Datatilsynet

STORTINGET
Postboks 1700 Sentrum
0026 OSLO

Deres referanse	Vår referanse	Dato
	20/03500-10	04.03.2022

Vedtak om overtredelsesgebyr - Melding om avvik - Stortinget

1. Innledning

Datatilsynet viser til innsendt melding av 6. september 2020 om brudd på personopplysningssikkerheten, varsel om overtredelsesgebyr av 13. januar 2022 samt Stortingets tilsvar av 14. februar 2022.

Vi viser også til øvrig korrespondanse, og dokumentasjon som er gjort tilgjengelig for oss som kan knyttes til den aktuelle meldingen om brudd på personopplysningssikkerheten. Den samlede dokumentasjonen ligger til grunn for vedtaket. Det er angrepet i 2020 som ligger til grunn for vedtaket. Hendelsene i mars 2021 er av en annen karakter, og vil ikke ha betydning for dette vedtaket.

I det følgende vil Multi Faktor Autentisering (MFA), tofaktorautentisering og sterk autentisering bety det samme. I fortsettelsen vil disse omtales under samlebetegnelsen «tofaktorautentisering».

2. Datatilsynets merknader til Stortingets svar

Datatilsynet har merket seg at Stortinget erkjenner at IT-sikkerheten kunne vært bedre da angrepet inntraff.

Dernest påpeker Stortingets administrasjon at oppfølgingen av ROS 2020 må ses i lys av at Stortingets administrasjon våren 2020 var sterkt preget av pandemien og nedstengningen som traff landet i begynnelsen av mars 2020, og den påfølgende ferieavvikling. Det gjøres også et poeng av at stortingsrepresentantene og de ansatte i partigruppene ikke var underlagt instruksjonsmyndighet fra Stortingets direktør, og at dette gjorde den videre prosess tidkrevende.

Datatilsynet kan ikke se at dette er momenter som har vesentlig betydning for hvorvidt overtredelsesgebyr skal gis og størrelsen på dette.

3. Vedtak om overtredelsesgebyr

Ut fra opplysningene i saken, mener Datatilsynet at Stortinget har overtrådt reglene om personopplysningssikkerhet i personvernforordningen:

I medhold av personopplysningsloven § 26 andre ledd, jf. personvernforordningen artikkel 58 nr. 2 bokstav i), jf. artikkel 83, ilegges Stortinget et overtredelsesgebyr på to millioner – 2 000 000 – kroner til statskassen for ikke å ha gjennomført egnede tekniske og organisatoriske tiltak, herunder tofaktorautentisering, for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen for å oppnå vedvarende konfidensialitet, integritet og robusthet, jf. personvernforordningen artikkel 32 nr. 1 bokstav b) og d), jf. artikkel 5 nr. 1 bokstav f).

Bakgrunnen og begrunnelsen for vedtaket følger under.

4. Saksforholdet

Stortinget ble 2. september 2020 gjort kjent med at det var utsatt for et datainnbrudd (uautorisert pålogging) knyttet til epostkontoene til et ukjent antall stortingsrepresentanter og ansatte i administrasjonen og gruppesekretariatene. Det var en av de ansatte som varslet administrasjonen etter at vedkommende hadde blitt kontaktet av sin bank om forsøk på misbruk av betalingskort i utlandet.

Etterfølgende undersøkelser avdekket at angripere hadde lastet ned ulike mengder data og at disse dataene kunne inneholde personopplysninger som stammet fra de berørte ansattes epostkontoer. Det ble i avviksmeldingen til Datatilsynet og etterfølgende tilleggsmelding opplyst om at det blant annet dreide seg om bank- og kontoinformasjon, inkl. personopplysninger om tredjeparter, fødselsnummer og helseopplysninger.

Mulige konsekvenser for de berørte av angrepet kan være misbruk av identitet, misbruk av betalingskort og bruk av informasjon til utpressing.

Stortingets administrasjon ble senere kjent med at personopplysninger fra 13 epostkontoer kunne være på avveie. De berørte ble informert og fulgt opp for å begrense skade. Personer som var omtalt i e-postene til de rammede (tredjeparter) ble varslet.

Som følge av hendelsen iverksatte Stortinget en rekke risikoreduserende og forebyggende tiltak. Det ble blant annet innført nye krav til passord, omfanget av sikkerhetslogging ble utvidet og retningslinjer for mobile enheter ble oppdatert. Det ble også startet et arbeid med å innføre tofaktorautentisering. I tillegg ble det iverksatt opplæringstiltak av ansatte for å øke bevisstgjøringen rundt informasjonssikkerhet.

Stortinget har tett kontakt med relevante sikkerhetsmyndigheter i denne saken. Forholdet er anmeldt til politiet og PST etterforsker saken.

5. Relevante rettsregler og veiledning om tofaktorautentisering som sikkerhetstiltak

Avvikene gjelder brudd på konfidensialitet, integritet og robusthet. I personvernforordningen artikkel 32 heter det:

«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.»

I personvernforordningen artikkel 5 nr. 1 bokstav f) er det uttalt at personopplysninger *«skal behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og konfidensialitet»)».*

Artikkel 32 stiller krav til at det gjennomføres en konkret kartlegging av risiko for fysiske personers rettigheter og friheter, sammenholdt med sannsynlighets- og alvorlighetsgrad. Kartleggingen må knyttes til den aktuelle virksomheten og deres behandling av personopplysninger.

Videre stiller bestemmelsen krav om at det skal gjennomføres egnede tekniske og organisatoriske tiltak for å oppnå egnet nivå av informasjonssikkerhet knyttet til nærmere angitte områder i artikkel 32 nr. 1 bokstav a) til d). Dette må anses som en plikt til å håndtere og redusere risikoene som identifiseres i kartleggingen gjennom innføring av tiltak. Disse kan enten være tekniske tiltak i form av fysisk sikkerhet som for eksempel autentiseringsløsninger, eller organisatoriske tiltak i form av for eksempel rutiner og opplæring av personell.

I Datatilsynets vurdering av hva som må anses som egnede tiltak, vil en virksomhets egen vurdering av risiko og nødvendige tiltak tillegges stor vekt.

Stortingets administrasjon forplikter som behandlingsansvarlig å gjøre seg kjent med regelverket på personvernområdet, herunder kravene til å gjennomføre risikovurderinger og iverksette nødvendige tiltak for å oppnå et tilfredsstillende sikkerhetsnivå. Dette følger av personvernforordningen artikkel 5 nr. 2.

Vi legger til grunn at det kan foreligge alternative tiltak for å sikre tilstrekkelig og effektivt sikkerhetsnivå. Innføring av tofaktorautentisering er et eksempel på sikkerhetstiltak som er

anerkjent som effektivt og lett tilgjengelig. Vi viser i den forbindelse til at både Datatilsynet og Nasjonal Sikkerhetsmyndighet (NSM) på sine nettsteder har publisert utfyllende informasjon om hvorfor og når tofaktorautentisering skal eller bør innføres.

På NSMs nettsted er det gitt tydelige anbefalinger om bruk av tofaktorautentisering ved opprettelse av bl.a. epostkontoer. NSM anbefaler i tillegg krav om unike passord per tjeneste.

På Datatilsynets nettsted informerer vi om sterk autentisering som sikkerhetstiltak. Det heter her:

> *Mange tjenester baserer seg kun på noe man vet i form av et brukernavn og passord. Svært mange bruker også samme passord på flere ulike tjenester. Noe som gjør deg som bruker enda mer utsatt for at andre logger seg inn som deg på ulike tjenester.*
>
> *Ofte vil en tjeneste stille krav til kompleksiteten av passordet slik som krav om minimumslengde, krav om bruke av tall, små og store bokstaver, og eventuelt spesialtegn. Dette kan redusere muligheten til å gjette passord, men brukere har en tendens til å bruke samme type mønster. Sommer2017 er en type passord som mange dessverre bruker. Det er også vanlig at brukere gjenbruker det samme passordet på flere tjenester.*
>
> *Hvis passordet skulle komme på avveier, har det ingen betydning hvor sterkt/komplekst passordet er. Det er dessverre mange måter et passord kan komme på avveier på. For eksempel lekkasje fra andre steder hvor brukeren benytter samme passord, skadevare på pc-en til brukere som plukker opp brukernavn og passord, «Man in the middle»-angrep og phising-angrep.*
>
> *Derfor er tofaktorautentisering en mye sikrere løsning. Ved bruk av slik autentisering vil konsekvensene av at brukernavn og passord kommer på avveier være langt mindre.*
>
> *I Norge har vi sett eksempler på at både politiske partier og skoler har erfart at noen har tilegnet seg uautorisert tilgang på systemer grunnet mangel på sterk autentisering.*
>
> *Datatilsynet kan pålegge bruk av sterk autentisering hvis vi vurderer at det er nødvendig for å ivareta sikkerheten.*

Datatilsynet utelukker ikke at andre tiltak vil kunne medføre tilsvarende nivå av sikkerhet som tofaktorautentisering.

6. Datatilsynets vurdering av Stortingets løsning for autentisering av brukere

Stortinget hadde ikke innført en tilstrekkelig løsning for tofaktorautentisering for alle brukere av deres e-post systemer på tidspunktet for sikkerhetsbruddet i september 2020. I den siste versjonen av ROS-analysen knyttet til autentisering som var ferdig i mars 2020, ble manglende tofaktorautentisering identifisert som «høy risiko» for tilgang for uautoriserte.

I Stortingets redegjørelse av 8. desember 2020 fremgår det at det er et pågående arbeid for å innføre tofaktorautentisering for brukerne på alle løsninger der det er teknisk mulig, herunder også epost.

Vi har også notert oss at manglende sikkerhetskultur ble identifisert som «høy risiko» for uautorisert tilgang til Stortingets systemer i ROS-analysen i 2020. I ROS-analysens avsluttende oppsummering fremkommer det at det oppleves utfordrende at ulike brukergrupper ikke er underlagt instruksjonsmyndighet fra Stortingets administrasjon. Manglende sikkerhetskultur, lav kompetanse og lite fokus på personvern er vurdert som en svært høy risiko.

Beskrivelsen i ROS-analysen avdekker etter vårt syn sårbarheter som kunne ha vært kompensert med organisatoriske tiltak, slik artikkel 32 pålegger. Eksempel på slike tiltak er kartlegging av de ansattes kunnskap om informasjonssikkerhet og personvern, og målrettet opplæring av de ansatte.

Som organisatoriske tiltak vil retningslinjer og rutiner for bruk av virksomhetens epostkonto kunne være effektive og nødvendige for å redusere risikoen de menneskelige faktorene utgjør. Disse bør være en del av styringssystemet for personvern og informasjonssikkerhet, som er besluttet av ledelsen i virksomheten.

Datatilsynet ser alvorlig på at det fra Stortingets side ikke har vært iverksatt tekniske tiltak som kunne ha forebygget overtredelsen, f.eks. gjennom bruk av tofaktorautentisering. Manglende eller mangelfulle sikkerhetstiltak øker sannsynligheten for sikkerhetsbrudd. Konsekvensen kan være svært alvorlig for de virksomhetene og deres ansatte som rammes av hendelser som dette.

Angrep via ansattes epost anses som en velkjent og reell angrepsvektor ved datasikkerhetsbrudd. Tilgang til epostkontoer er en kjent metode for tilgang til ytterligere systemer i en virksomhet.

Sikker autentisering anses som et enkelt og essensielt sikkerhetstiltak for å redusere risikoen for slike angrep.

Inntrengerne har i dette tilfellet fått tilgang til et antall av Stortingets e-postkontoer pga. manglende sikkerhetstiltak. Stortinget hadde i forkant gjennomført en risikovurdering som konkluderte med at tofaktorautentisering skulle innføres. Dette har imidlertid tatt uforholdsmessig lang tid.

Ved Datatilsynets gjennomlesing av ROS-analysen i mai 2021, var ikke innføringen av tofaktorautentisering ferdigstilt. Stortingets manglende innføring av de sikkerhetstiltakene som Stortinget selv har ansett som nødvendige på dette området, har gjort at tjenesten ble værende mindre robust og sårbar for angrep. Datatilsynet mener det er klart at dersom nødvendige tekniske og organisatoriske sikkerhetstiltak hadde blitt gjennomført på et tidligere tidspunkt, så ville Stortingets infrastruktur ha vært mer robust, og angrepet kunne ha vært unngått.

Manglende innføring av egnede tiltak for å håndtere en identifisert sårbarhet, i dette tilfellet endring av autentiseringsløsningen, i tillegg til mangelfulle organisatoriske tiltak, anses å utgjøre brudd på personvernforordningen artikkel 32 nr. 1 bokstav b) og d). De nevnte bestemmelsene krever at den behandlingsansvarlige etablerer et sikkerhetsnivå som er egnet til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i tjenestene.

7. Personvernforordningens regler om overtredelsesgebyr

I personopplysningsloven § 26 andre ledd er det bestemt at Datatilsynet kan ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 58, jf. artikkel 83 nr. 1 og 2.

Adgangen til å ilegge overtredelsesgebyr skal være et virkemiddel for å sikre effektiv etterlevelse og håndhevelse av personopplysningsloven. Overtredelsesgebyr er å anse som straff etter Den europeiske menneskerettskonvensjonen artikkel 6.

Datatilsynet legger derfor til grunn at det kreves klar sannsynlighetsovervekt for lovovertredelse for å kunne ilegge gebyr. Saksforholdet og spørsmålet om å ilegge overtredelsesgebyr er vurdert med utgangspunkt i dette beviskravet.

Vi viser i denne sammenheng til kapittel IX i forvaltningsloven om administrative sanksjoner. Med en administrativ sanksjon menes en negativ reaksjon som kan ilegges av et forvaltningsorgan, som retter seg mot en begått overtredelse av lov, forskrift eller individuell avgjørelse, og som regnes som straff etter den europeiske menneskerettskonvensjonen (EMK).

Det fremgår direkte av ordlyden i straffeloven § 27 at det gjelder et objektivt straffansvar for foretak. Høyesterett har i dom av 5. april 2021 (HR-2021-797-A), lagt til grunn at objektivt ansvar for foretaksstraff ikke er forenlig med straffebegrepet i Den europeiske menneskerettskonvensjon, slik det er tolket av Den europeiske menneskerettsdomstol.

I brev av 2. juni 2021 har Kommunal- og moderniseringsdepartementet oversendt Justis- og beredskapsdepartementets orientering av 12. mai 2021 om betydningen av denne høyesterettsdommen for administrative sanksjoner. Justis- og beredskapsdepartementet uttaler følgende:

> «I påvente av utredningen om foretaksstraff og eventuelle forslag til lovendringer, anbefaler vi at departementene orienterer sine underliggende etater om Høyesteretts avgjørelse, og at denne inntil videre legges til grunn også ved ileggelse av overtredelsesgebyr overfor foretak. Dette innebærer at det ved ileggelse av overtredelsesgebyr overfor foretak stilles krav om at den som har opptrådt på vegne av foretaket har utvist alminnelig uaktsomhet.»

Artikkel 83 gir i utgangspunktet anvisning på at ileggelse av overtredelsesgebyr beror på en skjønnsmessig helhetsvurdering, men legger føringer på skjønnsutøvelsen ved å trekke frem momenter som skal ha særlig vekt. Det fremgår av artikkel 83 nr. 1 at Datatilsynet skal sikre

at ilegging av overtredelsesgebyr i hvert enkelt tilfelle er virkningsfull, står i et rimelig forhold til overtredelsen og virker avskrekkende.

8. Datatilsynets vurdering av om overtredelsesgebyr skal ilegges

I vår vurdering av om vi skal ilegge overtredelsesgebyr, har vi særlig lagt vekt på følgende momenter:

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

Bruddet på personopplysningssikkerheten omfatter brudd på konfidensialitet, integritet og robusthet. I denne saken må det konkret legges til grunn at de folkevalgte og de ansatte ved Stortinget har en klar og beskyttelsesverdig interesse i at opplysninger om dem blir behandlet på en sikker måte.

Uautorisert tilgang til Stortingets systemer kan få alvorlige konsekvenser for den enkelte og for andres personopplysninger som epostkassene potensielt inneholder. Hendelsen kan ha medført at omgivelsene får tilgang til informasjon som de(n) registrerte ikke selv har valgt å gjøre kjent, og det er ukjent i hvilken grad disse opplysningene kan ha blitt spredt.

Bruddet på personopplysningssikkerheten har medført at representantene har mistet kontroll over personopplysningene som ligger i deres epostkontoer. Som en konsekvens av mangelfulle sikkerhetstiltak vil det være en sannsynlighet for at de folkevalgte kan bli utsatt for utpressing. Hendelsen kan også medføre at upålitelig informasjon fra falske aktører sendes ut fra de folkevalgtes epostkontoer.

Vi vil også fremheve at vi anser at dette bruddet kan ha medført en potensiell risiko for større angrep på Stortinget som institusjon, med epostsystemet som angrepsvektor.

Allmennpreventive grunner og hensynet til at reglene skal ha effekt og virke etter sin hensikt taler da med styrke for en streng reaksjon, og for at det ilegges overtredelsesgebyr.

a) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt

Saken viser at det har vært svikt hos Stortingets administrasjons ivaretakelse av ansvarlighetsprinsippet som følger av personvernforordningen artikkel 5, nr. 2. Datatilsynet finner at Stortingets administrasjon, ved Stortingets direktør, har opptrådt grovt uaktsomt, jf. HR-2021-797-A, jf. også personvernforordningen artikkel 5 nr. 2, for ikke å ha implementert en løsning for tofaktorautentisering ved opprettelse av epostkonto for de folkevalgte. Effekten av sikker autentisering som tiltak må anses å være velkjent, sammenholdt med at Stortinget selv hadde identifisert den høye risikoen mangelen på et slikt tiltak utgjorde. Videre finner vi det klanderverdig at Stortinget heller ikke fulgte opp den kjente sårbarheten med organisatoriske tiltak som til en viss grad kunne ha demmet opp for de tekniske manglene.

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

Etter angrepet ble det blant annet innført nye krav til passord, utvidet omfang av sikkerhetslogging, oppdaterte retningslinjer for mobile enheter og startet et arbeid med innføring av tofaktorautentisering. I tillegg ble det iverksatt opplæringstiltak av ansatte for å øke bevisstgjøringen rundt informasjonssikkerhet.

c) 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

Stortingets administrasjon tok en betydelig risiko da det ved opprettelsen av epostkontoer ikke ble innført tofaktorautentisering; og har et ansvar for at dette ikke ble gjort. At dette ikke var gjort på tidspunktet for det andre angrepet er en skjerpende omstendighet.

d) eventuelle relevante tidligere overtredelser begått av den behandlingsansvarlige eller databehandleren

Det er ingen tidligere overtredelser fra Stortingets administrasjon.

e) graden av samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den

Det har ikke vært noe samarbeid mellom Datatilsynet og Stortingets administrasjon for å bøte på skaden.

f) kategoriene av personopplysninger som er berørt av overtredelsen

Etterfølgende undersøkelser avdekket at angriperne hadde lastet ned ulike mengder data, bl.a. omfattet dette bank- og kontoinformasjon, fødselsnummer, helseopplysninger og personopplysninger om tredjeparter. Dette fremgår av innsendt melding av 6. september 2020. Det er en skjerpende omstendighet at helseopplysninger er kommet på avveier.

g) hvilken måte tilsynsmyndigheten fikk kunnskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen

Stortinget varslet Datatilsynet om bruddet på personopplysningssikkerheten ved melding av 6. september 2020. Stortinget har videre besvart våre forespørsler om ytterligere informasjon, samt lagt til rette for å gi Datatilsynet tilgang til relevant dokumentasjon i forbindelse med vår undersøkelse av saken.

h) dersom tiltak nevnt i artikkel 58 nr. 2 tidligere er blitt truffet overfor den berørte behandlingsansvarlige eller databehandler med hensyn til samme saksgjenstand, at nevnte tiltak overholdes

Det er ikke truffet tiltak overfor Stortinget med hensyn til samme saksgjenstand.

i) overholdelse av godkjente atferdsnormer i henhold til artikkel 40 eller godkjente sertifiseringsmekanismer i henhold til artikkel 42

Dette er ikke relevant for saken.

j) 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

Datatilsynet legger til grunn at Stortinget må regnes som et attraktivt mål for dataangrep, og at det ut fra en risikovurdering burde ha vært lagt et betydelig strengere sikkerhetsregime til grunn. ROS-analysen beskriver ulike tiltak i den oppsummerende delen, blant annet obligatorisk opplæring i informasjonssikkerhet og dokumentasjon på gjennomgått opplæring, samt tydeliggjøring av sanksjonsmuligheter overfor egne ansatte og avtale med partigrupper for å kunne gi samme sanksjoner der.

I skjerpende retning legges det til grunn at en løsning med tofaktorautentisering ikke var implementert i løsningen, til tross for at dette må regnes som et kjent og effektivt sikkerhetstiltak. Stortinget hadde selv identifisert manglende autentisering som en sårbarhet.

9. Samlet vurdering

Etter Datatilsynets vurdering, er saken prinsipielt viktig. Datatilsynet anser det som svært alvorlig at Stortingets administrasjon har vist manglende evne til å iverksette nødvendige sikkerhetstiltak som administrasjonen selv har identifisert behovet for i kartleggingen av risikoen ved behandling av personopplysninger. Vi presiserer at personvernforordningen stiller krav om at resultatet fra slike kartlegginger skal følges opp med egnede tiltak, og at det er nettopp dette som er formålet med å gjennomføre risikovurderinger, jf. personvernforordningen artikkel 32 nr. 1 bokstav b. Hendelsen som utløste meldingen til Datatilsynet og som danner grunnlag for vedtaket, kunne og burde ha vært unngått dersom Stortinget hadde iverksatt tiltak for å avhjelpe de sårbarhetene som ble gjort kjent gjennom risikovurderingen.

Vi legger til grunn at Stortingets administrasjon har en egeninteresse i å innrette Stortingets datasystemer i tråd med anbefalinger fra nasjonale fagmyndigheter. Det er administrasjonen som har ansvaret for driften av disse systemene, og ansvaret for å innføre de sikkerhetstiltakene som er nødvendige for å gjøre systemene robuste, i samsvar med lovens krav, jf. personvernforordningen artikkel 5 nr. 2, jf. artikkel 5 nr. 1 bokstav f, jf også artikkel 32 nr. 1 bokstav b.

Etter en samlet vurdering har Datatilsynet kommet til at Stortinget skal ilegges et overtredelsesgebyr.

10. Gebyrets størrelse

I forarbeidene til ny personopplysninglov (Prop. 56 LS (2017-2018)) uttaler departementet at

> «som utgangspunkt [skal] de samme reglene for overtredelsesgebyr gjelde for offentlige organer som for private, da dette er ordningen etter gjeldende personopplysningslov.»

Når det gjelder gebyrets størrelse, skal de samme momenter som ved vurdering av om gebyr skal ilegges, tillegges særlig vekt. Gebyret bør settes så høyt at det får virkning også utover den konkrete saken, samtidig som gebyrets størrelse må stå i et rimelig forhold til overtredelsen og virksomheten, jf. art. 83 nr. 1.

Etter en totalvurdering av sakens omstendigheter, og da særlig sett hen til alvorligheten i overtredelsen og lovverkets krav om at ileggelsen av overtredelsesgebyr i hvert enkelt tilfelle skal være virkningsfull, forholdsmessig og avskrekkende, har vi kommet til at et overtredelsesgebyr på **to millioner – 2 000 000 – kroner** anses som riktig.

11. Klage

Dere kan klage på vedtaket. En eventuell klage må sendes til oss **innen mandag 15. august 2022.** Dersom vi opprettholder vårt vedtak, vil vi sende saken til Personvernnemnda for klagebehandling, jf. personopplysningsloven § 22.

12. Innsyn og offentlighet

Dere har rett til innsyn i sakens dokumenter, jf. forvaltningsloven § 18. Vi vil også informere dere om at alle dokumentene i utgangspunktet er offentlige, jf. offentlighetsloven § 3, men understreker samtidig at sikkerhetsdokumentasjon som hovedregel er unntatt offentlighet, jf. offentlighetsloven § 13 og forvaltningsloven § 13 første ledd nr. 2.

Dersom dere har spørsmål, kan dere ta kontakt med saksbehandler Knut B. Kaspersen.

Med vennlig hilsen

Janne Stang Dahl
fungerende direktør

Knut Brede Kaspersen
juridisk fagdirektør

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer