

Udskriftsdato: mandag den 12. januar 2026

CIR1H nr 9596 af 25/05/2018 (Historisk)

Rigsadvokatmeddelelsen, afsnittet: Sager om overtrædelse af databeskyttelsesreglerne

Ministerium: Justitsministeriet

Journalnummer: CMS VB 7128

Senere ændringer til forskriften

CIR1H nr 9061 af 05/02/2020

Rigsadvokatmeddelelsen, afsnittet: Sager om overtrædelse af databeskyttelsesreglerne

25. maj 2018

1. Overblik og tjekliste

Politiet skal under efterforskningen være særligt opmærksom på:

- I relevant omfang at foretage en indledende bevissikring, se nærmere under pkt. 2.2.

Anklagemyndigheden skal være særligt opmærksom på:

- At der skal indhentes en udtalelse fra Datatilsynet i alle straffesager om overtrædelse af databeskyttelseslovgivningen, herunder i forhold til sanktionsspørgsmålet.
- At sager om overtrædelse af databeskyttelseslovgivningen er et anklagerfagligt fokusområde i retspraksis, hvilket bl.a. medfører, at
 - Sagerne ikke må afgøres med bødeforelæg, før sanktionsniveauet er tilstrækkelig afklaret i retspraksis
 - Politikredsene skal forelægge alle sager for den regionale statsadvokat med henblik på vurdering af strafpåstanden. Se nærmere under pkt. 3.3.
 - Politikredsene skal drøfte ankespørgsmålet med den regionale statsadvokat i alle byretssager, hvis anklagemyndigheden ikke får fuldt ud medhold i strafpåstanden. 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.
- Muligheden for at nedlægge påstand om rettighedsfrakendelse. Se nærmere under pkt. 5.5.
- At Datatilsynet skal inddrages ved spørgsmål om eventuel anke.
- At Datatilsynet skal orienteres om samt have kopi af alle endelige afgørelser.

2. Politiets efterforskning og sagsbehandling

2.1 Grænseoverskridende kriminalitet/international retshjælp

Sager om overtrædelse af databeskyttelseslovgivningen kan – f.eks. når det drejer sig om ulovlige offentliggørelser 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. Rigsadvokaten er i færd med at udarbejde et nyt afsnit i Rigsadvokatmeddelelsen om International retshjælp. Spørgsmål vedrørende international retshjælp kan rettes til International enhed hos Rigsadvokaten.

Sager om overtrædelse af databeskyttelseslovgivningen, der vedrører virksomheder etableret i andre EU-lande, vil typisk blive håndteret af myndighederne i den pågældende medlemsstat. Det kan dog alligevel blive nødvendigt, at politiet yder Datatilsynet bistand i forbindelse med den nationale efterforskning.

2.2. Indledende bevissikring

I det omfang der ikke er sket en eventuel bevissikring i samarbejde med Datatilsynet forud for modtagelsen af en politianmeldelse, skal politiet i sager om overtrædelser af databeskyttelseslovgivningen i relevant omfang så hurtigt som muligt foretage en indledende bevissikring.

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

2.3. Rigspolitiets bistand

2.3.1. 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.

2.3.2. Rigspolitiets Databeskyttelsesenhed

Rigspolitiets Databeskyttelsesenhed varetager en række opgaver knyttet til politiets efterlevelse af databeskyttelsesretten og har i den forbindelse bl.a. fokus på løbende at følge retsudviklingen nationalt og internationalt. I forbindelse med efterforskning af sager om overtrædelse af databeskyttelsesreglerne og under straffesagens forberedelse kan politikredsen rette henvendelse til Rigspolitiets Databeskyttelsesenhed vedrørende afklaring af ethvert spørgsmål af databeskyttelsesretlig karakter, som sagens behandling måtte give anledning til. Enheden kan i den forbindelse ikke bistå i forhold til rent anklagerfaglige forhold, men kan f.eks. bistå med juridisk informationssøgning, afklaring af praktiske spørgsmål og afdækning af databeskyttelsesretlige tvivlsspørgsmål mv.

Databeskyttelsesenheden – og dansk politis databeskyttelsesrådgiver – fungerer i øvrigt som politiets kontaktpunkt for Datatilsynet.

2.4. Datatilsynets bistand

I forbindelse med efterforskningen af sager om databeskyttelse og under straffesagens forberedelse kan politikredsen rette henvendelse til Datatilsynet vedrørende spørgsmål af databeskyttelsesretlig karakter samt om behovet for yderligere efterforskningsskridt.

3. Forberedelse

Databeskyttelse er et anklagerfagligt fokusområde i retspraksis. Det indebærer blandt andet, at politikredsen skal forelægge alle sager for den regionale statsadvokat med henblik på vurdering af sanktionsspørgsmålet og skal forelægge sager, hvor anklagemyndigheden ikke har fået medhold i strafpåstanden. Der henvises desuden til pkt. 3.3. om forelæggelse for de regionale statsadvokaturer.

3.1. Sager, som er anmeldt af Datatilsynet

En stor del af sagerne vedrørende overtrædelse af reglerne om databeskyttelse må forventes at udspringe af en anmeldelse fra Datatilsynet.

Datatilsynet fører tilsyn med overholdelsen af databeskyttelsesforordningen, databeskyttelsesloven og regler udstedt i medfør heraf. Der henvises til Datatilsynets hjemmeside www.datatilsynet.dk.

Når Datatilsynet vurderer, at der i en konkret sag er grundlag for en straffesag for overtrædelse af databeskyttelseslovgivningen, og sagen ikke kan afgøres med et administrativt bødeforelæg, indgiver Datatilsynet politianmeldelse. Før Datatilsynet anmelder en sag til politiet, er retsgrundlag og faktum nøje vurderet. Endvidere er der om muligt foretaget indledende bevissikring i sagen. Forud for en anmeldelse kan der desuden have været korrespondance mellem tilsynet og den dataansvarlige eller databehandleren, mellem Datatilsynet og den registrerede samt eventuelt mellem Datatilsynet og databeskyttelsesmyndigheder i andre EU-lande, hvis overtrædelsen har grænseoverskridende karakter. Datatilsynets politianmeldelse indeholder på den baggrund en redegørelse for tilsynets vurdering af sagen, herunder niveauet for en bøde, og evt. bevismateriale, f.eks. i form af billedmateriale eller skærmprents, der dokumenterer utilsigtede eller tilsigtede offentliggørelser på internettet.

Datatilsynet sender en kopi af alle politianmeldelser vedrørende overtrædelse af databeskyttelsesreglerne til Rigspolitiets Databeskyttelsesenhed til orientering, jf. pkt. 2.3.2. ovenfor.

Datatilsynet skal høres i sager om overtrædelse af databeskyttelsesforordningen, databeskyttelsesloven og eventuel særregulering fastsat i overensstemmelse med forordningen, inden der træffes afgørelse om tiltalepåkravet. Datatilsynets udtalelse vil indeholde en redegørelse for tilsynets vurdering, herunder niveauet for bøder – og i det omfang, det er muligt, også i forhold til niveauet i andre EU-lande. Hørings-svaret 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.).

I sager, som Datatilsynet har politianmeldt, skal anklagemyndigheden derfor høre Datatilsynet, inden der træffes afgørelse om tiltalepåkravet. I sager, hvor anklagemyndigheden rejser tiltale i overensstemmelse med Datatilsynets indstilling i forbindelse med politianmeldelsen, herunder i forhold til sanktions-påkravet, skal anklagemyndigheden alene orientere Datatilsynet om, at der er rejst tiltale i overensstemmelse med tilsynets indstilling. I sager, hvor politikredsen ikke er enig i Datatilsynets indstilling om tiltalepåkravet, skal påkravet forelægges for den regionale statsadvokat i overensstemmelse med retningslinjerne i Rigsadvokatmeddelelsens afsnit om Særlov – Samarbejde med særmyndigheder i særlovssager. Da afklaring af straffniveauet ved overtrædelse af databeskyttelsesreglerne indtil videre er et anklagerfagligt fokusområde i retspraksis, skal alle sager desuden forelægges for de regionale statsadvokaturer med henblik på en vurdering af sanktionspåkravet. Se nærmere nedenfor i pkt. 3.3.

Hvis der efter politianmeldelsen fremkommer nye oplysninger i sagen, for eksempel oplysning om, 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.

3.2. Sager, som ikke er anmeldt af Datatilsynet

Når politiet modtager en anmeldelse fra andre end Datatilsynet, må politiet på baggrund af den modtagne anmeldelse vurdere, om der er behov for yderligere efterforskning i sagen, f.eks. ved indhentelse af nærmere oplysninger om de faktiske forhold, afhøringer mv. Om rette ansvarssubjekt se pkt. 4.5 om ”Ansvarssubjekter”.

Det skal i hver enkelt sag overvejes, om der allerede i forbindelse med efterforskningen af en sag, skal indhentes en udtalelse fra Datatilsynet, f.eks. med henblik på at få afklaret, hvorvidt der i den konkrete sag vurderes at være sket en overtrædelse af databeskyttelsesreglerne.

I sager, hvor der er sket politianmeldelse uden om Datatilsynet, skal anklagemyndigheden indhente en udtalelse fra Datatilsynet, inden der træffes afgørelse om tiltalesspørgsmålet. Anklagemyndigheden skal i den forbindelse 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.

Udtalelsen fra Datatilsynet vil, ligesom i sager som anmeldes af Datatilsynet, jf. pkt. 3.1., indeholde Datatilsynets vurdering af tiltalesspørgsmålet, 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.

Datatilsynet sender en kopi af deres udtalelse til Rigspolitiets Databeskyttelsesenhed til orientering.

3.3. Forelæggelse for de regionale statsadvokaturer

Politikredsen skal forelægge alle sager, hvor kredsene ikke er enig i Datatilsynets indstilling om tiltalesspørgsmålet for den regionale statsadvokat.

I tilfælde af uenighed om tiltalesspørgsmålet skal Datatilsynet have lejlighed til at komme med en udtalelse om spørgsmålet, inden politikredsen forelægger sagen for statsadvokaten. Det kan i praksis for eksempel ske ved, at politikredsen skriftligt orienterer Datatilsynet om, hvordan politikredsen vurderer sagen, og giver Datatilsynet en frist til at komme med en udtalelse.

Hvis der herefter fortsat ikke er enighed mellem politikredsen og Datatilsynet, skal politikredsen forelægge spørgsmålet for statsadvokaten med en begrundet indstilling.

Derudover er afklaring af straffniveauet ved overtrædelse af databeskyttelsesreglerne indtil videre et anklagerfagligt fokusområde i retspraksis. Det betyder, at alle sager skal forelægges for de regionale statsadvokaturer med henblik på en vurdering af sanktionsspørgsmålet.

I tilfælde af uenighed mellem anklagemyndigheden og Datatilsynet om sanktionsspørgsmålet skal Datatilsynet have lejlighed til at komme med en udtalelse om spørgsmålet. Det kan i praksis ske ved, at den regionale statsadvokatur orienterer Datatilsynet om, hvordan anklagemyndigheden vurderer sagen, og giver Datatilsynet mulighed for at komme med en udtalelse.

Der henvises til Rigsadvokatmeddelelsens afsnit om Særlov – Samarbejde med særmyndigheder i særlovssager.

4. Jura

4.1. Anvendelsesområde for databeskyttelsesforordningen og databeskyttelsesloven

Den 25. maj 2018 afløses persondataloven af nye databeskyttelsesregler. De nye regler findes først og fremmest i databeskyttelsesforordningen, der suppleres af databeskyttelsesloven og anden særregulering.

Databeskyttelsesforordningen har direkte virkning i Danmark, hvilket bl.a. betyder, *at* forordningen virker som en lov i Danmark, og *at* eventuel modstridende eksisterende dansk lovgivning skal ophæves.

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. En personoplysning er enhver form for information om en identificeret eller identificerbar fysisk person eller en enkeltmandsejet virksomhed. Begrebet personoplysning omfatter også billeder, lyd/stemme, fingeraftryk og genetiske kendetegn, og det er uden betydning, om identifikationsoplysningerne er alment kendt eller umiddelbart tilgængelig. Også de tilfælde, hvor det for den indviede vil være muligt at forstå, hvem en oplysning vedrører, er omfattet af definitionen.

Det er desuden en forudsætning for reglerens anvendelse, at behandlingen af personoplysningerne foretages helt eller delvist ved hjælp af automatisk behandling, eller at oplysningerne vil blive indeholdt i et register. Begrebet "automatisk databehandling" er sammenfaldende med "elektronisk databehandling", som blev anvendt i databeskyttelsesdirektivet og persondataloven.

Forordningen finder bl.a. geografisk anvendelse på behandling af personoplysninger, som foretages som led i aktiviteter, der udføres for en dataansvarlig eller en databehandler, som er etableret i EU – uanset om behandlingen finder sted i EU eller ej. Reglerne 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, 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, for så vidt angår deres adfærd finder sted i EU.

I langt de fleste tilfælde vil en behandling af personoplysninger, som foregår i Danmark, være omfattet af den danske lovgivning, dvs. forordningen 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 være lovgivningen i dette land, der gælder. Det betyder, at f.eks. Facebooks aktiviteter er reguleret af irsk lovgivning, fordi Facebook har sit europæiske domicil i Irland.

Se i øvrigt forordningens artikel 2 og 3 samt databeskyttelseslovens §§ 1-4 for nærmere vedrørende reglerens anvendelsesområde og forordningens artikel 4 for definitioner.

4.2. Oversigt over indholdet af databeskyttelsesloven og databeskyttelsesforordningen

Databeskyttelsesforordningen indeholder bl.a.:

- Regler for, hvornår der må behandles personoplysninger. Begrebet "behandling" omfatter enhver form for håndtering af oplysninger, f.eks. indsamling, registrering, systematisering, opbevaring, tilpasning, søgning, brug, videregivelse, formidling og sletning.
- Regler om den registreredes rettigheder. Den registrerede er den person, oplysningerne vedrører, og vedkommende har forskellige databeskyttelsesretlige rettigheder, herunder ret til at få besked om, at der behandles oplysninger om vedkommende (oplysningspligt), ret til at se oplysninger om vedkommende selv (indsigtsret) og ret til – i visse situationer – at få oplysninger rettet eller slettet.
- Regler om sikkerhedskrav, herunder regler om hvornår personoplysninger må overføres til lande uden for EU.

Der sondres mellem forskellige kategorier af personoplysninger.

Forordningens artikel 9 omhandler personoplysninger 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.

Forordningens artikel 10 omhandler personoplysninger vedrørende straffedomme og lovovertrædelser, mens artikel 6 er en opsamlingsbestemmelse, der omhandler alle de personoplysninger, der ikke er omfattet af artikel 9 og 10.

Databeskyttelsesloven supplerer databeskyttelsesforordningens regler. Loven indeholder således for eksempel supplerende behandlingsregler og undtagelser fra reglerne om den registreredes rettigheder. Databeskyttelsesloven indeholder derudover desuden straffebestemmelser for overtrædelser af forordningen, herunder en udvidet adgang til at strafforfølge offentlige myndigheder. Se nærmere nedenfor under pkt. 4.6.

Se i øvrigt Datatilsynets hjemmeside 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.

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 defineres 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, antaget, 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 databeskyttelsesforordningen/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 databeskyttelsesreglerne alt efter, om der er tale om en dataansvarlig eller en databehandler.

Definitionen på henholdsvis en dataansvarlig og en databehandler findes i forordningens artikel 4, nr. 7 og nr. 8.

Afgrænsningen kan i visse tilfælde give anledning til tvivl. Du kan læse mere om afgrænsningen mellem at være dataansvarlig og databehandler i Datatilsynets og Justitsministeriets vejledning om dataansvarlige og databehandlere, som kan findes på Datatilsynets hjemmeside.

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

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, pkt. 3.1.3., 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.

5. Straf og andre retsfølger

5.1. Generelt om sanktionsspørgsmålet i sager om overtrædelse af databeskyttelsesforordningen mv.

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

Tidligere blev overtrædelser af de persondataretlige regler 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 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 alvorlighed, 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.

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.

De nye regler lægger således op til en væsentlig 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 retspraksis 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. Omvendt fremgår det endvidere af forarbejderne til databeskyttelsesloven, at bødeniveauet efter persondataloven bør videreføres for overtrædelser, hvor forordningens anvendelse er udvidet med databeskyttelsesloven til at også at finde anvendelse på behandling af oplysninger om virksomheder (kreditoplysningsbureauer og advarselsregistre).

Der er ikke i forordningen eller bemærkninger 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 fremtidige størrelse i disse sager. Afklaring af strafniveauet 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 ukomplicerede sager uden bevismæssige tvivlsspørgsmål.

5.2. Hensynene bag reglerne

Hensynene bag databeskyttelsesreglerne og den væsentlige 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.
- Det fremgår af præambelbetragtning 148, at der for at styrke håndhævelsen af forordningens regler bør pålægges sanktioner for overtrædelse af forordningen.
- De pålagte bøder bør være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning. Det følger 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, er:

- Overtrædelsens karakter, alvor og varighed under hensyntagen til 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 overtrædelse, 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 er således bindende for EU-landene. 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 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.

5.5. Påstand om rettighedsfrakendelse

Anklagemyndigheden skal 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 § 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. De typer virksomhed, der er omfattet af bestemmelsen i § 26, er advarselsregistervirksomhed, kreditoplysningsbureauvirksomhed og virksomhed ved behandling af oplysninger, der udelukkende finder sted med henblik på at føre retsinformationssystemer.

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. 5-6 (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 statslige myndighed kan disponere over.

Eksempel:

X-styrelse kan i 2017 disponere over et samlet beløb på 95 mio. kr. Det betyder, at styrelsen vil kunne få en bøde på op til 1,9 mio. kr. (2 pct.) eller 3,8 mio. kr. (4 pct.).

For kommuner, regioner mv. vil bøden skulle beregnes på grundlag af de samme principper som for statslige myndigheder, dvs. på grundlag af det samlede beløb, som den pågældende 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 bødeløft, 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 databeskyttelseslovgivningen, skal Datatilsynet underrettes om sagens udfald samt 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

I sager, hvor tiltalespørgsmålet har været forelagt for den regionale statsadvokat, for eksempel fordi der har været uenighed mellem politikredsen og Datatilsynet om tiltalespørgsmålet, herunder sanktionspåstanden, skal politikredsen – inden ankefristens udløb – underrette statsadvokaten om udfaldet af sagen.

Sager om overtrædelse af databeskyttelsesforordningen er et anklagerfagligt fokusområde i retspraksis, og politikredsene skal derfor desuden – inden ankefristens udløb – forelægge ankespørgsmålet med den regionale statsadvokat i alle sager, hvor anklagemyndigheden ikke har fået medhold i strafpåstanden.

6.3. Afgørelser til Vidensbasen

Sager om overtrædelse af databeskyttelsesreglerne er et anklagerfagligt fokusområde i retspraksis, og det betyder, at alle endelige domme skal 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
 - Artikel 29-gruppens vejledning om Retten til dataportabilitet

Rigsadvokaturen, den 25. maj 2018

RIGSADVOKATEN

/ Rigsadvokaten