Datum
2023-04-03

Diarienummer
20221107:074

Utbildningsnämnden, genom
bildningsförvaltningen

Kompletterande frågor gällande granskning av plattformar i utbildningsverksamheten

Ärendet och nulägesanalys

I anslutning till att en incident inträffade i Vklass har jag initierat en granskning av plattformar liknande Vklass i utbildningsverksamheten i november 2022. Jag har fått en lista med olika system som användas i utbildningsverksamheten och verksamhetsutvecklaren har vid flera möten muntligen redogjort för varje system. Jag har därutöver tagit stickprover från registrerade behandlingar och kikat närmare på vissa systemleverantörer.

Senare praxis poängterar att varje dataflöde ska identifieras och t.ex. ska en personuppgiftsansvarig utses för varje flöde (t.ex. Datatilsynets beslut för Google workspace). Jag kan konstatera att utbildningsnämnden har en komplex uppsättning av system, vilka också är integrerade i varandra och skickar uppgifter mellan varandra. Det har varit svårt i granskningen att kunna få en tydlig överblick över systemen och hur de interagerar med varandra (vilka personuppgifter som skickas och hanteras var). GDPR i sin grund bygger på ordning och reda, struktur, att känna till vilka personuppgifter man behandlar och varför, att registrera behandlingarna, att informera de registrerade om behandlingarna, ha en rättslig grund, följa principerna, beakta rättigheterna etc.

De digitala systemen inom utbildning innehåller *extra skyddsvärda personuppgifter* (personuppgifter om barn, omdömen, betyg), som inte sällan kan tangera uppgifter om hälsa (dyslexi, diagnoser, extra insatser etc) och etnicitet (modersmål) vilka är *känsliga personuppgifter*. Det påkallar ytterligare en varsam och GDPR-förenlig hantering.

Det finns även pågående ärenden hos tillsynsmyndigheter i både Sverige, Danmark och andra länder gällande till exempel molntjänster i skolan, varför frågan om GDPR-förenligheten inom utbildningsverksamheten är ytterst angelägen. Utbildningsnämnden måste vara beredd på att snabbt kunna ställa om, om så krävs.

Postadress
Danderyds kommun
Dataskyddsombud
Box 66
182 05 DJURSHOLM

Besöksadress

Växel
08-588 910 00

Direkt
xx-xxxxx

E-post

Webb
www.danderyd.se

I anledning av allt detta vill jag få svar på några kompletterande frågor.

1. Finns dokumenterat vilka uppgifter som byts mellan det ena systemet till det andra och vice versa? Finns dokumenterade konkreta dataflöden (alltså vilka typer av personuppgifter som flödar), som inte är på generell nivå? (art 6 dataskyddsförordningen)

2. Är behandlingarna av personuppgifter inom de digitala systemen registrerade? Är registreringarna som finns korrekta och uppdaterade (till exempel att det verkligen finns ett personuppgiftsbiträdesavtal i fall där det registrerats att personuppgiftsbiträdesavtal ska finnas eller att systemet verkligen inte innebär en tredjelandsöverföring i fall där det registrerats att tredjelandsöverföring inte finns)? (art 6)

3. Hur säkerställs att gallring sker i varje system? Är dokumenthanteringsplanen knuten till gallringen i system? Om systemen inte gallras med visst intervall, varför? Avser verksamheten att ändra detta i så fall? (art 5)

4. Ange för varje system som används om utbildningsnämnden identifierat en hög risk för personers fri- och rättigheter identifieras eller inte (till exempel genom tredjelandsöverföring, eller personuppgifternas karaktär)?

5. För de system som innebär en hög risk, har konsekvensbedömning gjorts? Har DSO fått granska konsekvensbedömningen? Om inte, när kommer konsekvensbedömning för respektive system med identifierad hög risk göras? (art 35)

6. Hur följs gjorda konsekvensbedömningar upp och med vilket intervall? Vem har ansvaret för att implementera och vidareutveckla riskminimerande åtgärder? (art 35)

7. Finns personuppgiftsbiträdesavtal med samtliga systemleverantörer? Följs dessa upp? Vem påtalar brister eller för dialog med leverantören? (art 28, det är nämnden som ska ge biträdet instruktioner för personuppgiftsbehandlingen)

8. Hur säkerställs korrekt hantering av uppgifter modersmål och funktionsnedsättning (hälsa) i Edlevo/Indra? Hur följs hanteringen upp? (art 9)

9. I de system där skolarna kan göra individuella avsteg, hur säkerställer kommunen att avsteg inte görs som innebär risker för

personuppgifter eller strider mot GDPR? Finns systemrutiner eller förhållnings- och användarregler för de system med identifierad hög risk, samt för alla andra system?

10. Finns rutin för behörighetstilldelning i systemen på generell nivå och för varje system? Hur görs bedömningen för behörighetstilldelning i varje system?

11. Finns rutin för känsliga personuppgifter (hälsa, etnicitet etc) och extra skyddsvärda personuppgifter (barn, omdömen, hälsa) ska hanteras på generell nivå och för varje system? Hur följs den upp?

12. Finns rutin för hantering av sekretessbelagda uppgifter för varje systemen på generell nivå och för varje system? Hur följs den upp?

13. Finns rutin för fritextfält i varje system, där utrymme för fritext finns? Hur följs den upp?

14. Mot bakgrund av Integritetsskyddsmyndighetens pågående granskning av Google workspace, vad har utbildningsnämnden för kontinuitetsplanering eller plan gällande Google worspace/classroom? Hur resoneras gällande pseudonymerisering och andra alternativ?

15. Vem ansvarar för infrastrukturen i den digitala miljön? Får ledningsgruppen rapportering om implementering och uppföljning vad gäller den digitala miljön? Finns en ändamålsenlig plan framåt? Finns en vision för den digitala miljön – hur vill utbildningsnämnden att den ska se ut?

Ta hjälp av huvudkontaktombudet och kontaktombud vid behov. Svara senast **den 30 juni 2023**. Vid behov går det att begära att få längre tid. Det går också bra att ställa frågor till undertecknad. Granskningen är inte avslutad, utan detta är endast ett delmoment i den pågående granskningen.

Med vänlig hälsning Anne Hännestrand, dataskyddsombud