Datum
2023-10-17

Diarienummer
20221107:74

Utbildningsnämnden

Dataskyddsombudets granskning och rekommendationer för grundskolans system i utbildningsverksamheten (er ref UN 2023/0804)

Inledning

Dataskyddsombudet (jag) har i november 2022 inlett granskning av grundskolans plattformar i utbildningsverksamheten. Utbildningsnämnden är personuppgiftsansvarig för behandlingarna. I och med skolplikten är utbildningsnämndens ansvar stort eftersom elever inte har annat till val än att arbeta i utbildningsverksamhetens system och dessutom ska kunna lita på att utbildningsnämnden hanterar deras personuppgifter korrekt. Jag har inte granskat hanteringen i förskola, gymnasium eller kultur och fritid.

Granskningen har gått till så att jag initialt fått en muntlig föredragning och redogörelse för systemen av verksamheten, med möjlighet att ställa frågor. Därefter har jag skriftligen ställt verksamheten femton (15) frågor. Bildningsförvaltningen har avgränsat sig till att besvara frågorna för de största systemen för grundskola och bilagt ca 20 dokument. Jag har gått igenom det mottagna materialet på generell nivå, med avsikt att inte gå in på varje detalj, utan att fokusera på de stora dragen. Jag har vidare hållit mig till de frågor jag ställt och de handlingar jag fått in, varför min översyn är begränsad till detta och alltså inte uttömmande. Det kan finnas andra fokusområden inom dataskydd i utbildningsverksamheten, som jag inte berör här.

Jag kommer härmed att avsluta granskningen. Mina rekommendationer har flätats in löpande i texten. Påtalade frågeställningar i denna skrivelse behöver alltså inte besvaras till mig, men verksamheten rekommenderas att arbeta vidare med frågeställningarna. Eventuellt kommer granskningen följas upp i ett senare skede. Verksamheten bör se över om det finns ett behov att vidta liknande genomlysning och kvalitetssäkring vad gäller förskola, gymnasium samt kultur och fritid.

Postadress
Danderyds kommun
Dataskyddsombud
Box 66
182 05 DJURSHOLM

Besöksadress

Växel
08-588 910 00

Direkt

E-post
dataskydd@danderyd.se

Webb
www.danderyd.se

Sammanfattning

Dataskyddsombudet (jag) har granskat grundskolans plattformar i utbildningsverksamheten i Danderyds kommun. Utbildningsnämnden är personuppgiftsansvarig för behandlingarna och i och med skolplikten är utbildningsnämndens ansvar stort. Systemen i utbildningsverksamheten behandlar extra ömtåliga personuppgifter som till exempel uppgifter om barn, personnummer och integritetsnära information (*extra skyddsvärda personuppgifter)*, uppgifter om hälsa (*känsliga personuppgifter* och *sekretessbelagda uppgifter)* samt uppgifter om etnisk bakgrund (modersmål) och religion (kost) (*känsliga personuppgifter)*.

Granskningen har visat flera positiva inslag. Vissa dokument finns på plats och flera förslag på styrdokument har tagits fram. Begränsning av nedladdning av appar har sen tidigare skett. Verksamheten har själva identifierat flera utvecklingsområden. Granskningen har också motiverat till gränsöverskridande samarbete med ömsesidigt kunskapsutbyte mellan olika professioner och verksamheter, som jag gärna ser fortsätter. Generellt bedöms kunskapsnivån om dataskydd ha höjts i verksamheten.

Granskningen har identifierat att de största systemen i grundskolan – som verksamheten har avgränsat granskningen till – har brister och utvecklingsområden i huvudsak enligt följande.

- Avsaknad av styrdokument på flera områden.
- Risker för röjande av *känsliga* och *extra skyddsvärda personuppgifter* i Google Workspace samt bristande gallring och avsaknad av reservplan.
- Brister vad gäller vissa pågående personuppgiftsbehandlingar.
- Bristande gallring av personuppgifter i samtliga system.
- Behandlingsregistret behöver uppdateras.
- Det saknas konsekvensbedömningar[1].
- Vissa brister i andra system samt uppkomna risker genom skolors möjlighet till individuella avsnitt och behörighetstilldelning.

Bristerna är bekymmersamma. Utbildningsnämnden rekommenderas att prioritera och stärka upp personuppgiftshanteringen på dessa områden genom att besluta och vidta *tekniska* och *organisatoriska åtgärder*. Det är nämndens och ledningens ansvar, inte enskilda handläggares. Verksamheten har begränsat sitt svar till de största systemen i grundskolan, vilket kan indikera att motsvarande brister eller fler, finns i andra av grundskolans system och inom andra av nämndens och förvaltningens ansvarsområden.

[1] Jfr. art 35 dataskyddsförordningen (https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679).

Innehåll

Dataskyddsombudets granskning och rekommendation

Jag lämnar härmed följande synpunkter och rekommendationer.

Tack till verksamheten

1. Tack till verksamheten som inkommit med huvudsakligen bra underlag och svar som underlättat granskningen. Verksamheten har också under granskningens gång skrivit fram flera förslag på styrdokument och ansträngt sig för att dels svara på frågorna, dels få till en korrekt hantering.

Gällande rätt som utgångspunkt

2. *Varje upplysning* i skolarbeten och i system som *direkt* eller *indirekt* kan identifiera en person är **personuppgifter**.[2]

    - För att exemplifiera. Låt säga att en elev skriver en skolpromemoria om sin familj, sina kompisar, familjens högtidstraditioner, sitt modersmål eller ursprungsland, sina allergier, sin dyslexi, diabetes eller knäskada, politiska reflektioner eller om vad som gör eleven glad eller ledsen.

    - Utgör skolarbetet en personuppgiftsbehandling? Ja. Dels utgör promemorian en behandling av upplysningar som kan knytas direkt eller indirekt till en specifik elev, dels innehåller promemorian behandling av *extra skyddsvärda* (uppgifter om barn, integritetsnära information) och *känsliga personuppgifter* (hälsa, politisk åskådning, etnisk bakgrund, religion) och *sekretessbelagda personuppgifter* (hälsa).

    Även tatueringar, foton på eleven, elevens målningar och porträtt utgör personuppgifter om eleven direkt eller indirekt kan identifieras.

3. För all typ av personuppgiftsbehandling krävs en **rättslig grund**. De rättsliga grunder som kommunen huvudsakligen kan stödja sig på är *nödvändigt* för

    a. *avtal*,
    b. *rättslig förpliktelse* och
    c. *allmänt intresse/myndighetsutövning*.[3]

[2] Art 4.1 dataskyddsförordningen (https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679).
[3] Art 6 dataskyddsförordningen (https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679).

Den rättsliga grunden samtycke kan inte användas eftersom elever och skolan inte är jämställda, och samtycket därmed inte frivilligt, vilket är ett krav. Vanligast inom utbildningsverksamheten är *nödvändigt* för *allmänt intresse*.

4. Därutöver måste **principerna** i dataskyddsförordningen följas och beaktas vid all personuppgiftsbehandling.[4]

   Personuppgifterna ska

   a. behandlas lagligt, korrekt och öppet/transparent,

   b. endast samlas in för ett bestämt ändamål (*ändamålsbegränsning*),

   c. inte vara mer omfattande än vad som krävs (*uppgiftsminimering*),

   d. i sig vara korrekta,

   e. inte sparas längre än vad som är nödvändigt för det bestämda ändamålet (*lagringsminimering*),

   f. behandlas på ett sätt som säkerställer lämplig säkerhet (*integritet och konfidentialitet*) och

   g. den personuppgiftsansvarige ska ansvara för och kunna visa att ovan punkter efterlevs (*nämndens ansvarsskyldighet*).

5. Personuppgifter om barn, personnummer och annan integritetskänslig eller ”pinsam” information utgör ***extra skyddsvärda personuppgifter*** och ska behandlas skyddsvärt.

6. Behandling av ***känsliga personuppgifter*** som etniskt ursprung (modersmål), politiska åskådning, religion (kost), fackförening, genetiska och biometriska uppgifter, hälsa (dyslexi, diagnos, särskilt stöd eller anpassning, sjukfrånvaro) eller sexualliv/sexuell läggning är som utgångspunkt *förbjuden*.[5] Även om utbildningsnämnden har stöd i undantagen för viss behandling av sådana personuppgifter, ska behandlingen stå i *proportion* till *syftet* med behandlingen. Detta betyder att behandlingar av *känsliga personuppgifter* ska vara återhållsamma.

7. Registrerade (elever, lärare, administratörer) har även en rad **allmänna rättigheter,** vilka alltid måste beaktas vid all personuppgiftsbehandling, enligt följande.

[4] Art 5 dataskyddsförordningen (https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679).
[5] Art 9 dataskyddsförordningen.

- Respekt för privat- och familjeliv (kommunikation) [6]
- Skydd av personuppgifter[7]
- Rätt till effektivt rättsmedel[8]
- Rätt till privatliv[9]
- Rätt till rättvis rättegång[10]
- Enskild har skydd mot betydande intrång i den personliga integriteten av det allmänna[11]

Därutöver tillerkänns den registrerade även en rad **rättigheter i dataskyddsförordningen**, som rätt till information och transparens, rätt att få ut ett behandlingsregister på individuell nivå, rätt till rättelse, radering, invändning, dataportabilitet och begränsning.[12]

8. **Barn** har generellt svårare att förstå konsekvenserna av bristande hantering av personuppgifter samt att känna till och tillvarata sina rättigheter. Det finns därför alltid en presumtion för försiktighet vad gäller all behandling av barns personuppgifter.

9. Hur ska då punkterna 2-8 kunna beaktas och implementeras av utbildningsnämnden? För att säkerställa och kunna visa att behandlingar utförs i enlighet med dataskyddsförordningen ska utbildningsnämnden besluta om och vidta tekniska och organisatoriska åtgärder.[13]

    - **Tekniska åtgärder** innebär till exempel reglerad behörighetstilldelning, systembegränsningar, upprätthålla tillräcklig stark säkerhet i förhållande till personuppgifternas natur, ”*lätt att göra rätt och svårt att göra fel*”, ”*privacy by design*”, hjälptext i fritextfält, automatisk systemgallring och så vidare.

    - **Organisatoriska åtgärder** innebär till exempel att ha relevanta styrdokument på plats, att GDPR ska vara prioriterat av

[6] Art 7, 8 och 47 Europeiska unionens stadga om de grundläggande rättigheterna (https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:12012P/TXT).
[7] Art 7, 8 och 47 Europeiska unionens stadga om de grundläggande rättigheterna (https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:12012P/TXT).
[8] Art 7, 8 och 47 Europeiska unionens stadga om de grundläggande rättigheterna (https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:12012P/TXT).
[9] Art 6, 8 och 12 (lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna).
[10] Art 6, 8 och 12 (lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna).
[11] 2 kap. 6 § regeringsformen.
[12] Kapitel 3 dataskyddsförordningen (https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679).
[13] Art. 24 dataskyddsförordningen (https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679).

ledningen, tillräcklig resursfördelning, minska sårbarheten genom att flera personer har tillräcklig kunskap om systemen och GDPR, och att handläggare ska ha tillräckligt med tid för att kontrollera att det blev rätt samt kunna utföra manuell gallring och så vidare.

10. Ju mer sköra personuppgifter som behandlas, desto större krav ställs på utbildningsnämndens tekniska och organisatoriska åtgärder. Beaktande av gällande rätt (punkterna 2-9) måste vara en given utgångspunkt för all hantering av personuppgifter i utbildningsverksamheten.

Varför granskas utbildningsverksamhetens system?

11. Med grund i gällande rätt (punkterna 2-9) bedöms utbildningsverksamheten ha en särställning i jämförelse med personuppgiftsbehandlingar i andra nämnder. Behandlingen av personuppgifter rör mer prekära uppgifter som *känsliga, extra skyddsvärda personuppgifte*r och *sekretessbelagda uppgifter*. Utifrån personuppgifternas sköra natur finns en i grunden identifierad hög risk.

12. En problematik som finns i utbildningsverksamheten är användningen av amerikanska molntjänster som Google Workspace.

    Även om ett adekvansbeslut mellan EU och USA (fortsättningsvis kallat *Ramverket*) nu har tagits som möjliggör användningen av amerikanska molntjänster under vissa förutsättningar, kvarstår många av de risker som finns med amerikanska molntjänster. Till exempel fortgår amerikansk underrättelseinhämtningen på ”*bulk*”, vilket utgör en risk för röjande av utbildningsnämndens personuppgifter. Min utredning om *Ramverket* bifogas i bilaga 2.

13. Vidare har utbildningsverksamheten en uppsjö av system (vilka är mer eller mindre integrerade i varandra) och obefintlig gallring. Det finns möjlighet för skolorna att göra individuella avsteg från kommunens regler, utan att skolorna informerats i tillräcklig utsträckning om riskerna avstegen innebär.

14. Därtill har tillsynsmyndigheter, både i Sverige och i andra länder, pågående tillsynsärenden vad gäller Google Workspace. Verksamheten måste dels stå beredd, dels ha tillräcklig kunskap om sina dataflöden för att snabbt kunna ställa om, efter att besluten meddelas i dessa tillsynsärenden.

Generell information och medskick

Flera positiva inslag

15. Flera positiva inslag har framkommit under granskningen. Viss kartläggning, dokumentation och konsekvensbedömning av Google Workspace finns på plats. Flera förslag på styrdokument har tagits fram under granskningens gång, se punkten 27. Verksamheten har sedan tidigare begränsat skolornas användning av appar, vilket är positivt eftersom apparna ofta innebär dataskyddsrisker. Verksamheten har själva identifierat flera utvecklingsområden, vilket tyder på en kunskap och insikt i frågorna. Det har funnits ett engagemang i verksamheten att svara på granskningen.

16. Granskningen har också motiverat till gränsöverskridande samarbete med ömsesidigt kunskapsutbyte mellan olika professioner och verksamheter, som jag gärna ser fortsätter. Generellt bedöms kunskapsnivån om dataskydd ha höjts i verksamheten.

Omdefiniera sin tolkning av begreppet personuppgifter

17. I verksamhetens handlingar ges uttryck för att det bara är elevers, lärares och administratörers *namn* som behandlas i systemen – det är en för snäv och felaktig uppfattning om vad personuppgifter är.

18. Se punkten 2. Verksamheten rekommenderas att utvidga sin syn på vad som utgör personuppgifter och höja kunskapen. En positiv följd av detta kommer att bli att dataskyddsförordningen naturligt implementeras i större utsträckning i det löpande arbetet.

Utbildningsnämnden är personuppgiftsansvarig

19. Det är utbildningsnämnden som är personuppgiftsansvarig för all behandling av personuppgifter inom nämndens verksamhet. Det är nämnden som ska bestämma ändamål och medel med behandlingarna.[14] Det är nämndens och ledningens ansvar, inte enskilda handläggares. Vissa löpande systemfrågor kan givetvis skötas inom den löpande verkställigheten, men förbise inte att nämnden har det yttersta ansvaret och att nämnden ska ta besluten, eller att delegation finnas, i det fall *överväganden* och *bedömningar* krävs.

20. Det innebär också att nämnden i lämpligt format måste informeras om risker/brister med aktuell eller tilltänkt personuppgiftshantering och vilka alternativ som finns. För att nämnden ska kunna informeras om detta måste ledningen givetvis också vara involverad.

[14] Art 4.7 dataskyddsförordningen (https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679).

21. Verksamhetens processer för beslut om och vidtagande av *tekniska* och *organisatoriska åtgärder* bör ses över. Mot bakgrund av förvaltningens storlek skulle kontaktombuden, som arbetar med det operativa dataskyddsarbetet, behöva vara flera.
22. Mot bakgrund av vad som angetts under punkterna 10-13 bör bildningsförvaltningen vara särskilt noga med att informera utbildningsnämnden, i jämförelse med andra förvaltningar och nämnder.

Upphandling och omförhandling

23. Flera av utbildningsnämndens avtal löper ut inom den närmsta tiden. Se till att utreda och definiera en säker personuppgiftshantering innan nya system upphandlas eller omförhandlas. Ta stöd av dataskyddssamordnare och förvaltningens kontaktombud.
24. Kommunen, liksom utbildningsnämnden, bör tydliggöra personuppgiftshanteringen i samband med upphandlingen så att leverantören redan vid anbud är insatt i vilka krav kommunen ställer. Det kommer underlätta tecknandet av personuppgiftsbiträdesavtal och minska risken för att leverantörer upphandlas som inte kan säkerställa ett fullgott skydd.
25. Trots att *Ramverket*, adekvansbeslutet mellan EU och USA, nu finns rekommenderas en fortsatt vaksamhet med amerikanska molntjänster. Se bilaga 2 s. 6 för mina rekommendationer i denna del.

Ha koll på flödet av personuppgifter

26. Olika scheman[15] visar på att utbildningsverksamheten har en komplex IT-struktur med flera system som skickar personuppgifter mellan varandra. Verksamheten måste ha det ordnat med vilka personuppgifter som skickas och hämtas var. En korrekt hantering utifrån gällande rätt (punkterna 2-9) måste tillgodoses för samtliga behandlingar. Se punkten 27, eftersom dokumenten inte är antagna och beslutade är området än så länge oreglerat.

Styrdokument och register

Föreslagna dokument

27. Verksamheten har bifogat flera *förslag* till styrdokument som inte följer kommunens grafiska profil och styrdokumentsmall. Dokumenten är inte beslutade. Verksamheten måste, gärna

[15] Dokumenten *Integrationskarta personkonton skola, Integrationskarta skola* och *Flödesschema attribut skola.*

omgående, se över om dokumenten kan beslutas, gärna med beaktande av mina rekommendationer. I och med att dokumenten inte är antagna eller beslutade är många områden fortfarande oreglerade.

Brister i behandlingsregistret

28. Utbildningsförvaltningen har uppgett att samtliga behandlingar av personuppgifter inte är registrerade, utan att workshop ska hållas med dataskyddssamordnare hösten 2023. Workshopen har hållits.

29. Eftersom behandlingsregistret fastställer grunden för kommunens behandlingar och dess laglighet, kan bristande behandlingsregister innebära en risk för att registrerade får sämre möjligheter att tillvarata sin rätt. Mot bakgrund av att utbildningsnämndens prekära personuppgiftsbehandlingar bör detta arbete prioriteras upp.

Avsaknad av styrdokument för sekretessbelagda uppgifter

30. På fråga om förvaltningen har styrdokument för sekretessbelagda uppgifter redogör förvaltningen för det styrdokument som håller på att tas fram av kommunledningskontoret för hanteringen av ärenden som rör personer med sekretessmarkering.

31. Den ställda frågan avsåg alla typer av sekretessbelagda uppgifter som hanteras av verksamheten, och inte bara gällande personer med sekretessmarkering. Verksamheten rekommenderas att se över huruvida det behövs ett styrdokument för hanteringen av sekretessbelagda uppgifter. Vidare bör det definieras hur de sekretessbelagda uppgifterna ska hanteras, att samtliga slagningar måste vara arbetsrelaterade, att ge personal information om att loggning sker, att påminna om att tystnadsplikten gäller och så vidare.

Styrdokument för fritextfält

32. Jag tycker den framtagna ej beslutade rutinen för fritextfält ger ett bra stöd till verksamheten. Se punkt 27, eftersom dokumentet inte är antaget och beslutat är området än så länge oreglerat.

Rutin och handlingsplan

33. Verksamheten har inkommit med förslag på *Generell rutin*. Jag bedömer att innehållet är huvudsakligen bra. Se punkt 27, eftersom dokumentet inte är antaget och beslutat är området än så länge oreglerat. Även samtliga rättigheter i punkten 7 behöver beaktas.

34. Vad gäller delningen av personuppgifter, se över om delningen ryms inom personuppgiftsbehandlingens ändamål. Blanda inte ihop samtycke för att vaccinera sig med den rättsliga grunden samtycke

inom dataskyddsförordningen. Notera att en ”DPIA” heter *konsekvensbedömning*.

Google Workspace

35. Google Workspace är en amerikansk molntjänst med säte i USA. Varje elev har en egen profil och tillhör ett eller flera *classroom.* I Google Workspace hanteras foton, läxinlämning och allt skolarbete.

Redan identifierade brister kvarstår

36. I konsekvensbedömningen för Google Workspace har före detta dataskyddsombud i juni 2021 lämnat flera anmärkningar, som bristande gallring, bristande hantering *av extra skyddsvärda personuppgifter*[16], möjligheten *för elever eller skolor*[17] att lägga till eget material och molntjänstproblematiken *innefattande risken för röjande av personuppgifter samt bristande efterlevnad av rättigheter*[18].

37. Samtliga brister kvarstår idag, mer än två år senare, vilket verksamheten rekommenderas att analysera. Även om *Ramverket* nu är framtaget förändrar det egentligen inte denna bedömning eftersom underrättelseinhämtning och risken för röjande av personuppgifterna fortfarande finns där.

38. Vissa av dessa identifierade brister som att implementera gallring/radering och begränsa/reglera möjligheter för skolors individuella avsteg torde varken vara tidskrävande eller kostnadsdrivande, varför det är obegripligt att bristerna inte har rättats till.

Känsliga och extra skyddsvärda personuppgifter

39. I ett av verksamhetens föreslagna dokument[19] står att *känsliga personuppgifter*[20] och *extra skyddsvärda personuppgifter*[21] inte får hanteras i Google Workspace.

40. Jag ser positivt på bestämmelsen, men bedömer att den inte är möjlig att efterleva, se punkten 2. Den bör därför i stället formuleras som en målsättning i kombination med insatta riskminimerande åtgärder som kontinuerlig gallring, framtagna styrdokument med förhållningsregler, instruktioner i Google Workspace för att minska riskerna och begränsning/reglering av skolornas individuella avsteg

[16] Definierade i punkten 5.
[17] Egen anmärkning i kursivt.
[18] Egen anmärkning i kursivt.
[19] Dokument *Varför och hur Google Workspace.*
[20] Definierade i punkt 6.
[21] Definierade i punkt 5.

och så vidare. Se punkten 27, eftersom dokumentet inte är antaget och beslutat är området än så länge oreglerat.

Bristande gallring

41. Verksamhetens aktuella hantering i Google Workspace innebär att foton, läxor och allt annat skolarbete sparas från förskoleklass till åk 9. När eleven går ut åk 9 sätts kontot i karantän i 90 dagar. Om eleven påbörjar gymnasiestudier återöppnas elevens konto med skolmaterial från förskoleklass till gymnasieexamen. Början av gallring för allt material från förskoleklass till gymnasieexamen, sker då tidigast 90 dagar efter avslutade gymnasiestudier. Utbildningsnämnden är ansvarig för alla denna mängd personuppgifter, till synes helt i onödan.

42. Verksamheten bör se över hanteringen utifrån gällande rätt (punkterna 2-9) och bestämma när gallring kan ske (exempelvis efter 6 månader, ett år eller efter kursens avslut och tid för överklagande löpt ut)? Viss möjlighet för undantag kan ske för vissa elevers särskilda behov, utifrån barnkonventionens krav om *barnets bästa*.

43. I en kammarrättsdom har en elevs *framtidsbrev* som en ung elev skrivit till sig själv bedömts utgöra allmän handling[22] och behövde lämnas ut till allmänheten, såvida den inte uppfyllde någon sekretessgrund.

Finns ett alternativ?

44. Verksamheten har uppgett att det enda primära alternativet till den amerikanska molntjänstens Google Workspace, är papper och penna. Jag vill understryka att kostnaden inte är en giltig grund att frånträda sitt ansvar enligt dataskyddsförordningen och att absolut miniminivå är att säkra upp med riskminimerande åtgärder.

Registrerade har förlorat möjlighet till information

45. Efter att före detta dataskyddsombud anmärkt på konsekvensbedömningen om Google Workspace i juni 2021, har även jag granskat den, den 24 oktober 2022. Detta skedde efter att jag uppmärksammat att konsekvensbedömningen uppdaterats utan att jag fått yttra mig. Jag noterar att mitt yttrande den 24 oktober 2022 inte bilagts konsekvensbedömningen.

46. Ett av mina främsta uppdrag som dataskyddsombud är att bevaka registrerades rätt och en av dataskyddsförordningens främst grunder är att säkerställa registrerades rätt till information och transparens. Detta urholkas om dataskyddsombudets bedömning inte bifogas till

[22] Kammarrätten i Stockholms dom mål nr 5854-22, meddelad den 6 december 2022.

konsekvensbedömningen. Hanteringen visar också på en bristande förståelse för registrerades rätt till information och kommuns ansvar för sina personuppgiftsbehandlingar. Verksamheten bör se över hanteringen.

Övriga personuppgiftsbehandlingar i utbildningsverksamheten

47. Det av verksamheten bifogade dokumentet *Övergripande beskrivning hantering av personuppgifter 2020* utgör en sammanställning över personuppgiftsbehandlingar som sker i utbildningsverksamheten. Jag instämmer i att dokumentet måste revideras, även om dokumentet utgör en god grund att revidera ifrån.

48. Verksamheten måste se över hur dokument förhåller sig till verksamhetens registrerade behandlingar i *Draftit*. Givetvis måste en koppling och enhetlighet finnas häremellan.

49. Dokumentet[23] tar inte tillräcklig höjd, jfr. punkterna 2-9. Identifierat ändamål och aktuella gallringsbestämmelser saknas. Detta kan innebära att registrerade fråntas sina rättigheter, vilket verksamheten bör se över.

Kommunikation med vårdnadshavare

50. En av verksamhetens behandlingar[24] rör kommunikation mellan skola och vårdnadshavare via ej krypterad e-post. Min rekommendation är att skolan bör kommunicera med vårdnadshavare på ett säkrare sätt. Detta gäller särskilt om det rör sig om *extra skyddsvärda* eller *känsliga personuppgifter*, eller *sekretessbelagda uppgifter*. Det har det senaste halvåret också noterats flera personuppgiftsincidenter som rört e-posthantering. En bättre metod vore om kommunikation kunde ske genom säkra kanaler med bank id/logg in (utan tredjelandsöverföring), vilket verksamheten bör se över.

Foto och film för elevarbeten

51. En av verksamhetens behandlingar[25] rör foto och film för elevarbeten. Verksamheten bör se till att identifiera rättslig grund samt vidta riskminimerande åtgärder utifrån principerna om uppgiftsminimering, integritet, säkerhet och konfidentialitet, samt ha regler för filmning och förvaring, samt kontinuerliga gallringsrutiner vid inaktualitet.

---

[23] Verksamhetens dokument *Övergripande beskrivning hantering av personuppgifter 2020*.
[24] Verksamhetens dokument *Övergripande beskrivning hantering av personuppgifter 2020*.
[25] Verksamhetens dokument *Övergripande beskrivning hantering av personuppgifter 2020*.

Uppgift om lagföring av elever

52. En av verksamhetens behandlingar[26] rör uppgifter om elevers lagöverträdelser, till exempel narkotikabrott, i samband med disciplinärenden. Verksamheten bör se över hanteringen enligt följande.

    a. All personuppgiftsbehandling i kommunens verksamhet kräver att behandlingen är *nödvändig*.[27] Är det *nödvändigt* för handläggningen i disciplinärendet att uppgift om lagföring inhämtas och på vilken rättslig grund? Det vanliga torde vara att eventuell avstängning/disciplinär åtgärd sker direkt efter en inträffad akut händelse och att eventuell dom gällande händelsen avkunnas långt senare. Vad gäller trygghet och studiero måste skolan ändå hantera dessa delar, även utan att uppgift om lagföring inhämtas eller antecknas.

       Om så ska ske krävs också att hanteringen är korrekt utifrån gällande rätt, se punkterna 2-9.

    b. Inhämtas domen, eller antecknas endast lagföringen? Kom ihåg principen om uppgiftsminimering.[28]

    c. Finns implementerade rutiner för när, var och hur uppgiften bör inhämtas och var den ska sparas? Kan uppgiften gallras vid inaktualitet?

    d. Uppgift om lagföringen bör ha en klar koppling till skolan, som till exempel lagföring för skadegörelse eller misshandel i skolans lokaler, och ha en koppling till disciplinärendet mot eleven. Säkerställ att personuppgiftsbehandlingen inte får andra syften och ändamål än det bestämda.

    e. Jag kan också se att en uppgift om utdömt skadestånd (till exempel att eleven ska ersätta skolan för skadegörelse eller stöld) skulle kunna behandlas inom ramen för fakturering, men denna behandling har inte tagits upp i verksamhetens dokument.

---

[26] Verksamhetens dokument *Övergripande beskrivning hantering av personuppgifter 2020*.
[27] Art. 6 dataskyddsförordningen (https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679).
[28] Art 5 dataskyddsförordningen (https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679).

Barn på sociala medier och hemsida

53. En av verksamhetens behandlingar[29] rör personuppgiftsbehandling av foto och film på elever och barn för publicering på hemsida eller i sociala medier. Jag avråder, och har gjort vid upprepade tillfällen, från sådan personuppgiftsbehandling.

    a. Personuppgiftsbehandlingen om barn rör *extra skyddsvärda personuppgifter*, vilka kommunen då delar med allmänheten i hela världen, sociala mediet/tredje part och tredjeland, vilket innebär att kommunen tappar kontrollen över personuppgiftshanteringen.

    b. Behandlingen är vidare inte *nödvändig* för *en rättslig grund* vilket är ett lagkrav. Se punkten 3.

    c. Personuppgifterna (till exempel fotot på barnet) går inte att full ut rätta eller radera om barnet ångrar sig eller om publiceringen har inkräktat på rätten till privatliv. Se punkten 7.

    d. Det nyligen ingångna *Ramverket* förändrar inte min bedömning. I det fall verksamheten ska ha kvar en sådan behandling rekommenderas att verksamheten gör en konsekvensbedömning inbegripet riskminimerande åtgärder, som täta gallringsfrister på det sociala mediet och bildbanken med mera. En konsekvensbedömning kan dock inte läka bristande regelefterlevnad.

Generella gallringsbrister

54. Jag noterar obefintliga och bristande gallringsrutiner och rekommenderar att gallringsrutinerna på samtliga plan ses över omgående. Masshantering av personuppgifter medför att ett tungt ansvar vilar på utbildningsnämnden, vilket till synes sker i alldeles för stor omfattning och i fall där uppgifterna kan och bör gallras. Översyn bör ske vid samtliga omförhandlingar av avtal och personuppgiftsbiträdesavtal.

55. Avtala om gallring eller annan hantering av utbildningsnämndens personuppgifter, för det fall att avtal med leverantör sägs upp eller avslutas.

56. Jag ser positivt på att dokumenthanteringsplanen ska revideras av verksamheten och påminner om att regler för gallring måste dokumenteras i dokumenthanteringsplanen och behandlingsregistret.

---

[29] I verksamhetens dokument *Övergripande beskrivning hantering av personuppgifter 2020*.

Bristande gallring i Vklass

57. I systemet Vklass behandlas elevers personuppgifter om utvecklingssamtal, elevers kunskapsinhämtning, individuella elevplaner, elevomdömen och varningar om att eleven ej kommer uppnå fullgott betyg.

58. Vad gäller Vklass framstår det som att personuppgifterna aldrig gallras, utan endast läggs i olika behörighetslager. Verksamheten bör se över hur länge personuppgifterna behöver sparas och införa gallringsfrister. Inte att förglömma den större incidenten av obehörigt röjande som skett i Vklass, där elevers personuppgifter publicerades på nätet i utpressningssyfte.[30] Finns inte uppgifterna kvar, kan de inte röjas.

Brister vad gäller konsekvensbedömningar

59. Verksamheten behöver göra en konsekvensbedömning i samtliga behandlingar där det finns en hög risk för personers fri- och rättigheter.[31] Avsikten med konsekvensbedömningar är att ta höjd och sätta in riskminimerande åtgärder till den grad att risken för personuppgifterna är acceptabel/godtagbar, och om detta inte kan uppnås bör andra alternativ övervägas.

60. Verksamheten har endast totalt gjort en konsekvensbedömning och den gäller Google Workspace. I och med skolplikten är utbildningsnämndens ansvar stort. Jag ser dock positivt på att verksamheten nu överväger att se över riskerna för de olika systemen.

61. I dokumentet framgår att översyn bör göras årligen, vilket jag tycker är bra. Glöm inte att översyn även måste göras vid ändrade förhållanden, såsom vid inträffade incidenter, ändringar vad gäller *Ramverket* eller på *Ramverkets* deltagarlista, vilket bör läggas till.

62. Verksamheten har uppgett att uppföljning med riskminimerande åtgärder bevakas på systemförvaltarnivå. Glöm inte att bedömningarna måste dokumenteras för att kunna visa på GDPR-efterlevnad samt att den personuppgiftsansvariga nämnden måste informeras i lämpligt format om risker/brister för att de ska kunna ta, och kunna visa på att det tar, sitt personuppgiftsansvar.[32]

---

[30] Det är fortfarande inte helt klart om Danderyds kommuns elever berörts av röjandet, men sannolikt är det så.
[31] Art. 35 dataskyddsförordningen (https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679).
[32] Art. 5.2 dataskyddsförordningen (https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679).

Identifierade systemnära brister

System som hanterar uppgifter om modersmål, funktionsnedsättning med mera

63. På min fråga om hanteringen för uppgifter om modersmål, funktionsnedsättning med mera redogör verksamheten främst för behörighetstilldelningen, alltså vilken anställd som har behörighet till vilka personuppgifter. Detta är en viktig del. Vissa generella principer kan dock med fördel fastslås i styrdokumentsform för att säkra en korrekt hantering. Till exempel att slagningar i systemet ska ha arbetsanknytning, informera personal om att loggning sker, att minimera risker, införa hjälptext i fritextfält, påminna personal om tystnadsplikten för sekretessbelagda uppgifter och så vidare. Detta bör verksamheten se över.

Skolornas möjlighet att göra individuella avsteg och appar

64. Skolorna har viss möjlighet att göra individuella avsteg och tillval i system. På min fråga om hur verksamheten säkerställer att skolan inte gör avsteg som innebär risker för personuppgifterna, har verksamheten endast skickat in en generell beskrivning om vad systemen är avsedda för att hantera.

65. Avsaknad av tydligare regler blev också ett bekymmer i den större personuppgiftsincidenten i Vklass där elevers personuppgifter publicerats på en sida på nätet i utpressningssyfte.[33] Förvaltningen hade bestämt att foton på elever inte skulle hanteras i aktuellt system, men skolorna hade möjlighet till individuella avsteg och därför fanns det foton på elever i systemet, vilka dessutom hade godkänts av personal på skolorna. Hade foton inte funnits i systemet, hade röjande av foton på elever inte kunnat ske.[34]

66. Införandet av tekniska och organisatoriska åtgärder för begränsa skolornas möjligheter till individuella avsteg bör ses över. Av vad verksamheten i dialog har uppgett har användningen av appar i utbildningsverksamheten limiterats, vilket jag ser positivt på.

67. I de delar där verksamheten bedömer att skolor har möjlighet att göra individuella avsteg, utan någon större risk för personuppgifterna, bör skolorna få stöd i vad detta innebär. Ska behandlingen registreras? Beaktas principerna och rättigheterna? Behöver varje elev ingå eget avtal med leverantören (avråds) eller tar skolan ut en licens för samtliga elever (rekommenderas)? Innebär

[33] Det är fortfarande inte helt klart om Danderyds kommuns elever berörts av röjandet, men sannolikt är det så.
[34] Det är fortfarande inte helt klart om Danderyds kommuns elever berörts av röjandet, men sannolikt är det så.

tilltänkt avsteg en tredjelandsöverföring, och måste någon åtgärd vidtas på grund av det?

Behörighetstilldelning

68. Verksamhetens föreslagna dokument visar på en struktur om behörighetstilldelning, vilket är positivt. Se likväl punkt 27, eftersom dokumentet inte är antaget och beslutat är området än så länge oreglerat.

69. Olika system verkar ha olika stränga behörighetskrav.[35] Ibland kan detta vara givet utifrån de olika systemens natur, men till exempel verkar Edlevo ha en mjukare skrivning om behörighetstilldelningen än andra leverantörer, utan angivet skäl. Verksamheten bör göra en översyn av behörighetstilldelningen i styrdokumentsform samt i praktiken.

Slutsats

Dataskyddsombudet (jag) har granskat utbildningsverksamhetens plattformar i Danderyds kommun. Utbildningsnämnden är personuppgiftsansvarig för behandlingarna. I och med skolplikten är utbildningsnämndens ansvar stort eftersom elever inte har annat till val än att arbeta i utbildningsverksamhetens system och dessutom ska kunna lita på att utbildningsnämnden hanterar deras personuppgifter korrekt.

Systemen i utbildningsverksamheten är särskilt prekära utifrån att de behandlar extra ömtåliga personuppgifter som till exempel följande.

- Uppgifter om barn, personnummer och integritetsnära information vilket utgör *extra skyddsvärda personuppgifter*.
- Uppgifter om hälsa (dyslexi, diagnoser, särskilt stöd eller särskilda anpassningar för elever) som utgör både *känsliga personuppgifter* och *sekretessbelagda uppgifter*.
- Uppgifter om etnisk bakgrund (modersmål) och religion (kost) vilket utgör *känsliga personuppgifter*.

Granskningen har identifierat att de största systemen i grundskolan – som verksamheten har avgränsat granskningen till – har brister och utvecklingsområden som måste stärkas upp enligt följande.

- Avsaknad av styrdokument (förslag på styrdokument är framtagna inom ramen för granskningen, men har ej beslutats av verksamheten varför området än så länge är oreglerat).

[35] Verksamhetens dokument *Behörighetstilldelning*.

- Risker för röjande av *känsliga* och *extra skyddsvärda personuppgifter* i Google Workspace samt bristande gallring och avsaknad av reservplan.
- Brister vad gäller vissa personuppgiftsbehandlingar; kommunikation med vårdnadshavare, foto och film för elevarbeten, dokumentation om lagföring av elever samt elever på sociala medier och hemsida.
- Bristande gallring av personuppgifter i samtliga system.
- Behandlingsregistret där samtliga utbildningsverksamhetens behandlingar ska vara registrerade, behöver uppdateras.
- Det saknas konsekvensbedömningar för alla system utom Google Workspace.[36]
- Brister i andra system som behandlar *känsliga personuppgifter* samt uppkomna risker genom skolors möjlighet till individuella avsnitt och behörighetstilldelning.

Bristerna är bekymmersamma på flera plan. Verksamheten rekommenderas att prioritera och stärka upp personuppgiftshanteringen på dessa områden genom *tekniska* och *organisatoriska åtgärder*, med beaktande av dataskyddslagstiftningen och mina rekommendationer.

Verksamheten har begränsat sitt svar i granskningen till de största systemen i grundskolan, vilket kan indikera att motsvarande brister eller fler finns även i andra av verksamhetens system eller inom nämndens eller förvaltningens andra ansvarsområden.

Även flera positiva element har framkommit av granskningen. Viss kartläggning, dokumentation och konsekvensbedömning av Google Workspace finns på plats. Flera ej beslutade styrdokument har tagits fram. Begränsning av nedladdning appar har sen tidigare skett. Verksamheten har själva identifierat flera utvecklingsområden. Granskningen har också motiverat till gränsöverskridande samarbete med ömsesidigt kunskapsutbyte mellan olika professioner och verksamheter, som jag gärna ser fortsätter. Generellt bedöms kunskapsnivån inom dataskydds ha höjts i verksamheten.

Det kan inte nog understrykas hur viktigt det är att verksamheten får tid att arbeta och strukturera upp dataskyddsarbetet och beakta mina i denna granskning lämna rekommendationer. Detta är utbildningsnämndens och ledningens ansvar, och inte enskilda handläggares. En intensifierad kraftansamling av grovjobbet kan räcka ganska långt, även om arbetet sedan

[36] Art 35 dataskyddsförordningen (https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679).

måste hållas löpande. Även utbildningsnämnden nämnden bör lyfta och prioritera dataskyddsarbetet, utifrån sitt personuppgiftsansvar.

Utbildningsnämnden bör kontinuerligt informeras i lämpligt format, så att nämnden kan ta, och visa på att den tar, sitt personuppgiftsansvar för dessa prekära uppgifter.[37] Denna handling ska diarieföras i förvaltningens ärendehanteringssystem och ledning samt den personuppgiftsansvariga utbildningsnämnden ska delges informationen.

Anne Hännestrand
Dataskyddsombud

Bilaga:

1. Dataskyddsombudets granskning och rekommendationer för system i utbildningsverksamheten (denna)
2. Dataskyddsombudets PM med rekommendationer efter adekvansbeslutet *EU-US Data Privacy Framework*

[37] Art 5.2 dataskyddsförordningen (https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679).