Datatilsynet

BERGEN KOMMUNE BYRÅDSAVDELING FOR
FINANS, NÆRING OG EIENDOM
Postboks 7700 Lønnskontoret

5020 BERGEN

Deres referanse	Vår referanse	Dato
2019/70422-70	20/02181-3	03.09.2020

Vedtak om overtredelsesgebyr - Bergen kommune - Melding om avvik i Vigilo

1. Innledning

Vi viser til korrespondanse i forbindelse med brudd på personopplysningssikkerheten i Bergen kommune, første gang meldt til Datatilsynet den 2. oktober 2019 (vårt ref.nr. 19/02985-1), tilleggsmelding av 3. desember 2019 (19/02985-8), Bergen kommunes redegjørelse til Datatilsynet (19/02985-6), internkontrollrapport fra Byrådsleders avdeling – Seksjon for internkontroll av 2. desember 2019 (19/02985-9), varsel om overtredelsesgebyr av 15. mai 2020, svarbrev på varsel om overtredelsesgebyr av 30. juni 2020 (20/02181-2) og den øvrige korrespondansen i saken.

Vi viser også til melding om brudd på personopplysningssikkerheten fra Bergen kommune av 11. november 2019 (19/03476-1).

Vi har behandlet sakene med ref.nr. 19/02985 og 19/03476 sammen. Grunnen til dette er at begge de innmeldte hendelsene handler om sperret adresse i Folkeregisteret og ivaretakelse av konfidensialitet (se pkt. 3 om adressesperre). Begge sakene omhandler bruk av Vigilo i skolene og er omtalt i den nevnte interkontrollrapporten fra byrådsleders avdeling.[1] I behandlingen av denne saken har vi lagt til grunn de faktiske opplysningene i internkontrollrapporten, og i det følgende vil vi fortløpende henvise til denne.

Vi har i dette vedtaket ikke behandlet avviket om kommunikasjon i det som viste seg å være en «gruppe-chat». Dette avviket er omtalt i internkontroll-rapporten, men kan ikke regnes som et avvik som kommunen bærer ansvaret for. Tjenesten «gruppe-chat» var ikke bestilt av kommunen. Hendelsen var en kombinasjon av at ny funksjonalitet ble satt i produksjon uten at dette ble kommunisert til behandlingsansvarlig og brukerfeil («svar alle» ble brukt i stedet for «svar»).

[1] Se internkontrollrapporten av 2. desember 2019 side 13.

I svarbrev av 30. juni 2020 ber kommunen Datatilsynet belyse forholdet mellom behandlingsansvarliges og databehandlers ansvar i saken. Datatilsynet finner det naturlig å ta dette opp i eget brev med Vigilo.

I ovennevnte svarbrev opplyser kommunen at de aksepterer overtredelsesgebyret pålydende 3 000 000 – 3 millioner – kroner.

2. Vedtak om overtredelsesgebyr
I medhold av personopplysningsloven § 26 andre ledd kan Datatilsynet ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 58 nr. 2 bokstav i), jf. artikkel 83 nr. 7.

Bergen kommune pålegges i medhold av personopplysningsloven § 26 andre ledd, jf. personvernforordningen artikkel 83, å betale et overtredelsesgebyr til statskassen på ***3 000 000*** *– tre millioner – kroner for å ha unnlatt å gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et egnet sikkerhetsnivå med hensyn til risikoen, og sikring av vedvarende konfidensialitet og integritet, jf. personvernforordningen artikkel 5 nr. 1 bokstav f, og personvernforordningen artikkel 32 nr. 1 bokstav b.*

Varselet om overtredelsesgebyr er nærmere begrunnet under pkt. 5 og 6 i dette brevet.

3. De faktiske forholdene
Internkontrollrapporten inneholder en beskrivelse av de faktiske forholdene i saken, se rapportens kapittel 4, side 10, om personvern og informasjonssikkerhet, for en beskrivelse av bruddet på informasjonssikkerheten. Rapporten er i sin helhet tilgjengeliggjort på kommunens hjemmeside, og vi viser derfor til den:

https://www.bergen.kommune.no/hvaskjer/barnehage-og-skole/har-mottatt-rapport-etter-intern-gjennomgang-av-avviket-i-vigilo

I internkontrollrapporten (på side 13) er det oppgitt at det i perioden august – november 2019 har inntruffet flere hendelser som kommunen karakteriserer som «avvik». Disse avvikene er i rapporten beskrevet slik:

- *E-poster med skoletilhørighet til foreldre uten foreldreansvar*
- *Tilgang til opplysninger om barn uten å ha et foreldreansvar*
- *Kommunikasjon i det som viste seg å være en "gruppe-chat"*

I internkontrollrapporten, på side 13, oppgir kommunen at det totalt var registrert 10 avvik i perioden august til 21. november 2019, som gjelder kommunikasjonsløsningen i Vigilo:

- *Fire av avvikene gjelder gruppemeldinger i kommunikasjonsmodulen, hvor meldinger som er ment for én person er mottatt av flere personer.*
- *Fem avvik gjelder urettmessig innsyn for personer uten foreldreansvar.*
- *Ett avvik gjelder en elev som fikk fars navn inn i sin e-post.*

To av disse avvikene gjelder urettmessig innsyn der barnet bor på fortrolig adresse. Ett av avvikene gjelder utsending av adresseliste til hele klassetrinnet hvor en foresatt er oppgitt med teksten «fortrolig adresse».

Dette siste avviket er meldt til Datatilsynet (19/03476). Ikke alle avvikene er meldt til Datatilsynet, men kan sies å inngå som en del av det innmeldte bruddet (19/02985). Avviket som er meldt inn til Datatilsynet i sak 19/02985 var ikke definert med gradert adresse, men det var angitt ukjent adresse.

Ni av avvikene er oppdaget av foreldre ved skolen, som deretter varslet kommunen. Ett av avvikene ble oppdaget av en skole ved gjennomgang av opplysninger om foresatte.

Hendelsesforløpet i de aktuelle avvikene er som følger:

Sak19/3476
Kontaktliste ble sendt ut til foresatte på ett klassetrinn (113 foresatte). Kontaktlisten inneholdt teksten «fortrolig adresse» i adressefeltet til en foresatt (selve adressen er ikke distribuert). Kontaktlærer var ikke kjent med at den foresatte hadde fortrolig adresse eller at teksten «fortrolig adresse» gikk frem av adresselisten. Selv om mottakere av klasselisten ikke fikk oppgitt den aktuelle adressen, ville konfidensialiteten til den berørte være brutt ved at navnet på skolen kom fram.

Sak 19/2985
3. september tok en forelder kontakt med personvernombudet i Bergen kommune med ønske om innsyn i informasjonen som var lagret i Vigilo. Vedkommende hadde blitt oppmerksom på at person A var registrert i systemet med en relasjon til et barn, til tross for at A ikke hadde foreldreansvar for dette barnet. Med bakgrunn i denne hendelsen, ble det oppdaget at det var en automatikk i at foresatte uten foreldreansvar fikk tilgang til informasjon om barnet, via den nye digitale løsningen. Informasjon om barn og foresatte er overført fra gammelt system. For å få inn nye barn i systemet, ble det søkt til Skatteetaten om å benytte standard 0-16 folkeregisteruttrekk.[2] Dette folkeregisteruttrekket ble levert av EVRY. Opplysningene ble hentet inn for å oppdatere registrene med informasjon om nye barn og foresatte. Fra dette uttrekket fikk Bergen kommune inn informasjon om barn og deres biologiske foreldre (evt. adopsjonsforeldre), og informasjon om foreldreansvar.

Dette er en adressesperre som ikke omfattes av kodene 4, 6 og 7 (se nedenfor om adressesperre), men har vært tilbudt kommunene fra Folkeregisteret i en periode fra 2001 til 2019. Denne tjenesten er stoppet av Skatteetaten, ettersom etaten har konkludert med at det ikke foreligger lovhjemmel til å utlevere denne typen opplysninger, se nærmere nedenfor i Skatteetatens redegjørelse i e-post av 30. oktober 2019.

Adressesperre
Saken gjelder urettmessig innsyn i opplysninger om personer som har fortrolige eller strengt fortrolige adresser (adressesperre). Utgangspunktet er lov om folkeregistrering

[2] Gjelder uttrekk på barn 0-16 år.

(folkeregisterloven) kap. 10[3]. Folkeregisterloven § 10-4 bestemmer at registrerte «opplysninger som er gradert i medhold av beskyttelsesinstruksen[4], skal sperres i Folkeregisteret». Kode 4, 6 og 7 er koder som brukes i Folkeregisteret for å skille tilfellene fra hverandre. Kode 6 er den alvorligste og klassifiseres som strengt fortrolig. For kode 6 gis det aldri ut noen adresse. Fortrolig adresse kode 7 kan gis til offentlige myndigheter som har lovhjemmel. Tilsvarende gjelder for kode 4 som for barn vil være barneverninstitusjon eller asylmottak.

En opplysning som er gradert etter folkeregisterloven kan nedgraderes. Dette må gjøres av den etat som har gradert opplysningen, jf. beskyttelsesinstruksen § 5. Selv om opplysninger er nedgradert, kan det likevel være et beskyttelsesbehov for de berørte, som må ivaretas av kommunen.

Personvernombudet i Skatteetaten, har i e-post av 30. oktober 2019 opplyst følgende:

> ***«Begrepet foresatte***
> *Kommunene har hatt behov for informasjon om foresatte for å vurdere hvem som kan opptre på vegne av barnet. Begrepet foresatte finnes ikke i folkeregisteret, og er ikke definert i folkeregisterloven og -forskrift. For å dekke kommunenes behov, har Skatteetaten via vår distributør Evry distribuert et felt som heter foresatte til skoler og tannhelsetjeneste siden 2002. Informasjonen ble opprettet etter ønske fra kommunene, og modelleres på bakgrunn av informasjon om barnet og barnets bostedsadresse, hvor den eller de foreldrene som har samme bostedsadresse omtales som foresatte. Det var også for å avhjelpe at kommuner ikke hadde hjemmel i opplæringsloven til å få utlevert informasjon om foreldreansvar. I 2017 fikk kommunene hjemmel til å hente inn informasjon om foreldreansvar, men mange kommuner har ikke benyttet seg av denne muligheten.*
>
> *Det at Skatteetaten har distribuert informasjon om hvem som er foresatte kan ha skapt forvirring hos kommunene.*
>
> *Tiltak for å stoppe all distribusjonen av foresatt-informasjon har vært under gjennomføring siden mars da vår vurdering er at vi ikke kan distribuere det som må anses som et konstruert felt som ikke er dekket av folkeregisterloven. Inntil distribusjonen er avviklet på en forsvarlig måte har Skatteetaten iverksatt en kortsiktig løsning, hvor foresatt-informasjon fjernes for barn med de aktuelle adressekodene 4, 6 og 7. Vi vil informere kommunene og systemleverandørene om endringene.*
>
> ***Innhold i folkeregisteret***
> *Folkeregisteret inneholder kun informasjon om hvem som er foreldre og hvem som har foreldreansvar. Hvem som har foreldreansvar tilsvarer ikke hvem som har daglig omsorg for barnet. Folkeregisteret har ikke informasjon om daglig omsorg.*

[3] Lov om folkeregistrering av 2016-12-09-88
[4] Beskyttelsesinstruksen av 1972-03-17-3352

Opplysninger om barnevernstiltak, besøksforbud og liknende er ikke inkludert i folkeregisteret. Dette endres ikke med modernisert folkeregister. Dette er informasjon som skolene får fra andre kilder, og som kan påvirke foreldrenes rettigheter overfor egne barn. Disse opplysningene må kommunen selv føre inn manuelt i sitt system. Kommunen og deres systemleverandør er ansvarlig for at opplysninger som er registrert manuelt ikke blir overskrevet ved en folkeregisteroppdatering.

Alle kommuner har fått informasjon om hvilke barn som har skjermingsbehov knyttet til adresse. Informasjonen om skjermet adresse utløser en plikt hos kommunen, som behandlingsansvarlig, til å gjøre nærmere undersøkelser.»

Bruddet på informasjonssikkerheten berører tre familier, med til sammen sju barn, som har bopel med sperret adresse. De berørte familiene er blitt kontaktet av Bergen kommune. Dernest har 477 foresatte som ikke skulle hatt tilgang til informasjon om barnet, mottatt en e-post med navn på barnets skole. Ved innlogging i Vigilo har disse foresatte hatt mulighet til å få tilgang til følgende opplysninger: Barnets navn, skole/barnehage, klasse, ansatte ved skolen, navn på andre foresatte til barnet. I denne gruppen har en foresatt som tidligere har hatt adressesperre kode 7, endret navn for å unngå at den andre forelderen får informasjon som gjør at han får vite hvor mor og barn oppholder seg.

Årsakene til bruddet på personopplysningssikkerheten
Bergen kommune (prosjektet) hadde ved oppstart av kommunikasjonsmodulen Vigilo i august 2019 manglende kunnskap om hvordan løsningen fungerte, se internkontrollrapporten pkt.2, hvor det heter:

«Prosjektet skjønte ikke før i september hvor kritisk importen fra Det sentrale folkeregisteret (DSF) var. De fanget ikke opp leverandørs informasjon om dette på samling i juni, og hadde ikke grunnlaget for å sette inn nødvendige tiltak.»

De risikovurderingene som var gjort var mangelfulle og inneholdt ingen vurdering av risiko knyttet til behandling av informasjon om personrelasjoner (foresatte og barn med spesifikke koder). I internkontrollrapporten pkt. 2 heter det:

«Prosjekteier og styringsgruppe har ikke tatt nødvendige grep for å redusere prosjektets risiko knyttet til innføringen av kommunikasjonsmodulen. Endringen i prosjektplanen i desember 2018 som medførte parallell innføring av Vigilo i både barnehager og skoler har, sammen med sene leveranser fra leverandør, gjort at prosjektet ikke har utført nødvendig kvalitetssikring av kommunikasjonsløsningen.»

Videre heter det i internkontrollrapporten pkt. 6.3:

«Det er et krav at systemeiere skal utarbeide en risikovurdering for personvernkonsekvenser. Seksjon for internkontroll har fått tilgang til en slik risikovurdering for hele Vigilo-løsningen datert 1. april. Risikovurderingen er slik vi har kunnet finne, ikke behandlet i prosjektets styringsgruppe, og synes heller ikke revidert av prosjektet. Vi har fått opplyst at risikovurderingen datert 1. april er gjort

med utgangspunkt at det var Fellesdata som skulle benyttes som kilde for Vigilo. Ikke DSF slik løsningen ble.

I styringsgruppens møte 2. april ble det lagt til grunn at det skal lages utkast til notat vedrørende risikofaktorer. Slik vi har fått opplyst ble det ikke gjort en risikovurdering av selve løsningen, men det ble gjort en risikovurdering av pålogging til løsningen. Risiko for selve løsningen ble kun diskutert muntlig».

Informasjonen som skulle kvalitetssikre personrelasjoner og bruke løsningen kom sent og var mangelfull. I internkontrollrapporten pkt. 2 heter det:

«Skolene var ikke istandsatt til å kvalitetssikre data vedrørende foresatte i løsningen. En lenge varslet retningslinje for personvern og informasjonssikkerhet er i november enda ikke sendt ut fra BBSI [Byrådsavdelingen for Barnehage, Skole, Idrett] *sentralt til skolene.»*

Det heter videre om dette i internkontrollrapporten pkt. 6.5:

Første fil fra DSF ble lest inn i Vigilo med barn og foresatte 12. mai. Det er i epost fra prosjektleder til prosjekteier opplyst om at «epost om å kontrollere ble sendt ut til alle enheter fra prosjektet». Slik Seksjon for internkontroll kan finne, ble det ikke sendt ut noen epost om å kvalitetssikre persondata til skolene i mai eller i juni».

Innføringen av Vigilo skulle ha vært utsatt til den nødvendige kvalitetssikringen forelå, fremgår det av internkontrollrapportens pkt. 2 på side 5, hvor det heter:

«Beslutning i april og juni om å tilby løsningen ut til alle skoler, skulle ikke vært fattet. Vi mener at grunnlaget for beslutningene var mangelfullt, og at utrullingen skulle vært utsatt.»

Datatilsynet er ikke tillagt myndighet til å håndheve beskyttelsesinstruksen, men ønsker å påpeke at denne instruksen er sentral i vurderingen av behandlingen av graderte adresser fra Folkeregisteret, bl.a. ved bestemmelser om bruken av opplysningene, se § 7.

4 Reglene i personvernforordningen

De aktuelle rettsreglene i denne saken er:

Artikkel 5. Prinsipper for behandling av personopplysninger

1. *Personopplysninger skal*
   [...]
   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»).

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,

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.

Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

5 Lovovertredelsen

De innmeldte bruddene på personopplysningssikkerheten gjelder mangelfull sikring av vedvarende konfidensialitet i behandlingssystemet Vigilo. Personopplysninger som skulle ha vært skjermet, har vært tilgjengelige for uvedkommende. I et tilfelle ble en kontaktliste med opplysning om «fortrolig adresse» distribuert til foresatte på ett klassetrinn. I et annet tilfelle fikk foresatte uten foreldreansvar tilgang til informasjon om barn. Dette er i strid med personvernforordningen artikkel 32 nr. 1 bokstav b), jf. artikkel 5 nr. 1 bokstav f). Vi viser her til pkt. 3 i dette brevet, og oppsummeringen på side 5 i internkontrollrapporten.

Det har ikke vært gjennomført en tilfredsstillende risikovurdering ved innføring av kommunikasjonsmodulen Vigilo. Blant annet er det ikke foretatt en risikovurdering for bruken av personrelasjoner ved adressesperre. En av årsakene til bruddet på informasjonssikkerheten er at det ikke har vært iverksatt tilstrekkelige tiltak for å begrense risikoen. Se nærmere under pkt. 3.

Det er heller ikke kommunisert informasjon om foresatte og barn med spesifikke koder nedover i systemet. Det er gitt enkelte signaler om slik informasjon, bl.a. på samling på Gardermoen 13. juni 2019, og «Prosedyre – 20.06.2019 – Nytt skolesystem, Vigilo», se internkontrollrapporten på side 16. Disse prosedyrene ble ikke fulgt opp før innfasingen av kommunikasjonsmodulen Vigilo ved skolestart. Dette utgjør et brudd på artikkel 24 nr. 2. Internkontrollrapporten omtaler dette under pkt. 9 på side 27.

Bruddene omfatter barn som ikke skal kontaktes av den andre forelderen. Det er derfor viktig at disse har en adressesperre som fungerer. I verste fall kan manglende adressesperre få konsekvenser for liv og helse. At Bergen kommune ikke har gjennomført en tilstrekkelig risikovurdering og ikke kommunisert tydelige rutiner nedover i systemet er et brudd på ansvarsprinsippet i artikkel 5 nr. 2.

6 Vurdering av personvernforordningens regler om overtredelsesgebyr

6.1 Generelt 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. 7.

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).

For foretak er skyldvurderingen særegen. I forvaltningsloven § 46 første ledd heter det:

«Når det er fastsatt i lov at det kan ilegges administrativ sanksjon overfor et foretak, kan sanksjonen ilegges selv om ingen enkeltperson har utvist skyld».

I Prop. 62 L (2015-2016) side 199 uttales det om § 46:

«Formuleringen om at 'ingen enkeltperson har utvist skyld' er hentet fra paragrafen om foretaksstraff i straffeloven § 27 første ledd og skal forstås på samme måte. Ansvaret er derfor som utgangspunkt objektivt».

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.

6.2 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,

Ved oppstart av kommunikasjonsløsningen Vigilo er det påvist at prosjektgruppen hadde mangelfull kunnskap om hvordan løsningen fungerte (se internkontrollrapporten pkt. 2). Prosjektgruppen ble opprettet i forbindelse med etableringen av Vigilo i det skoleadministrative system i Bergen kommune.

Den risikovurderingen som er gjort er ikke tilstrekkelig. Etter vår vurdering, har kommunen i for stor grad hatt fokus på pålogging til løsningen, og i for liten grad på funksjonaliteten i løsningen. Datatilsynet har forstått det slik at risikoen ved funksjonaliteten er blitt diskutert muntlig. Ved at denne delen av risikovurderingen ikke er nedfelt skriftlig, vil den ikke kunne etterprøves. Det vises her til internrapporten, bl.a. på side 27.

Datatilsynet konstaterer at det ikke er gjennomført en risikovurdering av konsekvensene for personrelasjonene til de som har adressesperre. Datatilsynet finner det lite tvilsomt at behandling av denne type personopplysninger vil kunne medføre fare for liv og helse for de berørte.

Prosjektgruppen har heller ikke hatt tilstrekkelig kunnskap om at filen fra Folkeregisteret som ble lest inn i Vigilo 12. mai inneholdt opplysninger om foresatte uten forelderansvar. Vigilo informerte kommunen om dette i juni 2019, men kommunen fulgte ikke opp. Først etter at avviket ble konstatert, varslet Bergen kommune fra til Vigilo om at fortrolige og strengt fortrolige adresser skulle fjernes fra fremtidige oppdateringer.

Det må også betegnes som svært alvorlig at en klasseliste inneholdende opplysning som indirekte kunne føre til at en fortrolig adresse ble kjent av uvedkommende (en fortrolig adresse er distribuert på et helt klassetrinn (113 foresatte)).

Det at avvikene i 9 av 10 tilfeller er oppdaget av berørte selv tyder på dårlig internkontroll, og er inntrykk av at Bergen kommune ikke hadde oversikt over risikoen ved å ta i bruk Vigilo.

b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt

Vi vurderer det som hevet over tvil at Bergen kommune har hatt kunnskap om nødvendigheten av å etablere organisatoriske og tekniske tiltak i systemet. Ved å ikke ta de nødvendige skrittene, har Bergen kommune handlet grovt uaktsomt.

Datatilsynet finner at det er en klar sannsynlighetsovervekt for at Bergen kommune har overtrådt artiklene 5, 24, og 32 i personvernforordningen.

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

Bergen kommune har arbeidet sammen med Vigilo for å få på plass en funksjonalitet i kommunikasjonsløsningen som vil medføre at bruddet på personopplysningssikkerheten blir lukket.

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 klar plassering av ansvaret for å oppfylle dette regelverkets krav hos den behandlingsansvarlige, jf. ansvarsprinsippet i artikkel 5 nr. 2. Bergen kommune har ikke sikret at kommunikasjonsløsningen Vigilo hadde nødvendig funksjonalitet for beskyttelse av adresser hvor konfidensialitet var nødvendig. Det kan derfor konstateres at Bergen kommune har utvist mangelfull ivaretakelse av ansvar for å sikre at løsningen var i samsvar med personvernforordningen.

Datatilsynet vil påpeke at det er Bergen kommune som er behandlingsansvarlig for personopplysningene som er benyttet i kommunikasjonsløsningen Vigilo, og skal sørge for konfidensialitet i løsningen. Kommunen har et tydelig og selvstendig ansvar for dette, selv om det kommer fram at Vigilo som leverandør kunne og burde ha informert kommunen om kritiske punkter i løsningen og uttrekk av data fra Folkeregisteret. Dette kommer tydelig fram i dokumentasjon fra kommunen, bl.a. i internkontrollrapporten på side 7 hvor det heter *«at Vigilo som leverandør på en langt bedre måte skulle informert kommunen om kritiske punkter i løsningen og uttrekk av data fra Det sentrale folkeregister».*

I internkontrollrapporten på side 7 står det at *«risikostyringen i prosjektet synes mangelfull og usystematisk, og at risikovurderingen av personvern og informasjonssikkerhet fra april ikke synes revidert».*

Slik Datatilsynet ser det, har mangelfull opplæring av personell som skal behandle personopplysninger fra Folkeregisteret medført at man ikke i tilstrekkelig grad har tatt problemet med adressesperre på alvor. Personer som har en adressesperre har en sterk forventning om at slike opplysninger behandles med den største grad av konfidensialitet. I de alvorligste tilfellene hvor opplysningene ikke er blitt behandlet med den konfidensialitet som er nødvendig, vil dette kunne medføre fare for andre personers liv og helse.

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

Det kan ikke konstateres tidligere relevante overtredelser.

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

Datatilsynet har hatt jevnlig kontakt med Bergen etter at bruddet på personopplysningssikkerhet ble meldt inn høsten 2019.

g) kategoriene av personopplysninger som er berørt av overtredelsen

Det er opplysninger om adressesperre som har vært berørt av overtredelsen. Se nærmere pkt. 3.

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

Datatilsynet fikk kunnskap om dette gjennom innmeldt brudd på personopplysningssikkerheten 2. oktober 2019.

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

Brudd på atferdsnormer har ikke vært et tema i forbindelse med dette avviket.

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 direkte eller indirekte tap som et resultat av overtredelsen.

6.3 Oppsummering og konklusjon

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, artikkel 24 og artikkel 32.

Datatilsynet legger særlig vekt på at Bergen kommune ikke har kommunisert i organisasjonen retningslinjer for å etablere konfidensialitet av opplysningene om adressesperre. Datatilsynet vurderer dette som alvorlig. De berørte har en klar og beskyttelsesverdig interesse i at personopplysninger om adressesperre blir behandlet konfidensielt. 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.

Vi har etter dette kommet til at overtredelsesgebyr bør ilegges.

7 Gebyrets størrelse
De forhold som vi 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 må gebyrets størrelse stå i et rimelig forhold til overtredelsen og virksomheten, jf. personvernforordningen art. 83 nr. 1.

Vi har særlig sett hen til at Bergen kommune har behandlet opplysninger om adressesperre i strid med lovfestede krav og forpliktelser som skal ivareta de registrertes behov for beskyttelse. Borgerne må kunne forvente at offentlige organer følger de regler som er gitt, ikke minst når de samme reglene skal beskytte individets liv og helse. Datatilsynet viser også til artikkel 5 nr. 2 som påpeker det særlige ansvar den behandlingsansvarlige har for å påse at artikkel 5 nr. 1 bokstav f) overholdes.

At det er barn med et særlig beskyttelsesbehov som er rammet, gjør denne saken særlig alvorlig.

Et gebyr i denne saken vil etter vår vurdering kunne ha en betydelig allmennpreventiv virkning. Vi har lagt til grunn at gebyret i denne saken vil være et signal til Bergen kommune, og til andre kommuner, om at personopplysninger om personer med et særlig beskyttelsesbehov må vernes, og at slike personopplysninger blir behandlet i samsvar med de kravene som personopplysningsloven og personvernforordningen oppstiller.

Etter en totalvurdering av saken, og kriteriene i forordningen artikkel 83, har vi kommet til at et overtredelsesgebyr på **3.000.000 kroner** vil være å anse som passende.

8 Inndrivelse av overtredelsesgebyr
Overtredelsesgebyret forfaller til betaling fire uker etter at vedtaket er endelig, jf. personopplysningsloven (2018) § 27. Vedtaket er tvangsgrunnlag for utlegg. Inndrivelse av kravet vil bli gjennomført av Statens innkrevingssentral.

9 Klageadgang
Dere kan klage på vedtaket. En eventuell klage må sendes til oss **innen tre uker** etter at dette brevet er mottatt, jf. forvaltningsloven §§ 28 og 29. Dersom vi opprettholder vårt vedtak, vil vi sende saken til Personvernnemnda for klagebehandling, jf. personopplysningsloven § 22.

10 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.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Knut Brede Kaspersen
juridisk fagdirektør

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer