Stockholms stad

GDPR Årsrapport

2023

Utbildningsnämnden

GDPR årsrapport
December 2023

Dnr:
Utgivningsdatum:
Kontaktperson: Hanna Virtanen

1 Bakgrund

Dataskyddsförordningen (GDPR) reglerar hur myndigheter, bolag och andra organisationer får hantera personuppgifter. Syftet är att skydda enskildas fri- och rättigheter, bland annat rätten till privatliv och skyddet för enskildas personuppgifter, och säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU. Som personuppgift räknas all typ av information som kan kopplas till en fysisk person. Utbildningsnämnden behandlar personuppgifter i stor omfattning, i många situationer av känslig karaktär och om personer i beroendeställning (elever och anställda).

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att utbildningsnämnden behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett Dataskyddsombud (DSO). DSO:n har till uppgift att övervaka verksamhetens dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för nämnden att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnden ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Innehåll

2 Sammanfattning

Inom ramen för dataskyddsombudets uppdrag lämnas följande årsrapport till utbildningsnämnden. Årsrapporten består av en rapportering av sex olika områden där nämndens efterlevnad enligt vissa kontrollpunkter redovisas. Därutöver sammanfattar dataskyddsombudet övriga observationer utifrån samtliga krav som åligger en personuppgiftsansvarig och där dataskyddsombudet bedömt att åtgärder krävs för att uppfylla kraven.

Inom utbildningsnämnden finns en god medvetenhet kring vikten av att skydda de personuppgifter som nämnden har blivit anförtrodd att hantera. I jämförelse med dataskyddsombudets årsrapport från 2022 har nämndens efterlevnad och skyddet för enskildas integritet förbättrats inom flera områden. Nämnden har idag (som personuppgiftsansvarig) en fullständig registerförteckning, en dokumenterad process för personuppgiftsincidenter och har även antagit andra styrdokument inom området. Inom områdena registerförteckning, styrdokument och personuppgiftsincidenter bedöms därmed inga brister längre finnas som är omfattande.

Även om nämndens dataskyddsarbete förbättrats under 2023 inom flera områden, krävs fortsatt åtgärder för att komma till en hög mognadsnivå i dataskyddsarbetet och ett läge där kraven i dataskyddsförordningen efterlevs i stort.

Områden som i dagsläget bedöms kräva åtgärder är konsekvensbedömningar och rätten till tillgång (registerutdrag). Även om konsekvensbedömningar gjorts för centrala verksamhetssystem tidigare, har nämnden inga upparbetade rutiner för att följa upp risker från dem eller rutiner som fångar upp nya personuppgiftsbehandlingar där konsekvensbedömningar krävs. Gällande rätten till tillgång (registerutdrag) har enbart en begäran om att utöva denna rättighet lämnats inom den lagstadgade tiden och dataskyddsombudet anser också att kopior på själva personuppgifterna ska lämnas ut i samband med en begäran. I dagsläget anger rutinen att inga kopior lämnas ut vid en begäran.

Dataskyddsombudet har även observerat avvikelser gentemot dataskyddskraven inom tre andra områden (utöver de obligatoriska rapporteringsområdena), rätten till information, uppföljning av personuppgiftsbiträden och gallring/arkivering. Dessa redovisas närmare i rapporten under rubriken ”Övrigt att rapportera”.

3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som personuppgiftsansvarig (”PUA”) som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som dataskyddsförordningen avser.

De obligatoriska rapporteringsområdena är registerförteckning, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter.

Nedan redogörs för nämndens status och Dataskyddsombudets (DSO:ns) slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	Det finns 229 införda registreringar i förteckningen.
Har nödvändiga uppdateringar gjorts?	Ja, hela registerförteckningen har uppdaterats under 2023.
Bedöms registerförteckningen vara fullständig?	Ja, registerförteckningen bedöms vara komplett i de delar som rör nämnden som personuppgiftsansvarig. I övrigt saknas en registerförteckning för nämnden som biträde.
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

För att något ska gå att skydda måste det först vara synligt för verksamheten. Det följer därför i klartext av dataskydds-förordningen (artikel 30) att nämnden måste inventera alla personuppgifter som behandlas i verksamheten, både i rollen som

personuppgiftsansvarig och personuppgiftsbiträde, och dokumentera dem i en så kallad registerförteckning.

En registerförteckning skapar intern synlighet och förståelse för vilka personuppgifter som behandlas samt hur de hanteras. Informationen i registerförteckningen är även ett hjälpmedel att uppfylla andra krav, exempelvis information till enskilda och vid utlämnande av personuppgifter i ett registerutdrag. Registerförteckningen är därför dataskyddsarbetets centrala utgångspunkt.

3.1.3 Resultat

Utbildningsförvaltningen har under 2023 haft ett pågående projekt vars syfte varit att skapa en komplett registerförteckning för utbildningsnämnden som personuppgiftsansvarig i enlighet med kraven i artikel 30 i dataskyddsförordningen. Registerförteckningen bedöms idag vara i stora delar komplett i de delar som rör nämnden som personuppgiftsansvarig.

Därutöver har utbildningsförvaltningen idag en roll kallad ”registeransvarig” vars uppdrag är att ha översikt att samtliga personuppgiftsbehandlingar dokumenteras i registerförteckningen och för att, tillsammans med andra funktioner, säkerställa att det finns rutiner för upprättande och hanteringen av registerförteckningen. Nämnden har därmed rutiner som säkerställer att förteckningen hålls uppdaterad.

Kravet på en registerförteckning gäller också nämnden som personuppgiftsbiträde och denna förteckning saknas för närvarande. Det är framför allt när nämnden förvaltar system för andra nämnder inom den pedagogiska verksamheten som nämnden agerar biträde.

3.1.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.1.5 DSO ger råd och rekommendationer till PUA

Utbildningsnämnden har en, i stort, komplett registerförteckning och rutiner för att säkerställa att den hålls uppdaterad övertid. Registerförteckningen för nämnden som biträde saknas dock fortfarande. Dataskyddsombudet rekommenderar att komplettera registerförteckningen med de personuppgiftsbehandlingar som rör nämnden som personuppgiftsbiträde.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Ja, styrande dokument finns på plats.
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Ja
Är dokumenten uppdaterade?	Ja
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Delvis

3.2.2 Syfte

Det aktuella området syftar till att den personuppgiftsansvarige genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar den personuppgiftsansvarige till medarbetare i verksamheten och registrerade om vad som gäller och vad som förväntas av medarbetarna, när de hanterar de registrerades personuppgifter. Att styrdokument finns nedtecknade, beslutade och kommunicerade medför att medarbetaren får dataskyddsinformation och kan behålla kunskapen över tid och tillämpa den på ett konsekvent sätt.

Bristande styrning på grund av att lämplig styrande dokumentation saknas kan leda till *bristande kvalitet* i hur verksamheten utför

aktiviteterna, men även till att verksamheten *använder värdefulla resurser* till fel saker.

3.2.3 Resultat

Under 2023 har utbildningsförvaltningen antagit ett antal nya styrdokument relaterat till dataskyddsområdet, bland annat lokal anvisning för informationssäkerhet, anvisning vid informationssäkerhetsincidenter och processbeskrivning för rätten till tillgång (registerutdrag). Även nya anvisningar vid kamerabevakning i skolan har antagits. De nyaste styrdokumenten har dock ännu inte kommunicerats ut till samtliga berörda medarbetare. Sedan tidigare har förvaltningen antagit anvisningar för hantering av personuppgifter i kommunikationsverktyg, digitala dokument och datafiler på utbildningsförvaltningen.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

3.2.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet bedömer att nödvändiga styrdokument finns på plats, men vissa av de nyligen antagna styrdokumenten har ännu inte kommunicerats ut till verksamheten. Dataskyddsombudet rekommenderar att styrdokumenten kommuniceras ut till berörda och att relevanta delar av övriga styrdokument tas upp regelbundet, exempelvis hur en medarbetare hanterar känsliga och extra skyddsvärda personuppgifter.

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

3.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	Förvaltningen har klassat informationen i respektive system i stället för själva behandlingarna. För system och tjänster som inte hanteras av central förvaltning, utan hanteras lokalt på enheter, är det dock osäkert vad som genomförts.
Är klassade personuppgiftsbehandlingar aktuella?	De personuppgiftsbehandlingar som finns i utbildningsnämndens IT-system är klassade och aktuella. När det gäller ostrukturerade personuppgifter är det i nuläget inte klarlagt.

3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd så ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Utan informationsklassningen har verksamheten inte förutsättningar att välja rätt åtgärder för att skydda sin information. Det är därför av stor betydelse för dataskyddsarbetet att den personuppgiftsansvarige har en uppdaterad bild av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar.

3.3.3 Resultat

De IT-system och tjänster som har hanterats av central förvaltning är informationsklassade. När det gäller system och tjänster som inte har hanterats av central förvaltning, utan hanteras lokalt på enheter är det oklart i vilken utsträckning de är klassade eftersom de inte sparas centralt, utan på respektive enhet.

Informationsklassning är dock endast första steget i att kunna genomföra tekniska och organisatoriska åtgärder. När

informationens skyddsvärda är känd, ska åtgärder vidtas för att skydda informationen.

3.3.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.3.5 DSO ger råd och rekommendationer till PUA

System är enbart bärare av information, men det är informationen som ska klassificeras oavsett i vilket IT-system eller tjänst den finns. Såsom framkom i årsrapporten 2022 gör dataskyddsombudet samma bedömning även för 2023. För att säkerställa att de IT-system och tjänster som utbildningsnämnden använder har samma klassificering när den använder samma typ av uppgifter, så bör nämnden fokusera på att klassificera sin information i stället för att klassificera informationen i respektive IT-system eller tjänst.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Nej. De behandlingar som har konsekvensbedömts är kopplade till utbildningsnämndens centrala verksamhetssystem.
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Nej
Är de genomförda bedömningarna aktuella?	Nej

3.4.2 Syfte

Konsekvensbedömningar hjälper en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas. Baserat på bedömningen ska riskminimerande åtgärder vidtas. Konsekvensbedömningen ska göras innan en personuppgiftsbehandling påbörjas. Det är därför viktigt att förvaltningen har processer för att fånga upp nya personuppgiftsbehandlingar, exempelvis i projekt eller nyutveckling av IT-tjänster, och kunna bedöma om en konsekvensbedömning krävs.

Konsekvensbedömningen anses liksom registerförteckning och informationsklassning vara ett viktigt verktyg för verksamhetens dataskyddsarbete. Det finns ett uttryckligt krav enligt dataskyddsförordningen att utföra konsekvensbedömningar för alla behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1). Detta kan exempelvis vara om personuppgifter i stor omfattning behandlas om personer i beroendeställning, som elever, eller vid systematisk övervakning.

Utöver att dataskyddsförordningen ställer krav på att en konsekvensbedömning görs, är den ett utmärkt verktyg för att förbättra dataskyddet eftersom processer där personuppgifter behandlas systematiskt gås igenom för att identifiera risker eller avvikelser mot lagkrav. Konsekvensbedömningar är också ett sätt

att höja kunskapen om dataskydd hos medarbetare eftersom man då tvingas utvärdera sin informationshantering i förhållande till dataskyddskraven.

3.4.3 Resultat

Konsekvensbedömningar för personuppgiftsbehandlingar i utbildningsnämndens centrala verksamhetssystem genomfördes under 2021 som del av en insats för att uppfylla kraven på konsekvensbedömningar. Dataskyddsombudet bedömer att de konsekvensbedömningar som genomfördes under 2021 inte fullt ut uppfyller de formella kraven för en konsekvensbedömning och de har inte heller följts upp sedan dess.

I de lokala anvisningarna för informationssäkerhet och i stadens styrdokument för informationssäkerhet anges att vissa roller har ansvar för att en konsekvensbedömning görs, men styrdokumenten är idag inte fullt ut implementerade i verksamheten.

Sedan insatsen 2021 har inga nya konsekvensbedömningar gjorts vilket pekar på att konsekvensbedömningar inte är integrerade i förvaltningens arbete med informationsklassningar och riskanalyser. Dessutom saknas processbeskrivningar för att säkerställa att nya personuppgiftsbehandlingar genomgår en konsekvensbedömning. Kravet på en konsekvensbedömning beror inte enbart på hur många personers personuppgifter som hanteras, utan kan även krävas exempelvis för personuppgiftsbehandlingar i ett mindre projekt där uppgifter om elevers hälsa behandlas.

Det saknas också en systematisk genomgång över vilka pågående personuppgiftsbehandlingar som kräver en konsekvensbedömning. Nämndens registerförteckning har tidigare varit systembaserad och därmed inte lämplig för denna typ av genomgång, men nu finns möjlighet att utifrån registerförteckningen identifiera krav på när en konsekvensbedömning ska göras.

3.4.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
X	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga

	Inga brister av nämnvärd betydelse identifierade

3.4.5 DSO ger råd och rekommendationer till PUA

Av Integritetsskyddsmyndighetens (IMY:s) vägledning för när en konsekvensbedömning krävs går det att utläsa att de flesta av de behandlingar som sker inom utbildningsnämndens verksamhetsområde ska konsekvensbedömmas enligt dataskyddsförordningen eftersom nämnden behandlar en stor mängd personuppgifter, i många fall även känsliga, om ett stort antal personer.

Som nämns ovan, utgör konsekvensbedömningar inte bara ett uttryckligt krav enligt dataskyddsförordningen utan är också ett verktyg för förvaltningen att förbättra dataskyddet där det finns höga risker för enskildas integritet.

För att kunna dra nytta av konsekvensbedömningar och uppfylla lagkraven på desamma krävs först att personuppgiftsbehandlingar som anses utgöra ”hög risk” identifieras (dvs. behandlingar där en konsekvensbedömning krävs). Dataskyddsombudets bedömer att nämnden idag inte har genomförda konsekvensbedömningar som uppfyller kraven i dataskyddsförordningen. Därmed rekommenderar dataskyddsombudet att nämnden säkerställer att konsekvensbedömningar görs för befintliga personuppgiftsbehandlingar – detta kan göras utifrån registerförteckningen eller informationsklassningar – och även att en bedömning om en konsekvensbedömning krävs eller inte uttryckligen framgår av process- eller rutinbeskrivningar där nya personuppgiftsbehandlingar initieras, exempelvis processer relaterade till projekt eller inköp av IT-tjänster.

3.5 Individens rättigheter avseende rätten till tillgång (registerutdrag)

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	4 begäran om registerutdrag
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	1

3.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt ska garantera att den registrerade har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt förordningen att den personuppgiftsansvarig, utbildningsnämnden, tillgodoser rättigheterna i fråga.

Rättigheterna medför en rätt att ställa krav på att verksamheten vidtar vissa åtgärder, som exempelvis att lämna ut ett så kallat registerutdrag eller att rätta vissa uppgifter. Verksamheten har enligt dataskyddsförordningen artikel 12.3 en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran.

Om verksamheten inte klarar av att hantera en begäran från en registrerad person i enlighet med dataskyddsförordningens krav, kan det skada allmänhetens förtroende för hur nämnden hanterar personuppgifter. Det kan även leda till tillsynsärenden från IMY, med sanktioner som följd.

3.5.3 Resultat

Under 2023 har fyra begäran om registerutdrag hanterats. Av dessa har en begäran lämnats i tid, övriga tre har gått över den stadgade trettiodagarsfristen med några dagar. Dataskyddsombudet noterar

även att nuvarande processbeskrivning anger att de faktiska personuppgifterna inte ska lämnas ut i första skedet. Det är dataskyddsombudets bedömning att detta inte är förenligt med hur kraven kring rätten till tillgång är utformade. En personuppgiftsansvarig har krav på att underlätta utövandet av rättigheterna och själva syftet med registerutdrag (rätten till tillgång) är att kunna få insyn i vilka personuppgifter som behandlas och kontrollera lagligheten i behandlingen, vilket är svårt att göra utan att få tillgång till de faktiska personuppgifterna.

Statistik för hantering av begäran om att få utöva övriga rättigheter saknas då inte alla begäran registreras, enbart när ett formellt beslut om att inte tillmötesgå begäran fattas.

3.5.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
X	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

3.5.5 DSO ger råd och rekommendationer till PUA

Som anges ovan är de registrerades rättigheter centralt i förordningen. Det är viktigt att den personuppgiftsansvarige kan säkerställa att dessa rättigheter kan uppfyllas. Tidigare tillsynsbeslut tydliggör också att en personuppgiftsansvarig ska underlätta utövandet och att den lagstadgade fristen är ett maximum – registerutdrag ska lämnas ut skyndsamt. Europeiska dataskyddsstyrelsen (EDPB) har också meddelat att tillsynsmyndigheterna under 2024 avser genomföra en koordinerad insats om hur personuppgiftsansvariga hanterar rätten till tillgång. Detta kommer förmodligen leda till tillsynsärenden från IMY.

Dataskyddsombudet rekommenderar därför att processbeskrivningen för registerutdrag (rätten till tillgång) ses över för att säkerställa att svar lämnas i tid och för att tydliggöra att tillgång till de faktiska personuppgifterna eller en kopia på dem ska lämna ut i första skedet om inte individen uttryckligen anger att dessa inte önskas.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Incidenterna har upptäckts både internt av medarbetare och av personuppgiftsbiträden.
Hur många personuppgiftsincidenter har dokumenterats?	36
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	11 har ansetts behöva rapporteras
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	11 har ansetts behöva rapporterats

3.6.2 Syfte

Personuppgiftsincidenter är säkerhetsincidenter där personuppgifter, oavsiktligt eller avsiktligt, har förvanskats, raderats, är otillgängliga för verksamheten eller blivit tillgängliga för obehöriga.

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering. Incidenthanteringsprocessen ska leda till förbättringar i dataskyddet och förhindra framtida incidenter.

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se artikel 33). Detta innebär att de flesta personuppgiftsincidenter ska rapporteras till IMY, inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter, ska

rapportering även ske till de berörda registrerade personerna, utan dröjsmål.

Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt rapportering till de berörda personerna. Bristande förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner från IMY:s sida.

Enligt dataskyddsförordningen artikel 33.5 ska alla personuppgifts-incidenter dokumenteras, det vill säga även i de fall då incidenten inte ska rapporteras till IMY. Bristande dokumentering innebär en brist och leder även till problem med att få fram korrekta siffror avseende hur väl verksamheten lever upp till rapporteringsfristerna.

3.6.3 Resultat

Utbildningsförvaltningen har under 2023 antagit en ny anvisning för hantering av informationssäkerhetsincidenter. Då alla personuppgiftsincidenter klassas som informationssäkerhetsincidenter gäller anvisningen även för personuppgiftsincidenter. Anvisningen har ännu inte kommunicerats ut till samtliga i organisationen, men följs vid en incident.

Anvisningen och tillhörande mallar anger i dagsläget inte uttryckligen att åtgärder för att förhindra framtida incidenter alltid ska vidtas vid en incident. Vid allvarliga eller kritiska incidenter ska ett uppföljningsmöte ske för att dra lärdomar, men för övriga incidenter saknas tydliga anvisningar om att åtgärder bör ske.

Under 2023 har 36 incidenter rapporterats in, varav 11 har anmälts vidare till IMY. Alla avdelningar har dock inte rapporterat in incidenter vilket kan bero på en okunskap om vad en personuppgiftsincident är och hur den ska rapporteras.

3.6.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga

	Inga brister av nämnvärd betydelse identifierade

3.6.5 DSO ger råd och rekommendationer till PUA

I stort har nämnden en förmåga att upptäcka och hantera personuppgiftsincidenter. Dataskyddsombudet rekommenderar dock att relevanta delar av anvisningen kommuniceras ut till samtliga medarbetare så att alla känner till definitionen av en incident och vet hur den ska rapporteras.

Som nämns ovan anger anvisningen och rapporteringsmallarna inte tydligt nog att åtgärder för att förhindra framtida incidenter alltid ska vidtas. Dataskyddsombudet rekommenderar därför också att mallarna revideras så att varje incident ska kräva minst en åtgärd och att incidenter följs upp för att identifiera och införa förbättringar.

4 Genomförda granskningar under året

4.1 Sammanfattning

Dataskyddsombudsrollen var vakant under stora delar av 2023, därför har inga enskilda granskningar gjorts under året. Under 2022 genomfördes en granskning av utbildningsnämndens hantering av kamerabevakning på nämndens skolor. Förvaltningen har under året arbetat med DSO:s rekommendationer. Dataskyddsombudet avser följa upp skolornas kamerabevakning i slutet av 2024. Därutöver planeras följande särskilda granskningar:

- Personuppgiftsbehandlingar i sociala medier och samtycke som rättslig grund.
- Hantering av känsliga och extra skyddsvärda personuppgifter

5 Risker inom dataskydd

5.1 Sammanfattning

Utifrån de obligatoriska rapporteringsområdena har följande risker bedömts kräva omgående insatser eller åtgärder:

- Konsekvensbedömningar
- Individens rättigheter (rätten till tillgång/registerutdrag)

5.2 Resultatet av riskkartläggningen

Risk 1 - Konsekvensbedömning

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
X	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Risk 2 – Individens rättigheter (rätten till tillgång/registerutdrag)

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
X	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

5.3 DSO ger råd och rekommendationer till PUA

Utbildningsnämnden har under 2023 förbättrat sitt dataskyddsarbete inom flera områden i jämförelse med 2022. Av de brister som har framkommit i årets granskning bedömer dataskyddsombudet att de mest centrala riskerna i nuläget är avsaknaden av genomförda konsekvensbedömningar för pågående personuppgiftsbehandlingar och individens rättigheter vad gäller rätten till tillgång (registerutdrag).

Risk avseende konsekvensbedömningar

Som nämns ovan har vissa konsekvensbedömningar utifrån centrala verksamhetssystem gjorts under 2021 men dessa har inte följts upp sedan dess. Utbildningsnämnden behandlar personuppgifter om barn och elever i stor omfattning vilket betyder att en

konsekvensbedömning troligen kommer att krävas för många av nämndens personuppgiftsbehandlingar.

Dataskyddsombudet rekommenderar därför nämnden att:

1. Identifiera vilka pågående personuppgiftsbehandlingar uppfyller kritikerna för när en konsekvensbedömning krävs.
2. Genomföra eller uppdatera konsekvensbedömningarna i enlighet med de formella kraven i dataskyddsförordningen, tillsammans med en handlingsplan för de utestående riskerna från konsekvensbedömningen.
3. Säkerställa att konsekvensbedömningar görs för framtida personuppgiftsbehandlingar genom att se över befintliga rutiner/processer där nya personuppgiftsbehandlingar initieras (exempelvis vid köp av en ny IT-tjänst eller projekt).

Risk avseende individens rättigheter (rätten till tillgång/registerutdrag)

En av rättigheterna som personer vars personuppgifter nämnden behandlar har är rätten till tillgång till sina personuppgifter, även kallat registerutdrag.

Under 2023 har enbart en begäran om att utöva rättigheten hanterats i tid av totalt fyra begäran. Därutöver har dataskyddsombudet noterat att nuvarande rutin, som grundar sig på tidigare dataskyddsombudets rekommendation, anger att ingen tillgång eller kopior på de faktiska personuppgifterna lämnas ut i första skedet. Enbart om den registrerade uttryckligen begär om att få ta del av dem lämnas de faktiska uppgifterna.

Sedan framtagandet av förvaltningens rutin har europeiska dataskyddsstyrelsen (EDPB) publicerat en vägledning om rätten till tillgång[1] och IMY avslutat tillsynsärenden gällande rätten till tillgång[2]. Dataskyddsombudet bedömer att nämnden inte kan ha som en rutin att inte ge tillgång eller lämna ut kopior i första skedet eftersom nämnden dels har krav på sig att underlätta utövande av individers rättigheter, dels eftersom syftet med rättigheten är att kunna kontrollera lagligheten och riktigheten i hur personuppgifterna behandlas vilket blir svårt utan att ta del av de faktiska personuppgifterna.

[1] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_sv
[2] https://www.imy.se/tillsyner/spotify-ratten-till-tillgang/

Därför rekommenderar dataskyddsombudet att processen för begäran om registerutdrag ses över för att säkerställa att en begäran hanteras inom den lagstadgade tiden och att även tillgång eller kopior på de faktiska personuppgifterna lämnas ut (om inte individen särskilt anger att inga kopior önskas).

6 Övrigt att rapportera

6.1 Sammanfattning

Utöver de sex obligatoriska rapporteringsområdena och punkterna ovan har dataskyddsombudet observerat tre avvikelser gentemot kraven i dataskyddsförordningen som bedöms kräva åtgärd och därför tas upp i årsrapporten. Dessa redovisas nedan.

6.2 Övriga observationer

Rätten till information/informationsplikten

Dataskyddsförordningen ställer krav på att enskilda vars personuppgifter behandlas får information om hur detta sker och om bland annat de rättigheter som den enskilde har. Detta framgår av artikel 12 och 13 i dataskyddsförordningen. Den så kallade informationsplikten reglerar i detalj vad gäller vilken typ av information som ska ges och när (beroende på om personuppgifterna samlas indirekt från den enskilde eller från en annan källa). I övrigt innefattar informationsplikten bland annat att informationen ska ges på ett begripligt och tillgängligt sätt.

Skolorna informerar vårdnadshavare och elever vid läsårsstart. Informationen innehåller till viss del den informations som krävs, men beskrivningen utgår främst från IT-system som används och inte de faktiska personuppgiftsbehandlingarna. Övriga personer vars personuppgifter behandlas, exempelvis anställda, informeras inte särskilt om i dagsläget. Eftersom nämnden nu har en fullständig registerförteckning finns förutsättningar att identifiera kategorier av personer vars personuppgifter behandlas (exempelvis elever, vårdnadshavare, anställer eller andra) och skapa informationstexter till dessa målgrupper utifrån informationen i registerförteckningen.

Uppföljning av personuppgiftsbiträden

Personuppgiftsbiträden är företag eller organisationer som behandlar personuppgifter för nämndens räkning. Om ett personuppgiftsbiträde anlitas ska ett personuppgiftsbiträdesavtal (PUB-avtal) tecknas. Syftet med avtalet är att säkerställa att enskildas personuppgifter skyddas även när det är någon annan som

behandlar personuppgifterna genom att instruktioner ges för hur biträdet får behandla personuppgifterna.

Utbildningsförvaltningen har processer för att säkerställa att personuppgiftsbiträdesavtal tecknas och att krav på biträdet ställs, det saknas dock rutiner för hur biträden följs upp efter att personuppgiftsbiträdesavtalet tecknats.

Gallring och arkivering

Lagringsminimering är en av dataskyddsprinciperna och handlar om att personuppgifter endast får behandlas så länge de behövs för syftet. Inom offentlig förvaltning innebär lagringsminimering att hanteringsanvisningar tagits fram som anger om informationen ska gallras, i så fall när, eller om den ska bevaras (arkiveras) samt att gallring och arkivering sker enligt anvisningarna.

Utbildningsförvaltningen har under 2023 startat ett projekt som ska omhänderta arkivering och gallring i de IT-system inom Skolplattformen som ska bytas ut. Personuppgifter behandlas även i andra system utanför Skolplattformen där arkiverings- och gallringsrutiner saknas. Även i dessa fall pågår ett arbete med att kunna gallra och arkivera i system där detta idag inte sker. Dataskyddsombudet anser dock att gallring och arkivering av förvaltningens information är en viktig fråga, varför den tas upp i denna rapport, och har andra fördelar förutom att principen om lagringsmining följs, exempelvis att skadan av ett intrång eller läckage blir mindre eftersom färre personuppgifter behandlas i ett system.

6.3 DSO ger råd och rekommendationer till PUA

Utifrån ovanstående observationer rekommenderar dataskyddsombudet att ett arbete genomförs för att säkerställa den enskildas rätt till information om hur nämnden behandlar deras personuppgifter tillgodoses. I och med att nämnden nu har en fullständig registerförteckning, kan den användas som grund för att ta fram informationstexter till de grupper av individer vars personuppgifter nämnden hanterar.

Därutöver rekommenderar dataskyddsombudet att rutiner tas fram för hur personuppgiftsbiträdens personuppgiftshantering följs upp, exempelvis genom att inkludera uppföljning i övrig avtalsuppföljning, och att arkivering- och/eller gallringsrutiner eller funktioner tas fram där dessa saknas.