Stockholms stad

GDPR Årsrapport 2025

Bilaga till verksamhetsberättelse
Förskolenämnden

GDPR årsrapport 2025

Dnr: FÖF 2025/372
Kontaktperson: Cecilia Adriano

1 Bakgrund

Dataskyddsförordningen (hädanefter GDPR) trädde i kraft som lag i Sverige den 25 maj 2018. Förordningen har som övergripande syfte att skydda individers grundläggande rättigheter och friheter, särskilt rätten till skydd av personuppgifter. Förordningen utgår från principer om laglighet, korrekthet, transparens, riktighet, ändamålsbegränsning, dataminimering, lagringsbegränsning, integritet och konfidentialitet. Dessa principer syftar till att säkerställa att personuppgifter hanteras på ett ansvarsfullt, rättvist och rättssäkert sätt, i linje med de mänskliga rättigheterna. Förordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna inom EU.

Inom Stockholm stad har varje nämnd och styrelse ett tydligt ansvar att säkerställa att personuppgiftsbehandlingar inom den egna verksamheten sker i enlighet med GDPR-krav. Detta innefattar bland annat att Förskolenämnden (hädanefter nämnden) behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Denna årsrapport är ett medel för nämnden att ta emot de råd och rekommendationer som dataskyddsombudet (DSO) är skyldig att ge till ansvarig enligt GDPR samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar.

GDPR bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnden ska kunna *visa* att verksamheten efterlever GDPR. Årsrapporten är en mycket viktig del av denna *dokumenteringsskyldighe*t. Årsrapporten är även ett medel för nämndens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

2 Sammanfattning

Inom ramen för DSO:s uppdrag lämnas härmed årsrapport för 2025 till nämnden. Rapporten omfattar sex centrala områden där nämndens efterlevnad av GDPR har granskats utifrån definierade kontrollpunkter.

Under året har nämnden tagit viktiga steg i arbetet med dataskydd bland annat genom att anta lokala anvisningar för informationssäkerhet och hantering av informationssäkerhetsincidenter inklusive personuppgiftsincidenter. Två personuppgiftsincidenter har anmälts till Integritetsskyddsmyndigheten (hädanefter IMY) inom föreskriven tidsram enligt art. 33 GDPR vilket visar att förvaltningen har förmåga att identifiera och rapportera incidenter i tid.

Trots framsteg kvarstår flera utvecklingsområden. Rutiner för hantering av registrerades rättigheter, särskilt rätten till tillgång (registerutdrag) saknas och behöver färdigställas. Arbetet med konsekvensbedömningar (hädanefter DPIA) är delvis genomfört men behöver kompletteras och hållas aktuellt för samtliga högriskbehandlingar. Informationsklassning av IT-system och tjänster har påbörjats men är inte fullständigt uppdaterad vilket är en förutsättning för att kunna vidta lämpliga tekniska och organisatoriska skyddsåtgärder enligt art. 32 GDPR.

DSO rekommenderar att nämnden upprättar en strukturerad och långsiktig plan för arbetet med dataskydd under kommande år. Syftet är att skapa en tydlig överblick över prioriteringar och säkerställa att resurser fördelas effektivt. En samlad bedömning bör göras utifrån nämndens övergripande mål och prioriteringar eftersom dataskydd enligt en ska integreras i verksamhetens styrning och målstruktur. Detta möjliggör ett systematiskt, riskbaserat och proportionerligt arbetssätt i enlighet med principerna om inbyggt dataskydd och dataskydd som standard (artikel 25 GDPR) vilket är avgörande för att uppfylla kraven i förordningen och minimerar rättsliga och förtroendemässiga risker.

3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som Personuppgiftsansvarig (hädanefter PuA) som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som GDPR avser.

De obligatoriska rapporteringsområdena är registerförteckning, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, DPIA, 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 137
Har nödvändiga uppdateringar gjorts?	Delvis. Det är ett pågående arbete
Bedöms registerförteckningen vara fullständig?	Delvis.
Har verksamheten lämpliga rutiner för registerföring?	Ja, en rutin/stödmaterial är framtagen. Kontaktvägar finns. Support i förvaltningen

3.1.2 Syfte

Enligt art. 30 i GDPR ska varje PuA föra en förteckning över verksamhetens behandlingar av personuppgifter – en så kallad registerförteckning. Denna ska bland annat innehålla uppgifter om syftet med behandlingen, kategorier av personuppgifter samt lagringsperioder. Registerförteckningen utgör en grundläggande förutsättning för att kunna uppfylla förordningens krav på dokumentation av personuppgiftsbehandlingar.
Registerförteckningen utgör även ett centralt verktyg för att säkerställa efterlevnad av principen om ansvarsskyldighet enligt art. 5.2 GDPR vilken innebär att PuA ska kunna styrka att de grundläggande principerna för behandling av personuppgifter efterlevs.

3.1.3 Resultat

Förvaltningen har hittills utfört ett betydande och strukturerat arbete med att ta fram en registerförteckning anpassad efter förvaltningens hanteringsanvisningar och processer. En betydande del av arbetet är genomfört och arbetet är pågående När arbetet är grundlagt kommer registerförteckningen att utgöra ett viktigt stöd i det systematiska dataskyddsarbetet och bidra till ökad transparens och effektivitet i förvaltningens informationshantering. För att säkerställa att registerförteckningen fortsätter att vara ett relevant och användbart. verktyg krävs att den uppdateras löpande i takt med förändringar i verksamhetens behandling av personuppgifter

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

Nämnden har ett pågående arbete med att uppdatera registerförteckningen. DSO rekommenderar därför att förvaltningen fortsätter med detta arbete på ett systematiskt sätt.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Lokala anvisningar antagen, uppdaterad och godkänd.
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

Styrdokument utgör en grundläggande förutsättning för att säkerställa att behandling av personuppgifter sker i enlighet med GDPR. Genom att tydliggöra ansvarsfördelning, arbetsprocesser och krav på efterlevnad bidrar styrdokument till en rättssäker, transparent och enhetlig hantering. Inom den offentlig sektor där krav på rättssäkerhet och insyn är särskilt höga är styrdokument avgörande för att möjliggöra ett systematiskt dataskyddsarbete som stärker allmänhetens förtroende och verksamhetens förmåga att uppfylla lagstadgade skyldigheter.

3.2.3 Resultat

Under 2025 har nämnden uppdaterat och godkänt en lokal anvisning för informationssäkerhet vilken även omfattar dataskydd samt en anvisning för hantering av informationssäkerhetsincidenter inklusive personuppgiftsincidenter. Den lokala anvisningen tydliggör roller och ansvar inom dataskydd och informationssäkerhet på förvaltningen vilket skapar goda förutsättningar för ett systematiskt och strukturerat arbete i enlighet med GDPR och tillämpliga föreskrifter.
Arbete med framtagande och fastställande av lokala rutiner för hantering av de registrerades rättigheter är pågående.

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
x	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

Nämnden bör fortsatt färdigställa, uppdatera och implementera lokala rutiner för hantering av registrerades rättigheter i enlighet med art. 12–22 i GDPR. Rutinerna ska säkerställa att stadens övergripande riktlinjer anpassas till den lokala verksamheten och att begäran om exempelvis rätten till tillgång (registerutdrag), rättelse, radering och begränsning av behandling kan hanteras effektivt och rättssäkert. Detta är nödvändigt för att uppfylla kraven på transparens, rättssäkerhet och skyndsam handläggning enligt IMY:s vägledningar och GDPR principer.

Nämnden bör även säkerställa implementering av antagna lokala styrdokument för dataskydd. Implementeringen ska genomföras på ett sätt som medvetandegör verksamheten om gällande rutiner och säkerställer att dessa efterlevs i det dagliga arbetet. Detta är nödvändigt för att uppfylla kraven på ansvarsskyldighet enligt art. 5.2 i GDPR och för att följa IMY:s vägledningar om systematiskt dataskyddsarbete. Vidare bör lokala styrdokument kompletteras med en kontinuitetsplan som säkerställer drift och återhämtning vid incidenter.

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 Nämnden har även sammanställt en lista under 2025 över befintliga system och tjänster utöver de som tillhör stadens portföljstyrning och dessa klassas efter en prioriteringsordning med start under hösten 2025 och fortsätter vidare in i 2026.
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 säkerställa att personuppgiftsbehandling sker i enlighet med GDPR ska lämpliga tekniska och organisatoriska åtgärder alltid tillämpas. Syftet är att skydda individers rätt till integritet och att förebygga obehörig åtkomst, förlust, ändring eller spridning av personuppgifter. Genom att tillämpa tekniska och organisatoriska skyddsåtgärder säkerställs hantering av personuppgifter på ett säkert, korrekt och lagligenligt sätt vilket bidrar till ett systematiskt dataskyddsarbete och minimerar risken för dataskyddsincidenter. Som stöd för att identifiera och bedöma behovet av skyddsåtgärder är stadens riktlinje att använda SKR:s verktyg KLASSA. Verktyget ger ett strukturerat stöd för att klassificera all information utifrån dess känslighet, tillgänglighet och riktighet vilket underlättar val av säkerhetsnivå och åtgärder dock anses KLASSA vara ett bra stöd för informationssäkerhet men räcker inte för att uppfylla GDPR och IMY:s krav. Kompletterande åtgärder som DPIA, behandlingsregister och avtal krävs.

3.3.3 Resultat

Nämndens 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 och behandlingar som omfattas av stadens portföljstyrning och som tillhör nämnden inte identifieras. Därmed är det oklart om all information som tillhör nämnden genomgått informationsklassning. Däremot har nämnden under 2025 sammanställt en lista över befintliga system och tjänster som inte omfattas av stadens portföljstyrning. Dessa klassas efter en prioriteringsordning med start under hösten 2025 och fortsätter vidare in i 2026.

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

Nämnden bör säkerställa att informationsklassning av IT-system och tjänster är aktuell och komplett inklusive identifiera information och behandlingar som tillhör nämnden. Informationsklassning är endast det första steget i arbetet med informationssäkerhet och dataskydd. När skyddsvärdet är fastställt ska förvaltningen vidta lämpliga tekniska och organisatoriska åtgärder för att skydda informationen i enlighet med GDPR, stadens riktlinjer och IMY:s vägledningar om säkerhetsåtgärder. Detta är nödvändigt för att uppfylla kraven på integritet, konfidentialitet och ansvarsskyldighet enligt art. 5 och 32 GDPR.
Som en del av detta arbete bör en handlingsplan upprättas/genomföras. Först bör en inventering av informationstillgångar göras för att identifiera all information som tillhör nämnden i befintliga IT-system och tjänster. Därefter bör informationsklassningen uppdateras enligt stadens modell. När klassningen är klar bör en riskanalys genomföras för att bedöma risk och sårbarheter. Utifrån riskanalys bör tekniska och

organisatoriska åtgärder implementeras, exempelvis åtkomstkontroller, kryptering, loggning och utbildning av personal. Slutligen bör en rutin för kontinuerlig uppföljning och årlig revision etableras för att säkerställa att klassning och kompletterande skyddsåtgärder är aktuella och effektiva.

3.4 Konsekvensbedömningar (DPIA)

3.4.1 Sammanfattning

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

3.4.2 Syfte

DPIA avseende dataskydd syftar till att säkerställa att en planerad behandling av personuppgifter inte medför oskäliga eller lagstridiga risker för den enskildas rättigheter och friheter. Enligt art. 35.1 GDPR ska en sådan bedömning genomföras när ”*en typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter*”. DPIA utgör ett centralt verktyg för att i ett tidigt skede identifiera, analysera och hantera risker. Genom att införa DPIA som en integrerad del av verksamhetens dataskyddsarbete stärks förmågan att uppfylla skyldigheterna under GDPR.

3.4.3 Resultat

Under året har nämnden påbörjat arbetet med DPIA för vissa identifierade högriskbehandlingar i enlighet med art. 35 i GDPR. Bedömningarna är dock endast delvis genomförda och omfattar

med stor sannolikhet inte samtliga högriskbehandlingar. Dessutom är flera av de genomförda bedömningarna inte fullt uppdaterade vilket innebär att risker för de registrerades fri- och rättigheter inte är helt kartlagda.

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

Nämnden bör fortsätta arbetet med att säkerställa att en systematisk bedömning görs av om befintliga personuppgiftsbehandlingar kräver en DPIA i enlighet med art. 35 i GDPR och IMY:s vägledningar. För att uppnå detta bör förslagsvis bedömningen om DPIA-krav inkluderas i registerförteckningen så att det tydligt framgår om en DPIA har gjorts eller om den är nödvändig. Vidare bör förvaltningen se över sina processer för att hantera nya personuppgiftsbehandlingar, exempelvis vid projekt för att säkerställa att DPIA genomförs där så krävs.

Förvaltningen har därmed ett fortsatt behov av att uppdatera befintliga DPIA och säkerställa att nya bedömningar görs för alla relevanta behandlingar. Detta är avgörande för att identifiera och hantera risker för de registrerades fri- och rättigheter i ett tidigt skede och för att uppfylla kraven på ansvarsskyldighet enligt art. 5.2 GDPR.

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
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	-

3.5.2 Syfte

Enligt GDPR har den registrerade flera rättigheter inklusive rätt till tillgång, rättelse, radering, begränsning av behandling, dataportabilitet samt invändning mot behandling. Dessa rättigheter syftar till att ge den registrerade kontroll över sina personuppgifter och hur de behandlas.

Verksamheten är skyldig att hantera begäran om utövande av rättigheter *skyndsamt och utan onödigt dröjsmål. Begäran ska besvaras senast en (1) månad efter att ha mottagit begäran. (art.. 12, GDPR).* Vid behov kan tidsfristen förlängas med ytterligare sextio (60) dagar beroende på ärendets komplexitet och omfattning vilket då ska kommuniceras med den registrerade.

Bristande förmåga att hantera en begäran från en registrerad i enlighet med GDPR kan medföra betydande konsekvenser. En sådan brist riskerar att allvarligt minska allmänhetens förtroende för nämndens förmåga att säkerställa en rättssäker och transparent behandling av personuppgifter. Vidare kan detta leda till att IMY initierar tillsynsärenden vilket i sin tur kan resultera i förelägganden, administrativa sanktionsavgifter eller andra rättsliga påföljder. Det är därför av yttersta vikt att nämnden har etablerade rutiner och tillräckliga resurser för att uppfylla de registrerades rättigheter.

3.5.3 Resultat

I den mån det har varit möjligt att kartlägga antal begäran har inga förfrågningar inkommit till nämnden under 2025. Förvaltningen saknar fortfarande beslutade och formaliserade rutiner för hur en begäran om t.ex. registerutdrag ska hanteras. Nuvarande arbetssätt baseras på tidigare organisatoriska strukturer och utpekade funktioner vilket innebär att hanteringen inte är fullt systematiserad. Detta medför ett fortsatt behov av att fastställa rutiner som säkerställer en rättssäker, skyndsam och enhetlig process i enlighet med IMY:s vägledningar och art.12–15 i GDPR.

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

3.5.4 DSO ger råd och rekommendationer till PuA

Nämnden bör färdigställa och implementera lokala rutiner för hantering av registrerades rättigheter, särskilt rätten till tillgång (registerutdrag) i enlighet med GDPR och IMY:s vägledningar. Rutinerna ska säkerställa att begäran hanteras rättssäkert, skyndsamt och enhetligt. Utöver detta bör en rutin för uppföljning och kontroll etableras för att säkerställa att rutinerna efterlevs och att hanteringen sker i enlighet med gällande regelverk Detta är avgörande för att uppfylla kraven på transparens och ansvarsskyldighet enligt art. 5.2 GDPR.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Stadenövergripande kommunikation samt genom anställd
Hur många personuppgiftsincidenter har dokumenterats?	2
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	2
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Samtliga

3.6.2 Syfte

Syftet med hantering av personuppgiftsincidenter är att säkerställa att verksamheten snabbt, effektivt och på ett strukturerat sätt kan identifiera, bedöma, åtgärda och rapportera incidenter som innebär hög risk för de registrerades integritet. En personuppgiftsincident definieras enligt GDPR som en säkerhetsrelaterad händelse som leder till oavsiktligt eller otillåten förlust, ändring, spridning eller åtkomst av personuppgifter.

Genom att tillämpa rutiner för incidenthantering kan verksamheten begränsa negativa konsekvenser för berörda individer, säkerställa att nödvändiga tekniska och organisatoriska åtgärder vidtas och uppfylla skyldigheten att rapportera incidenter till IMY inom 72 timmar enligt art. 33 GDPR.

3.6.3 Resultat

Under 2025 har nämnden godkänt en lokal anvisning för hantering av informationssäkerhetsincidenter vilken även omfattar personuppgiftsincidenter. Anvisningen tydliggör ansvar och processer för rapportering och hantering av incidenter i enlighet

med GDPR. Detta utgör ett viktigt steg mot ett mer systematiskt arbete med informationssäkerhet och dataskydd inom förvaltningen.

Vidare har två personuppgiftsincidenter anmälts till IMY inom den tidsram som krävs enligt art. 33 i GDPR. Detta visar att förvaltningen har förmåga att identifiera och rapportera incidenter i tid. Samtidigt kvarstår behovet av att säkerställa att rutinerna implementeras fullt ut i verksamheten och att uppföljning sker regelbundet, förslagsvis genom medvetandegörande insatser såsom utbildning, intern kommunikation och återkommande informationsspridning

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

Nämnden bör säkerställa att rutiner för hantering av informationssäkerhetsincidenter och personuppgiftsincidenter implementeras fullt ut i verksamheten. Utöver dokumenterade rutiner bör medvetandegörande insatser genomföras, exempelvis utbildning och intern kommunikation, för att säkerställa att alla berörda medarbetare känner till och följer rutinerna.

Vidare bör en process för regelbunden uppföljning och kontroll etableras för att säkerställa att incidenter hanteras i enlighet med art. 33 i GDPR och IMY:s vägledningar. Detta är avgörande för att upprätthålla ansvarsskyldighet, minska risker och säkerställa att rapportering sker inom föreskriven tidsram.

4 Risker inom dataskydd

4.1 Sammanfattning

Uppbyggnaden av nämnden dataskyddsarbete har fortsatt under 2025. Inför kommande verksamhetsår bör nämnden prioritera tre centrala områden för att säkerställa ett systematiskt och riskbaserat dataskyddsarbete.

- **Uppdatering och kvalitetssäkring av registerförteckningen** för att uppfylla kraven på ansvarsskyldighet enligt art. 30 GDPR.
- **Full implementering av lokala anvisningar för informationssäkerhet och dataskydd** kompletterat med förslagsvis en kontinuitetsplan för drift och återhämtning vid incidenter.
- **Etablering av en process för regelbunden och systematisk uppföljning** samt höja medvetenhet om dataskydd i verksamheten genom förslagsvis generell/riktad utbildning, intern kommunikation och återkommande informationsinsatser.

Dessa åtgärder är avgörande för att minska risker, säkerställa rättssäker hantering av personuppgifter och uppfylla kraven i GDPR.

4.1 DSO ger råd och rekommendationer till PuA

DSO rekommenderar att nämnden upprättar en strukturerad och långsiktig plan för arbetet med dataskydd under kommande år. Syftet är att skapa en tydlig överblick över prioriteringar och säkerställa att resurser fördelas effektivt. En samlad bedömning bör göras utifrån nämndens övergripande mål och prioriteringar eftersom dataskydd enligt GDPR ska integreras i verksamhetens styrning och målstruktur. Detta möjliggör ett systematiskt, riskbaserat och proportionerligt arbetssätt i enlighet med principerna om inbyggt dataskydd och dataskydd som standard (artikel 25 GDPR) vilket är avgörande för att uppfylla kraven i förordningen och minimerar rättsliga och förtroendemässiga risker.

Nämnden bör under det kommande året fortsätta arbetet med att uppdatera och kvalitetssäkra registerförteckningen samt prioritera

implementeringen av lokala anvisningar för informationssäkerhet och dataskydd. Vidare bör en process för kontinuerlig och systematisk uppföljning och kontroll etableras för att säkerställa och följa upp arbetet med informationssäkerhet och dataskydd. Detta är avgörande för att upprätthålla ansvarsskyldighet, minska risker och säkerställa att behandling av personuppgifter sker i enlighet med GDPR och IMY:s vägledningar.

Utöver detta bör nämnden höja medvetenheten om informationssäkerhet och dataskydd i verksamheten genom riktade insatser såsom utbildning, intern kommunikation och återkommande informationsspridning. För att skapa struktur och kontinuitet i arbetet bör en ändamålsenlig årsplanering införas. Klassning av befintliga system och tjänster ska fortsätta genomföras vilket är en förutsättning för att kunna vidta lämpliga tekniska och organisatoriska skyddsåtgärder i enlighet med art. 32 GDPR.