemærkninger, pkt. 2.8.3.7), at der vil være grundlag for, at straffen stiger til fængsel i tilfælde, hvor der for eksempel er sket en forsætlig offentliggørelse af særligt beskyttelsesværdige oplysninger, såsom følsomme oplysninger, i et meget betydeligt omfang.

Der er ikke i forordningen eller i bemærkningerne til databeskyttelsesloven anført et nærmere bødeniveau for overtrædelse af databeskyttelsesreglerne. Når der i retspraksis på forskellige områder er fastlagt et bødeniveau, vil Datatilsynet begynde at kunne udstede administrative bødeforelæg i ukomplicerede sager uden bevismæssige tvivlsspørgsmål, jf. databeskyttelseslovens § 42.

5.1.1. Hensynene bag reglerne

Hensynene bag databeskyttelsesreglerne og den markante skærpelse af bødeniveauet er blandt andet følgende:

- Databeskyttelse er en grundlæggende rettighed efter EU's Charter om grundlæggende rettigheder og traktaten om Den Europæiske Unions funktionsmåde (TEUF). Det fremgår af databeskyttelsesforordningens præambelbetragtning 1.
  - Den hastige teknologiske udvikling og globaliseringen har skabt nye udfordringer, hvad angår beskyttelse af personoplysninger. Denne udvikling kræver en stærk og mere sammenhængende databeskyttelsesramme i EU, som understøttes af effektiv håndhævelse for at skabe den tillid, der gør det muligt, at den digitale økonomi kan udvikle sig på det indre marked.
- De hidtidige regler om databeskyttelse blev implementeret forskelligt i de forskellige EU-lande, og der har derfor været forskellige beskyttelsesniveauer. Det fremgår af databeskyttelsesforordningens præambelbetragtning 9.
- De nye regler skal sikre et ensartet og højt niveau for beskyttelse af fysiske personer og fjerne hindringerne for udveksling af personoplysninger inden for EU, og reglerne skal anvendes konsekvent og ensartet i EU. Det fremgår af databeskyttelsesforordningens præambelbetragtning 10.
- Der skal være harmonisering mellem sanktionerne i de forskellige EU lande, så dataansvarlige og databehandlere ikke kan "forum-shoppe", dvs. spekulere i at etablere sig i lande, hvor strafniveauet er lavere end i andre lande. Det fremgår bl.a. af Betænkning nr. 1565 afgivet af Justitsministeriet om Databeskyttelsesforordningen (2016/679) – de retlige rammer for dansk lovgivning.
- For at styrke håndhævelsen af forordningens regler bør der pålægges sanktioner for overtrædelse af forordningen. Det fremgår af forordningens præambelbetragtning 148.
- De pålagte bøder bør være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning. Det fremgår af forordningens præambelbetragtning 151.

5.1.2. Momenter af betydning for sanktionsspørgsmålet (forordningens artikel 83, stk. 2)

I forordningens artikel 83, stk. 2, er beskrevet en lang række momenter, som skal indgå, når der skal træffes afgørelse om, hvorvidt der skal pålægges en bøde for overtrædelse af forordningen mv. og om bødens størrelse.

Det fremgår af databeskyttelseslovens § 41, stk. 3, at databeskyttelsesforordningens artikel 83, stk. 2, skal følges ved pålæggelse af straf efter lovens § 41, stk. 1 og 2.

De momenter, der efter artikel 83, stk. 2, bl.a. skal lægges vægt på ved afgørelsen af, om der skal pålægges og udmåles en sanktion, og om bødens størrelse, er:

- Overtrædelsens karakter, alvor og varighed under hensyntagen til den pågældende behandlings karakter, omfang eller formål samt antal registrerede, der er berørt, og omfanget af den skade, som de har lidt,
- hvorvidt overtrædelsen blev begået forsætligt eller uagtsomt,
- eventuelle foranstaltninger der er truffet af den dataansvarlige eller databehandleren for at begrænse den skade, som den registrerede har lidt,
- den dataansvarliges eller databehandlerens grad af ansvar under hensyntagen til tekniske og organisatoriske foranstaltninger, som de har gennemført,
- den dataansvarliges eller databehandlerens eventuelle relevante tidligere overtrædelser,
- graden af samarbejde med tilsynsmyndigheden for at afhjælpe overtrædelsen og begrænse de negative konsekvenser, som overtrædelsen måtte have givet anledning til,
- de kategorier af personoplysninger, der er berørt af overtrædelsen,
- den måde hvorpå tilsynsmyndigheden fik kendskab til overtrædelsen, navnlig om den dataansvarlige eller databehandleren har underrettet om overtrædelsen, og i givet fald i hvilket omfang,
- overholdelse af eventuelt tidligere korrigerende beføjelser, som Datatilsynet har truffet afgørelse om over for den pågældende dataansvarlige eller databehandler med hensyn til samme genstand,
- overholdelse af godkendte adfærdskodekser eller certificeringsmekanismer, og
- om der er andre skærpende eller formildende faktorer ved sagens omstændigheder, såsom opnåede økonomiske fordele eller undgåede tab som direkte eller indirekte følge af overtrædelsen.

Opremsningen er ikke udtømmende og suppleres af de almindelige bestemmelser i straffelovens §§ 80-82.

Hvad der nærmere forstås ved de enkelte kriterier er endvidere uddybet i Artikel 29-gruppens retningslinjer af 3. oktober 2017 vedrørende anvendelse og fastsættelse af administrative bøder i overensstemmelse med forordning (EU) 16/679. Retningslinjerne er udstedt af Artikel 29-gruppen – forløberen til det Europæiske Databeskyttelsesråd – under henvisning til forordningens artikel 70, stk. 1, litra k. Retningslinjerne findes på datatilsynets hjemmeside under vejledninger og skabeloner.

De enkelte kriterier i artikel 83 og deres betydning for bødefastsættelse er desuden beskrevet i Datatilsynets bødevejledning vedrørende udmåling af bøder til virksomheder, der ligeledes ligger på tilsynets hjemmeside. Se nærmere om bødeberegning nedenfor under pkt. 5.2.2. (om juridiske personer).

5.1.3. Forældelse

Det følger af straffelovens § 93, at forældelsesfristen er 2 år, når der ikke er hjemlet højere straf end 1 års fængsel for en overtrædelse, og 5 år, når der ikke er hjemlet højere straf end 4 års fængsel.

De generelle forældelsesfrister i straffelovens § 93 er fraveget ved overtrædelse af databeskyttelsesloven. Det følger således af databeskyttelseslovens § 41, stk. 7, at forældelsesfristen for overtrædelse af databeskyttelsesforordningen og -loven er 5 år. Baggrunden herfor er ifølge forarbejderne, at sagerne forventes at kunne antage en vis størrelse og kompleksitet, der kan gøre det vanskeligt at anlægge sag inden for de almindelige forældelsesfrister. Forarbejderne peger endvidere på, at behovet for at inddrage tilsynsmyndighederne også kan forlænge sagsbehandlingstiden.

Det følger af straffelovens § 93, stk. 4, at når samme handling indebærer flere lovovertrædelser med forskellige forældelsesfrister efter § 93, gælder den længste af forældelsesfristerne for samtlige overtrædelser. Efter ordlyden af § 93, stk. 4, gælder princippet om den længste forældelsesfrist kun mellem forældelsesfrister, der er fastsat efter § 93, stk. 1-3, hvilket forældelsesfristen for overtrædelse af databeskyttelsesloven ikke er. Det er dog den almindelige antagelse, at § 93, stk. 4, også ”griber” forældelsesfrister, der er fastsat i henhold til særlovsbestemmelser. Det følger i et vist omfang også af straffelovens § 2, hvorefter bl.a. § 93 gælder for alle strafbare forhold, dvs. også for særlovsovertrædelser. Konsekvensen heraf er, at straffelovsbestemmelser med databeskyttelsesretlige elementer vil blive ”grebet” af den længere forældelsesfrist i databeskyttelsesloven, når et forhold indebærer overtrædelse af begge regelsæt. Se nærmere om behandlingen af sager om straffelovsbestemmelser med databeskyttelsesretlige elementer under pkt. 3.10.

5.2. Strafudmåling i sager mod juridiske personer

5.2.1. Ansvarssubjekter

Ved overtrædelser, der er begået inden for en virksomhed, skal retningslinjerne for valg af ansvarssubjekt som beskrevet i afsnittet i Rigsadvokatmeddelelsen om Strafansvar for juridiske personer som udgangspunkt følges.

Det bemærkes dog, at det i sager om overtrædelse af de databeskyttelsesretlige regler og i sager om overtrædelser med databeskyttelsesretlige elementer altid er den dataansvarlige eller databehandleren, der er ansvarssubjekt.

Det er som udgangspunkt arbejdsgiveren, f.eks. en virksomhed, der er ansvarlig for de behandlinger, der finder sted i forbindelse med virksomhedens aktiviteter. Det omfatter normalt situationer, hvor medarbejdere handler inden for instruks. Den pågældende arbejdsgiver kan imidlertid også være ansvarlig, hvor medarbejdere handler uden for instruks, men klart i arbejdsgiverens interesse.

Dataansvaret skal som udgangspunkt placeres hos enten arbejdsgiveren, dvs. virksomheden, eller hos medarbejderen, dvs. den fysiske person.

Se nærmere om definitionen på ”dataansvar” og ”databehandler” oven for pkt. 4.1.1.4. og om, hvornår den ansatte bliver selvstændig dataansvarlig i pkt. 2 i Datatilsynets ”Bødevejledning - Udmåling af bøder til fysiske personer”.

5.2.2. Bødeberegning i sager om juridiske personers overtrædelse af de databeskyttelsesretlige regler

Som det fremgår af pkt. 3.4.1. og pkt. 3.5.2.1. skal Datatilsynet høres i alle sager om overtrædelse af de databeskyttelsesretlige regler, inden der træffes afgørelse om tiltalespørgsmålet. Datatilsynets udtalelse eller politianmeldelse vil indeholde tilsynets vurdering af tiltalespørgsmålet, herunder en indstilling om sanktionsspørgsmålet.

Datatilsynet har udarbejdet og offentliggjort en vejledning om fastsættelse af bøder i forbindelse med juridiske personers overtrædelser af databeskyttelsesreglerne. Tilsynet vedlægger "Bødevejledning – udmåling af bøder til virksomheder" og eventuelt relevant praksis som bilag til deres udtalelse eller politianmeldelse i alle sager mod juridiske personer. Bødevejledningen skal bilageres ind på sagen sammen med tilsynets udtalelse og eventuelt relevant praksis fremsendt af tilsynet. Bødevejledningen ligger desuden offentligt tilgængeligt på Datatilsynets hjemmeside under punktet "vejledning"

Det fremgår af vejledningen, at Datatilsynet ved beregningen af den indstillede bødes størrelse tager udgangspunkt i et grundbeløb, der beregnes på baggrund af *dels* overtrædelsens karakter (de forskellige overtrædelser inddeles i forskellige kategorier afhængigt af deres generelle alvor), *dels* den dataansvarlige juridiske persons størrelse (fastsat ud fra virksomhedens samlede globale årlige omsætning).

Efter at have fastlagt grundbeløbet justeres bøden efter overtrædelsens karakter, alvor og varighed i det konkrete tilfælde. Derefter kan der ske en stigning af beløbet ved skærpende omstændigheder og/eller et fald ved formildende omstændigheder.

Bøden må ikke overstige maksimummet fastsat i databeskyttelsesforordningens artikel 83, stk. 4-6. Hvis det er tilfældet, skal bødes justeres.

Endelig er der mulighed for – på opfordring fra virksomheden – under særlige omstændigheder at tage hensyn til virksomhedens betalingsevne. Se nærmere herom under pkt. 5.2.3.

Sammenfattende kan Datatilsynets model for beregning af bøder i forbindelse med juridiske personers overtrædelse af de databeskyttelsesretlige regler sættes op på følgende måde:

Grundbeløb Justering på baggrund af en konkret vurdering af overtrædelsens karakter, alvor og varighed (+/-) Skærpende omstændigheder (+) Formildende omstændigheder (-)
Bødens størrelse med hensyntagen til overtrædelse og sagens omstændigheder Eventuel justering for databeskyttelsesforordningens maksimum (-)

Eventuel justering efter betalingsevne (-)
Endeligt bødebeløb

Datatilsynets bødevejledning skal være normerende for både Datatilsynets indstilling til bødepåstanden og for anklagemyndighedens påstand i retten. Det er i den forbindelse vigtigt at være opmærksom på, at strafudmålingsprincipperne i straffelovens kapitel 10 også finder anvendelse på sager om overtrædelse af de databeskyttelsesretlige regler.

5.2.3. Regulering ift. betalingsevne

Datatilsynet gennemgår i pkt. 7 i tilsynets bødevejledning under hvilke omstændigheder, der kan ske regulering af bødens størrelse i forhold til virksomhedens betalingsevne.

Det fremgår af vejledningen, at en nedsættelse af bøden på grund af manglende betalingsevne kun skal overvejes, hvis den bødepålagte anmoder om det. Inden nedsættelse af bøden overvejes, kan mere moderate betalingsbetingelser, som f.eks. udsættelse af betalingen, overvejes.

Det fremgår desuden af vejledningen, at en nedsættelse af bøden på grund af manglende betalingsevne kræver ekstraordinære omstændigheder. Nedsættelse kan ifølge vejledningen kun ske, hvis der foreligger objektive beviser for, at den pålagte bøde med sikkerhed vil bringe den pågældende virksomheds økonomiske levedygtighed i fare og få dens aktiver til at miste al værdi.

Endelig fremgår det af bødevejledningen, at argumenter om manglende betalingsevne fra dataansvarlige, der er en del af store virksomheder, hvor datterselskaber kan søge økonomisk støtte hos deres moderselskab, ikke kan tages i betragtning.

5.2.4. Rettighedsfrakendelse

I sager vedrørende den type virksomhed, der er omfattet af databeskyttelseslovens § 26, det vil sige advarselsregistervirksomhed, kreditoplysningsbureauvirksomhed og virksomhed ved behandling af oplysninger, der udelukkende finder sted med henblik på at føre retsinformationssystemer, skal anklagemyndigheden overveje, om der skal nedlægges påstand om rettighedsfrakendelse, jf. databeskyttelseslovens § 43.

Det fremgår af databeskyttelseslovens § 43, at den, der driver eller er beskæftiget med virksomhed som nævnt i lovens § 26 eller som privat databehandler opbevarer personoplysninger, ved dom for strafbart forhold kan frakendes retten til at drive den pågældende type virksomhed, hvis det udviste forhold begrunder en nærliggende fare for misbrug.

Straffelovens bestemmelser i § 79, stk. 3 og 4, om tidsmæssig begrænsning af frakendelsen af retten og om umiddelbar udelukkelse af denne under sagens behandling mv. finder også anvendelse.

5.3. Strafudmåling i sager mod fysiske personer

5.3.1. Bødeberegning i sager om fysiske personers overtrædelse af de databeskyttelsesretlige regler

Som det fremgår af pkt. 3.4.1. og pkt. 3.5.2.1. skal Datatilsynet høres i alle sager om overtrædelse af de databeskyttelsesretlige regler, inden der træffes afgørelse om tiltalespørgsmålet. Datatilsynets udtalelse eller politianmeldelse vil indeholde tilsynets vurdering af tiltalespørgsmålet, herunder en indstilling om sanktionsspørgsmålet.

Datatilsynet har udarbejdet og offentliggjort en vejledning om fastsættelse af bøder i forbindelse med fysiske personers overtrædelser af databeskyttelsesreglerne. Tilsynet vedlægger "Bødevejledning – Udmåling af bøder til fysiske personer" og eventuelt relevant praksis som bilag til deres udtalelse eller politianmeldelse i alle sager mod fysiske personer. Bødevejledningen skal bilageres ind på sagen sammen med tilsynets udtalelse og eventuelt relevant praksis fremsendt af tilsynet. Bødevejledningen ligger desuden offentligt tilgængeligt på Datatilsynets hjemmeside under punktet "vejledning".

Det fremgår af bødevejledningen, at formålet med vejledningen bl.a. er at danne et klart og gennemskueligt grundlag for tilsynets bødeindstillinger for at sikre, at der gennem retspraksis skabes systematik i bødefastsættelsen.

Da databeskyttelsesforordningen og –loven lægger op til et væsentligt forhøjet bødeniveau i forhold til, hvad overtrædelser af persondataloven blev takseret til, vil bødeniveauet ses væsentligt forhøjet i forhold til tidligere praksis.

Datatilsynet gennemgår i vejledningen bl.a. hvilke momenter, der efter artikel 83 skal tages hensyn til ved udmålingen, herunder hvilke skærpende og formildende omstændigheder Datatilsynet har tillagt vægt i tilsynets tidligere indstillinger.

Det fremgår endvidere af vejledningen, at der på visse områder er tale om relativt sammenlignelige overtrædelser, hvorfor der kan udmåles standardbøder (f.eks. i sager om offentliggørelse af oplysninger på sociale medier).

Det er hensigten med bødevejledningen, at den skal være normerende for både Datatilsynets indstilling til bødepåstand og for anklagemyndighedens påstand i retten. Det er i den forbindelse vigtigt at være opmærksom på, at strafudmålingsprincipperne i straffelovens kapitel 10 også finder anvendelse på sager om overtrædelse af de databeskyttelsesretlige regler.

5.3.2. Bødeudmåling

Når bøder for overtrædelse af straffeloven idømmes eller vedtages i retten, fastsættes bødestraffen i dagbøder. Det følger af straffelovens § 51, stk. 1. I sager om straffelovsovertrædelser med databeskyttelsesretlige elementer skal der således udmåles dagbøder (eller frihedsstraf). Bødefastsættelse i form af dagbøder sker dels ved at regulere antallet af dagbøder, dels ved at regulere størrelsen af den enkelte dagbod. Der udmåles mindst 1 og højest 60 dagbøder. Se nærmere om overtrædelser med databeskyttelsesretlige elementer under pkt. 3.10.

Bøder idømt efter speciallovgivning (herunder de databeskyttelsesretlige regler) idømmes derimod som sumbøder, dvs. som ét fast beløb. Datatilsynet angiver derfor en samlet bødepåstand (eventuelt én

indstilling per forhold, hvis en sag indeholder flere overtrædelser af de databeskyttelsesretlige regler) i tilsynets indstillinger/politianmeldelser.

I et sagskompleks hvor en af lovovertrædelserne medfører en dagbod, mens en anden overtrædelse medfører en sumbøde, fastsætter retten som udgangspunkt en fælles straf af dagbod. Det følger af straffeloven § 88, stk. 3. I sådanne sager skal anklagemyndigheden således omregne den indstillede sumbøde til dagbøder og i den forbindelse være opmærksom på de regler for bødens fastsættelse, der fremgår af straffelovens § 51, stk. 1.

5.3.3. Regulering ift. betalingsevne

Ved bødeudmålingen i relation til fysiske personer er der ikke – på samme måde som i relation til bødeudmåling til juridiske personer – fastsat et bødemaksimum. Det fremgår dog af præambelbetragtning 150, at der i relation hertil skal tages hensyn til det generelle indkomstniveau i det pågældende EU-land samt personens økonomiske situation.

Bøderne nedsættes derfor for unge under 18 år og for personer med særlig lav indtægt i overensstemmelse med ordningen på færdselslovens område. Det er alderen og indtægtsforholdene på gerningstidspunktet, der er afgørende for spørgsmålet om bødenedsættelse.

Nærmere retningslinjer, herunder indtægtsgrænser for bødenedsættelse, kan findes i Rigsadvokatmeddelelsen afsnittet om Strafudmåling (§§ 80-84), pkt. 5, om straf og andre retsfølger.

5.3.4. Fængselsstraf

Der er efter databeskyttelseslovens § 41, stk. 1 og 2, mulighed for at idømme fængselsstraf for overtrædelse af de strafbelagte bestemmelser i forordningen, loven og regler fastsat i medfør heraf.

Det fremgår af forarbejderne til databeskyttelsesloven (Lovforslag nr. L 68 af 25. oktober 2017, de almindelige bemærkninger, pkt. 2.8.3.7), at der vil være grundlag for, at straffen stiger til fængsel i tilfælde, hvor der for eksempel er sket en forsætlig offentliggørelse af særligt beskyttelsesværdige oplysninger, såsom følsomme oplysninger, i et meget betydeligt omfang.

5.3.4.1. Udmåling af tillægsbøder

Det fremgår af databeskyttelsesforordningens artikel 83, stk. 3, at hvis en dataansvarlig eller en databehandler forsætligt eller uagtsomt i forbindelse med de samme eller forbundne behandlingsaktiviteter overtræder flere bestemmelser i databeskyttelsesforordningen, må den administrative bødes samlede størrelse ikke overstige beløbet for den alvorligste overtrædelse.

Derudover er der ikke i de databeskyttelsesretlige regler – som på visse andre særlovsområder – fastsat særlige regler om straf i sammenstød, herunder om straffastsættelse i tilfælde af sammenstød. Det indebærer, at straffelovens almindelige regler herom finder anvendelse.

Det fremgår således af straffelovens § 88, stk. 1, at der skal fastsættes en fælles straf i sager, hvor nogen ved en eller flere handlinger har begået flere lovovertrædelser. Det fremgår af stk. 2, at i sager indehol-

dende flere forhold, hvor en overtrædelse medfører fængsel, mens en anden overtrædelse medfører bøde, kan retten – i stedet for en fælles fængselsstraf – idømme bøde ved siden af fængsel.

Det er Rigsadvokatens opfattelse, at anklagemyndigheden som udgangspunkt ikke skal nedlægge påstand om, at der udmåles tillægsbøder for databeskyttelsesretlige overtrædelser i sager, hvor der samtidig idømmes frihedsstraf. Det er dog Rigsadvokatens opfattelse, at anklagemyndigheden bl.a. skal overveje at nedlægge påstand om udmåling af tillægsbøder, hvis den tiltalte ved lovovertrædelsen har opnået eller tilsigtet at opnå økonomisk vinding for sig selv eller andre.

5.4. Sanktionsspørgsmålet i forhold til offentlige myndigheder

5.4.1. Strafforfølgning mod offentlige myndigheder

Der er efter databeskyttelsesloven en udvidet adgang til at strafforfølge offentlige myndigheder mv. i forhold til de almindelige principper i straffelovens § 27, stk. 2, hvorefter statslige myndigheder og kommuner alene kan straffes i anledning af overtrædelser, der begås ved udøvelse af virksomhed, der svarer til eller kan sidestilles med virksomhed udøvet af private.

Efter databeskyttelseslovens § 41, stk. 6, 2. pkt., kan offentlige myndigheder og institutioner mv., som er omfattet af forvaltningslovens § 1, stk. 1 eller 2, uanset straffelovens § 27, stk. 2, også straffes i anledning af overtrædelser af loven, der begås ved udøvelse af virksomhed, der ikke svarer til eller kan sidestilles med virksomhed udøvet af private.

Domstolene (og evt. andre offentlige myndigheder, som ikke er omfattet af forvaltningslovens § 1, stk. 1 eller 2,) kan alene straffes i overensstemmelse med straffelovens § 27, stk. 2.

I straffesager mod en offentlig myndighed mv. skal de almindelige principper for valg af ansvarssubjekt for overtrædelser begået inden for rammerne af en virksomhed som udgangspunkt følges, jf. afsnittet i Rigsadvokatmeddelelsen om Strafansvar for juridiske personer, pkt. 3.1.3.

Det bemærkes dog, at det i sager om overtrædelse af de databeskyttelsesretlige regler og i sager om overtrædelser med databeskyttelsesretlige elementer altid er den dataansvarlige eller databehandleren, der er ansvarssubjekt.

Det er som udgangspunkt arbejdsgiveren, f.eks. en offentlig myndighed, der er ansvarlig for de behandlinger, der finder sted i forbindelse med myndighedens aktiviteter. Det omfatter normalt situationer, hvor medarbejdere handler inden for instruks. Den pågældende arbejdsgiver kan imidlertid også være ansvarlig, hvor medarbejdere handler uden for instruks, men klart i arbejdsgiverens interesse.

Dataansvaret skal som udgangspunkt placeres hos enten arbejdsgiveren, dvs. myndigheden, eller hos medarbejderen, dvs. den fysiske person

Se nærmere om definitionen på ”dataansvar” og ”databehandler” ovenfor under pkt. 4.1.1.4. og om, hvornår den ansatte bliver selvstændig dataansvarlig i pkt. 2 i Datatilsynets Bødevejledning - Udmåling i sager mod fysiske personer

5.4.2. Generelt om sanktionsspørgsmålet i forhold til offentlige myndigheder

Det er forudsat i forarbejderne til databeskyttelsesloven, at bødeniveauet for offentlige myndigheders overtrædelser af databeskyttelsesloven skal være lavere end for private aktørers overtrædelser.

Bødeloftet for offentlige myndigheder for overtrædelser omfattet af forordningens artikel 83, stk. 4, forudsættes at være 2 % af myndighedens driftsbevilling, dog maksimalt 8 mio. kr., henholdsvis 4 % af driftsbevillingen, maksimalt 16 mio. kr. for overtrædelser omfattet af forordningens artikel 83, stk. 5 og 6.

Med driftsbevillingen menes som udgangspunkt det samlede beløb, som den offentlige myndighed kan disponere over.

Samtidig med, at bødeloftet er lavere for offentlige myndigheder end for private, er det også forudsat, at forhøjelsen af bødeniveauet for offentlige myndigheder skal være lavere. Det fremgår af forarbejderne til databeskyttelsesloven (Lovforslag nr. L 68 af 25. oktober 2017, de alm. bemærkninger, pkt. 2.8.3.8).

Der skal ved udstedelse af bøder til offentlige myndigheder også tages hensyn til myndigheders særlige situation, der består i, at myndigheder – i modsætning til private aktører – efter lovgivningen er pålagt at varetage lovbestemte opgaver, og myndigheder derfor ikke uden videre i alle tilfælde blot kan standse en behandling for derved at bringe en eventuel ulovlig tilstand til ophør.

Det fremgår af forarbejderne til databeskyttelsesloven (Lovforslag nr. L 68 af 25. oktober 2017, de almindelige bemærkninger, pkt. 2.8.3.8), at det særlige, lavere bødeloft, der forudsætningsvist lægges op til for offentlige myndigheders overtrædelser af forordningen og loven, ikke gælder for private databehandlere, der for eksempel opbevarer oplysninger for det offentlige.

I øvrigt skal de generelle retningslinjer for fastsættelse af sanktionen i forhold til skærpende og formildende omstændigheder følges, jf. pkt. 5.1.2.

Datatilsynet forventes at udarbejde en bødevejledning vedrørende udmåling af bøder til offentlige myndigheder. Bødevejledningen vil blive offentliggjort på Datatilsynets hjemmeside under ”vejledninger”.

6. Efter dom

6.1. Underretning af Datatilsynet

Snarest muligt efter afslutningen af en sag, hvor der er rejst tiltale for overtrædelse af databeskyttelsesreglerne, skal Datatilsynet underrettes om sagens udfald og have tilsendt en kopi af dommen. Underretningen skal ske hurtigst muligt og i så god tid, at Datatilsynet har mulighed for at udtale sig i forhold til spørgsmålet om anke inden udløbet af ankefristen.

Tilsvarende gælder i forhold til sager vedrørende overtrædelse af tv-overvågningslovens § 4 c.

6.2. Underretning af statsadvokaten

Politikredsen skal forelægge alle domme om overtrædelse af de databeskyttelsesretlige regler, hvor anklagemyndigheden ikke har fået fuldt medhold (herunder i strafpåstanden), for statsadvokaten, inden ankefristens udløb.

Det samme gælder i forhold til sager vedrørende overtrædelse af tv-overvågningslovens § 4 c.

Derudover skal sager om overtrædelser med databeskyttelsesretlige elementer, hvori anklagemyndigheden har nedlagt påstand om bødestraf udmålt under iagttagelse af bødeniveauet for overtrædelse af databeskyttelsesforordningen og databeskyttelsesloven og ikke har fået fuldt ud medhold (herunder i strafpåstanden), også forelægges for statsadvokaten, inden ankefristens udløb, jf. pkt. 3.10.4.

6.3. Afgørelser til Vidensbasen

Alle endelige domme om overtrædelse af de databeskyttelsesretlige regler skal sendes til Vidensbasen.

Tilsvarende gælder i forhold til sager vedr. overtrædelse af tv-overvågningslovens § 4 c.

Derudover skal alle endelige domme om overtrædelser med databeskyttelsesretlige elementer (jf. pkt. 3.10. ovenfor), hvori der er nedlagt påstand om en bøde under iagttagelse af strafniveauet for overtrædelser af databeskyttelsesforordningen og databeskyttelsesloven, indsendes til Vidensbasen.

7. Love og forarbejder

Databeskyttelsesforordningen

- Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)
- Berigtigelse af 23. maj 2018 til Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)

Love

Databeskyttelsesloven

- Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)

Retshåndhævelsesloven

- Lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger
- Lov nr. 503 af 23. maj 2018 om ændring af lov om retshåndhævende myndigheders behandling af personoplysninger, lov om massemediers informationsdatabaser og forskellige andre love (konsekvensændringer som følge af databeskyttelsesloven og databeskyttelsesforordningen samt massemedieansvarslovens anvendelse på offentligt tilgængelige informationsdatabaser m.v.)

Tv-overvågningsloven

- Lov nr. 506 af 23. maj 2018 om ændring af lov om tv-overvågning og lov om retshåndhævende myndigheders behandling af personoplysninger

Relevante forarbejder

- Lovforslag nr. L 68 af 25. oktober 2017 om lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).
- Betænkning nr. 1565 afgivet af Justitsministeriet om Databeskyttelsesforordningen (2016/679) – de retlige rammer for dansk lovgivning.
- Betænkning afgivet af Retsudvalget den 9. maj 2018 over Forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)
- Lovforslag nr. 205 af 21. marts 2018 om ændring af lov om tv-overvågning og lov om retshåndhævende myndigheders behandling af personoplysninger

Videnspakker mv.

- Diverse vejledninger på Datatilsynets hjemmeside, bl.a.
  - Generel informationspjece om Databeskyttelsesforordningen
  - Artikel 29-gruppens retningslinjer af 3. oktober 2017 vedrørende anvendelse og fastsættelse af administrative bøder i overensstemmelse med forordning (EU) 16/679.
  - Overførsel til tredjelande
  - Samtykke
  - Dataansvarlige og databehandlere
  - Registreredes rettigheder
  - Bødevejledning om udmåling af bøder til fysiske personer
  - Bødevejledning om udmåling af bøder til virksomheder

Bilag

Bilag 1 - Overtrædelser af straffeloven og andre særregler med databeskyttelsesretlige elementer (Datatilsynet, 14. september 2021)

DATATILSYNET

14. september 2021

J.nr. SJ-STD-KEO
Dok.nr. 263114
KEO

Overtrædelser af straffeloven og andre særregler med databeskyttelsesretlige elementer

1. Indledning

Databeskyttelsesforordningen[1] har siden den 25. maj 2018 fundet anvendelse i Danmark og regulerer enhver behandling af personoplysninger, som falder inden for forordningens materielle og territoriale anvendelsesområde.

Databeskyttelsesforordningen giver inden for en lang række områder mulighed for, at der i national ret kan fastsættes bestemmelser for at tilpasse anvendelsen af forordningen, hvilket er sket bl.a. i databeskyttelsesloven[2], hvis formål først og fremmest er at supplere reglerne i databeskyttelsesforordningen.

Straffeloven indeholder en række bestemmelser med databeskyttelsesretlige elementer, dvs. bestemmelser hvor gerningsindholdet efter omstændighederne kan udgøre en overtrædelse af databeskyttelsesreglerne. Disse bestemmelser ligger inden for det nationale råderum, og udmålingen af straf for overtrædelse af bestemmelserne skal ske under iagttagelse af strafniveauet for overtrædelser af databeskyttelsesforordningen og databeskyttelsesloven.

Følgende straffelovsbestemmelser kan efter omstændighederne indeholde databeskyttelsesretlige elementer, der falder inden for databeskyttelsesforordningen og databeskyttelseslovens anvendelsesområde:

- tavshedspligt (§§ 152-152f)
- registermisbrug (§ 155)
- optagelse og videregivelse af børnepornografisk materiale (§ 226 og § 235)
- blufærdighedskrænkelse (§ 232)
- meddelelseshemmelighed, hemmelig lydoptagelse og hacking (§ 263)
- billedoptagelse, registreringer af færden og videregivelse (§§ 264a-264d)
- racisme (§ 266b)
- æreskrænkelse (§ 267)

[1] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).
[2] Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

Det bemærkes, at opremsningen ikke er udtømmende, ligesom det ikke er alle overtrædelser af de nævnte bestemmelser, som vil udgøre en overtrædelse af databeskyttelsesregleme. Afgørende for denne vurdering er, at gerningsindholdet er omfattet af databeskyttelsesforordningens anvendelsesområde, *jf.* nedenfor under pkt. 2. Se nedenfor under pkt. 4 for eksempler på situationer, der udgør både en overtrædelse af straffeloven og de databeskyttelsesretlige regler.

Formålet med dette notat er, at notatet skal kunne danne grundlag for en vurdering af, om en overtrædelse af straffeloven eller andre særregler med databeskyttelsesretlige elementer også er omfattet af de databeskyttelsesretlige regler.

2. Databeskyttelsesforordningens materielle anvendelsesområde

Databeskyttelsesforordningen finder i medfør af dennes artikel 2, stk. 1, anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikke-automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Begrebet "automatisk databehandling" er sammenfaldende med "edb" eller "elektronisk behandling"[3].

Automatisk/elektronisk skal i den forbindelse forstås bredt, idet en mundtlig og/eller manuel videregivelse også kan være omfattet af databeskyttelsesregleme, hvis den dataansvarlige er i besiddelse af oplysningerne elektronisk[4].

Databeskyttelsesforordningen gælder imidlertid bl.a. ikke for behandling af personoplysninger, som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter, *jf.* artikel 2, stk. 2, litra c.

Datatilsynet har den 16. december 2020 offentliggjort en hjemmesidetekst om, hvilke kriterier der skal indgå i vurderingen af, om en offentliggørelse af personoplysninger kan anses for omfattet af undtagelsesbestemmelsen[5]. Det fremgår heraf, at:

> "Ved vurderingen af, om en privatpersons offentliggørelse af personoplysninger på internettet kan anses for at være sket i rent private sammenhænge – og dermed falder uden for databeskyttelsesreglernes anvendelsesområde – skal der foretages en konkret helhedsvurdering af offentliggørelsen, herunder om aktiviteten kan anses for at være legitim, ligesom der også kan lægges vægt på, om der er tale om en aktivitet, der anses for sædvanlig i den konkrete sammenhæng. I den forbindelse kan bl.a. inddrages karakteren af de offentliggjorte oplysninger, konteksten, hvori oplysningerne er offentliggjort og formålet med offentliggørelsen. Det kan også indgå i vurderingen, om behandlingen er uden forbindelse med erhvervsmæssig eller kommerciel aktivitet."

Det skal understreges, at undtagelsesbestemmelsen i videre omfang finder anvendelse, hvis der er tale om behandlinger, som ikke involverer en egentlig offentliggørelse. I den forbindelse skal der imidlertid stadig foretages en konkret helhedsvurdering af behandlingen.

Databeskyttelsesforordningen finder endvidere ikke anvendelse, hvis det vil være i strid med informations- og ytringsfriheden i artikel 10 i Den Europæiske Menneskerettighedskonvention

[3] Betænkning nr. 1565 - Databeskyttelsesforordningen (2016/679) – og de retlige rammer for dansk lovgivning S. 31
[4] jf. U.2011.2343H.
[5] https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/dec/nye-afgoerelser-behandling-af-personoplysninger-i-rent-private-sammenhaenge

eller artikel 11 i Den Europæiske Unions Charter om Grundlæggende Rettigheder, *jf.* databeskyttelseslovens § 3.

3. Definition af personoplysninger og behandling

3.1. Personoplysninger

Ved personoplysninger forstås enhver form for information om en identificeret eller identificerbar fysisk person («den registrerede»); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet, *jf.* artikel 4, nr. 1.

Personoplysninger kan for eksempel være navne, adresser, personnumre, registreringsnumre, et billede, et fingeraftryk, en stemme, lægejournaler eller biologisk materiale, når det i praksis er muligt at identificere en person ud fra oplysningerne eller i kombination med andre.

Også "subjektive" oplysninger, udtalelser eller vurderinger kan udgøre personoplysninger, hvis oplysningen knytter sig til en bestemt person. Udsagnet "Thomas er en svindler" vil derfor udgøre personoplysninger om Thomas, forudsat at den pågældende person kan identificeres.

Endelig behøver personoplysninger ikke at være sande eller bevist, for at der er tale om personoplysninger.

3.2. Behandling

Behandling omfatter ifølge artikel 4, nr. 2, enhver aktivitet eller række af aktiviteter — med eller uden brug af automatisk behandling — som personoplysninger eller en samling af personoplysninger gøres til genstand for.

Behandling er f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

4. Eksempler på fælles "anvendelsesområde"

Afgørende for, om en bestemmelse i straffeloven eller andre særregler indeholder databeskyttelsesretlige elementer, er således, om den udøvede handling, for hvilken der er rejst tiltale, kan anses for at være en (automatisk/elektronisk) *behandling af personoplysninger*. Det forudsættes således i alle de nedenstående eksempler, at der er tale om en behandling af personoplysninger, som dette er defineret i afsnit 3, og at behandlingen af oplysninger ikke finder sted som led i rent personlige eller familiemæssige aktiviteter.

Som eksempel kan nævnes:

4.1. Straffelovens § 152

En persons videregivelse eller udnyttelse af fortrolige personoplysninger kan udgøre en overtrædelse af både straffelovens § 152 og de databeskyttelsesretlige regler. Det kunne f.eks. være tilfældet ved den kommunale medarbejders – eventuelt mundtlige – videregivelse af personoplysninger fra kommunens elektroniske sagsbehandlingssystem til pressen. Det kunne også være en forsvareres telefoniske videregivelse af oplysninger fra et lukket retsmøde og fra sagens akter, eller en politibetjents indhentning og videregivelse af personoplysninger fra politiets centrale systemer til en privatdetektiv (hvilket udgør en overtrædelse af både straffelovens § 152 og § 155).

4.2. Straffelovens § 155
En (offentligt ansat) person misbruger sin adgang til et register, hvortil vedkommende har adgang i kraft af sit arbejde. Dette kunne f.eks. være en politiassistent, som – i privat øjemed og uden tjenestelig begrundelse – foretager opslag i og videregiver personoplysninger fra et eller flere af politiets registre (hvilket kan udgøre en overtrædelse af både straffelovens § 152 og § 155).

4.3. Straffelovens § 226 og § 235
En person fotograferer og deler pornografiske videoer af personer under 18 år på internettet.

4.4. Straffelovens § 232
Blufærdighedskrænkelse ved f.eks. at sende billeder af en person i forskellige seksuelle situationer til andre via mail eller sms.

4.5. Straffelovens § 263
En person, der uberettiget skaffer sig adgang til en anden persons Facebook-konto og ændrer brugernavn, profilbillede m.v.

En persons installering af keyloggere på computere opstillet på biblioteker, hvorved pågældende aflurer brugernavn og adgangskoder til NemID.

En person foretager hemmelig lydoptagelse af andre personer. F.eks. ved aflytning af tidligere samlever ved hjælp af skjult radiosender eller ved skjult båndoptagelse af lukket møde.

4.6. Straffelovens § 264a
En person fotograferer andre personer, der befinder sig på et ikke frit tilgængeligt sted. Dette kan f.eks. være videooptagelse af personer, der går til og fra konfliktramt arbejdsplads.

4.7. Straffelovens § 264 d
En person videregiver nøgenbilleder af en anden person på internettet uden den afbildede persons samtykke.

4.8. Straffelovens § 266b
En person udtaler sig på en måde, som må anses for racisme omfattet af § 266b, og offentliggør i den forbindelse oplysninger om enkelpersoners race, etniske oprindelse, tro og/eller seksuelle orientering. Dette kan f.eks. ske ved racistisk opslag på Facebook eller i en blog på internettet.

4.9. Straffelovens § 267
Det er en konkret vurdering, i hvilken forbindelse der særligt skal sondres mellem oplysningernes karakter. Er der tale om subjektive personoplysninger i form af meningstilkendelser - f.eks. "Thomas er en svindler" – er udbredelsen heraf typisk ikke af en sådan karakter og alvor at det bør medføre en strafferetlig sanktion i henhold til databeskyttelsesreglerne. Er der derimod tale om mere objektive oplysninger – f.eks. oplysninger om konstaterbare strafbare forhold eller helbredsoplysninger – vil udbredelsen heraf kunne medføre strafferetlige sanktioner.

4.10. Sundhedslovgivningen
Som nævnt ovenfor kan overtrædelser af sundhedslovgivningen efter omstændighederne ligeledes falde inden for databeskyttelsesforordningen og databeskyttelseslovens anvendelsesområde. Det vil eksempelvis gælde, hvis en sygeplejerske videregiver helbredsoplysninger eller andre fortrolige personoplysninger i strid med sundhedslovens betingelser herfor eller hvis en læge foretager et uberettiget opslag i en elektronisk patientjournal i strid med sundhedslovens betingelser for indhentning af oplysninger.

Bilag 2 - Notat om Datatilsynets behandling af sager om såkaldt registermisbrug, mv. (Datatilsynet, 7. juli 2022)

DATATILSYNET

7. juli 2022

J.nr. 2021-212-2505
Dok.nr. 493630
MJG

Notat om Datatilsynets behandling af sager om såkaldt registermisbrug, mv.

I notatet konkluderes følgende:

- *Udgangspunktet bør fortsat være, at det er arbejdsgiverorganisationen, der er dataansvarlig, medmindre der er klare holdepunkter for at sige, at sundhedspersonens registeropslag er sket til varetagelse af egne formål, der ligger klart uden for organisationens aktiviteter.*

- *I tilfælde, hvor sundhedspersonen må anses for dataansvarlig, må det efter omstændighederne samtidig overvejes, om organisationen har levet op til sine forpligtelser efter forordningens artikel 32.*

- *Det anerkendes, at bagatelgrænsen i straffelovens § 155 til en vis grad svarer til grænsen for strafværdighed for overtrædelser af databeskyttelsesforordningen.*

- *Denne bagatelgrænse kan dog ikke anvendes som kriterium for, hvornår straffesager med databeskyttelsesretligt indhold bør forelægges Datatilsynet.*

- *Der fastsættes en række vejledende bødesatser for registermisbrug, jf. bilaget til dette notat.*

- *De i bilaget angivne tilfælde, hvor et forhold kan anses for ikke strafværdigt efter databeskyttelsesreglerne, kan inddrages i politiet/anklagemyndighedens vurdering af, hvornår en sag bør forelægges Datatilsynet.*

- *Datatilsynet genoptager nu sin behandling af de sager om registermisbrug, som tilsynet har haft berosat.*

1. Datatilsynets behandling af registermisbrugssager

"Registermisbrug" eller "uberettigede registeropslag" betegner i dette notat de tilfælde, hvor en fysisk person, der som led i sit arbejde har fået tildelt en adgang til et register med personoplysninger, anvender denne adgang på en måde, som ikke er hjemlet i det relevante retsgrundlag, og hvor der (derfor) heller ikke er hjemmel til behandlingen af personoplysninger i databeskyttelsesforordningen og databeskyttelsesloven.

Tilfælde af uberettigede opslag i elektroniske registre kan principielt opstå på flere forskellige samfundsområder, herunder hos både myndigheder og private organisationer. I praksis ser Datatilsynet dog stort set kun tilfælde af registermisbrug på sundhedsområdet, dvs. hvor såkaldte sundhedspersoner slår op i elektroniske register, som indeholder helbredsoplysninger, f.eks. Sundhedsplatformen, Fælles Medicinkort, Det Danske Vaccinationsregister, eller andre patientjournaler.

Datatilsynet behandler sager om registermisbrug på sundhedsområdet som følge af klager fra patienter (registrerede), som via offentligt tilgængelige log-muligheder har konstatereret et opslag, hospitalers m.fl.s anmeldelser af sikkerhedsbrud i anledning af registermisbrug, og anmodninger fra politiet/anklagemyndigheden om en udtalelse om strafværdighed (på baggrund af den registreredes politianmeldelse af registermisbruget).

Datatilsynet har sat sine sager om registermisbrug på sundhedsområdet i bero. Det skyldtes primært, at der var opstået 1) usikkerhed om, hvorvidt det er sundhedspersonen (den ansatte) eller arbejdsgiverorganisationen, der bør anses for ansvarssubjekt, og 2) uklarhed om det rette sanktionsniveau.

Datatilsynets berostillelse af registermisbrugssagerne blev kommunikeret til politi og anklagemyndighed[1].

2. Ansvarssubjekt

Udgangspunktet er, at arbejdsgiverorganisationen er dataansvarlig

Hvem, der er det rette ansvarssubjekt for uberettigede registeropslag, er i databeskyttelsesretlig sammenhæng et spørgsmål om, hvem der er dataansvarlig. Ansvarssubjektet er altså den, der bestemmer, til hvilke formål og med hvilke hjælpemidler personoplysningerne behandles, jf. databeskyttelsesforordningens artikel 4, nr. 7.

Udgangspunktet er, at det er arbejdsgiverorganisationen (f.eks. en region eller en kommune), som er dataansvarlig for en sundhedspersons registeropslag, og at den ansatte sundhedsperson således ikke selv personligt er dataansvarlig for sådanne opslag. Der henvises i den forbindelse til den kommenteret databeskyttelsesforordning[2] s. 272, hvor følgende fremgår:

> "Det er dén organisation mv. som sådan – f.eks. den offentlige myndighed eller den private virksomhed – som oplysningerne behandles på egne af, der er dataansvarlig, medmindre der er klare holdepunkter for at sige, at en fysisk person er den dataansvarlige, f.eks. hvis en fysisk person, der arbejder i en virksomhed eller en

1 Bl.a. blev der oplyst følgende til anklagemyndigheden i konkrete sager: "Datatilsynet er blevet opmærksomme på forhold, der har givet tilsynet anledning til at genovervejе håndteringen af overtrædelser af de databeskyttelsesretlige regler i forbindelse med misbrug af registeradgang. Datatilsynet kan dertil oplyse, at tilsynet skal genovervejе nærværende sag, samt en række andre lignende sager. Sagen afventer således tilsynets endelige stillingtagen til håndteringen af denne sagstype."
2 Kristian Korfitz Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, DJØFs forlag, 2020.

organisation, anvender oplysningerne til (egne) formål, der ligger klart uden for virksomhedens aktiviteter, jf. også princippet i forordningens artikel 28, stk. 10[3]. Det må generelt antages, at en organisation mv. er ansvarlig for de behandlinger, der finder sted i forbindelse med dennes aktiviteter."

Det anførte er afspejlet i Datatilsynets vejledning om udmåling af bøder til fysiske personer[4]. Under vejledningens pkt. 2 ("Dataansvar") fremgår følgende:

"**2.2.** Det er udgangspunktet, at en arbejdsgiver, fx offentlige myndigheder, virksomheder, organisationer mv., er ansvarlig for de behandlinger, der finder sted i forbindelse med dennes aktiviteter. Dette omfatter normalt situationer, hvor medarbejdere handler inden for instruks. Den pågældende arbejdsgiver kan imidlertid også være ansvarlig, hvor medarbejdere handler uden for instruks, men klart i arbejdsgiverens interesse. Som eksempel kan nævnes en situation, hvor en medarbejder er nødsaget til at fremsende et vigtigt dokument indeholdende personoplysninger ukrypteret på vegne af sin arbejdsgiver – og medarbejderen i den konkrete situation vurderer, at arbejdsgiveren ville have godkendt fremsendelsen – på trods af, at modtageren ikke understøtter et krypteringsniveau, der imødegår de risici, som fremsendelsen af dokumentet kræver.

I disse tilfælde, hvor medarbejderen handler uden for instruks, men klart i arbejdsgiverens interesse, beror vurderingen i vid udstrækning på karakteren af den konkrete instruks, herunder om det måtte stå klart for medarbejderen, at den pågældende behandling af personoplysninger var uønsket af arbejdsgiveren.

2.3. Dataansvaret skal placeres hos enten arbejdsgiveren, dvs. den offentlige myndighed, virksomheden, organisationen mv. eller medarbejderen, dvs. den fysiske person. Nærværende afsnit vedrører de momenter, der skal lægges vægt på ved vurderingen af, hvorvår en fysisk person – f.eks. en medarbejder hos en offentlig myndighed, virksomhed eller organisation – bliver selvstændig dataansvarlig. Det vil i hvert tilfælde bero på en konkret vurdering, om medarbejderen bliver selvstændig dataansvarlig. Dette gør sig særligt gældende i situationer, hvor der er klare holdepunkter for at sige, at vedkommende behandler oplysningerne til egne formål, der ligger klart uden for arbejdsgiverens aktiviteter, jf. også princippet i forordningens artikel 28, stk. 10. Som et eksempel på, at en fysisk person behandler personoplysninger til egne formål, og klart uden for arbejdsgiverens aktiviteter, kan nævnes den situation, hvor en sundhedsperson foretager uberettigede opslag i et centralt system, f.eks. Sundhedsplatformen, til rent private formål. Dette kunne eksempelvis være opslag om helbredsoplysninger vedrørende et familiemedlem. Dette kunne også være tilfældet i situationer, hvor medarbejderen har handlet i det, som den pågældende medarbejder fejlagtigt har vurderet, var arbejdsgiverens interesse, men hvor arbejdsgiveren har givet klare instrukser om det modsatte.

At den fysiske persons behandling af oplysningerne sker i virksomhedens interesse betyder således ikke nødvendigvis, at det er arbejdsgiveren, der skal anses som dataansvarlig. Omvendt betyder det ikke nødvendigvis at den fysiske person skal anses som dataansvarlig, alene fordi denne handler imod en instruks fra arbejdsgiveren. Begge momenter bør imidlertid indgå i en samlet vurdering af, om medarbejderen bliver selvstændig dataansvarlig eller ej."

Ansatte sundhedspersoner kan således ensidigt, med sine handlinger pådrage sig en rolle som dataansvarlig.

Databeskyttelsesforordningens artikel 2, stk. 2, litra c, finder ikke anvendelse

Selvom en sundhedspersons uberettigede registeropslag kan være motiveret i rent private forhold, f.eks. privat nysgerrighed vedrørende et familiemedlems helbred, vil bestemmelsen i artikel 2, stk. 2, litra c (om rent personlige eller familiemæssige aktiviteter, der undtages fra for-

3 Bestemmelsen har følgende ordlyd: "Hvis en databehandler overtræder denne forordning ved at fastlægge formålene med og hjælpemidlerne til behandling, anses databehandleren for at være en dataansvarlig for så vidt angår den pågældende behandling, uden at dette berører artikel 82, 83 og 84."

4 "Bødevejledning - Udmåling af bøder til fysiske personer", Datatilsynet, februar 2022. Vejledningen kan findes på tilsynets hjemmeside: https://www.datatilsynet.dk/databeskyttelse/vejledninger.

ordningens anvendelsesområde), imidlertid ikke finde anvendelse. Det skyldes, at sådanne opslag generelt ikke i kan siges at være normale og legitime private aktiviteter[5].

Relevante regler i databeskyttelsesforordningen

Uanset om det er sundhedspersonen eller arbejdsgiverorganisationen, der anses for at være dataansvarlig, gælder det grundlæggende databeskyttelsesretlige krav om, at der skal være et behandlingsgrundlag i databeskyttelsesforordningens artikel 6, ligesom betingelserne i artikel 9 for behandling af særlige kategorier af personoplysninger efter omstændighederne skal være opfyldt.

Arbejdsgiverorganisationen skal som dataansvarlig således leve op til de grundlæggende hjemmelsbestemmelser i artikel 6 og 9, men også til bestemmelserne i databeskyttelsesforordningens afdeling 2 om personoplysningssikkerhed, herunder artikel 32, hvorefter der skal sikres bl.a. "passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici".

Efter omstændighederne skal der f.eks. sikres "vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester" og "en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed."

Artikel 32, stk. 4, fastslår endvidere følgende:

> "Den dataansvarlige og databehandleren tager skridt til at sikre, at enhver fysisk person, der udfører arbejde for den dataansvarlige eller databehandleren, og som får adgang til personoplysninger, kun behandler disse efter instruks fra den dataansvarlige, medmindre behandling kræves i henhold til EU-retten eller medlemsstaternes nationale ret."

Praksis hos andre europæiske datatilsyn

Datatilsynet har som nævnt spurgt de andre europæiske datatilsynsmyndigheder, hvordan disse håndterer sager vedrørende ansatte, som misbruger en betroet adgang til et register, herunder om rette ansvarssubjekt er arbejdsgiverorganisationen eller den ansatte.

Svarene fra tilsynsmyndighederne i Ungarn, Holland, Bulgarien, Slovakiet, Irland, Norge, Finland, Tyskland, Frankrig og Spanien, viser ikke et entydigt billede.

Fælles for svarene er dog, at de respektive tilsynsmyndigheder har behandlet få eller ingen sager om emnet, og at sagerne, som tilsynsmyndighederne refererer til, ikke i alle tilfælde synes sammenlignelige. Flere af tilsynene henviser til enkeltsager, hvor tilsynet enten valgte at rette ansvaret mod arbejdsgiverorganisationen eller den ansatte. Det kan dog næppe alene på denne baggrund konkluderes, at de pågældende tilsyn har en fastlagt praksis, netop fordi der henvises til så få sager.

På baggrund af Datatilsynet forespørgsel må det umiddelbart konkluderes, at der blandt de europæiske datatilsynsmyndigheder ikke er en ensartet tilgang til spørgsmålet om, hvem der er rette ansvarssubjekt, og at svarene ikke er retningsgivende for Datatilsynets vurdering. I

5 Der henvises til den kommenterede databeskyttelsesforordning, s. 218, hvor følgende fremgår: "Udtrykket 'rent personlige eller familiemæssige aktiviteter' må dække over en række forskellige typer af behandlinger, som privatpersoner foretager. Der skal være tale om sædvanlige og legitime private aktiviteter, således at bestemmelsen ikke anvendes til at omgå reglerne for lovlig behandling."

den forbindelse er der ikke kun lagt vægt på, at der ikke synes at være en klar linje for håndteringen af disse typer sager, men også på, at samfundsforholdene – herunder digitaliseringsgraden – i de pågældende lande ikke ubetinget er sammenlignelige med danske forhold.

Konklusion

Der er ikke på baggrund af hverken svarene fra de europæiske datatilsyn eller på baggrund af dansk praksis umiddelbart belæg for at ændre den tilgang, som er beskrevet i Datatilsynets bødevejledning og i den kommenterede databeskyttelsesforordning.

Udgangspunktet bør således fortsat være, at det er arbejdsgiverorganisationen, der er dataansvarlig, medmindre der er klare holdepunkter for at sige, at sundhedspersonens registeropslag er sket til varetagelse af egne formål, der ligger klart uden for organisationens aktiviteter.

I en række tilfælde vil det ikke umiddelbart være muligt at fastslå, om formålet med et registeropslag er sket til varetagelse af egne, private formål. Det gælder f.eks., hvor der i sygehusregi slås op på personer, som er eller for nylig har været patienter det pågældende sted. En række forhold kan dog indikere, at opslag(ene) ikke er sagligt begrundede, f.eks. hvis der er foretaget et meget stort antal opslag på den samme person, hvis opslagene er foretaget uden for normal arbejdstid, eller hvis der er forhold, der i øvrigt kunne indikere en usaglig beveggrund for opslagene.

I tilfælde, hvor sundhedspersonen må anses for dataansvarlig, er det ikke udelukket, at arbejdsgiverorganisationen samtidig kan være ansvarlig efter forordningens artikel 32. Det må således overvejes, om organisationen – selv hvor sundhedspersonen foretager uberettigede registeropslag, som vedkommende er dataansvarlig for – har levet op til sine forpligtelser efter artikel 32.

3. Sanktionsniveau

Henvendelser fra anklagemyndigheden

Anklagemyndigheden har rejst spørgsmål om forholdet mellem databeskyttelsesregleme og straffelovens § 155[6] (embedsmisbrug) i tilfælde af uberettigede registeropslag, herunder om der kan fastsættes nærmere retningslinjer for sanktioneringen af forhold, som kan subsumeres under begge bestemmelser. Der er også rejst spørgsmål om, om bagatelgrænsen i straffelovens § 155 kan overføres til de databeskyttelsesretlige regler. Rigsadvokaten har beskrevet bagatelgrænsen i relation til registeropslag på bl.a. følgende måde:

> "Det fremgår af indledningen til afsnittet om straffelovens kapitel 16 i den kommenterede straffelov, 11. udgave, at disciplinær indskriden ofte vil være tilstrækkelig og foretrækkes frem for offentlig tiltale i ordinære tilfælde af tilsidesættelse af tjenestepligter, således at tiltale efter straffeloven kun rejses i grovere tilfælde.
>
> ...

6 "Misbruger nogen, som virker i offentlig tjeneste eller hverv, sin stilling til at krænke privates eller det offentliges ret, straffes han med bøde eller fængsel indtil 4 måneder. Sker det for at skaffe sig eller andre uberettiget fordel, kan fængsel indtil 2 år anvendes."

> ...[O]pslag, der er foretaget alene af nysgerrighed, og hvor medarbejderen ikke foretager noget i anledning af oplysningerne, som hovedregel ikke har en sådan grovhed, at der kan blive tale om et ansvar efter straffelovens § 155."[7]

Spørgsmålet er, om et opslag, der falder under bagatelgrænsen i straffelovens § 155, også kan anses for at være en straffri overtrædelse af de databeskyttelsesretlige regler, eller om sager, der falder under bagatelgrænsen i § 155, i stedet skal straffes efter databeskyttelsesforordningen.

Derudover har anklagemyndigheden mere generelt efterspurgt retningslinjer for sanktioneringen af registermisbrug (udgangspunkter for bøder), og for forelæggelse af sager for Datatilsynet.

Bagatelgrænsen i straffelovens § 155

Databeskyttelsesforordningen indeholder ikke et kriterium om grovhed. De databeskyttelsesretlige regler vil således i mange tilfælde kunne være overtrådt, selvom forholdet ikke har en sådan alvor, at gerningsindholdet i § 155 er realiseret. At databeskyttelsesforordningen er overtrådt, er dog ikke i alle tilfælde ensbetydende med, at forholdet er *strafværdigt*. Derimod vil forholdet kunne "sanktioneres" på anden måde, som det også er tilfældet med Datatilsynets øvrige sager, hvor der ofte er anledning til kritik, men kun i de færreste sager er anledning til politianmeldelse.

I praksis vil der derfor i mange tilfælde kunne være et vist sammenfald mellem bagatelgrænsen i straffelovens § 155 og den grovhed, som Datatilsynets sager kræver, før tilsynet finder, at forholdet er strafværdigt efter databeskyttelsesreglerne.

Ligesom bagatelgrænsen i straffeloven imidlertid ikke kan defineres nærmere, kan grænsen for strafværdige forhold efter de databeskyttelsesretlige regler heller ikke beskrives nærmere, end at der kræves forhold af en vis alvor og grovhed. I praksis vil der dog som nævnt kunne anerkendes et sammenfald til en vis grad.

Straffelovens § 155 og databeskyttelsesforordningen regulerer dog ikke i alle detaljer de samme forhold, og der kan derfor næppe siges at være et direkte "vertikalt hierarki" i reglerne, således at sager, der falder under straffelovens bagatelgrænse altid opfanges af databeskyttelsesforordningen:

Det er klart, at der er forhold, der *ikke* kan kategoriseres som embedsmisbrug, men som alligevel vil være en uberettiget behandling af personoplysninger (f.eks. et tilfælde af registermisbrug, som ikke er alvorligt nok til at skulle straffes efter straffeloven). Men det må også være klart, at der er forhold, som *kan* kategoriseres som embedsmisbrug, men som ikke nødvendigvis vil udgøre en overtrædelse af det databeskyttelsesretlige krav om behandlingshjemmel (som eksempel kan nævnes tilfælde, som slet ikke indebærer nogen behandling af personoplysninger, men dog vil det formentlig også gælde den situation, hvor f.eks. en polititjenestemand uretmæssigt behandler oplysninger om sig selv i politiets systemer).

Politiets og anklagemyndighedens forelæggelsespraksis for Datatilsynet

7 Rigsadvokatens udateret notat med titlen "Notat om praksis vedrørende bagatelgrænsen i str. § 155"

Idet der ikke er fuldstændigt sammenfald mellem de livsforhold, som straffelovens § 155 og databeskyttelsesforordningen regulerer, kan bagatelgrænsen i § 155 ikke anvendes som kriterium for, hvornår straffesager med databeskyttelsesretligt indhold bør forelægges Datatilsynet.

Det er dog hensigtsmæssigt, at der i politiet og anklagemyndigheden fastsætte visse rammer for, hvornår Datatilsynet inddrages i straffesager. Der ses således fra tid til anden eksempler på, at Datatilsynet høres over forhold, som ret oplagt ikke er strafværdige.

Straks nedenfor er der taget stilling til nogle typesituationer, der vurderes ud fra strafværdighed, og i bilaget til dette notat er der fastsat nogle udgangspunkter for bødepåstande. Der vil kunne tages udgangspunkt i disse typetilfælde og de tilhørende bødepåstande, når politi/anklagemyndighed skal vurdere, om sagen skal forelægges for Datatilsynet, således at klare tilfælde, som ifølge bilaget ikke er strafværdige, ikke skal forelægges Datatilsynet.

Bødepåstande i notatets bilag

Der fastsættes nogle vejledende udgangspunkter for bødepåstande i registermisbrugssager. Der henvises til notatets bilag. Udgangspunkterne i bilaget angår alle registermisbrug og er ikke begrænset til sundhedssektoren.

Der henvises til skemaet i bilaget, der omfatter følgende fire forskellige situationer:

1) opslag på oplysninger om sig selv

2) opslag på oplysninger om personer, som man tager vare på (mindreårige børn, demente forældre, personer under ens værge, mv.)

3) opslag på andre personer (hvis oplysninger man ikke har nogen rimelig adkomst til)

4) opslag på de nævnte personer *med efterfølgende brug/videregivelse/offentliggørelse*.

Bilaget forholder sig herudover til bøder i situationer med *enkelte*, *flere* eller *mange* opslag i hver af de fire typetilfælde.

Der er taget udgangspunkt i den gældende bødevejledning[8] vedr. fysiske personer, hvoraf det fremgår, at offentliggørelse af artikel 6-oplysninger bør sanktioneres med bøder på 10-15.000 kr., og videregivelse af artikel 9-oplysninger bør sanktioneres med bøder på 15-25.000 kr.

Der sondres dog i bilaget ikke mellem, om der er tale om artikel 6- eller 9-oplysninger. I stedet skal der anlægges en mere overordnet vurdering af oplysningernes følsomhed i forbindelse med uberettigede opslag og evt. senere brug. Konkret kan denne vurdering betyde, at artikel 6-oplysninger anses for følsomme, hvis sagens omstændigheder konkret tilsiger det, og omvendt, at behandling af artikel 9-oplysninger ikke anses for alvorligt, afhængig af hvilken konkret oplysning og kontekst, der er tale om.

Ifølge bilaget vil en række tilfælde af registermisbrug anses for straffri efter databeskyttelsesforordningen. Det betyder ikke, at disse tilfælde er tilladelige. Der vil således stadig være tale

8 "Bødevejledning - Udmåling af bøder til fysiske personer", Datatilsynet, februar 2022. Vejledningen kan findes på tilsynets hjemmeside: https://www.datatilsynet.dk/databeskyttelse/vejledninger.

om en overtrædelse af de databeskyttelsesretlige regler, som kan sanktioneres på anden vis, ligesom der efter omstændighederne vil kunne være tale om overtrædelser af særregler (f.eks. sundhedslovens bestemmelser om anvendelse af sundhedsregistre), ligesom der i særlige tilfælde vil kunne foreligge embedsmisbrug efter straffeloven § 155. Ofte vil sådanne tilfælde også rammes af disciplinære sanktioner.

Bilagets udgangspunkter søger at ramme en passende balance mellem, at der på den ene side skal være en vis rimelighed i sanktionsniveauet – også i forhold til danske retspraksis i øvrigt – og på den anden side, at bødeniveauet efter databeskyttelsesforordningen reelt skal virke effektivt og afskrækkende, og at sanktionsniveauet derfor skal hæves markant i forhold til niveauet efter databeskyttelsesloven.

Der tages forbehold for, at bødesatserne er et vejledende udgangspunkt, der kan op- og nedjusteres afhængig af omstændighederne i den konkrete sag.

Det følger af databeskyttelsesforordningens præambelbetragtning nr. 150, at der skal tages højde for det generelle indkomstniveau i medlemsstaten og personens økonomiske situation, når bødestørrelsen skal fastlægges. Den tiltaltes indkomstforhold vil således skulle indgå i udmålingen af bødestørrelsen. Datatilsynet har som udgangspunkt ikke kendskab til indkomstforholdene, når tilsynet indstiller sagen til politiet. Datatilsynets indstillinger tager derfor udgangspunkt i et gennemsnitligt indtægtsniveau. Bødestørrelsen vil herefter kunne justeres i opadgående eller nedadgående retning, hvis der fremkommer oplysninger om særligt lav eller særligt høj indkomst.

4. Genoptagelse af Datatilsynets sager

De sager, som Datatilsynet har stillet i bero – inklusive sager, som ligger hos politi/anklagemyndighed – genoptages nu og vurderes af tilsynet efter retningslinjerne i dette notat og i bilaget.

/ MJG 7. juli 2022

Bilag

Standardiserede bødetakster for registermisbrug (ikke kun på sundhedsområdet)

Type behandling	Overtrædelsens karakter Der sondres ikke mellem, om der er tale om artikel 6- eller 9-oplysninger. I stedet skal der anlægges en mere overordnet vurdering af oplysningernes følsomhed i forbindelse med uberettigede opslag og evt. senere brug.*	**Bøde ved få tilfælde** Få eller enkeltstående tilfælde (normalt 1-10 opslag), eller opslag, der på anden måde er indskrænket eller afgrænset i omfang, periode, antal og karakter af tilgåede oplysninger mv.	**Bøde ved flere tilfælde** Typisk mellem 10 og 50 tilfælde, eller hvor aktiviteten f.eks. på grund af dens tidsmæssige udstrækning el.lign. kan sidestilles hermed	**Bøde ved mange tilfælde** F.eks. over 50 opslag, eller hvor der er tale om færre opslag, men hvor registermisbruget har stået på i en lang periode, eller på anden måde er af meget omfattende karakter
Opslag på sig selv	Den ansatte slår alene op på oplysninger om sig selv.	**Ikke strafværdigt efter databeskyttelsesforordningen****		
Opslag på nær familie til eget brug (uden videregivelse el.lign.)	Den ansatte slår op på nære familiemedlemmer, som vedkommende typisk har et ansvar for, f.eks. en dement forælder på plejehjem, mindreårige børn, eller personer, som den ansatte er værge for.	**Ikke strafværdigt efter databeskyttelsesforordningen****		
Opslag på andre til eget brug (uden videregivelse el.lign.)	Den ansatte slår op på familiemedlemmer eller bekendte, som vedkommende ikke har ansvar for, og hvor der ikke kan siges, at være rimelig grund til opslaget (f.eks. voksne børn, tidligere ægtefæller, bekendte). Omfatter også restgruppen af alle andre personer, som den ansatte ikke kender.	**0-10.000 kr.**	**5-15.000 kr.**	**10-20.000 kr.**
Opslag på andre end sig selv med efterfølgende videregivelse	Disse tilfælde omfatter principielt alle andre registrerede end den ansatte selv, hvor der sker videregivelse til bestemte personer eller offentliggørelse. Hvis videregivelsen sker til den person, der er slået op på (og ikke til andre), kan det efter omstændighederne medføre, at forholdet ikke anses for strafværdigt.	**10-25.000 kr.**	**20-50.000 kr.**	**40-100.000 kr. eller efter omstændighederne fængsel*** **

* Konkret kan denne vurdering betyde, at artikel 6-oplysninger anses for følsomme, hvis sagens omstændigheder konkret tilsiger det, eller omvendt, at behandling mv. af artikel 9-oplysninger ikke anses for følsomt.

** Der vil i disse tilfælde efter omstændighederne kunne være tale om overtrædelser af særregler (f.eks. sundhedslovens bestemmelser om anvendelse af sundhedsregistre), ligesom der i særlige tilfælde vil kunne foreligge embedsmisbrug efter straffelovens § 155. Registermisbrug af vil endvidere kunne medføre ansættelsesretlige sanktioner eller (på sundhedsområdet) efter omstændighederne autorisationsfratagelse.

*** Det er i forarbejderne til databeskyttelseslovens § 41, stk. 2, forudsat, 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."

Rigsadvokaten, den 12. august 2022

RIGSADVOKATEN

/ Rigsadvokaten