Stockholms stad

GDPR Årsrapport Förskolenämnden

2023

Förskolenämnden

Dnr: 2024/25

GDPR årsrapport
December 2023

Dnr: FÖF 2024/25
Utgivningsdatum: 2024-01-23
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. 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 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 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 förskolenämnden.

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.

Förskoleförvaltningen inrättades den 1 juli 2023 varför förvaltningens dataskyddsarbete fortfarande är under uppbyggnad. Därför finns inte vissa av de grundläggande komponenterna av ett systematiskt dataskyddsarbete på plats, främst en komplett registerförteckning och antagna styrdokument. Från tidigare organisation finns dock arbetssätt och kompetens, men dataskyddsarbetet behöver anpassas till den nya organisationen. Dataskyddsombudet rekommenderar nämnden att fokusera på att färdigställa sin registerförteckning och ta fram styrdokument, däribland för hantering av personuppgiftsincidenter.

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

För att något ska gå att skydda måste det först vara synligt för verksamheten. Det följer därför av dataskyddsförordningen (artikel 30) att nämnden måste inventera alla personuppgifter som behandlas i verksamheten 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 utgångspunkter.

3.1.3 Resultat

Förskoleförvaltningen var fram till den sista juni en del av utbildningsförvaltningen och då ingick även de personuppgiftsbehandlingar som nu tillhör förskolenämnden i registerförteckningen upprättad inom utbildningsförvaltningen som då var systembaserad. Utbildningsförvaltningen har under hösten 2023 genomfört ett arbete med att ta fram en ny processbaserad registerförteckning som ska ersätta den systembaserade.

Registerförteckningen ska nämligen utgå från personuppgiftsbehandlingar, vilka personuppgifter som hanteras av nämnden för vilka syften, och inte system eftersom ett system kan innehålla många olika typer av personuppgiftsbehandlingar för olika syften som då inte framgår av en systembaserad registerförteckning. Eftersom förskolenämndens registerförteckning utgår från den systembaserade registerförteckningen är den i behov av uppdatering. Förvaltningen har för avsikt att uppdatera registerförteckningen under 2024.

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
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

3.1.5 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 registerförteckning utifrån ett systemperspektiv kommer den inte kunna fånga upp de faktiska personuppgiftsbehandlingar som sker. Det blir även svårare att uppfylla andra krav, exempelvis enskildas rätt till information om hur nämnden behandlas deras personuppgifter och hantering av registerutdrag.

Dataskyddsombudet rekommenderar därmed att registerförteckningen uppdateras för att utgå från faktiska personuppgiftsbehandlingar som sker och inte system.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Inga styrdokument har formellt antagits av den nya organisationen.
Håller innehållet i de existerande dokumenten lämplig kvalitet?	-
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	-
Är dokumenten uppdaterade?	-
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	-

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

Förskoleförvaltningen inrättades den 1 juli och har under hösten 2023 arbetat med att ta fram nödvändiga styrdokument inom dataskyddsområdet. Dessa styrdokument är dock ännu inte antagna, så därför saknas för närvarande formellt antagna styrdokument som styr nämndens dataskyddsarbete. Funktioner och arbetssätt från den gamla organisationen har dock följt med i den nya organisationen även om dessa ännu inte formellt antagits i ett styrdokument.

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

Dataskyddsombudet rekommenderar att nödvändiga styrdokument, framför allt den lokala anvisningen för informationssäkerhet, anvisning för informationssäkerhetsincidenter, rutin för rätten till tillgång (registerutdrag) och instruktioner till enskilda medarbetare om hur de ska hantera personuppgifter på ett säkert sätt, färdigställs och antas formellt samt kommuniceras ut till organisationen. Förvaltningen avser formellt anta styrdokument inom dataskyddsområdet i början av 2024.

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

De IT-system och tjänster som förvaltas av utbildningsförvaltningen inom ramen för portföljstyrningen av stadens pedagogiska verksamheter har informationsklassats och dessa uppdateras också årligen. I nuläget har dock inte all information som tillhör förskolenämnden identifierats därmed är det oklart om all information tillhörande nämnden 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
	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. 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

I dagsläget saknas processer för att säkerställa att framtida och befintliga personuppgiftsbehandlingar genomgår en konsekvensbedömning. Detta beror främst på att styrdokument på området ännu inte antagits och att en fullständig registerförteckning saknas.

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 processer för att fånga upp nya och befintliga personuppgiftsbehandlingar där en konsekvensbedömning krävs, dels en registerförteckning som ger en helhetsbild över de faktiska personuppgiftsbehandlingarna som sker. Dessa är nödvändiga för att kunna identifiera behovet av en konsekvensbedömning och därför rekommenderas att det av styrdokument eller rutiner framgår att konsekvensbedömningar ska genomföras innan nya personuppgiftsbehandlingar inleds, där så krävs, och behovet av konsekvensbedömningar för befintliga personuppgiftsbehandlingar kartläggs efter att en fullständig registerförteckning finns på plats.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	0 begäran om registerutdrag
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	-

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

Sedan 1 juni 2023 då förskoleförvaltningen inrättades har inga begäran om att utöva rättigheter inkommit. I dagsläget saknas också beslutade rutiner för hur en begäran om registerutdrag ska hanteras. Förvaltningen utgår dock 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 processer. Förvaltningen avser anta beslutade rutiner i början av 2024.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Inga incidenter har rapporterats sedan 1 juli 2023.
Hur många personuppgiftsincidenter har dokumenterats?	-
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	-
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	-

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

Sedan 1 juli 2023 då förskoleförvaltningen inrättades har inga personuppgiftsincidenter rapporterats in. Ett arbete pågår med att ta fram en beslutad anvisning för informationssäkerhetsincidenter, som personuppgiftsincidenter är en del av.

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

Dataskyddsombudet rekommenderar att anvisningen för informationssäkerhetsincidenter beslutas och kommuniceras ut i organisationen för att medarbetare ska kunna identifiera en incident och veta hur den ska rapporteras. Anvisningen planeras antas formellt av förvaltningen i början av 2024.

4 Genomförda granskningar under året

4.1 Sammanfattning

Dataskyddsombudsrollen har varit vakant delar av 2023, därmed har inga specifika granskningar gjorts under året. Eftersom förskoleförvaltningens dataskyddsarbete fortfarande är under uppbyggnad, avser dataskyddsombudet inte göra några specifika granskningar under nästa år utan dataskyddsombudet kommer fokusera på att ge råd och stöd för att säkerställa att de grundläggande dataskyddskraven efterlevs.

5 Risker inom dataskydd

5.1 Sammanfattning

Förskolenämndens dataskyddsarbete är fortfarande under uppbyggnad och därmed finns vissa grundstenar ännu inte på plats. Utifrån dataskyddsombudets rapportering ovan, bedöms följande områden kräva omgående insatser eller åtgärder:

- Registerförteckningen
- Styrdokument
- Personuppgiftsincidenter

5.2 Resultatet av riskkartläggningen

Risk 1 - Registerförteckning

	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 – Styrdokument

	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 – 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

Av de avvikelser som framkommit bedömer dataskyddsombudet att de mest centrala riskerna i nuläget är avsaknaden av en komplett registerförteckning, styrdokument och process för personuppgiftsincidenter. Som nämns ovan rekommenderar dataskyddsombudet att registerförteckningen färdigställs och styrdokument inom dataskyddsområdet färdigställs, däribland anvisning för informationssäkerhetsincidenter som kommuniceras till medarbetare för att säkerställa att incidenter upptäcks, hanteras och förbättringar vidtas.