RETTEN I RANDERS

Udskrift af dombogen

D O M

afsagt den 1. september 2023

Rettens nr. 2-2233/2022
Politiets nr. 4200-84266-00057-21

Anklagemyndigheden
mod
Favrskov kommune
CVR nr.

Anklageskrift er modtaget den 27. maj 2022.

Favrskov kommune er tiltalt for overtrædelse af

Europa-Parlamentets og Rådets Forordning (EU) 2016/79 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger om fri udveksling af sådanne oplysninger og om op-hævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) artikel 83, stk. 2 og stk. 4, jf. litra a, jf. stk. 9, jf. artikel 32, stk. 1 samt lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af behandling af personoplysninger om fri udveksling af sådanne oplysninger § 41, stk. 1, nr. 1, jf. stk. 3 jf. stk. 6, ved i en perio-den fra den 22. august 2019 til den 13. august 2020 kl. 07.30 ikke at have overholdt sin forpligtelse som dataansvarlig til at gennemføre tekniske og or-ganisatoriske foranstaltninger, der passede til risici af varierende sandsynlig-hed og alvor for de registreredes rettigheder, idet Favrskov Kommune ikke havde sørget for at kryptere kommunens bærbare computere, hvilket medfør-te et utilstrækkeligt sikkerhedsniveau og tillige havde den konsekvens, at et sikkerhedsbrud medførte en unødig høj risiko for de registrerede, idet en bærbar computer - indeholdende personoplysninger af følsom karakter om ca. 100 personer i kommunens botilbud for borgere med fysisk eller psykisk nedsat funktionsevne – på et tidspunkt i perioden fra den 12. august 2020 kl. 18.00 til den 13. august 2020 kl. 07.30 blev stjålet fra en skuffe i forbindelse med et indbrud i sundhedscenteret, Adresse i By.

Påstande

Anklagemyndigheden har nedlagt påstand om bøde.

Tiltalte har nægtet sig skyldig.

Sagens oplysninger

Repræsentant for Favrskov kommune, Vidne 1, har forklaret, at han har været ansat som Stilling 1 ved Favrskov Kommune siden maj 2005. IT-sikkerhed hører under hans ansvarsområde. I december 2018 blev der udviklet på en allerede eksisterende IT-masterplan, som løbende op-dateres. På det strategiske plan skulle der være krypteret data på deres hard-diske. Planen indeholdt bunker af andre aktiviteter, som skulle iværksættes i forhold til opdateringer for brugernes gavn og sikkerhed. Kryptering blev ik-ke top prioriteret, da der var andre ting, som de vurderede var vigtigere grundet det tekniske setup. Det var en kæmpe opgave at sætte kryptering i gang, hvilket de var klar over, men der var andre ting, som også var vigtigere på daværende tidspunkt. De ville blandt andet sikre multifaktorer på webma-ils og lignende. De ville også forberede segmentering af nettet, da det ville give en bedre beskyttelse. Kryptering dukkede op og kom ind som en del af planen, da de fulgte med i de nyeste tekniske muligheder og sikkerhedskrav. De skiftede også VPN klient på grund af sikkerhed. Kryptering af computere skulle laves, da de overvejede, om de skulle begynde at bruge computerne lokalt. De har dog ikke indført brug af lokal computer, men muligheden lig-ger stadig i deres strategi. Hvis de skal bruger computerne lokalt, skal de væ-re krypteret. I Favrskov Kommune benytter de sig af fjernskrivebord som ar-bejdsplatform. Krypteringsprojektet blev løbende drøftet på deres teamleder-møder, men de vurderede, at andre ting var mere presserende. Hændelsen med tyveriet satte dog turbo på processen. En medarbejder kom til at instal-lere et program lokalt, hvor der blev lagt persondata på. Der er nogle klare retningslinjer for, hvordan man skal agere sikkert med sin computer. I ret-ningslinjerne står det klart, at det er Favrskov skrivebordet, der skal benyttes og ikke ens lokale skrivebord. Som medarbejder er det muligt at gemme ting på sit lokale skrivebord. Der kunne f.eks. gemmes et PowerPoint på det lo-kale skrivebord, men det skal være uden personoplysninger. Favrskov Kom-mune formidler sikkerhedsprocedurer ud på mange forskellige kanaler, her-under blandet gennem en introvideo, sikkerhedsvideoer, flyers og lignende. Det fremgår af sikkerhedsoplysningerne, at der ikke må ligges persondata på eget skrivebord. Baggrunden for at lave kryptering på computerne var, at man kunne arbejde på sin lokale computer. De havde i tankerne, at alt hvad brugerne skulle benytte, skulle ligge på kommunens skrivebord. Det har ikke fyldt ret meget, at nogle medarbejdere kunne finde på at lagre data lokalt på sin computer. Favrskov Kommune har omkring 3.300-3.400 IT-brugere. Den 13. august 2020, hvor indbruddet fandt sted, blev en skillelinje. De ting de la-vede i den optil den 13. august 2020 havde til formål at forbedre sikkerheden generelt. Deres strategi er, at alle medarbejdere arbejder på deres fælles skri-vebord, hvorved de bærbare computer ikke er noget specielt i sig selv, da da-ta altid kan findes på deres fælles skrivebord. De vil sikre deres servermiljø, og at medarbejderne har de rigtige adgange til de rigtige systemer.

Computerne bliver ikke scannet for persondata eller tjekket på anden måde. Medarbejderne er oplyst om, at de ikke skal ligge noget på deres private skri-

vebord, for hvis de mister computeren, så er det væk. Medarbejderne var gjort opmærksom på, at der kunne ske sikkerhedsbrud, hvis de ikke fulgte disse retningslinjer. Alle blev oplyst om, at alt arbejde skulle foregå på Favrskov skrivebordet. Instruksen om, at medarbejderne ikke måtte bruge computerne lokalt, var også et sikkerhedstiltag. Hvis det lokale skrivebord benyttes, bliver der ikke lavet backup og data vil derfor forsvinde, samt der er risiko for sikkerhedsbrud. Der er ikke log på det lokale skrivebord, hvilket man har pligt til, hvis der lagres data derpå. Favrskov Kommune har en sik-kerhedstrekant, hvor der tydeligt står, hvordan man må gemme oplysninger på sin computer.

På forsvarerens spørgsmål har Vidne 1 forklaret, at det tekniske setup var grund til, at der ikke blev lavet kryptering. Medarbejderne i Favrskov Kommune har mulighed for at arbejde hjemme, hvor de kan tilgå og arbejde på det fælles skrivebord. Nogle kommuner har valgt at benytte sig af nogle andre strategier. De valgte løsningen med at arbejde fra et fælles skrivebord, da det fungerede bedst for dem på daværende tidspunkt. Deres system funge-rer ligesom Citrix, hvor deres fagsystemer ligger på og kan tilgås fra en fæl-les platform. Fordelen ved denne løsning er, at ingen data går tabt, de skal ik-ke tage backup, og hvis en computer bliver stjålet, vil der ikke ske sikker-hedsbrud, medmindre en medarbejder har brudt reglerne. De tager backup i datacenteret, så de skal ikke tænkte på at sikkerhedsopdatere de enkelte computere. De har løbende overvejet at forbedre deres sikkerhed, og i 2018 kom kryptering af computerne på tale. Der var flere muligheder i spil. Det var deres vurdering på daværende tidspunkt, at det ikke var det, som de skul-le kaste sig over først. De var blandt andet ramt af nogle hackerangreb, da deres webmail ikke var sikret. Favrskov Kommune har imellem 2.200 – 2.300 computere. Det kunne tage op til 5 timer pr. computer at kryptere dem. De fandt ud af, at opgaven indebar, at hver enkelt computer skulle kal-des ind til IT-kontoret for at blive krypteret. De har fået computerne krypte-reret nu. Hele situationen opstod i coronaperioden, hvilket ikke gjorde det nemmere, men de forsøgte at gøre det så effektivt som muligt. De ansatte en mand til at håndtere opgaven, som benyttede Gecko Bookings systemer, hvor alle brugere skulle booke en tid til at aflevere deres computer til krypte-ring. I 2018 valgte de andre sikkerhedstiltag som f.eks. yderligere segmente-ring af netværket. Det betød, at deres server stod på et centralt sted, der var adskilt fra den lokale computer, hvilket var med henblik på at begrænse tra-fikmængden og for ikke at blive inficeret og hacket. Der var også noget med firewalls på strategiplanen, som de vurderede var vigtigere, da de havde haft 13 hackerangreb over en forholdsvis kort periode. Overvågning af logs var også en ting, som de havde fokus på for at få mere viden om hackerangrebe-ne. De forsøgte at holde øje med medarbejderes log. Når medarbejderne til-gik Outlook/webmail og fjernskrivebordet hjemmefra, skulle de logge ind med brugernavn, kode og NemID. Det blev efterfølgende skærpet yderligere, og NemID blev erstattet af mit-ID. Ukrainekrigen har også gjort, at de måtte lave nogle ændringer i deres firewall. Center for Cybersikkerhed har sendt nogle anbefalinger ud, som de skulle forholde sig til. Staten har strengere sik-

kerhedskrav end kommunerne. Det kan ikke lade sig gøre at have et sikkerhedsniveau på 100 %, da der altid kan opstå sikkerhedsbrud. Selv sikkerhedsfirmaer kan ikke have en 100 % sikkerhedsgaranti.

På den computer, som blev stjålet, var der oplysninger om navne, adresse og muligvis også CPR-numre på nogel borgere. Han er lidt i tvivl om CPR-num-re var fjernet, men det har han hørt. Det var oplysninger, som var offentlig kendte, som man også ville kunne finde ved at se på en postkasse aller søge personen på krak, hvis de ikke har adressebeskyttelse. Det var oplysninger på personer med særlige behov. De har ikke kendskab til, at nogen skulle have misbrugt oplysningerne. Computeren var låst, så man skal have harddisken ud og have et vist kendskab til, hvordan man kan tilgå dataen. Tyveriet ligne-de et brugstyveri, hvor det blev stjålet forskelligt teknisk udstyr, såsom com-puter, iPad og lignende. Der blev ikke stjålet papirer med persondata. Han husker ikke om computerne skal være i en aflåst skuffe, men den må i hvert fald ikke ligge synlig i f.eks. en bil. Den pågældende medarbejder, der over-trådte deres regler, har muligvis haft en personlig samtale i sin afdeling. Han var ikke ansat i medarbejderens afdeling, men han tror, at medarbejderen har været til en samtale. Den pågældende er ikke ansat i kommunen mere, men ikke på grund af denne episode.

På anklagerens spørgsmål har han forklaret, at computeren skulle opbevares i et aflåst lokale, hvilket står skrevet i deres reglement. Den må ikke være syn-lig i hjemmet, og hoveddøren skal være låst, hvis man forlader hjemmet. Man skal heller ikke have alarm i hjemmet. Kryptering kom ind på deres master-plan i 2018, men det var ikke noget nyt. Det kom nogle år før, men for at ud-nytte muligheden bedst muligt, skal der være en TPM chip i computeren. De skiftede 250 computere, som slet ikke duede.

Vidne 2 har som vidne forklaret, at hun er ansat i Favrskov Kommune og har været det siden 2006. Hun er Stilling 2 af Service og support i IT-afdelingen. De holder blandt andet styr på kommunens computere. På et ledermøder snakkede de om deres masterplan, hvor kryptering af kommu-nens harddiske var på tale. Emnet blev medtaget på deres møde, da de var begyndt at snakke om, at de skulle pushe programmer ud lokalt på compu-terne, men det gik de fra igen. De sagde altid til kommunens medarbejdere, at de ikke måtte gemme noget lokalt, men at de skulle gemme på det fælles skrivebord. Alle medarbejdere fik også oplyst, at de skulle arbejde i de sikre programmer. Hun har tit undervist og introduceret nye medarbejdere, hvilket hun nok også gjorde i 2014. Hun havde altid punktet om at gemme i fagsy-stemerne med. Senere blev der lavet en introduktionsvideo, som de sendte ud til nye medarbejdere, og ophørte med fysisk undervisning. De opfordrede al-tid nye medarbejder til at se videoen. Hun lavede også intro til de nye ledere, hvor hun opfordrede dem til at få deres medarbejdere til at gå kommunenens IT-retningslinjer igennem. De har medarbejderne i telefonen, hvis de ikke kan finde ud IT'en, og så bliver de igen opfordret til at se filmene. De har e-lear-ning om, hvordan man gemmer følsomme oplysninger. De kan gå ind og se,

hvis den enkelte medarbejder ikke har gennemført kurserne. Hun står ikke for at følge op på det, så hun ved ikke, hvordan det bliver gjort. Hun tror, at der bliver sendt en mail ud til dem, som ikke har gennemført det, hvor de op-fordres til at få det gjort. Der kan derfor være nogle medarbejdere, som ikke har set videoerne. Man får at vide, at følsomme oplysninger ikke må ligge i Outlook mere end en måned, og at alt hvad der er følsomme personoplysnin-ger skal gemmes i fagsystemerne. Det kan være forskellige fagsystemer, som bruges i de forskellige afdelinger. De bliver oplyst om, at de skal gemme det der, for at passe på borgerens data. De har også en sikkerhedstrekant, som er delt ud til medarbejderne. Hun ved ikke, om det står på sikkerhedstrekanten, hvad der sker, hvis de ikke gør brug af fagsystemerne. Men hun tror, at alle ved det, da det er almen viden, på grund af alt den snak der har været om sikkerhed og hacking. De tjekker ikke, om mails i Outlook bliver slettet efter de 30 dage, men de er ved at undersøge, hvordan de kan gøre det. Hun er ik-ke bekendt med, om andre kommuner laver kontrol. De skriver tydeligt ud til medarbejderne, at de skal overholde det. De forsøger at formidle mange ting, som de skal overholde, så der er meget, som nye medarbejdere skal forholde sig til. I 2018 tog de kryptering ind i deres masterplan, da det var oppe at vende, at medarbejderne kunne begynde at ligge data på deres lokale skrive-bord. De skulle være klar med Bit-Locker, som er en kryptering. Kryptering var nyt for hende dengang, men vist ikke for alle. Hun var ikke opmærksom på muligheden for kryptering, før hun hørte nærmere om den dengang.

På forsvarerens spørgsmål har hun forklaret, at der igennem lederne blev fuldt op på, at medarbejderne så deres e-learningskurser om sikkerhed. De havde også nogle undervisningshold fire gange om året for de nye ledere, hvor de gør meget ud af at sige, at det er vigtigt. Lederne får at vide, at de skal tjekke log og rettigheder. Der kommer løbende link til e-learning, og dem som ikke har gennemført, får en reminder om at få det gennemført. Le-deren får også en reminder. De kigger også på hvem, der har adgang til per-sondata. Det er BDO'en, som har lavet e-learningskurserne, men hun tror, at alle med en e-mail i kommunen får tilsendt oplysningerne om e-learning, da det kan være relevant for mange. Hun tror, at der kun har været ét andet tid-ligere sikkerhedsbrud.

På anklagerens spørgsmål har hun forklaret, at det ikke var Favrskov kommunes data, der blev lækket ved det andet sikkerhedsbrud, men en medarbejders private familiebilleder, som var mistet, da hendes iPad blev stjålet. Medarbejderen fik at vide, at hvis billederne ikke lå i skyen, så kunne de ikke hjælpe hende med at få dem tilbage. Denne episode skete før 2018. De får en melding hver gang, der er sket et tyveri, og i den forbindelse spørger de ind til læk af data, da det kan være en mulighed. De kan ikke forhindre folk i at gemme fortrolige lokalt, hvis de vil gemme.

Vidne 3 har som vidne forklaret, at han i 2020 var ansat i Favrskov Kommune. Han blev ansat den 1. juli 2014 som Stilling 3 i handi-cap og psykiatri. Han havde en arbejdscomputer, hvor der fulgte nogle IT-

sikkerhedsoplysninger med. Der stod blandt andet, at de skulle arbejde i fagsystemerne, som var sikre. Han arbejdede fortrinsvist i de sikre programmer. Han brugte også et Mindmap program til at skabe et overblik over, hvor borgere boede. Han brugte et gratis program, som hedder FreeMind. Han havde tidligere brugt programmet privat. Han ved også, at det bruges i andre kommuner. Da han downloadede programmet, vidste han ikke, at det blev brugt i andre kommuner, men det har han fundet ud af efterfølgende. Han havde gemt oplysninger på de tilbud, som var i kommunen til beboere med varige fysiske og psykiske handicap, hvor han havde delt borgerne op efter bopæl. Han havde oplysninger om 102 personer i programmet. Oplysningerne, der omfattede navne og cpr-numre på personerne, var koblet op på adresserne. Han holdt det ikke hemmeligt, at han brugte programmet. Han tænkte dog på et tidspunkt, at det måske ikke var så godt at bruge det på grund af GDPR, og derfor stoppede han med at bruge det. Det var et gratis program som lå lokalt på hans computer. Han stoppede med at bruge det i 2019/2020. I au-gust 2020 var programmet stadig på hans computer. I forlængelse af at han blev opdateret på GDPR-reglerne slettede han programmet.

Foreholdt bilag 1.10, afhøringsrapport, har han forklaret, at det godt kan passe, at han til politiet har forklaret, at oplysninger, som lå i FreeMind, var navne og adresser på borgerne. Når han benyttede FreeMind, oprettede han dokumenter med oplysninger med borgernes navne og personnumre, knyttet op på adresserne. Dokumenterne blev gemt lokalt på hans computer. Han slettede FreeMind før tyveriet, men dokumenterne med oplysningerne lå sta-dig på computeren. Da hans computer blev stjålet, var der oplysninger om cirka 100 personer. Han opdagede i august 2020, at oplysningerne stadig lå på computeren, men han brugte ikke programmet aktivt længere. Man skulle downloade og bruge FreeMind for at tilgå dokumenterne med oplysningerne. Han var klar over, at det stadig kunne ligge i en mappe, selvom han havde slettet programmet.

Da han blev ansat, fik han at vide, at han skulle overholde IT-retningslinjer-ne. Han husker ikke, hvad han præcis fik at vide, men han skulle i hvert fald arbejde i fagsystemerne. Han husker ikke, om han fik at vide, at de ikke måt-te gemme ooplysninger lokalt, men han vidste det godt. Han kender lidt til kryptering, da han nu er ansat i anden kommune. Da han var ansat i Favrskov kommune, var han ikke bekendt med, om hans computer var krypteret eller ej. Han husker ikke, om der var givet retningslinjer om at downloade andre programmer.

På forsvarerens spørgsmål har han forklaret, at oplysningerne på computeren var gemt i en mappe for sig. Man skal selv vide, at man skal kigge efter et FreeMind dokument på computeren, og man skal have FreeMind installeret på sin computer for at kunne åbne mappen. I programmet kunne man se et Mind Map over de forskellige enheder, hvor borgernes navne og cpr-numre fremgik. Han slettede i de senere versioner cpr-numrene, da han ikke skulle bruge dem til noget. Det var derfor kun i de første versioner af dokumentet,

at cpr.nr. fremgik. For at komme ind på hans computer, skal man logge ind med to koder. Der var ikke andre sikkerhedsforanstaltninger end de to ko-der. Alarmsystemet i bygningen virkede ikke den dag, hvor computeren blev stjålet. Hvis han gik fra kontoret, var computeren låst ned i en skuffe.

Vidne 4 har som vidne forklaret, at han er Stilling 4 ved Datatilsynet. Han arbejder med sikkerhedsbrud, der bliver indberettet til dem. I den forbindelse finder han ud af, hvad der er sket, og hvad der skal ske fremadrettet. Han har ikke arbejdet på sagen vedrørende Favrskov Kom-mune. Alt beror på en konkret risikovurdering for hver enkelt sag. Hvis man laver en risikofyldt aktivitet, skal man lave en modforanstaltning der imøde-går risikoen. Når man sender sine medarbejder ud i byen med en mobil en-hed/computer, er den eneste effektive modforanstaltning for beskyttelse af data, der ligger lokalt på en enhed/computer, er en kryptering af enheden/ computeren. Hvis man laver en kryptering, så sikrer man fortrolighed på computeren. Computeren er umulig at komme til, hvis den er sikret ordent-ligt. Det findes også andre foranstaltninger, såsom integritetsbeskyttelse eller hindring i lokal lagring, men kryptering er den mest effektive tekniske foran-staltning. Kryptering har været kendt i mange år og er almindelig branche-praksis. Det står blandt andet i "NIST" fra 2000, som er de Nationale sikker-hedsstandarder og i ISO27. Iso har været integereret i Windows siden 2007/ 2008. I 2018 burde man kende til kryptering som IT-medarbejder. Organisa-torisk sikkerhedsforanstaltinger er gode, men man kan fortsat risikere, at me-darbejdere gemmer lokalt på computeren alligevel. Erfaringer viser, at hvis medarbedjerne ser, at der er en mulighed for at lagre lokalt, vil de også gøre det. Kryptering er derfor den bedst tekniske løsning, så man ikke behøver læ-ne sig op ad, at folk gør, som der bliver sagt eller aftalt. Man kan centralt styre og installere kryptering på computerne via MDM-systemer. Man vil og-så via MDM-systemer kunne slette oplysninger på computeren og se, hvor den befinder sig. Det er nemt at kryptere computerne. Hvis man ikke har et centralt styringssystem, kan man udstikke politikker, hvor igennem man sty-rer, at der oploades og installeres kryptering lokalt af medarbejderne, eller selv tage ud og foretage krypteringen lokalt på computeren. Hvis en harddisk ikke er krypteret og computeren bliver stjålet, er det let at tilgå et drev. Man skal blot pille harddisken ud og koble den til et andet udstyr, hvorefter der er fri adgang til filerne på drevet. I hans verden skal man have kryptering på sin harddisk.

På forsvarerens spørgsmål har han forklaret, at han arbejder med tekniske foranstaltninger. Han ved ikke, om alle kommuner har kryptering på deres computere, men han ved, at de har ved Nyborg Kommune. Det kan godt væ-re, at nogle kommuner ikke har. Det handler om prioritering fra kommune til kommune, men der er nogle minimumskrav til sikkerheden fra statens side. I deres seneste undersøgelse har flertallet af de adspurgte kommuner svaret, at de har krypteret deres cpmputere. Det har været en IT-teknisk standard at kryotere i mange år. Det har ikke lige så længe været en kommunal standard at kryptere computerne. I kommunerne har kryptering siden 2020 væreten

del af de tekniske minimumskrav. Minimumskravene er anbefalinger. Det er ikke et krav, at de skal følges, men det kan være en god idé at gøre det.

På anklagerens spørgsmål har han forklaret, at kryptering er let, hvorfor man anvende dem også til sine servere. Ved at foretage kryptering, er man sikker på, at oplysningerne på serveren eller lokalt på computeren er i sikkerhed og ikke kan tilgås i tilfælde af tyveri. Risikoen for at oplysninger kommer i de forkerte hænder er større ved mobile enheder, og behovet for kryptering er derfor også større på disse.

På forsvarerens spørgsmål har han forklaret, at kryptering er billig og nemt. Når han har læst kommunen beskrivelse af deres arbejde med krypteringen igennem, forstår han de sådan, at kommunen også har foretaget andre foranstaltninger ved computerene, og derfor har det været besværligt og taget tid. Hvis man har besluttet sig for at anvende kryptering, så er det ikke en kompleks opgave, men det tager selvfølgelig tid alt afhængig af, hvilken platform de benytter.

Vidne 5 har som vidne forklaret, at hun er Stilling 5 ved Datatilsynet. Hun har været ansat i Datatilsynet i et års tid. Hun har tidli-gere været ansat i politi og anklagemyndig, hvor hun arbejdede som databes-kyttelsesrådgiver. I Datatilsynet behandler de brud på persondata. De modta-ger omkring 9.000 brud om året. Nogle af brudene kan se selv sanktionere imod og andre bliver politianmeldt. Indenfor databeskyttelsesområdet har de flere reaktionsmuligheder såsom påbud, forbud, udtale kritik og i grovere sa-ger kan de indgive en politianmeldelse, hvis virksomheden eller den offentlige myndighed står til en bøde. Mange brud giver ikke anledning til reaktioner, men tilsynet går ind i de groveste sager. Vedrørende Favrskov Kommune har de vurderet, at der skulle ske en politianmeldelse, da de mener, at kommunen skal have en bøde. De vægter, at der er tale om en offentlig myndighed, som behandler mange personfølsomme og fortrolige oplysninger. Det kan have konsekvenser for mange personer, hvis deres oplysninger bliver delt. Der er især vigtigt for kommuner at passe ekstra på, da borgerne ikke selv kan væl-ge, om kommunen behandler deres personoplysninger og derfor har en for-ventning om, at der bliver passet på deres oplysninger. En gængs ting er, at man bruger kryptering på sine computere. Når man skal lave sikkerhedsfor-anstaltninger, kan der være organisatoriske og tekniske foranstaltninger. Favrskov Kommune har lavet organisatoriske foranstaltninger ved at sige, at medarbejderne arbejde på en bestemt måde. Det er bare ikke nok i dette til-fælde, da mennesker begår fejl. Efter praksis er organisatoriske foranstaltnin-ger ikke nok i sig selv. Nogle gange kan man ikke lave begge dele, men det kunne kommunen godt i dette tilfælde. Det er simpel, enkelt og billigt at kryptere computerne. Det kan være svært at lave tekniske foranstaltninger, men det er en konkret vurdering. Datatilsynet har i denne sag lagt vægt på, at den manglende kryptering har stået på over en længere periode. Det var alle kommunens computere, som ikke var krypteret og kommune var klar over, at de burde kryptere dem. Det fremgår også af anbefalinger til kommunerne.

Det er nyt for Datatilsynet, at man kan straffe offentlige myndigheder, og de er ved at udvikle praksis. Der findes i forordningen et bødeloft. De nationale myndigheder / folketinget har bestemt, at man skal kunne straffes med bøde, men at bødeloftet skulle sættes ned. Man kan ikke sammenligne offentlige og private virksomheder i forhold til bødeniveauet. Det er op til retten at tage stilling til bødeniveauet. Det fremgår af forordningen, at bøderne skal være effektive og afskrækkende, men de er ikke voldsomme. I denne sag er der en indstilling på 75.000 kr. i bøde, hvor der er lagt vægt på grovhed og Kommunens driftsbevilling. Der findes en tidligere dom over Hørsholm kommune med en bøde på 50.000 kr. og en indstilling i en politianmeldelse mod Gladsaxe kommune, hvor der er tale om en bøde på 100.000 kr., så denne sag lig-ger midt i. Det er samme forbrydelsestype. I denne sag er derkonkret tale om oplysninger om 100 personer på en enkelt computer, men det kunne have været alle computere i kommunen, da ingen var krypteret. Det er dog formil-dende omstændighed, at kun 100 personer er berørte. Men det er ren tilfæl-dighed, at det kun er 100 personer, da det kunne have været mange flere. Man skal derfor ikke fokusere på, at det kun var 100 personer, det gik ud over. Hvis kommunen havde krypteret alle andre end den ene computer, hav-de vi nok ikke siddet med sagen i retten. Det er den potentielle risiko og om-fanget, der skal ses på. Kommunen havde gjort noget, men efter praksis, er det bare ikke nok. Kryptering er udenfor hendes område, da hun er jurist, så hun kan ikke sige om det er nemt at foretage kryptering. Fagpersoner fortæl-ler hende, at det er billigt og nemt at gøre.

På forsvarerens spørgsmål har hun forklaret, at i denne sag er det ikke afgø-rende, at det er gået ud over 100 personer, men at det nemt at lave krypte-ring. Hvis de havde været på besøg ved kommunen i 2020, så ved hun ikke, om de ville have fået en bøde. Hun har kun været ansat ved Datatilsynet i et år, og det er sådan de gør nu. Kommunen kunne have lavet andre tekniske foranstaltninger, såsom at indstille computere til, at man ikke kan gemme no-get på dem. Det er ikke tilstrækkeligt blot at sige til medarbejdere, at de ikke må gemme lokalt på computeren. Det er Datatilsynets praksis at politianmel-de de kommuner, der ikke har krypteret sine computere. De har foretaget en modenhedsundersøgelse, hvor de har stillet spørgsmål 55 kommuner. Undersøgelsen er ikke færdig endnu, så hun kender ikke resultatet af undersøgel-sen. Det er tilsynets opfattelse, at det koster kommuner en bøde, hvis de ikke har kryptering på deres computere. De oplysninger der lå på den stjålne com-puter var fornavn, efternavn og cpr-nummer, og der fremgik oplysninger, hvoraf man kunne udlede, at det var personer med fysisk eller psykisk nedsat funktionsevne. Jo mere beskyttede oplysninger, der behandles, jo bedre skal sikkerheden være, da de kan misbruges. Når de skal vurdere en sag, så kig-ger de på karakteren af de oplysninger, der er kommet ud. De har ikke haft mulighed for at tjekke computeren, da den er væk. Kommuner har pligt til at indberette sandfærdigt, og det er kommunen der har givet dem de oplysnin-ger, som de har vurderet sagen på grundlag af. De har baseret en politianmel-delse ud fra det, som der er sendt ind fra kommunen. Hun kender ikke til de

nærmere tekniske ting omkring kryptering, men det er ikke noget nyt, så kommunen har været bekendt med muligheden. Kommunen har været for langsom, da de burde have gjort for lang tid siden. En sag kan være værre, hvis man slet ikke har gjort noget. Det er Datatilsynets opfattelse, at alle computere i alle kommuner skal krypteres, da det er gængs praksis, og man-gelnde kryptering giver en bøde. Hun er ikke bekendt med, om de har været ude på fysiske tilsyn.

Tiltalte er tidligere straffet

ved bødeforlæg af 9. maj 2022 for overtrædelse af lov om godkendelse og syn af køretøjer § 13. stk. 1, jf. stk. 3, jf. § 3, stk. 1 med en bøde på 2.000 kr.

Rettens begrundelse og afgørelse
Efter forklaringerne af Vidne 1 og Vidne 2 lægger retten til grund, at Favrskov Kommune har foretaget en række organisatoriske sikker-hedsforanstaltninger i forhold til kommunens bærbare computere ved at give medarbejderne instruktion om, at de ikke måtte gemme oplysninger på de lo-kale computere og anvise, at de skulle arbejde i fagsystemerne på Favrskov skrivebord og i Sensun Bosted. Retten lægger efter forklaringerne videre til grund, at kommunens bærbare computere var beskyttet med password, og at kryptering af de bærbare computere var en del af kommunene IT-masterplan siden 2018.

Retten lægger efter Vidne 3's forklaring til grund, at hans bærba-re arbejdscomputer blev stjålet ved et indbrud mellem den 12. og 13. august 2020. Computeren lå under indbruddet i en aflåst skuffe. På computeren hav-de han haft installeret et freeware-program "FreeMind", som han brugte til at skabe overblik over kommunens botilbud. I programmet havde han lavet do-kumenter med oplysninger om 102 beboere i botibuddene, som først inde-holdt navne og personnumre på beboerne, og senere kun beboernes navne. Beboerne kunne via dokumenterne knyttes til botilbuddene, der var til perso-ner med fysiske og psykiske handicap. Retten lægger efter hans forkalring til grund, at han på tidspunktet for tyveriet havde slettet FreeMind på compute-ren, men at dokumenterne fortsat var gemt på computerens harddisk. Kom-munen havde endnu ikke krypteret computerene på tidspunktet for tyveriet, og tyveriet indebar derfor et brud på persondatasikkerheden, idet der på computeren lå personoplysninger om ca. 102 beboere, herunder oplysninger af følsom karakter og oplysninger om personnumre.

Selvom kommunen havde retningslinjer for, at der ikke måtte lagres lokalt på de bærbare computere og foretaget en række øvrige organisatoriske sikker-hedsforanstaltninger, finder retten efter en samlet vurdering, at kommunen ved ikke at kryptere computerne eller iværksætte andre passende tekniske foranstaltninger, ikke har gennemført de fornødne tekniske sikkerhedsforan-staltninger på kommunens mellem 2.200 -2.300 bærbære computere for at

sikre et sikkerhedsniveau, der passer til de risici, der var for de registreredes rettigheder. Retten har herved lagt vægt på, at kommunen måtte påregne, at ikke alle ansatte fulgte interne retningslinjer, og på den generelle risiko for tyveri og anden bortkomst, der er forbundet med, at medarbejderne har en bærbar computer til rådighed.

Retten har ved bødefastsættelsen særligt lagt vægt på, at der er tale om en alvorlig overtrædelse af databeskyttelsesforordningens artikel 32, idet kommunen forud for tyveriet på sin IT-masterplan siden 2018 havde vurderet, at yderligere tekniske foranstaltninger i form af kryptering af de bærbare computere var en nødvendig foranstaltning. Bøden er i overensstemmelse med Datatilsynets indstilling beregnet på grundlag af Favrskov Kommunes seneste offentliggjorte foregående driftsbevilling og indbyggertal forud for endelig dom.

Bøde fastsættes derfor til 75.000 kr., jf. Europa-Parlamentets og Rådets Forordning (EU) 2016/79 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger om fri udveksling af sådan-ne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) artikel 83, stk. 2 og stk. 4, jf. litra a, jf. stk. 9, jf. artikel 32, stk. 1 samt lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af behandling af personoplysninger om fri udveks-ling af sådanne oplysninger § 41, stk. 1, nr. 1, jf. stk. 3 jf. stk. 6.

Thi kendes for ret:

Favrskov kommune skal betale en bøde på 75.000 kr.

Tiltalte skal betale sagens omkostninger.

Dommer