Udskrift af dombogen

Adv. DS 0100-84266-00038-21

D O M

afsagt den 1. oktober 2024 i sag

SS 4-7513/2023
Anklagemyndigheden
mod
Tiltalte (Forening)
CVR nr.

Sagens baggrund og parternes påstande

Anklageskriftet er modtaget den 15. marts 2023.

Tiltalte (Forening) 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 august 2018 til juli 2020 ikke at have overholdt sin forpligtelse som dataansvarlig til at gennemføre passende tekniske og organisatoris-ke foranstaltninger, der passede til risiciene af varierende sandsynlighed og alvor for de registreredes rettigheder, idet Tiltalte (Forening) ikke havde sikret sig imod, at uvedkommende - i forbindelse med tyveri af computere fra Tiltalte (Forening)s kontorer og ved phishingangreb - kunne få uautorise-ret adgang til personoplysninger, herunder enkelte følsomme oplysninger i form af blandt andet helbredsoplysninger samt fortrolige oplysninger i form af personnumre, der blev opbevaret i medarbejdernes Outlook eller lokalt på medarbejdernes computere, idet Tiltalte (Forening) blandt andet ikke havde sørget for at kryptere computerne eller indføre foranstaltninger om multifaktorgodkendelse ved login, hvilket medførte et utilstrækkeligt sikker-hedsniveau og brud på persondatasikkerheden samt unødig høj risiko for de registrerede, idet der på computerne lå personoplysninger om mindst 1347 registrerede.

Anklagemyndigheden har nedlagt påstand om en bødestraf på 800.000 kr.

Tiltalte har påstået frifindelse, subsidært at der udmåles en mindre bøde end påstået af anklagemyndigheden.

Sagen er blevet hovedforhandlet over to dage den 19. juni 2024 og den 3.

september 2024.

Forklaringer

Der er afgivet forklaring af Partsrepræsentant som partsrepræsentant for Tiltalte (Forening) og vidneforklaringer fra Vidne 1 og Vidne 2 begge fra Datatilsynet.

Partsrepræsentant har under hovedforhandlingen de 19. juni 2023 afgivet følgende forklaring, der er gengivet i retsbogen af den 1. juli 2024:

"...
Partsrepræsentant forklarede som partsrepræsentant, at han blev ansat i Tiltalte (Forening) den 1. juni 2018 som administrerende direktør. Tidligere har han blandt andet arbejdet i 8 år som departementschef i Ministerie. Han er uddannet cand.scient.pol., og han har ikke en faglig baggrund inden for IT, men har med tiden fået mere forstand på det.

Tiltalte (Forening) er en forening, som primært består af 35.000 frivillige og 400.000 medlemmer. Det er en meget decentral, NGO-lignende organisa-tion, hvor der selvfølgelig også er ansatte, men tyngden i organisationen er alle de frivillige, som laver aktiviteter rundt omkring i Danmark.

Forevist bilag 2-1-1 forklarede Partsrepræsentant, at diagrammet illustrerer både den fri-villige del af organisationen og den lønnede administration. Administrationen varetages delt fra dels hovedkvarteret, som ligger på Vej i København, men også de lokalafdelinger, der findes rundt omkring, hvor de ansatte har ansvaret – også for den frivillige del af organisationen som en slags servicehovedkvarter. Man har både en rolle i forhold til selve den ansat-te del af organisationen, men også som service, blandt andet på IT-området, i forhold til de frivillige. Han er direktør for organisationen, og der er ca. 600 ansatte. Tiltalte (Forening) lever af de indtægter, som de selv skaffer, og kun ca. 3 % kommer fra offentlige midler.

De frivillige har ikke adgang til Tiltalte (Forening)s IT-netværk. Det er meget forskelligt, hvem der er ansat i Tiltalte (Forening). Det er alt fra psykologer, der rådgiver, til telefonister, som ringer og forsøger at overbevi-se nogen om, at de skal være medlemmer, til PR-folk, som håndterer pressen, til jurister og økonomer. Der er kun få ligheder med en almindelig virksom-hed. Hos Tiltalte (Forening) er der meget mere fokus på den del, som pe-ger udad, den servicerende del af den frivillige organisation. En meget stor del af det, som foregår på hovedkvarteret på Vej i Køben-havn, er at servicere den meget store frivillige del.

I den periode fra 2018 til 2020, som er opfattet af denne sag, havde man en IT-afdeling, men den var ikke særligt udbygget. Da Partsrepræsentant blev ansat i 2018, var IT-området et af de områder, som foreningen godt vidste, at de var nødt

til at gøre noget ved, fordi det ikke havde været prioriteret, og fordi der ikke havde været tilstrækkelig økonomi til at forholde sig til området. Det var et sikkerhedsspørgsmål, men det gjaldt lige så meget almindelige driftsmæssige ting. De er en forening, som også lever af, at gode folk hjælper dem med at gøre noget for en billig penge, fordi de gerne vil støtte dem. På IT-området var mange af foreningens programmer udviklet af folk, som gerne ville gøre dem en god tjeneste, og i takt med, at de folk ikke længere var der, begyndte der at tegne sig et billede af et IT-system, som ikke hang tilstrækkeligt meget sammen. Der var behov for, at man så på det på en helt anden måde. Han kan ikke sige præcis, hvor mange ansatte, der beskæftigede sig med IT, men der er i dag formodentlig tre gange flere it-medarbejdere ansat end i ger-ningsperioden. Der er i dag omkring 35 ansatte i IT-afdelingen i dag, og det er derfor ikke usandsynligt, at der i gerningsperioden var ca. 10 ansatte.

Partsrepræsentant kan kun spekulere over, om der blev gjort nogle særlige tiltag hos Tiltalte (Forening) op til databeskyttelsesforordningens indførelse den 25. maj 2018, fordi det var før hans tid i foreningen. Da Partsrepræsentant efter sin ansættel-se spurgte ind it-arbejdet, var det ikke noget, som man havde gjort meget ud af. Man vidste i organisationen, at der var noget på vej på it-området, og at det lød svært. Ham bekendt, blev der ikke i forbindelse med indførelsen af GDPR lavet særlige datebeskyttelsesinitiativer inden de nye regler trådte i kraft.

Partsrepræsentant har været indblandet med hensyn til de fire indberetninger om brud på it-sikkerheden Datatilsynet. Mange af besvarelserne til Datatilsynet er under-skrevet og fremsendt af Partsrepræsentant, og foreholdt bilag 1-2-2, side 2, fra august 2018 bekræftede han indholdet af indberetningen. På dette tidspunkt vidste man dårligt nok i Tiltalte (Forening), hvad GDPR betød, og hvordan man skulle adressere problemstillingen. Det, som de primært gjorde noget ved, var at undgå at komme til at betale falske fakturaer. På det tidspunkt var man i Tiltalte (Forening) i tvivl om, hvordan de skulle gribe sikkerhedsproble-matikken an, men hændelsen gav anledning til, at man indførte forskellige til-tag og begyndte at overveje indførelse af multifaktorgodkendelse (MFA).

Foreholdt bilag 1-2-2, side 5, forklarede Partsrepræsentant, at tallene omkring sikker-hedsbruddets omfang byggede på en formodning på det tidspunkt. Det gæl-der for denne indberetning, men også for de senere indberetninger, at hvis de var i tvivl om sikkerhedsbruddets størrelse, så angav de den mest omfattende mulighed.

Foreholdt bilag 1-2-2, side 7, forklarede Partsrepræsentant, at de umiddelbart indførte tiltag, som var relativt lette at indføre ved at ændre tekniske procedurer. De var klar over, at de blev nødt til at have nogle mere generelle sikkerhedsfor-anstaltninger, hvorfor de skitserede overvejelsen af MFA. Det var i forbin-delse med denne indberetning, at organisationen første gang begyndte at overveje MFA.

Adspurgt af forsvareren forklarede Partsrepræsentant, at der blev lavet forsøg med ind-førelsen af MFA hos en række centrale medarbejdere efter sikkerhedsbruddet i 2018. Det var for at få erfaring og overblik over, hvad der kunne lade sig gøre, hvordan de gjorde det rent teknisk, og hvad det kostede. Partsrepræsentant husker at forsøgene viste, at foreningen havde meget gamle computere, hvilket gjor-de, at det ikke kunne lade sig gøre at indføre MFA på mange af computerne. En af erfaringerne var derfor, at det ville kræve, at de skulle skifte en stor del af deres computere ud, hvilket ville koste mange penge. Partsrepræsentant mener derfor ikke, at Tiltalte (Forening) sad på hænderne, og han synes, at de tog it-sikkerheden alvorligt og begyndte at undersøge, hvordan det kunne lade sig gøre, men også med behørig respekt for, om de overhovedet havde en IT-af-deling og en computerbeholdning, som var i stand til det. Der var også nogle overvejelser om, hvad det ville koste at skifte to tredjedele af organisationens computere ud.

Adspurgt på ny af anklageren forklarede Partsrepræsentant, at organisationens compute-re på daværende tidspunkt ikke var krypterede. De var omfattet af almindeli-ge passwords som de fleste computere på det tidspunkt, men både MFA og egentlig kryptering var der ikke tale om. De havde regler internt for, hvordan man skulle opbevare personoplysninger, men den ekstra opmærksomhed, der kom vedrørende databeskyttelse med persondataforordningen, var de ikke gearet til. De havde dog hele tiden haft et grundberedskab i forhold til, at man ikke måtte opbevare personfølsomme oplysninger på computerne.

Foreholdt bilag 1-2-3, vedrørende første tiltalepunkt, forklarede Partsrepræsentant, at han var bekendt med indberetningen af den pågældende hændelse. Indberet-ninger foregår på den måde, at der er et udvalg, som står for den praktiske behandling. Alle eventuelle indberetninger forelægges Partsrepræsentant, og han beslut-ter derpå, hvad der skal gøres. Partsrepræsentant forklarede, at der blev stjålet 6 forskel-lige bærbare computere fra Tiltalte (Forening)s hovedkontor. De perso-noplysninger, der lå på de stjålne computere, omfattede blandt andet infor-mation til historier, som blev bragt i organisationens magasin. I det tilfælde var det nogle artikler om kvinders Udeladthistorier, der var blevet publiceret i Tiltalte (Forening)s Magasin. Det var kvindernes person-lige historier, som de havde valgt at stå frem med og dele. På nuværende tidspunkt har organisationen retningslinjer for, at alle computere skal være låst inde, men det havde de ikke på det tidspunkt.

Foreholdt bilag 1-2-3, side 6, forklarede Partsrepræsentant, at der også lå andre oplys-ninger på computerne. Der lå blandt andet en lønseddel, som en af medarbej-derne havde liggende på sin egen PC, hvilket er imod reglerne. Det var kun i forbindelse med historierne om de Udeladt kvinder, at der var helbredsop-lysninger og fortrolige oplysninger involveret. Computerne var ikke krypteret på det tidspunkt, og de var heller ikke forsynet med MFA. Foreholdt bilag 1-2-3, side 7, forklarede Partsrepræsentant, at tre af computerne var blevet brugt af fra-trådte medarbejdere, to var var blevet brugt af redaktøren af Magasin og én to var var blevet brugt af en kommunikationsmedarbejder, som havde

arbejdet med artiklerne. Den sidste computer, der blev stjålet, var blevet købt til Partsrepræsentant selv, men ikke taget i anvendelse endnu, så der var ikke oplysnin-gert på den.

Artiklerne med case-historier lå på to af computerne. Partsrepræsentant husker ikke præ-cis hvordan artiklerne blev opbevaret på computerne, men oplysningerne var tilgængelige, hvorfor Tiltalte (Forening) indberettede tyveriet til Datatil-synet. For én medarbejders vedkommende lå personens egen lønseddel til-gængelig på den stjålne computer. Det er ikke tilladt, men de oplysninger som i denne sammenhæng kunne være problematiske, var artiklerne, fordi de indeholdt information om kvinder, som fortalte deres historier til Tiltalte (Forening)s margasin.

Foreholdt bilag 2-3-2, forklarede Partsrepræsentant, at det er rigtigt, at der var 34 perso-ner, der var berørt af den første hændelse, herunder 28 case-personer, 3 tidli-gere og 3 nuværende medarbejdere. De personfølsomme oplysninger vedrør-te dog kun de interviews med kvinderne, som på det tidspunkt allerede var blevet offentliggjort i Magasin. Det vil sige, at der ikke blev opbevaret oplysninger på computerne, som ikke allerede var blevet offentliggjort.

Foreholdt bilag 2-3-3, forklarede Partsrepræsentant, at materialet blev brugt til artikler i bladet og almindelig kommunikation via sociale medier. Der var både intervi-ews og billedmateriale. Begge dele var allerede blevet offentliggjort, da com-puterne blev stjålet. Partsrepræsentant ved ikke, hvorfor artiklerne stadig lå på compu-terne efter offentliggørelsen, men det burde ikke have været tilfældet.

Allerede på gerningstidspunktet havde Tiltalte (Forening) regler om, at man ikke måtte opbevare personfølsomme og fortrolige oplysninger tilgæn-geligt på sin computer. Det skulle lagres i analogt arkiv eller på eksternt drev, der var låst inden. Efter tyveriet blev databeskyttelsen drøftet i et sik-kerhedsudvalgsmøde, og der blev truffet beslutning om, at alle oplysningerne på computerne skulle krypteres. Det blev konstateret, at de skulle investere i en helt ny IT-pakke, som blandt andet indebar udskiftning at mange compu-tere.

Adspurgt af forsvareren, forklarede Partsrepræsentant, at redaktøren, der havde case-hi-storierne liggende på sin computer, typisk først får historierne, når de er fær-dige, og der lå ikke yderligere personoplysninger på computerne. Efter ind-beretningen bad Datatilsynet ikke om yderligere information, så Tiltalte (Forening) meddelte ikke Datatilsynet, at der alene var tale om allerede of-fentliggjorte artikler. Tiltalte (Forening) drøftede ikke sagens fakta med Datatilsynet efter de foretog anmeldelsen. Der har ikke efterfølgende været indikationer på, at oplysningerne på de stjålne computerne er blevet mis-brugt.

Adspurgt af på ny af anklageren forklarede Partsrepræsentant, at Tiltalte (Forening) indberettede hændelsen, og at de ikke hørte mere fra Datatilsynet, før de

modtog et udkast til en pressemeddelelse fra Datatilsynet om overgivelse af sagen til politiet med påstand om en bøde på 800.000 kr.

Foreholdt bilag 1-2-4, vedrørende andet tiltalepunkt, forklarede Partsrepræsentant, at han var med til at udarbejde indberetningen, og at det drejede sig om tyveri af fem computere fra kontoret i Århus.

Foreholdt bilag 1-2-4, side 4, forklarede Partsrepræsentant, at almindelige oplysninger typisk gælder aftaler og tider, der bliver skrevet ned på computeren, hvor in-gen personoplysninger indgår. Aftalerne kan også anonymiseres, og man kan komme i rådgivningen uden at opgive navn, så der vil under ingen omstæn-digheder være personnummer involveret. Det vil normalt alene være navn og måske et telefonnummer, der registreres. Det var navnlig tyveriet af en com-puter, der blev benyttet af en af foreningens psykologer i rådgivningen af Patienter, som organisationen var mest bekymret for. Psykologen havde samtaler med Patienter, som fortalte alvorlige historier til rådgivningen, og som måske var blevet dokumenteret på computeren i en eller anden ud-strækning. Foreningen var nervøs for, at psykologen muligvis havde den in-formation liggende på computeren, men det viste sig efterfølgende, at psyko-logen dokumenterede samtalerne analogt på et stykke papir, som hun opbe-varede i et pengeskab. Det vidste Tiltalte (Forening) dog ikke, da de ind-berettede hændelsen. De skulle indberette hændelsen hurtigt, og de indberet-tede derfor det værst tænkelige, fordi der var risiko for, at personfølsomme oplysninger lå på computeren.

Tiltalte (Forening) opbevarer ikke CPR-numre eller journaloplysninger på computerne. Tiltalte (Forening) virker ikke som et sygehus, og de har derfor ikke personoplysninger om folk. Personer kan komme i rådgivningen uden at opgive sit navn. De har ingen journaliseringspligt, og i denne situati-on var der derfor ikke oplysninger af den karakter, som kunne kobles direkte til en persons sygdom. Det kunne der have været hos den pågældende psyko-log, men det viste sig ikke at være tilfældet. Partsrepræsentant konstaterede dette efter-følgende ved at spørge ind til, hvordan psykologen dokumenterede sine sam-taler.

Partsrepræsentant mener derfor ikke, at der var helbredoplysninger på nogen af de fem computere, der blev stjålet. Der var almindelige oplysninger om aftaler, nav-ne og telefonnumre. Partsrepræsentant husker ikke, hvorfor foreningen angav i skemaet i bilag 1-2-4, at der lå CPR-numre på de fem stjålne computere.

Foreholdt bilag 1-2-4-1, forklarede Partsrepræsentant, at han var med til at udarbejde indberetningen, og han kan bekræfte informationen i denne. Tiltalte (Forening) iværksatte 3 konkrete tiltag efter de to indbrud. Rent fysisk blev det gjort væsentligt sværere at komme ind i foreningens bygninger. Herudo-ver blev der lagt vægt på det adfærdsmæssige ved at sikre, at alle låste deres computere inde, og der blev iværksat løbende kampagner med fokus på it-sikkerhed. De havde retningslinjer omkring, at det var i strid med reglerne at

opbevare følsomme oplysninger i Outlook efter endt sagsbehandling. I forbindelse med de to tyverier modtog man fra fagfolk rådgivning om at tage fat på kryptering.

Efter indberetningen fandt foreningen ud af, at på omkring halvdelen af foreningens computere kunne oplysningerne krypteres, hvilket man gik i gang med. Derudover traf man beslutning om at indføre multifaktorgodkendelse. Grunden til, at foreningen ikke sørgede for kryptering af alle oplysninger ef-ter det første tyveri var, at der ikke var kapacitet til det i IT-afdelingen. Som direktør havde Partsrepræsentant også overvejelser om, hvor mange penge, der var til rådighed, og derfor måtte han have udgifterne godkendt i forretningsudvalget. Han tror, at processen tager længere tid for en organisation som Tiltalte (Forening), end den gør for private virksomheder og offentlige organisatio-ner.

Adspurgt af forsvareren, forklarede Partsrepræsentant, at de andre involverede medar-bejdere, udover psykologen, typisk behandlede almindelige oplysninger for eksempel i forbindelse med receptionistopgaver.

Af anklageren foreholdt bilag 1-2-5, vedrørende tredje tiltalepunkt, forklare-de Partsrepræsentant, at årsagen til hændelsen var et phishing-angreb, som omfattede al-mindelige personoplysninger og fem CPR-numre. Tiltalte (Forening) kunne rekonstruere, hvad der lå på den computer, som var blevet hacket. Fo-reningen forsøgte at finde ud af, om nogle af de hackende oplysninger efter-følgende var blevet misbrugt, men det viste sig ikke at være tilfældet.

Tiltalte (Forening) hyrede professionel assistance til at finde ud af, hvor phishing-angrebet kom fra, hvilken type angreb, der var tale om, og om hvordan man kunne undgå lignende angreb i fremtiden.

Tiltalte (Forening) besluttede i januar 2020, på baggrund af IT-chefens anbefaling, at MFA skulle indføres på alle computere. Der blev bevilget pen-ge til det, og det var planen, at installationen af MFA skulle begynde i marts 2020.

Foreholdt bilag 1-2-5-1, forklarede Partsrepræsentant, at tilhørsforhold til fagforeninger ikke var omfattet af hændelsen, og at Tiltalte (Forening) skønnede, at der var ca. 16 berørte af sikkerhedsbruddet.

Adspurgt af forsvareren forklarede Partsrepræsentant, at beslutningen om, at MFA skulle indføres i marts 2020, blev taget den 14. og 15. januar 2020, og at phishing-angrebet skete et par uger derefter. På det tidspunkt var det altså besluttet, og der var bevilliget penge til, at MFA skulle indføres. Det ærgrede derfor Partsrepræsentant, at angrebet ikke skete et par måneder senere, for så ville angrebet kunne have været forhindret. Foreningen kunne heller ikke i dette tilfælde konstatere, at nogle af de kompromitterede oplysninger er blevet misbrugt.

Den 11. marts 2020 blev Danmark på grund af coranapandemien lukket ned, og Tiltalte (Forening) fulgte anbefalingerne om, at medarbejderne i videst muligt omfang skulle arbejde hjemme. Foreningen måtte derfor i perioden fra marts til juni sætte udviklingen af MFA på pause, fordi IT-folkene blev tvun-get til at sikre, at foreningens medarbejde kunne arbejde hjemmefra med der-es computere.

Adspurgt på ny af anklageren forklarede Partsrepræsentant, at der også var sikkerheds-mæssige problemstillinger forbundet med at rykke arbejdspladsen hjem, og det var også IT-medarbejdernes opgave at sørge for, at IT-sikkerheden var til stede.

Foreholdt bilag 1-2-6, vedrørende fjerde tiltalepunkt, forklarede Partsrepræsentant, at han var med til at udarbejde indberetningen til Datatilsynet. Det var én me-darbejder, hvis computer, der blev hacket fra Nigeria, og der var risiko for, at hele den medarbejders Outlook-konto var blevet kopieret. På dette tidspunkt var Tiltalte (Forening) gået i gang med at indføre MFA på foreningens computere, men de var ikke nået til den computer, der blev hacket. De blev først færdige med at indføre af MFA i begyndelsen af juni.

Foreholdt bilag 1-2-6, side 6, forklarede Partsrepræsentant, at antallet af berørte var 1.100 personer. Den ene person, der blev hacket, var ansat i Tiltalte (Forening) og havde dermed e-mailadresser på alle medarbejdere i foreningen. Det var derfor potentielt alle ansattes computere, som man kunne få adgang til på grund af sikkerhedsbruddet.

De helbredsoplysningerne, der blev kompromitteret, handlede om tre medar-bejdere, der havde været på barsel og havde født. Sikkerhedsbruddet omfat-tede fire CPR-numre på nuværende medarbejdere, ét CPR-nummer på en tid-ligere medarbejder, og CPR-numrene på de tre børn, der var blevet født af de medarbejdere, der var på barsel. Det beroede på en fejl, at de pågældende oplysninger var i den pågældende computer. Der lå ikke andre personfølsom-me oplysninger i den hackede Outlook konto.

Tiltalte (Forening) opdagede dette phishing-angreb, fordi de på dette tidspunkt havde installeret overvågning.

Foreholdt bilag 1-2-6-3, side 3, forklarede Partsrepræsentant, at han var involveret i be-svarelsen. Det var relativt enkelt at kortlægge, hvad der lå på den computer, der blev hacket. De brugte den professionelle eksterne assistance til at vurde-re, hvad risikoen var for, at informationen faktisk var blevet misbrugt til no-get. De fik angrebet lukket ned inden for en time. Det var i strid med forenin-gens regler, at den berørte medarbejder havde personoplysningerne liggende tilgængelige, hvorfor den pågældende medarbejder havde begået en fejl.

Adspurgt af forsvareren omkring bilag 1-2-6, side 5, forklarede Partsrepræsentant, at overvågningssystemet, der opdagede angrebet, er et eksempel på nogle af de

sikkerhedssystemer, som foreningen havde indført på dette tidspunkt. De vil-le ikke have fået advarslerne, hvis angrebet var foregået på et tidligere tids-punkt. Det var også en del den nye af sikkerhedsprocedure, at de gik fra at have dækning inden for almindelig arbejdstid til også at have dækning uden for arbejdstiden. Når det er anført i indberetningen, at ledelsesstruktur blev kompromitteret, handlede det om den ene medarbejders oversigt over tidlige-re medarbejdere, som vedkommende selv havde genereret på sin computer. Tiltalte (Forening) har heller ikke efterfølgende haft nogle indikationer af, at oplysningerne er blevet brugt.

Adspurgt på ny af anklageren forklarede Partsrepræsentant, at det ikke er teknisk van-skeligt at kryptere oplysningerne på computerne, men foreningens problem var, at en del af computerne ikke var klar til det. Det gjorde, at det blev dyrt og besværligt, og det var en udfordring, der gjorde, at de ikke kunne indføre krypteringen fra den ene dag til den anden. Det samme gælder for indførelsen af MFA. I sig selv er det nemt, hvis man havde moderne computere, men det havde foreningen som bekendt ikke ikke på det tidspunkt.

Adspurgt af anklageren forklarede Partsrepræsentant, at bødepåstanden på 800.000 kr. udgør mange penge for en forening som Tiltalte (Forening). Alle de pen-ge, som foreningen indsamler, går direkte til støtte af Patienter, og 800.000 kr. er penge som man i givet fald skal tage fra arbejdet med Udeladt-sagen. I forbindelse med udmålingen af en bøde, kan Partsrepræsentant ikke forstå, hvor-for Tiltalte (Forening) ikke opfattes mere på linje med en offentlig myn-dighed i strafudmålingen, fordi de i høj grad fungerer som en offentlig myn-dighed. Foreningen er ikke en virksomhed, som skal producere et overskud, en bundlinje eller betale udbytte til aktionærer.

Foreholdt Tiltalte (Forening)s årsregnskab for 2020, bilag 5-2, side 27, forklarede Partsrepræsentant, at foreningens indtægter varierer meget fra år til år. Det af-hænger blandt andet af konjunkturerne i samfundet, og hvis der for eksempel er corona og forsamlingsrestriktioner, har det stor betydning for, hvor mange penge, de kan indsamle. I tallet på 76 millioner kr., er der ca. 7 millioner kr., som stammer fra donationer i form af indsamlinger i forbindelse med for ek-sempel begravelser, som så er blevet doneret til Tiltalte (Forening) efter-følgende, og efter hans opfattelse skal dette beløb fratrækkes de 76 millioner kr. Genbrugsbutikkernes indtægt var på 26 millioner kroner. Posten ”arrangementer kampagner og øvrige aktiviteter” dækker for eksempel over kampagnen ”Kampagne” og andre tilsvarende initiativer.

Status på it-sikkerheden i Tiltalte (Forening) i dag er, at der er indført kryptering og MFA på alle de computere, der benyttes i foreningen, og der er døgnovervågning af hele systemet og eksterne aftaler med nogle, der for ek-sempel laver aftalte phishing-angreb på foreningen, så man kan lære at for-svare sig mod dem.

Adspurgt af forsvareren forklarede Partsrepræsentant, at tidligere også har arbejdet

blandt andet direktør i Styrelse, og han havde inden han blev di-rektør i Tiltalte (Forening) mange erfaringer fra den offentlige sektor. Da han trådte til, var det derfor med et udgangspunkt i den offentlige sektor, at han vurderede, at Tiltalte (Forening) havde et stort stykke arbejde at gø-re blandt andet med it-sikkerheden.

I dag er Partsrepræsentant sikker på, at Tiltalte (Forening) har godt styr på it-sikker-heden, og der er mange andre NGO-organisationer, der spørger om, hvad de har gjort på området. Partsrepræsentant mener ikke, at foreningen er helt på niveau med den offentlige sektor, men det er tæt på. Datatilsynet har undersøgt forenin-gens forskningsafdeling, som indeholder meget data, og foreningen fik at vi-de, at alt var som det skulle være. Der har været en tilsvarende undersøgelse på HR-området, hvor alt også virkede som det skulle.

I forbindelse med de to phishing-angreb omfattet af denne sag modtog fore-ningen brev fra Datatilsynet om, at tilsynet ikke ville gøre mere ved indberet-ningerne, og i forbindelse med de to tyverier, hørte Tiltalte (Forening) ik-ke mere fra Datatilsynet, før de fik at vide, at foreningen ville blive politian-meldt.

Foreholdt udkastet til pressemeddelelsen i bilag 6, forklarede Partsrepræsentant, at fore-ningen fik orienteringen om pressemeddelelsen på mail, dagen før, at den skulle offentliggøres. Partsrepræsentant var chokeret, da han så den, og han troede, at når de ikke havde hørt noget i anledning af indberetningerne, var det Datatil-synets vurdering, at alt var i orden. Da han så beløbet på 800.000 kr., troede han, at punktummet var sat forkert, og han kunne ikke forestille sig, at bøden for det, som han vidste, at de havde gjort forkert, kunne være så stor. Da man fik udkastet, gjorde man straks Datatilsynet opmærksom på, at forenin-gen intet havde noget at gøre med patientjournaler, og denne fejl blev rettet i den endelige pressemeddelelse. Det var Tiltalte (Forening)s opfattelse, at Datatilsynet havde misforstået, hvilken type oplysninger, som foreningen lå inde med, og det lykkedes ikke på noget tidspunkt at komme i dialog med Datatilsynet, om hvilke oplysninger, det rent faktisk drejede sig om.
..."

Partsrepræsentant har til retsbogen af 3. september 2024 afgivet følgende supple-rede forklaring:

"...
Adspurgt af forsvareren forklarede Partsrepræsentant, at der ikke i Tiltalte (Forening) på noget tidspunkt er behandlet patientjournaler, herunder sket re-gistrering af patientoplysninger. I Udeladtrådgivningen føres samtaler med Patienter og pårørende, og nogle gange er der tale om anonym rådgiv-ning. Oplysninger fra sådanne samtaler opbevares eller behandles ikke elek-tronisk, men notater fra samtalerne bliver nogle gange skrevet ned på papir, som opbevares i et pengeskab. Det var f.eks. tilfældet med den psykolog hos Tiltalte (Forening) i Aarhus, der fik stjålet sin computer i december

2019.

Foreholdt retsbogen af 1. juli 2024 side 3, 1. nye afsnit, vedrørende bilag 1-2-2, side 5, forklarede vidnet, at da Tiltalte (Forening) lavede denne ind-beretning, var man i tvivl om, hvorvidt der på computerne havde været per-sonfølsomme oplysninger, men det viste sig efterfølgende, at det ikke var til-fældet.

Der var ingen dialog med Datatilsynet i forbindelse med indberetningerne, og da man fik oplysningerne om, at Datatilsynet ikke ville gå videre med de to indberetninger vedrørende phishingangrebene i januar og maj 2020, gik man ud fra, at Tiltalte (Forening) ikke ville høre mere i anledning af disse to indberetninger. Da man den 28. september 2021 modtog udkastet til Datatil-synets pressemeddelelse, var man meget forundret over, at Datatilsynet lagde til grund, at der var tale om patientjournaler. Datatilsynet blev straks kontak-tet, og den fejlagtige oplysning om elektronisk opbevaring af patientjournaler udgik i den pressemeddelelse, der blev udsendt til offentligheden i forbindelse med politianmeldelsen den 29. september 2020.

Foreholdt retsbogen af 1. juli 2024, side 4, første afsnit, forklarede Partsrepræsentant, at det alene var seks og ikke 7 computere, der blev stjålet fra Tiltalte (Forening)s kontor i København den 2. oktober 2019 .

Foreholdt retsbogen af 1. juli 2024, side 7, afsnit 7, forklarede Partsrepræsentant, at det alene var de ansattes mailadresser og ikke deres computere, man kunne få adgang til på grund af sikkerhedsbruddet. Der var tale om kontaktoplysnin-ger i den pågældende medarbejders Outlook konto.

Adspurgt af anklageren forklarede Partsrepræsentant, at han ikke kan huske, om de stjål-ne computere alle var bærbare computere. Det er rigtigt, at Tiltalte (Forening) konsekvent har brugt ordet "bærbare computere" i deres indberet-ning til Datatilsynet.
..."

Vidnet IT-Sikkerhedskonsulent Vidne 1 har til retsbogen afgivet følgende forklaring:

"...
Vidne 1 forklarede, at han blev ansat i Datatilsynet for ca. to år siden som IT-sikkerhedskonsulent. Han er uddannet datalog og datama-tiker, og hans hovedopgave er håndtering af brud, herunder vurderingen af alvorligheden af brud og høringer i forbindelse med brud og indberetninger. Han er også med på tilsynsbesøg, hvor han håndterer det IT-tekniske. Sags-behandlingen i sagen vedrørende Tiltalte (Forening) foregik før, at vidnet startede i Datatilsynet, og vidnet har ikke været involveret behandlingen, men han har læst op på sagen.

Der er mange definitioner, der bliver brugt i forbindelse med sikkerhedsbrud og sikkerhedshændelser, og når Datatilsynet håndterer sådanne ”brud på persondatasikkerheden” , refererer de til GDPR forordningens artikel 4 stk. 12, hvor definitionen af et brud på persondatasikkerheden fremgår.

GDPR forordningens artikel 32 angår behandlingssikkerhed og bestemmer, at der skal sikres passende sikkerhed i forbindelse med behandling af personoplysninger. Et af Datatilsynets primære kanaler til at sikre, at der ikke sker brud på datasikkerheden, er blandt andet indberetningerne, og i 2023 modtog tilsynet lige over 9000 indberetninger fra private virksomheder og offentlige myndigheder, og vidnet er blandt de ansatte hos Datatilsynet, der visiterer indberetningerne. Typisk klassificerer Datatilsynet indberetningerne med farvekategorier, der spænder fra ”hvid” , når det konstateres, at et muligt brud falder uden for definitionen i artikel 4, stk. 12. I de tilfælde ringer Datatilsy-net typisk til indberetteren og fortæller dem, hvorfor det er uden for definiti-onen, og at de vil modtage et afsluttende brev. Farvekategorien ”grøn” dæk-ker over brud på persondatasikkerheden, som Datatilsynet ikke vil forfølge ud fra ressourcehensyn, og farvekategorien ”gul” dækker over brud på persondatasikkerheden, hvor Datatilsynet nøjes med at bestemme, at den dataansvarlige skal underrette de berørte registrerede. Farvekategorien ”rød” benyttes over for de indberetninger, som Datatilsynet mener er så alvorlige, at de skal forfølges yderligere. Indberetningerne farvemarkeres i den indledende visitering og ”røde” indberetninger bliver taget op ugentligt, hvor det blandt andet vurderes, om der er tale om så alvorlige brud, at der skal ske høring og om indberetningen giver anledning til politianmeldelse.

Afgørende efter forordningens artikel 32 er, at der skal findes et passende sikkerhedsniveau baseret på risiko og omkostningsniveau, hvilket er den dataansvarliges ansvar. ”Tekniske foranstaltninger” dækker over alt det udstyr, som skal købes og installeres, imens ”organisatoriske foranstaltninger” typisk findes i form af retningslinjer til medarbejdere. Databeskyttelsesforordningen indeholder ikke krav om, hvilke konkrete tekniske foranstaltninger, der skal indføres.

Kryptering og MFA er to meget brugbare tekniske sikkerhedsforanstaltnin-ger. Det har været muligt at foretage kryptering i mange år, og der er tale om en helt basal sikkerhedsforanstaltning. Langt de fleste organisationer bruger i dag computere med Windows styresystemer, og kryptering har været kendt i disse systemer i rigtig mange år. Den første bitlocker-kryptering til Windows kom i 2007 og er blevet udviklet siden. I 2014 kom en ny teknologi med en TPM-chip, der kan håndtere alle nøglerne, der styrer krypteringen, hvilket gjorde det meget nemmere at kryptere oplysningerne.

Ved tyveri af bærbare computere er kryptering særlig relevant, fordi tyven kun kan få adgang til lagrede data ved brug af den rette nøgle, der typisk ak-tiveres ved hjælp af et password, der skal bruges for at kunne logge ind på computeren. Hvis computeren ikke er krypteret, kan kriminelle se compute-

rens data, selv hvis de ikke har et login til computeren, og kryptering er der-for en vigtig og afgørende sikkerhedsforanstaltning.

Phishing er et forsøg på at lokke nogen til at gøre noget, og navnet kommer af, at man spreder links eller skadelige koder med håbet om, at nogle klikker på linket. Et hackerangreb er som regel målrettet, og man ved, hvad og hvem, man går efter. Phishing-angreb er meget almindelige, og man kan for-svare sig mod dem ved at indføre interne phishing-simulationer for at lære medarbejdere, hvad de skal være opmærksomme på. Mange phishing-angreb ligner hinanden. De er skrevet på dårligt sprog og kan som regel gennemsku-es, men problemet er dog, at kriminelle bliver bedre til at lave angrebene for eksempel ved brug af kunstig intelligens til at få grafikken til at se rigtig ud.

Ved multifaktorgodkendelse (MFA) har man ud over et brugernavn og et password en faktor mere enten i form en chip eller en kodegenerator, som kan lave en midlertidig talkode, der ikke kan genbruges. MFA er en basal sikkerhedsforanstaltning, og det er efter vidnets opfattelse ikke bekosteligt at indføre MFA. Ved brug af MFA sænkes sandsynligheden for at uvedkom-mende får adgang til et system.

Vedrørende de to konkrete tilfælde, hvor Tiltalte (Forening) fik stjålet bærbare computere, at det var et stort sikkerhedsproblem, at personoplysnin-gerne på computerne ikke var krypteret. Det ville være forventeligt, at de bærbare computere var krypteret, når nu der var mulighed for, at de kunne forlade huset. Det er Datatilsynets holdning, at hvis der er tale om person henførbare data, så skal oplysningerne krypteres. Med hensyn til phishing-an-grebene, hvor koder er blevet lokket ud af folk, så havde MFA antageligvis stoppet loginforsøgene. Kryptering og MFA havde efter vidnets opfattelse været passende sikkerhedsforanstaltninger i den konkrete sag.

Vidnet er teknikker og ikke jurist, og det er ikke vidntes beslutning, om der skal laves en politianmeldelse i forbindelse med en indberetning til Datatilsy-net. Vidnet tages med på råd, og han kan komme med sin vurdering, hvis han synes, at noget er graverende, og at sikkerheden ikke passer til den risiko, som virksomheden har.
..."

Vidnet chefkonsulent Vidne 2 har til retsbogen afgivet følgende forklaring:

"...
Vidnet forklarede, at hun er jurist og ansat i Datatilsynet, hvor hun har været ansat i to år som souschef og chefkonsulent. Hun arbejder i den enhed, som arbejder med brud på persondatasikkerheden og brudsager. Når der sker brud på personsikkerheden, skal alle, herunder private virksomheder, fore-ninger og offentlige myndigheder anmelde det til Datatilsynet, som fortiden modtager ca. 9.000 anmeldelser årligt.

Datatilsynets politianmeldelse fra den 29. september 2021 af Tiltalte (Forening) blev indgivet før, at vidnet blev ansat, men vidnet har efter sin an-sættelse været inde over sagen og blandt andet gennemgået bilagene. Det er også vidnet, der har udarbejdet Datatilsynets supplerende udtalelse af 7. juni 2024 om politianmeldelsen (bilag 5) og bemærkningerne om beregningen af bøden af 7. august 2014 (bilag 8).

Artikel 32 i databeskyttelsesforordningen er en bindende regel, som handler om behandlingssikkerheden, og hvordan man beskytter personoplysninger. Det fremgår ikke udtømmende af bestemmelsen hvilke bestemte sikkerheds-foranstaltninger, der skal træffes i den enkelte organisation, da graden af de påkrævede foranstaltninger blandt andet beror hvilke typer personoplysnin-ger, som behandles, og hvordan de behandles. Beskyttelsesniveauet kan være forskelligt alt afhængigt af, hvad risikoen er, og det kan derfor ikke siges præcist, hvilke sikkerhedsforanstaltninger, der skal iværksættes i den enkelte situation. Der der gælder dog nogle standardmæssige foranstaltninger for ek-sempel kryptering og multifaktorgodkendelse ved login.

Principperne i artikel 32 var også gældende inden forordningen trådte i kraft. Dette fremgik blandt andet af databeskyttelsesdirektivet, der blev gennemført ved persondataloven fra 2000, som var gældende indtil databeskyttelses- for-ordningen trådte i kraft i Danmark i 2018 .

Vidnet forklarede videre, at den omstændighed, at der er sket et brud, ikke er det samme, som at sige, at der ikke er indført de rette sikkerhedsforanstalt-ninger, men virksomhederne og organisationerne skal så at sige beskytte sig mod, at det går galt og inden, at det går galt.

Det der førte til Datatilsynets politianmeldelse af Tiltalte (Forening) den 29. september 2021 omhandler det generelle dårlige sikkerhedsniveau hos Tiltalte (Forening) og ikke kun de fire konkrete brud på datasikkerheden som Tiltalte (Forening) indberettede i oktober og december 2019 og ja-nuar og maj 2020. Blandt andet grund af den manglende kryptering og multi-faktorgodkendelse ved login, kunne det have gået galt i mange andre tilfæl-de.

Mange af de indberetninger om brud på datasikkerheden, som Datatilsynet modtager hvert år, fører ikke til politianmeldelser. I sådanne tilfælde vejleder Datatilsynet i stedet virksomheden, og der bliver blandt andet lagt vægt på, om virksomheden iværksætter foranstaltninger, der sikre at brud undgås i fremtiden.

Artikel 32 henviser til, at der skal foretages passende og organisoriske foran-staltninger. Det kan for eksempel være undervisning af medarbejder og/eller tekniske foranstaltninger som kryptering og multifaktorgodkendelse. Krypte-ring og multifaktorgodkendelse har været tekniske foranstaltninger, der har

været kendt i en årrække inden de 4 brud på datasikkerheden, som Tiltalte (Forening) indberettede i 2019 og 2020. Der er tale om sikkerhedsforanstaltninger, som ikke er svære at installere.

Det følger af GDPR reglerne, herunder artikel 32. pkt. 1, litra d, at den dataansvarlige er forpligtet til løbende at vurdere, om de sikkerhedsforanstaltninger, der er iværksat forsat lever op til standarderne og skal herunder vurdere om beskyttelsesniveauet skal forberedes i takt med, at organisationen udvik-ler sig eller, at trusselbillede ændre sig. Hvis man behandler personoplysnin-ger, hvilket forstås bredt, var det efter vidnets opfattelse også før 2018 en helt gængs sikkerhedsforanstaltning at foretage kryptering af alle former for personoplysninger. Der kan således også være behov for at bruge kryptering ved behandling af almindelige oplysninger så som emailadresser og navne. Det er kendt, at emailadresser kan bruges af kriminelle til at begå kriminali-tet. Personhenførebare oplysninger bør derfor altid krypteres. I forbindelse med datasikkerheden er det ikke et krav, at oplysninger rent faktisk er blevet misbrugt. At der er risiko for misbrug kan også indebærer et brud på GDPR reglerne. Det er et krav, at datasikkerheden er på plads inden, at man begyn-der at behandle personhenførbare oplysninger elektronisk.

Adspurgt om Datatilsynet overfor Tiltalte (Forening) fulgte op på de 4 konkrete indberetninger, forklarede vidnet, at Datatilsynet ikke bad om yder-ligere oplysninger om bruddene end dem, som som fremgik af indberetnin-gerne. De yderlige oplysninger Datatilsynet modtog fra Tiltalte (Forening), tog man højde for inden, at Datatilsynet traf afgørelsen om politianmel-delsen. Datatilsynets politianmeldelse og denne straffesag omhandler ikke kun de konkrete brud og de følsomme oplysninger, som Tiltalte (Forening) nævnte i indberetningerne som ved tyverierne af computerne og phis-hingangrebene potentielt kunne var blevet misbrugt, men sagen omhandler også alle de andre oplysninger i Tiltalte (Forening)s systemer, hvor det kunne have været risiko misbrug.

Foreholdt at Partsrepræsentant har forklaret, at der ikke var personfølsomme oplysninger i forbindelse med de computere, der blev stjålet ved tyverierne i oktober og december 2019, forklarede vidnet, at Datatilsynet ikke ville kunne modbevise dette, men Datatilsynet henholder sig til, hvad der kunne være sket med de oplysninger, der lå på computerne. Datatilsynet rejser også sa-ger, hvor der ikke er sket direkte brud, men hvor det generelle sikkerhedsni-veau er for dårligt, som det var tilfældet i denne sag. Den dataansvarlige skal beskytte sig, inden det går galt, og mod at det går galt.

Selvom der i forbindelse med de phishingangreb, der blev anmeldt den 4. februar 2020 og den 20. maj 2020, blev sendt såkaldte lukkebreve fra Datatilsy-net til Tiltalte (Forening) om, at tilsynet ikke ville foretage sig yderligere i anledning af de skete brud, blev det i samme breve understreget, at tilsynet vil kunne genoptage sagerne eller lade dem indgå i vurderingen af eventuelle fremtidige brud- eller klagesager.

Foreholdt at Tiltalte (Forening) ikke hørte mere fra Datatilsynet inden beslutningen om politianmeldelsen blev truffet af det øverste ledelseslag i Datatilsynet, forklarede vidnet, at hun ikke kender til detaljerne i forbindelse med beslutningen i september 2021 om indgivelsen af politianmeldelsen.

Vidnet forklarede vedrørende det første brud om tyveriet af seks computere i oktober 2019, at hvis det havde været det eneste brud på datasikkerheden, som var sket hos Tiltalte (Forening), vil vidnet ikke tro, at det i sig selv ville have ført til en politianmeldelse.

Vedrørende den lønseddel, der var lagret på en ikke krypteret computer, forklarede vidnet, at oplysninger om løn m.v. er en følsom og fortrolig oplys-ning. Ansatte i en organisation er også beskyttet af databeskyttelsesforord-ningens artikel 32.

Computere, der ikke bruges til elektronisk behandling af personoplysninger er ikke omfattet af databeskyttelsesreglerne, men hvis der f.eks. lagres oplysninger om navngivne personer, der søger rådgivning hos f.eks. Tiltalte (Forening), finder databeskyttelsesreglerne anvendelse.

Vidnet forklarede vedrørende phishingangrebet den 12. maj 2020, der efter det oplyste angik almindelige personoplysninger for nuværende og tidligere medarbejdere samt 8 cpr. numre, herunder 3 mindreåriges cpr. nummer, forklarede vidnet, at cpr. numre, herunder cpr-numre på medarbejdernes børn, har karakter af personfølsomme oplysninger, fordi de kan misbruges i for-skellige sammenhænge.

Hvis en medarbejder har handlet i strid med de instruktioner vedrørende datasikkerhed, der gælder i en organisation, er kryptering er gængs og enkel foranstaltning til at sikre mod misbrug. Ansatte og andre kan lave fejl, og det er derfor ikke tilstrækkeligt at indskærpe overfor medarbejderne, at personhenførbare oplysninger ikke må behandles i Outlook, hvis computeren f.eks. ikke er krypteret.

Adspurgt af forsvareren forklarede vidnet, at en af de ting, der kan ske er, at medarbejdere ikke retter sig efter forskrifterne om datasikkerhed. Vidnet kan ikke svare på, om alle organisationer og offentlige instanser er på plads med kryptering. Det er rigtigt, at Datatilsynet senest i juni 2024 har politianmeldt Kommune for at benytte computere, der ikke var krypteret.

Hvis man har anmeldt et sikkerhedsbrud og Datatilsynet har fremsendt et kvitteringsbrev, hvoraf det fremgår, at Datatilsynet ikke foretager yderligere, og hvis der ikke kommer flere anmelder, forklarede vidnet, at Datatilsynet stadig kan foretage en samlet vurdering efterfølgende. Adspurgt om Datatil-synet har praksis for at åbne lukkede sager, forklarede vidnet, at det kan hun ikke sige noget generelt om.

Foreholdt af anklageren Datatilsynets udtalelser om bødepåstanden af 7. juni 2024 og 7. august 2024 i forhold 1, bilag 5 og 8, vedstod vidnet indholdet af udtalelserne. Datatilsynet indstiller fortsat efter en samlet bedømmelse, at Tiltalte (Forening) idømmes en bøde på 800.000 kr. for de brud på data-sikkerheden, de er sket i denne sag. Udgangspunktet for beregningen af bøde er foreningens regnskab for 2020, der er det regnskabsår, der ligger forud for indgivelsen af politianmeldelsen.

Anbefalingerne fra sammenslutningen af datatilsynene i EU landene er, at der overfor private virksomheder skal tages udgangspunkt i virksomhedens glo-bale opsætning, men det er Datatilsynets opfattelse, at det ikke er rimeligt i forhold til Tiltalte (Forening)s særlige karakter at tage udgangspunkt i et generelt omsætningstal, der f.eks. også indeholder indsamlede midler. Dette er baggrunden for, at der ved bødeindstillingen er taget udgangspunkt i fore-ningens indtægter fra genbrug og donationer. Det fremgår at motiverne til GDPR reglerne, at bødens størrelse skal være effektiv, afskrækkende og stå i rimelig forhold til overtrædelsen og således være proportional. Der skal f.eks. tages hensyn til, hvilke databeskyttelsesforanstaltninger organisationen har truffet, og Datatilsynet har betragtet det som en skærpende omstændig-hed, at Tiltalte (Forening) var længe om at indføre kryptering og multi-faktorgodkendelse.

Adspurgt om Datatilsynet ved en bødeindstilling ser på de faktorer om straf-beregning, der fremgår af straffelovens § 81 og 82, forklarede vidnet, at det gør tilsynet ikke, men overlader dette til domstolene. Det overlades herunder til domstolene at tage hensyn til f.eks. lang sagsbehandlingstid. Det fremgår direkte af GDPR reglerne og motiverne, at der skal fastsættes lavere bøder til offentlige myndigheder. Det er de enkelte medlemslande i EU, der bestem-mer om offentlige myndigheder skal straffes for brud på datasikkerheden, hvilket Folketinget har valgt i Danmark.

Foreholdt Partsrepræsentants forklaring om, at Tiltalte (Forening) efter hans opfattelse, på grund af organisationens særlige stilling og formål, ved afgørel-sen af bødens størrelse bør sidestilles med offentlige myndigheder, forklarede vidnet, at Datatilsynet ved indstillingen af en bøde på 800.000 kr. har taget hensyn til Tiltalte (Forening)s særlige stilling.

Adspurgt af forsvareren forklarede vidnet, at forordningens artikel 83, pkt. 3, angår en virksomheds samlede globale årlige omsætning i det forudgående regnskabsår, hvilket i Danmark fortolkes som det regnskabsår, der ligger for-ud for det år i hvilket politianmeldelse indgives.

Foreholdt bilag 5-2, side 34 forklarede vidnet, at reglerne primært er lavet med private virksomheder for øje. Vidnet bekræftede opfattelsen af, at de indtægter som Tiltalte (Forening) modtog ved indsamlinger m.v. ikke kan sidestilles med en privat virksomheds omsætning.

Vidnet forklarede, at de har lagt de faktiske omstændigheder til grund, som de har kunne læse ud fra de 4 indberetninger fra Tiltalte (Forening).
..."

Rettens begrundelse og afgørelse

Den 4. oktober 2019 indberettede Tiltalte (Forening) til Datatilsynet, at der fra foreningens hovedkontor i København den 2. oktober 2019 i tidsrum-met mellem kl.19.29 og 21.16 var sket tyveri af 6 bærbare computere, der in-deholdt personhenførbare oplysninger, jf. bilag 1-2-3.

Den 6. december 2019 indberettede Tiltalte (Forening) til Datatilsynet, at der fra foreningens kontor i Aarhus natten til den 4. december 2019 var sket tyveri af 5 computere, der indeholdt personhenførbare oplysninger, jf. bilag 1-2-4.

Den 4. februar 2020 indberettede Tiltalte (Forening) til Datatilsynet, at foreningen i perioden den 29. til 31. januar 2020 havde været udsat for et phishingangreb, der berørte personhenførbare oplysninger vedrørende medarbejdere i Tiltalte (Forening) og muligvis eksterne samarbejdspartnere, jf. bilag 1-2-5. Ved en skrivelse af 30. november 2020 til Tiltalte (Forening) meddelte Datatilsynet med henvisning til indberetningen af 4. februar 2020, at tilsynet "på det foreliggende grundlag ikke (vil) foretage sig yderligere overfor Tiltalte (Forening) i anledning af det skete brud på persondata-sikkerheden.". Tilsynet meddelte også, at man " vil kunne genoptage nærvæ-rende sag eller lade den indgå i vurderingen af eventuelle fremtidige brud -eller klagesager.", jf. bilag 1-2-5-2.

Den 20. maj 2020 indberettede Tiltalte (Forening) til Datatilsynet, at foreningen den 12. maj 2020 havde været udsat for et phishingangreb, der be-rørte personhenførbare oplysninger vedrørende medarbejdere i Tiltalte (Forening) og andre. Det fremgik blandt andet af indberetningen, at 1.100 personer kunne være berørt af phishingangrebet, jf. bilag 1-2-6. En skrivelse med et indhold, der svarer til indholdet af skrivelsen af 30. november 2020 til Tiltalte (Forening), blev af Datatilsynet den 22. januar 2021 sendt til Tiltalte (Forening) med henvisning til indberetningen af 20. maj 2020, jf. bilag 1-2-6-4.

Den 29. september 2021 indsendte Datatilsynet til Københavns Politi en politianmeldelse af Tiltalte (Forening) for overtrædelse af databeskyttelsesforordningens artikel 32, stk. 1, og på baggrund af denne anmeldelse og politiets efterforskning modtog retten den 15. marts 2023 det anklageskrift, som denne dom angår.

Det lægges ved sagens afgørelse til grund, at der på de i alt 11 bærbare computere, der blev stjålet fra Tiltalte (Forening)s kontorer i København og

Aarhus den 2. oktober 2029 og den 4. december 2019 blev foretaget elektronisk behandling af personoplysninger, herunder at der på computerne blev opbevaret personoplysninger, herunder cpr. numre. Tilsvarende gælder for de computere tilhørende Tiltalte (Forening), der var udsat for phishing-angreb i januar og maj 2020. Retten henviser i den forbindelse blandt andet til indholdet af de 4 indberetninger som Tiltalte (Forening) indsendte til Datatilsynet den 4. oktober 2019, den 6. december 2019, den 4. februar 2020 og den 20. maj 2020 og til forklaringen fra Partsrepræsentant. På grund af den elektroniske behandling af personoplysningerne er Tiltalte (Forening), som dataansvarlig efter databeskyttelsesforordningens artikel 32, stk. 1, for-pligtet til at gennemføre passende tekniske og organisatoriske foranstaltnin-ger til at imødegå risikoen for misbrug af personoplysningerne. Det lægges efter indholdet af indberetningerne til grund, at der på de omhandlede com-putere lå oplysningerne om mindst 1.347 registrerede personer.

Efter bevisførelsen, herunder forklaringen fra Partsrepræsentant, lægger retten endvidere til grund, at Tiltalte (Forening) i 2019 ikke havde sørget for at kryptere computerne, hvilket er en foranstaltning, der direkte er nævnt i databeskyttelsesforordningens artikel 32, stk. 1, litra a. Det lægges endvidere til grund, at de computere, der var udsat for phishingangrebet, ikke var sikret ved multifaktorgodkendelse ved login. Retten bemærker i den forbindelse, at der under de foreliggende omstændigheder er holdepunkter for at antage, at også andre af Tiltalte (Forening)s computere, udover dem, der er omfat-tet af indberetningerne, i gerningsperioden fra august 2018 til juli 2020 ikke var krypterede eller forsynet multifaktorgodkendelse ved login. Blandt andet på baggrund af vidneforklaringen fra Vidne 1 lægger retten til grund, at kryptering og multifaktorgodkendelse ved login også før gernings-perioden i denne sag var kendte og tilgængelige foranstaltninger til sikring af datasikkerheden.

Efter indholdet af de to skrivelser af 30. november 2020 og 22. januar 2021 fra Datatilsynet til Tiltalte (Forening), sendt i anledning af indberetnin-gerne af de to phishingangreb af 4. februar 2020 og 20. maj 2020, finder ret-ten, at det ikke er udelukket, at anklagemyndigheden medtager de to phishin-gangreb i anklageskriftet.

På den anførte baggrund og de i øvrigt foreliggende oplysninger er det be-vist, at Tiltalte (Forening) er skyldig i overensstemmelse med den rejste tiltale.

Straffastsættelse

Straffen fastsættes til en bøde på 75.000 kr., jf. databeskyttelsesforordnin-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.

Datatilsynet har i forbindelse med politianmeldelsen indstillet, at Tiltalte (Forening)

idømmes en bøde på 800.000 kr., hvilken indstilling anklage-myndigheden har fulgt i sagen. Det fremgår af pkt. 150 og 151 i præamblen til databeskyttelsesforordningen, at der med forordningen er tilsigtet en harmonisering i EU af sanktionerne for overtrædelse af reglerne. Det fremgår endvidere, at de kompetente nationale domstole bør tage hensyn til en anbefaling fra den nationale tilsynsmyndighed, der har taget skridt til bøden, samt at de idømte bøder under alle omstændigheder skal være effektive, stå i rime-ligt forhold til overtrædelsen og have en afskrækkende virkning.

Ved fastsættelsen af bøden til 75.000 kr. lægger retten afgørende vægt på karakteren af den virksomhed, som Tiltalte (Forening) udøver, herunder foreningens formål. Det tillægges i den forbindelse også betydning, at det læg-ges til grund, at Tiltalte (Forening) ikke skal generere indtægter til andet end det, der ligger i foreningens formål. Herudover er der ved fastsættelsen af bødens størrelse taget hensyn til sagsbehandlingstiden, idet retten lægger til grund, at sagen ikke er kompleks, men alene angår en vurdering af betyd-ningen af, at Tiltalte (Forening) ikke i 2019 og 2020 anvendte krypterede computere og ikke havde indført multifaktorgodkendelse ved login.

Thi kendes for ret:

Tiltalte (Forening) straffes med en bøde på 75.000 kr.

Tiltalte skal betale sagens omkostninger.

Dommer