RETTEN I HELSINGØR

D O M

afsagt den 12. september 2022

Rettens nr. 1-2152/2021
Politiets nr. 0900-84266-00006-20

Anklagemyndigheden
mod
Tiltalte Kommune
CVR nr.

Anklageskrift er modtaget den 10. juni 2021.

Tiltalte Kommune er tiltalt for overtrædelse af

databeskyttelsesforordningens artikel 32, stk. 1, jf. databeskyttelseslo-vens § 41, stk. 1, nr. 1, jf. stk. 3, jf. stk. 6, jf. databeskyttelsesforordnin-gens artikel 83, stk. 2 og stk. 4, litra a, jf. stk. 9,
ved i perioden fra forud for den 10. september 2019 og indtil i hvert fald den 21. oktober 2019, ikke at have overholdt sin forpligtigelse som dataansvarlig til at gennemføre tekniske og organisatoriske foranstaltninger, der passede til risiciene af varierende sandsynlighed og alvor for de registreredes rettigheder, idet Tiltalte Kommune ikke havde sørget for at kryptere kommunens computere, hvilket medførte et utilstrækkeligt sikkerhedsniveau og tillige havde den konsekvens, at et sikkerhedsbrud der bestod i at en medarbejder fra Tiltalte Kommune den 21. oktober 2019 fik stjålet en arbejdscomputer fra sin bil medførte en unødig høj risiko for de registrerede, i det der på computeren lå oplysninger om ca. 1600 medarbejdere i Tiltalte Kommune, herunder oplysninger af følsom karakter og oplysning om personnumre.

Påstande

Anklagemyndigheden har nedlagt påstand om bødestraf.

Tiltalte Kommune har nægtet sig skyldig.

Sagens oplysninger

Der er under sagen afgivet forklaring af Vidne 1, Vidne 2, Vidne 3, Vidne 4 og Vidne 5.

Vidne 1 har forklaret, at hun ikke længere er ansat i Tiltalte Kommune. Hun var fra december 2017 til marts i år ansat i kommunen som udviklingskonsulent og programleder i forhold til GDPR. Hun var ikke in-

volveret i den konkrete sag, idet det ikke havde noget med programledelse at gøre. Hun er ikke bekendt med, hvad der var det IT-tekniske problem i forbindelse med hændelsen. Hun er ikke bekendt med, hvad kommunen gjorde efter hændelsen for fremtidigt at imødegå sikkerhedsrisici. Hun var ikke inde over kryptering af kommunens computere og ved ikke, om kommunen foretog nogen form for kryptering. Hun antager, at kommunens IT-afdeling er bekendt hermed, for IT-sikkerheden blev varetaget af IT-afdelingen. Vidne 4 var en af medarbejderne i IT-afdelingen, som vidnet talte med, og det er muligt, at Vidne 4 vil kunne fortælle mere. Det er hendes ind-tryk, at kommunen havde en Citrix-løsning, og at denne løsning fungerede fint. Hun ved dog, at der havde været udfordringer med Citrix, inden hun blev ansat. Hun ved også, at kommunen overgik til et andet system. Hun er uddannet Cand.scient.pol., og hendes arbejdsopgaver i forhold til GDPR lovgivningen bestod i at opdatere kommunens persondatapolitik. De havde i den forbindelse besøg af Kammeradvokaten, og der blev foretaget Gap-ana-lyser af alle kommunens opgaveområder. Man startede med at lave en grun-dig gennemgang af kommunens skole-og fritidsområde, og modellen blev efterfølgende anvendt på kommunens øvrige områder.

Vidne 2 har forklaret, at han siden årsskiftet 2019/2020 har været ansat som Tiltalte Kommunes IT-centerchef. Forinden havde han i en periode været kommunens centerchef for Kultur og Fritid. Han blev først bekendt med hændelsen fra oktober 2019, da han tiltrådte sin nye stil-ling. Som alle øvrige ansatte i kommunen deltog han i et kursus om databes-kyttelse og modtog skriftlige vejledninger herom, og han er godt klar over, at man skal være særlig opmærksom på håndteringen af personfølsomme oplysninger. Han er ikke teknikker og kan ikke give en teknisk begrundelse for, hvorledes bruddet på persondatasikkerheden kunne ske. Han har dog læst, at der blev gemt en OST-fil på computeren. Han ved ikke, hvad der lig-ger på en sådan fil. Kommunens IT-teknikker på tidspunktet for hændelsen er ikke længere ansat i kommunen, og vedkommende bor i udlandet. Han er ikke klar over, hvad der var kommunens umiddelbare reaktion på hændels-en, og hvornår de berørte ansatte blev orienteret om hændelsen. Han mener, at han selv fik et brev i e-boks om sikkerhedsbruddet. Han ved, at kommu-nen havde udfordringer med Citrix-løsningen på tidspunktet for hændelsen. De ansatte oplevede systemnedbrud, og at de ikke hjemmefra kunne arbejde i de systemer, som de sædvanligvis arbejdede i. Kommunen forsøgte uden held at få IT-leverandøren til at udbedre forholdene, og det betød, at nøgle-medarbejdere måtte løse deres arbejdsopgaver udenom Citrix. Det var dog ikke kutymen, at kommunens medarbejdere arbejdede uden for Citrix. Da han tiltrådte fik han også en teknisk beskrivelse af, hvori problemerne be-stod, men hans viden på området var ikke særlig stor, og han har nok ikke forstået det. Han deltog ikke i beslutningsprocessen om, hvilken model kommunen skulle vælge til afløsning af VDI-løsning, men efter sin tiltræden blev han en del af arbejdet med at implementere den valgte model. Direktio-nen traf beslutning om, at kommunen skulle lease computere, og at ATEA skulle stå for den tekniske support. Kommunen lavede dens egen sikker-

hedsmodel med dobbelt-faktor login og mulighed for at fjernslette alt fra devices, som bortkom.

Vidne 3 har forklaret, at han er ansat som dataarkitekt i Datatilsy-net, og at han i oktober 2019 havde titel af IT-sikkerhedskonsulent samme sted. Han har en kandidat fra DTU i softwareteknologi og en Ph.d. i krypto-logi. Han blev først bekendt med sagen fra Tiltalte Kommune, da han blev indkaldt som vidne, og har derfor ikke behandlet sagen i Datatilsynet. Problemstillingen er, at data på en computers harddisk kan flyttes til en an-den computer og være tilgængelig for enhver uden login. I efteråret 2019 havde det længe været praksis, at man i det offentlige skulle tage stilling til, om harddiske skulle krypteres. Vejledningen til sikkerhedsbekendtgørelsen, der beskriver dette, stammer fra 2000 og "lå ved siden af" persondataloven. Når sikkerhedsvejledningen fra 2018 indeholder eksempler på sikkerheds-foranstaltninger, som man kan bruge til at sikre overholdelse af databeskyt-telsesforordningen, herunder kryptering af personoplysninger, er der tale om en opfordring til den dataansvarlige om at overveje de nævnte foranstaltnin-ger. Man kan ikke som arbejdsgiver regne med, at de ansatte i tilstrækkelig grad beskytter persondataoplysninger, og arbejdsgiveren er derfor nødt til at have nogle procedurer til at holde styr på det, særligt ved de ansattes brug af mobile devices. Efter hans opfattelse bør kommunen sikre, at harddiske krypteres uanset om man arbejder i Citrix eller ej. Det behøver ikke være be-kosteligt at implementere. Hvis kommunen ikke benytter sig af Mobile De-vice Management, MDM, er det til gengæld både besværligt og bekosteligt at overholde forpligtelsen som dataansvarlig. Han kan ikke umiddelbart og uden nærmere kendskab til omstændighederne forholde til den beslutning, som Tiltalte Kommunes direktion traf den 10. september 2019. Det sam-me gælder den omtalte Model 4 og det hidtidige sikkerhedsniveau i kommu-nen. For en kommunes vedkommende ville det give mening at have MDM, og at computere krypteres i overensstemmelse med sikkerhedsvejledningen. Det var efter hans opfattelse common knowledge for IT-kyndige i efteråret 2019.

Foreholdt uddrag af Retten i Aarhus' dom af 12. februar 2021 har vidnet forklaret, at den rollefordeling, som han og Person beskrev under vidneafhøringerne, gjaldt i forhold til tilsynsbesøg.

Vidnet har endvidere forklaret, at kryptering er én af de løsninger, som en kommune kan vælge, men det er ikke den eneste måde at sikre datasikkerheden på. Når der er tale om mobile devices, ser han imidlertid ikke andre muligheder end kryptering, hvis man vil sikre sig mod datalæk i forbindelse med bortkomst/tyveri. Han vil vurdere, at kryptering er en passende foran-staltning. I et af forsvareren beskrevet tilfælde med en p-vagt, der har en bærbar computer, som alene indeholder oplysninger om de enkelte vejes sta-tus som privat eller offentlig vej, og som ikke tages med hjem og derfor er "skalsikret" på arbejdspladsen, kan han ikke sige, at man skal kryptere computeren. I et af anklageren beskrevet tilfælde med en HR-medarbejder, der

anvender sin computer til hjemmearbejde, vurderer han, at det fornuftige vil være, at computeren er krypteret.

Vidne 4 har forklaret, at hun har været ansat i Tiltalte Kommune i knap 22 år, og at hun de seneste 4-5 år har haft stilling som kommunens informationssikkerhedskoordinater. Det er hendes opgave at sikre sikkerheden og awareness hos medarbejderne i forhold til ISO 27001, som kommunen ikke er certificeret i men skal efterleve principperne i. Hun er oprindelig uddannet edb-assistent og har læst videre som datanom og gen-nem hele sin ansættelse i kommunen taget forskellige kurser. Da tyveriet fandt sted i oktober 2019, var kommunens medarbejder-pc'ere ikke kryptere-de. Hun er ikke teknikker men tænker, at baggrunden herfor var, at Citrix, som de anvendte på det tidspunkt, indebar, at der ikke lå noget på medarbej-dernes pc'ere. Alt lå på en central server, som medarbejderne tilgik med der-es password. Citrix-løsningen havde også den fordel, at de kunne genbruge kommunens gamle pc'ere. Til gengæld var der problemer med tilgængelig-heden, for systemet gik tit ned. Hun husker ikke, hvor længe det stod på. Hun kan huske, at de på et tidspunkt skiftede over til ATEAs Citrix-løsning. Det kan godt være, at det var i 2018. Som følge af problemerne, fik enkelte medarbejdere lov til at installere Outlook på deres pc. Hun er ikke klar over, hvor mange medarbejdere, det drejede sig om, og hvor mange af dem, som arbejdede i HR-afdelingen, men medarbejderen, der fik stjålet sin pc'er, var en af dem.

Hun ved ikke, om de overvejede at kryptere disse medarbejderes pc'ere. Det var noget, som support og deres teknikafdeling var inde over. Hun var ikke involveret i at installere Outlook på pc'er og ved ikke, om det indebar en yderligere sikkerhedsrisiko at medarbejdere arbejdede lokalt på deres pc. Det var først efter tyveriet, at kommunens teknikere fik at vide, at der blev lagret en fil på pc'ens harddisk, hvis man havde fået installeret Outlook på sin pc, og at filen på harddisken på HR-medarbejderens pc indeholdt person-følsomme oplysninger. De havde instrueret medarbejderne om ikke at have noget liggende på deres pc's skrivebord, og at der ikke måtte ligge personføl-somme oplysninger i Outlook. De personfølsomme oplysninger lå i en sendt post i Outlook på den stjålne pc'er. Inden tyveriet var der truffet en beslut-ning om, at kommunens medarbejdere skulle have en ny type pc'ere, hvor harddisken ville være krypteret, og hvor medarbejderne kun kunne installere programmer, som IT-afdelingen lagde op i en portal. Hun er ikke bekendt med oplægget til direktionen, der mundede ud i en beslutning af 10. septem-ber 2019 om valg af den nye IT-løsning, men hun var klar over, at man ønskede en ny løsning, der var sikrere, og at det indebar, at alle medarbejde-re skulle have nye pc'ere. Det var hendes opfattelse, at kommunen tog hånd om de problemer, der var med den gamle maskinpark.

Vidne 5 har forklaret, at han er ansat i Datatilsynet som IT-sikkerheds-specialist og jurist. Han har beskæftiget sig med IT-sikkerhed siden de tidli-ge 80'ere, hvor han hackede sin først computer. Han har indgående indsigt i

de krav, der stilles på det IT-tekniske og GDPR-området. Han har ikke været involveret i den konkrete sag med ved, at den har været behandlet i Datatil-synet. Såvel persondataloven, der gjaldt før 2018, som GDPR indeholder nogle afvejningshensyn til hvad der efter de gamle regler er "fornøden sik-kerhed" og efter de nye regler "passende sikkerhed", og i den sammenhæng går man ind og vurderer, hvad der er risikoen for de registreredes rettigheder og vejer det på over for de sikkerhedsforanstaltninger, der vil være passende. De sikkerhedsforanstaltninger der kan og må være passende, er det, der er normalt inden for det pågældende behandlingsområde og det, man kan gøre på en god og ordentlig måde set i forhold til de risici, der nu engang er. Der er ikke nogen facitliste og ingen ultimative krav. Allerede i 2007 blev det knæsat, at kryptering af harddisken var en god måde at beskytte de oplysnin-ger, der var på harddisken så som personoplysninger og forretningshemme-ligheder. På daværende tidspunkt var der desuden indbygget et krypterings-redskab i de styresystemer, man købte, uanset om det var til en Mac compu-ter eller en pc, hvor styresystemet typisk var fra Microsoft. Så når man hav-de installeret det pågældende styresystem, var det gratis at bruge krypte-ringsredskabet. Mac computere fik den første krypteringsmulighed med Fi-rewall i 2003, og for Microsoft styresystemer fik man Vista i 2007, og hvis man benyttede de pågældende styresystemer, var det noget, man blot kunne slå til. Som dataansvarlig eller virksomhedsejer kunne man derved tvinge dem, der loggede sig på ens netværk, til at have krypteringen slået til på der-es maskiner, så man kunne beskytte de data, der lå på harddisken.

Som udgangspunkt ville kryptering allerede før 2019 have været en passen-de sikkerhedsforanstaltning i overensstemmelse med forordningen, hvis man behandlede personoplysninger på et lokalt drev, for computere bliver stjålet, uanset hvor de befinder sig, og sandsynligheden for, at noget kunne gå galt, var det højere, hvis man tog computeren med ud. Det var en kendt og hyp-pigt forekommende risiko, og da man nemt kunne imødegå det ved at kryp-tere computeren, var det den måde, man skulle gøre det på. Det har været kendt viden siden 2007 og en fast praksis i de organisationer, han været en del af, fra ca. det tidspunkt måske lidt senere. ISO 27001 er en styrings stan-dard, hvor man får lagt et regime ned over sin virksomhed, så man kunne styre processerne. Staten var forpligtet til at efterleve standarden, men kom-munerne og regionerne skulle følge principperne. Kryptering er nævnt i standarden og i flere af udvidelserne til standarden, ligesom kryptering jo er nævnt flere gange i forordningen som et af de gode redskaber til at sikre sit udstyr. Det er korrekt, at man kan benytte sig af både tekniske og organisato-riske foranstaltninger. Man starter sædvanligvis med at identificere risikos-cenarierne. Hvis et af dem er, at man behandler oplysninger på computerens harddisk, kan man teknisk forhindre, at det kan lade sig gøre. En organisato-risk foranstaltning kunne være at fortælle medarbejderne, at de ikke må bru-ge harddisken. Det er dog et almen kendt fænomen, at nogen alligevel gør det, for eksempel fordi det er nemt og de har travlt, og derfor kan det være godt og nødvendigt at have et ekstra lag af sikkerhed på i form af kryptering.

Forholdsordre om, at medarbejdere, der fik lov til at arbejde udenom Citrix-løsningen, skulle slette personfølsomme oplysninger, når de var færdige, er i og for sig udmærkede, men de løser ikke problemet i forhold til de situatio-ner, hvor folk alligevel glemmer at gøre det. Det er en kendt problemstilling, og så har man et effektivt redskab til at opnå sikkerheden, som er indbygget i de typisk anvendte styresystemer. I den situation, hvor man har ladet me-darbejdere arbejde på en lokal computer, har man omgået de sikkerhedsme-kanismer, der var i Citrix-løsningen, og så er man nødt til at forholde sig til misbrugsscenarierne, herunder at computeren bliver stjålet. Hvis man bruger Outlook stationært eller Outlook 385, så gemmer det det i en ost-fil eller en pst-fil, så man ikke skal vente på, at den henter det hele en gang til, når man starter maskinen op. Hvis harddisken ikke er krypteret, vil ost-filen eller pst-filen ligge i et læsbart format på harddisken. Det er hans klare opfattelse, at det burde en IT-afdeling i 2019 have viden om allerede inden, man tog det pågældende redskab i brug. Man burde da have overvejet de forskellige risi-koscenarier, særligt når man afviger fra sine normale mønstre. I det omfang man tillader medarbejdere at tage deres maskiner med hjem, vil det ikke væ-re i overensstemmelse med principperne om passende sikkerhed, hvis man ikke krypterer harddisken, når der ligger persondata på harddisken. Det gæl-der uanset om det er en midlertidig løsning eller noget, man gør fast.

Det nemmest ville have været, hvis IT-afdelingen havde slået krypterings-redskabet, som findes i styresystemet, til og tvunget det ned over maskiner-ne. For Microsofts vedkommende hedder det BitLocker. Det tidligere styre-system XP var usikkert og blev ikke længere sikkerhedsopdateret efter 2014, og så krævede det endnu flere sikkerhedsforanstaltninger at anvende det. Databeskyttelsesforordningen giver nogle gode retningslinjer for, hvilke re-aktioner der er passende, og Datatilsynet politianmelder kun i de sager, hvor en dataansvarlig har forset sig og burde have vidst bedre, og hvor man er ude i en grovere overtrædelse eller hvor man indlysende har negligeret nogle standarder i branchen eller i hvert faldt ikke fulgt med tiden eller i øvrigt gjort noget, der er himmelråbende forkert. Forseelsen skal være kvalificeret forkert, og det kan for eksempel være, at man ikke grundig nok har vurderet de risikoscenarier, man kunne blive udsat for, og implementeret de sikker-hedsforanstaltninger, som er kendte på det tidspunkt og i øvrigt er nemme at indbygge i sit system eller i sin måde at behandle persondata på. Både data-beskyttelsesforordningens almindelige regler og dansk rets almindelige reg-ler om proportionalitet gør, at Datatilsynet i alle sager overvejer, hvad der er den rette sanktion. Datatilsynet har set et langt større misbrugsmønster, hvor de kriminelle også går efter personernes data, og hele ransomware-bølgen er udtryk for, at man ikke kun lukker computeren ned for at få penge ud af dem, man har angrebet, men tillige ekstraherer personoplysninger for at læg-ge et dobbelt pres på den dataansvarlige eller tillige lægge pres på de enkelte registrerede ved at lække personoplysningerne eller misbruge kreditkortop-lysninger.

Der findes mange metoder til at få adgang til andres personoplysninger, og

den nemmeste og mest banale er at pille harddisk ud af enheden. Offentlige myndigheder og større finansielle institution er typisk i besiddelse af personoplysninger, som den registrerede ikke kan undgå bliver behandlet, og i forhold til sådanne institutioner har vi som borgere en forventning om, at de må være rigtig gode til at håndtere oplysningerne. Det har i flere sager været noget, som Datatilsynet har lagt vægt på ved vurderingen af forholdets grov-hed. Det gør ikke nogen forskel, at der i den foreliggende sag var tale om de ansatte personoplysninger. Ansættelsesretlige optegnelser kan ofte være me-re indgribende end det at have en banal skattesag hos det lokale skattecenter, da der kan være oplysninger om ens helbredsmæssige tilstand, advarselssituationer og fagforeningensforhold. Ved mange typer af identitetsmisbrug er det ofte således, at den ondsindede starter med at få nogle grundoplysninger om en person, for eksempel navn og bopæl. På baggrund af det kan de bygge en troværdig historie op. Da vores samfund tillægger cpr-nummeret meget stor vægt, skaber det en troværdig historie om en person, hvis man også kan cpr-nummeret, og foruden identitetsmisbrug kan det bruges til at få et angrebspunkt i forhold til andre ting vedrørende personen. Der er sager, hvor cpr-nummeret isoleret set har ført til misbrug, og der findes også trykte afgø-relser, herunder den såkaldte Brobizz-sag, hvor cpr-nummeret blev brugt til at indsamle oplysninger om ekskæresters kørselsmønster.

Det er underordnet, at der ikke er eksempler på, at der er sket misbrug af de 1.600 medarbejderes cpr-nummer, for det er den potentielle risiko, der er forbundet med bruddet på datasikkerheden, der er afgørende. Dertil kom-mer, at vi jo ikke ved, om den person, der har stjålet computeren, har gjort noget i forhold til personoplysningerne. Det, som databeskyttelsesforordnin-gen fokuserer på, er det mulige misbrug. Det er det, som sikkerhedsforanstaltningerne i artikel 32 skal fastsættes efter. Han skal ikke second guesse på det, som PwC er kommet frem til i deres revision af kommunens generel-le IT-kontroller vedrørende regnskabsaflæggelsen for 2019. Uanset, at kom-munens computere var mere end 4 år gamle og havde Windows 7 som styre-system, så var XP den sidste version, der ikke understøttede BitLocker. Den næste version hed Windows Vista, der kom i 2007, og Vista var forgænge-ren til Windows 7. Windows 7 var født med BitLocker. Det var sådan, at hvis man brugte fjerncomputere til at logge på et fælles netværk som Tiltalte Kommunes, så var det muligt at presse såkaldte MSI pakker ud og lægge dem ind på maskinen som led i log-on skridtet, så selv hvis man ikke havde installeret det på det tidspunkt, var der i Microsofts serverstyresystem muligheder for at gøre det. Vel og mærke helt tilbage siden XP, dvs. fra før 2003. Vidne 3 er en dygtig tekniker, især indenfor kryptologi. Han mener ikke, at det er rigtigt, når Vidne 3 i retsmødet den 22. august 2022 er citeret for at sige, at det både er besværligt og bekosteligt at overhol-de forpligtelsen som dataansvarlig, hvis man ikke benytter sig af MDM. Det krævede selvfølgelig, at maskinerne var på kommunens netværk, og det an-tager han, for det er og var det normale.

Når det i vejledningen fra 2001 om hjemmearbejdspladser og senere vejled-

ninger blot anbefales, at man krypterer, når man laver lokallagring, skyldes det, at alle Datatilsynets vejledninger afspejler de situationer, der nu engang er i forhold til artikel 32, og man kunne have valgt noget andet end krypte-ring, for eksempel at fjerne skriveadgangen for de pågældende medarbejder-ne. Udgangspunktet er, at der er en bred mulighed for at løse problemstillin-gerne, men at kryptering er den nærmest foreliggende. Det er et brugsscena-rie, der er beskrevet i vejledningerne, for der er, som tidligere nævnt, ikke en facitliste til artikel 32 andet end at sikkerheden skal være passende i forhold til de risici og med de afvejninger, som artikel 32 opremser. Der ville være andre måder at opfylde kravet om passende sikkerhedsforanstaltninger end kryptering, for man kunne forhindre, at medarbejderne kunne skrive til hard-disken eller slet ikke havde en harddisk i deres maskine. I forhold til forkla-ringen fra Vidne 3 om de to tilfælde skitseret af henholdsvis for-svareren og anklageren, så har Datatilsynet jo ikke nogen mening om situati-oner, hvor der ikke er involveret personoplysninger, og han er derfor enig i Vidne 3's vurdering vedrørende situationen med p-vagten. Han er også enig i Vidne 3's vurdering i den anden situation. Det vil i den situation endda være særdeles fornuftigt at kryptere computeren, og han me-ner, at det er den eneste løsning, der er brugbar rent praktisk. Datatilsynet inddrager også formildende omstændigheder i vurderingen. Det er klart også noget, de kigger på. Han er ikke bekendt med, hvilke formildende omstæn-digheder der eventuelt er lagt vægt på i denne sag. Uddraget på side 483 i betænkningen om Databeskyttelsesforordningen under afsnittet om behand-lingssikkerhed gengiver blot ordlyden af artikel 32.

Det væsentlige - også i betænkningen - at fokusere på, er, at hvis ens system er af ældre dato og derfor af en eller anden grund ikke kan bibringes til-strækkelig sikkerhed, skal de organisatoriske sikkerhedsforanstaltninger væ-re tilstrækkelige. Man kan altså ikke i et sådan tilfælde operere me d en mindre grad af sikkerhed. Hvis en kommune får at vide af sin IT-rådgiver, at det ikke kan lade sig gøre at presse krypteringspakker ned over maskinerne eller at det er forbundet med byrdefulde omkostninger, kan det sagtens være forsvarligt at udskifte maskinparken. Man kan blot ikke vente uendelig. Og i den mellemliggende periode, hvor man som Tiltalte Kommune giver medarbejdere lov til at arbejde uden om Citrix, må man lave en fornyet sik-kerhedsvurdering. Enhver ændring bør få den sikkerhedsansvarlige til at vurdere, om sikkerhedsforanstaltningerne til fulde slår til i den nye behand-lingssituation. Den sikkerhedsansvarlige må hele tiden revurdere risikobille-det i forhold til de behandlinger, som den dataansvarlige foretager. I forhold til det anførte i uddraget på side 484 i betænkningen under afsnit 5.10.4 Overvejelser er det væsentlige at holde fast i, at sikkerhed på IT-området er en dynamisk størrelse, og at artikel 32 skal fortolkes i den tid, man er i. Det er netop grunden til, at forordningen er lavet med den bredde, den nu engang har. Der er ikke hjemmel i hverken databeskyttelsesloven eller i forordnin-gen til at lave noget der minder om bekendtgørelser eller lignende.

Der er blevet dokumenteret fra Datatilsynets politianmeldelse af 10. marts

2020 (bilag 2), eksempel på orienteringsbrev til medarbejderne ved Tiltalte Kommune (bilag 2-3), Tiltalte Kommunes svar af 12. november 2019 til Datatilsynet (bilag 2-5), afhøringsrapport af 15. december 2020 (bilag 2-6), udateret indstilling til Tiltalte Kommunes direktion med di-rektionens beslutning af 10. september 2019 vedrørende kommunens fremti-dige IT-løsning (bilag 3-2), PwCs revisionsrapport af 20. marts 2020 (bilag 3-5) samt Tiltalte Kommunes udaterede medarbejderguide om IT-sikker-hed (bilag 3-9).

Rettens begrundelse og afgørelse

Tyveriet den 21. oktober 2019 af en arbejdscomputer tilhørende en medarbejder fra Tiltalte Kommunes HR-afdeling indebar et brud på persondatasikkerheden, idet der på computeren lå personoplysninger om ca. 1.600 medarbejdere ved kommunen, herunder oplysninger af følsom karakter og oplysning om personnumre. Den stjålne computers harddisk var ikke krypteret, og selvom kommunen havde retningslinjer for, at personoplysninger af føl-som karakter ikke måtte ligge på kommunens computere, og en række øvri-ge organisatoriske sikkerhedsforanstaltninger, finder retten, at kommunen ikke havde gennemført passende tekniske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der var for de registreredes rettigheder. Retten lægger i den forbindelse 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 kan borttage arbejdscomputere fra arbejdspladsen.

Efter en samlet vurdering af sagen, herunder at kommunen forud for sikkerhedsbruddet selv havde vurderet, at kryptering af kommunens harddiske var en nødvendig foranstaltning, finder retten, at der er tale om en alvorlig overtrædelse af databeskyttelsesforordningens artikel 32, og at overtrædelsen som indstillet af Datatilsynet skal sanktioneres med en bøde, der beregnes på baggrund af Tiltalte Kommunes seneste offentliggjorte foregående driftsbevilling forud for endelig dom. Bøden fastsættes derfor til 50.000 kr., jf. 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.

Thi kendes for ret:

Tiltalte Kommune, skal betale en bøde på 50.000 kr.

Tiltalte Kommune skal betale sagens omkostninger.

Dommer

/