

Udskriftsdato: 26. december 2025

CIR1H nr 9061 af 05/02/2020 (Historisk)

## Rigsadvokatmeddelelsen, afsnittet: Databeskyttelse

Ministerium: Justitsministeriet

Journalnummer: CMS VB 7845

### Senere ændringer til forskriften

CIR1H nr 9751 af 27/09/2021

# Rigsadvokatmeddelelsen, afsnittet: Databeskyttelse

## 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 tiltaleespørgsmålet. Se nærmere under pkt. 3.5.2.1.*
- *At sager om overtrædelse af databeskyttelsesreglerne er et anklagerfagligt fokusområde i retspraksis, hvilket bl.a. medfører, at*
  - *Sagerne ikke må afgøres med bødeforelæg, før sanktionsniveauet er tilstrækkelig afklaret i retspraksis.*
  - *Sager, hvor anmeldelsen er indgivet af Datatilsynet, skal behandles i samarbejde mellem politikredsen og den regionale statsadvokat. Se nærmere under pkt. 3.4.4.*
  - *Politikredsen skal forelægge tiltaleespørgsmålet (herunder straffpåstanden) for den regionale statsadvokat i alle sager om overtrædelse af databeskyttelsesreglerne. Se nærmere under pkt. 3.6.*
  - *Sager, hvor anklagemyndigheden ikke har fået medhold i tiltalen og/eller straffpåstanden, skal forelægges for den regionale statsadvokat inden ankefristens udløb. Se nærmere under pkt. 6.*
  - *Endelige domme skal indberettes til Rigsadvokaten, herunder med henblik på optagelse i Vidensbasen. Se nærmere under pkt. 6.*
- *Muligheden for at nedlægge påstand om rettighedsfrakendelse. Se nærmere under pkt. 5.5.*
- *At Datatilsynet skal inddrages ved spørgsmål om eventuel anke. Se nærmere under pkt. 6.*
- *At Datatilsynet skal orienteres om og have kopi af alle endelige afgørelser.*

## 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 overholdelsen af databeskyttelsesforordningen, databeskyttelsesloven og regler udstedt i medfør heraf. Der henvises til Datatilsynets hjemmeside [www.datatilsynet.dk](http://www.datatilsynet.dk).

Borgere mv. kan klage over eller indberette en overtrædelse af det databeskyttelsesretlige regelsæt 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, 3.4 og 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 Center for Databeskyttelse 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. Listen over kontaktpersoner findes på anklagemyndighedens Vidensbase.

Rigspolitiets Center for Databeskyttelse 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 Center for Databeskyttelse 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/generelt-om-databeskyttelse/danmark-eu-og-resten-af-verden/internationale-virksomheder/>.

### ***3.2.3. Bistand fra Rigspolitiets National Cyber Crime Center (NC3)***

I konkrete sager kan Rigspolitiets Nationale Cyber Crime Center (NC3) bistå Datatilsynet og politikredse under efterforskningen, herunder i forbindelse med bevissikring, gennemgang af beslaglagte datamedier mv.

### ***3.3. Anklagerfagligt fokusområde***

Databeskyttelse er et anklagerfagligt fokusområde i retspraksis. Det indebærer blandt andet, at sager, som er anmeldt af Datatilsynet, skal behandles i samarbejde mellem politikredsen og den regionale statsadvokat, og at politikredsen skal forelægge tiltalerspørgsmålet (herunder strafpåstanden) for den regionale statsadvokat i alle sager om overtrædelse af databeskyttelsesreglerne, se nærmere nedenfor pkt. 3.4.4 og 3.6.

Sager, hvor politikredsen vurderer, at der kan ske henlæggelse eller påtaleopgivelse efter retsplejelovens §§ 749 eller 721, skal dog ikke forelægges for den regionale statsadvokat, 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.

Politikredsen skal endvidere forelægge alle domme, hvor anklagemyndigheden ikke har fået fuldt medhold (herunder i strafpåstanden), for den regionale statsadvokat 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 tiltaleespørgsmålet, herunder en indstilling om sanktionsspørgsmålet, se nærmere pkt. 3.5.2.

### ***3.4.3. 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.
- 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.

### ***3.4.4. Samarbejde mellem politikredsen og den regionale statsadvokat***

Sager, som er anmeldt af Datatilsynet til en politikreds, vil typisk være omfangsrige, komplekse og/eller af principiel karakter. Derfor skal sagerne fra et tidligt tidspunkt behandles i et tæt samarbejde mellem politikredsen og den regionale statsadvokat. Hurtigst muligt efter modtagelsen af anmeldelsen fra Datatilsynet skal politikredsen derfor tage kontakt til den regionale statsadvokat med henblik på nærmere aftale om samarbejdets omfang, der afhænger af sagens karakter.

Det nærmere indhold af et sådant samarbejde fastlægges ved konkret aftale mellem politikredsen og statsadvokaten og kan f.eks. bestå i, at statsadvokaten løbende følger sagens behandling og yder faglig rådgivning og sparring. Statsadvokaterne skal endvidere tage initiativ til at koordinere behandlingen af sager, som omhandler samme type af overtrædelser.

Datatilsynet orienterer generelt Rigsadvokatens Databeskyttelsesenhed ved indgivelse af politianmeldelser og sender ligeledes politianmeldelserne i kopi, jf. ovenfor pkt. 3.2.1. På baggrund heraf vil Rigsadvokaten tillige orientere den relevante politikreds og den regionale statsadvokat om de konkrete sager, således at det pågældende samarbejde sikres.

## ***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. 4.2.2.
- 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.

##### ***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 foreløbigt vurderer, at der er tale om et forhold, der af Datatilsynet ville blive afvist eller sanktioneret med tilsynets korrigerende beføjelser efter databeskyttelsesforordningens artikel 58, 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 Center for Databeskyttelse 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 tiltaleespørgsmålet. 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 tiltaleespørgsmålet, 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. 4.2.2.
- 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. Forelæggelse for de regionale statsadvokaturer***

Afklaring af, hvornår der er tale om en strafbar overtrædelse af databeskyttelsesreglerne og af straffniveauet, er indtil videre et anklagerfagligt fokusområde i retspraksis, jf. ovenfor pkt. 3.3. Politikredsen skal derfor forelægge tiltaleespørgsmålet (herunder strafpåstanden) for den regionale statsadvokat i alle sager om overtrædelse af databeskyttelsesreglerne.

Sager, hvor politikredsen vurderer, at der kan ske henlæggelse eller påtaleopgivelse efter retsplejelovens §§ 749 eller 721 skal dog ikke forelægges for den regionale statsadvokat, 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 den regionale statsadvokat skal politikredsen høre Datatilsynet, inden der træffes afgørelse om tiltaleespørgsmålet, jf. ovenfor pkt. 3.5.2.1. I tilfælde af uenighed mellem anklagemyndigheden og Datatilsynet følges retningslinjerne i Rigsadvokatmeddelelsens afsnit ”samarbejdet med særmyndigheder i særlovssager”.

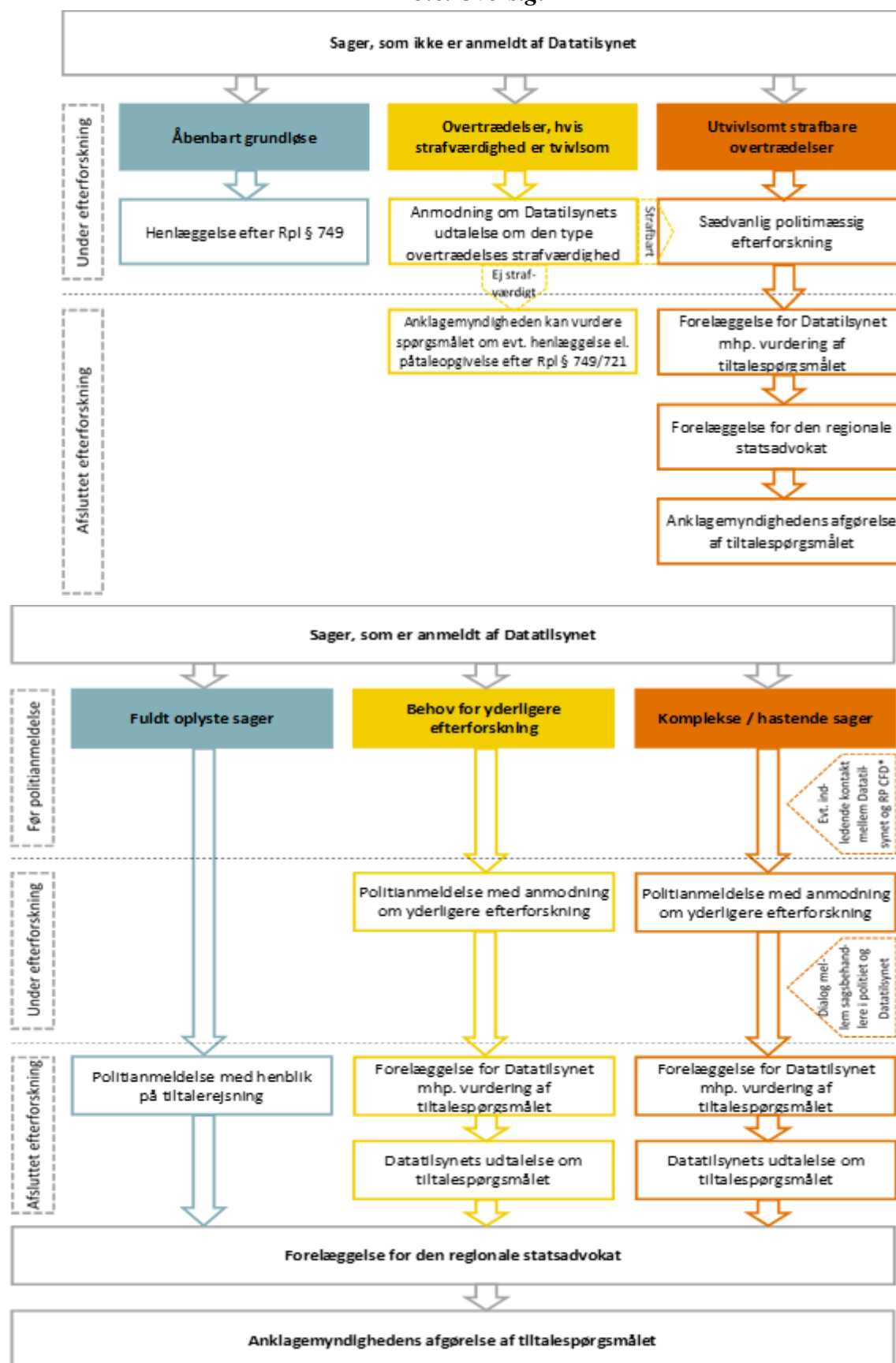
Anklagemyndigheden skal orientere Datatilsynet ved tiltalerejsning.

### ***3.7. 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 Rigsadvokatmeddelelsens afsnit om overtrædelse af databeskyttelsesreglerne.

### 3.8. Oversigt



## 4. Jura

### *4.1. Anvendelsesområde for 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 behandling af personoplysninger, der foretages af offentlige myndigheder og private virksomheder, foreninger mv.

#### *4.1.1. Materielt og territorielt anvendelsesområde*

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 også billeder, lyd/stemme, fingeraftryk og genetiske kendetegn, og det er uden betydning, om identifikationsoplysningerne er alment kendt eller umiddelbart tilgængelige. Også de tilfælde, hvor det alene for den indviede vil være muligt at forstå, hvem en oplysning vedrører, er omfattet af definitionen.

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

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 "dataansvarlig" og "databehandler" nedenfor pkt. 4.4.

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 udover 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 forordningens artikel 4 for definitioner.

## **4.2. Databeskyttelsesforordningen og databeskyttelsesloven**

### **4.2.1. Oversigt over de grundlæggende begreber og regler i databeskyttelsesforordningen**

Databeskyttelsesforordningen indeholder bl.a.:

- Regler for hvornår der må behandles personoplysninger, også kaldet behandlingsgrundlag, jf. forordningens artikel 6 -10.
  - Begrebet ”behandling” omfatter enhver form for håndtering af oplysninger, f.eks. indsamling, registrering, systematisering, opbevaring, tilpasning, søgning, brug, videregivelse, formidling og sletning, jf. definitionen i forordningens artikel 4, nr. 2.
  - Forordningen suppleres af behandlingsreglerne i databeskyttelseslovens kapitel 3.
- 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, jf. forordningens kapitel IV.
  - Begrebet ”dataansvarlig” omfatter enhver 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.
  - Se nærmere nedenfor om dataansvarlige og databehandlere under pkt. 4.4.
- Regler om den registreredes rettigheder, jf. forordningens kapitel III og artikel 34.
  - Den registrerede er den person, oplysningerne vedrører, og vedkommende har forskellige rettigheder, herunder ret til at få besked om, at der behandles oplysninger 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.
  - Forordningen suppleres af databeskyttelseslovens §§ 22 og 23.
- Regler om behandlingssikkerhed, jf. forordningens artikel 32.
- Regler om overførsel af personoplysninger til tredjelande eller internationale organisationer, jf. forordningens kapitel V.

### **4.2.2. Typer af personoplysninger**

Der gælder forskellige betingelser og procedurer for behandling af personoplysninger afhængig af oplysningernes karakter:

- 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 behandling af personoplysninger, der ikke reguleres af særlovgivning (bl.a. databeskyttelsesloven), skal ske i overensstemmelse med forordningens 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.

Som udgangspunkt gælder der et forbud mod behandling af følsomme personoplysninger, jf. forordningens artikel 9, stk. 1, medmindre der kan identificeres en undtagelse til forbuddet i enten forordningens artikel 9, stk. 2, eller bestemmelser, der gennemfører artikel 9.

Ved enhver behandling af følsomme personoplysninger skal der, udover forordningens artikel 9, stk. 2, eller bestemmelser, der gennemfører artikel 9, tillige være et lovligt grundlag for behandlingen i forordningens artikel 6. Der henvises til Datatilsynets informationstekst herom <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/nov/behandling-af-foelsomme-oplysninger/>.

**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](http://www.datatilsynet.dk) for en nærmere beskrivelse af reglernes indhold.

#### ***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 traditionelle sager, som er under efterforskning, eller hvor der tages stilling til strafansvar og strafudmåling. Udover 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. Roller og ansvar – dataansvarlig eller databehandler***

I databeskyttelsesretten sondres der mellem dataansvarlige og databehandlere. Der gælder forskellige forpligtelser efter databeskyttelsesforordningen/databeskyttelsesloven 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 reglerne i databeskyttelsesforordningen. 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 Data-tilsynets hjemmeside.

#### ***4.5. 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 følges.

#### ***4.6. 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 følges, jf. afsnittet i Rigsadvokatmeddelelsen om strafansvar for juridiske personer, pkt. 3.1.3.

## **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.

I artikel 83, stk. 2, er 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. 5.3.

For så vidt angår straffniveauet 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 bodemaksimum 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.

Når den samlede globale årlige omsætning skal fastlægges, kan det være relevant at foretage en nærmere analyse af en eventuel koncerns opbygning. Det følger i den forbindelse af forordningens præambelbetragtning 150, at der ved denne vurdering skal tages udgangspunkt i retspraksis på det konkurrenceretlige område i relation til artikel 101 og 102 i Traktaten om Den Europæiske Unions Funktionsmåde.

Ved bødeudmålingen i relation til privatpersoner er der ikke på samme måde 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.

Se nærmere om strafudmåling i relation til offentlige myndigheder under pkt. 5.6.

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.

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, og det er således ikke muligt på nuværende tidspunkt at give mere konkrete retningslinjer for bødernes størrelse i disse sager. Afklaring af straffniveauet er derfor indtil videre et anklagerfagligt fokusområde i retspraksis med henblik på, at Rigsadvokaten på sigt kan udarbejde nogle mere konkrete retningslinjer til anklagemyndigheden om strafudmålingen i sager om overtrædelse af databeskyttelsesreglerne. Når der i retspraksis på forskellige områder er fastlagt et bødeniveau, vil Datatilsynet desuden begynde at kunne udstede administrative bødeforelæg i ukomplerede sager uden bevismæssige tvivlsspørgsmål, jf. databeskyttelseslovens § 42.

## ***5.2. 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 straffniveauet 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.

### ***5.3. 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 adfærdscodekser 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.

#### ***5.4. Fængselsstraf***

Der er efter databeskyttelseslovens § 41, stk. 1 og 2, mulighed for at idømme fængselsstraf for overtrædelse af de straffelagte 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.

#### ***5.5. Påstand om 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.

#### ***5.6. Sanktionsspørgsmålet i forhold til offentlige myndigheder***

##### ***5.6.1. Generelt om sanktionsspørgsmålet i forhold til offentlige myndigheder***

Det er forudsat i 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 (lovforslagets § 41), 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 (lovens § 41, stk. 1, nr. 4-6 og stk. 2, nr. 2-5, samt nr. 1 vedrørende §§ 5-13, 20 og 21).

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. 5.3.

## **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.

### ***6.2. Underretning af statsadvokaten***

Da databeskyttelse er et anklagerfagligt fokusområde i retspraksis, jf. ovenfor pkt. 3.3, skal politikredsen forelægge alle domme, hvor anklagemyndigheden ikke har fået fuldt medhold (herunder i strafpåstanden), for den regionale statsadvokat inden ankefristens udløb.

### ***6.3. Afgørelser til Vidensbasen***

Da databeskyttelse er et anklagerfagligt fokusområde i retspraksis, jf. ovenfor pkt. 3.3, skal alle endelige domme sendes 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.)

### 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)

### 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

*Rigsadvokaturen, den 5. februar 2020*

RIGSADVOKATEN

/ Rigsadvokaten