

D O M

afsagt den 23. marts 2026 af Vestre Landsrets 16. afdeling (dommerne Hanne Aagaard, Thomas Elholm og Morten Kornbo Dybro (kst.) med domsmænd) i ankesag

V.L. S – 0113 – 25

Anklagemyndigheden

mod

Tiltalte (Region)

(advokat Dan Bjerg Geary, Aarhus)

Retten i Kolding har den 23. december 2024 afsagt dom i 1. instans (rettens nr. 3-5399/2023).

Påstande

Tiltalte (Region) har påstået frifindelse, subsidiært formildelse.

Anklagemyndigheden har påstået stadfæstelse, dog således at der for så vidt angår beregningen af bødens størrelse skal tages udgangspunkt i Tiltalte (Region)s nettodriftsudgifter for 2021, jf. Datatilsynets udtalelse af 22. august 2025.

Supplerende oplysninger

Datatilsynet har til brug for ankesagen afgivet supplerende udtalelser af 22. august og 7. oktober 2025 samt af 18. februar og 5. marts 2026.

Af et bilag til udtalelsen af 22. august 2025 fremgår bl.a., at Tiltalte (Region)s nettodriftsudgifter vedrørende sundhed i 2019 udgjorde ca. 36 mia. kr., i 2020 ca. 37,8 mia. kr. og i 2021 ca. 39,2 mia. kr.

Tiltalte (Region) har fremlagt en række bilag, herunder kontrakt mellem Hospital og Person 2 fra 2006, databehandleraftale af 22. maj 2018, udtalelse af 12. september 2025 fra Vidne 4, udtalelse af 22. september 2025 fra Person 3, og mails af 10. februar og 2. marts 2026 fra Person 2.

Forklaringer

Vidne 1 har for landsretten i det væsentlige forklaret som i 1. instans. Der er endvidere afgivet forklaring af Vidne 5, Vidne 6 og Vidne 4.

Vidne 1 har supplerende forklaret, at han fra 2016 har været IT-direktør i Tiltalte (Region). Udover den centrale IT-afdeling, som han er leder af, har regionen en række decentrale IT-enheder, som bl.a. står for drift og support. Hans afdeling har en række tværgående opgaver, herunder driftsopgaver, men han er ikke som sådan ansvarlig for de decentrale enheder. Det er korrekt, at regionen var dataansvarlig i forbindelse med de sikkerhedsbrud, der er omfattet af sagens forhold 1 og 2.

CBCL-databasen, som omhandlet i forhold 1, blev anvendt til bl.a. spørgeskemaundersøgelser, herunder i perioden fra 4. januar 2019 til 23. august 2020. Der var ca. 23.000 personer registreret i databasen, men det var ikke alle, der indgik i den konkrete undersøgelse. Hans afdeling vejleder ikke de kliniske afdelinger, og det var på det tidspunkt den decentrale enhed, der stod for gennemførelsen af undersøgelsen, men med støtte og sparring fra hans enhed. Så vidt han husker, rummede databasen ikke de mest følsomme personoplysninger, men det drejede sig vist nok om navn og fødselsdato samt de helbredsoplysninger, som brugerne selv havde indberettet via spørgeskemaerne. Der var således ikke tale om diagnoser indlagt af klinikere. Regionen håndterer og opbevarer mange slags data, herunder data, som ville være mere problematiske i forbindelse med sikkerhedsbrud.

Der var en række tekniske og organisatoriske sikkerhedsforanstaltninger knyttet til anvendelsen af databasen. Adgang til databasen krævede login. Det var således kun personer med et login, som kunne tilgå informationerne, og det kunne kun ske i løbet af en 14-dages periode. Alle handlinger i systemet blev logget. Login var ikke den eneste sikkerhedsforanstaltning, idet der også blev anvendt tests, kryptering og foranstaltninger mod hacking m.v.

De gør generelt meget for at sikre hele IT-landskabet i regionen, og de generelle sikkerhedstiltag vil også kunne beskytte det konkrete datasystem.

Regionen arbejder løbende med at forbedre sikkerheden, og de overvejede også sikkerheden i det konkrete datasystem, som er fra 2005, men som de ikke selv har opbygget. De er derfor afhængige af dem, der har bygget systemet, og de stiller krav til IT-leverandørerne om at levere sikre systemer. De benytter også eksperter til at identificere relevante sikkerhedsforanstaltninger. Regionen har selv ansvaret for at stille kravene til leverandørerne. Kravene i forhold til CBCL-databasen fremgår af databehandleraftalen med Person 2. Regionen gik ud fra, at Person 2 ville leve op til kravene. Det var de nødt til at stole på. Det er komplekst at etablere et sådant datasystem, og det er ikke inden for regionens ekspertise.

Der var kun en enkelt person, som i forbindelse med sin besvarelse af spørgeskemaet i CBCL-databasen var i stand til at gennemskue URL-sårbarheden, og som dermed fik adgang til oplysninger om andre deltagere i undersøgelsen. Vedkommende forsøgte 10 gange at få adgang til andres oplysninger, og det lykkedes i fem af tilfældene. Hvis man angav et andet nummer i URL'en, fik man automatisk adgang til et andet dokument med en anden persons personfølsomme oplysninger. Den pågældende virkede meget IT-kyndig, og han var den eneste af de ca. 4.000 personer, der benyttede spørgeskemaerne, som gennemskuede det. Regionen var ikke selv bekendt med sårbarheden. De opdagede den først, da de blev gjort opmærksom på den af brugeren. Leverandøren blev herefter bedt om at afhjælpe sårbarheden, hvilket lykkedes. Det er sådan, man skal forstå hans forklaring for byretten om, at problemet kunne løses. Hvis de på forhånd havde vidst, at der var et problem, kunne de have undgået det, men de var ikke klar over problemet. De mente på det tidspunkt, at systemet var tilstrækkeligt sikkert. Han er ikke klar over, om det var vanskeligt at løse problemet, eller om det medførte en ekstra opkrævning fra leverandøren, men normalt vil fejl blive håndteret uden beregning. Problemet blev løst inden for 1 måned.

Han mener, at han første gang blev bekendt med problemerne vedrørende URL-sårbarhed i forbindelse med Datatilsynets reaktion på sikkerhedsbruddet i forskningsprojektet om de gravide kvinder. Han blev opmærksom på det, fordi Datatilsynet i brevet af 17. juli 2020 i en fodnote henviser til OWASP, som nærmere har beskrevet sårbarheden. Anmeldelsen vedrørende sikkerhedsbruddet i CBCL-databasen kom i august samme år.

Det er ikke hans opfattelse, at de burde have kendt til URL-sårbarheden i CBCL-databasen, eller at de burde have håndteret situationen anderledes. Regionen har 1.160 da-tasystemer med potentielle sårbarheder, og det er ikke regionen selv, der udvikler syste-merne. Det kan derfor ikke forventes, at de på forhånd kender alle mulige fejlkilder, og det er vanskeligt at teste for fejl, som man ikke kender til. Derfor kunne de ikke have undgået sikkerhedsbruddet i CBCL-databasen ved at teste. Han ved ikke, hvad Datatilsynet mener med, at URL-sårbarheden har været alment kendt siden 2003. Den har muligvis været kendt af Datatilsynet og af andre lignende organisationer. Det er ikke ensbetydende med, at han og regionen skulle have været bekendt med sårbarheden. Sårbarhed med URL er bare en blandt mange sårbarheder. OWASP er en non-profit sikkerhedsorganisation, men orga-nisationens virke er rettet mod IT-udviklere. Det er ikke noget, som en sundhedsorganisa-tion har fokus på. Regionen er derfor nødt til at hente hjælp fra eksperter og må forvente at kunne få tilstrækkelig hjælp.

Regionens risikovurderinger på IT-området bliver løbende revideret. Der blev også lavet en ny risikovurdering efter tilbagemeldingen fra Datatilsynet, hvor regionen blev gjort opmærksom på URL-sårbarheden. Hvert år er der nye forhold, som man skal være opmærk-som på. Der ville derfor under alle omstændigheder være sket en revidering af risikovurde-ningen. De risici, der er oplistet på OWASP top-10 over sårbarheder, blev i 2020 indarbej-det i risikovurderingen.

Det er korrekt, at der blev indberettet et andet sikkerhedsbrud vedrørende URL den 25. maj 2018. URL-sårbarheden fra 2018-sagen er imidlertid ikke sammenlignelig med den nuvæ-rende sag. I sagen fra 2018 opstod sårbarheden i forbindelse med brug af e-Boks. Sagen drejede sig dermed om en applikation, som regionen ikke har ansvar for. Der var tale om en menneskelig fejl hos regionen, hvor en liste med oplysninger var blevet placeret forkert i systemet. De havde derfor fokus på organisatoriske foranstaltninger. I nærværende sag er der derimod tale om en systemfejl.

Sikkerhedsbrud skal indberettes til Datatilsynet inden for en frist på 72 timer. Den slags indberetninger var nye for regionen i 2018, og da sikkerhedsbrud ofte er komplicerede, har man ikke nødvendigvis alle oplysninger inden for 72 timer. Det er derfor sket, at de har givet divergerende oplysninger, hvilket de er blevet kritiseret for. Siden 2018 er de dog blevet klogere på, hvordan de skal beskrive og indberette sikkerhedsbrud. Indberetningerne er blevet mere præcise.

Når man læser indberetningen vedrørende bruddet fra den 25. maj 2018, kan man få det indtryk, at de to sager er mere sammenlignelige, end tilfældet er. Han mener ikke, at sagen fra maj 2018 burde have skærpet regionens opmærksomhed på URL-sårbarhed. Regionen stiller sikkerhedskrav til deres leverandører, efterhånden som regionen bliver opmærksom på de forskellige sårbarheder. Regionen stoledes på Person 2. Han kan ikke svare på, om det ville have været muligt at indhente supplerende ekspertviden.

Det er korrekt, at den i forhold 2 omhandlede PowerPoint-præsentation med de bagvedliggende cpr-numre var tilgængelig via internettet fra 2011 og frem, herunder i tidsrummet fra 25. maj 2018 til 5. februar 2020. Præsentationen omhandlede registrering af cancertilfælde, og der var derfor tale om helbredsoplysninger, men oplysningerne var begrænsede. Præsentationen kunne tilgås uden login eller anden adgangsbegrænsning. Regionen blev først opmærksom på problemet den 4. februar 2020, da de fik en henvendelse fra en borger.

PowerPoint-præsentationen blev uploadet på hjemmesiden i 2011. Det skete i forbindelse med et møde, hvor en læge præsenterede en række data til brug for forbedring af cancerbehandlingen. Lægen havde fået en ekstern til at hjælpe med at udarbejde materialet, herunder en graf med de indlejrede oplysninger. Deltagerne på mødet bad lægen om at dele materialet, og det blev herefter lagt på hjemmesiden.

Regionen var allerede på det tidspunkt opmærksom på problemet med indlejrede data, men personoplysningerne blev ikke fanget i det manuelle tjek. Regionen benyttede fra 2013 også et værktøj, som automatisk scanner for cpr-numre, men værktøjet opdagede ikke oplysningerne, fordi det ikke kunne scanne for indlejrede personoplysninger i grafer og figurer. I 2014 fik regionen ny hjemmeside, og en stor mængde dokumenter blev i den forbindelse lagt på et dokumentarkiv, herunder den pågældende PowerPoint-præsentation, som derefter ikke længere var direkte tilgængelig på hjemmesiden. Desværre var præsentationen i mellemtiden blevet indekseret af Google, og man kunne derfor via Google-søgning finde frem til den. Det blev først stoppet i 2020, da man blev opmærksom på sikkerhedsbruddet.

I 2011 benyttede regionen sig af manuelle kontroller og andre foranstaltninger, som blev udført af bl.a. de forskellige webredaktører. I 2013 indså de, at der var brug for at supplere de manuelle kontroller med tekniske hjælpemidler, og de anskaffede derfor værktøjet Cpr-

tjek. De var opmærksomme på, at værktøjet ikke kunne finde bagvedliggende, indlejrede oplysninger. Derfor var scanningsværktøjet kun et supplement, og det var det bedste på markedet på det tidspunkt. Sårbarheden skulle derfor håndteres via andre foranstaltninger, herunder manuelle tjek foretaget af webredaktører m.fl.

Regionen havde og har en lang række manuelle rutiner for at tjekke for personoplysninger. De har løbende gjort medarbejdere og webredaktører opmærksomme på problemet med indlejrede persondata i PowerPoint-præsentationer, og de har skærpet retningslinjerne efter, at Datatilsynet gjorde opmærksom på problemet. Der har været undervisning af medarbejderne med fokus på de forskellige problemer med indlejrede oplysninger i forskellige filtyper siden 2010. I 2019 blev der lagt en advarsel om skjulte data i dokumenter på regionens intranet, og i 2020 blev der udsendt en reminder til alle webredaktører om at undgå skjulte data i dokumenter. Informationerne på intranettet udskiftes løbende, og der er ikke en fuld historik over ændringerne, men i forbindelse med sagen er en række medarbejdere blevet udspurgt om problemet. Flere webredaktører har bekræftet, at de allerede i 2012, 2014 og 2015 var opmærksomme på disse problemer, idet Datatilsynet havde henledt opmærksomheden på det. Flere af webredaktørerne har således bekræftet, at der løbende, også før 2019, har været undervisningssituationer, hvor der er blevet gjort opmærksom på problemet.

Webredaktørerne er ansvarlige for det indhold, som lægges på inter- og intranettet. Det manuelle tjek for f.eks. cpr-numre foretages af dem, men en af dem har i forbindelse med sagen givet udtryk for, at de ikke nødvendigvis ville have været i stand til at finde frem til de indlejrede personoplysninger, fordi det er en længere og kompliceret proces. Det ville ikke have været tilstrækkeligt blot at højreklikke på grafen i PowerPointen.

Regionen har lavet en beregning, der viser, at en manuel gennemgang af alle dokumenter, som er offentliggjort i perioden fra 2011 til 2020, for indlejrede data, ville kræve 1.500 årsværk. Der er tale om ca. 60 mio. dokumenter. Det ville være praktisk umuligt.

Efter hans opfattelse har regionen hele tiden haft passende organisatoriske og tekniske sikkerhedsforanstaltninger inden for det muliges rammer. Regionen bruger standarden i Fællesregional Informationssikkerhedspolitik fra 2015, der er et rammeværk for beskyttelse af IT-sikkerheden. Den er baseret på en internationalt anerkendt standard med en risikobaseret tilgang. I en organisation som Tiltalte (Region) med 1.160 datasystemer, ca.

100.000 end-points og 3.500 servere skal man være klar over, at det ikke vil være praktisk muligt at sikre alt på samme niveau. Alle 1.160 datasystemer m.v. indebærer potentielle risici. Menneskelige fejl er formentlig den største fejlkilde, men de oplever også fejl og sårbarheder i produkterne fra leverandørerne. Det er i tiltagende grad en kompleks opgave at undgå de forskellige risici og leve op til kravene.

De fællesregionale regler udmøntes i regionens forskellige enheder. Også inden GDPR-reglerne trådte i kraft i 2018, blev der gjort et stort arbejde for datasikkerheden. Mange af de fremlagte dokumenter i sagen vidner om det store arbejde. Sikkerhedsbilledet ændrer sig konstant, og dermed også de forskellige dokumenter. Der er mange regler, der skal overholdes i forbindelse med forskningsprojekter – ikke kun GDPR-reglerne. Regionen får løbende kontrolbesøg fra myndigheder m.v. Det indgår som en del af den overordnede compliance.

Regionens beredskabsplaner er udtryk for et forsøg på at tage højde for det, som potentielt kunne indtræffe, f.eks. hvis et datasystem bliver hacket eller pludseligt bliver utilgængeligt. Man kan altid gøre mere sikkerhedsmæssigt, men det er en balance ud fra en risikobaseret tilgang. Man kan ikke eliminere alle risici. Da GDPR-reglerne blev indført, havde regionen ca. 5 ansatte i afdelingen for IT-sikkerhed; i dag er de 50. Det er dog fortsat svært at undgå alle fejl.

Regionens risikovurderingsskabelon blev tilpasset de nye GDPR-regler i 2018. Risikovurderingen tager udgangspunkt i tre nøglebegreber, hvor tilgængelighed handler om adgang, integritet handler om tillid til oplysningerne, og fortrolighed handler om, at kun dem, som skal have adgang, får adgang. Der er tale om almindeligt benyttede begreber inden for området. Det fremgår af risikovurderingen for CBCL-databasen, at regionen har forholdt sig til, om man kan få adgang til systemet uden at være tildelt en adgang, og at risikoen er vurderet som lav.

Vidne 5 har forklaret, at han er ansat i Datatilsynet som sikkerhedskonsulent, og at han bl.a. deltager i tilsyn. Sikkerhedskonsulenterne har bl.a. til opgave at undersøge, hvad der er sket i sagerne om brud på datasikkerheden. Sagerne overgår senere til juristerne med henblik på at vurdere en eventuel politianmeldelse. Han laver ikke længere selv politianmeldelserne, som det var tilfældet før.

Det indgår som en del af Datatilsynets opgave at vejlede om datasikkerhed. Det sker bl.a. ved offentliggørelse af information på hjemmesiden, men også via tilsynets afgørelser. Tilsynets rådgivning er generel og overordnet. Der rådgives ikke i detaljer om, hvordan man f.eks. skal kode en webapplikation for at gøre den sikker. GDPR-reglerne er heller ikke specifikke. Kravene til de enkelte IT-løsninger beror på de konkrete omstændigheder.

Det er korrekt, at Datatilsynet mener, at Tiltalte (Region)s sikkerhedsforanstaltninger ikke har været tilstrækkelige i forbindelse med sikkerhedsbruddene i forhold 1 og 2. Et sikkerhedsbrud er imidlertid ikke i sig selv ensbetydende med, at sikkerheden ikke har været tilstrækkelig. Programmering af f.eks. en webapplikation til brug for en database er et håndværk som andre håndværk. Hvis man skal lave en sikker software, skal man vide, hvilke risici der skal undgås. Det er den dataansvarliges ansvar at fortælle IT-leverandøren, hvad der kræves af systemet. Spørgsmålet er så, om den dataansvarlige har tilstrækkelig viden til at kunne det. En region, som håndterer store mængder data, bør have de nødvendige ressourcer og kompetencer til at håndtere den opgave.

Et datasystem skal kunne sørge for, at brugerne ikke kan tilgå oplysninger, som de ikke har ret til. Det er i den forbindelse underordnet, om brugeren bevidst klikker sig frem til en URL-adresse, som han ikke må få vist, eller om det sker ved et uheld. Under en session, der typisk foregår, fra man logger på, til man logger af en applikation, skal systemet kunne styre alt, hvad der bliver vist for brugeren. Styringen skal foregå via brugerens identitet. Hvis systemet ikke på denne måde er i stand til at styre, hvad brugeren ser under en session, har det ikke noget formål at anvende et bruger-login. Det har siden 1980'erne været kendt, at URL-adresser i visse sammenhænge kan udgøre en sårbarhed. Sårbarheden er i stigende grad blevet problematisk, efterhånden som der er kommet mere online aktivitet via internettet.

OWASP er en organisation, som i flere årtier har offentliggjort information om datasikkerhed og risici. På organisationens liste over sårbarheder har Broken Access Control løbende figureret på top-10. Denne sårbarhed fremgår således også på kopien af skærbilledet fra OWASPs hjemmeside fra den 8. februar 2003. Broken Access Control er en samlebetegnelse for forskellige sårbarheder, herunder at et login ikke giver tilstrækkelig sikkerhed, hvis man ikke efterfølgende styrer, hvad personen må tilgå af data under en session. URL-problemer kan opstå både pga. menneskelige fejl og andre fejl, men resultatet er, at man får adgang til noget, som man ikke skulle.

Dataansvarlige skal sørge for, at deres datasystemer bliver testet for sårbarheder. Uanset om Tiltalte (Region) på daværende tidspunkt kendte til URL-sårbarheden, burde regionen således have testet systemet og derigennem fundet sårbarheden. Hvis man arbejder med IT-sikkerhed, ved man, at systemerne har sårbarheder, og at man derfor er nødt til at teste og udvikle sine systemer. Det ville være mærkeligt, hvis en organisation med så store IT-opgaver som Tiltalte (Region) ikke kendte til OWASP.

Dataforordningens art. 32 stiller også krav til databehandlere, der er lige så forpligtet til at arbejde med sikkerheden, som dataansvarlige. Det er imidlertid uklart, om databehandleraftalen med Person 2 overhovedet er omfattet af art. 32, og om Person 2 efter aftalen har ansvar for sikkerheden i den software, som han har udviklet. Tiltalte (Region) kunne have stillet krav til test og dokumentation eller selv have foretaget tests, eventuelt med hjælp fra eksterne eksperter. Regionen kunne også have orienteret sig i information fra OWASP eller lignende for at sikre sig, at kravene var opfyldt. Regionen burde have kontrolleret, om systemet var egnet til at sikre det, som systemet skulle. Der var også på det tidspunkt tekniske og andre foranstaltninger, som ville have gjort det muligt at undgå URL-sårbarheder, og som bl.a. blev benyttet af private virksomheder.

De foranstaltninger, der beskrives i Tiltalte (Region)s risikovurdering fra 2018 for CBCL-databasen, er ikke tilstrækkelige. Logning kan kun bruges til efterfølgende at se, hvad der er sket. Det er ikke præventivt. Kryptering er en standardforanstaltning, som er vigtig, men den beskytter ikke mod uvedkommendes adgang. Login er vigtigt i den konkrete situation, men en-faktorlogin anses fra og med 2015 ikke for tilstrækkeligt sikkert. Et stærkt login nedsætter risikoen for databrud, men det fjerner ikke problemet, hvis der fortsat eksisterer en URL-sårbarhed, når brugeren er inde i systemet. I sagen med CBCL-databasen var antallet af brugere begrænset via login, og det var nok ikke sandsynligt, at brugerne ville udnytte sårbarheden. Imidlertid var login svagt, så blot en enkelt hacker kunne have tilgået det hele. Det var problemet. Datasikkerhed er altid et spørgsmål om sandsynlighed og risiko. Det vil sige en afvejning mellem på den ene side sandsynligheden for, at noget går galt, og på den anden side konsekvensen, hvis det sker. Det var forkert af Tiltalte (Region) at vurdere risikoen for sikkerhedsbrud som lav, fordi der var tale om et svagt login. Konsekvensen burde også have været vurderet som ekstremt høj, fordi der var tale om alvorlige konsekvenser i form af afsløring af mindreåriges helbredsoplysninger.

ger. Set i lyset af sagens alvor, har regionen ikke gjort tilstrækkeligt. Det kan skyldes en misvisende risikovurdering.

Datatilsynets afgørelse af 17. juli 2020 har han været med til at udarbejde, men det er ikke ham, der har truffet afgørelsen. Den nævnte sag viste allerede i maj 2018, at hvis brugeren af et datasystem kan ændre en URL-adresse, bevidst eller ubevidst, har man et problem. Fejlene skete, fordi brugerne skulle kopiere URL-adressen over i en browser og i den forbindelse landede et forkert sted, hvor de fik adgang til oplysninger, som de ikke skulle.

Den tidligere sag og nærværende sag er sammenlignelige på den måde, at de begge handler om URL, og at Datatilsynet i begge sager ser på, om regionen har haft passende foranstaltninger og sørget for bl.a. at teste og udvikle systemerne.

Det er hans opfattelse, at regionen ikke har truffet tilstrækkelige foranstaltninger i forhold til sagen om de indlejrede oplysninger i PowerPoint-præsentationen. Datatilsynet har advaret om denne sårbarhedstype siden 2008, dels på tilsynets hjemmeside, dels via målrettet vejledning i mange hundrede breve og e-mails gennem tiden. Det var et kendt problem. Den dataansvarlige skal løbende sørge for at teste, om de anvendte sikkerhedsforanstaltninger fungerer. Det fremgår af Person 3's udtalelse, at de daværende scannings-værktøjer ikke var effektive, men det skulle regionen have fundet ud af, inden deres scanningsværktøj blev taget i brug. Datatilsynet har ikke selv erfaring med dette scannings-værktøj. Regionen kunne fra og med maj 2018 have brugt en enkel organisatorisk foranstaltning ved at udpege nogle få personer som ansvarlige for at tjekke for denne sårbarhed. Hvis læger og professorer selv kan offentliggøre på hjemmesiden, kan man ikke forvente, at systemet er tilstrækkeligt sikkert. Regionen burde have begrænset adgangen til offentliggørelse til nogle få personer og have sørget for at uddanne dem.

Det er hans vurdering, at regionen med det i sagen fremlagte uddannelsesmateriale havde fat i noget af det rigtige. Han kan dog ikke af materialet se, om der var fokus på netop den type sårbarhed. Den pågældende PowerPoint-præsentation havde været tilgængelig meget længe. De vurderede derfor, at regionens sikkerhedsforanstaltninger var utilstrækkelige. Det indgik også i vurderingen, at regionen havde baseret sig på et utilstrækkeligt scanningsværktøj. Det følger af dataforordningens art. 32, at man skal have tilstrækkelige foranstaltninger, ikke ultimative foranstaltninger, så enhver fejl undgås. Man skal således have kendskab til og tjekke sine værktøjer, ligesom man løbende skal uddanne de ansatte og

f.eks. have en webredaktør, der kontrollerer materialet. Derved udelukkes fejlene ikke, men det vil efter omstændighederne være tilstrækkelige sikkerhedsforanstaltninger.

Datatilsynet var ikke bekendt med, om den enkelte læge selv kunne uploade materialet. Hvis materialet ved en fejl var blevet lagt ud, kunne det opdages ved en manuel gennemgang. Det ville have været en stor opgave, men bruddet stod på i lang tid, og regionen havde mange år til at ordne det. Han er ikke bekendt med, at det skulle dreje sig om 60 mio. dokumenter, og at det ville kræve 1.500 årsværk at kontrollere dokumenterne. Han tror ikke, at Datatilsynet har været bekendt med tallene, men det er oplysninger, som må indgå i straffesagen.

Hvis regionen havde fjernet PowerPoint-præsentationen fra internettet tidligere, ville problemet have været løst. Han er ikke bekendt med, om der var nogle værktøjer, som ville være gode nok til at finde fejlen. Datatilsynet har fokus på datasikkerheden, ikke de økonomiske rammer. Hans opgave som IT-sikkerhedskonsulent er at beskrive IT-problemerne; det er ikke hans opgave at vurdere, hvad det ville kræve at rydde op i data.

Han er blevet præsenteret for foranstaltninger, som regionen efterfølgende har truffet. Det var hans opfattelse, at foranstaltningerne vedrørende webredaktion og uddannelse var til-tag, der først blev iværksat efter sikkerhedsbruddet, eller at disse tiltag i hvert fald havde fået et andet format. Det ville muligvis have ændret hans vurdering, hvis han havde vidst, at der også før sikkerhedsbruddet var foranstaltninger i regionen i form af løbende undervisning af personale og instruktion af webredaktører m.v. Den skriftlige udtalelse, som er fremsendt af regionen ved mail af 14. januar 2022, hvor der står, at der foruden screeningsværktøj også var andre sikkerhedsforanstaltninger som undervisning af webredaktører og generel awareness for medarbejderne, kunne godt tyde på, at Datatilsynet har været i en misforståelse angående tidspunktet for iværksættelse af disse foranstaltninger. I politianmeldelsen af 17. september 2021 giver Datatilsynet udtryk for, at regionen først efter sikkerhedsbruddet har implementeret sådanne foranstaltninger. Efter hans vurdering var det Datatilsynets opfattelse, at der ikke var andre værktøjer end screeningsværktøjet. Efter dataforordningens art. 32 er det dog heller ikke tilstrækkeligt med uddannelse af medarbejderne. Der kræves også bl.a. løbende testning af, om de truffe foranstaltninger er tilstrækkelige. Det beror på en konkret risikovurdering, hvor ofte der skal foretages testning.

I forbindelse med sikkerhedsbrud som f.eks. URL-sårbarheden i forhold 1 overvejer Datatilsynet, hvem der skal sanktioneres, herunder overvejes både den dataansvarlige og databehandleren. Det er en konkret vurdering, men den dataansvarlige vil næsten altid være ansvarlig for sikkerhedsbruddet i et eller andet omfang. Datatilsynet har før oplevet, at store IT-leverandører til offentlige myndigheder afviser at have et ansvar efter GDPR-reglerne, når der opstår sikkerhedsbrud. Ansvarsplacering er dog ikke en del af hans arbejdsområde. Det fremgår ikke af databehandleraftalen af 22. maj 2018 med Person 2, om aftalen også omfattede kodningen af CBCL-systemet, der skete mange år før aftalen.

Der blev under høringen af regionen spurgt til, hvilke test der blev gennemført, men som han husker det, blev spørgsmålet aldrig besvaret. Det fremgår af den supplerende udtalelse af 18. februar 2026 fra Datatilsynet, at det var uklart, hvad der blev testet. De tests, som Person 2 angiver, vedrører ikke den type sårbarhed, som sagen angår. URL-sårbarheden var en kendt sårbarhed, og den var simpel at finde frem til. Man kender ikke ”hullerne” på forhånd. Det er derfor, man tester.

Vidne 6 har forklaret, at hun siden maj 2022 er ansat som jurist ved Datatilsynet.

Datatilsynets værktøjskasse i forbindelse med sikkerhedsbrud fremgår overordnet af dataforordningens art. 58, stk. 2. Det drejer sig om påbud, forbud og kritik samt indstilling til bøde. De anvender kriterierne i art. 83, stk. 2, og inddrager dem i vurderingen af den konkrete sags grovhed og strafværdighed. Sagen om de gravide kvinder fra 2018, hvor Datatilsynet i 2020 udtalte alvorlig kritik af Tiltalte (Region), har indgået i vurderingen af grovheden i nærværende sag, idet regionen efter Datatilsynets opfattelse burde have kendt til URL-sårbarheden allerede før 2020.

Ved fastsættelse af bødeniveauet ser Datatilsynet overordnet på kriterierne i dataforordningens art. 83. Derudover lægges der vægt på driftsbevillingen, hvis det er en kommune, og nettodriftsudgifterne, hvis det er en region. I det foreliggende tilfælde er det relevant at se på dommen mod Region Midtjylland, som blev afgjort med en bøde på 300.000 kr.

Det fremgår af Datatilsynets udtalelse af 22. august 2025, at bødefastsættelsen skal ske ud fra en samlet vurdering, og at nettodriftsudgifterne kun er et blandt flere momenter. I den konkrete sag har Datatilsynet ud fra en samlet vurdering ikke fundet, at forskellen mellem nettodriftsudgifterne for 2019 og 2021 skal have betydning for bødens størrelse. Datatilsy-

net er således fortsat af den opfattelse, at en bøde for hvert af forholdene passende kan fastsættes til 500.000 kr. Datatilsynet er imidlertid af den opfattelse, at der skal tages udgangspunkt i netto driftsudgifterne for 2021. Det skyldes en afgørelse fra EU's databeskyttelsesråd, hvor man i forbindelse med en privat virksomhed lægger vægt på virksomhedens senest offentliggjorte årsregnskab på det tidspunkt, hvor tilsynsmyndigheden træffer afgørelse, herunder indgivelse af politianmeldelse. Fremgangsmåden er fulgt i en dom fra Østre Landsret.

I nærværende sag er der i forbindelse med bødeberegningen taget hensyn til, at det drejer sig om en offentlig myndighed. Efter lovbemærkningerne gælder et bødeloft på 8 mio. kr. for overtrædelse af dataforordningens art. 32. Det fremgår tillige, hvad der skal lægges vægt på.

Det fremgår af Datatilsynets udtalelse af 8. maj 2024, at de begrænsede skadevirkninger af sikkerhedsbruddene i sagen efter Datatilsynets opfattelse ikke skal anses for en formildende omstændighed. Det skyldes, at dataforordningens art. 32 er et risikodelikt, og at det er en tilfældighed, at personoplysningerne ikke blev tilgået i videre omfang end sket. Hun har ikke selv været med til at behandle bødeberegningen i nærværende sag, men så vidt hun ved, er den baseret på de nye retningslinjer fra EDPB, hvoraf det fremgår, at der ønskes en vis harmonisering på EU-niveau, og at den slags momenter ikke skal være formildende.

Vidne 4 har forklaret, at han bistår topledelse med IT-rådgivning. Han har ikke arbejdet for Tiltalte (Region) i 2025, men han har tidligere bistået regionen med bl.a. undervisning og træning i IT-beredskab og -ledelse. Han har også hjulpet regionen som IT-konsulent i forbindelse med en rådgivningsvirksomhed, som han tidligere var en del af. Det ligger nogle år tilbage. Han har ikke haft forretningsforbindelser med Vidne 1, men han kender ham fra et erhvervsnetværk.

I 2013 var der ikke et værktøj til rådighed, der kunne scanne dokumenter for indlejrede informationer, herunder CPR-numre. Det var fortsat tilfældet i 2018. Der er mange falske positive. Hvis værktøjet for eksempel leder efter talkombinationer med 14 cifre, kan det fejlagtigt komme til at medtage kontonumre eller andre tal. Han mener, at en manuel kontrol suppleret af et automatisk scanningsværktøj samlet er en rimelig og passende foranstaltning. Et automatisk scanningsværktøj genererer typisk en alarm, når værktøjet finder noget, hvorefter det skal følges op af en manuel kontrol. Han tror ikke, at nogen virksom-

hed ville påtage sig at foretage en manuel kontrol af 60 mio. dokumenter. Man arbejder ikke med garantier inden for IT-sikkerhed. Man vurderer sikkerhedsindsatsen i forhold til sandsynlighed og konsekvens.

Han er enig med Person 3 i, at indlejrede data ikke var den mest oplagte fejlkilde at teste for. Han ville selv have fokuseret på undervisning og instruktion, så lægerne var opmærksomme på, hvad de lagde ud på nettet. Den pågældende hændelse ville han have anset for være i kategorien lav risiko. Det var potentielt meget usandsynligt, at den ville føre til sikkerhedsbrud.

Google og andre søgemaskiner vil ikke kunne fange indlejrede oplysninger. Særligt på det tidspunkt var det svært at finde metadata i dokumenter og filer. Man ville skulle scanne hvert enkelt dokument manuelt. Det vil være en næsten umulig opgave at finde de dokumenter i Googleindeks, som tidligere måtte være slettet fra regionens hjemmeside. Cache er et hukommelseslager, som ligger i Googles hukommelse. Det er uden for regionens kontrol. Man kan ikke spørge Google, hvor bestemte filer med indlejrede data ligger, og hvis man endelig fandt et dokument, ville det kræve, at man åbnede og kontrollerede det.

Han ved ikke, om der findes 300.000 forskellige slags IT-trusler, men der er mange, og der kommer hele tiden nye til. Nogle er mere kritiske end andre. Alle regionens systemer er potentielt eksponeret for dem.

Regionens risikovurdering fra 2018 ligner en meget almindelig tilgang til IT-sikkerhed, hvor man ser på sandsynlighed og konsekvenser. Grundigheden er i orden. Der indgår brugerstyring og sessionsafgrænsning. Der er forskel på, hvordan man foretog risikovurderinger i 2018 i forhold til i dag.

Det er en fornuftig mængde tests, der er beskrevet af Person 2 i mail af 10. februar 2026. Der er tale om gængse tests, også efter 2018-standarder, og der mangler ikke noget, selv om man sikkert ville kunne tilføje flere. Han kender ikke Person 2 eller hans virksomhed, men han kan se af certificeringen, at Person 2 har en indgående viden og forståelse af området.

De tekniske og organisatoriske foranstaltninger vedrørende CBCL-databasen, som er beskrevet i støttebilaget, svarer til almindelig praksis i 2018. Sårbarheder vedrørende URL

har været kendt i to årtier. Der er tale om en sårbarhed, som hundredvis af andre. Den er ikke usædvanlig. Hvis han skulle svare på, om regionen burde have kendt til sårbarheden, kan han ikke svare nej.

Det er helt almindeligt, at der ligger indlejrede data i grafer, som henter information fra f.eks. excel-filer. Det er derimod ikke almindeligt kendt, at det kan være personoplysninger. Han har ikke været klar over, at problemet med indlejrede persondata i PowerPoints har været kendt i en årrække. Han kender ikke værktøjet Cpr-tjek. Han har fået demonstreret forskellige værktøjer, men han har ikke selv arbejdet med dem. Han kan ikke svare på, om regionen burde have indset, at der ikke fandtes tekniske løsninger, der kunne finde CPR-numre i grafer m.v. Man kan finde den slags data via en manuel proces, hvor man åbner grafen for at se, om der gemmer sig noget bagved. Det ville være en omstændelig proces. En manuel gennemgang foretaget af tredjepart ville ikke være udelukket, men han har aldrig selv anvendt denne mulighed eller hørt om andre, som har.

Landsrettens begrundelse og resultat

Skyldsspørgsmålet

Det kan lægges til grund som ubestridt, at Tiltalte (Region) var dataansvarlig i forbindelse med de brud på persondatasikkerheden, der er anført i forhold 1 og 2, jf. databeskyttelsesforordningens art. 4, nr. 7.

Spørgsmålet er herefter, om Tiltalte (Region) som dataansvarlig i gerningsperioderne har gennemført passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de foreliggende risici, jf. databeskyttelsesforordningens art. 32, stk. 1.

Vedrørende forhold 1

Det fremgår af sagens oplysninger, at Tiltalte (Region) anvendte CBCL-databasen, der indeholdt person- og helbredsoplysninger om ca. 23.000 borgere, og at databasen i perioden fra 4. januar 2019 til 23. august 2020 blev anvendt til en spørgeskemaundersøgelse.

Det fremgår endvidere, at deltagerne i undersøgelsen blev tildelt et login, og at det efter login var muligt at ændre i URL-adresser i datasystemet, hvorved der kunne tilgås helbreds- og personoplysninger om andre deltagere i undersøgelsen. Denne mulighed blev

udnyttet af en af deltagerne i undersøgelsen, som det lykkedes at tilgå oplysninger vedrørende fem andre deltagere, og som derefter den 23. august 2020 gjorde Tiltalte (Region) opmærksom på sikkerhedsbruddet.

Vidne 1 har forklaret, at Tiltalte (Region) ikke selv var bekendt med sårbarheden vedrørende URL-adresserne, før sikkerhedsbruddet blev konstateret.

Vidne 5 har forklaret, at sårbarheder vedrørende URL-adresser har været et kendt sikkerhedsproblem siden 1980'erne, og at sikkerhedsorganisationen OWASP i hvert fald siden 2003 har anført denne type sårbarhed på deres top-10-liste over IT-sårbarheder under betegnelsen Broken Access Control. Han har endvidere forklaret, at det ville være mærkeligt, hvis en organisation med så store IT-opgaver som Tiltalte (Region) ikke kendte til OWASP.

Vidne 4 har forklaret, at sårbarheder vedrørende URL har været kendt i to årtier, og at der ikke er tale om nogen usædvanlig sårbarhed, hvorfor han ikke kan svare nej til, at Tiltalte (Region) burde have kendt til sårbarheden.

Det fremgår af sagens oplysninger, at Tiltalte (Region) den 25. maj 2018 anmeldte et andet brud på datasikkerheden, som havde med URL at gøre.

På den anførte baggrund lægger landsretten til grund, at Tiltalte (Region) under hele gerningsperioden som minimum burde have været bekendt med den sårbarhed, som anvendelse af URL-adresser indebærer, samt den risiko for utilsigtet adgang, som er forbundet hermed.

Vidne 1 har endvidere forklaret, at der var truffet passende foranstaltninger bl.a. i form af krav om login med en begrænset gyldighed på 14 dage, logning af alle handlinger i systemet, anvendelse af tests og kryptering samt foranstaltninger mod hacking. Desuden havde regionen indgået en databehandlersaftale vedrørende CBCL-databasen med en IT-leverandør, og der var grund til at tro, at leverandøren levede op til sikkerhedskravene, herunder ved at foretage relevante tests.

Det fremgår af Vidne 5's forklaring, at det anvendte login til CBCL-databasen efter hans opfattelse var svagt, og at anvendelse af login ikke afhjælper den på-

gældende URL-sårbarhed eller systemets manglende evne til at styre, hvad der kan vises for brugeren efter login. Tiltalte (Region) burde derfor have stillet andre krav til IT-leverandøren og eventuelt fået en ekstern konsulent til at se på mulige sårbarheder, ligesom regionen løbende burde have kontrolleret, om datasystemet var egnet til at sikre det, som systemet skulle.

Efter bevisførelsen for landsretten, herunder de fremlagte oplysninger om tests fra databehandler Person 2, lægger landsretten til grund, at CBCL-systemet ikke har været tilstrækkeligt testet eller kontrolleret for sårbarheder vedrørende URL eller manglende sessionsafgrænsning.

På den anførte baggrund finder landsretten, at Tiltalte (Region) har handlet uagtsomt ved ikke at have gennemført passende tekniske og organisatoriske foranstaltninger, jf. databeskyttelsesforordningens art. 32, stk. 1.

Landsretten tiltræder herefter, at Tiltalte (Region) er fundet skyldig i forhold 1.

Vedrørende forhold 2

Det fremgår af sagens oplysninger, at der i 2011 blev uploadet en PowerPoint-præsentation vedrørende cancerbehandling på Tiltalte (Region)s hjemmeside, og at det via en graf i præsentationen var muligt – efter en nærmere bestemt procedure – at tilgå en række bagvedliggende CPR-numre. Præsentationen kunne tilgås via internettet indtil den 5. februar 2020, hvor Tiltalte (Region) blev gjort opmærksom på sikkerhedsbruddet via en henvendelse fra en borger.

Det fremgår endvidere, at Tiltalte (Region) fik en ny hjemmeside i 2014 eller 2015, og at der i den forbindelse blev flyttet en mængde data fra hjemmesiden til et dokumentarkiv, herunder den pågældende PowerPoint-præsentation, som dermed ikke længere var tilgængelig fra regionens hjemmeside. Præsentationen var dog i mellemtiden blevet indekseret af Google, og den kunne derfor fortsat fremsøges via Google indtil den 5. februar 2020.

Gerningsperioden i forhold 2 angår tidsrummet fra 25. maj 2018 til 5. februar 2020, og spørgsmålet om Tiltalte (Region)s forpligtelser efter databeskyttelsesforordningens art. 32, stk. 1, skal således bedømmes på dette tidspunkt.

Efter bevisførelsen for landsretten, herunder bl.a. forklaringen afgivet af Vidne 1, lægger landsretten til grund, at Tiltalte (Region) i gerningsperioden var bekendt med problemet med indlejrede data i filer. Det lægges endvidere bl.a. på baggrund af Vidne 4's forklaring til grund, at der på dette tidspunkt ikke fandtes tekniske værktøjer, som effektivt ville kunne fremsøge sådanne indlejrede data, og at en kontrol af regionens dokumentarkiv for at finde eventuelle indlejrede data i forskellige filer i givet fald skulle ske manuelt, og at det ville være en omfattende opgave.

Vidne 5 har forklaret, at det efter hans vurdering var Datatilsynets opfattelse på tidspunktet for politianmeldelsen, at Tiltalte (Region) alene havde tekniske sikkerhedsforanstaltninger i form af et utilstrækkeligt scanningsværktøj, og at det muligvis ville have ændret hans vurdering, hvis det måtte lægges til grund, at regionen også forud for konstateringen af sikkerhedsbruddet havde foranstaltninger i form af løbende undervisning af personale og instruktion af webredaktører.

Efter bevisførelsen for landsretten, herunder forklaringen afgivet af Vidne 1 og regionens skriftlige udtalelse, som er fremsendt ved mail af 14. januar 2022, hvoraf det fremgår, at regionen foruden tekniske foranstaltninger også havde organisatoriske foranstaltninger i form af undervisning af webredaktører og generel orientering af medarbejdere, lægger landsretten til grund, at Tiltalte (Region) både før og under gerningsperioden i et vist omfang har haft relevante organisatoriske sikkerhedsforanstaltninger.

På denne baggrund, og efter en samlet afvejning af risici i forhold til de trufne og mulige foranstaltninger, finder landsretten, at der ikke er det til domfældelse fornødne bevis for, at Tiltalte (Region) i forhold 2 ikke har haft passende tekniske og organisatoriske foranstaltninger, jf. databeskyttelsesforordningens art. 32, stk. 1.

Tiltalte (Region) frifindes derfor i forhold 2.

Sanktionsfastsættelsen

Landsretten finder, at bøden, der fastsættes efter de bestemmelser, som byretten har anført, passende kan fastsættes til 500.000 kr.

Der er ved bødefastsættelsen taget udgangspunkt i Datatilsynets bødeindstilling og i kriterierne i databeskyttelsesforordningens art. 83, stk. 2 og 9. Der er herved navnlig lagt vægt

på overtrædelsens karakter, alvor, varighed og konsekvenser, samt det forhold, at overtrædelsen er begået uagtsomt, og at Datatilsynet den 17. juli 2020 har udtrykt alvorlig kritik af Tiltalte (Region) for manglende datasikkerhed i forbindelse med håndtering af URL-adresser. Endelig er der lagt vægt på, at Tiltalte (Region) er en offentlig myndighed og på oplysningerne om regionens driftsbevillinger.

Med de anførte ændringer stadfæster landsretten dommen.

Efter ankesagens udfald skal statskassen betale sagens omkostninger for landsretten. Vederlaget til advokat Dan Bjerg Geary, der har været valgt forsvarer for Tiltalte (Region), skal dog ikke betales af statskassen, jf. retsplejelovens § 1007, stk. 2, idet der efter det oplyste ikke foreligger sådanne særlige omstændigheder, at der er grundlag for undtagelsesvis at bestemme, at statskassen helt eller delvist skal betale vederlaget til den valgte forsvarer.

T h i k e n d e s f o r r e t:

Tiltalte (Region) skal betale en bøde på 500.000 kr.

Byrettens afgørelse om sagsomkostninger stadfæstes.

Statskassen skal betale sagens omkostninger for landsretten, dog ikke vederlaget til den valgte forsvarer, advokat Dan Bjerg Geary.

Hanne Aagaard Thomas Elholm Morten Kornbo Dybro (kst.)