RETTEN I ROSKILDE

Udskrift af dombogen

D O M

afsagt den 9. marts 2022

Rettens nr. 9A-8331/2020
Politiets nr. 1200-84266-00011-20

Anklagemyndigheden
mod
Tiltalte Kommune
CVR nr.

Anklageskrift er modtaget den 23. november 2020.

Tiltalte Kommune, Adresse, By er tiltalt for

overtrædelse af databeskyttelsesforordningens artikel 32, stk. 1, 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, ved i perioden fra den 25. maj 2018 til november 2018 ikke at have over-holdt sin forpligtelse som dataansvarlig til at gennemføre tekniske og organisatoriske foranstaltninger, der passede til risicierne af varierende sandsynlighed og alvor for de registrerede rettigheder, idet medarbejderne i Tiltalte Kommunes afdeling, Center for Børn og Unge, i perioden fra den 5. januar 2016 til november 2018 uploadede 135 indstillingsskemaer på kommunens medar-bejderportal, heraf 21 indstillingsskemaer i tiden efter den 25. maj 2018, hvori der fremgik oplysninger om navn, fødselsdato, kontaktoplysninger, personnummer, økonomiske forhold, strafbare forhold, etnicitet, seksuelle forhold eller orientering og oplysninger om helbred, herunder psykiske og fysiske lidelser om 452 borgere, herunder 402 borgere under 18 år, hvilke oplysninger var tilgængelige på medarbejderportalen frem til den 5. november 2019, uden at der var etableret adgangskontrol, således at kun brugere, der havde et arbejdsbetinget behov for at have adgang til oplysningerne kunne tilgå dem, ligesom der ikke blev foretaget maskinel registrering (logning) af hvem der tilgik oplysningerne, der på medarbejderportalen kunne tilgås af al-le kommunens medarbejdere, hvilket udgjorde en unødigt høj risiko for de registrerede borgere for, at uvedkommende fik adgang til oplysningerne.

Påstande

Anklagemyndigheden har nedlagt påstand om, at tiltalte idømmes en bøde på 50.000 kr.

Tiltalte har erkendt sig skyldig, men er uenig i bødens størrelse.

Sagens oplysninger

Tiltalte Kommune ved Vidne 1 har forklaret, at han blev ansat i 2020 og således efter hændelsen, der førte til nærværende sag. Han er dog blevet bekendt med mange af de forhold, der gjorde sig gældende i kommunen på tidspunktet for hændelsen. Årsagen til at de pågældende indstillingsskemaer med personfølsomme oplysninger lå på medarbejderportalen var, at medarbejderportalen på daværende tidspunkt blev anvendt som fagsystem for en række områder, der ikke havde egne fagsystemer. Medarbejderportalen fungerede i grunden som en slags intranet for alle medarbejdere, hvor man kun-ne klikke sig ind på forskellige fagområder. Den blev dog i sagsbehandlingen for de pågældende områder også brugt som alternativ til et fællesdrev. Selve sagsbehandlingen er formentlig foretaget i et Worddokument, hvorefter det er lagt op på medarbejderportalen. Han kan ikke udtale sig om, hvorvidt kommunen på daværende tidspunkt havde gjort sig overvejelser om, hvorvidt denne konstellation var en god ide. Denne løsning blev brugt, da det var den, man havde. Der er adgangsstyring i medarbejderportalen, så det er ikke alle medarbejdere, der har adgang til alt. Det var der egentlig også på daværende tidspunkt, men det viste sig, at der var sket en fejl i denne adgangsstyring, som medførte, at alle kommunens medarbejdere teoretisk set havde adgang til de pågældende indstillingsskemaer. Havde adgangssikringen virket, havde brugen af medarbejderportalen været sikker nok til at kunne anvendes. Der er ikke nogen logning af adgangen til medarbejderportalen, så det er ikke muligt at se, hvem der har været inde og se på indstillingsskemaerne. En me-darbejder, der havde denne adgang, men som ikke burde have det, skulle en-ten klikke sig igennem en række menuer eller søge på ord, der indgik i indstillingsskemaerne, for at komme frem til dem. I maj 2018 blev der lavet kontrolsøgninger, hvor indstillingsskemaerne ikke dukkede op, men på et senere tidspunkt i november 2019 blev der igen lavet nogle kontrolsøgninger, hvor indstillingsskemaerne dukke op i søgeresultaterne. Dette tyder på, at fejlen i adgangsstyringen er opstået på et tidspunkt i den mellemliggende periode, men uden at det kan undersøges mere præcist hvornår. Antallet af medarbej-dere, der har haft adgang til indstillingsskemaerne er ikke så højt, som det er oplyst i sagen. Der er omkring 800 kommunale medarbejdere ansat på skoler, som slet ikke har adgang til medarbejderportalen, ligesom der er en lang ræk-ke medarbejdere, der ikke til dagligt har adgang til en computer og dermed heller ikke til medarbejderportalen. Disse medarbejderes adgang til indstillingsskemaerne har derfor været rent teoretisk. Det har teknisk set været mu-ligt for omkring 2.000 medarbejdere at tilgå indstillingsskemaerne, men set fra et praktisk synspunkt, er det mellem 500 og 800 medarbejdere, der har haft mulighed for at tilgå dem. Han kan ikke svare på, hvorledes man i kom-munen fra 2016 og frem til 2018 sikrede forsvarlig behandling af personføl-somme oplysninger. I november 2018 blev arbejdsgangene ændret, idet man overgik til et ESDH-system (elektronisk sags- og dokument behandlingssy-

stem), hvori dokumenter blev gemt i stedet for i medarbejderportalen. Han kender ikke årsagen hertil, men det har formentlig været, at man ikke mente, at løsningen med brug af medarbejderportalen var tidssvarende. Om det har været på grund af GDPR-regler eller blot for at lette sagsgange, det ved han ikke. Det er korrekt, at indstillingsskemaerne ikke blev slettet fra medarbej-derportalen i forbindelse med overgangen til sagsbehandling i ESDH-syste-met. Han ved ikke nærmere om, hvad der er årsagen til, at indstillingsskema-erne ikke blev slettet, men han ved, at adgangen til indstillingsskemaerne blev fjernet, så snart man blev opmærksom på, at for mange brugere havde ad-gang til dem. I november 2019 var der en kommunikationskonsulent med an-svar for medarbejderportalen som foretog nogle kontrolsøgninger, og ved disse kontrolsøgninger dukkede indstillingsskemaerne op. Konsulenten oply-ste dette til kommunens it-afdeling, som slettede indstillingsskemaerne fra medarbejderportalen, efter de havde sikret, at dokumenterne var behørigt jo-urnaliseret. Hændelsen blev derefter indberettet. Datatilsynet bad i to omgan-ge kommunen om svar på uddybende spørgsmål. Han var ikke med til besva-relsen af disse. Direktionen blev orienteret om hændelsen, og det blev drøf-tet, om man skulle informere de borgere, som indstillingsskemaerne vedrørte. Dette valgte man ikke at gøre, hvilket Datatilsynet var enige i. Efterfølgende blev der lavet kampagner til at instruere medarbejdere i, hvordan personføl-somme oplysninger skal behandles, og hvad de skal være opmærksomme på. Der blev også lavet vejledninger og videoer om emnet, som lå på medarbej-derportalen. Kommunen har ikke hørt fra nogle borgere, der har fået oplevet at få misbrugt de pågældende personlige oplysninger, og der er heller ikke nogen af kommunens medarbejdere, der har oplyst, at de havde opdaget, at de havde adgang til dokumenter, som de ikke burde have adgang til. Medar-bejderne er instrueret i at oplyse det, hvis de støder på sådanne forhold. Man lægger i kommunen stor vægt på, at medarbejderne har tillid til, at de kan oplyse om fejl, som de er blevet bekendt med.

Vidne 2 har som vidne forklaret, at at hun har været ansat i Datatilsynet siden maj 2019. Hun har tidligere været anklager i 8 år, og hendes overord-nede funktion i Datatilsynet har været at styrke behandlingen af straffesager på området. Hun har også siddet med i en taskforce i EU vedrørende en bø-devejledning på området. Persondataloven viderefører i vidt omfang de tidli-gere gældende regler. Førhen var sikkerhedsbekendtgørelsen gældende for offentlige myndigheder og indeholdt regler om logning mv. Databeskyttelses-forordningens artikel 32 har videreført de samme regler, som var gældende i henhold til sikkerhedsbekendtgørelsen, om end de er formuleret mere gene-relt. Det var dog førhen ikke muligt at sanktionere offentlige myndigheders overtrædelser af persondatareglerne med bøder. Dette har man fra EU's side valgt at give mulighed for, særligt begrundet i at det ikke er valgfrit for bor-gerne at få deres personlige oplysninger behandlet af det offentlige. Det fremgår af forarbejderne omkring bødeniveauet, at bødeloftet for offentlige myndigheder bør være lavere end for private, da der skal tages hensyn til, at der ofte er tale om lovbundne opgaver, og at det kan være vanskeligt at stop-pe en igangværende sagsbehandling i tilfælde af et brud på databeskyttelses-

reglerne. Det fremgår klart af forarbejderne, at bøderne på området skal være af en størrelse, hvor de har en afskrækkende effekt. Det er kun i Danmark og i Estland, hvor det ikke er tilsynsmyndigheden selv, der udsteder bøderne på området. Datatilsynet er ikke en ny myndighed, men har vurderet sager siden 1979, så det er ikke en ny opgave for Datatilsynet at vurdere og kategorisere brud på persondatareglerne. Datatilsynet kan udtale kritik eller alvorlig kritik, og de kan give påbud, eller de kan politianmelde forhold. Det er altid en konkret vurdering, hvilken reaktion der bør anvendes, og politianmeldelse sker kun i de groveste tilfælde, hvor de andre reaktioner ikke findes tilstræk-kelige. Politianmeldelser er altid en ledelsesbeslutning, og den bliver kun an-vendt, når der er tale om klare overtrædelser, hvor der ikke findes at kunne være fortolkningsspørgsmål omkring reglerne eller deres anvendelse. I den konkrete sag i Tiltalte Kommune kunne der ikke være tvivl om, at der var tale om en overtrædelse af reglerne. Der var tale om meget følsomme oplysnin-ger, som et stort antal medarbejdere havde adgang til uden at have arbejds-mæssigt behov for det. Hvis det antages, at størstedelen af kommunens me-darbejdere bor i kommunen, så er det op mod 10 % af kommunens borgere, der havde adgang til oplysningerne. Det er en skærpende omstændighed, at man på grund af kommunens manglende logning ikke kan følge op på, om der er sket misbrug af oplysningerne. Det har derfor heller ikke nogen betyd-ning for Datatilsynets vurdering, at der ikke konkret er påvist tegn på, at op-lysningerne har været i forkerte hænder. Det stod eksplicit nævnt i sikker-hedsbekendtgørelsen, at der skulle være adgangsstyring og logning, og det er de samme regler, der er videreført i databeskyttelsesforordningens artikel 32. Der er ikke i Danmark givet bøder til offentlige myndigheder for overtræ-delser af databeskyttelsesforordningen endnu, men der er indgivet flere sager, hvoraf denne er den første, der bliver prøvet ved domstolene. Datatilsynet har i deres indstilling til bødestørrelsen i nærværende sag taget en lang række faktorer med i vurderingen, så indstillingen er effektiv og proportional. Der er blandt andet taget hensyn til, at en bøde til en kommune i princippet beta-les af borgernes egne skattekroner, hvorfor bødeniveauet tænkes fastsat væ-sentligt lavere end i sager mod private virksomheder. Der er kigget på kom-munens indbyggertal og driftsbevilling. Derudover er der i høj grad også lagt vægt på grovheden af overtrædelsen. Det gør også en stor forskel, at der her er tale om en fast praksis, der over en længere periode har været klart i strid med reglerne, hvorimod der vil ses mildere på et brud, der skyldes en enkelt menneskelig fejl, hvilke man aldrig kan helgardere sig imod. Kommunen skal i henhold til forordningens artikel 32 fastsætte en "passende sikkerhed" , hvil-ket vil sige, at man skal gardere sig så godt man kan imod fejl. Det har ikke nogen afgørende betydning, at der i nærværende sag ikke er konstateret, at de personfølsomme oplysninger har været i forkerte hænder, idet skaden alle-rede er sket ved, at en så stor gruppe af uvedkommende har haft adgang til oplysningerne. Det har heller ikke afgørende betydning, at kommunens me-darbejdere har tavshedspligt, da denne kun omfatter de medarbejdere, der be-handler sagerne. Det har været lovpligtigt for kommunen at anmelde forhol-det, så det havde naturligvis været værre, hvis de ikke havde gjort det. Det er ikke alle lande, der har valgt at fastsætte nationale regler om bødestraffe til

offentlige myndigheder for overtrædelser af forordningen, men det har Danmark valgt. Datatilsynet havde i starten i vurderingen af bødeindstillingen taget udgangspunkt i kommunens regnskabsår forud for gerningstidspunktet, men på baggrund af en senere afgørelse fra Det Europæiske Databeskyttel-sesråd, tolker Datatilsynet nu retstilstanden således, at der skal tages ud-gangspunkt i regnskabsåret forud for den endelige dom.

Der har været fremlagt Datatilsynets politianmeldelse af 30. juni 2020 med bilag (forhold 1, bilag 4), Datatilsynets udtalelse til brug for straffesagen mod Tiltalte Kommune af 28. februar 2022 (bilag A) samt uddrag af de sagen omhandlende indstillingsskemaer.

Rettens begrundelse og afgørelse

Tiltalte har uden forbehold erkendt sig skyldig. Tilståelsen støttes af de oplysninger, der i øvrigt foreligger. Det er derfor bevist, at tiltalte er skyldig.

Straffen fastsættes til en bøde på 50.000 kr., jf. databeskyttelses-forordnin-gens artikel 32, stk. 1, 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

Retten har ved straffens udmåling lagt særlig vægt på omfanget og karakte-ren af de personfølsomme oplysninger i indstillingsskemaerne samt på antal-let af personer, der har haft uberettiget adgang til oplysningerne over en læn-gere periode.

Det findes ikke at kunne føre til et andet resultat, at det ikke har kunnet konstateres, at oplysningerne reelt er blevet tilgået af uvedkommende, idet dette skyldes, at kommunen ikke loggede adgangen til medarbejderportalen, mens den blev anvendt til sagsbehandling.

Retten finder ikke, at der foreligger sådanne særlige omstændigheder i sagen, at der er grundlag for undtagelsesvis at tilkende vederlag efter retsplejelovens § 1007, stk. 2, 1. pkt.

Thi kendes for ret:

Tiltalte Kommune skal betale en bøde på 50.000 kr.

Tiltalte Kommune skal betale sagens omkostninger.

Dommer