Barn- och utbildningsnämnden i Östersunds kommun

Diarienummer:
IMY-2023-1647

Ert diarienummer:
BOUN 00070-2023

Datum:
2023-11-28

Beslut efter tillsyn enligt dataskyddsförordningen - Barn- och utbildningsnämnden i Östersunds kommun

Integritetsskyddsmyndighetens beslut

Integritetsskyddsmyndigheten konstaterar att Barn- och utbildningsnämnden i Östersunds kommun (nämnden) brustit i sin skyldighet enligt artikel 35.1 i dataskyddsförordningen[1] att genomföra en konsekvensbedömning innan tjänsten Google Workspace for Education (Google Workspace) började användas i 24 av kommunens skolor hösten 2020.

Integritetsskyddsmyndigheten beslutar med stöd av 6 kap. 2 § dataskyddslagen[2] och artiklarna 58.2 och 83 i dataskyddsförordningen att Barn- och utbildningsnämnden i Östersunds kommun ska betala en administrativ sanktionsavgift på 300 000 (trehundratusen) kronor för överträdelsen av artikel 35.1 i dataskyddsförordningen.

Redogörelse för tillsynsärendet

Integritetsskyddsmyndigheten (IMY) har inlett tillsyn mot nämnden i syfte att granska om nämnden brustit i sin skyldighet enligt artikel 35.1 i dataskyddsförordningen att genomföra en konsekvensbedömning innan tjänsten Google Workspace började användas i 24 av kommunens skolor under hösten 2020.

Nämnden har i yttrande till IMY den 1 mars 2023, som kompletterades den 23 mars 2023, i huvudsak uppgett följande.

Under 2014 genomförde Regionförbundet i Jämtlands län en PUL-bedömning och riskanalys av Google Apps for Education, numera Google Workspace for Education. Sammanfattningsvis konstaterades att riskanalysen inte påvisade tillräckliga risker som kunde motivera att verksamheten skulle avstå från att använda molntjänsten. I maj 2020 fattade kommunen beslut om att migrera tjänsten till en egen domän och i juni 2020 startades tjänsten upp i kommunens egna IT-miljö. Nämnden har efter migreringen konstaterat att hanteringen brustit i fråga om upprättande av en ny

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[2] Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

konsekvensbedömning samt risk- och sårbarhetsanalys. Trots att bedömningen i och med migreringen resulterade i samma risker som vid analysen 2014 borde dokumentation ha upprättats utifrån gällande lagstiftning och den omständigheten att tjänsten flyttats till en egen domän. Nämnden har påbörjat en utbildningsinsats för systemadministratörer på IT-enheten som arbetar specifikt med tjänsten. Vid tidpunkten för nämndens yttrande hade utbildningen kommit halvvägs och det kunde redan då konstateras att tjänsten inte skötts enligt de instruktioner som nämnden fått. När utbildningen slutförts är nästa steg i åtgärdsplanen att genomföra en audit av tjänsten för att klarlägga vilka säkerhetsbrister som finns i systemet och därmed få ett underlag för vilka åtgärder som måste vidtas. Auditen är en del av konsultationen i den konsekvensbedömning som påbörjats. Eftersom auditen inte är färdigställd är konsekvensbedömningen inte heller det.

Google Workspace har använts i Östbergsskolan och i 23 skolor till i Östersunds kommun. Nämnden är personuppgiftsansvarig för behandlingen av personuppgifter vid användandet av tjänsten i dessa skolor. Google Workspace har använts för undervisning och kommunikation. Personalen delar ut planering och uppgifter till elever och elever ges möjlighet att lämna in skoluppgifter. Under pandemin har även funktionen Meet använts i viss utsträckning för att möjliggöra fjärrundervisning. Tjänsten används även för kommunikation mellan pedagoger och elever i syfte att kunna ge återkopplingar rörande skoluppgifter om exempelvis något saknas, behöver utvecklas, kompletteras eller liknande. Inga summativa bedömningar eller betyg lämnas genom tjänsten. Tjänsten används även för kommunikation mellan elever gällande skoluppgifter. Viss kommunikation kan även bestå av mer generell information till elever rörande lektioner.

Personuppgifter i form av förnamn, efternamn, e-postadress, klasstillhörighet och grupptillhörighet behandlas i tjänsten. I tjänsten behandlas uppgifter om 5 945 elever och 1 303 anställda. Ansvarig klasslärare kan bjuda in vårdnadshavare, som själv väljer om de vill acceptera eller neka inbjudan, till tjänsten för att ta del av klassuppgifter och veckosammanställningar. Den nuvarande tjänsten startades upp till skolstarten 2020, läsåret 2020/2021.

Nämnden genomförde inte en konsekvensbedömning inför införandet av tjänsten, men den har påbörjats och nämnden avvaktar nu konsultation (audit). Den påbörjade konsekvensbedömningen innefattar också frågan om användningen av tjänsten innebär en överföring av personuppgifter till ett tredje land (dvs. ett land utanför EU/EES).

Nämnden har i samband med slutkommunicering i ärendet inkommit med yttrande daterat den 12 september 2023 och uppgett bland annat följande. Den audit som vid senaste yttrandetillfället planerades att genomföras, som en del av konsultationen i konsekvensbedömningen, har slutförts. De säkerhetsbrister som framkommit i auditen har kommunen arbetat med att åtgärda. Utifrån att auditen påvisat många risker, har behovet varit stort att försöka arbeta fram lösningar så effektivt som möjligt, utan att kvalitén och säkerheten i arbetet påverkas. Många av åtgärderna är redan på plats. Nämnden har exempelvis tecknat avtal med Google om utökad licens, vilket bland annat innebär att data grundkrypteras, samt möjliggör för kommunens utbildade systemadministratörer att arbeta med de säkerhetsinställningar som krävs enligt genomförd audit. Likaså är många styrdokument fastställda, utbildningar är under framtagande, informationshanteringsplaner uppdaterade, begränsningar för lagring/behandling av information samt personuppgifter genomförda och starkare krypteringsarbete påbörjat. Nämnden har därefter den 7 november 2023 uppgett att

konsekvensbedömningen i princip var klar. Det som kvarstod var en fråga kring dataflöden.

Motivering av beslutet

Konsekvensbedömning

Tillämpliga bestämmelser m.m.
Med personuppgiftsansvarig avses, enligt artikel 4.7 i dataskyddsförordningen, en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.

Av artikel 35.1 i dataskyddsförordningen framgår att om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter, en så kallad konsekvensbedömning.

I skäl 75 till dataskyddsförordningen anges faktorer som ska beaktas vid bedömningen av risken för fysiska personers rättigheter och friheter. En faktor som kan beaktas är om behandlingen avser uppgifter som innefattar bedömningar av personliga aspekter såsom arbetsprestationer. Vidare ska beaktas om behandlingen innefattar personuppgifter om sårbara fysiska personer, framförallt barn, och gäller ett stort antal registrerade. I skäl 76 till dataskyddsförordningen anges att risken bör utvärderas på grundval av en objektiv bedömning, genom vilken fastställs huruvida behandlingen inbegriper en risk eller hög risk.

I artikel 35.3 i dataskyddsförordningen anges exempel på situationer när en konsekvensbedömning krävs. Därutöver anges i artikel 35.4 i dataskyddsförordningen att tillsynsmyndigheten ska upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som omfattas av kravet på sådan konsekvensbedömning. IMY har upprättat en sådan förteckning,[3] se bilaga, som baseras på Artikel 29-gruppens riktlinjer[4]. Av förteckningen framgår att en konsekvensbedömning avseende dataskydd ska göras om den planerade behandlingen uppfyller minst två av följande kriterier:

1. utvärderar eller poängsätter människor, till exempel ett företag som erbjuder genetiska tester till konsumenter för att bedöma och förutse risker för sjukdomar, ett kreditupplysningsföretag eller ett företag som profilerar internetanvändare,
2. behandlar personuppgifter i syfte att fatta automatiserade beslut som har rättsliga följder eller liknande betydande följder för den registrerade,
3. systematiskt övervakar människor, till exempel genom kameraövervakning av en allmän plats eller genom att samla in personuppgifter från internetanvändning i offentliga miljöer,

[3] Dnr DI-2018-13200
[4] Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, antagna den 4 april 2017 (WP 248 rev. 01).

4. behandlar känsliga personuppgifter enligt artikel 9 eller uppgifter som är av mycket personlig karaktär, till exempel ett sjukhus som lagrar patientjournaler, ett företag som samlar in lokaliseringsuppgifter eller en bank som hanterar finansiella uppgifter,
5. behandlar personuppgifter i stor omfattning,
6. kombinerar personuppgifter från två eller flera behandlingar på ett sätt som avviker från vad de registrerade rimligen kunnat förvänta sig, till exempel när man samkör register,
7. behandlar personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara, till exempel barn, anställda, asylsökande, äldre och patienter,
8. använder ny teknik eller nya organisatoriska lösningar, till exempel en sakernas internet-applikation (Internet of things, IoT),
9. behandlar personuppgifter i syfte att hindra registrerade från att få tillgång till en tjänst eller ingå ett avtal, till exempel när en bank granskar sina kunder mot en databas för kreditupplysning för att besluta om de ska erbjudas lån.

I förteckningen finns ett antal exempel på när två av kriterierna ska anses uppfyllda och en konsekvensbedömning alltså måste göras. I ett av dessa exempel anges att konsekvensbedömningar ska utföras inom offentlig sektor inför behandling av barns personuppgifter i skolverksamhet, om det är ett större antal registrerade (kriterium 5 och 7).

Integritetsskyddsmyndighetens bedömning

Nämnden har uppgett att den är personuppgiftsansvarig för den behandling av personuppgifter som sker vid användandet av tjänsten Google Workspace i de aktuella skolorna, vilket stöds av utredningen i ärendet. IMY konstaterar att nämnden har bestämt ändamål och medel med behandlingen av personuppgifterna. Nämnden är därför personuppgiftsansvarig för den aktuella behandlingen.

Av utredningen i ärendet framgår att en tidigare version av tjänsten, Google Apps for Education, användes av nämnden, men inte på en egen domän. Av utredningen framgår vidare att Östersunds kommun, i maj 2020, fattade beslut om att migrera den nya versionen av tjänsten, Google Workspace, till en egen domän och att tjänsten i juni 2020 startades upp i kommunens egen IT-miljö. Under hösten 2020 började nämnden använda tjänsten i 24 av kommunens skolor. IMY bedömer att de förändringar i användandet av tjänsten, som kommunen fattat beslut om i maj 2020, resulterat i en ny personuppgiftsbehandling hos nämnden.

I artikel 35.1 i dataskyddsförordningen anges att om en typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter, en så kallad konsekvensbedömning. Den fråga som IMY har att bedöma är om det funnits en skyldighet att utföra en konsekvensbedömning innan nämnden inledde personuppgiftsbehandlingen under hösten 2020.

För att fastställa vilka behandlingar som sannolikt leder till en hög risk ska tillsynsmyndigheten, enligt artikel 35.4 i dataskyddsförordningen, upprätta en förteckning över behandlingar där en konsekvensbedömning krävs. IMY har som

nämnts ovan upprättat en sådan förteckning[5] som baseras på Artikel 29-gruppens riktlinjer[6]. Av förteckningen framgår att konsekvensbedömningar ska göras om en personuppgiftsbehandling uppfyller minst två av de kriterier som anges i förteckningen. I förteckningen finns ett antal exempel på när två av kriterierna ska anses uppfyllda och en konsekvensbedömning alltså måste göras. I ett av dessa exempel anges att konsekvensbedömningar ska utföras inom offentlig sektor inför behandling av barns personuppgifter i skolverksamhet, om det är ett större antal registrerade (kriterium 5 och 7).

IMY konstaterar att den i ärendet aktuella behandlingen är en sådan behandling som anges i det nämnda exemplet. Behandlingen utförs i skolverksamhet och rör ett stort antal registrerade som i huvudsak är barn. Barnen befinner sig i egenskap av elever i en utsatt position i förhållande till den personuppgiftsansvarige. Vidare har behandlingen avsett anställda som befinner sig i ett beroendeförhållande gentemot nämnden. Behandlingen har dessutom till viss del innefattat återkoppling på skoluppgifter vilket får anses utgöra en utvärdering av de registrerades prestationer. IMY bedömer att den aktuella behandlingen, med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt har inneburit en hög risk för de registrerades fri- och rättigheter. Nämnden hade således en skyldighet att genomföra en konsekvensbedömning innan behandlingen inleddes hösten 2020.

Av utredningen framgår att nämnden inte utförde en konsekvensbedömning innan Google Workspace började användas i de aktuella skolorna hösten 2020 samt att arbetet med att genomföra en konsekvensbedömning ännu inte slutförts.

IMY bedömer mot den bakgrunden att nämnden brustit i sin skyldighet enligt artikel 35.1 i dataskyddsförordningen att genomföra en konsekvensbedömning innan tjänsten Google Workspace började användas i 24 skolor i Östersunds kommun under hösten 2020.

Val av ingripande

Tillämpliga bestämmelser
Vid överträdelser av dataskyddsförordningen har IMY ett antal korrigerande befogenheter att tillgå enligt artikel 58.2 a–j i dataskyddsförordningen, bland annat reprimand, föreläggande och sanktionsavgifter.

Av artikel 83.2 i dataskyddsförordningen framgår att IMY ska påföra administrativa sanktionsavgifter utöver eller i stället för de andra åtgärder som avses i artikel 58.2 beroende på omständigheterna i det enskilda fallet. Medlemsstaterna får fastställa regler för om och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter. Det framgår av artikel 83.7 i dataskyddsförordningen. Av 6 kap. 2 § dataskyddslagen framgår att IMY får ta ut sanktionsavgifter av myndigheter vid överträdelser som avses i artikel 83.4, 83.5 och 83.6 i dataskyddsförordningen och att artikel 83.1, 83.2 och 83.3 i förordningen då ska tillämpas.

I artikel 83.2 i dataskyddsförordningen anges de faktorer som ska beaktas vid beslut om administrativa sanktionsavgifter ska påföras och vid bestämmande av avgiftens storlek. Om det är fråga om en mindre överträdelse får IMY enligt skäl 148 till

[5] Dnr DI-2018-13200
[6] Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, antagna den 4 april 2017 (WP 248 rev. 01).

dataskyddsförordningen utfärda en reprimand istället för att påföra en sanktionsavgift. De faktorer som anges i artikel 83.2 i dataskyddsförordningen ska beaktas även vid bestämmandet av sanktionsavgiftens storlek. Varje tillsynsmyndighet ska säkerställa att påförandet av administrativa sanktionsavgifter i varje enskilt fall är effektivt, proportionellt och avskräckande. Det framgår av artikel 83.1 i dataskyddsförordningen.

Sanktionsavgift ska påföras
IMY har bedömt att nämnden har brustit i sin skyldighet enligt artikel 35.1 i dataskyddsförordningen att genomföra en konsekvensbedömning innan tjänsten Google Workspace började användas.

IMY konstaterar att behandlingen har innefattat 5 945 barn, vars personuppgifter är särskilt skyddsvärda samt att uppgifterna behandlas i ett sammanhang där barnen i egenskap av elever befinner sig i beroendeställning till den personuppgiftsansvarige. Vidare beaktar IMY att konsekvensbedömningen ännu inte slutförts trots att ca tre år har gått sedan behandlingen inleddes hösten 2020. IMY konstaterar vidare att underlåtelsen inneburit en förhållandevis hög grad av oaktsamhet eftersom det varit tydligt att behandlingen omfattades av kravet på konsekvensbedömning bland annat utifrån IMY:s förteckning enligt artikel 35.4. IMY bedömer därför att nämnden ska påföras en administrativ sanktionsavgift för överträdelsen.

Sanktionsavgiftens storlek
För överträdelser av bland annat artikel 35 i dataskyddsförordningen får sanktionsavgiften för offentliga myndigheter uppgå till högst 5 000 000 kronor. Det framgår av 6 kap. 2 § dataskyddslagen samt artikel 83.4 i dataskyddsförordningen. Vid bestämmande av sanktionsavgiftens storlek ska IMY beakta de omständigheter som anges i artikel 83.2 samt säkerställa att den administrativa sanktionsavgiften är effektiv, proportionell och avskräckande.

I bedömningen av överträdelsens allvarlighet beaktar IMY i enlighet med artikel 83.2 g i dataskyddsförordningen att behandlingen har omfattat uppgifter om barn, som är särskilt skyddsvärda enligt dataskyddsförordningen. Behandlingen har även till viss del innefattat särskilt skyddsvärda uppgifter som återkoppling på skoluppgifter.

När det gäller överträdelsens karaktär, svårighetsgrad och varaktighet enligt artikel 83.2 a i dataskyddsförordningen framgår av utredningen att det gått ca tre år sedan behandlingen inletts utan att nämnden slutfört konsekvensbedömningen. Vidare framgår att behandlingen har berört ett stort antal registrerade, såväl elever som anställda. Dessutom har tjänsten använts inom skolan – dvs. en verksamhet där den registrerade eleven befinner sig i en beroendeställning och utsatt position i förhållande till den personuppgiftsansvarige. Behandlingen har även avsett anställda som befinner sig i ett beroendeförhållande gentemot nämnden

IMY konstaterar vidare att nämnden varit medveten om att den inte har genomfört en konsekvensbedömning och att nämnden anser att den skulle genomfört en sådan bedömning. IMY konstaterar att denna underlåtelse inneburit en förhållandevis hög grad av oaktsamhet eftersom det varit tydligt att behandlingen omfattades av kravet på konsekvensbedömning bland annat utifrån IMY:s förteckning enligt artikel 35.4.

IMY konstaterar vidare att behandling av personuppgifter i en molntjänst som tillhandahålls av ett amerikanskt bolag sannolikt inneburit risk för att personuppgifterna överförs till tredjeland utan en skyddsnivå som är väsentligt likvärdig med den nivå

som garanteras inom unionen genom dataskyddsförordningen om inte särskilda skyddsåtgärder vidtas.

Utöver bedömningen av överträdelsens allvar ska IMY bedöma om det föreligger några försvårande eller förmildrande omständigheter som får betydelse för sanktionsavgiftens storlek. De åtgärder nämnden vidtagit efter att IMY inlett insyn, vilka framgår av yttrande från den 12 september 2023, bedömer IMY inte som förmildrande. Detta då det är fråga om åtgärder nämnden borde ha fastställt och genomfört innan tjänsten började användas. IMY bedömer att det saknas ytterligare försvårande eller förmildrande omständigheter, utöver de som beaktas vid bedömningen av allvarlighetsgraden ovan, som påverkar sanktionsavgiftens storlek.

IMY bestämmer utifrån en samlad bedömning av omständigheterna i ärendet att Barn- och utbildningsnämnden i Östersunds kommun ska betala en administrativ sanktionsavgift på 300 000 kronor. IMY bedömer att detta belopp är effektivt, proportionerligt och avskräckande.

IMY konstaterar att nämnden uppgett att konsekvensbedömningen är i princip klar och att det därför saknas skäl att förelägga nämnden att genomföra en konsekvens-bedömning.

Detta beslut har fattats av vikarierande generaldirektören Karin Lönnheden efter föredragning av juristen Nina Hellgren. Vid den slutliga handläggningen har även rättschefen David Törngren, juristen Cecilia Agnehall och enhetschefen Nidia Nordenström medverkat.

Karin Lönnheden, 2023-11-28 (Det här är en elektronisk signatur)

Bilaga
Förteckning enligt artikel 35.4 i dataskyddsförordningen
Information om betalning av sanktionsavgift

Kopia till
Nämndens dataskyddsombud

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till IMY. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till IMY senast tre veckor från den dag ni fick del av beslutet. Om ni är en part som företräder det allmänna ska överklagandet dock ha kommit in inom tre veckor från den dag då beslutet meddelades. Om överklagandet har kommit in i tid sänder IMY det vidare till Förvaltningsrätten i Stockholm för prövning.

Ni kan e-posta överklagandet till IMY om det inte innehåller några integritetskänsliga personuppgifter eller uppgifter som kan omfattas av sekretess. Myndighetens kontaktuppgifter framgår av beslutets första sida.