Datatilsynet

ØSTRE TOTEN KOMMUNE
Postboks 24
2851 LENA

| Deres referanse | Vår referanse | Dato |
|---|---|---|
| | 21/00480-14 | 07.01.2022 |

## Vedtak om overtredelsesgebyr og pålegg

Det vises til Østre Toten kommunes forhåndsvarsel og melding om brudd på personopplysningssikkerheten datert 22.01.2021 samt påfølgende tilleggsmeldinger.

I avviksmeldingen fremkom det at Østre Toten kommune hadde vært utsatt for et omfattende dataangrep. Angrepet ble oppdaget den 09.01.2021 da en rekke fagsystemer ble utilgjengelige.

I brev av 05.05.2021 ba vi Østre Toten kommune om en redegjørelse i saken. Kommunen svarte ut henvendelsen i brev datert 02.06.2021.

Datatilsynet varslet Østre Toten kommune om vedtak om overtredelsesgebyr og pålegg i brev av 18.10.2021. Kommunen har kommentert varselet i brev av 08.11.2021.

Vi er kjent med at kommunen har hatt tett kontakt med relevante sikkerhetsmyndigheter i sakens anledning. Forholdet er også anmeldt til politiet.

Kommunen har ellers gitt oss hyppige statusoppdateringer underveis i det etterfølgende og pågående etterforskningsarbeidet.

### 1. Vedtak om overtredelsesgebyr og pålegg

Datatilsynet har kommet til at Østre Toten kommune skal ilegges følgende 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 effektive sikkerhetstiltak ved pålogging, tilstrekkelig sikrede backup-systemer og tilstrekkelig 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.*

## 2. Nærmere beskrivelse av sikkerhetsbruddet og etterfølgende tiltak

Natt til 09.01.2021 ble Østre Toten kommune utsatt for et omfattende løsepengevirusangrep. Som konsekvens fikk ansatte ikke lenger tilgang til de fleste av kommunens IT-systemer, kommunens data var blitt kryptert og sikkerhetskopier slettet. Løsepengebrev ble funnet på en mengde lokasjoner.

Kommunen har anslått at ca. 30 000 dokumenter er omfattet av angrepet. Dokumentene inneholdt opplysninger om blant annet etnisk opprinnelse, politisk oppfatning, religiøs tro, fagforeningsmedlemskap, seksuelle forhold, helseforhold, pedagogiske diagnoser, fødselsnummer, MinID og bankkonto.

I tilleggsmelding innsendt 31.03.2021, fremgår det at etterforskningen i etterkant av angrepet har avdekket at data hentet ut under angrepet ble publisert på det mørke nettet («dark web»). Det skal dreie seg om flere typer dokumenter som inneholder ulike typer personopplysninger, og det er nærliggende å anta at disse dokumentene også inneholdt særlige kategorier av personopplysninger, om kommunens innbyggere og/eller ansatte. Etter kommunens anslag er ca. 2 000 dokumenter publisert.

Den 18.01.2021 ble KPMG involvert i etterforskningen for å yte teknisk bistand. KPMG fant blant annet at data fra Østre Toten kommunes Exchange-server sannsynligvis ble eksfiltrert til en IP-adresse i utlandet. Gjennomgang av nettverkslogger viser at det ble overført totalt 31,5 GB data. Videre hadde trusselaktøren eksportert et større antall mailbokser fra Exchange-serveren. Totalt utgjør postkasser og andre filer ca. 160 GB data. Trusselaktøren har hatt administratortilgang til alle datamaskiner, og alle filer fra serverne som ble undersøkt kan i prinsippet ha blitt eksfiltrert.

Den 30.03.2021 ble Østre Toten kommune og KPMG oppmerksomme på at trusselaktøren hadde publisert stjålne data på det mørke nettet.

Ved gjennomgang av det lekkede datamaterialet, fant KPMG informasjon som indikerte at trusselaktøren hadde hatt tilgang til kommunens infrastruktur tidligere enn først antatt. IT-avdelingen i kommunen identifiserte raskt en server som mesteparten av den lekkede informasjonen med stor sannsynlighet stammet fra (1 456 av 1 879 publiserte filer). Det er usikkert hvor mye data som ble eksfiltrert fra denne serveren. I rapporten fra KPMG fremkommer det at denne usikkerheten primært skyldtes manglende nettverkslogg bakover i tid.

I samarbeid med en ekstern part, hentet Atea IRT ut tilgjengelig logg fra kommunens brannmur. Av loggen fremkom det blant annet at trafikkloggene kun dekket tidsrommet fra

06.01.2021 til 09.01.2021. Det var usikkerhet knyttet til trafikkloggenes kvalitet og dekningsgrad, og det var kun begrenset logging av aktivitet mellom interne soner i nettverket. Manglende logging gjorde det vanskelig å fastslå hvor eksfiltrerte data hadde sitt opphav.

Kommunens brannmur var konfigurert til å sende logg (syslog) til en server, men lagringsdelen av denne serveren var ikke i drift, sannsynligvis grunnet en maskinvarefeil.

Videre var brannmuren sparsommelig konfigurert med tanke på logging, og mye interntrafikk ble aldri logget. Servere var ikke konfigurert til å sende logg til sentralt loggmottak og manglet også logging av viktige hendelser. Det fantes ikke sentralisert innsamling av logger, verken fra servere, klienter eller nettverksutstyr.

Backup-systemer var slettet, noe som utgjorde en vesentlig negativ faktor i arbeidet med å gjenopprette drift (tilgjengelighet) av systemene som var rammet. Det eksisterte derimot snapshots fra et antall servere som lettet arbeidet med gjenoppretting noe. Kommunen manglet beskyttelse av sikkerhetskopier mot tilsiktet og utilsiktet sletting, manipulering og avlesning, noe som er avgjørende for god informasjons- og personopplysningssikkerhet. Servere var også kryptert, hvilket gjorde at de tekniske undersøkelsene til å begynne med kun baserte seg på brannmurloggene fra tidsrommet 06.01.2021 til 09.01.2021.

Mens brannmurloggene ga god oversikt over trafikk til og fra internett, ga de begrenset innsikt i intern trafikk i kommunens IT-infrastruktur. Dette skyldtes både konfigurasjonen av brannmuren (mangelfull logging) og nettverkstopografien (mangelfull segmentering av nettverket).

Innledende angrepsvektor er ukjent. KPMG påpeker i sin rapport at brannmurlogger for hele perioden trusselaktøren har vært aktiv i infrastrukturen sannsynligvis ville bidratt til å avdekke angrepsvektoren. Det er også sannsynlig at systemlogger fra flere maskiner kunne kompensert for manglende brannmurlogger.

De tekniske undersøkelsene avdekket at det er svært sannsynlig at trusselaktøren har fått tilgang til infrastrukturen via fjernaksessløsninger som RDP, Citrix, VPN eller Teamviewer i kombinasjon med bruk av stjålne innloggingsdetaljer.

Østre Toten kommune benyttet ikke tofaktorautentisering eller tilsvarende sikkerhetstiltak for å opprettholde et sikkerhetsnivå egnet for å ivareta risikoen for uautorisert pålogging til sine systemer før hendelsen. Utnyttelse av stjålne innloggingsdetaljer ville derfor vært svært enkelt, forutsatt at kommunen eksponerte fjernaksessløsninger hvor kompromittert innloggingsinformasjon ville gitt tilgang. Alternativt kan trusselaktøren ha brukt metoder for sosial manipulasjon, for eksempel via e-post, og lurt en bruker til å installere skadevare som ga trusselaktøren nødvendig fotfeste.

En risiko- og sårbarhetsanalyse ville med all sannsynlighet avdekket behovet for tofaktorautentisering eller tilsvarende effektive sikkerhetstiltak for å beskytte kommunens

systemer. Både Nasjonal sikkerhetsmyndighet[1] og Datatilsynet[2] gir klare anbefalinger på dette området.

KPMG identifiserte et titalls e-postadresser og passord tilhørende ansatte i Østre Toten kommune som på ulike måter hadde fått lekket innloggingsdetaljer.

Kommunen varslet innbyggerne om dataangrepet. Informasjon om angrepet og den pågående prosessen med undersøkelser ble også fortløpende lagt ut på kommunens nettside.

Kommunen startet et omfattende arbeid med å utarbeide gode rutiner for behandling av personopplysninger og avvikshåndtering.

## 3. Rettslig grunnlag

Datatilsynet fører kontroll med etterlevelsen av personvernregelverket, jf. personvern-forordningen artikkel 57 flg.

### *3.1 Grunnprinsippene*

De grunnleggende prinsippene for behandling av personopplysninger fremgår av personvernforordningen artikkel 5. Vi viser særlig til artikkel 5 nr. 1 bokstav f, hvor det fremgår:

> «1. Personopplysninger skal (…)
> f) behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling (…), ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og konfidensialitet»)».

Det er den behandlingsansvarliges ansvar at prinsippene overholdes, og den behandlingsansvarlige skal kunne påvise dette, jf. artikkel 5 nr. 2.

### *3.2 Kravene til personopplysningssikkerhet og styringssystemer*

Personvernforordningen artikkel 32 regulerer kravene til sikkerhet ved behandlingen av personopplysninger. Under følger et utdrag av relevante deler av artikkel 32:

> «1. 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, (…)
> b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene (…).

[1] Råd og anbefalinger om passord: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/rad-og-anbefalinger-om-passord
[2] Passordanbefalinger | Datatilsynet

> 2. Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av (…) ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet».

Plikten til å gjennomføre egnede tekniske og organisatoriske tiltak fremgår tilsvarende av personvernforordningen artikkel 24, som regulerer den behandlingsansvarliges ansvar særskilt.

### *3.3 Særlig om ileggelse av overtredelsesgebyr*

Av personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26 annet ledd, fremgår det at Datatilsynet kan ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 83 ved brudd på regelverket. Overtredelsesgebyr er et virkemiddel for å sikre effektiv etterlevelse og håndhevelse av personvernregelverket.

I samsvar med Høyesteretts praksis, jf. Rt. 2012 side 1556, legger vi til grunn at overtredelsesgebyr er å anse som straff etter Den europeiske menneskerettighetskonvensjonen artikkel 6. Det kreves derfor klar sannsynlighetsovervekt for lovbrudd for å kunne ilegge gebyr.

I personvernforordningen artikkel 83 angis vilkårene for ileggelse av gebyr. Bestemmelsen inneholder blant annet en oversikt over hvilke momenter det skal tas hensyn til, både i vurderingen av hvorvidt overtredelsesgebyr skal ilegges og i utmålingen av gebyrets størrelse.

De relevante delene av artikkel 83 nr. 1 og nr. 2 gjengis under:

> «1. Hver tilsynsmyndighet skal sikre at ilegging av overtredelsesgebyr i henhold til denne artikkel for overtredelser av denne forordning nevnt i nr. 4, 5 og 6 i hvert enkelt tilfelle er virkningsfull, står i et rimelig forhold til overtredelsen og virker avskrekkende.
>
> 2. (…) Når det treffes avgjørelse om hvorvidt det skal ilegges overtredelsesgebyr samt om overtredelsesgebyrets størrelse, skal det i hvert enkelt tilfelle tas behørig hensyn til følgende:
> a) karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd,
> b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt,
> c) eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd,
> d) den behandlingsansvarliges eller databehandlerens grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32,
> e) eventuelle relevante tidligere overtredelser begått av den behandlingsansvarlige eller databehandleren,

f) graden av samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den,
g) kategoriene av personopplysninger som er berørt av overtredelsen,
h) på hvilken måte tilsynsmyndigheten fikk kjennskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen, (…)
k) enhver annen skjerpende eller formildende faktor ved saken, f.eks. økonomiske fordeler som er oppnådd, eller tap som er unngått, direkte eller indirekte, som følge av overtredelsen».

Artikkel 83 angir også rammene for overtredelsesgebyrets størrelsesorden. Vi viser i denne forbindelse til artikkel 83 nr. 4 og 5. De relevante delene av bestemmelsene lyder:

«4. Ved overtredelser av følgende bestemmelser skal det i samsvar med nr. 2 ilegges overtredelsesgebyr på opptil 10 000 000 euro (…):
a) den behandlingsansvarliges og databehandlerens forpliktelser i henhold til artikkel 8, 11, 25-39 samt 42 og 43 (…)».

5. Ved overtredelser av følgende bestemmelser skal det i samsvar med nr. 2 ilegges overtredelsesgebyr på opptil 20 000 000 euro (…):
a) de grunnleggende prinsippene for behandling, herunder vilkår for samtykke, i henhold til artikkel 5, 6, 7 og 9 (…)».

I personopplysningsloven § 26 første ledd fremgår det at personvernforordningen artikkel 83 nr. 4 gjelder tilsvarende for overtredelser av forordningen artikkel 24.

## 4. Datatilsynets vurdering

Som det fremgår over, var det store mangler ved Østre Toten kommunes 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. Dette utgjør i seg selv brudd på kravene til personopplysningssikkerhet i personvernforordningen artikkel 32, jf. artikkel 24.

Angrepet mot Østre Toten kommune er særlig alvorlig fordi det har rammet en betydelig del av kommunens data. Vi ser svært alvorlig på at kontrollen over personopplysninger om kommunens innbyggere og ansatte er fullstendig tapt gjennom det aktuelle dataangrepet. Opplysninger er delt på det mørke nettet i ukjent omfang.

At backup-systemer var slettet, var en vesentlig negativ faktor i arbeidet med å gjenopprette drift (tilgjengelighet) av systemene som var rammet. Det eksisterte derimot snapshots fra et antall servere som lettet arbeidet med gjenoppretting noe. At Østre Toten kommune ikke beskyttet sine sikkerhetskopier mot tilsiktet og utilsiktet sletting, manipulering og avlesning var en betydelig mangel ved kommunens styringssystem for informasjons- og personopplysningssikkerhet.

KPMG og Østre Toten kommune har pekt på at brannmuren var dårlig konfigurert med tanke på logging. Mye interntrafikk ble aldri logget, og serverne var ikke konfigurert til å sende logg til sentralt loggmottak. Det er pekt på at årsaken både er konfigurasjonen av brannmuren (mangelfull logging) og nettverkstopografien (mangelfull segmentering av nettverket). Vi vurderer dette som grunnleggende svakheter i kommunens informasjonssikkerhet som i seg selv innebærer 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 Østre Toten kommune brutt det grunnleggende prinsippet om plikten til å ivareta opplysningers konfidensialitet og integritet, jf. personvernforordningen artikkel 5 nr. 1 bokstav f.

### *4.1 Vurdering av om overtredelsesgebyr skal ilegges*

Datatilsynet har kommet til at kommunen har brutt personvernforordningen 32, jf. artikkel 24 og artikkel 5 nr. 1 bokstav f.

Under gjennomgår vi de momentene som vi anser relevante for vurderingen av om overtredelsesgebyr skal ilegges.

*a) karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd*

En betydelig del av kommunens data er rammet av angrepet, herunder særlige kategorier personopplysninger og opplysninger om barn, som begge har krav på et særskilt vern. Dataene er tapt for kommunen og delt i ukjent omfang på det mørke nettet. Det er dermed umulig å forhindre videre deling eller kompromittering av personopplysningene, noe som gjør saken særlig alvorlig.

*b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt*

Datatilsynet legger til grunn at Østre Toten kommune, representert ved rådmannen som øverste leder, har handlet uaktsomt ved ikke å sørge for tilstrekkelig personopplysningssikkerhet og internkontroll i kommunen.

*c) eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd*

Kommunen meldte raskt fra til relevante aktører, som politi og tilsynsmyndighet, etter at avviket ble oppdaget. Med ekstern bistand har kommunen gjort sitt ytterste for å følge opp saken og forhindre ytterligere skadevirkninger.

Videre gjorde kommunen raskt tiltak for å varsle innbyggerne om databruddet. Kommunen har også fortløpende lagt ut informasjon på kommunens nettside.

Kommunen har begynt arbeidet med å utarbeide gode rutiner for behandling av personopplysninger og avvikshåndtering.

*d) den behandlingsansvarliges eller databehandlerens grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32*
Østre Toten kommune har hatt grunnleggende mangler i personopplysnings- og informasjonssikkerheten og internkontrollarbeidet. På grunn av disse manglene har integriteten og konfidensialiteten til samtlige personopplysninger om kommunens innbyggere og ansatte blitt kompromittert.

*f) graden av samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den*
Kommunen meldte raskt fra til tilsynsmyndigheten og har i etterkant samarbeidet fullt ut i vår saksbehandlingsprosess, blant annet gjennom løpende oppdateringer.

*g) kategoriene av personopplysninger som er berørt av overtredelsen*
Særlige kategorier av personopplysninger og personopplysninger om barn er berørt av dataangrepet. Det er også sannsynlig at slike opplysninger er delt på det mørke nettet.

*h) på hvilken måte tilsynsmyndigheten fikk kjennskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen*
Kommunen meldte selv fra om avviket, i tråd med meldeplikten etter personvernforordningen artikkel 33. Avviket ble først meldt muntlig, men utfyllende opplysninger ble gitt skriftlig innen rimelig tid.

*Konklusjon*
Som nevnt, ser Datatilsynet svært 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.

Vi legger til grunn at kommunen har hatt grunnleggende mangler ved personopplysnings- og informasjonssikkerheten og internkontrollarbeidet. Vi har kommet til at kommunen har brutt personvernforordningen artikkel 32, jf. 24, og også det grunnleggende prinsippet om integritet og konfidensialitet i artikkel 5 nr. 1 bokstav f.

På denne bakgrunn har vi kommet til at Østre Toten kommune skal ilegges et overtredelsesgebyr, jf. artikkel 83 nr. 4 og 5, jf. også personopplysningsloven § 26.

### *4.2 Utmåling av gebyret*
I vurderingen av gebyrets størrelse, har vi sett hen til at dataangrepet kunne skje som følge av helt grunnleggende mangler ved kommunens personopplysnings- og informasjonssikkerhets-system. Kommunen har ikke etablert eller gjennomført internkontroll på en måte som har vært egnet til å fange opp disse sikkerhetshullene. Dette er i seg selv svært alvorlig.

Dataangrepet har også medført en betydelig del av kommunens data er kompromittert og tapt for fremtiden. Vi legger til grunn at angrepet har medført spredning av til dels svært

beskyttelsesverdige personopplysninger på det mørke nettet. Dette vil kunne være alvorlig for den enkelte registrerte, men har også omfattende konsekvenser for kommunens løpende drift. Også dette er et skjerpende moment i saken.

Denne saken illustrerer hvor alvorlige konsekvenser et dataangrep kan medføre og hvor viktig det derfor er å ha robust infrastruktur og tilstrekkelig beskyttelse mot sikkerhetsangrep utenfra.

Som følge av dataangrepet, har Østre Toten kommune måttet bruke store summer på å gjenopprette et fungerende IT-system og sørge for tilfredsstillende informasjonssikkerhet. Dette arbeidet er ikke sluttført. Ifølge opplysninger i media[3] har dataangrepet hittil kostet kommunen over kr. 32 000 000. Dette er nødvendigvis en enorm økonomisk belastning for en kommune med knapt 15 000 innbyggere[4]. Kommunens økonomiske situasjon er et moment som vil ha betydning for vår utmåling av gebyret, jf. personvernforordningen artikkel 83 nr. 2 bokstav k.

Det taler i kommunens favør at de selv meldte avviket til Datatilsynet og har vært svært samarbeidsvillige i etterkant. Kommunen har også gjort sitt ytterste for å gi god informasjon til innbyggerne.

Ved brudd på grunnleggende prinsipper om behandling av personopplysninger og krav til personopplysningssikkerhet, er utgangspunktet at et overtredelsesgebyr vil være høyt. Vi har likevel vektlagt at kommunen allerede har brukt betydelige summer på å gjenopprette og forbedre IT-systemene og personopplysningssikkerheten, noe som har satt Østre Toten kommune i en vanskelig økonomisk situasjon. Kommunens omfattende arbeid opp mot tilsynsmyndigheter, politi og innbyggere/ansatte i etterkant av at avviket ble oppdaget skal også få en viss betydning for overtredelsesgebyrets størrelse.

Datatilsynet har kommet til at et overtredelsesgebyr på 4 000 000 NOK er rimelig i denne saken.

Etter vår vurdering, gjenspeiler beløpet både lovbruddets alvor, kommunens økonomiske situasjon etter angrepet og kommunens omfattende arbeid i etterkant. Uten disse forholdene, ville gebyret bli satt vesentlig høyere.

### *4.3 Vurdering av om pålegg skal gis*

Sikkerhet ved behandlingen av personopplysninger, herunder informasjonssikkerhet, er i sin helhet et ledelsesansvar. Utførelsen av oppgaver kan delegeres, men ikke ansvaret. Som verktøy for å oppnå effektive tekniske og organisatoriske tiltak må ledelsen tilse at det foreligger styringssystemer for personopplysningssikkerhet som en del av internkontrollsystemet og virksomhetskontrollen.

---

[3] https://aktuellsikkerhet.no/cybersikkerhet-datainnbrudd-it-sikkerhet/ostre-toten-kommune-dataangrepet-har-kostet-oss-mer-enn-32-millioner/700321

[4] https://www.ssb.no/kommunefakta/ostre-toten

Den aktuelle saken viser store mangler ved Østre Toten kommunes arbeid med informasjonssikkerhet. Manglene har hatt svært alvorlige følger i form av tap av alle kommunens data gjennom et dataangrep.

På bakgrunn av dette, har vi funnet grunnlag for å gi Østre Toten kommune følgende pålegg:

> 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.

## 5. Informasjon om klageadgang

Dere kan klage på vedtaket innen tre uker etter at dere har mottatt dette brevet, jf. forvaltningsloven §§ 28 og 29.

En eventuell klage sendes til Datatilsynet. Dersom vi opprettholder vår avgjørelse, vil vi sende klagen til Personvernnemnda for avgjørelse, jf. personopplysningsloven § 22.

Dersom dere har spørsmål, kan dere ta kontakt med fagdirektør Kristine Stenbro eller undertegnede saksbehandler.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Susanne Lie
juridisk seniorrådgiver

*Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer*

Kopi til: ØSTRE TOTEN KOMMUNE, Inger Cock-Olsen