D O M

afsagt den 23. december 2024

Rettens nr. 3-5399/2023
Politiets nr. 3700-84266-00012-21

Anklagemyndigheden
mod
Tiltalte (Region)
CVR nr.

Der har medvirket domsmænd ved behandlingen af denne sag.

Anklageskrift er modtaget den 27. juni 2023.

Tiltalte (Region) er tiltalt for overtrædelse af

1.

databeskyttelseslovens § 41, stk. 1, nr. 1, jf. stk. 3, jf. stk. 6 jf. databeskyttelsesforordningens artikel 83, stk. 2, og stk. 4, litra a, jf. stk. 9, jf. artikel 32, stk. 1,
ved i en periode umiddelbart efter den 4. januar 2019 og frem til den 23. august 2020 ikke at have overholdt sin forpligtelse som dataansvarlig til at gennemføre passende tekniske og organisatoriske foranstaltninger, for at sikre et tilstrækkeligt sikkerhedsniveau, idet Tiltalte (Region) i forbin-delse med opsætning af en database til forskningsmæssige og kliniske formål ikke havde sikret sig imod, at uvedkommende ved at ændre en URL-adresse kunne opnå uautoriseret adgang til PDF-dokumenter i databasen, hvilket medførte at borgere, der var registreret i databasen, og som i øvrigt havde et login til databasen, kunne tilgå personoplysninger om de mere end 23.000 andre registrerede i databasen, herunder helbredsoplysninger om mindreårige tilknyttet psykiatrien.

2.

databeskyttelseslovens § 41, stk. 1, nr. 1, jf. stk. 3, jf. stk. 6 jf. databeskyttelsesforordningens artikel 83, stk. 2, og stk. 4, litra a, jf. stk. 9, jf. artikel 32, stk. 1,
ved i perioden fra den 25. maj 2018 til den 5. marts 2020 ikke at have overholdt sin forpligtelse som dataansvarlig til at gennemføre tekniske og organisatoriske foranstaltninger, for at sikre et tilstrækkeligt sikkerheds-niveau, idet Tiltalte (Region) ikke havde sikret sig imod, at der utilsigtet

lå personoplysninger på regionens hjemmeside, hvilket blandt andet med-førte, at en PowerPoint præsentation indeholdende oplysninger om 3.915 patienter - herunder oplysninger om personnummer og helbredsoplysninger -var tilgængelig på regionens hjemmeside, hvorved oplysningerne utilsigtet blev gjort tilgængelige for uvedkommende, hvilket udgjorde en unødigt høj risiko for de registrerede borgere og tab af fortrolighed af deres personoplys-ninger.

Påstande

Anklagemyndigheden har nedlagt påstand om bødestraf.

Tiltalte har nægtet sig skyldig.

Sagens oplysninger

It-direktør Vidne 1 har som partsrepræsentant for tiltalte forkla-ret, at han har været ansat i Tiltalte (Region) siden 2014, og fra 2016 som it-direktør.

Vedrørende forhold 1 har han forklaret bl.a., at han først kendte CBCL-sy-stemet, da de fik anmeldelsen fra en borger. De har 1.160 systemer i Tiltalte (Region). I CBCL-systemet er der en forskerdel og en spørgeskemadel. Han kender til spørgeskemadelen. Det kan bruges til, at brugerne kan give egenoplysninger om helbred, som er vigtige for behandling eller forskning. Det kræver, at man er logget ind i CBCL-systemet. Man skal således have login med password. Adgangen er tidsbegrænset til 14 dage, hvorefter den slettes. Brugerne er patienter og disses pårørende. Når der er foretaget be-svarelse i spørgeskemadelen, får brugeren en kvittering. Der er systemejere, som er ansvarlige for systemet. Det er ansatte i regionen. Oplysningerne fra brugerne gives i et spørgeskema. Det har så vist sig, at det har været muligt for en bruger at ændre i URL-adressen, og derigennem være heldig at få ad-gang til andres oplysninger. Det er sket i fem tilfælde. Det er en betingelse for at kunne udføre dette, at brugeren har været logget ind på CBCL-syste-met. Efter hans oplysninger har der øjensynligt været tale om en enkelt per-son med særlig indsigt i datasystemer. Der har ikke været adgang til patien-ters diagnoser fra sundhedsprofessionelle. Det har været oplysninger fra pati-enter eller patienters pårørendes beskrivelser af patienternes helbred. Han ved ikke, om patienternes cpr-nummer fremgik. Sikkerheden udgjordes af lo-gin-systemet. Der er forskellige yderligere adgangskontroller inde i selve sy-stemet. Det har imidlertid vist sig, at URL-adressen var tilgængelig, så man kunne manipulere den og få adgang til andres oplysninger. Han må medgive, at det ville have været muligt at forhindre det. Efter man blev gjort opmærk-som på bruddet, fik regionen sin eksterne leverandør til at ændre systemet, så det ikke længere var muligt at tilgå andres oplysninger som sket. Der findes i regionen en risikovurdering, der var udarbejdet på det tidspunkt, GDPR-reg-lerne trådte i kraft. CBCL-systemet er skabt i 2005. Regionen har altid haft

stor fokus på at beskytte borgernes oplysninger. Det var i 2018, at man lave-de risikovurderingen. Man opdagede imidlertid ikke problemet med mulighe-den for at ændre i URL-adresser og tilgå andres oplysninger i forbindelse med udarbejdelse af en risikovurdering. Han tror ikke, at man kunne forestil-le sig, at den situation kunne opstå. De regnede med, at systemet var sikkert. De bruger ekstern leverandør til at lave løbende kontroller af sikkerheden på alle deres systemer. De vurderer løbende, hvem der skal have adgang. CBCL-systemet er løbende kontrolleret for sikkerhedsproblemer. Det var en bruger med login, som gjorde opmærksom på, at det var muligt at ændre URL-adressen og tilgå andre brugeres oplysninger. De havde ikke selv opda-get, at der var et sikkerhedsproblem. Brugerne i regionen er ikke it-kyndige. De bruger eksterne leverandører til it. Det er rigtigt, at der tidligere har været en anmeldelse af et sikkerhedsbrud, som havde med URL at gøre. Så vidt han ved, var sagen teknisk ikke helt sammenlignelig med denne sag. Den tid-ligere sag beroede på en menneskelig fejl. Det er dog rigtigt, at begge sager havde noget at gøre med at ændre i URL. Det drejede sig om, at en liste med oplysninger var placeret forkert. Sagen blev påtalt af Datatilsynet ca. en må-ned før CBCL-sagen. I forhold til den tidligere sag vil han mene, at CBCL-sagen nok mere drejer sig om en systemfejl eller svaghed i systemets sikker-hed. Så vidt han husker, var der registreret omkring 23.000 personer i CBCL-systemet, hvor der lå oplysninger på disse. Han kan ikke sige præcist, om CBCL-systemet er ændret siden 2005, hvor det blev skabt. Han tror, at URL er en web-applikation, som er kodet af leverandøren. Der var tekniske muligheder for at skærme URL. De lukkede CBCL-systemet, da anmeldelsen kom. De tog straks kontakt til deres leverandør, som rettede op på proble-met. De orienterede også om problemet i organisationen. Det fremgår nu af deres retningslinjer angående krav til leverandører, at man skal være op-mærksom på sikkerhedsmæssige svagheder i relation til URL. Han ved ikke, om der er lavet en vurdering af risikoen for patienterne. Tiltalte (Region)s driftsbevilling for 2020 lå nok på omkring 26 milliarder kr. Regionen driver fire store sygehuse og psykiatrisygehuset. Psykiatrisygehuset står for ca. 10% af budgettet.

På spørgsmål fra forsvareren har han forklaret bl.a., at han er chef for regio-nalt it i regionen. Det er en central it-organisation. Derudover har hvert syge-hus sin egen it-afdeling. De decentrale it-afdelinger refererer ikke til ham, men de er selvfølgelig i kontakt med hinanden. Der er ret decentralt ansvar i Tiltalte (Region). I hans afdeling var de 250-300 ansatte på det tidspunkt. De udfører mange forskellige opgaver. De driver 1.160 it-systemer i regionen for, at sygehuse m.v. kan fungere. Der står 3.500 servere i Kolding. Der er ca. 100.000 endepunkter - d.v.s. PC'er, telefoner, tablets m.v. Tiltalte (Region) har været digitaliseret i 40 år. Det er afgørende for at opretholde den effektivitet, som man har. Det betyder så også, at de også har 40 år gamle systemer. De har en informationssikkerhedsafdeling med 20 ansatte, som udarbejder retningslinjer m.v. til alle ansatte i Tiltalte (Region). Der er 10 ansatte i operationel afdeling, som arbejder med cypersikkerhed. Det kan være imødegåelse af f.eks. hacking. Et system er noget, man kan logge ind i og

behandle data på. Det er altså et softwaresystem. Der er som sagt 1.160 systemer. Regionen bruger 20-30 millioner kr. om året i anlægsudgifter til it. Det er systemejerne, som er ansvarlige for, om et system er nødvendigt, f.eks. om et røntgensystem klinisk er nødvendigt. De er med til at udarbejde risikovurderinger. De ser med stor alvor på sikkerheden. De oplysninger, der kunne tilgås i CBCL-systemet, var ikke de mest følsomme oplysninger, der er i Tiltalte (Region)s systemer. Han medgiver, at der selvfølgelig er tale om fortrolige oplysninger. Det vigtigste hensyn i regionen går på, at de skal være i stand til at give patienterne den rigtige behandling. Det er en balance mellem dét og sikkerhedshensyn. Det er væsentligt, at man har de nødvendi-ge data på patienterne. Det er afgørende for behandlingen.

Foreholdt et dokument betegnet "Fællesregional Informationssikkerheds-politik"(bilag A) har han forklaret, at han kender dokumentet. Det beskriver, hvordan man på tværs af alle regionerne i Danmark vil arbejde med person-sikkerhed.

Foreholdt en instruks "Forbrug af it i Tiltalte (Region)" dateret 2019 og hæftet på en supplerende besvarelse af oplysninger til Datatilsynet (bilag 2.5) har han forklaret, at det er en informationssikkerhedshåndbog for hele Tiltalte (Region). Formålet er, at medarbejderne ved, hvordan de skal håndte-re følsomme oplysninger. Det er en håndbog over de overordnede sikker-hedshensyn. Der findes også niveauer derunder, som går på det mere praktis-ke, og som indeholder detaljerede oplysninger om sikkerhedshåndtering. Han vil tro, at der samlet set findes hundredvis eller tusindvis af sider, som beskri-ver noget om sikkerhed vedrørende it og databehandling. Der står også no-get om søgning og fortrolighed. I regionen er der hjemmesideredaktører, som har ansvaret for den delmængde af indhold, der er på hjemmesiderne i Tiltalte (Region).

Vedrørende forhold 1 har han forklaret, at CBCL-systemet ligger i psykiatri-en, som er en selvstændig enhed i Tiltalte (Region). Psykiatrien står for ca. 10% af budget og aktivitet i regionen. Psykiatrien har egen it-organisati-on. De er selvfølgelig underlagt samme krav som i øvrigt i regionen. I forbin-delse med GDPR-reglernes indførelse blev det almindeligt med risikovurde-ring. Der blev lavet en skabelon over gennemførelse af risikovurdering. Den blev lavet af en ekstern leverandør. Den bliver løbende justeret, baseret på er-faringen med sikkerhed.

Foreholdt et udfyldt spørgeskema fra regionen til Datatilsynet (bilag 1.4, side 3/8) har han forklaret, at spørgeskemaet blev fremsendt af Datatilsynet.

Vedrørende spørgsmål 2, svarede de omkring de tekniske foranstaltninger i anledning af databruddet. Det var første punkt i besvarelsen. Derefter rede-gjorde de også for de organisatoriske foranstaltninger i anledning af datab-ruddet.

Foreholdt et dokument af 21. april 2020 betegnet "Auditering af databehandleraftaler" (bilag N) har han forklaret, at det er udtryk for en jævnlig kontrol af deres leverandører. Det pågældende dokument drejer sig om kontrol af leverandøren af CBCL-systemet.

Vedrørende pkt. 3.3.8, side 3/9, har han forklaret, at det er deres leverandørs besvarelse i audit angående sikkerhedsforanstaltninger i relation til personoplysninger. Han har ikke anledning til at tro andet, end at leverandørerne svarer ærligt og sandfærdigt på spørgsmålet. Altså var der for ham at se ført en lang række kontroller.

Foreholdt en e-mail af 23. august 2020 fra Person (bilag 1.1, sidste si-de) har han forklaret, at der for ham at se, baseret på det under underskriften anførte, er tale om en person, som er meget it-kyndig og certificeret inden for it-sikkerhed.

Vedrørende forhold 2 har han forklaret bl.a., at en af regionens ansatte læger i 2011 lavede en PowerPoint præsentation til brug for noget uddannelse. PowerPoint præsentationen blev efterfølgende lagt op på regionens hjemmeside og var tilgængelig derpå. PowerPoint præsentationen indeholdt nogle grafer. Inde bag de pågældende grafer kunne man få adgang til personoplysninger. Det var, så vidt han er orienteret, meget teknisk at skaffe sig adgang. Efter hans oplysninger kræver adgang, at man skal gennem 15 komplekse trin for at kunne tilgå personoplysningerne. Man skal hente filen ned og gemme den på en PC, og så skal man åbne mapper og filer. Man skal således gennem mange trin. Han medgiver, at det er rigtigt, at der ikke kræves koder eller lo-gin for, at man kan hente oplysningerne frem. På dette tidspunkt lå PowerPo-int præsentationen i et dokumentarkiv. Den var ikke frit tilgængelig på Tiltalte (Region)s hjemmeside. Hvis man lavede en specifik Google-søgning, eller anden søgning på f.eks. søgeordet "lunge-kræft", så ville PowerPoint præsentationen komme frem blandt mange andre links. Den kunne således ik-ke søges frem direkte på hjemmesiden. Dokumentarkivet ligger under hjem-mesiden. I 2014 eller 2015 blev der lavet en ny hjemmeside. I den forbindelse blev alle links fjernet. Under den ny hjemmeside lå et dokumentarkiv med 80-100.000 filer. Han vil understrege, at PowerPoint præsentationen ikke kunne klikkes frem direkte på hjemmesiden. Det krævede en Google-fremsøgning, hvor den kunne dukke op blandt mange andre links. Dataene stammede fra Dansk Lungekræft Register. Der var ikke tale om diagnoseoplysninger. Det er rigtigt, at man kunne fremsøge navne bag grafen på personer, og at det drejer sig om lungekræft. Der var tale om ca. 4.000 personer. Så vidt han er orienteret, var der et andet sted i samme PowerPoint ca. 22 oplysninger om fødselsdatoer. Dataene var uploaded i 2011. Siden 2013 har Tiltalte (Region) skannet hjemmesider m.v. for cpr-numre i dokumenter. Imidlertid kun-ne deres cpr-skanner-værktøj ikke se ind bag dataene. Værktøjet var anskaf-fet via en ekstern leverandør, som havde oplyst, at værktøjet skannede alle interne dokumenter for cpr-numre. Skanningen kører løbende. Man havde også andre foranstaltninger. Det er rigtigt, at dersom lægen, der lavede Po-

werPointen, eller den webansvarlige havde indset, at dataene ikke burde være i PowerPointen, så havde sikkerhedsbruddet været undgået. Så efter hans opfattelse kan man vel godt sige, at det i 2011 var en menneskelig fejl. Derudover burde skanningsværktøjet også have opdaget det. De laver både manuelle tjek og automatiserede tjek ved uploads. Hvis begge dele svigter, så har man ikke mulighed for at opdage det. Han ved ikke, om skannings-værk-tøjet tjekker for andet end cpr-numre. Problemet blev rettet umiddelbart ef-ter, at de blev klar over, at dataene lå der. Han ved ikke, om der blev gjort noget særligt i forbindelse med indførelse af GDPR-reglerne. Regionen har nu anskaffet et nyt og udvidet skanningsværktøj. De prøver hele tiden tekno-logisk at følge med. Der er også krav om, at webredaktørerne skal uddannes i sikkerhed i forhold til hjemmesiderne. Han har en hel klar forventning om, at tilsvarende databrud ikke kan opstå igen. Det var i marts 2020, at regionen gik i gang med at eftersøge nye og bedre kontrolværktøjer.

På spørgsmål fra forsvareren har han forklaret bl.a., at deres leverandør hav-de oplyst, at de kunne tjekke for cpr-numre. De kunne også tjekke en lang række forskellige filformater -også PowerPoints-formater. Han havde ikke grund til at tro, at sikkerheden ikke var i orden. Det var en ekstern leveran-dør, som havde hjulpet lægen med at lave graferne i 2011. Det var heller ikke i overensstemmelse med de dagældende regler, at der kunne tilgås personlige oplysninger via PowerPoint præsentationen. PowerPoint præsentationen var tilgængelig på hjemmesiden indtil, at den ny hjemmeside kom i 2015. På regionens hjemmeside kunne man forud for 2015 klikke på et link, som førte over til PowerPoint præsentationen. Efter 2015 var dette ikke en mulighed. Hvis man søgte via WebCrawler på f.eks. Google, kunne man få præsentatio-nen frem via forskellige søgeord om lungekræft. PowerPoint præsentationen ville dukke op blandt rigtig mange andre links. Så vidt han ved, er det via logning konstateret, at PowerPoint præsentationen er søgt frem 15 gange. Det er på den måde muligt at fremsøge personoplysninger. Han ved ikke, om logningen kan vise andet.

Vidne 2 har som vidne forklaret bl.a., at han er ansat i Datatilsynet som it-sikkerhedskonsulent. Datatilsynet modtager anmeldelser om brud på datasikkerheden. De vurderer så, hvordan sagerne skal behandles. Man modtager ca. 300 anmeldelser om ugen. Der holdes et ugentligt visitationsmøde, hvor man udvælger sager til videre juridisk behandling. Han har viden om it-systemer, men han er ikke teknisk it-ekspert. Han har en uddannelse i politi-et, og han har i 25 år arbejdet med udvikling af it-systemer og it-sikkerhed. Datatilsynets sikkerhedskonsulenter er generalister.

Vedrørende forhold 1 har han forklaret, at det ikke kan undgås, at nogen kan ændre en URL-adresse. Det skyldes, at URL-adressen er synlig og læsbar. Derfor kan man skrive i den og ændre den. Der findes måder at sikre en URL. Det kan f.eks. være gennem etablering af login med kode. Et eksempel herpå er MitID. En simpel URL er som udgangspunkt ikke sikker, og det er nemt at søge ud fra en simpel URL. Hvis f.eks. en URL-adresse ender på

"1.pdf", så kan man jo forsøge at ændre slutningen af adressen til "2.pdf" for at se, om der skulle dukke noget op. En simpel URL skal kontrolleres. Man fik en henvendelse fra en borger, som havde været i stand til at søge personoplysninger frem ved at ændre lidt i URL. Modsat er det nemt at sikre en URL, f.eks. ved login. Ved nogle hjemmesider skal der bruges login med brugernavn og 8-cifret kode. Det giver så adgang til systemet. Det var hans og Datatilsynets vurdering, at Tiltalte (Region) burde have lavet sikker-hedsforanstaltninger til at undgå, at brugere kunne få adgang til andre bruge-res personlige oplysninger via URL. Der findes værktøjer, hvorved Tiltalte (Region) kunne have sikret dette, f.eks. ved sessionsafgrænsning/cookies, således brugere ikke kunne skifte til en anden URL. Det er ret nemt at lave. Sessionsafgrænsning er en forholdsvis simpel sikkerhedsforanstaltning. Efter hans erfaring ville det heller ikke have været en omkostningstung foranstalt-ning.

På spørgsmål fra forsvareren har han forklaret bl.a., at URL er almindelig kendt som en usikker måde at linke til personlige oplysninger. Datatilsynet vejleder ikke om tekniske løsninger. Datatilsynet vejleder om de overordnede sikkerhedskrav efter reglerne. Han kender ikke til, om tilsynet har vejlednin-ger liggende om sessionsafgrænsninger.

Vedrørende forhold 2 har han forklaret bl.a., at data kan udveksles mellem forskellige dokumenter, PowerPoints m.v. Ud fra et regneark med data kan man fremstille en graf, og hvis man trykker på grafen, kan man derved tilgå de bagvedliggende data. Det kan man efter hans opfattelse se på linket, og man kan derigennem sige sig selv, om man har et problem. Det er efter hans vurdering kendt stof, at det kan være et problem, at brugere kan tilgå bag-vedliggende data ved at klikke på en graf. Problemet kan ret nemt afhjælpes. I stedet for at skrive grafen ind i PowerPoint præsentationen, kunne man blot have lavet et screenshot af grafen og sat ind i præsentationen. Så kan der ik-ke ved klik på grafen tilgås bagvedliggende data. Det er kendt stof.

Vidne 3 har som vidne forklaret bl.a., at hun er uddan-net jurist. Hun er ansat som souschef i Datatilsynet. Hun har været ansat i 2½ år.

Databeskyttelsesforordningen har været gældende siden maj 2018. Af forordningens artikel 32 kan udledes, at der skal laves risikovurdering, når man behandler personfølsomme oplysninger. Det skal vurderes, om uvedkommende kan få adgang, og om de beskyttede kan miste fortroligheder i de opbevarede oplysninger. Det skal også vurderes, hvad konsekvenserne for de enkelte kan være. F.eks. er helbredsoplysninger særligt følsomme oplysninger. Risikovurderingen afhænger også af, hvad det er for personoplysninger, der behandles. Forordningen beskriver ikke udtømmende, hvad man skal gøre. Det er op til den dataansvarlige. Der er masser af praksis på området. Man skal hele tiden overveje og genoverveje sine risikovurderinger. Navnlig hvis man må erken-de brud på datasikkerheden.

Vedrørende forhold 1 har hun forklaret, at der er krav på beskyttelse af per-sonoplysninger. Hvis andre kan se helbredsoplysninger, er det allerede en overtrædelse. Der skal jo også ske forebyggelse mod eventuelle kriminelles udnyttelse af oplysningerne. Man skal vurdere, hvad risikoen potentielt har været. Det er uafhængigt af, hvad der konkret er sket. I dette tilfælde skete der heldigvis ikke en større udnyttelse. I Datatilsynet foretages der vurdering af de enkelte sager af både jurister og it-sikkerhedsfolk. Datatilsynet laver en samlet vurdering af grovheden af overtrædelserne.

Vedrørende forhold 2 har hun forklaret, at også den sikkerhed, der var forud for databeskyttelsesforordningens ikrafttræden, skal vurderes i lyset af regler-ne i databeskyttelsesforordningen. Egentlig er der ingen særlige ændringer i forhold til tidligere regler. Dog vil sagerne blive skrevet, som om det havde sin begyndelse i 2018, hvor GDPR-reglerne trådte i kraft. Den længere perio-de forud for 2018 vil dog indgå i tilsynets vurdering. Hvis først oplysningerne har kunnet tilgås af andre, er fortroligheden brudt.

Angående sanktionen har hun forklaret, at offentlige myndigheder også straf-fes efter forordningen. Folketinget har ved implementeringen af databeskyt-telsesforordningen, der er suppleret af databeskyttelsesloven, sendt et signal om, at reglerne skal tages alvorligt, og at bøder skal have en størrelse, hvor det kan mærkes. Efter databeskyttelseslovens forarbejder er der indlagt bøde-lofter for offentlige myndigheder på 8 millioner kr. for tilsidesættelse af for-pligtelser i henhold til databeskyttelsesforordningens artikel 32 m.v., jf. her-ved databeskyttelseslovens § 41. Der skal tages udgangspunkt i driftsbevillin-gens størrelse, således der proportionelt kan ske udligning for store og små dataansvarlige. Efter reglerne skal der ses på den samlede driftsbevilling for hele Tiltalte (Region), der er den dataansvarlige. Der er ikke hjemmel til kun at se på psykiatrien under Tiltalte (Region). Ved bødens fastsættelse ses også på, om der måtte være formildende eller skærpende omstændighe-der. Der er indført regler herom i databeskyttelsesforordningens artikel 83. Straffelovens § 82 og 83 gælder endvidere også på dette område. I denne sag er det Tiltalte (Region) i sin helhed, der er dataansvarlig.

Der har været fremlagt en supplerende udtalelse af 8. maj 2024 fra Datatilsy-net om bødens størrelse. I udtalelsen er bl.a. anført følgende:

> "...
> **1. Indledning - fornyet vurdering af bødernes størrelse** Datatilsynet fremsender hermed en supplerende udtalelse om bødestør-relsen i ovennævnte sager, som er berammet til domsforhandling i Ret-ten i Kolding den 21. maj 2024.
>
> Datatilsynet bemærker i den forbindelse, at bødeindstillingen i politian-meldelserne af 16. juli og 17. september 2021 er baseret på Tiltalte (Region)s driftsbudget i 2019 (nedenfor anvendes i stedet drifts-

budgettet for 2021), at der efterfølgende er indgivet flere politianmeldelser og afgjort flere sager om overtrædelse af databeskyttelsesforordningens artikel 32, og at European Data Protection Board (EDPB) den 24. maj 2023 har vedtaget retningslinjer om beregning af administrative bøder efter GDPR2, som tilsynet anvender ved bødeberegningen. Retningslinjerne vedlægges som bilag 1.

Datatilsynet har i politianmeldelserne indstillet til en bøde på 500.000 kr. for hvert af forholdene isoleret set. Som det fremgår nedenfor, fast-holder Datatilsynet denne indstilling.

1.1. Retningslinjer om beregning af bøder efter GDPR

EDPB vedtog som anført den 24. maj 2023 uddybende retningslinjer for udmåling af bøder efter GDPR (GL 04/22). Formålet med retningslinjerne er at sikre ensartethed og gennemsigtighed i forhold til bødeudmålingen på tværs af de europæiske tilsynsmyndigheder. De uddybende fælleseuropæiske retningslinjer angiver en model for bødeniveau og nogle rammer for bødefastsættelsen, men retningslinjerne fastsætter ik-ke konkrete bødetakster. Retningslinjerne angiver endvidere EDPS's fortolkning af de forskellige litra'er i artikel 83, stk. 2, herunder de forskellige forhold der skal lægges vægt på ved vurderingen af grovheden af overtrædelsen (litra a, b og g) og ved vurderingen af, om der forelig-ger skærpende eller formildende omstændigheder i sagen (de øvrige lit-ra'er - som ikke udgør en udtømmende opregning af de forhold, der kan lægges vægt på).

Det skal i den forbindelse bemærkes, at der på nuværende tidspunkt ik-ke er udarbejdet en dansk vejledning på området. Hertil skal Datatilsy-net gøre opmærksom på, at EDPB i deres retningslinjer om udmåling af bøder efter GDPR (GL 04/22) har anført (afsnit 1.3, punkt 10), at retningslinjerne gælder for beregningen af den bøde, der skal pålægges offentlige myndigheder og organer, med undtagelse af kapitel 4.3 g 6 (nedsættelse af bøde og beregning af bødemaksimum på baggrund af virksomhedens størrelse). Tilsynsmyndighederne står således frit for at anvende en metode svarende til den, der er beskrevet i retningslinjerne.

Datatilsynet har ved sin fornyede vurdering af sagen inddraget de principper, som fremgår af de fælleseuropæiske retningslinjer for bødeudmåling. herunder fortolkningen af de forskellige litra'er i forbindelse med vurderingen af forholdets grovhed (litra a, b og g) og tilstedevæ-relsen af eventuelle skærpende og formildende omstændigheder (de øv-rige litra'er). Det bemærkes, at retningslinjerne ikke har ført til, at sa-gerne skal bedømmes efter andre regler end dem, der har været gæl-dende siden 25. maj 2018, hvor databeskyttelsesforordningen begyndte at finde anvendelse.

Datatilsynet finder fortsat grundlag for at lægge vægt på de forhold,

der er anført i politianmeldelserne af 16. juli og 17. september 2021 og i udtalelsen af 4. maj 2023.

Dog finder Datatilsynet efter nærmere overvejelser ikke grundlag for at følgende forhold skal anses for at være egentlige formildende omstændigheder:

Politianmeldelsen af 16. juli 2021:

"Det må til gengæld anses for en formildende omstændighed, at sårbarheden i adgangen til databasen ikke ses at være udnyttet af andre end den pågældende borger, som blev opmærksom på forholdet, og at oplysningerne kun kunne tilgås af andre deltagere i forskningsprojektet. Den konkrete risiko for de registrerede har således været mindre, end hvis enhver kunne skabe sig adgang til oplysningerne."

Politianmeldelsen af 17. september 2021:

"Det må anses for en formildende omstændighed, at regionens log vi-ser, at oplysningerne alene er blevet tilgået af 16 personer, hvorfor den konkrete skade for de registrerede må antages at være lille."

Datatilsynet har herved lagt vægt på, at disse forhold må anses for at bero på en tilfældighed snarere end forhold, der kan tilregnes regionen. Datatilsynet bemærker i den forbindelse, at databeskyttelsesforordningens artikel 32, stk. 1, er et risikodelikt, hvor bestemmelsen derfor er overtrådt, hvis der ikke er etableret et passende sikkerhedsniveau, uan-set om der f.eks. er sket et brud på persondatasikkerheden som i dette tilfælde, hvor der konkret har været uautoriseret adgang til oplysnin-gerne for en større gruppe af personer. Overtrædelsen består således i, at der ikke var etableret et passende sikkerhedsniveau, og j forhold her-til kan det derimod tale i skærpende retning, at det utilstrækkelige sikkerhedsniveau konkret medførte, at der skete et brud på persondatasikkerheden, men det er altså ikke en forudsætning for, at der er sket en overtrædelse af databeskyttelsesforordningens artikel 32. Det bemær-kes i forlængelse heraf, at det er tilstrækkeligt til at konstituere et brud på persondatasikkerheden, at der har været uautoriseret adgang til personoplysninger, og at det således ikke er en betingelse, at adgangen hertil rent faktisk har været udnyttet af uvedkommende (dvs. at uvedkommende rent faktisk har tilgået/skaffet sig adgang til oplysningerne).

De ovennævnte forhold kan dog naturligvis tillægges vægt ved den samlede vurdering af forholdenes grovhed, hvor der i henhold til artikel 83, stk. 2, litra a, kan lægges vægt på antal berørte og den skade, som de har lidt. Datatilsynets finder dog i overensstemmelse med det anfør-te om fortolkningen af denne bestemmelse i EDPB's retningslinjer, at der både skal lægges vægt på antal konkrete og potentielt berørte og

den konkrete og potentielle skade de har lidt/kunne lide, jf. at der er ta-le om et risikodelik.

Denne ændrede vurdering fører dog ikke til en ændring i indstillingen af bødernes størrelse.

1.1.1. Uagtsomhedsvurderingen, jf. artikel 83, stk. 2, litra b
Datatilsynet finder, at overtrædelserne som minimum må anses for at være begået uagtsomt.

Datatilsynet bemærker, at dette forhold i givet fald må anses som et neutralt faktum i alvorlighedsvurderingen - og altså ikke som en formildende omstændighed. Det er således en forudsætning, at der som minimum foreligger uagtsomhed, førend der er tale om en strafbar overtrædelse.

I forhold til kravene til bl.a. uagtsomhedsvurderingen efter databeskyttelsesforordningen kan Datatilsynet henvise til følgende nyere praksis fra EU-domstolen:

...
1.2. Bødeberegningstidspunktet
Ifølge databeskyttelsesforordningens artikel 83, stk. 4, straffes overtrædelse af artikel 32, stk. 1, med administrative bøder på op til 10 mio. euro, eller hvis det drejer sig om en virksomhed, med op til 2 % af dens samlede globale omsætning i det forudgående regnskabsår, såfremt dette beløb er højere.

Det følger af en bindende afgørelse truffet af Det Europæiske Databeskyttelsesråd (EDPB) den 28. juli 2021 vedrørende WhatsApp, at det forudgående regnskabsår skal ses i forhold til tilsynsmyndighedens afgørelse om en bøde til den dataansvarlige.

Dette vil i Danmark svare til Datatilsynets politianmeldelse, da Datatilsynet ikke (for nuværende) selv kan udstede administrative bøder. Det betyder efter Datatilsynets opfattelse, at bødefastsættelsen i dette tilfæl-de skal ske under hensyntagen til regionens økonomiske forhold ud fra driftsbudgettet for 2021 -og ikke for 2019 som anført i politianmeldelserne.

Det er Datatilsynets umiddelbare vurdering, at dette også stemmer overens med præmisserne i Østre Landsrets dom afsagt 20. september 20237, hvor landsretten udtalte følgende:

> "Det fremgår af forordningens artikel 83, stk. 4 og 5, at der ved fastsættelse af bødens størrelse tages hensyn til den samlede globale omsætning i det forudgående regnskabsårs. og det fremgår

af afgørelse af 28. juli 2021 fra Det Europæiske Databeskyttel-sesråd. at der med "det forudgående regnskabsårs"tages ud-gangspunkt i det senest reviderede og offentliggjorte regnskab, når tilsynet træffer endelig afgørelse om bødens størrelse.

Bestemmelserne i forordningens artikel 83, stk. 4 og 5, hvorefter der ved bødefastsættelsen skal tages udgangspunkt i "det forud-gående regnskabsår" er udformet ud fra den forudsætning, at der pålægges en administrativ bøde, hvilket i de fleste tilfælde må forventes at indebære, at der vil være nær tidsmæssig sammen-hæng mellem gerningsperioden og det regnskabsår, som skal danne grundlag for fastsættelsen af den administrative bøde. Be-stemmelsen er således ikke affattet med sigte på den ordning, der er gældende i Danmark, hvor bødestraf idømmes af domstolene.

Det fremgår af præambelbetragtning 150, at der med forordnin-gen er tilsigtet en harmonisering af sanktioner, og af præambel 151 fremgår, at de kompetente nationale domstole bør tage hen-syn til en anbefaling fra den tilsynsmyndighed. der har taget skridt til en bøde. Endvidere skal de idømte bøder under alle om-stændigheder være effektive, stå i rimeligt forhold overtrædelsen og have afskrækkende virkning.

Landsretten finder, at bødefastsættelsen skal ske under hensynta-gen til virksomhedens økonomiske forhold ud fra regnskabsåret for 2018, der afspejler virksomhedens økonomiske situation i pe-rioden, hvor overtrædelsen fandt sted, og som var det senest re-viderede og offentliggjorte regnskab. da tilsynsmyndigheden, Da-tatilsynet, afsluttede sagsbehandlingen og anmeldte [hotelkæden) til politiet."

Datatilsynet bemærker således, at i ovennævnte sag var det seneste regnskab på tidspunktet for Datatilsynets politianmeldelse sammenfal-dende med det regnskab, der afspejlede den dataansvarliges økonomis-ke situation i perioden, hvor overtrædelsen fandt sted.

Det fremgår af politianmeldelserne, at Tiltalte (Region) i 2019 havde et samlet driftsbudget på 25,5 mia. kr.

Tiltalte (Region)s driftsbudget for 2020 var 26,8 mia. kr.8 og for 2021 var det 27,3 mia. kr. Henset til den samlede størrelse af driftsbud-gettet for 2019 er der tale om mindre forhøjelser, og Datatilsynet finder derfor ikke, at det skal føre til en ændret vurdering af bødestørrelsen.
..."

Rettens begrundelse og afgørelse

Skyldspørgsmålet:

Tiltalte (Region) har i begge forhold foretaget anmeldelse til Datatilsynet af datasikkerhedsbrud, og det er ubestridt, at Tiltalte (Region) er data-ansvarlig i begge forhold. Retten lægger herefter overordnet til grund, at der er sket brud på datasikkerheden i begge forhold, og at Tiltalte (Region) var den ansvarlige.

Vedrørende forhold 1:
Det kan efter oplysningerne i sagen lægges til grund, at patienter og pårøren-de til børn, der var under behandling hos Børne- og ungdomspsykiatrisk ambulatorium i Odense, modtog et login med henblik på at udfylde en webformular i en forsknings- og klinisk CBCL-database. Det kan videre lægges til grund, at der ikke var sessionsafgrænsning af dokumenter, gemt i databasen, og at man, efter at have logget sig ind, ved at ændre få cifre i URL-adressen, kunne skaffe sig adgang til personoplysninger, herunder helbredsoplysninger og i enkelte tilfælde personnumre, på andre patienter og forældre i Børne- og ungdomspsykiatrisk afdeling. Det er ubestridt, at der i databasen fandtes personoplysninger på mere end 23.000 registrerede personer, herunder helbredsoplysninger om mindreårige i psykiatrien.

Retten lægger til grund, at databasen har været anvendt til det omhandlede forskningsprojekt fra den 4. januar 2019.

Vidne 2 har forklaret, at det er et kendt problem, at en sim-pel URL ikke er sikker og nem at manipulere, og at en sådan URL-løsning skal kontrolleres. Vidnet har videre forklaret, at en usikker URL nemt kan sikres med login med brugernavn og kode samt sessionsafgrænsning.

Det kan videre lægges til grund, at Tiltalte (Region) den 25. maj 2018 an-meldte et brud på datasikkerheden, som havde med manipulering af en URL-adresse at gøre, og retten finder herefter at kunne lægge til grund, at Tiltalte (Region) havde kendskab til de sikkerhedsmæssige svagheder, der var forbundet med URL-adresser.

Efter forklaringen fra It-direktør Vidne 1 fremgår det, at Tiltalte (Region) forlod sig på, at CBCL-databasen var sikret gennem login og løbende kontroller af en ekstern leverandør.

Efter det anførte, herunder navnlig at Tiltalte (Region)s fokus på sikker-heden burde være skærpet efter den tidligere sag, finder retten, at Tiltalte (Region) har handlet i hvert fald groft uagtsomt ved ikke at have over-holdt sin forpligtelse som dataansvarlig til at gennemføre passende tekniske og organisatoriske foranstaltninger, for at sikre et tilstrækkeligt sikkerhedsni-veau, og at 23.000 personer herved potentielt var i risiko for at andre kunne tilgå deres personlige oplysninger.

Det er derfor bevist, at Tiltalte (Region) har gjort sig skyldig i overens-stemmelse med tiltalen i forhold 1.

Vedrørende forhold 2:
Det kan efter bevisførelsen lægges til grund, at der i 2011 i forbindelse med uddannelsesformål blev udarbejdet en PowerPoint præsentation med grafer udarbejdet på baggrund af bagvedliggende personoplysninger, og at Power-Point præsentationen var direkte tilgængelig på regionens hjemmeside frem til 2014 eller 2015, hvor den pågældende PowerPoint præsentation, i forbin-delse med en ændring af hjemmesiden, blev lagt på dokumentarkiv. Det kan videre lægges til grund, at PowerPoint præsentationen herefter kunne frem-findes via websøgning på forskellige søgemaskiner på søgeord, der havde med lungekræft at gøre, uden der krævedes login eller lignende, og at uved-kommende herved havde mulighed for at tilgå de bagvedliggende personop-lysninger.

Efter oplysningerne i sagen kan det lægges til grund, at en bruger kunne fremfinde PowerPoint præsentationen og ved at klikke på grafen, kunne tilgå personoplysninger på, potentielt 3.915 personer, hvoraf 672 fortsat var i live, og at oplysningerne indeholdt bl.a. personnumre og helbredsoplysninger, her-under oplysninger om dødsårsag og/eller operationstype.

Vidne 2 har forklaret, at det er et kendt problem, at man ved at klikke på en graf, kan tilgå bagvedliggende data, og at sikkerheds-svagheden nemt kan afhjælpes, f.eks. ved at indsætte et screenshot af grafen i en PowerPoint præsentation, således der ikke ved klik på grafen kan tilgås bagvedliggende oplysninger.

It-direktør Vidne 1 har ved sin forklaring henvist til, at datasikker-heden bestod i et scanningsværktøj, som scannede for cpr-numre. Det kan ef-ter det fremkomne lægges til grund, at scanningsværktøjet ikke kunne scanne de bag websiderne liggende oplysninger for personnumre, eller for så vidt for andre oplysninger.

Efter det anførte finder retten, at Tiltalte (Region) har handlet uagtsomt ved ikke at have et tilstrækkeligt kendskab til virkningen af sine egne sikker-hedsforanstaltninger, og ved ikke løbende at gennemføre kontroller af virk-ningen af sikkerhedsforanstaltningerne, der var forbundet med screening af filer, og derved ikke har opretholdt et tilstrækkeligt sikkerhedsniveau, hvor-ved personoplysninger kunne tilgås af uvedkommende, hvilket potentielt ud-gjorde en unødig høj risiko for de 3.915 registrerede borgere og tab af for-trolighed af deres personoplysninger.

Det er derfor bevist, at tiltalte er skyldig i overensstemmelse med tiltalen i forhold 2, dog med den begrænsning, at gerningsperioden, efter anklagemyn-dighedens påstand slutter den 5. februar 2020.

Sanktionen:

Retten finder, at det i Datatilsynets supplerende udtalelse af 8. maj 2024 anførte om bødefastsættelse, herunder formildende og skærpende omstændigheder, jf. databeskyttelsesfordningens artikel 83, stk. 2 har betydning for rettens fastsættelse af bøden.

Som anført af Østre Landsret i U.2023.5579Ø, fremgår det af databeskyttelsesforordningens præambel 150, at der med forordningen er tilsigtet en harmonisering af sanktioner, ligesom det fremgår af databeskyttelsesforordnin-gens præambel 151, at de kompetente nationale domstole bør tage hensyn til en anbefaling fra den tilsynsmyndighed, der har taget skridt til en bøde. Det er videre anført, at de idømte bøder under alle omstændigheder skal være effektive, stå rimeligt i forhold til overtrædelsen og have afskrækkende virk-ning.

Retten har ved bødens fastsættelse lagt vægt på Tiltalte (Region)s driftsbevilling for 2019 på 25,5 milliarder kroner. Det er Tiltalte (Region), der er dataansvarlig i begge forhold, og det derfor regionens samlede driftsbevil-ling, og ikke kun den del, der kan henføres til enkeltsygehuse eller behandlingsområder, der skal lægges til grund i forbindelse med bødeberegningen.

Retten har videre lagt vægt på, at Tiltalte (Region) i forhold 1 tidligere havde fået alvorlig kritik for en lignende overtrædelse, samt på karakteren af de personoplysninger, der er omfattet af sagen, gerningsperiodens varighed, og det ret store antal registrerede personer, der har været berørt og potentielt udsat for risiko for at lide skade, og endvidere på det forholdsvis begrænsede antal berørte, der konkret har fået offentliggjort personoplysninger.

Uanset Tiltalte (Region) efterfølgende har taget skridt til at undgå lignen-de databrud, finder retten, at der ikke er påvist omstændigheder i skærpende eller formildende retning, der giver grundlag for at fravige Datatilsynets ind-stilling til bøde i sagen.

Herefter og efter en samlet vurdering finder retten, at den samlede bøde passende kan fastsættes til 1.000.000 kroner, jf. databeskyttelseslovens § 41, stk. 1, nr. 1, jf. stk. 3, jf. stk. 6 jf. databeskyttelsesforordningens artikel 83, stk. 2, og stk. 4, litra a, jf. stk. 9, jf. artikel 32, stk. 1.

Thi kendes for ret:

Tiltalte (Region) skal betale en bøde på 1.000.000 kr.

Tiltalte skal betale sagens omkostninger.

Dommer