Stockholms stad, utbildningsnämnden
Utbildningsförvaltningen
Box 22049
104 22 Stockholm

Tillsyn enligt EU:s dataskyddsförordning 2016/679- mot Utbildningsnämnden i Stockholms stad

Innehåll

Datainspektionens beslut

Överträdelserna
Datainspektionen konstaterar att Utbildningsnämnden i Stockholms stad har behandlat personuppgifter i strid med artikel 5.1 f i dataskyddsförordningen[1] som ställer krav på en lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling samt i strid med artikel 32.1 som ställer krav på att den personuppgiftsansvarige vidtar lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken för fysiska personers rättigheter och friheter genom att:

- i modulen Skolpliktsbevakning, under perioden 25 maj 2018 fram till 27 augusti 2020, haft en behörighetstilldelning som har varit mer omfattande än vad som är nödvändigt mot bakgrund av vad respektive rollinnehavare behöver för att utföra sitt arbete samt genom att obehöriga personer haft åtkomst till integritetskänsliga personuppgifter rörande elever med skyddad identitet.

- i delsystemet Elevdokumentationen, under perioden 26 oktober 2018 fram till november 2019, har obehöriga personer haft åtkomst till personuppgifter rörande ett mycket stort antal elever varav en del har varit integritetskänsliga/känsliga personuppgifter.

- i delsystemet Startsidan för vårdnadshavare, under perioden 27 juni 2019 fram till 24 augusti 2019, har obehöriga personer haft åtkomst till personuppgifter rörande vårdnadshavare.

- i delsystemet Administrationsgränssnittet, under perioden 25 maj 2018 fram till 26 augusti 2019, har obehöriga personer haft åtkomst till integritetskänsliga personuppgifter rörande lärare med skyddad identitet.

[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).

Datainspektionen konstaterar att Utbildningsnämnden i Stockholms stad, under perioden 25 maj 2018 fram till 27 augusti 2020, har behandlat personuppgifter i delsystemen Skolpliktsbevakning, Elevdokumentationen, Startsidan för vårdnadshavare och Administrationsgränssnittet i strid med artikel 35, genom att inte ha genomfört konsekvensbedömningar för dessa system trots att behandlingarna sannolikt leder till hög risk för fysiska personers fri- och rättigheter eftersom det är frågan om stora system, med många barn registrerade och med både känsliga- och integritetskänsliga personuppgifter.

Administrativ sanktionsavgift
Datainspektionen beslutar med stöd av artiklarna 58.2 och 83 dataskyddsförordningen och 6 kap. 2 § dataskyddslagen[2] att Utbildningsnämnden i Stockholms stad för överträdelserna av artikel 5.1 och artikel 32.1 i dataskyddsförordningen ska betala en administrativ sanktionsavgift på 4 000 000 (fyra miljoner) kronor.

Förelägganden
Datainspektionen förelägger med stöd av artikel 58.2 d i dataskyddsförordningen utbildningsnämnden att snarast genomföra en konsekvensbedömning i enlighet med artikel 35 i dataskyddsförordningen avseende delsystemen Skolpliktsbevakning, Elevdokumentationen och Startsidan för vårdnadshavare.

Datainspektionen förelägger med stöd av artikel 58.2 d i dataskyddsförordningen Utbildningsnämnden i Stockholms stad att begränsa behörighetstilldelningar i modulen Skolpliktbevakningen till enbart de personer som har ett behov av att behandla personuppgifter för att utföra sina arbetsuppgifter.

[2] Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

1. Redogörelse för tillsynsärendet

Datainspektionen har genom anmälningar om personuppgiftsincidenter från Utbildningsnämnden i Stockholms stad uppmärksammats på obehörig åtkomst till elevuppgifter i Skolplattformen.

Av de inkomna anmälningarna har framkommit att den digitala plattform som används i Stockholms stad, Skolplattformen, är ett stadsövergripande projekt och plattformen består av sex delsystem. Det har även framkommit att Utbildningsnämnden i Stockholms stad är personuppgiftsansvarig för de personuppgiftsbehandlingar i Skolplattformen som incidenterna avser.

Datainspektionen har mot bakgrund av dessa anmälningar inlett den aktuella tillsynen den 24 juni 2019 (dnr 2019-7024) av utbildningsnämndens behandling av personuppgifter, i syfte att granska säkerhetsåtgärderna för åtkomsten till personuppgifter inom ramen för två moduler i delsystemet Barn- och elevregistret:

- Skolpliktsbevakning
- Interkommunala avtal

Efter att tillsynen inletts kom utbildningsnämnden in med ytterligare anmälningar om personuppgiftsincidenter. Mot bakgrund av de uppgifter som framkom i dessa anmälningar beslutade Datainspektionen den 18 juni 2020 att utvidga tillsynen till att omfatta även en granskning av säkerhetsåtgärder för åtkomsten till personuppgifter inom ramen för delsystemen:

- Elevdokumentation
- Startsidan för vårdnadshavare (Startsidan)
- Administrationsgränssnittet ”Kontaktuppgifter lärare”(Administrationsgränssnittet)

Avseende Interkommunala avtal har det framkommit att det utgör en modul i Barn- och elevregistret. Denna modul har inte implementerats fullt ut och används av ett begränsat antal användare. I modulen Interkommunala avtal har det funnits nio elever. Incidenten i modulen omfattade inte barn med skyddad identitet såsom det angavs i anmälan om personuppgiftsincidenten. Mot denna bakgrund har Datainspektionen inte närmare granskat modulen Interkommunala avtal.

När det gäller Skolpliktsbevakningen är det en modul[3] i Barn- och elevregistret som utgör ett administrativt systemstöd för att utbildningsnämnden ska kunna fullgöra sina skyldigheter enligt skollagen (2010:800). Av den inkomna anmälan om personuppgiftsincidenten har det framkommit att obehörig personal har haft möjlighet att se uppgifter om sekretessmarkerade personer. Datainspektionen har mot bakgrund av detta granskat de *tekniska åtgärder* som nämnden vidtagit för att säkerställa en lämplig säkerhetsnivå i modulen. Inspektionen har även granskat *organisatoriska åtgärder* i form av behörighetstilldelning i aktuell modul.

De inkomna personuppgiftsincidenterna avseende delsystemen Elevdokumentation, Startsidan samt Administrationsgränssnittet har rört tekniska brister. Datainspektionen har därför enbart granskat de *tekniska åtgärder* som har vidtagits för att säkerställa en lämplig säkerhetsnivå i dessa tre delsystem.

Datainspektionens granskning avser även skyldigheten att utföra en konsekvensbedömning enligt artikel 35 i dataskyddsförordningen avseende de aktuella delsystemen.

Utbildningsnämnden ansvarar för 139 grundskolor, 32 grundsärskolor, 28 gymnasieskolor och sex gymnasiesärskolor. Datainspektionens aktuella granskning avser inte vuxenutbildning eller förskoleverksamhet.

2. Motivering av beslut

2.1 Tillämpliga bestämmelser

Personuppgiftsansvarig är enligt definitionen i artikel 4 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; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de

[3] Utbildningsnämnden har uppgett att Skolpliktsbevakning är både en modul och ett eget processområde.

särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

Enligt artikel 5.1 f i dataskyddsförordningen ska personuppgifter behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet).

Artikel 32.1 i dataskyddsförordningen föreskriver att den personuppgiftsansvarige ska - med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter - vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Detta inbegriper enligt artikel 32.1 punkterna b och d i dataskyddsförordningen, när det är lämpligt,

- förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna, och
- ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

I skäl 74 till dataskyddsförordningen anges följande:

> *Personuppgiftsansvariga bör åläggas ansvaret för all behandling av personuppgifter som de utför eller som utförs på deras vägnar. Personuppgiftsansvariga bör särskilt vara skyldiga att vidta lämpliga och effektiva åtgärder och kunna visa att behandlingen är förenlig med denna förordning, även vad gäller åtgärdernas effektivitet. Man bör inom dessa åtgärder beakta behandlingens art, omfattning, sammanhang och ändamål samt risken för fysiska personers rättigheter och friheter.*

Enligt artikel 35 ska en personuppgiftsansvarig göra en bedömning av en planerad behandlings konsekvenser för skyddet av personuppgifter, särskilt om en behandling ska ske med ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål sannolikt leder till en hög risk för

fysiska personers rättigheter och friheter. Detta inbegriper enligt artikel 35.3 b att en konsekvensbedömning enligt artikel 35.1 särskilt ska krävas i fall behandling sker i stor omfattning av särskilda kategorier av uppgifter som avses i artikel 9.1 eller av personuppgifter som rör fällande domar i brottmål och överträdelser som avses i artikel 10.

2.2 Personuppgiftsansvaret

Vad Utbildningsnämnden i Stockholms stad anfört under handläggningen
Utbildningsnämnden i Stockholms stad är personuppgiftsansvarig för de personuppgiftsbehandlingar som har skett i delsystemen Barn- och elevregistret (modulen) Skolpliktsbevakning, Elevdokumentation, Startsidan och Administrationsgränssnittet. Utbildningsnämnden är dock inte personuppgiftsansvarig för de personuppgiftsbehandlingar som har skett i sistnämnda delsystem inom ramen för förskoleverksamhet och vuxenutbildning.

Utbildningsnämnden nyttjar idag ett flertal system och e-tjänster som en del i dess pedagogiska och administrativa verksamheter. Nämnden ansvarar för drift och utveckling av kommunal verksamhet inom förskola, grundskola, grundsärskola, fritidshem, gymnasieskola och gymnasiesärskola. Utbildningsnämnden är ytterst ansvarig för hur den egna verksamheten hanterar informationen. Vidare ansvarar nämnden för att informationen skyddas i enlighet med stadens riktlinjer för informationssäkerhet och dataskyddslagstiftning, som dataskyddsförordningen. Kommunstyrelsen ansvarar för att systemet uppfyller kraven på säkerhet och är systemägare. Efter beslut i fullmäktige flyttades hela ansvaret för Skolplattformen till utbildningsnämnden från och med den 1 januari 2020. Detta innebär att utbildningsnämnden är såväl systemägare som informationsägare.

Datainspektionens bedömning
Inget i ärendet talar emot utbildningsnämndens konstaterande att de aktuella personuppgiftsbehandlingar som denna tillsyn omfattar har skett för utbildningsnämndens ändamål att bedriva kommunal skolverksamhet. Detsamma gäller även utbildningsnämndens uppfattning att det är Utbildningsnämnden i Stockholms stad som är personuppgiftsansvarig för de personuppgiftsbehandlingar som har skett i delsystemen Barn- och elevregistret (modulen) Skolpliktsbevakning, Elevdokumentation, Startsidan och Administrationsgränssnittet. Den aktuella tillsynen omfattar inte

personuppgiftsbehandlingar som har skett inom ramen för förskoleverksamhet och vuxenutbildning, därför faller frågan om personuppgiftsansvaret för sistnämnda behandlingar utanför den aktuella tillsynen.

2.3 Skolpliktsbevakning

Vad Utbildningsnämnden i Stockholms stad anfört under handläggningen

Allmänt om Skolpliktsbevakning
Skolplattformen består av sex delsystem och Barn- och elevregistret utgör ett av dessa delsystem. Det finns 101 moduler i Barn- och elevregistret som är indelade i åtta processområden. Skolpliktsbevakningen är ett av de åtta processområdena i Barn- och elevregistret. Processområdet Skolpliktsbevakning stödjer arbetet med skolpliktsbevakning inom kommunala grundskolor samt avseende elever i fristående skolor där Stockholms stad utgör hemkommun. I funktionen ingår även processerna kring det kommunala aktivitetsansvaret. Det administrativa systemstödet används för att fullgöra utbildningsnämndens skyldigheter avseende skolplikt enligt skollagen (2010:800) samt handläggning och beslut i ärenden kopplat till detta (främst enligt 7 kap. skollagen men även 24 kap. 23 §). Det administrativa ansvaret innebär att säkerställa att elever inom ett visst geografiskt område blir placerade på en skola nära hemmet.

I modulen Skolpliktsbevakning behandlas uppgifter om 1 322 aktiva skolpliktbevakningar (antal registrerade) varav 83 elever är under sju år. Av dessa 1 322 aktiva skolpliktsbevakningar har 60 elever skyddade personuppgifter.

De personuppgifter som behandlas i aktuell modul är bl. a. namn, adress, modersmål, skolplacering, vårdnadshavare och kontaktuppgifter till dessa (telefonnummer och e-postadress) samt historik av skolplacering och kontaktpersoner. Vidare behandlas beslut som innehåller personuppgifter avseende en specifik elev där skolplikten har upphört, fortsatt bevakning (t.ex. föreläggande av vite eller ärende hos Skatteverket), medgivande att fullgöra skolplikten på annat sätt samt uppskjuten skolplikt (särskilda skäl). Modulen innehåller uppgift om att en elev går på resursskola eller grundsärskola.

Tekniska brister
Den 5 oktober 2018 upptäcktes att samtliga användare som hade behörighet till modulen Skolpliktsbevakning hade möjlighet att se samtliga sekretessmarkerade[4] elever utan skolplacering. Denna brist uppges bero att systemet saknade logik för att i funktionaliteten för skolpliktsbevakning begränsa behörigheten för sekretessmarkerade personer. Orsaken till det är okänt. När modulen implementerades i juli 2017 hade utbildningsnämnden ingen kännedom om några brister. Skolpliktsbevakningen på stadens kommunala grundskolor utgår från boendeområde. Sekretessmarkerade personer som är oplacerade saknar boendeområde i systemet. Rutinen är att anställda på skolorna inte ska kunna se dessa elever då denna handläggning endast sker centralt.

Antal användare som potentiellt skulle ha kunnat felaktigt sett sekretessmarkerade personer är 1 302. Nämnden har endast kännedom om att en skoladministratör felaktigt sett uppgiften om sekretessmarkerade elever. Denne ska ha fått fram tre sekretessmarkerade elever i sökresultatet. Det fanns totalt 60 elever med sekretessmarkering i Skolpliktsbevakning. Det har inte varit möjligt att med logghistorik få fram det exakta antalet användare som haft obehörig åtkomst i praktiken eftersom det inte finns specifika loggar för modulen Skolpliktsbevakning.

När bristen upptäcktes den 5 oktober 2018 var det inte verifierat att användare såg mer information än de var behöriga att se. Den 5 november 2018, dvs. en månad efter upptäckt, kunde nämnden verifiera att användare såg mer information än de var behöriga att se. Leverantören arbetade fram en rättning som kom i produktion den 9 november 2018.

Organisatoriska brister
Avseende behörighetstilldelningen i Skolpliktsbevakningen har nämnden uppgett att det finns åtta rollinnehavare med olika behörighet;

- Gr systemansvarig Sthlm,
- Gr Administratör Ersättningar Sthlm,
- Gr Titta Sthlm,
- Gr Administratör Språkcentrum Sthlm,
- Gr PMO-ansvarig Sthlm,

[4] Med sekretessmarkerade personer avses elever med skyddade personuppgifter.

- Gr Administratör Skola Sthlm,
- Gr Skolpliktsbevakning Central Admin Sthlm
- Gr Titta Ekonomi Sthlm.

Nämnden uppger att fyra[5] av de åtta ovan angivna rollinnehavarna inte behöver ha den åtkomst till Skolpliktsbevakningen som de har. Detta beror på att utbildningsförvaltningen inte kan se att dessa rollinnehavare behöver ha tillgång till Skolpliktsbevakningen alternativt att det inte är säkerställt att rollen enbart har tillgång till uppgifter som krävs för att fullgöra arbetsuppgifterna. Förvaltningen har därför begärt att detta ska justeras.

Datainspektionens bedömning

Personuppgifternas art och krav på säkerhet
Datainspektionen konstaterar inledningsvis att det i modulen Skolpliktsbevakning behandlas uppgifter om elever, såsom namn, adress, personnummer, vårdnadshavare och kontaktuppgifter till dessa (telefonnummer och e-postadress), modersmål, kommun, skolplacering (skola och årskurs), historik av skolplacering samt kontaktpersoner (namn, adress, personnummer, telefonnummer samt e-post). Det behandlas även uppgifter om elever som har skyddad identitet. Vidare kan personuppgifter i vissa beslut behandlas i modulen såsom fortsatt bevakning av en specifik elev som rör föreläggande av vite eller utredning eller ärende hos Skatteverket, medgivande att fullgöra skolplikten på annat sätt (filminspelning, nordisk skolgång eller utlandsresa) samt uppskjuten skolplikt (särskilda skäl).

Datainspektionen anser att uppgifter om skyddad identitet är mycket skyddsvärda/integritetskänsliga då riskerna för de registrerades friheter och rättigheter är stora vid behandling av dessa personuppgifter. Uppgift om att en elev går på resursskola eller grundsärskola som också behandlas i Skolpliktsbevakning är en känslig personuppgift[6] då det avslöjar uppgift om hälsa.

Mot bakgrund av karaktären och arten av de personuppgiftsbehandlingar som har skett i Skolpliktsbevakningen samt riskerna för de registrerades friheter

[5] Gr Administratör Ersättningar Sthlm, Gr Administratör Språkcentrum Sthlm, Gr PMO-ansvarig Sthlm samt Gr Titta Ekonomi Sthlm.
[6] Artikel 9 i dataskyddsförordningen.

och rättigheter anser Datainspektionen att det ställs höga krav på de tekniska och organisatoriska åtgärder som utbildningsnämnden haft att vidta för att säkerställa en lämplig säkerhetsnivå i enlighet med artikel 32 i dataskyddsförordningen.

Tekniska brister
Av utredningen i ärendet framgår att obehöriga personer har kunnat komma åt integritetskänsliga personuppgifter rörande elever med skyddad identitet. Eftersom det inte finns någon logguppföljning i modulen Skolpliktsbevakning går det inte att i efterhand uppge det exakta antalet användare som haft faktisk obehörig åtkomst till dessa uppgifter. Den tekniska bristen i Skolpliktsbevakning som nu granskats har inneburit att 1 302 användare potentiellt har obehörigen kunnat komma åt personuppgifter avseende 60 elever med skyddad identitet. Orsaken till detta beror enligt nämnden på svagheter i systemet som omöjliggjorde behörighetsbegränsning till uppgifter om elever med skyddad identitet. Det finns ingen uppgift om när bristen inträffade men modulen implementerades i juli 2017 och bristen upptäcktes den 5 oktober 2018.

Organisatoriska brister
Datainspektionens granskning av det aktuella delsystemet avser både kraven på tekniska åtgärder samt organisatoriska åtgärder enligt artikel 32. Av utredningen i ärendet framkommer även att behörighetstilldelningen i Skolpliktsbevakningen är mer omfattande än vad som är nödvändigt i förhållande till vad respektive rollinnehavare behöver för att utföra sina arbetsuppgifter. Utbildningsnämnden har uppgett att en översyn av de åtta behörighetsrollerna ska initieras inom kort.

Sammantagen bedömning
Både den omständigheten att obehöriga personer haft åtkomst till/har kunnat komma åt integritetskänsliga personuppgifter rörande elever med skyddad identitet samt att det finns en mer omfattande behörighet till uppgifter i Skolpliktsbevakningen än nödvändigt strider mot artikel 32.1 dataskyddsförordningen. Enligt artikel 32.1 ska utbildningsnämnden med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter, vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

Datainspektionen bedömer att en lämplig säkerhet i detta fall omfattar en förmåga att fortlöpande säkerställa konfidentialitet hos behandlingssystemen och –tjänsterna. Genom att nämnden har tilldelat mer omfattande behörigheter samt att obehöriga har fått åtkomst till personuppgifter om elever med skyddad identitet är det Datainspektionens bedömning att utbildningsnämnden brustit i förmågan att fortlöpande säkerställa konfidentialitet för uppgifterna som behandlas i behandlingssystemen och -tjänsterna enligt kravet i artikel 32.1 i dataskyddsförordningen.

Kravet på lämplig säkerhet inbegriper även att ha ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska vidtagna åtgärderna för att säkerställa behandlingens säkerhet vilket inte heller har förelegat i detta fall. Datainspektionen konstaterar att om utbildningsnämnden hade haft ett sådant förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de vidtagna åtgärderna hade nämnden kunnat säkerställa/upptäcka om de tekniska åtgärderna stämmer överens med de vidtagna organisatoriska åtgärderna. Vad gäller den organisatoriska bristen (den omfattande behörigheten) är även det enligt Datainspektionens bedömning en sådan brist i behörighetsbegränsningen som borde ha upptäckts om utbildningsnämnden regelbundet hade kontrollerat behörigheten. Även detta är en brist i kraven på lämplig säkerhet enligt artikel 32.1 i dataskyddsförordningen.

Utbildningsnämnden i Stockholms stad har sammanfattningsvis behandlat personuppgifter i modulen Skolpliktsbevakning i Skolplattformen i strid med artikel 32 i dataskyddsförordningen.

Datainspektionen bedömer även att utbildningsnämnden har behandlat personuppgifter i strid med artikel 5.1 f i dataskyddsförordningen i det aktuella delsystemet. Detta eftersom nämnden inte har säkerställt en lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling genom användning av lämpliga tekniska åtgärder.

2.4 Elevdokumentationen

Vad Utbildningsnämnden i Stockholms stad anfört under handläggningen

Allmänt om Elevdokumentationen
Elevdokumentationen är ett av sex delsystem som Skolplattformen består av. I delsystemet Elevdokumentation finns totalt 464 611 registrerade, varav 122 699 är elever i kommunal grundskola och gymnasieskola. Av dessa elever har 787 skyddade personuppgifter. I detta delsystem finns 233 066 registrerade vårdnadshavare och 34 756 anställda (en del av dessa anställda arbetar inom barnomsorg och vuxenutbildning som inte omfattas av tillsynen).

De personuppgifter som behandlas i aktuellt delsystem är bl. a. betyg, resultat på nationella prov, rapportering av resultat till Statistiska Centralbyrån, SCB, bedömningsstöd som innebär dokumentation av elevens kunskapsnivå, uppgifter om att vissa elever behöver extra anpassningar, dokumentation kring utredningar och åtgärdsprogram, personuppgifter för arbetet med utvecklingssamtal och skriftliga omdömen.

Tekniska brister
Den 21 augusti 2019 uppdagades via en tråd på Twitter att en vårdnadshavare hade upptäckt en dataläcka i Elevdokumentationen. Personen bakom Twitterkontot har med egen access och inloggning via Bank-ID analyserat trafiken och anropen mellan frontend- och backendsystemet.[7] Personen har sedan tagit ut delar av dessa anrop och manipulerat dessa för att på så sätt komma över andra personers information.

[7] Begreppen används av Utbildningsnämnden i Stockholms stad och deras funktion kan allmänt beskrivas enligt följande. Separationen av frontend och backendsystem förenklar dataprocessen när det handlar om flerskiktad utveckling och underhåll av datasystem. Ett frontendsystem används främst för att skicka frågor och förfrågningar och ta emot data från backendsystemet. Det ger användarna möjlighet att interagera och använda ett informationssystem. Vanligtvis har frontendsystem mycket begränsade beräknings- eller affärslogikbehandlingsfunktioner och förlitar sig på data och funktioner från backendsystemet. Ett frontendsystem kan inkludera eller bestå av ett text- eller grafiskt användargränssnitt (GUI) och/eller en frontend-klientapplikation som är ansluten till backendsystemet. Backendsystemet hanterar databaser och databehandlingskomponenter och ser till att ta fram svaren på frontendsystemets förfrågningar ur databaser och databehandlingskomponenter.

Nämnden har uppgett att när inloggning sker i Elevdokumentationen i Skolplattformen exponeras persondata genom ett API[8]. På grund av en teknisk brist i APIet kunde personer, med viss kunskap om nätverkssystem och programmering, övervaka anrop gjorda från ett inloggat klientläge, kopiera och modifiera dem. På det sättet kunde nya anrop göras och personuppgifter som inte skulle vara tillgängliga för personen blev tillgängliga. Detta innebär att personuppgifter var tillgängliga beroende på vilka förfrågningar en individ gjorde, oavsett behörighet. Det gav i sin tur åtkomst till personuppgifter utan korrekt behörighet.

Denna brist har inneburit att obehöriga personer har kunnat komma åt följande uppgifter om andra elever: förnamn, efternamn, personnummer, skoltyp (t.ex. grundsärskola), årskurs, skol-ID, klass, elevens omdöme ur modulen utvecklingssamtal, om det är en integrerad användare eller inte samt migrerade IUP[9]-dokument från Skolwebben.

Alla registrerade vårdnadshavare i Skolplattformen har på grund av den aktuella bristen haft möjlighet att obehörigen ta del av information. Enligt utbildningsnämnden har en person utnyttjat denna möjlighet och gjort personsökningar på 101 unika personer. Bristen har funnits sedan delsystemet lanserades. Modulen där bristen fanns har varit i drift sedan den 26 oktober 2018. Denna brist hade inte fångats i tidigare funktions- och säkerhetstester innan funktionen sattes i produktion.

Bristen i delsystemet åtgärdades genom kodändringar som färdigställdes under november 2019. Elevdokumentationen stängdes efter att bristen upptäcktes fram till att samtliga upptäckta brister åtgärdades.

[8] Ett applikationsprogrammeringsgränssnitt (API) är en uppsättning protokoll, rutiner, funktioner och/eller kommandon som programmerare använder för att utveckla programvara eller underlätta interaktion mellan olika system. API: er är vanligtvis användbara för programmering av GUI-komponenter (grafiskt användargränssnitt), såväl som för att ett program kan begära och tillgodose tjänster från ett annat program.
[9] Individuell utvecklingsplan.

Datainspektionens bedömning

Krav på säkerhet
Datainspektionen konstaterar inledningsvis att i delsystemet Elevdokumentation i Skolplattformen sker omfattande personuppgiftsbehandlingar som rör tusentals elever, vårdnadshavare och lärare.

Enligt artikel 9 i dataskyddsförordningen är uppgifter om hälsa så kallade känsliga personuppgifter enligt dataskyddsförordningen. I förarbeten, Behandling av personuppgifter på utbildningsområdet (prop. 2017/18:218 s.57) anges följande:

> *Som har nämnts ovan behandlas vidare känsliga personuppgifter om hälsa vid prövning av mottagande i grundsärskolan, specialskolan, gymnasiesärskolan, och särskild utbildning för vuxna enligt 7, 18 och 21 kap. skollagen. Även en uppgift om att en elev går i en sådan skola är en känslig uppgift.*

Datainspektionen konstaterar vidare att i delsystemet Elevdokumentationen behandlas uppgifter som rör elevers hälsa såsom uppgifter som förekommer i olika utredningar om elever, särskilda anpassningar m.m. Även uppgifter om att vissa elever går till en särskola innebär behandling av känsliga personuppgifter.

Därutöver tillkommer omfattande personuppgiftsbehandlingar i Elevdokumentationen som inte utgör känsliga personuppgifter enligt dataskyddsförordningen men är att anse som extra integritetskänsliga såsom uppgifter som rör omdömen och uppgifter från utvecklingssamtal.

Mot bakgrund av omfattningen av de personuppgiftsbehandlingar som sker i delsystemet Elevdokumentation, behandlingarnas art och karaktär samt riskerna för de registrerades friheter och rättigheter anser Datainspektionen att mycket höga krav ska ställas på de tekniska åtgärder som ska vidtas för att säkerställa en lämplig säkerhetsnivå i enlighet med artikel 32 i dataskyddsförordningen.

Bedömning av tekniska åtgärder

Den tekniska bristen i Elevdokumentationen som nu granskas har inneburit att obehöriga personer har kunnat komma åt andras personuppgifter genom att övervaka anrop gjorda från ett inloggat klientläge, kopiera och modifiera dem. På sådant sätt kunde nya anrop göras och personuppgifter som inte skulle vara tillgängliga blev tillgängliga. Enligt utbildningsnämndens uppgifter kunde obehöriga personer komma åt bl. a. andras förnamn, efternamn, personnummer, skoltyp (t.ex. grundsärskola), årskurs, skol-ID, klass och elevers omdömen ur modulen utvecklingssamtal. Denna tekniska brist har inneburit att samtliga registrerade vårdnadshavare i Skolplattformen har haft möjlighet att obehörigen ta del av information om alla registrerade elever, innefattande känsliga och integritetskänsliga uppgifter rörande eleverna.

Datainspektionen konstaterar att de tekniska säkerhetsåtgärderna som har vidtagits i delsystemet Elevdokumentationen i Skolplattformen har varit bristfälliga då obehöriga personer har på ett enkelt sätt kunnat komma åt omfattande känsliga och integritetskänsliga personuppgifter rörande tusentals elever. Utbildningsnämnden har således brustit i sin skyldighet enligt artikel 32.1 i dataskyddsförordningen att med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter, vidta lämpliga tekniska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

Den aktuella tekniska bristen som nu granskas i delsystemet Elevdokumentationen borde enligt Datainspektionens bedömning ha upptäckts i ett tidigt skede, innan behandlingen av personuppgifterna påbörjades. Datainspektionen bedömer att en lämplig säkerhet i detta fall omfattar en förmåga att fortlöpande säkerställa konfidentialitet hos behandlingssystemen och –tjänsterna.

Kravet på lämplig säkerhet inbegriper även att ha ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska vidtagna åtgärderna för att säkerställa behandlingens säkerhet. Att den aktuella tekniska bristen upptäcktes av en vårdnadshavare lång tid efter att delsystemet Elevdokumentationen lanserades, visar att utbildningsnämnden varken har sett till att fortlöpande säkerställa konfidentialitet i detta delsystem eller haft ett förfarande för att regelbundet testa, undersöka och

utvärdera effektiviteten hos de tekniska vidtagna åtgärderna på ett sätt som uppfyller kraven i dataskyddsförordningen. Datainspektionen konstaterar att även detta är en brist i kraven på lämplig säkerhet enligt artikel 32.1 i dataskyddsförordningen.

Sammanfattningsvis så har Utbildningsnämnden i Stockholms stad behandlat personuppgifter i Elevdokumentationen som är en del av Skolplattformen i strid med artikel 32 i dataskyddsförordningen.

Datainspektionen bedömer även att utbildningsnämnden har behandlat personuppgifter i det aktuella delsystemet i strid med artikel 5.1 f i dataskyddsförordningen. Detta eftersom nämnden inte har säkerställt en lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling genom användning av lämpliga tekniska åtgärder.

2.5 Startsidan

Vad Utbildningsnämnden i Stockholms stad har anfört under handläggningen

Allmänt om Startsidan
Startsidan är ett av de sex delsystem som Skolplattformen består av. En modul i delsystemet Startsidan heter ”kontakter” där personuppgifter från School Data Sync Database (SDS DB) behandlas, som i sin tur hämtar information från delsystemet Barn- och elevregistret. Personuppgifter behandlas för att säkerställa vårdnadshavares åtkomst till information om rätt skola och klass utifrån kopplingen mellan vårdnadshavare och barn/elev och barn/elevs koppling till klasser/grupper. Detta styrs utifrån information i Barn- och elevregistret.

Bland de personuppgifter som behandlas i Startsidan är elevers och lärares namn, e-postadress, skolkoppling, koppling till grupper, koppling till avdelningar, mentorsgrupper samt kurser. Det behandlas även uppgifter om vårdnadshavares namn, personnummer, adress, e-postadress, telefonnummer samt koppling till barn.

I delsystemet Startsidan finns totalt 440 695 registrerade, varav 31 847 är anställda, 233 062 vårdnadshavare och 122 699 elever i kommunal grundskola och gymnasieskola.

Tekniska bristen
Den 27 juni 2019 infördes en ny funktionalitet på Startsidan där vårdnadshavare kunde söka på andra vårdnadshavare med barn i samma klass under förutsättning att vårdnadshavarna samtyckt till det. Den 24 augusti 2019 uppdagades det att de tekniska åtgärderna har brustit då en vårdnadshavare genom att ändra anrop i utvecklarverktyget i sin webbläsare med hjälp av personnummer kunde söka fram andra vårdnadshavare som fanns registrerade på Startsidan. Bristen har inneburit att alla registrerade vårdnadshavare i Skolplattformen har haft möjlighet att ta del av obehörig information. Denna brist har funnits sedan den nya funktionaliteten infördes i juni 2019. Utbildningsnämnden har identifierat en vårdnadshavare som har kommit åt obehörig information om sju unika personer. Ingen av de drabbade hade skyddad identitet.

Den tekniska bristen åtgärdades samma dag den uppdagades, den 24 augusti 2019, genom en kodändring som togs fram.

Datainspektionens bedömning

Krav på säkerhet
Datainspektionen konstaterar inledningsvis att i delsystemet Startsidan i Skolplattformen sker omfattande personuppgiftsbehandlingar som rör tusentals elever, vårdnadshavare och lärare. Det behandlas varierande uppgifter såsom vårdnadshavares personnummer, adress, e-postadress, telefonnummer samt koppling till barn.

Mot bakgrund av omfattningen av de personuppgiftsbehandlingar som sker i delsystemet Startsidan, behandlingarnas art och karaktär samt riskerna för de registrerades friheter och rättigheter anser Datainspektionen att höga krav ska ställas på de tekniska åtgärder som ska vidtas för att säkerställa en lämplig säkerhetsnivå i enlighet med artikel 32 i dataskyddsförordningen.

Bedömningen av tekniska åtgärder
Den tekniska bristen i Startsidan som nu granskas har inneburit att vårdnadshavare genom att ändra anrop i utvecklarverktyget i sin webbläsare med hjälp av personnummer kunde söka fram andra vårdnadshavare som finns registrerade på Startsidan. Detta innebär att vårdnadshavare har på ett enkelt sätt obehörigen kunnat komma åt andra vårdnadshavares personuppgifter. Utbildningsnämnden har således brustit i sin skyldighet

enligt artikel 32.1 i dataskyddsförordningen att med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter, vidta lämpliga tekniska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken i det aktuella delsystemet.

Datainspektionen bedömer att en lämplig säkerhet i detta fall omfattar en förmåga att fortlöpande säkerställa konfidentialitet hos behandlingssystemen och –tjänsterna. Den aktuella tekniska bristen borde enligt Datainspektionens bedömning ha upptäckts i ett tidigt skede innan behandlingen av personuppgifterna påbörjades. Att den aktuella bristen upptäcktes av en vårdnadshavare efter att delsystemet Startsidan lanserades, visar att utbildningsnämnden inte heller haft ett förfarande som uppfyller kraven i dataskyddsförordningen för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska vidtagna åtgärderna. Även detta är brist i kraven på lämplig säkerhet enligt artikel 32.1 i dataskyddsförordningen.

Utbildningsnämnden i Stockholms stad har således behandlat personuppgifter i det aktuella delsystemet i strid med artikel 32 i dataskyddsförordningen.

Datainspektionen bedömer vidare att Utbildningsnämnden i Stockholms stad har behandlat personuppgifterna i det aktuella delsystemet i strid med artikel 5.1 f i dataskyddsförordningen eftersom nämnden inte har säkerställt en lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling.

2.6 Administrationsgränssnittet

Vad Utbildningsnämnden i Stockholms stad har anfört under handläggningen

Allmänt om Administrationsgränssnittet
Administrationsgränssnittet var gemensamt för de två delsystemen Frånvaro/Närvaro och Schema i Skolplattformen, där inställningar för dessa delsystem utförs. Systemet läste data från Barn- och elevregistret som är källsystemet för grunddata i det aktuella delsystemet. Datat administrerades i detta gränssnitt och visades sedan upp för användarna i olika gränssnitt utifrån rollen i systemet och beroende på de inställningar som gjordes. Administrationsgränssnittet var inte avsett för vårdnadshavare. Personer med

en kombination av roller som exempelvis lärare eller kanslist som även är vårdnadshavare hade ingen tillgång till uppgifterna kopplade till rollen vårdnadshavare vid inloggning i detta gränssnitt. Personer som enbart hade rollen vårdnadshavare fick dock vid inloggning i Administrationsgränssnittet åtkomst till uppgifter kopplade till egna barn.

Bland de personuppgifter som hanterades är namn, personnummer, e-post, telefonnummer, avdelningens- eller grupp/klasstillhörighet, lärares koppling till grupp/klass/avdelning, lektionsinformation (grupp/klass/ämne/kurs, sal och tid), frånvarouppgifter (närvaro/frånvaro, orsak till frånvaro, giltig/ogiltig) samt ansökan om ledighet.

Tekniska brister

Den 26 augusti 2019 uppdagades att vårdnadshavare via sökning på Google hittat länkar för inloggning till Administrationsgränssnittet dit vårdnadshavare inte ska kunna logga in. Den aktuella bristen har inneburit att vårdnadshavare har kunnat ta fram rapporter för ”Kontaktuppgifter lärare” där namn, e-postadress och arbetstelefonnummer visats. Vidare har gränssnittet inte visat sig vara anpassat för hantering av sekretessbelagda uppgifter. Individer med skyddad identitet har inte haft en markering som avslöjar detta. Detta innebär att personer med skyddad identitet kan ha omfattats av den aktuella bristen, men att dessa inte går att urskilja från övriga registrerade.

Bristen har funnits sedan funktionen lanserades, troligtvis sedan augusti 2017**.** Den upptäcktes internt den 19 november 2018 och bedömdes då av utbildningsnämnden vara trivial eftersom utredningen då gjorde gällande att inga uppgifter som vårdnadshavare inte kunde se i ett annat gränssnitt visades. De skillnader som fanns t.ex. åtkomst till ”Kontaktuppgifter-Lärare”, sades då endast visa elevens aktuella lärare och vilka ämnen de har med eleven. Det sades även att inga kontaktuppgifter visades. Bristen skulle lösas med en kodsammanslagning som då planerades under 2019. Releasen som rättningen skulle omfattas av tidigt 2019 sköts dock på framtiden.

De personuppgifter som visades till följd av den aktuella bristen är kontaktuppgifter till lärare, såsom namn, klass, skola, ämne/kurs, e-postadress (både arbets- och privatadress) samt telefonnummer (både arbets- och privatnummer).

Det går inte att avgöra hur många vårdnadshavare som har loggat in i detta gränssnitt och felaktigt tagit del av uppgifter. Det går inte heller att få fram hur många av de lärare som rapporterna omfattar dessutom haft sin privata e-postadress inlagd i Barn- och elevregistret och som därmed kunnat visas för obehöriga. Utbildningsnämnden kan inte ange antalet registrerade som påverkades av denna tekniska brist. I dagsläget är det mellan 50 och 60 lärare som har skyddad identitet i detta delsystem. Utbildningsnämnden kan inte heller uppskatta vad den aktuella bristen inneburit för de registrerade eftersom nämnden inte har fått indikationer på konsekvenser.

Efter att sårbarheten uppdagades och kunde bekräftas begärde Stockholms stad den 26 augusti 2019 att leverantören skulle stänga åtkomsten för vårdnadshavare. Delsystemet stängdes ner och är inte längre i drift.

Datainspektionens bedömning

Krav på säkerhet

Datainspektionen konstaterar inledningsvis att i Administrationsgränssnittet behandlades uppgifter rörande lärare, såsom e-postadress (både arbets- och privatadress) samt telefonnummer (både arbets- och privatnummer). Det behandlades även uppgifter rörande lärare som har skyddad identitet. Datainspektionen anser såsom tidigare nämnts att uppgifter som rör personer med skyddade identitet är mycket skyddsvärda/integritetskänsliga då riskerna för de registrerades friheter och rättigheter är stora vid behandling av dessa personuppgifter. Mot bakgrund av karaktären och arten av de personuppgiftsbehandlingar som har skett i Administrationsgränssnittet samt riskerna för de registrerades friheter och rättigheter anser Datainspektionen att höga krav ska ställas på de tekniska åtgärder som ska vidtas för att säkerställa en lämplig säkerhetsnivå i enlighet med artikel 32 i dataskyddsförordningen.

Bedömningen av tekniska åtgärder

I Administrationsgränssnittet har vårdnadshavare via sökning på Google kunnat hitta länkar för inloggning till Administrationsgränssnittet dit vårdnadshavare inte ska kunna logga in. I detta gränssnitt har vårdnadshavare kunnat ta fram uppgifter om bl. a. lärares privata kontaktuppgifter såsom e-postadress och privata telefonnummer. Detta gränssnitt har också visat sig inte vara anpassat för hantering av uppgifter om individer med skyddad

identitet. Detta innebär att obehöriga personer har kunnat komma åt uppgifter om personer med skyddad identitet.

Eftersom den aktuella bristen har inneburit att obehöriga personer har haft möjlighet att komma åt uppgifter om personer med skyddad identitet har utbildningsnämnden brustit i sin skyldighet enligt artikel 32.1 i dataskyddsförordningen att med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter vidta lämpliga tekniska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

Datainspektionen bedömer att en lämplig säkerhet i detta fall omfattar en förmåga att fortlöpande säkerställa konfidentialitet hos behandlingssystemen och –tjänsterna. Den aktuella tekniska bristen borde enligt Datainspektionens bedömning ha upptäckts i ett tidigt skede innan behandlingen av personuppgifterna påbörjades. Den nämnda bristen har funnits under en lång period sedan systemet lanserades. Utbildningsnämnden blev uppmärksammad på bristen under november 2018, men valde att inte åtgärda den förrän bristen uppdagades på nytt i augusti 2019. Utbildningsnämnden har således brustit i nödvändigheten av att fortlöpande säkerställa konfidentialitet i det aktuella gränssnittet. Kravet på lämplig säkerhet inbegriper även att ha ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de vidtagna tekniska åtgärderna för att säkerställa behandlingens säkerhet vilket inte heller har förelegat i detta fall mot bakgrund av vad som ovan anförts.

Utbildningsnämnden i Stockholms stad har således behandlat personuppgifter i det aktuella delsystemet i strid med artikel 32 i dataskyddsförordningen.

Datainspektionen bedömer även i denna del att utbildningsnämnden har behandlat personuppgifter i det aktuella gränssnittet i strid med artikel 5.1 f i dataskyddsförordningen eftersom nämnden inte har säkerställt en lämplig säkerhet för personuppgifterna.

2.7 Konsekvensbedömningen

Vad Utbildningsnämnden i Stockholms stad anfört under handläggningen
Utbildningsnämnden uppger att eftersom Barn- och elevregistret produktionssattes innan den 25 maj 2018 har ingen heltäckande konsekvensbedömning enligt artikel 35 i dataskyddsförordningen ännu genomförts. Däremot har konsekvensbedömningar genomförts fortlöpande då nya funktionaliteter har lagts till.

Nämnden anser att en konsekvensbedömning behöver göras och arbete med detta pågår och ska slutföras i december 2020. De sårbarheter som har upptäckts vid penetrationstester har skyndsamt åtgärdats.
Utbildningsnämnden har vidare angett att det arbetas med en riskhanteringsplan, där det som upptäcks vid risk-och konsekvensanalyser åtgärdas systematiskt i enlighet med stadens riskmatris och att målsättningen är att det inom kort kommer att finnas en aktiv riskhantering för hela Skolplattformen. Utbildningsnämnden har en framtagen process för att säkerställa en adekvat informationssäkerhet som innebär att risk och konsekvensanalyser ska genomföras

Gällande Administrationsgränssnittet kommer ingen konsekvensbedömning att göras för denna del eftersom gränssnittet har avvecklats och inte längre är i bruk.

Datainspektionens bedömning
I de delsystem och moduler som varit föremål för Datainspektionens granskning behandlas elevers, skolpersonals samt vårdnadshavares personuppgifter av olika känslighetsgrad. De aktuella delsystem som omfattas av den aktuella tillsynen inbegriper behandling av ett stort antal personuppgifter om ett stort antal registrerade, som till stor del är barn, vilka i dataskyddsförordningen framhävs som sårbara fysiska personer[10].
Datainspektionen konstaterar att i de aktuella delsystemen sker omfattande personuppgiftsbehandling med olika typer av personuppgifter såsom betyg, utredningar om elever, utvecklingssamtal, särskilda anpassningar, barn- och vuxna med skyddad identitet. Vidare behandlas även känsliga personuppgifter i viss omfattning dvs. särskilda kategorier av uppgifter som avses i artikel 9.1 såsom hälsouppgifter. Det är således frågan om en

[10] Se skäl 75 i dataskyddsförordningen.

omfattande personuppgiftsbehandling om ett stort antal registrerade i systemet.

Datainspektionen konstaterar att det är frågan om en behandling som med beaktande av dess art, omfattning, sammanhang och ändamål sannolikt leder till en hög risk för fysiska personer rättigheter och friheter på ett sådant sätt som kräver att utbildningsnämnden skulle ha genomfört en konsekvensbedömning enligt artikel 35 dataskyddsförordningen. Av artikel 35.3 (b) framgår vidare att en konsekvensbedömning enligt punkt 1 särskilt ska krävas när det rör sig om behandling i stor omfattning av särskilda kategorier av uppgifter som avses i artikel 9.1. Datainspektionen konstaterar att behandlingen av personuppgifterna i de aktuella delsystemen är av den karaktären som anges i artikel 35.3 b dataskyddsförordningen, vilket är en omständighet som särskilt kräver en konsekvensbedömning.

Datainspektionen har, med ledning av riktlinjer från Artikel 29-arbetsgruppen och de kriterier som gruppen tagit fram[11], antagit en förteckning över när en konsekvensbedömning ska göras.[12]

Utöver de situationer som anges i artikel 35.3 i dataskyddsförordningen, och med beaktande av undantaget i artikel 35.10, ska en konsekvensbedömning avseende dataskydd göras om den planerade behandlingen uppfyller minst två av de nio kriterier som nämns i förteckningen.

I det här fallet behandlas känsliga uppgifter eller uppgifter av mycket personlig karaktär, uppgifter i stor omfattning samt uppgifter som rör sårbara registrerade vilka är tre av nio kriterier som enligt förteckningen talar för att en konsekvensbedömning ska genomföras.

Vidare anges i förteckningen när en konsekvensbedömning inte krävs. Det krävs inte någon konsekvensbedömning för behandlingar som har kontrollerats av en tillsynsmyndighet eller ett dataskyddsombud i enlighet

---

[11] 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, senast reviderade och antagna den 4 oktober 2017, WP 248 rev. 01. 2 (6) http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236. The European Data Protection Board (EDPB) har godkänt riktlinjerna den 25 maj 2018 https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents.pdf.

[12] Förteckning enligt artikel 35.4 i Dataskyddsförordningen, dnr DI-2018-13200

med artikel 20 i direktiv 95/46/EG och vars genomförande inte har ändrats sedan föregående kontroll. Som en god praxis bör dock en konsekvensbedömning ses över kontinuerligt och utvärderas regelbundet. Datainspektionen konstaterar att det inte föreligger någon omständighet som talar för att en konsekvensbedömning inte krävs. I 29-gruppens riktlinjer specificeras att även om det inte krävs en konsekvensbedömning den 25 maj 2018 är det nödvändigt för den personuppgiftsansvarige att utföra en sådan konsekvensbedömning, vid lämplig tidpunkt och som en del av dennes allmänna ansvarsskyldigheter.[13]
Datainspektionen konstaterar att den behandling av personuppgifter som sker i de aktuella delsystemen i Skolplattformen sannolikt leder till hög risk för fysiska personers rättigheter och friheter på ett sådant sätt att en konsekvensbedömning enligt artikel 35 i dataskyddsförordningen behöver genomföras i respektive delsystem som omfattas av den här tillsynen, för att bedöma den planerade behandlingens konsekvenser för skyddet av personuppgifter i enlighet med artikel 35.

Det faktum att systemet lanserades före den 25 maj 2018 påverkar inte inspektionens bedömning. Utbildningsnämnden uppger att anledningen till att de aktuella bristerna som orsakat de incidenter som inträffat i respektive delsystem inte upptäckts tidigare är att ingen heltäckande konsekvensbedömning har utförts.

Datainspektionen har i nu aktuell granskning bedömt att det har funnits tekniska brister i flera delsystem som tillsynen omfattat. Inspektionen har även bedömt att behörighetstilldelningarna har varit mer omfattande i den modulen där frågan har granskats (Skolpliktsbevakning). Mot bakgrund av utbildningsnämndens egna uppgifter som har framkommit i ärendet gällande konsekvensbedömning anser Datainspektionen att utbildningsnämnden, under perioden 25 maj 2018 fram till 27 augusti 2020, inte har genomfört en konsekvensbedömning som täcker delsystemen Skolpliktsbevakning, Elevdokumentation, Startsidan samt Administrationsgränssnittet i sin helhet. Om nämnden skulle ha gjort en fullständig konsekvensbedömning så kunde de konstaterade bristerna sannolikt undvikits. Utbildningsnämnden har således inte genomfört en konsekvensbedömning som uppfyller kraven i

[13] 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, senast reviderade och antagna den 4 oktober 2017, WP 248 rev. 01. 2 (6) s. 15-16 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

artikel 35 i de aktuella delsystemen och har därmed behandlat personuppgifter i strid med aktuell bestämmelse.

3. Val av ingripande

3.1 Möjliga ingripandeåtgärder

Datainspektionen har ett antal korrigerande befogenheter att tillgå enligt artikel 58.2 a–j i dataskyddsförordningen, bland annat att förelägga den personuppgiftsansvariga att se till att behandlingen sker i enlighet med förordningen och om så krävs på ett specifikt sätt och inom en specifik period.

Av led (i) i artikel 58.2 och artikel 83.2 i dataskyddskyddsförordningen framgår att Datainspektionen har befogenhet att påföra administrativa sanktionsavgifter i enlighet med artikel 83. Beroende på omständigheterna i det enskilda fallet ska administrativa sanktionsavgifter påföras utöver eller i stället för de andra åtgärder som avses i artikel 58.2.

Vidare framgår av artikel 83.2 vilka faktorer som ska beaktas vid beslut om att administrativa sanktionsavgifter ska påföras och vid bestämmande av avgiftens storlek.

Om det är fråga om en mindre överträdelse får Datainspektionen enligt vad som anges i skäl 148 i dataskyddsförordningen i stället för att påföra en sanktionsavgift utfärda en reprimand enligt artikel 58.2 b i dataskyddsförordningen. Hänsyn ska tas till försvårande och förmildrande omständigheter i fallet, såsom överträdelsens karaktär, svårighetsgrad och varaktighet samt tidigare överträdelser av relevans.

För myndigheter får enligt artikel 83.7 nationella kompletterande bestämmelser införas gällande administrativa sanktionsavgifter. Av 6 kap. 2 § dataskyddslagen framgår att tillsynsmyndigheten får ta ut en sanktionsavgift av en myndighet vid överträdelser som avses i artikel 83.4, 83.5 och 83.6 i dataskyddsförordningen. Då ska artikel 83.1, 83.2 och 83.3 i förordningen tillämpas.

3.2 Föreläggande

Datainspektionen har konstaterat att Utbildningsnämnden i Stockholms stad, genom att ha mer omfattande behörighetstilldelning än nödvändigt i delsystemet/modulen Skolpliktbevakningen, har behandlat personuppgifter i strid med artiklarna 5.1 f och 32.1 i dataskyddsförordningen.

Vidare har konstaterats att utbildningsnämnden, även om konsekvensbedömningar genomförts fortlöpande då nya funktionaliteter har lagts till, inte har uppfyllt kraven på att fullgöra en konsekvensbedömning i enlighet med artikel 35 i dataskyddsförordningen.

Utbildningsnämnden i Stockholms stad ska därför föreläggas att se till att behandlingen i dessa delar sker i enlighet med dataskyddsförordningen enligt följande.

Datainspektionen förelägger utbildningsnämnden, med stöd av artikel 58.2 d i dataskyddsförordningen, att begränsa behörighetstilldelningar i modulen Skolpliktbevakningen till de personer som har ett behov av att behandla personuppgifterna för att utföra sina arbetsuppgifter i den aktuella modulen.

Datainspektionen förelägger vidare utbildningsnämnden, med stöd av artikel 58.2 d i dataskyddsförordningen, att snarast genomföra en konsekvensbedömning i delsystemen Skolpliktsbevakning, Elevdokumentationen och Startsidan för vårdnadshavare som uppfyller kraven i artikel 35 i dataskyddsförordningen.

3.3 Sanktionsavgift ska påföras

Datainspektionen har ovan bedömt att utbildningsnämnden i de aktuella delsystemen har överträtt artikel 5 och artikel 32 i dataskyddsförordningen. Dessa artiklar omfattas av artikel 83.4 respektive 83.5 och vid en överträdelse av dessa ska tillsynsmyndigheten överväga att påföra administrativ sanktionsavgift utöver, eller i stället för, andra korrigerande åtgärder.

Mot bakgrund av att de konstaterade överträdelserna i delsystemen Skolpliktsbevakning, Elevdokumentation, Administrationsgränssnittet och Startsidan har rört ett mycket stort antal registrerade däribland barn och elever, samt omfattat brister i hantering av känsliga och integritetskänsliga personuppgifter däribland uppgifter om personer med skyddad identitet, uppgifter om hälsa, betyg m.m. är det inte frågan om en mindre överträdelse.

Det finns således inte skäl att ersätta sanktionsavgiften med en reprimand. Utbildningsnämnden ska således påföras administrativa sanktionsavgifter.

3.4 Fastställande av sanktionsavgiftens storlek

Generella bestämmelser
Enligt artikel 83.1 i dataskyddsförordningen ska varje tillsynsmyndighet säkerställa att påförandet av administrativa sanktionsavgifter i varje enskilt fall är effektivt, proportionellt och avskräckande.

För myndigheter gäller enligt 6 kap. 2 § andra stycket dataskyddslagen att sanktionsavgifterna ska bestämmas till högst 5 000 000 kronor vid överträdelser som avses i artikel 83.4 i dataskyddsförordning och till högst 10 000 000 kronor vid överträdelser som avses i artikel 83.5 och 83.6. Överträdelser av artikel 5 omfattas av den högre sanktionsavgiften enligt artikel 83.5, medan överträdelser av artikel 32 och 35 omfattas av det lägre maxbeloppet enligt artikel 83.4.

I artikel 83.2 i dataskyddsförordningen anges de faktorer som ska beaktas vid bestämmande av sanktionsavgiftens storlek. Vid bedömningen av storleken på sanktionsavgift ska bl. a. hänsyn tas till artikel 83.2 a (överträdelsens karaktär, svårighetsgrad och varaktighet), b (uppsåt eller oaktsamhet), g (kategorier av personuppgifter), h (hur överträdelsen kom till Datainspektionens kännedom) och k (annan försvårande eller förmildrande faktor till exempel direkt eller indirekt ekonomisk vinst) i dataskyddsförordningen.

Bedömning av förmildrande och försvårande omständigheter
Vid Datainspektionens bedömning av sanktionsavgift har hänsyn tagits till att det har varit överträdelser rörande flera artiklar i dataskyddsförordningen, varvid överträdelse av artikel 5 är att bedöma som allvarligare och omfattas av den högre sanktionsavgiften. För att sanktionsavgifter ska vara effektiva och avskräckande måste en proportionalitetsbedömning göras i varje enskilt fall.

En personuppgiftsansvarig ska innan lansering av ett nytt system säkerställa lämplig säkerhet. Kraven på den personuppgiftsansvarige och de åtgärder som vidtas för att säkerställa lämplig säkerhet måste ställas högt när det är frågan om en stor mängd registrerade och särskilt när det är frågan om uppgifter om t.ex. hälsa och skyddade personuppgifter, som innebär att känsliga och integritetskänsliga personuppgiftsbehandlingar sker.

I aktuellt fall har särskilt beaktats att Utbildningsnämnden i Stockholms stad har behandlat en omfattande mängd personuppgifter i den digitala plattform som används i Stockholms stad, Skolplattformen, och att överträdelserna har berört uppgifter om ett mycket stort antal registrerade, i vart fall över hundratusen registrerade. De aktuella överträdelserna har omfattat både integritetskänsliga och känsliga personuppgifter rörande barn som är extra skyddsvärda. Överträdelserna har även medfört att obehöriga kunnat få åtkomst till uppgifter om personer med skyddad identitet. Detta är personuppgifter som till sin art har ett högt skyddsvärde då det kan få mycket allvarliga konsekvenser för den enskilde fysiske personen om obehöriga får del av uppgifterna.

Vidare har följande försvårande och förmildrande omständigheter vägts in i de olika delsystemen som har granskats.

Skolpliktsbevakning

Försvårande omständigheter i modulen Skolpliktsbevakning är de risker för enskildas liv som orsakats av att obehöriga personer haft åtkomst till integritetskänsliga personuppgifter rörande ungefär 60 elever med skyddad identitet. En annan försvårande omständighet som inspektionen har beaktat är att utbildningsnämnden fortfarande inte har åtgärdat behörigheterna i modulen så att respektive användare endast har åtkomst till de uppgifter som hen behöver för att utföra sina arbetsuppgifter.

Elevdokumentationen

Det som har varit försvårande omständigheter gällande de brister som har funnits i Elevdokumentationen är att de tekniska bristerna som denna tillsyn omfattar har möjliggjort obehörig åtkomst till känsliga och mycket integritetskänsliga personuppgifter rörande i vart fall över hundratusen elever. Alla registrerade vårdnadshavare har, genom att på ett förhållandevis enkelt sätt manipulera systemet, haft möjlighet att komma åt uppgifter såsom personnummer, uppgifter om elever som går i särskola och elevers betyg och omdömen. De tekniska bristerna i Elevdokumentationen har utifrån utredningen i ärendet funnits under en period som är längre än ett halvår och upptäcktes av en vårdnadshavare.

Som förmildrande omständighet har utbildningsnämndens agerande att åtgärda bristerna efter upptäckten vägts in i bedömningen av sanktionsavgiftens storlek.

Startsidan
Den tekniska bristen i delsystemet Startsidan har uppkommit i samband med lansering av en ny funktionalitet. Det som har varit försvårande omständigheter är att bristen upptäcktes av en vårdnadshavare och inte av utbildningsnämnden. Detta tyder på att utbildningsnämnden inte har tillräckliga testförföranden vid lansering av nya funktionaliteter. Som förmildrande omständighet har inspektionen tagit hänsyn till att den aktuella bristen har funnits under en kort period samt att utbildningsnämnden åtgärdade bristen skyndsamt efter upptäckten.

Administrationsgränssnittet
Det som har varit försvårande gällande de brister som funnits i delsystemet Administrationsgränssnittet är att bristerna har kunnat medföra att obehöriga haft åtkomst till uppgifter om ungefär 50-60 anställda med skyddad identitet, vilket kan få mycket allvarliga konsekvenser för de enskilda individerna. Andra försvårande omständigheter som har vägts in i bedömningen av sanktionsavgiften är att de tekniska bristerna har funnits under en period som överstiger ett år och att utbildningsnämnden som under november 2018 blev uppmärksammad på att det fanns brister i Administrationsgränssnittet, inte vidtog åtgärder förrän bristerna uppdagades på nytt i augusti 2019.

Samlad bedömning av sanktionsavgiftens storlek
Datainspektionen bestämmer utifrån en samlad bedömning att Utbildningsnämnden i Stockholms stad ska betala en administrativ sanktionsavgift på 4 000 000 (fyra miljoner) kronor för de konstaterade överträdelserna i delsystemen Skolpliktsbevakning, Elevdokumentationen, Administrationsgränssnittet samt Startsidan för vårdnadshavare.

Detta beslut har fattats av generaldirektören Lena Lindgren Schelin efter föredragning av juristerna Salli Fanaei och Ranja Bunni. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom, enhetschefen Malin Blixt samt informationssäkerhetsspecialisten Adolf Slama medverkat.

Lena Lindgren Schelin, 2020-11-23 (Det här är en elektronisk signatur)

Bilaga
Hur man betalar sanktionsavgift.

Kopia för kännedom till:
Dataskyddsombudet för Utbildningsnämnden i Stockholm stad.

4. Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades. Om överklagandet har kommit in i rätt tid sänder Datainspektionen det vidare till Förvaltningsrätten i Stockholm för prövning.

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