

GDPR Årsrapport

2022

Utbildningsnämnden

GDPR årsrapport
Januari 2023

Dnr:
Utgivningsdatum:
Kontaktperson: Johan Adolfsson

1 Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnd och bolagsstyrelse 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 integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för nämnd och styrelse 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 nämnd/bolagsstyrelse 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.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnd eller bolagsstyrelse ska kunna visa att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna *dokumenteringskyldighet*. Årsrapporten är även ett medel för nämnds/bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

1	Bakgrund	3
2	Sammanfattning	5
3	Obligatoriska rapporteringsområden	6
3.1	Registerförteckning.....	6
3.2	Styrdokument	9
3.3	Tekniska och organisatoriska åtgärder för personuppgifts- behandlingar.....	11
3.4	Konsekvensbedömningar	13
3.5	Individens rättigheter	15
3.6	Personuppgiftsincidenter	17
4	Genomförda granskningar under året	19
4.1	Sammanfattning	19
5	Risker inom dataskydd	20
5.1	Sammanfattning	20
5.2	Resultatet av riskkartläggningen	20
5.3	DSO ger råd och rekommendationer till PUA	21

2 Sammanfattning

I egenskap av ert dataskyddsombud lämnar jag följande årsrapport.

Dataskyddsförordningens syfte är att skydda de registrerades personuppgifter och personliga integritet. Det görs genom att säkerställa att den personuppgiftsansvarige (utbildningsnämnden) inte behandlar personuppgifter på ett sådant sätt som inte är förenligt med det syfte och ändamål för vilket de samlades in. Dataskyddsförordningen utgår från behandlingen av personuppgifter, det vill säga allt vad som den personuppgiftsansvarige gör med personuppgifterna.

Dataskyddsförordningen utgår inte från IT-system och tjänster utan utifrån verksamhetens processer. Nämndens olika verksamhetsprocesser, vilka personuppgifter som finns kopplade till dessa och vad som sker med personuppgifterna följs därför upp. IT-system och tjänster är bärare av informationen och används för att genomföra behandlingarna som nämnden har beslutat om. IT-system och tjänster måste vara anpassade för att kunna ge ett adekvat skydd för den typ av personuppgifter som ska behandlas i systemen/tjänsterna.

I rapporten framgår att flera av de risker som lyftes i föregående årsrapport kvarstår fortsatt även 2022. Det ska dock poängteras att utbildningsförvaltningen under 2022 har påbörjat arbeten inom samtliga områden som ansågs prioriterade i 2021 års årsrapport. Det är viktigt att det arbete som har påbörjats färdigställs då dessa åtgärder kommer att minska de nuvarande riskerna och öka skyddet för de registrerade och deras personliga integritet.

Inom utbildningsnämnden finns en god medvetenhet kring vikten av att skydda de personuppgifter som nämnden har blivit anförtrodd att behandla. Vad gäller nämndens centrala verksamhetssystem så har nämnden god kunskap kring hur personuppgifterna hanteras.

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 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 133 införda registreringar i förteckningen. De är införda i olika mallar och flera av dessa registreringar är ännu inte färdigställda.
Har nödvändiga uppdateringar gjorts?	Nej, inga uppdateringar har gjorts de senaste åren.
Bedöms registerförteckningen vara fullständig?	Nej, då inget arbete har genomförts för att säkerställa att förteckningen är fullständig.
Har verksamheten lämpliga rutiner för registerföring?	Nej, projekt pågår inom utbildningsförvaltningen

3.1.2 Syfte

För att något ska gå att skydda måste det först vara synligt för verksamheten. Det följer därför i klartext av dataskyddsförordningen (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. Registerförteckningen är därför dataskyddsarbetets centrala utgångspunkter samt säkerställer att verksamheten beaktar att det finns en laglig grund för all personuppgiftsbehandling. Det är därför viktigt att den personuppgiftsansvarige får information om hur komplett verksamhetens förteckning är. Om dokumenteringskravet i dataskyddsförordningen uppfylls kan verksamheten arbeta effektivt, systematiskt och riskbaserat och samtidigt värna individens integritet, särskilt när känsliga och särskilt skyddsvärda personuppgifter behandlas av verksamheten.

En registerförteckning på plats leder till att verksamheten kan arbeta mer resurs- och kostnadseffektivt med sitt systematiska och riskbaserade dataskyddsarbete.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

Antalet behandlingar i svaret överensstämmer med den granskningen som dataskyddsombudet har genomfört.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Inga nödvändiga uppdateringar har skett under det senaste året. Utbildningsförvaltningen har under året tillsatt ett projekt för att skapa en ny förteckning.

DSO bedömer hur fullständig registerförteckningen är

Eftersom den nuvarande registerförteckningen är strukturerad utifrån de IT-system som används i verksamheten så missas den mesta av den ostrukturerade behandlingen. Vidare så finns risken att behandlingar dubbelregistreras i och med att samma typ av behandlingen sker i flera olika IT-system och tjänster.

Den nuvarande förteckningen över nämndens behandlingar av personuppgifter har inte uppdaterats de senaste åren. Vid en genomgång av förteckningen så framkommer en oklar struktur där flera olika mallar för registrering har använts. Både de stora centrala IT-systemen, exempelvis Barn- och elevregistret, och tillfälliga

behandlingar, som exempelvis personalresor har registrerats. Därmed blandas på ett oklart sätt registreringar av både IT-system och verksamhetsprocesser.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Under 2022 inledde utbildningsförvaltningen ett projekt som har till syfte att skapa en processbaserad förteckning. I ett första steg arbetar projektet med att ta fram processer för hur arbete med att skapa registerförteckningen samt ta fram lämpliga rutiner för hur förteckningen ska upprätthålla lämplig standard.

3.1.4 DSO anger hur allvarliga bristerna är på en skala

X	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
	Inga brister av nämnvärd betydelse identifierade

3.1.5 DSO ger råd och rekommendationer till PUA

Förteckningen över nämndens personuppgiftsbehandlingar utgör grunden för att kunna ha kontroll över vilka behandlingar av personuppgifter som sker inom nämndens verksamhetsområde.

Dataskyddsförordningen utgår från behandlingar och inte IT-system. Om den personuppgiftsansvarige bygger sin s.k. registerförteckning utifrån ett systemperspektiv så kommer det material som är ostrukturerat inte kunna upptäckas, vidare kommer samma behandlingar av personuppgifter att noteras i flera poster.

Under 2022 har utbildningsförvaltningen inlett ett arbete med att skapa en ny processbaserad förteckning. Målet med arbetet är att denna processorienterade förteckning ska ersätta den idag systemorienterade förteckningen. Det arbete som hitintills genomförts har fokuserat på att inventera nuvarande förteckning och att ta fram rekommendationer på hur en ny förteckning bör se ut och vad den bör innehålla. Vidare har projektet också jobbat med att ta fram processer för hur att identifiera behandlingar.

Som dataskyddsbud ser jag mycket positivt på det arbete som sker med att skapa en ny förteckning. Även då ett arbete pågår så är den nuvarande förteckning fortsatt bristfällig och uppfyller i nuläget inte kraven i förordningen, därmed kvarstår den tidigare risken fram tills att den nya förteckningen börjar komma på plats.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Nej, idag finns det fyra styrande dokument som rör behandlingen av personuppgifter.
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

Av art. 5.2 dataskyddsförordningen framgår det att den personuppgiftsansvarige måste kunna visa att denne efterlever dataskyddsförordningen. En röd tråd i Dataskyddsförordningen är att viktiga arbetsätt och rutiner ska vara dokumenterade.

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

Finns lämplig styrande dokumentation på plats?

Av svaret framgår att det idag finns fyra styrande dokument, men inget av dessa är av en övergripande strategisk karaktär som anger hur nämnden ska hantera personuppgifter.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

De fyra dokumenten innehåller delvis lämplig kvalitet, och har under året uppdaterats.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

X	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
	Inga brister av nämnvärd betydelse identifierade

3.2.5 DSO ger råd och rekommendationer till PUA

Det saknas strategiskt styrdokument för hur nämnden avser att behandla de registrerades personuppgifter. Som angivits ovan så är en av de grundläggande principerna att den personuppgiftsansvarige ska kunna visa hur denne efterlever förordningen. Detta kan ske genom att ha tydliga riktlinjer för sin verksamhet om hur personuppgifter ska behandlas. Genom övergripande styrdokumentation skapas förutsättning att styra hanteringen av personuppgifter så att det sker på ett likvärdigt sätt inom nämndens verksamhetsområde. Avsaknaden av dokumentation innebär också en ökad svårighet för de registrerade att tillvarata sina rättigheter eftersom det saknas dokumentation kring hur nämnden avser behandla de registrerades personuppgifter.

Dataskyddsbudet ser positivt på att det under 2022 har inletts ett arbete för att implementera ett ledningssystem för att bättre kunna styra arbetet med informationssäkerheten. Då arbetet med att implementera ledningsteam ännu inte är på plats så blir dataskyddsbudet råd fortsatt att utbildningsnämnden bör ta fram tydliga styrande dokument för sina verksamheter, som utgår ifrån stadens styrdokument. Detta för att säkerställa kännedom om hur personuppgifter ska behandlas, både för de registrerande och de som behandlar personuppgifter i sin anställning.

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlings

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

Av svaren framkommer att 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.

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 2021 gör dataskyddsombudet samma bedömning även för 2022. 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?	Till viss del. De behandlingar som har konsekvensbedömts är kopplade till utbildningsnämndens centrala verksamhetssystem.
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Ja
Är de genomförda bedömningarna aktuella?	Ja

3.4.2 Syfte

Konsekvensbedömningen hjälper en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas i projekt eller linjeverksamhet. En konsekvensbedömning har till syfte att identifiera och dokumentera risker kopplade till en viss behandling, samt att bedöma sannolikheten och konsekvensen om riskscenariot skulle inträffa. Baserat på bedömningen kan/ska riskförebyggande åtgärder vidtas.

Konsekvensbedömningen anses liksom registerförteckning och informationsklassning som ett viktigt verktyg för verksamhetens dataskyddsarbete. Kravet på konsekvensbedömning är dessutom ett uttryckligt krav enligt dataskyddsförordningen, och ska utföras för alla behandlingar som "sannolikt leder till en hög risk för fysiska personers rättigheter och friheter" (artikel 35.1). Notera att integritetsskyddsmyndigheten ("IMY") på sin webbplats har publicerat en förtydligande förteckning över när personuppgiftsbehandlingar kräver en konsekvensbedömning. Det är viktigt att PUA genom årsrapporten får en uppdaterad bild av hur fullständig verksamhetens situation är i fråga om konsekvensbedömningar avseende dataskydd.

3.4.3 Resultat

Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?

Personuppgiftsbehandlingarna i utbildningsnämndens centrala verksamhetssystem har konsekvensbedömts. Dock har inte en fullständig genomlysning av nämndens samtliga behandlingar gjorts.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Bedömningen är att samtliga högriskbehandlingar har konsekvensbedömts.

Är de genomförda konsekvensbedömningarna aktuella?

Bedömningen är att samtliga konsekvensbedömningar är aktuella.

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
	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

3.4.5 DSO ger råd och rekommendationer till PUA

Av IMY:s vägledning går det att utläsa att de flesta av de behandlingar som sker inom utbildningsnämndens verksamhetsområde bör konsekvensbedömmas enligt dataskyddsförordningen. De konsekvensbedömningar som har genomförts har varit kopplade till de behandlingar som sker i de centrala verksamhetssystemen.

Dataskyddsombudet gör fortsatt bedömningen att utbildningsnämnden bör säkerställa att processer finns framtagna för att säkerställa att konsekvensbedömningar sker för de behandlingar som berörs samt att dessa hålls uppdaterade.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	2 begäran om registerutdrag 2 begäran om radering
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	4 (alla).

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

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

Svaren visar att det under 2022 inkommit två begäran om så kallade registerutdrag och två begäran om radering. Av dessa har inga begäran gått över den stadgade trettiodagarsfristen.

Resultatet visar på att nämnden uppfyller kraven i förordningen i stort.

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
	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

3.5.5 DSO ger råd och rekommendationer till PUA

Som ovan angivet är de registrerades rättigheter centralt i förordningen. Det är viktigt att den personuppgiftsansvarige kan säkerställa att dessa rättigheter kan uppfyllas. I och med att det idag inte finns några tydliga framtagna skriftliga rutiner för hur de registrerades rättigheter ska hanteras. Det är också viktigt att utbildningsnämnden säkerställer att dess personuppgiftsbiträden har möjligheten att fullgöra sina skyldigheter enligt förordningen och kan leverera de underlag som behövs för att uppfylla de registrerades rättigheter.

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?	9
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	6 har ansetts behöva rapporteras.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	0, detta har berott på längre handläggningstider för att få in tillräckligt underlag för anmälan.

3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen (artikel 4.12) ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”

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.

Rapporteringskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringskyldigheten 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 personuppgiftsincidenter 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

Hur väl förmår verksamheten att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten?

Det framgår tydligt av utbildningsnämndens delegationsordning att det är utbildningsdirektören som beslutar om en incident ska anmälas till tillsynsmyndigheten. Alla incidenter rapporteras även till dataskyddsombudet innan det går till utbildningsdirektören för beslut. Utöver detta så finns ingen tydlig fastslagen rutin med ansvarsfördelning för hur personuppgiftsincidenter (utöver sådana som betecknas som ”major incidents”) ska hanteras, utan de hanteras ad hoc. Eftersom det saknas en tydlig rutin innebär det att det tar längre tid att handlägga incidenterna. Underlag från personuppgiftsbiträdena för att kunna gå vidare med handläggningen har vid flera tillfällen tagit lång tid att få.

Dock ska noteras att nämnden alltid anmäler de incidenter som uppdagats och bedöms ska anmälas till tillsynsmyndigheten.

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
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

3.6.5 DSO ger råd och rekommendationer till PUA

Eftersom det fortsatt saknas tydlig rutin för hur personuppgiftsincidenter ska hanteras rekommenderas utbildningsnämnden att säkerställa att en sådan rutin tas fram och görs känd i organisationen. Eftersom hanteringen idag löses ad hoc innebär det en risk för att 72-timmarsgränsen för när en incident ska anmälas till tillsynsmyndigheten passeras. Vidare kan en ytterligare orsak till sena anmälningar vara att utbildningsnämndens personuppgiftsbiträden har långa handläggningstider för att kunna ta fram de uppgifter som nämnden behöver för att kunna lämna in korrekta underlag till tillsynsmyndigheten.

Risken med att det saknas en tydlig rutin är att inte alla personuppgiftsincidenterna upptäcks och kan dokumenteras.

Det är positivt att förvaltningen mot slutet av året intensifierade sitt arbete med att ta fram rutiner för hur personuppgiftsincidenter ska hanteras.

4 Genomförda granskningar under året

4.1 Sammanfattning

Under 2022 genomfördes en granskning av utbildningsnämndens hantering av kamerabevakning på nämndens skolor.

Utbildningsförvaltningen har under 2021 och 2022 arbetat med att ta fram nya uppdaterade rutiner för skolornas användning av kamerabevakning. Under granskningen besöktes ca 15 skolenheter inom både grundskola och gymnasieskola. Granskningen visar att skolorna har oftast satt upp kameror på grund av en särskild

anledning som exempelvis hot och våld. Det granskningen vidare visar är att skolorna sällan därefter gör återkommande bedömningar av om det fortsatt föreligger ett behov av kamerabevakning. De bör påpekas att kamerabevakning är att anses som särskilt integritetskränkande och kamerabevakning ska vara en sista åtgärd för att komma åt de problem som verksamheterna eftersträvar att åtgärda. Och särskilt när det kommer till barn. Vidare visar granskning på ett behov av att tydligare följa upp och ta fram rutiner för hur kamerabevakning ska ske ute på skolorna. Granskningen visar också att skolorna efterfrågar ytterligare stöd kring hur de ska jobbar med kamerabevakning.

5 Risker inom dataskydd

5.1 Sammanfattning

Risker som bedöms kräva omgående insatser eller åtgärder:

- Registerförteckningen behöver färdigställas
- Avsaknaden av styrande dokumentation avseende efterlevnaden av dataskyddsförordningen
- Rutin för personuppgiftsincidenter

5.2 Resultatet av riskkartläggningen

Risk 1 - Registerförteckning

X	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
	Inga brister av nämnvärd betydelse identifierade

Risk 2 - Styrdokument

X	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
	Inga brister av nämnvärd betydelse identifierade

Risk 6 – Personuppgiftsincidenter

	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 flera utmaningar med att öka efterlevnaden av dataskyddslagstiftningen. Av de brister som har framkommit under året bedömer dataskyddsombudet att de tre mest centrala riskerna i nuläget är bristen på överblick över vilka behandlingar som sker, bristen att kunna visa på hur utbildningsnämnden efterlever dataskyddslagstiftningen samt brist på rutin för hantering och identifiering av personuppgiftsincidenter.

Risk avseende registerförteckning

Som angivits ovan så är registerförteckningen grundläggande för att den personuppgiftsansvarige ska ha kontroll över vilka personuppgiftsbehandlingar som sker inom ramen för nämndens verksamhetsområde. Det är positivt att ett arbete har påbörjats med att införa en processororienterad registerförteckning, men fram tills den är implementerad så kvarstår dock den aktuella risken kring att utbildningsnämnden inte har en klar bild över de behandlingar som sker.

Risk avseende dokumentation

Avsaknaden av dokumentation innebär att det finns en ökad risk för att behandling av personuppgifter sker på olika sätt inom nämndens verksamhetsområde. Det innebär även en ökad svårighet för de registrerade att tillvarata sina rättigheter när det saknas

dokumentation kring hur nämnden avser behandla de registrerades personuppgifter.

Dataskyddsombudet råder utbildningsnämnden att ta fram tydliga styrande dokument för sina verksamheter när det gäller hur personuppgifter ska användas och hanteras inom nämndens olika verksamhetsområden. Genom övergripande styrdokumentation skapas förutsättning att styra hanteringen av personuppgifter så att det sker på ett likvärdigt sätt inom nämndens verksamhetsområde. Dataskyddsombudet ser positivt på det arbete som pågår med att ta fram ledningssystem och styrande dokument och rekommenderar utbildningsnämnden att säkerställa att detta arbete slutförs och att ledningssystem och styrdokument görs kända i organisationen.

Risk avseende personuppgiftsincidenter

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering. Enligt dataskyddsförordningen ska alla personuppgiftsincidenter dokumenteras.

Eftersom det saknas fastställd tydlig rutin för hur personuppgiftsincidenter ska hanteras rekommenderas utbildningsnämnden att säkerställa att det påbörjade arbetet med att ta fram en sådan rutin slutförs och att den görs känd i organisationen.

Risken med att det saknas en tydlig rutin är att inte alla personuppgiftsincidenterna upptäcks och dokumenteras eller anmäls till tillsynsmyndigheten i tid.