Stockholms stad

GDPR Årsrapport

2024

Förskolenämnden

GDPR årsrapport
December 2024

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, främst rätten till privatliv och skyddet för enskildas personuppgifter, men även övriga rättigheter fastställda i EU:s rättighetsstadga.

Som personuppgift räknas all typ av information som kan kopplas till en fysisk person och den organisation som behandlar personuppgifterna behöver inte kunna göra detta själv utan det räcker att det är möjligt med rimliga och lagliga medel. Därmed hanterar varje organisation personuppgifter i någon omfattning och behöver förhålla sig till dataskyddslagstiftningen.

Enligt dataskyddsförordningen är varje nämnd inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnden 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 råd och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för nämnd 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 ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd 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.

Dataskyddsförordningens syfte är att skydda de enskildas personuppgifter och personliga integritet. Det görs genom att säkerställa att den personuppgiftsansvarige (förskolenämnden) enbart hanterar personuppgifterna i enlighet med de grundläggande principerna som anger bland annat att personuppgifter enbart får samlas in för uttryckligt angivna syften utifrån en rättslig grund och får inte lagras längre än nödvändigt för syftet. Dataskyddsförordningen ställer även andra specifika krav, som rapportering av personuppgiftsincidenter och rättigheter för enskilda vars personuppgifter den personuppgiftsansvarige hanterar.

Under 2024 har förskoleförvaltningen fortsatt uppbyggnaden av sitt systematiska dataskyddsarbete. Förvaltningen har nu styrdokument på plats i form av den lokala anvisningen för informationssäkerhet (där även dataskydd ingår) och anvisning för informationssäkerhetsincidenter (där personuppgiftsincidenter ingår). Dataskyddsombudet rekommenderar nämnden att fokusera på att färdigställa sin registerförteckning och sedan som nästa steg genomföra konsekvensbedömningar, där så krävs, och kartlägga sina informationsmängder för att säkerställa att nämndens information skyddas på ett lämpligt sätt samt ta fram rutiner för att hantera individers rättigheter.

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?	Ca 100 system i den förteckning som fanns på utbildningsförvaltningen
Har nödvändiga uppdateringar gjorts?	Delvis
Bedöms registerförteckningen vara fullständig?	Registerförteckningen utgår från system och anses därmed inte vara fullständig.
Har verksamheten lämpliga rutiner för registerföring?	Delvis

3.1.2 Syfte

Varje personuppgiftsansvarig ska enligt artikel 30 i GDPR ha en förteckning över sina personuppgiftsbehandlingar (en registerförteckning) där bland annat syfte, typer av personuppgifter och lagringstid framgår. Registerförteckningen är förutsättning för att överhuvudtaget kunna efterleva dataskyddsförordningens krav då flera övriga krav förutsätter att den personuppgiftsansvariga dokumenterat vilka personuppgifter

som behandlas, hur och varför. Registerförteckningen är också ett sätt att uppfylla principen om ansvarsskyldighet (artikel 5.2) som anger att den personuppgiftsansvarige ska kunna visa att de grundläggande principerna för behandling av personuppgifter efterlevs.

3.1.3 Resultat

Förskoleförvaltningen var fram till den sista juni 2023 en del av utbildningsförvaltningen och då ingick även de personuppgiftsbehandlingar som nu tillhör förskolenämnden i registerförteckningen upprättad inom utbildningsförvaltningen. Registerförteckningen från tiden då verksamheten tillhörde utbildningsförvaltningen är systembaserad. Registerförteckningen ska däremot utgå från personuppgiftsbehandlingar inte system, dvs. vilka personuppgifter som hanteras av nämnden för vilka syften. På förskoleförvaltningen har pågår ett arbete för att upprätta en ny registerförteckning som utgår från förvaltningens hanteringsanvisningar och processer i den.

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

Förskoleförvaltningen har ett pågående arbete med att uppdatera registerförteckningen. Dataskyddsombudet rekommenderar därför att förvaltningen fortsätter och slutför detta arbete.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Delvis
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?	Ja

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 2024 har förskoleförvaltningen tagit fram en lokal anvisning för informationssäkerhet, som även inkluderar dataskydd, och en anvisning för informationssäkerhetsincidenter, som även inkluderar personuppgiftsincidenter. Den lokala anvisningen fastställer roller

och ansvar inom dataskydd och informationssäkerhet på förvaltningen. Det finns därmed goda förutsättningar att bygga upp det systematiska arbetet. Dock saknas idag rutiner för att hantera individers rättigheter. Det är främst brådskande att en rutin för att hantera rätten till tillgång (registerutdrag) tas fram då denna typ av begäran kan vara omfattande och kommer att vara tidskrävande om förvaltningen saknar rutiner.

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
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

3.2.5 DSO ger råd och rekommendationer till PUA

Förskoleförvaltningen har under 2024 antagit två viktiga styrdokument som ligger till grund för förvaltningens dataskyddsarbete. Dock saknas i dagsläget rutiner för hantering av individers rättigheter. Dataskyddsombudet rekommenderar därför att rutiner för hantering av dessa rättigheter tas fram.

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?	Informationsklassning har skett av de system som används och som tillhör portföljstyrningen av stadens pedagogiska verksamheter
Är klassade personuppgiftsbehandlingar aktuella?	Årlig uppdatering av informationsklassning sker för system som förvaltas inom ramen för portföljstyrningen av stadens pedagogiska verksamheter

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

Förvaltningens IT-system och tjänster förvaltas främst av utbildningsförvaltningen inom ramen för portföljstyrningen av stadens pedagogiska verksamheter. Dessa IT-system och tjänster har informationsklassats, dock är flera av dessa inte uppdaterade. I nuläget har information som tillhör förskolenämnden inte identifierats därmed är det oklart om all information tillhörande nämnden har informationsklassats.

Informationsklassning är dock enbart 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
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

3.3.5 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. Därför är det viktigt att den information som tillhör förskolenämnden identifieras och klassificeras utifrån förskolenämndens krav. Om flera nämnder eller verksamheter använder samma system framgår inte de enskilda informationsmängdernas skyddsbehov av informationsklassningen på systemnivå och hanteringen och kraven kan inte anpassas efter behoven. Dataskyddsombudet rekommenderar att nämndens information kartläggs och klassificeras utifrån informationsmängd i enlighet med stadens riktlinjer för informationssäkerhet.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Nej
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Nej
Är de genomförda bedömningarna aktuella?	-

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 som ett viktigt verktyg för verksamhetens dataskyddsarbete. Det finns därutöver 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 barn eller anställda, eller vid övervakning eller profilering.

3.4.3 Resultat

Konsekvensbedömningar ska genomföras innan en personuppgiftsbehandling påbörjas men även för pågående personuppgiftsbehandlingar ska en konsekvensbedömning göras om kriterierna för detta är uppfylla. I dagsläget har ingen genomgång av nämndens personuppgiftsbehandlingar gjorts för att säkerställa att

konsekvensbedömningar gjorts där så krävs. Detta är ett arbete som med fördel kan genomföras i samband med att registerförteckningen uppdateras.

Vad gäller processer för att säkerställa att konsekvensbedömningar görs för nya personuppgiftsbehandlingar finns delvis angivet i den lokala anvisningen om ansvar kring detta. Förvaltningen behöver dock förtydliga ansvaret och även införliva kraven i processer som rör nya projekt eller inköp av tjänster för att säkerställa att dataskyddsfrågor inte tappas bort.

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

Som framgår av ovan saknas dels en bedömning av om nämndens befintliga personuppgiftsbehandlingar bör genomgå en konsekvensbedömning, dels delvis rutiner för att säkerställa att konsekvensbedömningar görs i framtiden, där så krävs. Dataskyddsombudet rekommenderar därför att inkludera bedömningen om en konsekvensbedömning krävs eller inte i registerförteckningen och se över sina processer där nya personuppgiftsbehandlingar uppstår, exempelvis projekt eller inköp av digitala tjänster, för att säkerställa att konsekvensbedömningar görs, där så krävs.

3.5 Individens rättigheter

3.5.1 Sammanfattning

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

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 2024 har en begäran om registerutdrag inkommit till förvaltningen. I dagsläget saknas dock beslutade rutiner för hur en begäran om registerutdrag ska hanteras. Förvaltningen utgår idag från arbetssätt som fanns i den tidigare organisationen och har utpekade funktioner för att hantera begäran från individer som vill utöva sina rättigheter enligt dataskyddsförordningen.

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.

Eftersom beslutade rutiner för att hantera registrerades rättigheter saknas för närvarande rekommenderar dataskyddsombudet att dessa tas fram - framför allt en rutinbeskrivning för registerutdrag (rätten till tillgång) då hantering av denna rättighet kräver upparbetade arbetssätt.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Anställda, medborgare
Hur många personuppgiftsincidenter har dokumenterats?	2
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	2 rapporterat till IMY.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Samtliga

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.

Rapporteringsskyldighet till tillsynsmyndigheten
Integritetsskyddsmyndigheten (IMY) 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.

Alla personuppgiftsincidenter klassas som informationssäkerhetsincidenter, därmed bör personuppgiftsincidenter hanteras enligt samma process som gäller för informationssäkerhetsincidenter för att undvika dubbelarbete även om dataskyddsförordningen ställer särskilda krav på just hantering av personuppgiftsincidenter.

3.6.3 Resultat

Under 2024 har en anvisning för informationssäkerhetsincidenter (inkluderar även personuppgiftsincidenter) antagits av förvaltningen och två personuppgiftsincidenter har rapporterats in. Båda dessa incidenter har rapporterats vidare till IMY. IMY har avslutat båda dessa ärenden utan åtgärd.

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

Under 2024 har förvaltningen antagit en anvisning för informationssäkerhetsincidenter och även rapporterat in två incidenter som bedömdes behöva rapporteras vidare till IMY. Utöver dessa två allvarligare incidenter har inga andra incidenter rapporterats. Dataskyddsombudet rekommenderar att förvaltningen fortsatt kommunicera kring incidentrutinen till medarbetare.

4 Risker inom dataskydd

4.1 Sammanfattning

Uppbyggnaden av förskolenämndens dataskyddsarbete har fortsatt under 2024 och inför 2025, utifrån dataskyddsombudets rapportering ovan, bedöms följande områden kräva omgående insatser eller åtgärder:

- Rutiner för individers rättigheter
- Konsekvensbedömningar
- Informationsklassning och kartläggning av nämndens informationsmängder

4.2 Resultatet av riskkartläggningen – områden med högst risker

Risk 1 – Rutiner för individers rättigheter

	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 – Konsekvensbedömningar

	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 3 – Informationsklassning och kartläggning av nämndens informationsmängder

	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

4.3 DSO ger råd och rekommendationer till PUA

Av de avvikelser som framkommit i rapporten bedömer dataskyddsombudet att de mest centrala riskerna i nuläget är avsaknaden av rutiner för att hantera individers rättigheter, konsekvensbedömningar och kartläggning av nämndens information, inklusive informationsklassningar.

Behovet av konsekvensbedömningar och även kartläggning av nämndens information (inklusive informationsklassningar) kan med fördel bedömas i samband med att registerförteckningen upprättas. Förvaltningen har redan ett pågående arbete med att uppdatera registerförteckningen och en naturlig fortsättning på det arbetet är då att säkerställa att konsekvensbedömningar och informationsklassningar genomförts. Därutöver behöver förvaltningen ta fram rutiner för hur registrerades rättigheter hanteras.