Personvernnemnda

PVN-2022-13 Brudd på personopplysnings- og informasjonssikkerheten i Østre Toten kommune - overtredelsesgebyr

Personvernnemndas vedtak 24. januar 2023 (Mari Bø Haugstad, Bjørnar Borvik, Hans Marius Graasvold, Heidi Talsethagen, Hans Marius Tessem, Morten Goodwin, Malin Tønseth)

Datatilsynets referanse: 21/00481-14

Saken gjelder klage fra Østre Toten kommune på Datatilsynets vedtak 7. januar 2022 der kommunen ble ilagt et overtredelsesgebyr på 4 000 000 kroner for brudd på kravene til sikkerhet og internkontroll ved behandling av personopplysninger, jf. personvernforordningen artikkel 32 og artikkel 24.

Sakens bakgrunn

Østre Toten kommune oppdaget natt til 9. januar 2021 at de var utsatt for et omfattende løsepengevirusangrep på sine IT-systemer. Angrepet ble oppdaget da kommunens ansatte ikke lenger hadde tilgang til kommunens IT-systemer.

En trusselaktør hadde skaffet seg urettmessig tilgang til kommunens IT-systemer. Hele den kommunale tjenesteleveransen, med få unntak, ble rammet i angrepet. Som en del av angrepet ble kommunens data kryptert og gjort utilgjengelig for kommunens ansatte og innbyggere. Det samme gjaldt sikkerhetskopiene. Trusselaktøren, som satt på krypteringsnøkkelen, etterlot seg løsepengebrev på flere lokasjoner i systemet. Trusselaktøren har mest sannsynlig hatt administratortilgang til alle datamaskiner hos kommunen.

Personopplysninger om kommunes innbyggere ble stjålet under angrepet. Betydelig mengder data, inkludert e-poster og ca. 30 000 dokumenter kom på avveier. Dette inkluderer opplysninger om barn og særlige kategorier av opplysninger omfattet av artikkel 9 nr. 1, herunder pasientjournalopplysninger. Et ukjent antall dokumenter ble publisert på det mørke nettet. Det mørke nettet er en del av Internett hvor informasjon gjøres tilgjengelig for alle, samtidig som det ikke er mulig å spore verken hvem som legger ut, eller laster ned, informasjonen.

Angrepet medførte at kommunens ansatte og innbyggere ikke lenger hadde tilgang til de fleste av kommunens IT-systemer. Av NSMs rapport «Nasjonalt digitalt risikobilde 2021» framkommer blant annet at barn og unges journaler på helsestasjonen var utilgjengelige, og at dataangrepet førte til at kommunen manglet fungerende IT-systemer i flere måneder. Manuelle systemer måtte etableres, blant annet ble alarmsystem på sykehjem erstattet med bjeller, og låsesystemet på kommunens bygninger fungerte ikke.

Kommunedirektøren varslet Datatilsynet 11. januar 2021 og sendte avviksmelding 13. januar 2021, samt et tillegg til avviksmeldingen 31. mars 2021. Kommunen hadde tett kontakt med sikkerhetsmyndighetene og politiet, og ga tilsynet statusoppdateringer underveis i etterforskningsarbeidet. Både IT-selskapet Atea IRT og revisjons- og rådgivningsselskapet KPMG ble engasjert i arbeidet med å håndtere hendelsen.

På Datatilsynets anmodning redegjorde kommunen for avviket 2. juni 2021.

Datatilsynet varslet Østre Toten kommune 18. oktober 2021 om at tilsynet ville treffe slikt vedtak:

> «I medhold av personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26 og pasientjournalloven § 29, ilegges Østre Toten kommune et overtredelsesgebyr på 4 000 000 NOK – fire millioner norske kroner – til statskassen, for overtredelse av kravene til sikkerhet og internkontroll ved behandling av personopplysninger, jf. personvernforordningen artikkel 32 og artikkel 24, jf. personopplysningsloven § 26 første ledd. Kommunen har blant annet manglet tofaktorautentisering ved pålogging, tilstrekkelig sikrede backup-systemer og logging av viktige hendelser i sitt nettverk.
>
> Østre Toten kommune pålegges å etablere og dokumentere at et egnet styringssystem for informasjonssikkerhet og personopplysningssikkerhet er implementert, jf. personvernforordningen artikkel 58 nr. 2 bokstav d. Som ledd i dette arbeidet pålegges kommunen å gjennomføre risiko- og sårbarhetsanalyser for alle sentrale systemer/løsninger i infrastrukturen, med det formål å identifisere behovet for risikoreduserende tiltak. Analysene skal dokumenteres i styringssystemet.»

Kommunen ga sine merknader til varselet 8. november 2021.

Datatilsynet traff 7. januar 2022 vedtak om overtredelsesgebyr og pålegg i tråd med utsendt varsel.

Kommunen klaget rettidig på Datatilsynets vedtak 26. januar 2022. Klagen gjaldt bare overtredelsesgebyret og ikke pålegget om å etablere og dokumentere et egnet styringssystem for informasjonssikkerhet og personopplysningssikkerhet. Datatilsynet vurderte klagen, men fant ikke grunn til å endre sitt vedtak. Datatilsynet oversendte saken til Personvernnemnda 22. juni 2022. I brev fra nemnda 27. juni 2022 fikk kommunen anledning til å komme med kommentarer. Kommunen har ikke inngitt kommentarer.

Saken ble behandlet i nemndas møter 8. november 2022, 13. desember 2022 og 24. januar 2023. Personvernnemnda hadde følgende sammensetning: Mari Bø Haugstad (leder), Bjørnar Borvik (nestleder), Hans Marius Graasvold, Heidi Talsethagen, Hans Marius Tessem, Morten Goodwin og Malin Tønseth. Sekretariatsleder Anette Klem Funderud var også til stede.

Datatilsynets vedtak i korte trekk

Datatilsynet gir innledningsvis en beskrivelse av sikkerhetsbruddet og etterfølgende tiltak, samt grunnprinsippene for behandling av personopplysninger og kravene til personopplysningssikkerhet og styringssystemer i personvernforordningen. Tilsynet redegjør også for sin myndighet til å ilegge overtredelsesgebyr, før de redegjør for sin vurdering

knyttet til overtredelsesgebyret og av om pålegg skal gis. I det følgende gjengis bare Datatilsynets vurdering knyttet til overtredelsesgebyret, som er det som er påklaget.

Vurdering av sikkerhetsbruddet

Datatilsynet påpeker store mangler ved kommunens personopplysningssikkerhet. Manglene knytter seg både til logg og logganalyse, sikring av backup og manglende tofaktorautentisering eller tilsvarende sikkerhetstiltak. Dette viser en svakhet både i kommunens evne til å identifisere hackerangrep og mangelfull informasjonssikkerhet i systemet og utgjør i seg selv brudd på kravene til personopplysningssikkerhet i personvernforordningen artikkel 32, jf. artikkel 24.

Angrepet er særlig alvorlig fordi det har rammet en betydelig del av kommunens data. Personopplysninger om kommunens innbyggere og ansatte er fullstendig tapt gjennom det aktuelle dataangrepet og opplysninger er delt på det mørke nettet i ukjent omfang.

At backupsystemer var slettet, var en vesentlig negativ faktor i arbeidet med å gjenopprette drift (tilgjengelighet) av systemene som var rammet. At kommunen ikke beskyttet sine sikkerhetskopier mot tilsiktet og utilsiktet sletting, manipulering og avlesning, var en betydelig mangel ved kommunens styringssystem for informasjons- og personopplysningssikkerhet.

Både konfigurasjonen av brannmurer (mangelfull logging) og nettverkstopografien (mangelfull segmentering av nettverket) representerer grunnleggende svakheter i kommunens informasjonssikkerhet som medfører brudd på personvernforordningen artikkel 32, jf. artikkel 24. Som en følge av mangelfulle informasjonssikkerhetstiltak, sammenholdt med ledelsens og ansattes manglende bevissthet rundt mulige sikkerhetstrusler og dataangrep, har kommunen brutt det grunnleggende prinsippet om plikten til å ivareta opplysningers konfidensialitet og integritet, jf. personvernforordningen artikkel 5 nr. 1 bokstav f.

Vurdering av om overtredelsesgebyr skal ilegges

Datatilsynet går gjennom de momentene tilsynet anser som relevante for vurderingen av om overtredelsesgebyr skal ilegges og konkluderer med at Østre Toten kommune skal ilegges et overtredelsesgebyr for overtredelsen av personvernforordningen artikkel 32, jf. 24, og artikkel 5 nr. 1 bokstav f.

Tilsynet ser alvorlig på avviket ettersom kontrollen over betydelige mengder data i kommunen er tapt. Dette omfatter særlige kategorier av personopplysninger og opplysninger om barn, som etter personvernregelverket har et spesielt vern. Personopplysninger er delt på det mørke nettet, noe som gjør det umulig å overskue konsekvensene av avviket.

Datatilsynet konkluderer med at kommunen har hatt grunnleggende mangler ved personopplysnings- og informasjonssikkerheten og internkontrollarbeidet.

Utmåling av gebyret

I vurderingen av gebyrets størrelse, har tilsynet sett hen til at årsaken til at dataangrepet kunne skje skyldtes grunnleggende mangler ved kommunens personopplysnings- og informasjonssikkerhetssystem. Kommunen hadde ikke etablert eller gjennomført internkontroll på en måte som var egnet til å fange opp disse sikkerhetshullene. Dette vurderer tilsynet som svært alvorlig.

Dataangrepet har medført at en betydelig del av kommunens data er kompromittert og tapt for framtiden. Angrepet har videre medført spredning av til dels svært beskyttelsesverdige personopplysninger på det mørke nettet. Dette kan være alvorlig for den enkelte registrerte, men har også omfattende konsekvenser for kommunens løpende drift. Dette er ansett som skjerpende momenter.

Saken illustrerer hvor alvorlige konsekvenser et dataangrep kan få og hvor viktig det derfor er å ha robust infrastruktur og tilstrekkelig beskyttelse mot angrep utenfra. Ifølge opplysninger i media har dataangrepet hittil kostet kommunen over 32 millioner kroner. Tilsynet er klar over at det er en enorm økonomisk belastning for en kommune med knapt 15 000 innbyggere. Kommunens økonomiske situasjon er et moment som har betydning ved utmåling av gebyret, jf. personvernforordningen artikkel 83 nr. 2 bokstav k og er hensyntatt i tilsynets vurdering. Det samme er det forhold at kommunen selv meldte avviket til Datatilsynet og at kommunen har vært svært samarbeidsvillig i etterkant. Det er også hensyntatt at kommunen har gjort sitt ytterste for å gi god informasjon til innbyggerne.

Datatilsynet har kommet til at et overtredelsesgebyr på 4 000 000 kroner er rimelig i denne saken. Etter tilsynets vurdering gjenspeiler beløpet både lovbruddets alvor, kommunens økonomiske situasjon etter angrepet og kommunens omfattende arbeid i etterkant. Uten disse forholdene ville gebyret blitt satt vesentlig høyere.

Om skyldkravet - uaktsomhet

Datatilsynet skriver i oversendelsesbrevet for klagen til Personvernnemnda at begrunnelsen for skyldkravet kunne vært bedre i vedtaket. I oversendelsesbrevet utdypes derfor dette punktet og hovedtrekkene gjengis her:

Det er klart overveiende sannsynlig at kommunedirektøren, som øverste representant for kommunens ledelse, har opptrådt uaktsomt. Etterlevelse av kravene i personvernregelverket er til enhver tid øverste leders ansvar. Kommunedirektøren, som øverste ansvarlig i kommunen, bærer derfor ansvaret for at kommunen til enhver tid har en tilstrekkelig god informasjons- og personopplysningssikkerhet.

Datatilsynet legger til grunn at personopplysnings- og informasjonssikkerheten i Østre Toten kommune var svært mangelfull da dataangrepet oppsto. Faktorer som logg/logganalyse, sikring av backup og tofaktorautentisering eller tilsvarende sikkerhetstiltak er grunnleggende forutsetninger for en fungerende og tilstrekkelig informasjons- og personopplysningssikkerhet. Etter tilsynets syn var sikkerheten i Østre Toten kommune så vidt mangelfull at området ikke kan ha vært fulgt opp godt nok av øverste leder.

Kommunen har gjennomført interne gjennomganger, men disse har ikke bidratt til å avdekke grunnleggende sikkerhetsmangler. Det er i seg selv alvorlig. Datatilsynet mener derfor at saken viser at det klart har vært en uaktsom svikt hos ledelsen i Østre Toten kommune hva gjelder ivaretakelse av grunnleggende krav til personopplysningssikkerhet, jf. personvernforordningen artikkel 5 nr. 1 bokstav f, jf. artikkel 24 og 32.

Kommunedirektøren må som øverste leder stå ansvarlig for denne svikten. Datatilsynet mener derfor at kommunedirektøren i Østre Toten kommune klart har opptrådt uaktsomt.

Østre Toten kommunes syn på saken i hovedtrekk

Generelt om kravene til sikring av personopplysninger

Angrepet som Østre Toten kommune ble utsatt for, er noe det er vanskelig å beskytte seg mot fullstendig. Å ha tiltak som verner mot tilsvarende hendelser som Østre Toten kommune ble utsatt for setter omfattende krav til informasjonssystemer, som i de fleste tilfelle ikke vil være gjennomførbare og innenfor de tekniske muligheter og kostnadsrammer som de fleste virksomheter har.

Østre Toten kommune har iverksatt tiltak så langt det er mulig innenfor de rammer som en kommune har. I en kommune må det prioriteres tiltak og kostnadsbruk, og at det prioriteres enkelte områder vil nødvendigvis gjøre at andre, og kanskje viktigere områder for bl.a. liv og helse, prioriteres lavere. I slike saker må kommunen se hele sin virksomhet under ett mht. bruk av kostnader, og det er også noe som personvernforordningen artikkel 24 og 32 legger opp til. Handlingen til kommunen kan derfor ikke anses å være uaktsom, som stilles som krav for ileggelse av overtredelsesgebyr.

Datatilsynet legger til grunn en for høy terskel for kravene til informasjonssikkerhet og stiller for strenge krav til hvordan personopplysninger skal sikres, hvilket går ut over intensjonen med personvernforordningens krav til sikkerhet ved behandlingen etter bl.a. artikkel 32. Kravene er ikke realistiske eller gjennomførbare om det skal oppnås full sikring, og i dette tilfellet er det tvilsomt om sikringstiltak ville ha forhindret dataangrepet.

Logg og logganalyse

Manglende nettverkslogg ville ikke forhindret angrepet, men hadde betydning for omfanget av data som var hentet ut og hvor de uthentede dataene var fra i kommunenes systemer. Loggene hadde betydning for den etterfølgende vurderingen av hendelsens omfang, men ville ikke kunne ha redusert virkningene av hendelsen.

Det er derfor ikke riktig at forhold knyttet til logging og logganalyse skal begrunne overtredelsesgebyr.

Sikring av backup

Det er ikke riktig at kommunen «har blant annet manglet effektive … tilstrekkelig sikrede backupsystemer» slik Datatilsynet legger til grunn. Backupsystemene ble satt ut som følge av dataangrepet. Systemene var tilstrekkelige før angrepet.

Det er heller ikke riktig at «Kommunen manglet beskyttelse av sikkerhetskopier mot tilsiktet og utilsiktet sletting, manipulering og avlesning». Beskyttelsen var til stede, men sto ikke mot dataangrepet. Muligheten til å beskytte systemer mot denne type angrep er begrenset.

Manglende tofaktorautentisering eller tilsvarende sikkerhetstiltak

Kommunen er uenig med tilsynet i at kommunen manglet effektive sikkerhetstiltak ved pålogging. Kommunen hadde tiltak for å forhindre uautorisert pålogging. Selv om Datatilsynet og NSM anbefaler tofaktorautentisering, er det ikke et krav etter forordningen, og ville trolig heller ikke avverget dette angrepet. En risikoanalyse ville kunne vise at tofaktorautentisering er et tiltak som kan redusere risikoen, men det er ikke klart om det ville vært tilstrekkelig til å avverge dette angrepet.

Manglende bevissthet knyttet til sikkerhetstrusler og dataangrep

Det er ikke riktig at ledelsen og ansatte i kommunen har hatt manglende bevissthet rundt mulige sikkerhetstrusler og dataangrep. Kommunen gjennomførte en uavhengig gjennomgang av IKT-sikkerheten i kommunen forut for angrepet.

På initiativ fra kommunedirektøren ble det foretatt en gjennomgang av kvalitetssystemet Compilo høsten 2020. Gjennomgangen viste at det var tildelt ansvar og det var definerte rapporteringslinjer. Det forelå blant annet en rutine for årlig rapportering på IKT-sikkerhet. Kommunedirektørens vurdering var at kommunen hadde et godt internkontrollsystem som også omfattet IKT og personvernsikkerhet. Gjennomgangen viste også at det var rom for forbedringer som kommunen ville jobbe videre med. KPMG uttaler i sin rapport 26. august 2021 at det ikke var noen indikasjon på at kommunen var dårligere stilt enn andre kommuner, og at tilstanden i sammenlignbare kommuner sannsynligvis ligger på omtrent samme nivå.

IT-sikkerhet var og er et pågående område med høy prioritet hos kommunen, men eventuelle tiltak er det tvilsomt ville ha motvirket dataangrepene hensyntatt angrepsvektoren som utnyttet menneskelige faktorer.

Størrelsen på overtredelsesgebyret

Østre Toten kommune erkjenner at det kunne vært ytterligere sikringstiltak på plass for å redusere risikoen for at trusselaktøren fikk tilgang til systemene, men de krav som Datatilsynet stiller for å hindre dette angrepet er for strenge. Kommunen har iverksatt de tekniske og organisatoriske tiltak som kan forventes av en kommune innenfor kravene etter artikkel 24 og 32.

Når det gjelder at et overtredelsesgebyr skal virke avskrekkende, så har Østre Toten kommune hatt en omfattende oppgave med å håndtere konsekvensene av angrepet. Dette i seg selv vil være avskrekkende for andre virksomheter og en oppfordring til å vurdere sine sikkerhetstiltak. Østre Toten kommune mener imidlertid at den sikkerheten og de tiltakene som var på plass ved angrepet var tilstrekkelig innenfor kravene etter personvernforordningen, og ytterligere tiltak ville trolig ikke ha avverget dataangrepet. Verken grunnlaget som vedtaket er basert på fra Datatilsynet eller kravene etter personvernforordningen artikkel 24 og 32 foreligger. Følgelig kan ikke overtredelsesgebyr ilegges.

Gebyrets størrelse står heller ikke i forhold til andre sammenlignbare saker. Nylig ble Stortinget ilagt et gebyr på 2 000 000 kroner. I denne saken ble det funnet at det forelå grov uaktsomhet, i motsetning til Østre Toten kommune som ble ansett å ha handlet uaktsomt. De ulike gebyrene for Østre Toten kommune og Stortinget er etter kommunens oppfatning brudd på kravet til likebehandling.

Kommunen er av den oppfatning at gebyret som er ilagt er uforholdsmessig vurdert opp mot de tiltak som kommunen hadde iverksatt, kunne iverksatt og mot størrelsen på gebyr i sammenlignbare saker.

Om det foreligger uaktsomhet

Etter HR-2021-797-A er det ikke tilstrekkelig at det foreligger ordinær uaktsomhet ved foretaksstraff. Det må foreligge subjektiv skyld, og da fra person som er ansvarlig for forholdet i virksomheten. Overtredelsesgebyr er videre å anse som straff, jf. Rt-2012-1556. Som en følge av dette kreves det klar sannsynlighetsovervekt for lovbrudd for å kunne ilegge gebyr.

Datatilsynet har lagt til grunn at Østre Toten kommune, representert ved kommunedirektøren som øverste leder, har handlet uaktsomt ved ikke å sørge for tilstrekkelig

personopplysningssikkerhet og internkontroll i kommunen. Som det følger av ovennevnte dom, må det foreligge uaktsomhet hos kommunedirektøren, dvs. skylden må foreligge hos personen – straff kan ikke idømmes på rent objektivt grunnlag ved at anonyme og kumulative feil legges til grunn – hvor det må være en sammenheng mellom den ansvarliges (kommunedirektøren) og forholdene som gir grunnlag for straffen (overtredelsesgebyret). Datatilsynet har ikke påvist at det foreligger slik uaktsomhet, og i vedtaket er ikke forholdet behandlet.

Om Østre Toten kommune anses å ha brutt personopplysningsloven, så vil uansett ikke kommunen være å straffe siden det ikke er påvist med klar sannsynlighetsovervekt at kommunedirektøren har handlet uaktsomt.

Vedtaket er dessuten ikke tilstrekkelig begrunnet, jf. forvaltningsloven § 25, ved at det forhold at kommunedirektøren skal være uaktsom ikke er grunngitt.

Personvernnemndas vurdering

Spørsmålet for nemnda er om Østre Toten kommune har brutt personvernforordningen ved ikke å ha iverksatt egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, jf. personvernforordningen artikkel 32 og artikkel 24. Dersom det foreligger brudd på personvernforordningen, skal nemnda ta stilling til om det skal ilegges overtredelsesgebyr etter artikkel 83, og i tilfelle med hvilket beløp.

Det stilles etter rettspraksis krav om klar sannsynlighetsovervekt for å ilegge sanksjoner som har karakter av straff etter Den europeiske menneskerettighetskonvensjon (EMK) artikkel 6, jf. Rt-2008-1409 og Rt-2012-1556. Det innebærer at ileggelse av overtredelsesgebyr etter personopplysningsloven § 26 forutsetter klar sannsynlighetsovervekt ved vurderingen av bevisene, både når det gjelder objektive og subjektive forhold.

Vilkår for ileggelse av overtredelsesgebyr

Etter personopplysningsloven § 26 kan Datatilsynet ilegge en behandlingsansvarlig, også offentlige myndigheter, overtredelsesgebyr etter personvernforordningen artikkel 83. De generelle vilkårene for ileggelse av overtredelsesgebyr følger av artikkel 83.

Ordlyden i artikkel 83 gir ikke et klart svar på hvilke krav som stilles til skyld. I juridisk litteratur, for eksempel i Skullerud m.fl., Personvernforordningen, Lovkommentar, (per 1. mai 2022, juridika.no) er det lagt til grunn i kapittel VIII, om artikkel 83 nr. 2, at det er «ikke et vilkår for ileggelse av overtredelsesgebyr at det foreligger skyld hos overtrederen eller noen som har opptrådt på dennes vegne.» Nemnda er kjent med at fortolkningen av artikkel 83 og kravet til skyld for ileggelse av overtredelsesgebyr for foretak er til vurdering i EU-domstolen, sak C-807/21 Deutsche Wohnen SE.

Høyesterett har i HR-2021-797-A, avsnitt 23 uttalt at det ikke er forenlig med EMK artikkel 6 nr. 2 og artikkel 7 å straffe et foretak dersom ingen har utvist skyld. Høyesterett viser til nyere praksis fra Den europeiske menneskerettsdomstolen (EMD) hvor det kreves en «mental link» mellom handlingen og de faktiske omstendighetene som statuerer straffansvaret, jf. særlig EMDs storkammerdom 28. juni 2018 G.I.E.M. S.r.l. med flere mot Italia (EMD-2006-1828) og EMDs dom 20. januar 2009 Sud Fondi S.r.l. med flere mot Italia (EMD-2001-75909).

Som en følge av denne rettsutviklingen, og at overtredelsesgebyr anses å ha karakter av straff, jf. Rt-2012-1556, ble forvaltningsloven § 46 endret i 2022 slik at det nå oppstilles et krav om

uaktsomhet ved ileggelse av overtredelsesgebyr for foretak og offentlige myndigheter, med mindre noe annet er bestemt. Offentlige myndigheter kan ikke påberope seg et vern etter EMK, men departementet har likevel valgt å likestille skyldkravet for offentlige myndigheter og foretak, jf. forvaltningsloven § 46 første ledd siste punktum. I en situasjon hvor det ikke foreligger en tolkningsuttalelse fra EU-domstolen om hvilke krav som stilles etter artikkel 83 når det gjelder skyld, legger nemnda til grunn at «ikke annet er bestemt» i personvernforordningen. Dette innebærer at det også for spørsmålet om å ilegge offentlige myndigheter et overtredelsesgebyr, gjelder et krav om uaktsomhet etter forvaltningsloven § 46.

Nemnda vil i det følgende først ta stilling til om det foreligger objektive brudd på personopplysningssikkerheten. Deretter vil nemnda vurdere de subjektive vilkårene. De nærmere vilkårene for å konstatere subjektiv skyld hos et foretak (her kommune) behandles også nedenfor.

Om det foreligger brudd på personopplysningssikkerheten – objektive vilkår

Personvernforordningen pålegger den behandlingsansvarlige en rekke krav når det gjelder plikten til å ivareta informasjonssikkerheten for de personopplysningene som behandles. Personvernforordningen artikkel 32 nr. 1 lyder:

> «Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet,
>
> a) pseudonymisering og kryptering av personopplysninger,
> b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene,
> c) evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,
> d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.»

Det er ingen tvil om at løsepengevirusangrepet objektivt medførte brudd på konfidensialiteten (personopplysninger ble stjålet, lekket og publisert på det mørke nettet), samt brudd på tilgjengeligheten når en stor mengde personopplysninger ble gjort utilgjengelig for kommunens ansatte og innbyggere over lengre tid. Kommunen manglet fungerende IT-systemer i flere måneder, noe som viser at systemet var sårbart og hadde manglende robusthet.

Omfanget av sikkerhetsbruddet var alvorlig. En betydelig del av kommunens data ble rammet. En stor mengde personopplysninger er fullstendig tapt og opplysninger er delt på det mørke nettet i ukjent omfang. Dette gjelder også personopplysninger om barn og det omfatter særlige kategorier av personopplysninger, jf. artikkel 9, herunder pasientjournalopplysninger.

Kommunen hadde få egnede tiltak på plass for å kunne oppdage sårbarheter, avverge uønskede hendelser og begrense skadevirkningene. Dette inkluderer tilstrekkelig logging, konfigurering av brannmur, segmentering av nettverket, forsvarlig tilgangsstyring, sikrede

backupløsninger eller andre sikkerhetstiltak. Slike sikkerhetstiltak ville gjort det vesentlig vanskeligere for trusselaktøren å få tilgang til kommunens IT-system. Nemnda er enig med kommunen i at tofaktorautentisering ikke er noe absolutt krav for å oppnå tilstrekkelig informasjonssikkerhet, men fraværet av en slik løsning må eventuelt kompenseres med andre egnede sikkerhetstiltak.

Oppgaven med å gjenopprette drift (tilgjengelighet) av de berørte systemene ble betydelig hemmet av at sikkerhetskopiene var blitt slettet. Manglende sikring av sikkerhetskopier mot både målrettet og utilsiktet sletting, manipulasjon og lesing, representerer etter nemndas vurdering en kritisk mangel. Sikker tilgang til brannmur- og systemlogger ville sannsynligvis bidratt til å avdekke angrepsmetoden og bidratt til en raskere gjenoppretting av systemet.

Nemnda er enig med Datatilsynet i at de ulike manglene ved kommunens systemer for informasjonssikkerhet, representerer grunnleggende svakheter i kommunenes informasjonssikkerhet som medfører at personvernforordningen artikkel 32, jf. artikkel 24 objektivt sett er brutt.

Om det foreligger brudd på personopplysningssikkerheten – subjektive vilkår

Ved ileggelse av overtredelsesgebyr overfor foretak stilles krav om at den eller de som har opptrådt på vegne av foretaket har utvist alminnelig uaktsomhet, jf. forvaltningsloven § 46 og Personvernnemndas merknader ovenfor.

Datatilsynet har under forberedelse av klagesaken og i oversendelsesbrevet til nemnda konkludert med at det er overveiende sannsynlig at kommunedirektøren har handlet uaktsomt. Nemnda er ikke enig i tilsynets uaktsomhetsvurdering og mener at Datatilsynet også har tatt et uriktig rettslig utgangspunkt når tilsynet skriver: «Kommunedirektøren, som øverste ansvarlig i kommunen, bærer derfor ansvaret for at kommunen til enhver tid har en tilstrekkelig god informasjons- og personopplysningssikkerhet». Uttalelsen gir etter nemndas vurdering uttrykk for at kommunedirektøren er objektivt ansvarlig for brudd på informasjons- og personopplysningssikkerheten, uavhengig av om han har handlet uaktsomt eller ikke. Det er ikke riktig lovforståelse.

Slik nemnda ser det må den manglende informasjonssikkerheten forklares ut fra et manglende fokus på informasjonssikkerhet over tid, lenge før kommunedirektøren tiltrådte i sin stilling et snaut halvår før sikkerhetsbruddet skjedde. Manglende fokus og oppmerksomhet på informasjonssikkerhet, og kanskje også manglende kompetanse hos de som har sittet med ansvaret for de ulike systemene, har resultert i sårbare systemer som ikke har vært rustet for den typen hackerangrep som kommunen ble utsatt for. Det er ikke mulig å plassere dette ansvaret hos én person ut fra de opplysningene som foreligger i saken. Det er heller ikke sannsynliggjort at manglende avdekking og opprydding av dette i løpet av høsten 2020 skyldes uaktsomhet hos kommunedirektøren.

Nemnda legger imidlertid til grunn at det etter rettspraksis ikke er et krav om at skylden individualiseres. Både anonyme og kumulative feil kan utgjøre grunnlag for ansvar ved ileggelse av foretaksstraff, jf. HR-2022-1271-A, avsnitt 46-50, hvor Høyesterett kommenterer EMDs storkammerdom 28. juni 2018 (G.I.E.M. S.r.l. med flere mot Italia (EMD-2006-1828)):

«EMD uttaler i dommen ikke noe uttrykkelig om at ansvar ikke kan bygges på kumulative og/eller anonyme feil. Dommen kan etter min mening heller ikke forstås slik at det gjelder noe krav om individualisering ved vurdering av skyld og straffansvar.

Slik jeg ser det, følger dette allerede av at kravet til subjektiv skyld også ved foretaksstraff innebærer at en eller flere personer som har handlet på vegne av foretaket, må ha handlet uaktsomt. Det er altså ikke tale om noe rent objektivt ansvar. Videre er det foretaket, og ikke noen fysisk person, som eventuelt ilegges straff. Har en eller flere personer på vegne av foretaket, som her, opptrådt uaktsomt, er det da vanskelig å se noen grunn til å kreve at det kan påvises hvilke enkeltpersoner skylden er knyttet til.

De rettssikkerhetsgarantier for siktede som praksis fra EMD bygger på, er ivaretatt der det foreligger anonyme og kumulative feil. Også ved slike feil vil det være mulig å imøtegå en anklage om at noen som har handlet på vegne av foretaket, har opptrådt uaktsomt. Ansvar kan dessuten ikke gjøres gjeldende ved force majeure eller hendelige uhell. Skulle det i den enkelte sak framstå som urimelig å ilegge foretaksstraff, påligger det uansett domstolene å frifinne det tiltalte foretaket etter straffeloven § 28.

Ved å akseptere anonyme og kumulative feil unngår man at krav om individualisering av skyld reduserer effektiviteten av foretaksstraffen, som i vårt land spiller en viktig rolle i håndhevelsen av regelverk som gjelder for offentlig og privat virksomhet. Man unngår dessuten at to eller flere foretak som har utvist den samme form for straffbar adferd, blir behandlet forskjellig avhengig av om det kan bringes på det rene hvilke personer som har foranlediget de aktuelle forhold.

Jeg kan på denne bakgrunn ikke se at det vil være i strid med EMK å ilegge foretaksstraff ved anonyme og kumulative feil.»

Spørsmålet for nemnda er dermed om en eller flere personer i kommunen med ansvar for sikkerhet har opptrådt uaktsomt når informasjonssikkerheten var slik den var da kommunen ble utsatt for løsepengevirusangrepet.

Ved vurderingen av hvor aktsomhetsnormen for informasjonssikkerhetsarbeidet i kommunen skal ligge, må det i noen grad ses hen til kommunens rammer når det gjelder økonomi, personell og kompetanse. Det innebærer også at man ved aktsomhetsvurderingen må foreta en helhetsvurdering av det forebyggende sikkerhetsarbeidet, risikohåndteringen og iverksatte sikkerhetstiltak.

Nemnda mener, som Datatilsynet, at kommunen i liten grad har jobbet systematisk og strukturert med IKT-sikkerhet. Det er ikke foretatt tilstrekkelige risikovurderinger som kunne avdekket manglende tiltak og som kunne redusert konsekvensen av angrep. Løsepengevirusangrep har lenge vært en kjent sikkerhetstrussel og flere rapporter fra informasjonssikkerhetsmyndigheter som NSM og NorSIS peker på at dette er en økende trussel. Dette stiller etter nemndas syn krav til regelmessige risikovurderinger, noe som ikke er gjort her.

Med den kunnskapen og oppmerksomheten som har vært i samfunnet om risikoen for hackerangrep av denne typen, vurderer nemnda at en eller flere personer i kommunen har opptrådt uaktsomt når nødvendige sikkerhetstiltak ikke er iverksatt. Manglende risikovurderinger har resultert i få tiltak for å oppdage sårbarheter og uønskede hendelser. Det

har igjen resultert i for dårlige systemer for å sikre gjenoppretting etter et slikt angrep og gjort systemet sårbart. Det foreligger også årsakssammenheng mellom disse unnlatelsene og det sikkerhetsbruddet som rammet kommunen.

Nemnda finner det klart sannsynliggjort at det er en eller flere personer i kommunen med ansvar for sikkerhet som har opptrådt uaktsomt når sikkerheten ikke var bedre ivaretatt enn den var i dette tilfellet.

Etter dette er også de subjektive vilkårene for å ilegge overtredelsesgebyr oppfylt.

Overtredelsesgebyr

Ved brudd på bestemmelser i personvernforordningen kan tilsynsmyndigheten ilegge overtredelsesgebyr, jf. artikkel 58 nr. 2 bokstav i, jf. artikkel 83. Overtredelse av artikkel 32 kan sanksjoneres med gebyr, jf. artikkel 83 nr. 4 bokstav a. Det samme gjelder brudd på artikkel 24, jf. personopplysningsloven § 26 som gir artikkel 83 nr. 4 tilsvarende anvendelse for overtredelser av blant annet denne bestemmelsen. For brudd på pasientjournalloven § 22 (informasjonssikkerhet) og § 23 (internkontroll) følger det samme av pasientjournalloven § 29.

Spørsmålet er om det skal ilegges et overtredelsesgebyr for brudd på de nevnte bestemmelsene, og dersom det skal ilegges gebyr, hvor stort gebyret skal være.

Det følger av artikkel 83 nr. 1 at ileggelse av overtredelsesgebyr i hvert enkelt tilfelle skal være virkningsfullt, stå i et rimelig forhold til overtredelsen og virke avskrekkende. Både ved vurderingen av om det skal ilegges gebyr og ved utmålingen av gebyret, skal det tas hensyn til momentene i personvernforordningen artikkel 83 nr. 2 bokstavene a til k.

Det er for denne vurderingen sentralt å se på overtredelsens karakter, alvorlighetsgrad og varighet, jf. artikkel 83 nr. 2 bokstav a. Det følger av bestemmelsen at det skal tas hensyn til den aktuelle behandlingens art, omfang eller formål, samt antall registrerte som er berørt og omfanget av den skade de har lidd.

Når det gjelder spørsmålene om gebyr skal ilegges og utmålingen av gebyret, tar nemnda utgangspunkt i Datatilsynets vurdering.

Nemnda har lagt vekt på at en betydelig mengde personopplysninger er kompromittert og tapt for framtiden. Opplysninger er også spredt på det mørke nettet i ukjent omfang. Opplysningene det gjelder omfatter også særlig kategorier av opplysninger, jf. artikkel 9, og det omfatter opplysninger om barn. Disse forholdene vektlegges i skjerpende retning.

Nemnda viser videre til at sikkerhetsbruddet skyldtes grunnleggende mangler ved kommunens personopplysnings- og informasjonssikkerhetssystem. Det var ikke etablert eller gjennomført internkontroll på en måte som var egnet til å fange opp disse sikkerhetshullene. Nemnda er enig med tilsynet i at dette er svært alvorlig.

Nemnda er enig med Datatilsynet i at kommunen, da sikkerhetsbruddet ble oppdaget, har opptrådt ansvarlig både overfor tilsynsmyndigheten og overfor borgerne. Selv om dette vektlegges formildende ved utmåling av gebyrets størrelse, kan det ikke medføre at gebyret bortfaller. Nemnda bemerker at betydningen av kommunens oppfølgning etter angrepet ikke er konkretisert i Datatilsynets vedtak, men legger til grunn at forholdet er tilstrekkelig

hensyntatt ved den endelige gebyrfastsettelsen. Det samme gjelder kommunens økonomiske situasjon, herunder de kostnadene sikkerhetsbruddet har påført dem allerede.

Østre Toten kommune har anført at tilsynet bryter med prinsippet om likebehandling og har vist til at Stortinget ble ilagt et gebyr på 2 000 000 kroner etter et datainnbrudd i september 2020. Datatilsynet har ved oversendelsen av saken til nemnda redegjort for sin vurdering i saken som gjaldt Stortingets brudd på personopplysningssikkerheten holdt opp mot tilsynets vurdering i denne saken. Tilsynet anser sikkerhetsbruddet i Østre Toten kommune som klart mer alvorlig og har blant annet vist til de omfattende konsekvensene der svært mange personopplysninger gikk tapt og/eller er publisert på det mørke nettet. I saken der Stortinget ble rammet av et dataangrep, ble 13 ansattes e-postkontoer kompromittert. Selv om manglende tofaktorautentisering gjorde seg gjeldende også hos Stortinget, var ikke manglene ved den øvrige personopplysnings- og informasjonssikkerheten av like alvorlig karakter. Nemnda har ikke hatt saken som gjelder Stortinget til vurdering, men kan ikke, ut fra det som er beskrevet, se at Datatilsynet har brutt med prinsippet om likebehandling ved utmåling av overtredelsesgebyr i foreliggende sak.

Østre Toten kommune ilegges etter dette et overtredelsesgebyr 4 000 000 kroner.

Østre Toten kommune får ikke medhold i klagen.

Konklusjon
Datatilsynets vedtak om å ilegge Østre Toten kommune et overtredelsesgebyr på 4 000 000 kroner for brudd på personopplysningssikkerheten opprettholdes.

Vedtaket er enstemmig.

Oslo, 24. januar 2023

Mari Bø Haugstad
Leder