Utbildningsförvaltningen
Avdelningen för utveckling och samordning

Utbildningsnämnden dnr 1.4.2-5702/2019
Datainspektionen dnr DI-2019-7024

Till
Datainspektionen
Box 8114
104 20 Stockholm

Yttrande angående behörighetsstyrningen hos utbildningsnämnden, Stockholms stad

Bakgrund

Utbildningsnämnden i Stockholms stad har den 3 december 2018 och den 3 april 2019 inkommit med anmälningar om personuppgiftsincidenter till Datainspektionen, dnr 1.4.2-9883/2018 respektive 1.4.2-2771/2019 avseende obehörig åtkomst av elevuppgifter.

Datainspektionen har beslutat att granska behörighetsstyrningen för åtkomsten till personuppgifter inom ramen för två moduler i Barn- och elevregistret (personuppgiftssamlingarna) hos utbildningsnämnden i Stockholms stad. Datainspektionen granskar även skyldigheten att informera de registrerade avseende de ovannämnda incidenterna.

Yttrande

Utbildningsnämnden, representerad av avdelningen för utveckling och samordning vid utbildningsförvaltningen, lämnar härmed följande svar.

Utbildningsnämnden nyttjar idag ett flertal system och e-tjänster som en del i dess pedagogiska och administrativa verksamheter. Digitala tjänster används i olika syften för att möta verksamhetens behov, både på central och lokal nivå och förvaltas av utbildningsnämnden, berörda facknämnder inom staden och leverantörer. Ansvaret för och tillhandahållandet av de digitala tjänsterna, där även åtkomst- och behörighetshanteringen inkluderas, kan ligga på flera aktörer inom Stockholms stad som exempelvis servicenämnden eller kommunstyrelsen.

Stockholms stads Skolplattform är ett stadsövergripande leveransobjekt där utbildningsnämnden i egenskap av informationsägare och kommunstyrelsen såsom systemägare ansvarar för den digitala plattformen. Stockholm stad använder PM3 som används för styrning av förvaltning och verksamhetsutveckling. Ansvaret utövas tillsammans med den verksamhetsnära representationen i objektets styrgrupp där även stadsdelsnämnderna som ansvarar för förskoleverksamheten samt arbetsmarknadsnämnden som ansvarar för vuxenutbildning är med. Styrgruppen har det yttersta ansvaret för det aktuella leveransobjektet. Detta gäller både det finansiella och att objektet uppfyller verksamhetens krav och mål.

I utbildningsnämndens informationsägaransvar tillsammans med representanterna i objektstyrgruppen ingår att säkerställa att informationen som hanteras inom objektet är tillförlitlig. Utbildningsnämnden är ytterst ansvarig för hur den egna verksamheten hanterar informationen i Barn- och elevregistret. Kommunstyrelsen ansvarar för att systemet uppfyller kraven på säkerhet i relation till skyddsvärdet som utbildningsnämnden fastställer för den information som hanteras i systemet.

Utbildningsnämnden ansvarar vidare för att informationen skyddas i enlighet med stadens riktlinjer för informationssäkerhet och gällande lagstiftning som dataskyddsförordningen med avseende på de skyddsåtgärder som riktar sig till verksamheten. Kommunstyrelsen har motsvarande skyldighet, men enbart avseende systemet ifråga. Utbildningsnämnden fastställer informationens skyddsvärde och verksamhetsspecifika risker samt säkerställer att implementering av de skyddsåtgärder som klassningen ger och som riktar sig till den egna verksamheten sker. Kommunstyrelsen ansvarar för implementeringen av systemrelaterade skyddsåtgärder. Kommunstyrelsen ansvarar även för att följa upp hur väl skyddsåtgärderna efterlevs i systemet. Utbildningsnämnden ansvarar för uppföljningen av hur väl skyddsåtgärderna efterlevs i den egna verksamheten.

1. Är utbildningsnämnden i Stockholms stad (ni) personuppgiftsansvarig för de personuppgiftsbehandlingar som har skett inom ramen för de aktuella personuppgiftsbehandlingarna enligt de ovannämnda incidenterna? Om ni anser att ni inte är den

personuppgiftsansvarige, uppge vem den personuppgiftsansvarige är samt varför ni anser det?

Ja, utbildningsnämnden i Stockholms stad är personuppgiftsansvarig för de personuppgiftsbehandlingar som har skett enligt incidenterna samt för nämndens verksamhet. Utbildningsnämnden ansvarar för drift och utveckling av kommunal verksamhet inom förskoleklass, grundskola, fritidshem, grundsärskola, gymnasieskola och gymnasiesärskola. Utbildningsnämnden ansvarar för 139 grundskolor, 32 grundsärskolor, 28 gymnasieskolor och sex gymnasiesärskolor. Stadsdelsnämnderna ansvarar för 560 kommunala förskolor. Detta innebär att staden ungefär har 323 500 vårdnadshavare och andra ansvariga vuxna, 92 000 elever, 32 000 barn i förskolor samt 23 000 pedagoger.

Utbildningsnämnden har också ett samordningsansvar för förskolorna inom staden. Detta innebär att utbildningsnämnden hanterar frågor som är stadsgemensamma för förskolorna i nära samverkan med stadsdelsnämnderna. Utbildningsnämnden ansvarar tillsammans med kommunstyrelsen för ärenden om riktlinjer, principer och uppföljning av förskoleverksamhet. Utbildningsnämnden tilldelar vidare behörigheter till de centrala funktionerna på stadsdelsnämnderna som arbetar med förskoleverksamheten samt till fristående anordnare.

Det ovanstående innebär dock inte att utbildningsnämnden är personuppgiftsansvarig för personuppgifter som behandlas inom ramen för förskoleverksamheten. Stadens stadsdelsnämnder har personuppgiftsansvaret för personuppgiftsbehandling som sker inom ramen för förskoleverksamhet. Arbetsmarknadsnämnden i Stockholm stad är personuppgiftsansvarig för personuppgiftsbehandling som sker inom vuxenutbildning.

Om ni anser att ni är personuppgiftsansvarig för personuppgiftsbehandlingar som har skett i de aktuella uppgiftssamlingarna vänligen svara på följande.

2. Beskriv personuppgiftsbehandlingen inom ramen för de aktuella uppgiftssamlingarna? Om behandlingarna sker i en del av ett system, ange namnet på systemet samt i vilken del av systemet behandlingarna sker.

A) Skolpliktsärendet

Behandling sker i utbildningsnämndens verksamhetssystem Barn- och elevregistret och Skolplikt är en modul i detta system. Modulen utgör ett administrativt systemstöd 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 §).

B) Ärendet med interkommunala avtal

Behandling sker i utbildningsnämndens verksamhetssystem Barn- och elevregistret och Interkommunala avtal är en modul i detta system. Modulen utgör ett administrativt systemstöd för att fullgöra utbildningsnämndens skyldigheter avseende skollagens regelverk om interkommunala elever samt handläggning och beslut i ärenden kopplade till dessa (se 10 kap. 25 och 27 §§ skollagen). Modulen Interkommunala avtal har inte implementerats fullt ut och används i dagsläget av ett begränsat antal användare. För närvarande finns endast personuppgifter avseende cirka tio elever i modulen.

3. Vilka personuppgifter behandlas inom ramen för de aktuella personuppgiftssamlingarna? Ange även vilka kategorier av uppgifter som behandlas såsom om känsliga personuppgifter behandlas och vilka uppgifter det rör. Se definitionen av känsliga personuppgifter nedan under Övriga upplysningar.

A) Skolpliktsärendet

I modulen behandlas följande personuppgifter:

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 kan även finnas namn, adress, personnummer och kontaktuppgifter (telefonnummer och e-postadress) till

kontaktperson eller annan ansvarig vuxen. Personuppgifter som tillhör annan ansvarig vuxen eller kontaktperson behandlas med samtycke som laglig grund.

Vidare behandlas följande beslut som innehåller personuppgifter som avser specifik elev:

- skolplikten har upphört (fullgjord skolplikt eller varaktig vistelse utomlands),
- fortsatt bevakning (annan orsak, föreläggande vid vite, skolplikt kvarstår efter utredning eller ärendet hos Skatteverket),
- medgivande att fullgöra skolplikten på annat sätt (annan orsak, filminspelning, nordisk skolgång eller utlandsresa), samt
- uppskjuten skolplikt (särskilda skäl).

Inga direkt känsliga personuppgifter hanteras inom modulen, men då modulen kan innehålla uppgifter om att en elev går på en resursskola eller grundsärskola kan det indirekt utgöra uppgifter om hälsa. Vidare kan uppgifter om modersmål finnas i modulen, vilket indirekt kan utgöra uppgifter om etnicitet.

B) Ärendet med interkommunala avtal

I modulen behandlas följande personuppgifter:

Personnummer, elevens namn, adress, boendekommun, avsändande kommun, mottagande kommun, lagrum för mottagande, ersättningsnivå kommuner emellan samt mottagande skola. Vidare finns ett fritextfält samt möjligheten att lägga till dokument. Det är även möjligt att ange om den interkommunala placeringen beror på vårdnadshavarens önskemål eller av särskilda skäl.

Inga direkt känsliga personuppgifter har hanterats inom modulen, men då modulen kan innehålla uppgifter om att en elev går på en resursskola eller grundsärskola kan det indirekt utgöra uppgifter om hälsa. Vidare är möjligt att i fritextfältet mata in uppgifter och ladda upp dokument som skulle kunna innehålla känsliga uppgifter, detta har dock i dagsläget inte gjorts.

4. Vilka grupper av registrerade finns inom ramen för uppgiftssamlingarna? Beskriv om det exempelvis finns barn i vilka åldrar och om det finns utsatta personer med skyddad identitet.

A) Skolpliktsärendet

I modulen sker behandling av samtliga elever som är folkbokförda i Stockholm i åldrarna 6 - 18 år. Elever med skyddade personuppgifter behandlas i modulen.

B) Ärendet med interkommunala avtal

I modulen sker endast behandling av elever i åldrarna 6 - 15 år som är folkbokförda i Stockholm och som går i skola i annan kommun samt elever folkbokförda i andra kommuner som går i Stockholm stads kommunala skolor. Utöver detta, kan under vissa förutsättningar även elever i åldrarna 16 - 18 år förekomma i modulen, exempelvis med anledning uppskjuten skolplikt enligt 7 kap 10 § skollagen, utebliven uppflyttning enligt 4 kap. 5 § skolförordningen eller att eleven fullgör utbildning efter att skolplikten upphört i enlighet med 7 kap. 15 § skollagen.

Modulen är även till för stadsdelsnämnderna att registrera förskolebarn. I och med att utbildningsnämnden upptäckte bristerna i modulen, rekommenderades stadsdelsnämnderna att inte använda funktionen.

5. Hur många antal registrerade finns det inom ramen för uppgiftssamlingarna? Hur många av dessa är elever? Hur många har skyddad identitet? Hur många av dem som har skyddad identitet är barn?

A) Skolpliktsärendet

För närvarande finns 1322 aktiva skolpliktsbevakningar (antal registrerade) varav 83 st. är under 7 år. Av 1322 aktiva skolpliktsbevakningar har 56 elever skyddade personuppgifter.

B) Ärendet med interkommunala avtal

För närvarande finns 9 elever som har interkommunala avtal i modulen. Inga elever har skyddade personuppgifter.

6. Har ni gjort en risk- och sårbarhetsanalys gällande hanteringen av personuppgifter inom ramen för de aktuella uppgiftssamlingarna? Om ja, när är den genomförd och vad resulterade den i?

Utbildningsnämnden har en process för återkommande informationsklassificeringar samt risk- och konsekvensanalyser av sina system. Som metod används stadens process för informationsklassificeringar. Metoden använder sig av Sveriges Kommuner och Landstings system KLASSA för att säkerställa en enhetlig värdering och hantering av nämndens informationssystem. Information om detta finns tillgänglig på stadens intranät. KLASSA består av klassificeringsområdena konfidentialitet, riktighet och tillgänglighet. Utbildningsnämnden använder Sveriges Kommuner och Landstings klassificeringsmatris som finns i tre säkerhetsnivåer, där tre är den högsta nivån.

Den 4 april 2019 genomfördes en ny informationsklassificering av Barn- och elevregistret, som hade till syfte att analysera vad som behöver skyddas, mot vad och hur. Syftet var även att uppdatera och justera tidigare klassningsunderlag. Informationsklassificering av Barn- och elevregistret ska ske årligen. 2018 års informationsklassificering visade på säkerhetsnivå 3 i konfidentialitet vilket innebär att röjande av information skulle medföra allvarlig skada. Informationsklassificeringen resulterade vidare i säkerhetsnivå 3 i riktighet då information som obehörigen, av misstag eller på grund av en funktionsstörning ändrats skulle medföra allvarlig skada. Avslutningsvis ledde även till säkerhetsnivå 2 i tillgänglighet. Detta innebär att ett avbrott skulle medföra betydande skada.

Den 8 april 2019 genomfördes en risk- och konsekvensanalys av Barn- och elevregistret för att kartlägga hot och risker samt upprätthålla ett starkt skydd för informationssäkerhet. Riskanalysen synliggjorde ett antal risker som utbildningsnämnden behöver och kommer att åtgärda samt bevaka i det fortlöpande förvaltningsarbetet. Arbetet med en riskåtgärdande handlingsplan för att minimera risken för incidenter har påbörjats. Arbetet kommer att bedrivas av kommunstyrelsen och utbildningsnämnden i samråd med

representanterna i styrgruppen. Utbildningsnämnden kommer utarbeta nya rutiner samt tydliggöra befintliga rutiner. Utbildningsnämnden ser behovet av återkommande uppföljning av vilka som har behörighet till systemet samt vilken behörighet de har för att säkerställa att rätt personer har rätt behörigheter fortlöpande.

Det finns framtagna lösningsförslag för IT-stöd vid hantering av behörigheter när en anställd slutar eller byter tjänst. Lösningsförslaget har dock inte kunnat implementeras då lösningsförslaget är beroende av integration från vårt HR-system som ännu inte godkänts. Kommunstyrelsens fortsatta arbete tar därför sikte på integrationerna i systemet. Kommunstyrelsens arbete sker i samverkan med leverantören för att kunna säkerställa korrekt och säker funktionalitet gällande behörighetsstyrning. Avslutningsvis ser utbildningsnämnden att utökning av loggar krävs för en systematisk och återkommande uppföljning.

Arbetet med handlingsplanen fortlöper under hösten och beräknas vara färdigställd i slutet av november 2019.

7. Hur sker tilldelning av behörigheter och vilka typer av behörigheter har ni inom ramen för uppgiftssamlingarna?

Rektorer och enhetschefer är behöriga att beställa och avbeställa behörigheter i Barn- och elevregistret åt sin personal. Detta görs genom en behörighetsblankett som skickas till en funktionsbrevlåda för grundskolans del och som därifrån vidarebefordras till leverantören. Rektor/enhetschef anger i blanketten vem som ska få behörighet och vilket omfång den ska ha behörighet till (enhet, avdelning, anordnare eller område enbart för personal som arbetar på central förvaltning). Även regi och skolform kan anges. Vidare ska information om vilken period den ska ha behörighet anges (om tillsvidare anges enbart från när behörigheten ska gälla), vilken behörighet/vilka behörigheter personen ska få, vem som beställer samt underskrift och datum.

De två varianter av behörigheter som finns är:

1. Administrativa roller.
   Dessa kan lägga till, ändra och ta bort uppgifter.
2. ”Titta”-roller.
   Dessa kan enbart se samt exportera information.

Det finns även en begränsning i respektive behörighetsroll avseende tillgången till sekretessmarkerade personer.

Vad gäller behörighetshanteringen för förskolan, finns vissa centrala funktioner vid utbildningsnämnden som har och behöver ha tillgång till Barn- och elevregistret förskola. Utbildningsnämnden tilldelar behörigheter för dessa funktioner men även för centrala funktioner (köhandläggare samt controllers) vid stadsdelsnämnderna som arbetar med förskoleverksamheten samt för Serviceförvaltningen som ansvarar för stadens kontaktcenter och avgiftshantering för förskola och fritidshem. Detta enligt uppdrag från kommunfullmäktige.

Tilldelning av behörighet för förskolans roller i Barn- och elevregistret sker utifrån ansökan som görs på avsedd blankett. Det är i första hand behörig chef som avgör behovet. De behörigheter som hanteras av utbildningsnämnden kontrolleras så att ansökt roll i Barn- och elevregistret är relevant mot personens arbetsuppgifter.

8. Vilka bedömningar ligger till grund för tilldelningen av behörigheterna?

I och med att det är enhetschef eller rektor som leder och fördelar arbetet, avgör ansvarig chef behovet av tillgång till systemet. Tilldelningen av behörigheten utgår från att enhetschefen eller rektor redan gjort en bedömning av lämpligheten och nödvändigheten. Vid beställning av behörighet får enhetschefen eller rektorn bekräfta att denne är införstådd i att Stockholms stad tillämpar principen att behörighet tilldelas efter relevant behov för att den anställde ska kunna utföra sina arbetsuppgifter enligt befogenheter samt att denne är införstådd i ansvaret att omgående meddela när behörigheten ska avslutas.

Behörighetstilldelaren kontrollerar att ansökt roll i Barn- och elevregistret är relevant mot personens arbetsuppgifter. Behörighetsroller i Barn- och elevregistret är anpassade efter användares behov av information för att utföra sitt arbete. Vid uppenbara felbeställningar har kontrollfrågor skickats till enhetschefen eller rektor så att beställaren återigen bekräftar

beställningen i de fall den stämmer. Enhetschefen eller rektor har i några fall också direkt avråtts från att beställa vissa roller.

Det finns ett pågående arbete som syftar till att rekommendera vilka behörigheter som varje användartyp/befattning bör ha för att administrationen ska ske på ett mer säkert, effektivt och användarvänligt sätt. En utredning av utbildningsnämndens behörighetsstyrning i samtliga digitala tjänster pågår och kommer till hösten att lämnas till utbildningsförvaltningens ledningsgrupp för beslut om åtgärdsplan. Utredningen har hittills synliggjort utmaningarna som finns då ansvaret för att få åtkomst till system och få behörigheter blivit utspritt mellan olika förvaltningar i staden och är komplext med många intressenter, rutiner som behöver förtydligas, manuell hantering, långa ledtider samt viss otydlighet i behörigheter. Utredningen överensstämmer med de risker som identifierats och de riskminimerande åtgärder som är planerade.

Utredningen lämnar även förslag till styrande principer ur ett verksamhetsmässigt perspektiv som syftar till att säkerställa korrekta, effektiva och säkra behörigheter. Dessa är bland andra att det ska finnas enhetliga och tydliga rutiner för hur behörigheter tilldelas, ändras och avslutas, att identiteter och åtkomst ska styras utifrån användarens uppdrag, att identiteter och åtkomst ska enkelt kunna kontrolleras och granskas för att se vem/vilka som har behörighet till vilket/vilka system, och att hantering av identiteter och åtkomst ska löpande planeras och kontrolleras av utbildningsnämnden.

9. Vilka faktiska åtkomstmöjligheter ger de olika tilldelade behörigheterna i de aktuella uppgiftssamlingarna?

I Barn- och elevregistret finns en organisationsstruktur som styr vilken nivå behörigheter tilldelas. Alla skolor kopplas mot en nivå i organisationsstrukturen. Användare som har behörighet på ett område ser samtliga skolor som är kopplade till det området samt alla elever och personal som hör till de skolorna så länge behörighetsrollen innehar behörighet att se dessa uppgifter

Strukturen är:
Stockholm
Regi (kommunal eller fristående)
Stadsdelar

Basområden eller geografiska områden inom varje stadsdel
Enhet (en specifik skola/förskola)

A) Skolpliktsärendet

1873 personer har roller som möjliggör tillgång till Skolpliktsbevakning. De roller som har tillgång till Skolpliktsbevakning är:

Gr Systemansvarig Sthlm (77st)
Gr Administratör Ersättningar Sthlm (62st)
Gr Titta Sthlm (961st)
Gr Administratör Språkcentrum Sthlm (16st)
Gr PMO-ansvarig Sthlm (17st)
Gr Administratör Skola Sthlm (978st)
Gr Skolpliktsbevakning Central Admin Sthlm (34st)
Gr Titta Ekonomi Sthlm (51st)

De ovanstående rollerna avser inte antal unika personer, vissa användare har flera roller. Samtliga dessa roller kan söka och se lista av skolpliktsbevakade personer bestående av personnummer, efternamn, förnamn, skolpliktsområde etc. För uttömmande uppräkning, se svar under fråga 3. Varje användare har till sin behörighetsroll ett omfång kopplat som anger vilka personer användaren får se vid sökning i funktionaliteten för skolpliktsbevakning. De flesta användare med rollerna Gr Administratör Skola Sthlm samt Gr Titta Sthlm har enbart behörighet till en skola och kan bara se de registrerade som hör till skolans skolpliktsbevakningsområde.

B) Ärendet med interkommunala avtal
1879 personer har roller som möjliggör tillgång till modulen Interkommunalt avtal, varav 793 personer på område ‘Barn i annan kommun’ (elever folkbokförda i Stockholm stad men som går i en skola i en annan kommun), 403 personer på område ‘Stockholm’ och 683 personer finns på övriga enstaka områden och enheter.

De roller som har tillgång till interkommunalt avtal är:

Gr Administratör Ersättningar Sthlm (62 st.)
Gr Systemansvarig Sthlm (77 st.)
Gr Titta Ekonomi Sthlm (51 st.)

Gr Titta Sthlm (960 st.)
Gr Administratör Skola Sthlm (977 st.)
Fsk Systemansvarig Sthlm (74 st.)
Fsk Ersättningshandläggare Sthlm (26 st.)
Fsk Köhandläggare Sthlm (56 st.)

De ovanstående rollerna avser inte antal unika personer, vissa användare har flera roller. Samtliga dessa roller kan söka och se lista av barn/elever som innefattas av interkommunalt avtal. Rollen Gr Administratör Skola Sthlm kan endast se elever inskrivna i den skolan administratören arbetar på. De kan inte se elever i andra skolor. Listan visar personnummer, efternamn, förnamn, boendekommun, avsändande kommun, mottagande kommun etc. För uttömmande uppräkning, se svar under fråga 3.

10. Finns det en policy, rutiner eller instruktioner för hur behörigheterna får användas i uppgiftssamlingarna? Var eller hur kan den anställde ta del av dessa?

Ja, Skolplattformen nyttjar stadens IT-infrastruktur där åtkomst och behörigheter till systemet begränsas enligt stadens regelverk för informationssäkerhet och medförda förutsättningar.
Staden har generella riktlinjer för informationssäkerhet som samtliga anställda kan ta del av via stadens intranät. Av riktlinjerna avseende användarregistrering framgår bland annat att all hantering av behörigheter ska ske enligt instruktion och att verksamhetschef beslutar om aktuell behörighet. Vid tilldelningen av behörigheter i centrala system ska beslut om beställningen fattas av verksamhetschefen eller rektor. Beställningsrutiner och instruktioner för lokala system ska tas fram av respektive förvaltning och användarna ska ha unik användaridentitet. Grupp-ID får bara tillåtas om det är absolut nödvändigt av verksamhets- eller driftskäl och ska då dokumenteras och godkännas av verksamhetsansvarig chef.

Vidare finns en mängd behörighetsrelaterad information som exempelvis anvisningar, beställningsformulär och instruktioner som avser användning av Skolplattformen och däribland Barn- och elevregistret. Den behörighetsrelaterade informationen finns på stadens intranät. På intranätet anges att Barn- och elevregistrets administratörer på respektive skola kan se vilka behörigheter som finns tilldelade på den specifika skolan. Det finns vidare korta förklaringar av de olika behörighetsrollerna

som finns för att klargöra vad rollen kan göra. Syftet är att mer omfattande behörighet än vad som är nödvändigt inte ska beställas. Det tydliggörs även att det är rektors ansvar att se till att rätt person har rätt behörighet. Även vikten av avanmälan samt nyanmälan av behörigheter betonas.

Utbildningsnämnden anordnar utbildningar för personal som arbetar i Barn- och elevregistret, där bland annat information om behörighetshantering ges till personalen.

11. Dokumenterar ni vilka användare som haft elektronisk tillgång till personuppgifter genom behandlingshistorik (loggar) i de aktuella uppgiftssamlingarna? Beskriv hur logguppföljningen sker.

I dagsläget finns det ingen funktionalitet som möjliggör dokumentation av användares specifika behandlingshistorik i modulerna Skolpliktsbevakning och Interkommunala avtal. I Barn- och elevregistret går det dock att se vilka som har haft en viss behörighet. Vidare loggas all sökning av behörig användare på sekretessmarkerad person eller sökurval som innefattar sekretessmarkerad person. Det är möjligt att ta fram loggar som avser en viss tidsperiod eller personer.

I användarloggen kan man söka fram händelser som utförts av användare. Ett exempel på detta är när en sökning görs av behörig person efter sekretessmarkerad elev eller personal och tar del av de sekretessbelagda personuppgifterna. Det skapas en logg om detta. Däremot går det inte alltid att se att det är specifikt via Skolpliktsbevakning eller Interkommunala avtal som loggningen har skett. Det går att jämföra personer i användarloggen med de som har en roll som ger tillgång till Skolpliktsbevakning eller Interkommunala avtal.

Det finns andra generella loggningar i systemet, men dessa avser inte modulerna Skolpliktsbevakning eller Interkommunala avtal specifikt.

12. Genomför ni systematiska och återkommande kontroller av loggarna för att se om någon obehörig åtkomst till uppgifterna förekommit? Beskriv dessa rutiner. Finns det rutiner för åtkomstkontroll på förekommen anledning.

I dagsläget genomförs inga återkommande eller slumpmässiga kontroller av loggarna. Uppföljning och kontroll av loggar sker när det finns skäl att misstänka att en användare använt sin behörighet på ett otillbörligt sätt. Kontrollen och uppföljningen sker då genom att utbildningsnämnden i samråd med kommunstyrelsen kontaktar leverantören och begär ut loggar från systemet.

13. På vilket sätt säkerställer ni behörighetsstyrningen vid uppdatering och testning av de aktuella delarna av systemet?

Skolplattformens tester utförs i acceptansmiljöer som är specifikt avsedda för test. De använder till övervägande del avidentifierad data vilket innebär att testanvändare inte arbetar med riktigt persondata. Drygt 1140 personers riktiga data används i testmiljön. Det rör sig om testpersonals personuppgifter som dessa medgivit samtycke till att behandlas med syfte att användas som testfall i kommande releaser. Avidentifiering kommer att ske den 6 september 2019. En översyn av samtyckeshantering vid användning av riktigt data har initierats och fortlöper under hösten 2019. Testdatat uppdateras två gånger per år och i samband med detta så sparar förvaltningen behörighetsuppgifterna för testanvändarna för att kunna återanvända dem efter att nya testdata har genererats. Behörigheterna för testanvändarna varierar beroende på vilken roll och funktion som ska testas. I 2019 års aktivitetsplan för Barn- och elevregistret kommer aktiviteter för att ta fram och förmedla instruktioner och riktlinjer avseende behörigheter för användare att läggas till. Aktivitetsplanen stäms av och förnyas för år 2020.

Vid vissa tillfällen behöver test även kunna genomföras i den s.k. pre-produktionsmiljön (som är en spegling av produktionsmiljöerna). Här används riktiga användardata och testanvändarna administreras via acceptanstestledaren vid utbildningsförvaltningen. Testanvändarna har samma behörigheter i produktionsmiljöerna, detta innebär att användarna inte ser mer än vad dessa borde. Utbildningsnämnden har sett ett

behov av att utarbeta processbeskrivningar och riktlinjer som stärker arbetet ytterligare. Detta pågår för närvarande och beslut väntas fattas under hösten.

När det gäller verifiering och kvalitetssäkring av releaser så genomgår de steg som görs i leverantörens produktutvecklingsprocess. Det innebär att det team som infört en ny funktionalitet eller gjort rättningar gör kodgranskning samt test i utvecklingsmiljön. I steg två genomförs systemtest för att säkra att ny funktionalitet och rättningar inte tillfört några oönskade beteenden på systemnivå. Allt detta enligt den gemensamma definitionen för när något är slutfört i processen för leverantörens produktutveckling.

Detta är begränsat till Barn- och elevregistrets egna testmöjligheter och kan inte jämföras med den produktionsliknande miljö som finns hos staden. Det betyder att simulerad data som finns i leverantörens tester inte kan jämföras med den som finns i stadens preproduktions- och produktionsmiljöer där alla roller och behörigheter finns representerade.

Enligt de inkomna anmälningarna om personuppgiftsincidenter har obehörig åtkomst inträffat inom ramen för skolpliktsbevakningen samt i barn- och elevregistret. Svara på följande frågor gällande de inträffade incidenterna:

14. Beskriv de inträffade incidenterna i respektive anmälan utförligt.

A) Skolpliktsärendet
Systemet saknade logik för att i funktionaliteten för skolpliktsbevakning begränsa behörigheten till sekretessmarkerade personer. Detta resulterade i att samtliga användare vars behörighetsroll inkluderade behörighet till skolpliktsbevakning samt att se sekretessmarkerade personer fick upp samtliga sekretessmarkerade utan skolplacering.

Antal användare som potentiellt skulle kunna ha sett sekretessmarkerade personer felaktigt är 1295. Troligen är antalet i praktiken betydligt lägre med anledning av att manualen för skolorna visar att man ska söka med område och ta fram sin enhet. I dessa sökningar kommer inte sekretessmarkerade

personer med i sökresultatet, sekretessmarkerade personer visades endast om man sökte utan område. Enheten för ersättning och skolplikt har även haft utbildning för skolorna där detta framgått tydligt. Minst hälften av stadens kommunala grundskolor hade vid tidpunkten för incidenten tagit del av utbildningen.

Utbildningsnämnden har endast kännedom om att en skoladministratör felaktigt sett uppgifter om sekretessmarkerade elever. Skoladministratören som kontaktade enheten för ersättning och skolplikt på utbildningsnämnden fick fram tre sekretessmarkerade elever i sökresultatet. Det fanns totalt 60 elever med sekretessmarkering i Skolpliktsbevakning. Då det inte gick att återskapa den exakta sökningen som administratören hade gjort, är orsakerna bakom antalet sekretessmarkerade elever i skoladministratörens sökresultat okända.

Vid upptäckt den 5 oktober 2018 var det inte verifierat om användare såg personer dessa inte var behöriga att se. Först den 5 november 2018 kunde man verifiera att användare såg mer information än de ska vara behöriga att se. Då eskalerades ärendet och leverantören arbetade snabbt fram en rättning. Denna rättning kom i produktion den 9 november 2018.

B) Ärendet med interkommunala avtal

Den 25 mars 2019 skickades en felanmälan till leverantören av Barn- och elevregistret gällande brister i behörighetsstyrningen i funktionaliteten för modulen Interkommunala avtal. I felanmälan angavs att användare inom förskoleverksamhet kunde söka upp elever i skolverksamhet. I modulen, som förskolan ännu inte börjat använda men har tillgång till, registreras ärenden som rör avtal mellan kommuner om barn som går i andra kommuners verksamhet. Det upptäcktes att för behörigheten för förskolan som tillhör stadens stadsdelsnämnder visas även uppgifter om skolelever och för behörigheten för skolan visas även uppgifter om förskolebarn. Personal på stadsdelsnämnderna som arbetar med förskola kan söka fram personuppgifter som rör elever inskrivna i fritidshem och fritidsklubb. Vidare skulle dessa potentiellt kunna se elever med skyddade personuppgifter och vilket fritidshem/fritidsklubb eleven är inskriven i. Användaren som upptäckte felet kontaktade även förvaltningen av Barn- och elevregistret hos utbildningsnämnden samt utbildningsnämndens

Dataskyddsombud för att informera om problemet.

Utbildningsnämnden tog kontakt med leverantören samma dag för att säkerställa att arbetet med att ta fram en rättning skulle ske skyndsamt. Nämnden begärde att leverantören prioriterade ärendet till en viss nivå vilket innebar att rättningstiden var 7 timmar och 30 minuter. Inom tre timmar från det att utbildningsnämnden kontaktat leverantören svarade leverantören att ett lösningsförslag är att rollen läggs på område, regi och verksamhet i stället för rollen fortsätts läggas på område. Klockan 17:47 samma dag meddelade leverantören att de tagit fram en rättning som innebär att hänsyn tas till rollens behörighet på skolform/verksamhet samt att det är planerat att levereras den 17 maj 2019. Rättningen implementerades den 17 maj 2019.

Då lösningen innebar bland annat att alla användare med behörighet på nivå ”område” måste läggas om till skolform/verksamhetsform och regi gjordes en tillfällig lösning. Lösningen innebär att modulen tas bort för stadsdelsnämnderna. Detta innebär inget hinder för dem då de ännu inte tagit funktionen i bruk.

Det långsiktiga arbetet med att komma tillrätta med behörighetstilldelningen samt konsekvenserna som uppstår vid korrekt behörighetstilldelning är påbörjat och fortlöper under hösten 2019. Det finns skäl för staden att misstänka att om enbart behörigheterna läggs om riskerar användare att inte se alla de uppgifter de behöver för att kunna fullfölja sina uppdrag i enlighet med skollagen. Av den anledningen behöver konsekvenserna utredas noga och risken för detta elimineras.

15. När inträffade respektive incident? Om ni inte kan uppge när förklara vad detta beror på. Beskriv även utförligt när incidenterna upptäcktes.

A) Skolpliktsärendet

Utbildningsnämnden kan inte ange när incidenten inträffade. Modulen implementerades juli 2017. Vid detta tillfälle hade utbildningsnämnden ingen kännedom om några brister. Utbildningsnämnden upptäckte incidenten 5 oktober 2018.

B) Ärendet med interkommunala avtal

Utbildningsnämnden bedömer att incidenten sannolikt inträffade i samband med en implementering i oktober 2018.

16. Vad har föranlett de inträffade incidenterna? Beskriv detta i detalj.

A) Skolpliktsärendet

Systemet saknade logik för att i funktionaliteten för skolpliktsbevakning begränsa behörigheten till sekretessmarkerade personer. Orsaken till detta är i dagsläget okänd. Detta resulterade att samtliga användare vars behörighetsroll inkluderade behörighet till skolpliktsbevakning samt att se sekretessmarkerade personer fick upp samtliga sekretessmarkerade utan skolplacering. En anställd som på en skola i kommunal regi utförde skolpliktsbevakning kunde se elever som hade skyddade personuppgifter. Rutinen är att anställda på skolorna inte ska kunna se dessa elever då denna handläggning endast sker centralt. Den anställde kunde inte se alla elever med skyddade personuppgifter i staden utan endast tre personer.

B) Ärendet med interkommunala avtal

Förskoleverksamheten och skolverksamheten ska i Barn- och elevregistret vara helt separata. Det rör sig om en brist i utvecklingen där en kontroll inte skett i funktionen gentemot användarens behörighet på skolform och verksamhetsform. Vidare migrerades behörigheter på ett felaktigt sätt från det föregående IT-stödet Bosko. Migreringen genomfördes genom att

behörigheterna lades in i nuvarande IT-stöd på samma sätt som de var upplagda i föregående IT-stöd. Det nya IT-stödet har inte samma grundstruktur som föregående vilket innebar att behörigheterna skulle lagts upp på ett annat sätt för att inte ge för bred behörighet. Utbildningsnämnden misstänker att vid tilldelning på korrekt nivå så får användare inte se barn och elever de måste för att staden ska kunna uppfylla kravet på platsgaranti i enlighet med 8 kap. 3 § skollagen.

17. Är det samma eller olika orsaker som ligger till grund för incidenterna? Är det de organisatoriska eller de tekniska åtgärderna som har brustit? Beskriv på vilket sätt.

A) Skolpliktsärendet

Incidenten inträffade på grund av lösningens implementering. Systemet saknade logik för att i funktionaliteten för skolpliktsbevakning begränsa behörigheten till sekretessmarkerade personer. Orsaken till detta är i dagsläget okänd. Skolpliktsbevakningen på stadens kommunala grundskolor utgår från boendeområde. Sekretessmarkerade personer som är oplacerade saknar boendeområde i systemet. Det rör sig därför om tekniska åtgärder som brustit.

B) Ärendet med interkommunala avtal

Incidenten inträffade på grund av rollstrukturens uppbyggnad i systemet. Det rör sig om en miss i utvecklingen där en kontroll inte skett i funktionen gentemot användarens behörighet på skolform och verksamhetsform. Vidare migrerades behörigheter på ett felaktigt sätt från det föregående IT-systemet för barn- och elevregister för grundskola och förskola då det nya IT-stödet inte har samma grundstruktur som föregående. Detta innebar att behörigheterna skulle lagts upp på ett annat sätt för att inte ge för bred behörighet. Det rör sig därför om tekniska åtgärder som brustit.

18. Hur många registrerade har påverkats av respektive incident samt på vilket sätt?

A) Skolpliktsärendet

Antalet registrerade som skolpersonal eventuellt felaktigt sett är 60 sekretessmarkerade elever. Utbildningsförvaltningen har enbart kännedom om att en skoladministratör med skolpliktsansvar sett mer än vad hen egentligen ska ha sett. Utbildningsnämnden har inte fått indikationer på att registrerade på något sätt ska ha påverkats av incidenten.

B) Ärendet med interkommunala avtal

Antalet registrerade som skolpersonal eventuellt felaktigt sett är 9 Inga elever var sekretessmarkerade. Utbildningsnämnden har inte fått indikationer på att registrerade på något sätt ska ha påverkats av incidenten

19. Har incidenterna omfattat uppgifter om personer som lever med skyddad identitet? Om ja, ange antalet registrerade som påverkats av respektive incident? Vad har respektive incident inneburit för dessa registrerade? Vad har varje incident inneburit för de övriga registrerade? Beskriv konsekvenserna av incidenterna.

A) Skolpliktsärendet

Incidenten har omfattat uppgifter om sekretessmarkerade elever. Antalet är 60 elever. Incidenten har inneburit att skoladministratörer med skolpliktsansvar kunnat se sekretessmarkerade elever som är oplacerade.

B) Ärendet med interkommunala avtal

Nej, incidenten har inte omfattat uppgifter om elever med skyddade personuppgifter. Incidenten har inneburit att personal som arbetar på stadsdelsnämnder kunnat se och söka fram personuppgifter som rör barn på fritidshem och fritidsklubb och därmed se vilket fritidshem eller fritidsklubb eleven är placerad på.

20. Enligt anmälningarna har incidenterna inneburit obehörig åtkomst internt eller externt. Lämna en detaljerad redogörelse om den obehöriga åtkomsten. Hur många har tagit del av informationen som de saknade behörighet till? Hur många har haft möjlighet att ta del av uppgifter som de saknade behörighet till? Svara även på sistnämnda frågor avseende barn med skyddad identitet.

A) Skolpliktsärendet

Incidenten har inneburit intern obehörig åtkomst. 133 personer har via Skolpliktsbevakning haft möjlighet att se uppgifter i modulen samt sekretessmarkerade personer. Detta innebär att 133 användare har haft en roll som gör att dessa kan se sekretessmarkerade elever. Detta innebär inte att samtliga användare tagit del av information de saknade behörigheter till. Utbildningsnämnden och leverantören kan ta fram hur många personer som har tillgång till rollerna och som har behörighet att se skyddade personuppgifter som del av Skolpliktsbevakning. Leverantören loggar de som söker på sekretessmarkerade personer, det är dock inte möjligt att se att detta kommer från modulen Skolpliktsbevakning. Utbildningsnämnden har enbart kännedom om att en skoladministratör med skolpliktsansvar sett elever hen inte borde haft behörighet att se.

I nuläget har bara personer med behörigheten område Stockholm möjlighet att se personer med skyddad identitet.

B) Ärendet med interkommunala avtal

Staden och leverantören kan ta fram hur många personer som har tillgång till rollerna och som har behörighet att se skyddad identitet som del av Interkommunala avtal. Leverantören loggar de som söker på sekretessmarkerade personer, det går dock inte att se om detta kommer från modulen Interkommunala avtal. 57 köhandläggare på stadsdelsnämnderna har haft en roll och behörighet som gör att dessa kan se Interkommunala avtal. Detta innebär inte att 57 användare tagit del av information de saknade behörigheter till. Utbildningsnämnden har ingen kännedom om någon köhandläggare tagit del av uppgifter dessa saknat behörighet till då det var utbildningsnämnden som upptäckte bristen.

21. Har ni åtgärdat incidenterna? Beskriv i detalj på vilket sätt.

A) Skolpliktsärendet

Ja, rättningen innebar att i modulen Skolpliktsbevakning ska endast användare som har behörighet till hela Stockholm kunna se personer som saknar nyckelkod/område och därmed har skyddade personuppgifter och är oplacerade.
I sökresultatet visas elever utifrån dataurvalet, det vill säga de elever användaren har rätt att se. Har den inloggade användaren däremot rätt att se hela område Stockholm, vilket avser handläggarna som arbetar på enheten för ersättning skolplikt, kommer även elever som inte har någon placering på någon enhet att visas i sökresultatet.
Rättningen levererades den 9 november 2018.

B) Ärendet med interkommunala avtal

Leverantören har gjort en ändring i modulen Interkommunala avtal, vilket innebär att systemet tar hänsyn till rollens behörighet på skolform/verksamhet. Staden har fått information om att rollerna måste läggas på område, regi och verksamhet för att styra användaren till rätt verksamhet samt att interkommunala avtal måste kopplas till skolform/verksamhet. Innan detta kan införas måste omfattande tester föras. För att tillfälligt lösa problemet har det gjorts en begränsning av vad behörighetsrollen på stadsdelsnämnderna kan se.

22. Har ni undanröjt eller minimerat risken för en liknande incident? Hur har ni gjort detta?

Staden arbetar fortlöpande undanröjande och riskminimerande där en tät dialog finns inom staden men även med leverantören för att säkerställa att systemen uppfyller kraven lagstiftningen ställer. Vidare har staden kontinuerliga och återkommande GDPR-forum tillsammans med leverantören för att säkra den personliga integriteten samt ändamålsenlig och säker utveckling av systemet.

Avseende modulen Interkommunala avtal är ett möte mellan utbildningsnämnden och leverantören inbokad september 2019 för att planera en långsiktig begränsning och tilldelning av behörigheter som är verksamhetsanpassad.

Arbetet med en riskåtgärdande handlingsplan för att minimera risken för incidenter utifrån en risk- och konsekvensanalys har påbörjats. Arbetet med handlingsplanen kommer att bedrivas av kommunstyrelsen och utbildningsnämnden i samråd med representanterna i objektets styrgrupp som ytterst styr och leder utvecklingen framåt. Utbildningsnämnden kommer utarbeta nya rutiner samt tydliggöra befintliga rutiner. Utbildningsnämnden ser även behovet av återkommande uppföljning av vilka som har behörighet till systemet samt vilken behörighet de har för att säkerställa att rätt personer har rätt behörigheter fortlöpande. Det finns framtagna lösningsförslag för IT-stöd vid hantering av behörigheter när en anställd slutar eller byter tjänst. Lösningsförslaget har dock inte kunnat implementeras då lösningsförslaget är beroende av integration från stadens HR-system som ännu inte godkänts. Kommunstyrelsens fortsatta arbete tar sikte på integrationerna i systemet. Kommunstyrelsens arbete sker i samverkan med leverantören för att kunna säkerställa korrekt och säker funktionalitet gällande behörighetsstyrning. Avslutningsvis ser utbildningsnämnden att utökning av loggar krävs för en systematisk och återkommande uppföljning.

Arbetet med handlingsplanen fortlöper under hösten och beräknas vara färdigställd slutet av november 2019.

Det finns ett pågående arbete som syftar till att rekommendera vilka behörigheter som varje användartyp/befattning bör ha för att administrationen ska ske på ett mer säkert, effektivt och användarvänligt sätt. En utredning av utbildningsnämndens behörighetsstyrning i samtliga digitala tjänster har gjorts och kommer till hösten att lämnas till förvaltningens ledningsgrupp för beslut om åtgärdsplan. Utredningen påvisar utmaningarna som finns då ansvaret för att få åtkomst till system och få behörigheter blivit utspridd och är komplext med många intressenter, en mängd rutiner som behöver förtydligas, manuell hantering, långa ledtider samt viss otydlighet i behörigheter. Utredningen konstaterar även utmaningen i ett otydligt förvaltningsansvar. Utbildningsnämnden bedömer därför att behörighetshanteringen är ett område som har utrymme för förbättringar. Utredningen överensstämmer med de risker som identifierats och de riskminimerande åtgärder som är planerade (se svar under fråga 6).

Utredningen kom fram till ett antal styrande principer som borde fastställas för att säkerställa att utbildningsnämnden har korrekta, effektiva och säkra behörigheter. Dessa är bland annat att det ska finnas enhetliga och tydliga rutiner för hur behörigheter tilldelas, ändras och avslutas, att identiteter och åtkomst ska styras utifrån användarens uppdrag, att identiteter och åtkomst ska enkelt kunna kontrolleras och granskas för att se vem/vilka som har behörighet till vilket/vilka system och att hantering av identiteter och åtkomst ska löpande planeras och kontrolleras av utbildningsnämnden.

23. Har ni lämnat information till de registrerade om incidenterna? Om inte, ange orsaken till att ni inte informerat de registrerade. Ange även vilken bestämmelse i dataskyddsförordningen (GDPR) ni har tillämpat.

Nej, då utbildningsnämnden inte bedömer att personuppgiftsincidenten sannolikt lett till en hög risk för fysiska personers rättigheter och friheter. Utbildningsnämnden har i enlighet med artikel 34 i dataskyddsförordningen genomfört tekniska skyddsåtgärder som leder till att obehörig åtkomst inte kan ske i modulerna. Utbildningsnämnden har vidtagit ytterligare åtgärder, en utredning om behörighetsstyrning är gjord och arbete med riskminimerande handlingsplan pågår.