Datatilsynet

BERGEN KOMMUNE
Postboks 7700
5020 BERGEN

Deres referanse	Vår referanse	Dato
2019/04991-9	18/02140-13/KBK	18.03.2019

Vedtak om pålegg og overtredelsesgebyr - Melding om avvik hos Bergen kommune

0. Innledning

Vi viser til melding om brudd på personopplysningssikkerheten (avviksmelding) fra Bergen kommune sendt 15. august 2018, Datatilsynets varsel om vedtak av 17. desember 2018, Bergens kommunes tilbakemelding på Datatilsynets varsel av 31. januar 2019 og annen relevant korrespondanse i saken.

Saken gjelder en hendelse hvor filer med brukernavn og passord til over 35 000 brukere i Bergen kommune har ligget åpent tilgjengelig for elever. Det har vært mulig å logge seg inn på skolens ulike informasjonssystem som en elev, ansatt eller administrator på skolen, og dermed få tilgang til personopplysninger om elever og ansatte.

Datatilsynet har merket seg de anførslene kommunen har kommet med om lovvalgspørsmålet, men kan ikke se at disse endrer vårt syn i saken. Bergen kommune har også gitt en kronologisk framstilling over de faktiske forhold i saken, hvor det bl.a. gis en redegjørelse for kommunens arbeid med innføring av tofaktorautentisering. Datatilsynet kan imidlertid ikke se at dette får innvirkning på vårt vedtak.

Når det gjelder de varslete vedtak, opplyser kommunen at disse må regnes som lukket. Vedrørende det varslete vedtak nr. 1 opplyses det at innføringen sluttføres i disse dager. Datatilsynet vil imidlertid påpeke at avviket først kan regnes som lukket når innføringen av tofaktorautentisering er sluttført. Vi opprettholder derfor vedtaket.

Når det gjelder det varslete vedtak nr. 2 tar vi til etterretning at avviket er lukket ved at dere etterlever personvernforordningen artikkel 5 og artikkel 32.[1] Det innebærer at Bergen kommune sikrer en vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet (artikkel 32 nr. 1 b), og at dere har en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er (artikkel 32 nr. 1 d).

[1] Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016, jf. lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven) § 1.

Ut fra opplysningene i saken, mener Datatilsynet at Bergen kommune har overtrådt reglene om personopplysningssikkerhet i personvernforordningen. Datatilsynet fatter tre ulike vedtak. Det ene vedtaket gjelder ileggelse av overtredelsesgebyr. De to andre vedtakene gjelder pålegg om å iverksette nærmere tiltak.

Nærmere redegjørelse for hva vedtaket om pålegg og overtredelsesgebyr innebærer og begrunnelse for det følger nedenfor.

1. Vedtak om pålegg og overtredelsesgebyr

1.1 Vedtak om pålegg

Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav d, fatter Datatilsynet vedtak om følgende pålegg:

1) *Bergen kommune må endre alle ansattes pålogging til alle informasjonssystemer som inneholder personopplysninger om elever, ved at det etableres sterk autentisering (tofaktorautentisering) for pålogging over eksterne nett og på elevnett[2], jf. personvernforordningen artikkel 5 nr. 1 bokstav f, jf. artikkel 32 nr. 1, jf. bokstav b*

1.2 Vedtak om overtredelsesgebyr

I medhold av personopplysningsloven § 26 andre ledd kan Datatilsynet ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 83.

Med hjemmel i personopplysningsloven § 26, jf. personvernforordningen art. 83, fatter Datatilsynet følgende vedtak om overtredelsesgebyr:

2) *Bergen kommune skal, i medhold av personopplysningsloven § 26 andre ledd, jf. personvernforordningen artikkel 83, betale et overtredelsesgebyr på* ***1.600.000 NOK – en million seks hundre tusen norske kroner –*** *til statskassen, for ikke å ha gjennomført egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, og sikring av vedvarende konfidensialitet, jf. personvernforordningen artikkel 5 nr. 1 bokstav f, og personvernforordningen 32 nr. 1. bokstav a og b.*

2. De faktiske forholdene og sakens gang

2.1 Gangen i saken

Datatilsynet ble kjent med saken etter at Bergen kommune fredag 15. august 2018 sendte ut pressemelding. Saken fikk stor interesse i media og Datatilsynet ble samme dag kontaktet av VG, Bergens Tidende, Bergensavisa og NRK.

[2] Vi mener her trådløse gjestenett som elever kan koble seg opp til og som er åpent for andre enn de ansatte.

Bergen kommune sendte melding om brudd på personopplysningssikkerheten (avviksmelding) til Datatilsynet den 15. august 2018.

Personvernombudet i Bergen kommune ga Datatilsynet en oppdatering om bruddet på personopplysningssikkerheten, ved e-post den 16. august. Vi mottok en tilleggsmelding fra Bergen kommune den 24. august, som inneholdt en rapport om det meldte bruddet på personopplysningssikkerheten, og et brev fra kommunen som hadde blitt sendt til foreldre og foresatte som var berørt av bruddet på personopplysningssikkerheten.

De foresatte til en av elevene ved den aktuelle skolen har i e-post av 10. september henvendt seg til Datatilsynet for å gi sin versjon av saken. Datatilsynet har også vært i telefonisk kontakt med:

- Bergen kommunes leverandør av eFeide, Identum
- Rektor ved den aktuelle skolen
- Vest politidistrikt v/ Ronny Haldorsen

2.2 Saken omfatter følgende systemer
Kommunen benytter FEIDE som påloggingsløsning i skolen. Bergen kommune har beskrevet denne løsningen slik:

> «FEIDE er en brukerkatalog for elever, som gir sentral brukerregistrering og «single sign-on» til ulike tjenester og system som er i bruk i skolen. eFeide er et verktøy for å opprette og administrere brukerne i FEIDE-brukerkatalogen.»

Slik Datatilsynet har forstått det er FEIDE en nasjonal innloggingsløsning som gjør det mulig å dele data i forbindelse med utdanning og forskning. Når ansatte og elever i grunnskolen i Bergen logger seg inn via FEIDE, får de tilgang til ulike systemer, som blant annet Its Learning. Its Learning er en læringsplattform som i tillegg til skolefaglig arbeid også inneholder vurderinger og evalueringer av enkeltelevers prestasjoner. Systemet gjør det mulig å kommunisere mellom elever og lærere, og man kan bruke fritekstfelt hvor lærere kan legge inn opplysninger om elever som er registrert i systemet.

En annen tjeneste som er tilgjengelig gjennom FEIDE i Bergen kommune er Conexus Engage. Det er et verktøy for den enkelte lærer hvor intensjonen er å lette lærerens arbeid knyttet til oppfølgingen av den enkelte elev. Tjenesten inneholder både kartlegging av faglige så vel som sosiale forhold om eleven.

Bergen kommune bruker eFeide som brukeradministrasjonsverktøy. eFeide er en skyløsning som gjør det mulig for ansatte og elever å logge seg inn på skolens systemer (via FEIDE) fra ulike enheter (bærbar datamaskin, smarttelefon, e.l.). Per 24. august 2018 hadde eFeide totalt 35 601 unike brukere i Bergen kommune. Bergen kommunes eFeide-system inneholder opplysninger om brukernes navn, brukernavn, passord, fødselsnummer, adresse, skoletilhørighet og skoleklasse. Ansatte er også registrert med telefonnummer.

eFeide leveres av Identum.

Nærmere om de faktiske forholdene i saken
I det følgende vil vi beskrive hvordan vi, basert på sakens dokumenter og informasjon innhentet fra ulike parter, oppfatter de faktiske forholdene i saken.

Tirsdag 15. mai 2018 mottok IKT Helpdesk i Bergen kommune en melding fra en ansatt ved en skole om at en mappe med flere filer som inneholdt brukernavn og passord, var tilgjengelig for elever. Dette hadde blitt oppdaget av en elev, som meldte dette til ansatte ved skolen. Den ansatte skriver følgende i e-posten til IKT Helpdesk i Bergen kommune:

> «Vi har en elev […] som ser svært ivrig i sine forsøk på å komme inn på Bergen kommunes skjulte sider i elevnettet. Han har klart å finne frem oversikt over brukernavn og passord til elevnettet – de gamle før eFeide. Det er ikke så mange som byttet passord enda (ja jeg vet vi er trege på det) men eleven har ikke misbrukt informasjonen han har funnet. Han har fortalt oss at han har funnet dem, og vist det superraskt – du gjør sånn, og sånn, og sånn…. Jeg har ikke mulighet til å henge med når han viser det.
>
> Han har i det siste hatt med seg en minnepenn hvor jeg tror han har et program han har laget hjemme. Han sa til min kollega at det ikke virket, det han prøvde på.
>
> Han har mye god kunnskap om ikt-systemer, og er svært opptatt av koding. Men jeg er bekymret for om han er på vei til «ville veier», slik at kompetansen hans kan bli brukt feil.
>
> Jeg har tatt beslag i den pc-en han brukte siste uke (men er nok pålogget en ny nå). Den bør vel retankes. […] Er det interessant for dere å sjekke loggen til maskinen før det gjøres? Og har dere mulighet til å se på loggfiler på hva han foretar seg.»

Eleven, som her er omtalt, fant at brukernavn og passord til konto med administratortilgang var i mappen som var tilgjengelig for elever. Dermed hadde han mulighet til å se opplysninger om alle brukere i kommunens FEIDE-katalog. Både elevens kontaktlærer og en annen lærer var i telefonisk kontakt med IKT-Helpdesk i forkant av e-posten for å informere om bruddet på personopplysningssikkerheten. Skolens rektor har bekreftet dette.

Eleven logget seg inn i eFeide fem ganger før han varslet skolen om sikkerhetsrisikoen. Første pålogging skjedde 13. mars 2018. Varselet fra eleven inneholdt opplysninger om flere forhold, blant annet om mappen med brukernavn og passord. Meldingen om mappen ble imidlertid ikke fulgt opp videre av ledelsen ved skolen.

Denne mappen har blitt brukt for å flytte data mellom ulike systemer som skolen bruker. Hvert år ved skolestart opprettes det nye brukere. Hver høstferie nullstilles passordene til alle brukerkontoer, slik at alle må lage et nytt passord når skolen begynner etter ferien. Ved passordbytte har ikke tidligere passord blitt sjekket og utelukket til senere bruk. Brukere har derfor hatt mulighet til å bytte tilbake til tidligere brukte passord etter høstferien.

Mellom 22. juni og 30. juli 2018 har noen tatt seg inn i brukeradministrasjonsverktøyet eFeide med en brukerkonto tilhørende Bergen kommune, og endret kontaktinformasjonen knyttet til Bergen kommunes kundeforhold hos Identum. Dette ble oppdaget av Identum mandag 13. august.

Tirsdag 14. august har eleven logget på læringsplattformen Its Learning med kontoen til rektor ved den nevnte skolen. Eleven har sendt en melding til flere personer via FEIDE. Meldingen inneholdt passordet til rektorens konto. Rektor har bekreftet at det ikke var han som logget seg inn på dette tidspunktet, og at det ikke var han som sendte meldingen.

På grunn av funn i sikkerhetslogger ble dette anmeldt til Vest politidistrikt torsdag 16. august. Politiet aksjonerte fredag morgen, og bekrefter at en elev innrømmer å stå bak både endringen i eFeide og meldingen fra rektorens konto. Han har innrømmet overfor politiet at han har gjettet seg til rektorens passord, og logget seg på Its Learning med totalt ti forskjellige kontoer.

Identum iverksatte tiltak etter å ha oppdaget dette, og nullstilte passord for alle administratorkontoer i Bergen kommune da dette ble oppdaget 13. august. Onsdag 15. august ble passord til samtlige kontoer nullstilt.

Identum v/Erik Lithun bekrefter i telefonsamtale med Datatilsynet mandag 10. september at selskapet høsten 2016 var i kontakt med Bergen kommune om bruk av eFeide. 17. mars 2017 sendte Identum et tilbud til Bergen kommune på eFeide med opsjon på bruk av tofaktorautentisering.

Personvernombudet i Bergen kommune har opplyst at det har påpekt behovet for tofaktorautentisering som et nødvendig sikkerhetstiltak for innlogging til eFeide.

Personvernombudet har på telefon opplyst at Bergen kommune har rutiner for tilgangskontroll til eFeide, men at disse ikke ble fulgt i dette tilfellet. Rutinene er i ettertid sendt til Datatilsynet per e-post.

Bergen kommune publiserte som nevnt en pressemelding om saken 15. august. De berørte har også blitt informert pr. brev.

Bergen kommune har, etter at saken ble kjent i media, innført tofaktorautentisering i brukeradministrasjonsverktøyet eFeide for kontoer med administratortilgang til eFeide (teknisk personell). Dette ble implementert fredag 17. august.

3 Regelverket på området

3.1 Hvilket regelverk skal anvendes – spørsmål om lovvalg

Den nye personopplysningsloven (personopplysningsloven 2018), som i § 1 inkorporerer EUs personvernforordning i norsk rett, trådte i kraft 20. juli 2018. Loven opphevet samtidig lov 14.04.2000 nr. 31 om behandling av personopplysninger (personopplysningsloven 2000) og reglene i personopplysningsforskrift 15.12.2000 nr. 1265 om behandling av

personopplysninger (personopplysningsforskriften 2000). På grunn av sakens hendelsesforløp, er det nødvendig å ta stilling til om saken skal vurderes etter personopplysningsloven av 2018 eller personopplysningsloven 2000.

Vi har kommet til at personopplysningsloven av 2018 må anvendes i saken. Dermed kommer også bestemmelsene i personvernforordningen til anvendelse, jf. lovens § 1. Dette gjelder alle sakens sider, også de som gjelder ileggelse av overtredelsesgebyr, jf. også personopplysningsloven § 26 andre ledd og § 33.

Denne saken gjelder brudd på regelverket som har oppstått på et tidspunkt forut for ikrafttredelsen av personopplysningsloven 2018. Regelverksbruddene har imidlertid vært kontinuerlige og har vedvart i tid, og ble oppdaget den 15. august, altså etter ikrafttredelsestidspunktet til den nye personopplysningsloven. De aktuelle hendelsene har med andre ord strukket seg over en lengre periode. Første gang det ble konstatert mangelfulle sikkerhetsrutiner var da dette ble rapportert til IKT Helpdesk 15. mai 2018. På dette tidspunktet gjaldt som personopplysningsloven 2000 og personopplysningsforskriften av 2000. Forskriften §§ 2-6, 2-11, 2-13 og 2-14 regulerte slike forhold som saken omhandler.

De aktuelle forholdene som er til vurdering, har altså oppstått før ikrafttredelsen av personopplysningsloven 2018, men de har vedvart og vært kontinuerlige en tid etter at den nye personopplysningsloven lov trådte i kraft den 20. juli.

Personopplysningsloven 2018 § 33 første ledd nedfeller en særskilt overgangsregel om overtredelsesgebyr som lyder som følger:

> «*Reglene om behandling av personopplysninger som gjaldt på handlingstidspunktet, skal legges til grunn når det treffes vedtak om overtredelsesgebyr. Lovgivningen på tidspunktet for avgjørelsen skal likevel anvendes når dette fører til et gunstigere resultat for den ansvarlige*.»

Når det treffes vedtak om overtredelsesgebyr skal altså spørsmål om lovvalg vurderes ut fra hva som må regnes som *handlingstidspunktet*. Datatilsynets vurdering er at handlingstidspunktet i denne saken er utstrakt i tid – den eller de lovstridige handlingene har oppstått før den 20. juli, men det har dreid seg om, og vil fortsette å dreie seg om, et konstant og kontinuerlig regelverksbrudd helt til den behandlingsansvarlige sørger for å bringe behandlingsaktivitetene i samsvar med regelverkets krav. Ettersom den behandlingsansvarlige ikke har foretatt seg noe for å sørge for å bringe de ulovlige behandlingsaktivitetene til opphør og i samsvar med regelverkets krav før i august i år, må handlingstidspunktet i § 33 anses å være etter ikrafttredelsestidspunktet til den nye personopplysningsloven. Det følger dermed av personopplysningsloven § 33 at denne saken skal vurderes etter personopplysningsloven 2018. Dette er for øvrig også i samsvar med EMK art 7, som viser til hhv. «handlingstidspunktet» og «den tid da [handlingen] ble begått».

Vi viser også til forarbeidene til personopplysningsloven 2018 (Prop. 56 LS (2017-2018) side 196), hvor departementet blant annet uttaler følgende om spørsmål om lovvalg mellom personopplysningsloven 2000 og personopplysningsloven 2018:

«*Utgangspunktet vil være at vedtak hos Datatilsynet og Personvernnemnda vil måtte fattes på grunnlag av de til enhver tid gjeldende materielle regler*».

Det samme følger av Personvernnemndas praksis i saker som ikke gjelder overtredelsesgebyr og som oversendt nemnda før ny lov, men som behandles etter ny lov. Se for eksempel PVN-2018-005 og PVN-2018-006.

På denne bakgrunn vurderer vi det som klart at saker som gjelder løpende eller vedvarende brudd på reglene må vurderes etter personopplysningsloven 2018 og personvernforordningen.

3.2 Reglene i personvernforordningen

Personvernforordningen regulerer alle sider av behandling av personopplysninger. Personvernforordningen artikkel 5 omhandler det som må sies å være kjernen i personvernretten, og artikkelen er helt sentral for tolkningen av forordningens øvre øvrige bestemmelser. Overtredelse av prinsippene i art. 5 kan i seg selv føre til ileggelse av sanksjoner, og det følger av art. 83 nr. 5 at overtredelser av art. 5 er blant de lovovertredelsene som kan resultere i de høyeste overtredelsesgebyrene, dvs. 20 000 000 euro (p.t. ca. 195 millioner NOK) for behandlingsansvarlige eller databehandlere som ikke er å regne som foretak.

Bestemmelsen i art. 5 lyder som følger:

Artikkel 5. Prinsipper for behandling av personopplysninger

1. Personopplysninger skal

a) behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte («lovlighet, rettferdighet og åpenhet»),

b) samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene; viderebehandling for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål skal, i samsvar med artikkel 89 nr. 1, ikke anses som uforenlig med de opprinnelige formålene («formålsbegrensning»),

c) være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»),

d) være korrekte og om nødvendig oppdaterte; det må treffes ethvert rimelig tiltak for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold slettes eller rettes («riktighet»),

e) lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for; personopplysninger kan lagres i lengre perioder dersom de utelukkende vil bli behandlet for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1, forutsatt at det gjennomføres egnede tekniske og organisatoriske tiltak som kreves i henhold til denne forordning for å sikre de registrertes rettigheter og friheter («lagringsbegrensning»),

f) 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»).

2. Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at nr. 1 overholdes («ansvar»).

Som det fremgår av bestemmelsen, gjelder art. 5 nr. 1 bokstav f personopplysningssikkerhet og prinsippet om plikt til å sikre nødvendig integritet og konfidensialitet. Art. 5 nr. 2 knesetter *ansvarsprinsippet*, som fastslår at det er den behandlingsansvarlige som har ansvaret for å overholde personvernprinsippene i art. 5 nr. 1.

Prinsippet i art. 5 nr. 1 bokstav f om integritet og konfidensialitet er nærmere beskrevet og utfylles av mer konkrete bestemmelser i personvernforordningen kapittel IV, se f.eks. artikkel 24 om iverksetting av nødvendige egnede tekniske og organisatoriske tiltak, artikkel 25 om krav til innebygget personvern og personvern som standardinnstilling, med videre.

Reglene om personopplysningssikkerhet fremgår av kapitel IV, avsnitt 2. Her er artikkel 32 sentral. I artikkel 32 nr. 1 bokstav a og b står det:

Artikkel 32. Sikkerhet ved behandlingen

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,

a) pseudonymisering og kryptering av personopplysninger,

b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene

3.3. Særlig om ileggelse av overtredelsesgebyr

Personvernforordningen overlater til medlemsstatene å fastsette om overtredelsesgebyr skal kunne ilegges offentlige myndigheter og organer, jf. artikkel 83 nr. 7. I personopplysnings-loven (2018) § 26 annet ledd er det bestemt at Datatilsynet kan ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 83, jf. artikkel 83 nr. 7.

I forarbeidene til ny personopplysningslov (Prop. 56 LS (2017-2018)) viser departementet til at

> «Datatilsynet i flere saker har ilagt administrative gebyrer mot offentlige organer, og departementet kan ikke se noen grunn til å ikke videreføre en slik adgang for Datatilsynet. Departementet viser også til at høringsinstansene generelt har vært positive til at overtredelsesgebyr skal kunne ilegges mot offentlige myndigheter.»

I personvernforordning artikkel 83 fremgår vilkårene for ileggelse av gebyr. Bestemmelsen inneholder bl.a. en oversikt over hvilke momenter det skal tas hensyn til når det vurderes både hvorvidt overtredelsesgebyr skal ilegges, og hvilke momenter som skal vurderes i forbindelse med utmålingen av gebyrets størrelse. Artikkelen angir også gebyrenes størrelsesorden, og det

fremgår av art. 83 nr. 4 og nr. 5 at maksimumssatsene avhenger av hvilke bestemmelser i personvernforordningen som er overtrådt.

I artikkel 83 nr. 1 og nr. 2 heter det:

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. Avhengig av omstendighetene i hvert enkelt tilfelle skal overtredelsesgebyr ilegges i tillegg til eller istedenfor tiltakene nevnt i artikkel 58 nr. 2 bokstav a)-h) og j). 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,

i) 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,

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

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.

Bestemmelsen 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. Av artikkelens første ledd går det frem at overtredelsesgebyret i hvert enkelt tilfelle skal være virkningsfullt, stå i et rimelig forhold til overtredelsen og virke avskrekkende.

Vi viser også til Personvernrådets retningslinjer vedrørende anvendelse og fastsettelse av overtredelsesgebyr i overensstemmelse med forordningen (EU) 2016/679 (WP 253), hvor

Personvernrådet redegjør for de generelle kriteriene i art. 83 nr. 1, og momentene i art. 83 nr. 2.[3]

4 Datatilsynets vurderinger og begrunnelse for vedtak

Avviksmeldingen har avdekket forhold som utgjør mulige brudd på personvernforordningen artikkel 32 nr. 1:

- Oppbevaring av en åpen og ubeskyttet digital mappe med filer som inneholder brukernavn og passord til informasjonssystemene i grunnskolen i Bergen kommune, i klartekst og på en slik måte at opplysningene er tilgjengelige for alle brukere av informasjonssystemene, dvs. lærere og elever i grunnskolen, er i strid med personvernforordningen art. 32 nr. 1. Dette avviket er lukket.

- Manglende iverksettelse av tofaktorautentisering for pålogging til informasjonssystemene, for å oppnå et nødvendig sikkerhetsnivå for å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene, utgjør et brudd på personvernforordningen artikkel 32 nr. 1

Nærmere begrunnelse for hvorfor vi mener det foreligger brudd på disse bestemmelsene fremgår nedenfor.

4.1 Begrunnelse for vedtak om pålegg om iverksetting av tiltak

Bergen kommune er behandlingsansvarlig for de behandlingene som er omtalt i saken. Identum er i denne sammenhengen å regne som databehandler for Bergen kommune. Datatilsynet mener at det foreligger brudd på bestemmelsen i personvernforordningen artikkel 32 nr. 1, som stiller krav til den behandlingsansvarlige og databehandleren om at det gjennomføres egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.

Den 17. august 2018 innførte Bergen kommune tofaktorautentisering for alle med administratortilgang i eFeide. Slik Datatilsynet ser det er det ikke tilstrekkelig at tofaktorautentisering kun omfatter de med administratortilgang. Bergen kommune må endre alle ansattes pålogging til alle informasjonssystem med personopplysninger om elever, ved at det etableres sterk autentisering (tofaktorautentisering) for pålogging over eksterne nett og på elevnett.

Datatilsynet viser i den forbindelse til at særlig barn har krav på høy beskyttelsesgrad når det behandles opplysninger om dem, se personvernforordningens fortalepunkt 38 hvor det heter:

> *«Barns personopplysninger fortjener et særlig vern, ettersom barn kan være mindre bevisste på aktuelle risikoer, konsekvenser og garantier, samt på de rettigheter de har når det gjelder behandling av personopplysninger.»*

[3] Opprinnelig utarbeidet av Artikkel 29-gruppen, men adoptert av Personvernrådet, se Personvernrådets «Endorsement 1/2018», pkt. 16. Dokumentene er tilgjengelige på https://edpb.europa.eu

4.2 Begrunnelse for vedtak om overtredelsesgebyr

Adgangen til å ilegge overtredelsesgebyr er gitt som et virkemiddel for å sikre effektiv etterlevelse og håndhevelse av personopplysningsloven. Internrettslig er overtredelsesgebyr ikke å anse som en straff, men en administrativ sanksjon. Det må imidlertid antas at overtredelsesgebyr er å anse som straff etter EMK (Den europeiske menneskerettskonvensjonen) artikkel 6, og i samsvar med Høyesteretts praksis, jf. Rt. 2012 side 1556 med videre henvisninger.

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.

Datatilsynet finner det klart at Bergen kommune har behandlet personopplysninger på en måte som er i strid med forordningen artikkel 32, se varsel om vedtak ovenfor.

Som nevnt over gir artikkel 83 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, idet det ses hen til at ileggelse av overtredelsesgebyr i hvert enkelt tilfelle skal være virkningsfull, forholdsmessig og avskrekkende.

Vi har særlig lagt vekt på følgende momenter i vår vurdering av om hvorvidt overtredelsesgebyr skal ilegges:

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 er et resultat av manglende tekniske og organisatoriske tiltak som sørger for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet og integritet, jf. forordningen artikkel 32. Vi viser også til personvernforordningens fortalepunkt 83.

Overtredelsen omfatter over 35.000 lærere og barn i grunnskolen i Bergen kommune. De registrertes brukernavn og passord kan potensielt ha vært eksponert for alle brukerne, i verste fall 35.000 personer. Overtredelsen omfatter i hovedsak barn, som i mindre grad har forutsetninger for å ivareta sine rettigheter og friheter. I tillegg er registrering av opplysninger om barn obligatorisk i grunnskolen i kommunen. Barna kan ikke velge om de vil være på denne plattformen, hvor bl.a. Its Learning inngår, Its Learning er obligatorisk for alle barn.

Uvedkommende kan ha fått tilgang til personopplysninger om mange, både på læringsplattformer, skoleadministrative system mv. Vi viser her til personvernforordningens fortalepunkt 38, hvor det påpekes at barns personopplysninger skal gis et særlig vern.

At barns rettigheter og friheter har vært utsatt gjør overtredelsen ekstra alvorlig, og Datatilsynet har lagt vekt på dette som en skjerpende omstendighet. Datatilsynet har også lagt vekt på at bruken av plattformen er obligatorisk for barna.

Allerede 15. mai meldte skolen fra om bruddet på personopplysningssikkerheten til IKT Helpdesk. Dette var et potensielt avvik som i så fall skulle ha vært meldt inn til Datatilsynet iht. den da gjeldende personopplysningsloven § 13, jf. personopplysningsforskriften 2000 § 2-6. Det ble imidlertid ikke gjort.

Det innmeldte bruddet på personopplysningssikkerheten gjelder perioden 22. juni til 15. august 2018. Bruddet på personopplysningssikkerheten må imidlertid regnes som oppstått fra senest det tidspunkt da skolen meldte dette inn til IKT Helpdesk. Vi bemerker også at dette ikke bare gjelder manglende innføring av tofaktorautentisering, men også mangelfull håndtering av mappe med brukernavn og passord, som lå åpent tilgjengelig. Den aktuelle konteksten tatt i betraktning, ser Datatilsynet på det som alvorlig at slike opplysninger lå åpent tilgjengelig over en lengre periode. Vi viser her til ansvarlighetsprinsippet i artikkel 5 nr. 2, jf. artikkel 5 nr. 1 bokstav f, idet det hviler en særskilt plikt på den behandlingsansvarlige til å overholde prinsippene i artikkel 5.

b) ***hvorvidt overtredelsen ble begått forsettlig eller uaktsomt***

I 2013/2014 hadde Datatilsynet flere kontroller rettet mot skolesektoren i norske kommuner. Etter disse kontrollene ble det konstatert mangler ved tilgangsstyringen for ansattes tilgang til personopplysninger om mange elever. Datatilsynet påla derfor kommunene å ta i bruk sterk autentisering, dvs. tofaktorautentisering, for ansattes tilgang til læringsplattformer og skoleadministrative systemer. Vårt standpunkt ble gjort kjent på våre hjemmesider, og overfor IT-miljøene i kommunene, blant annet gjennom foredrag, tilsyn og andre møter. Vi gjennomførte en stedlig kontroll med Møhlenpris skole i 2013 (Datatilsynets saksreferanse 13/00941), som var spesielt rettet mot bruk av kartleggingsverktøyet School Wide Information System (SWIS). Etter denne kontrollen påla vi Bergen kommune, i egenskap av å være behandlingsansvarlig, å ta i bruk sterk autentisering i forbindelse med bruk av SWIS ved denne skolen.

Datatilsynet har også laget en veileder for bruk av sterk autentisering/tofaktorautentisering, som er tilgjengelig på våre hjemmesider. Der redegjør vi nærmere for hvorfor sterk autentisering er nødvendig, og i hvilke tilfeller slik autentisering er nødvendig.

Identum, som er Bergen kommunes leverandør av eFeide, har opplyst at samtaler om bruk av eFeide startet høsten 2016, og at Identum ga Bergen kommune et tilbud på bruk av eFeide med opsjon på tofaktorautentisering 17. mars 2017. Over ett år senere var opsjonsavtalen ikke benyttet.

For det første har kommunen blitt varslet av sin leverandør om at bruk av tofaktorautentisering var et nødvendig sikkerhetstiltak, se ovenfor. For det andre har personvernombudet i Bergen kommune påpekt kravet for tofaktorautentisering ved bruk av eFeide, uten at ledelsen har gjort det nødvendige for etableringen.

Vi vurderer det som hevet over tvil at Bergen kommune har hatt kunnskap om nødvendigheten for etablering av tofaktorautentisering i eFeide. Ved ikke å ta de nødvendige skrittene, har kommunen handlet klanderverdig. Dette indikerer mangel på bevissthet om hvor viktig det er med nødvendige sikkerhetstiltak, og mangelfull ivaretakelse av ansvarsprinsippet. Dette må betegnes som uaktsomt, og etter vår vurdering er dette en alvorlig grad av uaktsomhet. Vi viser også til at Bergen kommune ikke fulgte opp da den ble kjent med de mulige regelverksbruddene.

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

Det er på det rene at Bergen kommune har rutiner for avvikshåndtering, men at varselet fra ansatte ikke ble sendt videre i systemet.

Da bruddet på personopplysningssikkerheten ble meldt inn fredag 17. august ble tilgang til mappen sperret. I ettertid har kommunen etablert tofaktorautentisering i brukeradministrasjonsverktøyet eFeide for kontoer med administratortilgang til eFeide.

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***

Personvernforordningen har innført en langt høyere grad av ansvarlighet for den behandlingsansvarlige, jf. ansvarlighetsprinsippet i artikkel 5. Bergen kommune har ikke gjennomført tekniske eller organisatoriske tiltak, som lever opp til prinsippene om innebygd personvern, jf. artikkel 25. Datatilsynet finner heller ikke at Bergen kommune har sikret et tilstrekkelig sikkerhetsnivå, jf. artikkel 32. Det kan derfor konstateres at Bergen kommune har utvist dårlig ansvarlighet i forhold til akseptabelt beskyttelsesnivå.

e) ***eventuelle relevante tidligere overtredelser begått av den behandlingsansvarlige eller databehandleren***

I saken mot Bergen kommune og Møhlenpris skole (se under pkt. b) ble det fattet vedtak om at kommunen måtte gjøre bruk av tofaktorautentisering i tilgangsstyringen.

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

Bergen kommune har meldt inn overtredelsen og har vært i dialog med Datatilsynet under sakens gang, uten at det har vært med på å redusere de mulige negative virkningene av overtredelsen.

g) ***kategoriene av personopplysninger som er berørt av overtredelsen***

Vi kan ikke konstatere at særlige kategorier av personopplysninger, slik dette er definert i personvernforordningen artikkel 9, har vært eksponert for uvedkommende. Da overtredelsen omfatter barn viser vi til personvernforordningens fortalepunkt 75, hvor det påpekes at det skal tas særlig hensyn til risikoen knyttet til barns personopplysninger, om behandlingen omfatter en stor mengde personopplysninger og berører et stort antall registrerte.

Opplysninger som har vært tilgjengelig er brukernavn, passord, fullt navn, skoletilhørighet og skoleklasse. I eFeide er det i tillegg mulig å se fødselsnummer og adresse til hver person. Ansatte er også registrert med telefonnummer, som var synlig i eFeide. I tillegg har sikkerhetssvikten medført at potensialet for tilgang til sensitive personopplysninger har vært til stede. Its Learning er et system som er tilgjengelig via eFeide. Her vil det kunne registreres sensitive personopplysninger om bl.a. fravær.

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

Datatilsynet ble først kjent med det aktuelle forholdet gjennom oppslag i media. Datatilsynet ble først varslet om bruddet på personopplysningssikkerheten fra Bergen kommune 15. august 2018.

i) ***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 har ikke tidligere vært gjennomført tiltak overfor Bergen kommune med hensyn til samme saksgjenstand.

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

Ikke relevant for saken.

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***

Datatilsynet har ikke konstatert at Bergen kommune har hatt økonomiske fordeler, eller unngått tap direkte eller indirekte som et resultat av overtredelsen.

I vurderingen av om overtredelsesgebyr skal ilegges, legger Datatilsynet særlig vekt på at overtredelsene betydelig har krenket grunnleggende prinsipper som forordningen verner, jf. forordningen artikkel 5 nr. 1 bokstav f hvor det heter 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»)».*

Datatilsynet legger særlig vekt på at det ikke var etablert tofaktorautentisering i eFeide, til tross for at kommunen hadde kunnskap om nødvendigheten av dette. Datatilsynet vurderer dette som alvorlig. Brukerne av kommunens tjenester har en klar og beskyttelsesverdig interesse mot mangelfulle sikkerhetstiltak hvor konfidensialitet er påkrevd. Dette kan få alvorlige konsekvenser for den enkelte både fordi omgivelsene får tilgang til informasjon som den registrerte ikke selv har valgt å gjøre kjent, og som det er obligatorisk å registrere, men også fordi tilgjengeligheten gjør det uforutsigbart hvor mange som har skaffet seg informasjonen. Allmennpreventive grunner og hensynet til at reglene skal ha effekt og virke

etter sin hensikt, taler da med styrke for at det reageres med et virkemiddel som overtredelsesgebyr.

Datatilsynet kan ikke se at de øvrige momenter som loven fremhever gjør seg gjeldende i nevneverdig grad – verken i skjerpende eller formildende retning.

Datatilsynet er etter dette kommet til at overtredelsesgebyr bør ilegges.

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.»

Departementet skriver videre at de har notert seg bekymringen som enkelte offentlige høringsinstanser har uttrykt, men departementet legger til grunn at det innenfor reglene i forordningen artikkel 83, som også angir de momenter det skal legges vekt på ved utmålingen av administrative gebyrer, ligger rom for et betydelig skjønn med hensyn til størrelsen på gebyret. Departementet uttaler at «[b]eløpsgrensene i forordningen artikkel 83 angir maksimalgrenser for utmåling av administrative gebyrer, mens det ikke er fastsatt noen minimumsgrenser.»

Når det gjelder gebyrets størrelse, skal de samme momenter som ved vurdering av om gebyr skal ilegges, tillegges særlig vekt. De forhold Datatilsynet har pekt på ovenfor taler for et gebyr av en viss størrelse. 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.

Vi har særlig sett hen til at kommunen ikke hadde etablert tofaktorautentisering til tross for kunnskap om at dette var nødvendig. Videre har vi sett på den generelle forventning borgerne skal kunne ha til at kommunale instanser følger de regler som er gitt, og særlig de som gir enkeltindivider rettigheter som er ment å være en beskyttelse mot utlevering av denne typen opplysninger.

Signalvirkningen av denne saken, de allmennpreventive hensyn, mener vi er tydelige. Det er viktig at slike hendelser ikke inntreffer, og at alle offentlige instanser som behandler innbyggernes personopplysninger og opplysninger om sårbare personer slik som barn, må være seg sitt ansvar bevisst.

Mangelfulle rutiner har ofte som konsekvens at risikoen for feil øker. I denne saken har svake rutiner og manglende etterlevelse av rutinene faktisk hatt en reell konsekvens som også tilsier en skjerpet reaksjon.

Det er også et moment av betydning at Bergen kommune er Norges nest største kommune målt i antall innbyggere. Videre er det oppgitt i Bergensavisen

(https://www.ba.no/nyhet/okonomi/politikk/bergen-kommune-1-1-milliard-kroner-i-overskudd/s/5-8-742795) at Bergen kommune hadde et betydelig overskudd i 2017, på 1,1 milliard norske kroner. Dette har vi også sett hen til.

Etter en totalvurdering av saken, 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 **1.600.000 NOK** anses som riktig.

5 Avsluttende merknader

Frist for gjennomføring av pålegget

Datatilsynet gir frist for gjennomføring av pålegget til **30. april 2019.** Kommunen må innen nevnte dato bekrefte skriftlig overfor Datatilsynet at pålegget er gjennomført. Med mindre annet er særskilt angitt kreves det ikke ytterligere dokumentasjon på at pålegget er gjennomført. Det gjøres imidlertid oppmerksom på at Datatilsynet vil kunne foreta en etterkontroll av dette.

Klageadgang
Dette vedtaket kan påklages i henhold til forvaltningslovens bestemmelser. Eventuell klage må fremsettes overfor Datatilsynet **innen tre uker** etter at vedtaket ble mottatt. En eventuell klage oversendes Personvernnemnda for klagebehandling. Datatilsynet gjør i den forbindelse oppmerksom på retten til innsyn i sakens dokumenter, jf. forvaltningsloven § 18.

Dersom dere har spørsmål kan dere kontakte Knut Kaspersen på telefon 22 39 69 07.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Knut Kaspersen
fagdirektør