Stockholms stad

Bilaga 6

GDPR Årsrapport

2025

Utbildningsnämnden

GDPR årsrapport
Januari 202X

Dnr: YYYY
Utgivningsdatum: 202X-MM-DD
Kontaktperson: Cecilia Adriano | DSO

1 Bakgrund

Dataskyddsförordningen (GDPR) har varit gällande lag i Sverige sedan den 25 maj 2018. Förordningens syfte är att skydda individers grundläggande rättigheter och friheter och särskilt rätten till skydd av personuppgifter. Förordningen har även till syfte att möjliggöra ett harmoniserat och rättssäkert utbyte av personuppgifter mellan medlemsstaterna inom EU/EES.

GDPR bygger på principerna ’laglighet, korrekthet och öppenhet’, ’ändamålsbegränsning’, ’uppgiftsminimering’, ’riktighet’, ’lagringsminimering’, ’integritet och konfidentialitet’ samt ’ansvarsskyldighet’ vilka tillsammans säkerställer att personuppgifter behandlas rättsenligt, ansvarsfullt och i enlighet med de mänskliga rättigheterna. Personuppgifter definieras här som all information som direkt eller indirekt kan hänföras till en identifierbar fysisk person. Begreppet är omfattande och inkluderar såväl uppenbara identifierare som mer sammansatta uppgifter.

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

Utbildningsnämnden (hädanefter nämnden) behandlar personuppgifter i betydande omfattning där uppgifter ofta är särskilt skyddsvärda. Dessa omfattar känsliga personuppgifter samt kan avse individer i beroendeställning. Detta medför att kraven på nämndens hantering av personuppgifter är särskilt höga både vad gäller rättslig efterlevnad och skydd av den enskildes integritet.

Årsrapporten utgör ett centralt underlag för att uppfylla den dokumentationsskyldighet som följer av gällande dataskyddsförordning och tjänar samtidigt som ett stöd för nämndens uppföljning och styrning av det systematiska arbetet med dataskydd samt bidrar till att öka förtroendet för hur personuppgifter hanteras.

Innehåll

2 Sammanfattning

Inom ramen för dataskyddsombudets (DSO) uppdrag lämnas härmed årsrapport för 2025 till nämnden. Rapporten omfattar tio (10) centrala områden där angivna kontrollpunkter bedömts utifrån definierade kriterier.

Inom nämnden råder en etablerad medvetenhet om den rättsliga skyldigheten att skydda personuppgifter i enlighet med GDPR. Föregående årsrapport visade på förbättrad regelefterlevnad inom flera områden jämfört med tidigare år. Det kvarstår dock ett tydligt behov av att vidareutveckla det systematiska dataskyddsarbetet för att uppnå en högre mognadsgrad och säkerställa att efterlevnaden motsvarar kraven i GDPR, särskilt avseende principerna om ansvarsskyldighet (art 5.2) och inbyggt dataskydd (art 25).

För att säkerställa en strukturerad och långsiktig kompetensutveckling rekommenderas att en strategisk utbildningsplan tas fram. En sådan plan bör utgå från nämndens behov, gällande regelverk och identifierade riskområden. Dessa insatser bör syfta till att:

- säkerställa att medarbetare får relevant och aktuell kunskap inom dataskydd och informationssäkerhet
- möjliggöra uppföljning och utvärdering
- skapa förutsättningar för kontinuitet och ansvarsfördelning i utbildningsarbetet

Planen bör fastställas årligen och inkludera både obligatoriska och behovsstyrda utbildningar samt tydliggöra målgrupper, ansvariga funktioner och tidpunkter för genomförande.

Utöver kompetensutveckling bör fortsatt fokus ligga på att:

- Samtliga IT-system omfattas av en uppdaterad informationsklassning och konsekvensbedömning (DPIA) enligt art 35 GDPR samt riskanalys med tillhörande handlingsplan och dokumenterade säkerhetsåtgärder. Dessa säkerhetsåtgärder bör genomföras i enlighet med principerna om inbyggt dataskydd och ansvarsskyldighet samt följas upp systematiskt.
- Etablera en övergripande rutin och process för regelbunden granskning av användarbehörigheter. Nämnden bör årligen genomföra en strukturerad kontroll av behörigheter i enlighet med principerna om integritet och konfidentialitet (art 5.1) samt ansvarsskyldighet. Arbetet bör dokumenteras och utföras i linje med IMY:s rekommendationer för systematiskt dataskyddsarbete och riskbaserat arbetssätt.

3 Rapporteringsområden

Denna årsrapport spänner över tio områden med ett antal krav inom respektive område som den personuppgiftsansvarige (hädanefter PuA) och i detta fall utbildningsnämnden, är skyldig att uppfylla enligt GDPR.

I det följande presenteras de områden som omfattas av granskningen tillsammans med de krav som är kopplade till respektive område. Därefter redovisas hur dessa krav har följts upp inom ramen för granskningen under 2025 inklusive en bedömning enligt färgkodad tabell (se nedan). En jämförelse med granskningen från 2024 samt en uppföljning av DSO:s rekommendationer från föregående år. En sammanfattning av nämndens efterlevnad per november 2025 ges, följt av DSO:s rekommendationer för det fortsatta dataskyddsarbetet inom respektive område.

Nedanstående färger och skala används för att bedöma efterlevnaden av respektive kontrollpunkt/krav:

	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 Registerförteckning

Enligt art 30 GDPR ska varje PuA föra en registerförteckning över nämndens behandlingar av personuppgifter. Denna ska bland annat innehålla uppgifter om syfte 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 vilket innebär att PuA ska kunna styrka att de grundläggande principerna för behandling av personuppgifter efterlevs.

3.1.1 Krav och uppföljning under granskning 2025

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2025	Resultat 2024
Nämndens registerförteckning är komplett	Granskning av informations-klassningsprotokoll och underlag från DPIA.		
Informationen i registerförteckningen är aktuell	Granskning av nämndens rutiner för uppdatering av registerförteckningen.		

3.1.2 Uppföljning av föregående års rekommendationer

Under 2025 har nämnden stärkt sitt arbete med att uppfylla kraven i GDPR. Bland annat genom att tillsätta en registeransvarig. Denna roll har haft i uppdrag att vidareutveckla och dokumentera rutiner och arbetssätt för upprättande, uppdatering och förvaltning av nämndens registerförteckning samt säkerställa systemets versionsuppdatering.

Arbetet har resulterat i förbättrad struktur och kontinuitet i dokumentationen av personuppgiftsbehandlingar. Flera delar av uppdraget har genomförts men vissa moment återstår eller har endast delvis fullgjorts. Det gäller särskilt den systematiska samordningen mellan registerförteckningen och övriga dataskyddsrelaterade processer såsom informationsklassningar och DPIA.

3.1.3 Nämndens efterlevnad av kraven

Systemstödet för registerförteckning har genomgått en uppdatering.

Registerförteckningen bedöms i dagsläget omfatta majoriteten av nämndens personuppgiftsbehandlingar. Rutiner för regelbunden översyn har etablerats med genomgångar planerade två gånger per år. Vid genomförda informationsklassningar och DPIA under 2025 har det framkommit att vissa personuppgiftsbehandlingar inte återfinns i den aktuella registerförteckningen. Detta indikerar att förteckningen inte fullt ut speglar samtliga behandlingar inom nämnden. I enlighet med principerna om ansvarsskyldighet och korrekthet finns det härmed ett fortsatt behov av att stärka kopplingen mellan registerförteckningen och övriga dataskyddsrelaterade processer. Detta är särskilt viktigt för att identifiera och dokumentera personuppgiftsbehandlingar som inte framgår av befintliga hanteringsanvisningar eller verksamhetsbeskrivningar.

3.1.4 DSO ger råd och rekommendationer till PuA

Nämnden har under 2025 fortsatt arbetet med registerförteckningen. För att säkerställa att registerförteckningen utgör ett heltäckande underlag för nämndens dataskyddsarbete rekommenderas att ytterligare rutiner och arbetssätt tas fram. Framöver rekommenderas att fokus fortsatt ligger på att slutföra detta arbete genom att bland annat:

- samordna registerförteckningen med informationsklassningsprocessen för att säkerställa att samtliga personuppgiftsbehandlingar identifieras och dokumenteras på ett systematiskt sätt i syfte att möjliggöra spårbarhet och kontinuitet över tid,
- etablera och dokumentera rutiner för systematisk uppföljning för att kunna styrka efterlevnad av dataskydd gällande registerförteckning,
- säkerställa att versionshantering är implementerade och att identifierade brister åtgärdas.

3.2 Grundläggande principer

De grundläggande principerna i GDPR (art 5) utgör kärnan i all behandling av personuppgifter inom EU/EES. Syftet med principerna är att säkerställa att personuppgifter behandlas på ett lagligt, korrekt och transparent sätt med respekt för individens rättigheter och integritet. Principerna ska vägleda både den praktiska hanteringen och den strategiska styrningen av

personuppgiftsbehandlingar och omfattar *laglighet, korrekthet och öppenhet*, *ändamålsbegränsning*, *dataminimering*, *riktighet*, *lagringsminimering*, *integritet och konfidentialitet* samt *ansvarsskyldighet*. Genom att tillämpa dessa principer säkerställs att personuppgifter hanteras på ett sätt som främjar rättssäkerhet, förtroende och efterlevnad av gällande dataskyddsregler.

3.2.1 Krav och uppföljning under granskning 2025

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2025	Resultat 2024
Kännedom om de grundläggande principer finns och dessa beaktas i nämndens arbete som rör personuppgifter	Granskning av stadens och nämndens rutiner vid inköp av nya tjänster, upphandling och projekt där personuppgifter förekommer.		
Medarbetare har fått grundläggande utbildning i dataskydd	Statistik över stadens obligatoriska e-utbildningar.		

3.2.2 Uppföljning av föregående års rekommendationer

Arbete pågår för att stärka stadens och nämndens styrdokument samt vägledningar så att de bland annat innehåller tydlig och konkret vägledning om den praktiska tillämpningen av de grundläggande dataskyddsprinciperna vid behandling av personuppgifter. Föregående år visade att befintliga dokument innehöll begränsad konkret vägledning vilket riskerar att påverka efterlevnaden av GDPR. Arbetet är ännu inte slutfört och det kvarstår ett betydande behov av ytterligare åtgärder för att uppfylla ansvarsskyldigheten.

Tidigare granskning har visat att det finns fortsatt behov av att öka efterlevnaden av kravet på genomförande av den obligatoriska utbildningen i dataskydd bland medarbetarna.

3.2.3 Nämndens efterlevnad av kraven

Per den 5 november visar genomförandestatus för den årliga obligatoriska e-utbildningen i dataskydd att en majoritet av medarbetarna ännu inte har uppfyllt kravet. 70 % av medarbetarna har inte genomfört utbildningen alls, 8 % har slutfört den, 6 % är pågående och 16 % har föregående år genomfört utbildningen men

inte i år. Jämfört med förra årets siffra på 72 % som inte gjort utbildningen alls är förbättringen marginell.
Detta indikerar ett betydande behov av ytterligare åtgärder för att säkerställa att samtliga medarbetare har genomgått utbildningen enligt stadens regelverk och i enlighet med art 24 och art 39 GDPR samt IMY:s rekommendationer om kontinuerlig utbildning.

Granskning under 2025 har visat att dataskyddsprinciper inte alltid integreras tillräckligt tidigt i nämndens rutiner vid till exempel inköp av nya tjänster, upphandling och projekt där personuppgifter förekommer vilket kan medföra risker för att personuppgiftsbehandlingar utformas på ett sätt som inte uppfyller kraven i GDPR. Detta kan i förlängningen leda till rättsliga brister, bristande regelefterlevnad och försvagad tillit till nämndens hantering av personuppgifter.

Informationsklassning genomförs i regel årligen och utgör ett viktigt verktyg för att bedöma informationssäkerhetskraven. Det är dock de grundläggande dataskyddsprinciperna som avgör om en personuppgiftsbehandling är förenlig med GDPR. För att säkerställa efterlevnad bör en bedömning av den planerade behandlingen i förhållande till dessa principer genomföras innan beslut fattas om systemets eller tjänstens utformning. Detta möjliggör att dataskydd integreras från början (Privacy by design) och att risker under GDPR kan hanteras systematiskt.

3.2.4 DSO ger råd och rekommendationer till PuA

DSO rekommenderar fortsatt arbete med att integrera dataskyddsprinciperna i relevanta beslutsprocesser. Syftet är att förstärka den interna styrningen och säkerställa en systematisk efterlevnad av tillämplig dataskyddslagstiftning. Detta innefattar:

- att dataskyddsprinciperna tydliggörs i styrande dokument såsom riktlinjer och vägledningar för upphandling och projekt och vid inköp av nya tjänster samt att rutiner etableras för att säkerställa att dataskyddsbedömningar initieras i ett tidigt skede av beslutsfattandet. En sådan struktur bidrar till ökad rättssäkerhet, förbättrad regelefterlevnad och ett mer robust dataskyddsarbete,
- att principen om inbyggt dataskydd beaktas vid upphandlingar och att kravställningen i övrigt utformas i enlighet med de grundläggande dataskyddsprinciperna. Detta innefattar att säkerhets- och integritetsaspekter integreras i kravspecifikationer, avtal och tekniska lösningar redan från början.

För att säkerställa en strukturerad och långsiktig kompetensutveckling inom nämnden rekommenderas att en strategisk utbildningsplan tas fram. En sådan plan bör utgå från nämndens behov, gällande regelverk och identifierade riskområden. Dessa insatser bör syfta till att:

- säkerställa att medarbetare får relevant och aktuell kunskap inom exempelvis dataskydd och informationssäkerhet,
- möjliggöra uppföljning och utvärdering av genomförda utbildningsinsatser,
- skapa förutsättningar för kontinuitet och ansvarsfördelning i utbildningsarbetet.

Planen bör fastställas årligen och inkludera både obligatoriska och behovsstyrda utbildningar samt tydliggöra målgrupper, ansvariga funktioner och tidpunkter för genomförande.

3.3 Personuppgiftsincidenter (PUI)

En PUI är en säkerhetsincident där personuppgifter oavsiktligt eller olagligt förstörs, förloras, ändras, röjs eller görs otillgängliga. Enligt GDPR ska sådana incidenter hanteras skyndsamt och strukturerat för att skydda de registrerades rättigheter och friheter samt för att uppfylla nämndens skyldigheter som att anmälan vissa typer av incidenter till Integritetsskyddsmyndigheten (IMY) inom 72 timmar. En effektiv hantering minskar risken för rättsliga konsekvenser och stärker förtroendet för nämndens dataskyddsarbete.

För att säkerställa en korrekt hantering av personuppgiftsincidenter krävs att medarbetare har tillräcklig kunskap för att kunna identifiera en incident och känna till hur den ska rapporteras i enlighet med gällande rutiner. Det är även nödvändigt att etablerade processer kommuniceras ut för att hantera bekräftade incidenter. En incident bör vidare leda till långsiktiga åtgärder som till exempel justering och översyn av rutiner och arbetssätt i syfte att förebygga framtida incidenter och stärka nämndens dataskyddsarbete.

3.3.1 Krav och uppföljning under granskning 2025

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2025	Resultat 2024
Medarbetare är informerade om definitionen och processen för	Granskning av nämndens rutiner för kommunicering av		

informationssäkerhets incidenter	anvisningen och antal incidenter per avdelning.		
Incidenterna har följts upp och föreslagna åtgärder har vidtagits.	Granskning av nämndens rutiner för uppföljning av incidenter.		

3.3.2 Uppföljning av föregående års rekommendationer

Som redogjorts i 2024 års GDPR årsrapport har anvisningar kommunicerats ut men alla avdelningar har med stor sannolikhet inte rapporterat in personuppgiftsincidenter. Anvisningar och mallar behöver fortsatt uppdaterats. , implementeras och förankras.

3.3.3 Nämndens efterlevnad av kraven

Nämnden har en beslutad anvisning för hantering av informationssäkerhetsincidenter som följs vid en konstaterad informationssäkerhetsincident. Då alla personuppgiftsincidenter klassas som informationssäkerhetsincidenter gäller anvisningen även för personuppgiftsincidenter.

För närvarande finns 32 diarieförda personuppgiftsincidenter varav fyra har anmälts till IMY i enlighet med art 33 GDPR. Det är sannolikt att ytterligare incidenter har inträffat utan att ha identifierats eller rapporterats vilket indikerar ett behov av att förstärka utbildningsinsatser och öka medvetenheten inom nämnden. En sådan förstärkning är avgörande för att säkerställa att incidenter upptäcks, rapporteras och hanteras i enlighet med gällande rätt.

3.3.4 DSO ger råd och rekommendationer till PuA

Nämnden uppvisar i stort en god förmåga att upptäcka och hantera personuppgiftsincidenter. Det kan dock inte uteslutas att samtliga avdelningar i nämnden har rapporterat incidenter under det gångna året. För att säkerställa en enhetlig och rättssäker hantering av personuppgiftsincidenter inom hela nämnden rekommenderas följande åtgärder:

- nämnden bör fortsatt säkerställa att relevanta delar av anvisningen för hantering av personuppgiftsincidenter

kommuniceras till samtliga medarbetare. Detta för att säkerställa att alla är införstådda med vad som utgör en personuppgiftsincident samt vilka rutiner som gäller för rapportering,

- en översyn och revidering av befintliga rapporteringsmallar och anvisningar genomföras i syfte att tydliggöra att varje rapporterad incident bör följas av minst en dokumenterad kortsiktig och långsiktig åtgärd för att förebygga liknande incidenter i framtiden. Det bör även framgå att incidenter ska följas upp systematiskt för att identifiera och införa relevanta förbättringsåtgärder.

3.4 Konsekvensbedömningar (DPIA)

En DPIA avseende dataskydd är ett krav när en planerad personuppgiftsbehandling sannolikt medför en hög risk för fysiska personers rättigheter och friheter. Syftet med en DPIA är att i ett tidigt skede identifiera, analysera och hantera potentiella risker kopplade till integritet och informationssäkerhet samt att säkerställa att lämpliga tekniska och organisatoriska skyddsåtgärder vidtas innan behandlingen inleds.

Genom att etablera en strukturerad och integrerad DPIA-process kan nämnden säkerställa efterlevnad av GDPR och även stärka förtroendet hos de registrerade och minska risken för sanktioner från tillsynsmyndigheten. Vidare främjar det ett systematiskt förbättringsarbete inom informationssäkerhet. En väl genomförd DPIA utgör ett centralt verktyg för att säkerställa att personuppgiftsbehandling sker på ett rättssäkert, ansvarsfullt och ändamålsenligt sätt. Genom att identifiera och analysera potentiella risker för de registrerades rättigheter och friheter möjliggör DPIA en strukturerad bedömning av proportionalitet, nödvändighet och lämpliga skyddsåtgärder.

Enligt stadens fastställda rutiner ska GDPR krav integreras i informationsklassningsprocessen. Processen omfattar momenten informationsklassning, handlingsplan, riskanalys samt – i de fall det är obligatoriskt – en DPIA.
Dataskyddskraven ska i huvudsak hanteras inom ramen för en handlingsplan. För behandlingar som sannolikt medför en hög risk för fysiska personers rättigheter och friheter ska en DPIA genomföras innan behandlingen påbörjas.
Ur dataskyddsperspektiv leder en informationsklassning till att personuppgifter skyddas genom att säkerhetsnivåer fastställs men själva klassningen tar inte ställning till om

personuppgiftsbehandlingen överhuvudtaget är tillåten enligt GDPR:s grundläggande principer och rättsliga grund (art 6). Informationsklassning är dessutom enbart det första steget i processen och bör följas av faktiska tekniska och organisatoriska säkerhetsåtgärder som säkerställer att de krav som följer av DPIA tas om hand och uppfylls.

3.4.1 Krav och uppföljning under granskning 2025

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2025	Resultat 2024
Nämndens registerförteckning är komplett	Granskning av nämndens dokumentation av konsekvensbedömningar.		
Rutiner för att säkerställa att DPIA görs, där så krävs, för framtida personuppgifts-behandlingar finns.	Granskning av nämndens rutiner.		
Riskminimerande åtgärder från konsekvens-bedömningar har följts upp och genomförts	Stickprov av de konsekvensbedömningar som genomförts.		

3.4.2 Uppföljning av föregående års rekommendationer

Under 2025 har nämnden genomfört ett antal konsekvensbedömningar. Nämndens efterlevnad inom området har förbättrats vilket indikerar en ökad medvetenhet och systematik i hanteringen av personuppgiftsbehandlingar med hög risk.

Nämnden har arbetat med att se över och uppdatera styrdokument och riktlinjer inom informationssäkerhet och dataskydd, vilket är en återkommande åtgärd som genomförs årligen. Utöver detta pågår ett kontinuerligt utvecklingsarbete för att förbättra processer, rutiner och verktyg som används vid konsekvensbedömningar. Uppdateringar som gjorts under våren och har börjat implementeras under hösten.

Det kvarstår dock ett fortsatt behov av betydande insatser för att fullt ut uppfylla de krav som ställs på konsekvensbedömningar. Detta innefattar bland annat att säkerställa att bedömningar initieras i rätt skede, att dokumentationen är tillräckligt detaljerad samt att

riskreducerande åtgärder identifieras och implementeras på ett strukturerat sätt.

3.4.3 Nämndens efterlevnad av kraven

Under 2025 har flera konsekvensbedömningar genomförts, bland annat inom ramen för upphandling. Samtidigt kvarstår behovet av att genomföra en övergripande genomgång av samtliga befintliga personuppgiftsbehandlingar i syfte att säkerställa att konsekvensbedömningar har genomförts i de fall där detta krävs.

Enligt vägledning från IMY bör en betydande andel av de personuppgiftsbehandlingar som förekommer inom nämndens verksamhetsområden omfattas av krav på DPIA. Detta innebär att ytterligare bedömningar kan komma att behöva initieras för att uppnå hög efterlevnad och stärka skyddet för den registrerades rättigheter och friheter.

Vidare saknas etablerade rutiner och processer för att säkerställa att framtida personuppgiftsbehandlingar genomgår DPIA med undantag för bland annat behandlingar som avser kamerabevakning. Även om ansvarsfördelning för konsekvensbedömningar anges i den lokala anvisningen för informationssäkerhet samt i stadens styrdokument är ansvarsförhållandena inte tillräckligt tydliga och styrdokumenten är ännu inte fullt implementerade i ordinarie arbete.

Vad gäller uppföljning av identifierade risker i samband med genomförda DPIA är det i dagsläget oklart vem som bär ansvar för att säkerställa att riskreducerande åtgärder vidtas. Uppföljningen har därför endast skett i begränsad omfattning, huvudsakligen genom enskilda medarbetares initiativ.

3.4.4 DSO ger råd och rekommendationer till PuA

Eftersom informationsklassningens alla steg inte har genomförts har förvaltningen inte aktivt arbetat med de åtgärder som ska följa en DPIA.

Mot bakgrund av den omfattande hanteringen av känsliga och särskilt skyddsvärda personuppgifter inom nämnden är det högst sannolikt att kriterierna för att genomföra en DPIA är uppfyllda för flertalet av de personuppgiftsbehandlingar som förekommer. Tidigare har utbildningsförvaltningen begränsat arbetet till att genomföra en informationsklassning, Det konstateras att DPIA inte tillämpas systematiskt inom nämnden vilket innebär risk för bristande regelefterlevnad. I flera fall har en riskanalys genomförts, men handlingsplan och DPIA har inte alltid upprättats.

För att säkerställa att DPIA genomförs i enlighet med lagkrav och praxis rekommenderas följande:

- fortsatt identifiera personuppgiftsbehandlingar och genomföra en systematisk kartläggning av samtliga personuppgiftsbehandlingar för att identifiera vilka som omfattas av DPIA-krav. Detta arbete bör ske i samverkan mellan aktuella funktioner,
- genomföra/upprätta DPIA för varje behandling som bedöms kunna medföra hög risk. Bedömningen ska dokumenteras och inkludera en analys av risker, proportionalitet, tekniska och organisatoriska skyddsåtgärder samt en plan för att mitigera risker.

3.5 Personuppgiftsbiträde (PuB) roller och ansvar

Enligt art 28 GDPR är ett personuppgiftsbiträde (nedan PuB) en fysisk eller juridisk person som behandlar personuppgifter för PuA:s räkning och endast enligt dokumenterade instruktioner. PuB får inte använda personuppgifterna för egna eller andra ändamål och ska vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder (art 32).

Förhållandet ska regleras genom ett skriftligt avtal som anger behandlingsändamål, säkerhetskrav, regler för biträden samt skyldighet att bistå PuA vid uppfyllande av registrerades rättigheter och incidenthantering. Det yttersta ansvaret för laglig behandling ligger hos PuA dock har biträdet egna skyldigheter och kan hållas ansvarigt vid bristande efterlevnad.

Varje nämnd och styrelse inom staden är var för sig PuA för personuppgiftsbehandlingar i den egna verksamheten. Det kan uppstå ett *internt PuB-förhållande* när en nämnd/styrelse inom staden behandlar personuppgifter för en annan nämnds/styrelses räkning. Detta regleras inom staden genom en *stadenintern instruktion.*

3.5.1 Krav och uppföljning under granskning 2025

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2025	Resultat 2024
Externa parter/leverantörer har kartlagts och en bedömning ifall parten/leverantören är personuppgiftsbiträde/gemensamt PuA är gjord	Granskning av nämndens rutiner vid upphandlingar, inköp av tjänster och samarbetsprojekt.		

Personuppgiftsbiträdesavtal har tecknats med personuppgiftsbiträden	Granskning av information i registerförteckningen.		
Personuppgiftsbiträdesavtal följs upp	Granskning av nämndens rutiner för uppföljning av incidenter.		

3.5.2 Uppföljning av föregående års rekommendationer

Nämnden har etablerade rutiner för att säkerställa att personuppgiftsbiträdesavtal (PUB-avtal) tecknas vid upphandlingar och inköp av tjänster. Innan ett PUB-avtal ingås genomförs en granskning av biträdet och den aktuella tjänsten utifrån informationssäkerhetskrav och eventuella tredjelandsöverföringar (art 28). Nämnden har rutiner för att säkerställa att personuppgiftsbiträdesavtal tecknas där så krävs men att uppföljning av dessa avtal inte sker systematiskt.

3.5.3 Nämndens efterlevnad

Nämnden har etablerade rutiner för att säkerställa att PUB-avtal tecknas vid upphandlingar och inköp av tjänster. Arbetet med att upprätta stadenintern instruktion för att reglera situationer där ett internt personuppgiftsbiträdesförhållande uppstår har påbörjats.
I dagsläget sker ingen särskild uppföljning av PUB-avtal även om dataskyddsfrågor kan behandlas inom ramen för annan avtalsuppföljning. Det kvarstår därför fortsatt behov av att utveckla strukturerade rutiner för uppföljning av PUB-avtal och biträdets hantering av personuppgifter.

3.5.4 Rekommendationer till PuA

Det finns fortsatt ett behov av att utveckla och stärka rutiner samt införa en systematisk uppföljning för att säkerställa ansvarsskyldighet vid hantering av PUB-avtal liksom att upprätthålla en enhetlig, skyndsam och konsekvent hantering av de registrerades rättigheter. DSO rekommenderar att fortsatt arbeta med att:

- införa en systematisk uppföljning av PUB-avtal genom att upprätta och implementera en dokumenterad rutin för regelbunden kontroll av att PuB följer avtalsvillkor och dataskyddskrav. Uppföljningen bör kopplas till internkontroll samt riskhantering,
- förankra och integrera rutiner och hantering av de registrerades rättigheter i ordinarie processer. För att

säkerställa enhetlig och skyndsam hantering bör riktad utbildning genomföras för berörda medarbetare,
- dokumentera och styrka ansvarsskyldigheten för att visa efterlevnad av GDPR genom att riktlinjer/styrdokument och registerförteckning uppdateras och används som kontrollverktyg. Till exempel genom standardiserade processer, fastställda krav och ansvar, verifiering av fullständighet/riktighet, riskanalyser och handlingsplan samt kontroll och ev. rapportering.

3.6 Tredjelandsöverföring

Överföring av personuppgifter till tredjeland innebär att personuppgifter görs tillgängliga för en mottagare utanför EU/EES där GDPR:s skyddsnivå inte gäller. Sådana överföringar är endast tillåtna enligt bestämmelserna i kapitel V GDPR. Det innefattar att det föreligger ett beslut om adekvat skyddsnivå enligt art 45, om lämpliga skyddsåtgärder ska har införts i enlighet med art 46 (ex. standardavtalsklausuler (SCC) eller bindande företagsbestämmelser (BCR) eller enligt undantag i art 49.

Innan en överföring sker bör nämnden genomföra en *Transfer Impact Assessment (TIA)* för att bedöma mottagarlandets rättsliga ramar och identifiera risker som kan påverka skyddet för personuppgifter. Bedömningen bör säkerställa att en väsentligen likvärdig skyddsnivå kan upprätthållas genom kompletterande tekniska och organisatoriska åtgärder. Överföringsmekanismen ska dokumenteras och den registrerade bör informeras om överföringen. Syftet med dessa krav är att säkerställa att den registrerades fri- och rättigheter inte förlorar sitt skydd vid behandling utanför EU/EES.

3.6.1 Krav och uppföljning under granskning 2025

Fråga/kontroll	Svar	Resultat 2025	Resultat 2024
Rutiner för att kontrollerat om personuppgifter överförs till tredje land (ett land utanför EU/ESS) finns.	Granskning av nämndens rutiner för tredjelandsöverföring		
Om uppgifter överförs till tredjeland har lagligheten säkerställts.	Granskning av nämndens rutiner vid tredjelandsöverföring		

3.6.2 Uppföljning av föregående års rekommendationer

Nämnden tillämpar en restriktiv hållning avseende överföring till tredjeland med ett ställningstagande som innebär att överföring till USA är tillåten under förutsättning att det amerikanska bolaget är anslutet till *EU–US Data Privacy Framework (DPF)* vilket utgör ett beslut om adekvat skyddsnivå enligt art 45 GDPR.

Vid upphandlingar och inköp av tjänster, vilket även framgår av nämndens mall för personuppgiftsbiträdesavtal, är tredjelandsöverföring som huvudregel inte tillåten. Om ett anlitande av leverantör ändå medför tredjelandsöverföring genomför nämnden en granskning av överföringens laglighet.

3.6.3 Nämndens efterlevnad av kraven

Under året har nämnden fortsatt tillämpat en restriktiv hållning avseende tredjelandsöverföringar där man genomfört bedömningar av laglighet i varje enskilt fall. TIA har utförts vid enstaka tillfällen med fokus på att säkerställa att överföringar sker lagenligt. För att ytterligare stärka rättssäkerheten bör bedömningarna utgå ifrån hela kapitel V GDPR där krav på TIA är inkluderat men också en bedömning om behovet av kompletterande tekniska och organisatoriska skyddsåtgärder.

3.6.4 DSO ger råd och rekommendationer till PuA

Nämnden har fortsatt att tillämpa en restriktiv hållning avseende tredjelandsöverföring men bedöms bli svår att upprätthållas fullt ut på längre sikt då nämnden i dagsläget har fler tredjelandsöverföringar jämfört med förra året. Därför rekommenderas att:

- nämnden kartlägger samtliga tredjelandsöverföringar i tjänster där nämndens personuppgiftsbiträdesavtal inte gäller och där leverantören enligt avtalsvillkoren har möjlighet att överföra personuppgifter,
- krav på TIA och bedömning av behov på kompletterande tekniska och organisatoriska skyddsåtgärder görs och förslagsvis integreras i upphandlingsprocessen samt i mallar för PUB-avtal,
- det är även av stor vikt att berörda funktioner inom nämnden får utbildning i GDPR:s ramverk för tredjelandsöverföring och praktisk tillämpning av TIA.
- rutiner för tredjelandsöverföringar följs upp och revideras regelbundet för att säkerställa att skyddsnivån bibehålls och att nya rättsliga krav beaktas.

3.7 Arkivering och gallring (lagringsminimering)

Lagringsminimering är en grundläggande princip i GDPR och innebär att personuppgifter endast får behandlas så länge de är nödvändiga för det ändamål de samlades in för. Myndigheter ska följa framtagna hanteringsanvisningar som anger om information ska gallras eller bevaras. Personuppgifter som inte ingår i allmänna handlingar ska rensas när de inte längre behövs. Att följa principen minskar inte bara risken för otillåten behandling utan minimerar även direkta och följdkonsekvenser vid intrång eller incidenter eftersom färre uppgifter finns kvar i systemen.

Nämnden ansvarar för sin arkiv- och informationshantering. Den information som skapas och hanteras inom offentlig verksamhet regleras av lagstiftning som ska säkerställa att informationen är ordnad, tillgänglig och sökbar samt att den bevaras så att alla ska kunna ta del av den.

Informationsflödet i nämnden bör styras och planeras. Som styrdokument för hanteringen av information används hanteringsanvisningar. I hanteringsanvisningarna anges de typer av handlingar och information som uppstår i nämnden och hur det bör hanteras, till exempel vilken information som ska bevaras långsiktig och vilken som ska gallras.

För att uppnå en ändamålsenlig och lagstadgad hantering av information bör nämnden säkerställa att principen om lagringsminimering tillämpas i alla delar av informationshanteringen. Detta innebär att personuppgifter (och andra handlingar) endast bör bevaras så länge de är nödvändiga för det ändamål de samlades in för eller för att uppfylla rättsliga förpliktelser. När personuppgifter inte längre behövs bör gallring ske i enlighet med fastställda bevarande- och gallringsrutiner. Samtidigt måste kraven i arkivlagen (1990:782) beaktas som anger att myndigheters arkiv ska bevaras, hållas ordnade och vårdas för att tillgodose rätten att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltning samt forskningsbehov. Gallring får endast ske med stöd i lag, förordning eller föreskrift vilket innebär att dokumentation av gallringsbeslut är avgörande.

3.7.1 Krav och uppföljning under granskning 2025

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2025	Resultat 2024
Hanteringsanvisningarna är upprättade och uppdaterade.	Granskning av nämndens rutiner för uppdatering och upprättande av hanteringsanvisningar.		
Arkivering och gallring genomförs enligt hanteringsanvisningen.	Stickprov av arkiverings- och gallringsrutiner i nämndens centrala system.		

3.7.2 Uppföljning av föregående års rekommendationer

Nämnden har etablerade rutiner för att säkerställa att lokala hanteringsanvisningar hålls uppdaterade. De tidigare rekommendationerna är fortgående eftersom implementering kräver ett omfattande och förvaltnings-/avdelningsövergripande arbete. Komplexiteten beror bland annat på att flera centrala system saknar inbyggda funktioner för gallring och arkivering, att arbetet måste samordnas med processer för upphandling, drift och avveckling samt att juridiska krav enligt arkivlagen (1990:782), offentlighets- och sekretesslagen (2009:400) och GDPR måste beaktas. Dessutom krävs tekniska lösningar som säkerställer att bevarande- och gallringsrutiner kan omsättas i praktiken vilket förutsätter samarbete mellan leverantör, nämnden, verksamhet och aktuella funktioner som till exempel arkiv.

Införandet av dessa funktioner är tidigare inplanerade och kommer att prioriteras i det fortsatta arbetet för att uppnå en ändamålsenlig och lagstadgad hantering av information.

3.7.3 Nämndens efterlevnad av kraven

I nämndens arkiv förvaras bland annat protokoll, diarieförda handlingar, projekthandlingar och informationsmaterial. Arkivet innehåller även journaler som exempelvis skolhälsovårdsjournaler vilka omfattas av sekretess enligt (OSL) offentlighets- och sekretesslagen (2009:400). Arkivfunktionen ansvarar för att upprätta arkivförteckningar, hanteringsanvisningar och instruktioner samt för att utreda och verkställa gallring i enlighet med Stadens arkivregler (KFs 2015:27).

Nämndens skolor är egna arkivbildare vilket innebär att de förvarar sina egna handlingar och har ansvar för sina respektive arkiv. Arkiv från nedlagda skolor förvaras på Stadsarkivet som är arkivmyndighet.

Flera av nämndens systemstöd saknar i dagsläget tekniska funktioner för arkivering och gallring. Dessa aspekter beaktas inte heller tillräckligt tidigt vid utvecklingen av system vilket medför att personuppgifter lagras längre än nödvändigt. Detta strider mot principen om lagringsminimering och innebär dessutom ökad risk ur informationssäkerhetsperspektiv eftersom konsekvenserna vid ett dataintrång blir mer omfattande.

3.7.4 DSO ger råd och rekommendationer till PuA

För att säkerställa en korrekt tillämpning bör fortsatt arbete med rutiner för livscykelhantering av information integreras från upphandling och införande till drift och avveckling. Tekniska funktioner för gallring och arkivering bör finnas i samtliga IT-system och införandet av dessa funktioner bör prioriteras med början i de centrala verksamhetskritiska systemen.

Det är också viktigt att arkivfunktionen kontinuerligt följer upp att hanteringsanvisningar är aktuella och att gallring verkställs i praktiken. Nämndens skolor som är egna arkivbildare bör följa stadens arkivregler (Kfs 2015:27) och säkerställa att handlingar som inte längre behövs gallras i enlighet med beslutade frister och handlingar som ska bevaras överförs till Stadsarkivet.

Genom att kombinera lagringsminimeringsprincipen med arkivlagens krav skapas en balans mellan dataskydd och offentlighetsprincipen vilket är centralt för en rättssäker och effektiv informationshantering.

För att kunna följa principen om lagringsminimering är det viktigt att säkerställa att personuppgifter rensas, gallras och arkiveras. Fokus bör omfatta både nämndens ansvar för informationshantering och det ansvar som åligger de aktörer som utvecklar och tillhandahåller systemstöden. Därför rekommenderas att:

- hanteringsanvisningar kompletteras med rutiner för rensning, gallring och arkivering av både allmänna handlingar, information och personuppgifter (detta inkluderar G-mappar, Teams, Outlook m.fl.)
  Revidering bör ske i samråd med ARF-enheten för att säkerställa förenlighet med principen om lagringsminimering, den registrerades rätt till radering och arkivlagen,

- systemstöd bör utvecklas så att systematisk arkivering och gallring är möjlig. Ett systemstöd bör inte kunna införas utan att det finns en plan för hur information tas om hand under hela dess livscykel.

3.8 Registrerades rättigheter

De registrerades rättigheter är grundläggande för en rättssäker och transparent behandling. Varje registrerad har rätt till tydlig information om ändamål, rättslig grund och kontaktuppgifter till PuA samt rätt att begära tillgång, rättelse, begränsning, radering och dataportabilitet. De kan invända mot behandling som sker med stöd av berättigat intresse eller för direktmarknadsföring (art 21).
Vid samtyckesbaserad behandling kan samtycke återkallas när som helst. Undantag från radering gäller bland annat vid rättslig förpliktelse eller uppgift av allmänt intresse. Slutligen har den registrerade rätt att inge klagomål till IMY.
Rutiner för att hantera dessa rättigheter bör vara tydliga, enhetliga och lättillgängliga.

3.8.1 Krav och uppföljning under granskning 2025

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2025	Resultat 2024
Rutiner för utlämnade av registerutdrag (rätten till tillgång) finns, utdraget lämnas ut enligt kraven i GDPR och inom den lagstadgade tidsramen	Granskning av nämndens rutiner för registerutdrag och hanterade registerutdrag under året.		
Enskilda har informerats om hur deras personuppgifter hanteras (rätt till information)	Granskning av nämndens informationstexter till registrerade.		
Rutiner för att hantera övriga rättigheter, dvs. begäran om radering, rättelse, invändning och begränsning (samt dataportabilitet, om tillämplig) finns och	Granskning av nämndens rutiner och stickprov av hanterade begäran under året.		

begäran hanteras inom den lagstadgade tidsramen			

3.8.2 Uppföljning av föregående års rekommendationer

Informationen till de registrerade bedömdes vara delvis adekvat men behöver uppdateras och kompletteras för att fullt ut uppfylla kraven i GDPR och då främst med hänsyn till personuppgiftsbehandlingar.

Processen för att hantera registrerades rättigheter har uppdaterats och implementerats inom Samordningsfunktionen för informationssäkerhet och dataskydd.

3.8.3 Nämndens efterlevnad av kraven

Nämnden har fortsatt vidtagit åtgärder för att effektivisera processen för registerutdrag bland annat genom att uppdatera processbeskrivningen, utbilda personuppgiftskoordinatorer och övriga berörda samt genomfört arbetet med framtagande av standardsvarsmallar.

Begränsningar i systemstöden kvarstår dock.

I dagsläget uppfylls inte principen om öppenhet och informationsskyldighet fullt ut samt att ansvarsfördelningen för informationsplikt är fortsatt otydlig. Arbete med att uppdatera och komplettera information är initierade och fortgående.

3.8.4 DSO ger råd och rekommendationer till PuA

För att säkerställa efterlevnad av GDPR:s krav på transparens, informationsskyldighet och rätt till registerutdrag behöver nämnden vidta förbättringsåtgärder. Nuvarande rutiner brister i tydlighet och ansvarsfördelning samt att systembegränsningar påverkar processen ofördelaktigt. Följande åtgärder rekommenderas därför:

- förtydliga ansvar och samordning för informationsplikten som till exempel vilken enhet/avdelning som är ansvarig för extern dataskyddsinformation (ex. webb) och vilken enhet/avdelning som bör ta fram mallar/vägledningar för enhetlig och begriplig information (på ex webb, utskick till extern part som vårdnadshavare),
- säkerställ att informationskraven uppfylls genom bland annat översyn av den information som lämnas till registrerade,

- stärk processen för registerutdrag genom att säkerställa systematisk uppföljning av utlämnande samt övervaka att systemleverantörer genomför nödvändiga anpassningar för korrekta och effektiva utdrag.

3.9 Känsliga och integritetskänsliga personuppgifter

Myndigheter får generellt behandla känsliga personuppgifter när behandlingen är nödvändig med hänsyn till ett allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet. Detta gäller under följande förutsättningar:

- Uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag.
- Behandlingen är nödvändig för handläggningen av ett ärende.
- Behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse.

För personuppgifter som behandlas inom hälso- och sjukvården, exempelvis inom elevhälsan gäller särskild reglering i patientdatalagen (2008:355).

IMY framhåller att känsliga personuppgifter omfattar uppgifter om etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, facklig tillhörighet, hälsa, sexualliv eller sexuell läggning samt genetiska och biometriska uppgifter som används för identifiering. Utöver dessa kategorier finns personuppgifter som kan betecknas som integritetskänsliga, exempelvis uppgifter om ekonomiska förhållanden, sociala förhållanden, värderande uppgifter (t.ex. från utvecklingssamtal) eller personnummer. Dessa uppgifter omfattas inte av art 9 och kräver således inget särskilt undantag för att behandlas men deras karaktär medför att de bör skyddas med förstärkta säkerhetsåtgärder.

Behandling av känsliga och integritetskänsliga personuppgifter får endast ske enligt fastställda rutiner och i system eller lagringsytor som uppfyller högt ställda krav på konfidentialitet, integritet och tillgänglighet. Detta innefattar tekniska och organisatoriska åtgärder såsom åtkomstkontroller, kryptering och loggning i enlighet med principerna om inbyggt dataskydd och dataskydd som standard. Vidare ska DPIA genomföras när behandlingarna kan medföra hög risk för den personliga integriteten.

3.9.1 Krav och uppföljning under granskning 2025

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2025	Resultat 2024
Om känsliga personuppgifter hanteras, har ett undantag enligt art 9 GDPR säkerställts.	Stickprov av personuppgiftsbehandlingar från registerförteckningen.		
Rutiner för hur och var känsliga och integritetskänsliga personuppgifter får hanteras finns och har kommunicerats till medarbetare	Granskning av nämndens rutiner och kommunicering av dessa.		

3.9.2 Uppföljning av föregående års rekommendationer

Nämnden har beslutade anvisningar för hantering av personuppgifter i kommunikationsverktyg och digitala dokument. För vissa IT-tjänster finns särskilda instruktioner om vilka typer av uppgifter som får hanteras. Rutiner och anvisningar kommuniceras via samordningsfunktionen för dataskydd och informationssäkerhet samt med grundskolornas personuppgiftskoordinatorer.

3.9.3 Nämndens efterlevnad av kraven

Trots befintliga rutiner uppstår frågor och osäkerhet om hur olika typer av personuppgifter får hanteras. Detta indikerar att information och eller rutiner inte är tillräckligt tydliga avseende vilken typ av personuppgift som får hanteras eller kommuniceras i respektive tjänst eller system. Det finns därför behov av att förtydliga riktlinjer, stödja i implementering och komplettera styrning för att säkerställa en enhetlig och korrekt tillämpning.

3.9.4 DSO ger råd och rekommendationer till PuA

Till viss del råder det fortfarande osäkerhet/otydlighet kring hantering av känsliga och integritetskänsliga personuppgifter som medför ökad risk för otillbörlig behandling av känsliga personuppgifter. För att minska osäkerheten och stärka efterlevnad av GDPR bör nämnden fortsätta arbete med:

- att uppdatera och komplettera vägledningar,

- intern kommunikation och utbildning (en del av utbildningsplanen beskriven ovan) bör förstärkas genom riktade insatser för medarbetare om hantering av känsliga personuppgifter med praktiska exempel och med IMY:s vägledning som grund,
- vidare bör systematisk kontroll och uppföljning införas genom regelbundna stickprovskontroller av personuppgiftsbehandling i system och dokument inklusive dokumentation på avvikelser och korrigerande åtgärder och harmoniseras med internkontrollarbetet.

3.10 Informationssäkerhet

Informationssäkerhet utgör en grundpelare för att uppfylla GDPR. Den omfattar organisatoriska och tekniska åtgärder som syftar till att säkerställa konfidentialitet, integritet och tillgänglighet för personuppgifter. Ett systematiskt informationssäkerhetsarbete minskar risken för obehörig åtkomst, förlust eller manipulation av data och är avgörande för en rättssäker och transparent behandling.

Nämndens riktlinjer kräver att alla informationstillgångar klassas med stöd av SKR:s verktyg KLASSA för att kunna välja rätt skyddsåtgärder. Klassning är idag en förutsättning för att välja adekvata skyddsåtgärder men i sig uppfyller den inte GDPR. När skyddsvärdet är fastställt måste tekniska och organisatoriska åtgärder vidtas för att säkerställa konfidentialitet, integritet och tillgänglighet. En central åtgärd är behörighetshantering som bör omfatta både teknisk åtkomststyrning och rutiner för att hålla behörigheter aktuella. Detta är särskilt viktigt då nämnden behandlar stora mängder personuppgifter inklusive känsliga uppgifter.

3.10.1 Krav och uppföljning under granskning 2025

Kontrollpunkt/krav	Metod för uppföljning	Resultat 2025	Resultat 2024
Informationstillgångar har informationsklassats	Granskning av genomförda informationsklassningar och information från registerförteckningen.		
Informationsklassningen inkluderar även tekniska	Stickprov av genomförda informationsklassningar.		

och organisatoriska säkerhetsåtgärder för att skydda personuppgifter			
Tillgång till personuppgifter har behörighetsstyrts enligt principen lägsta behörighet och behörigheterna följs upp regelbundet	Stickprov av behörighetsstruktur och rutiner för behörighetsadministration i nämndens centrala system.		

3.10.2 Uppföljning av föregående års rekommendationer

Nämnden har tidigare genomfört en översyn och uppdatering av styrdokument och riktlinjer avseende informationssäkerhet och dataskydd. Detta är en återkommande åtgärd som följer kraven på systematiskt och riskbaserat arbete. Utöver detta bedrivs ett kontinuerligt förbättringsarbete för att säkerställa att processer, rutiner och verktyg för informationsklassning, riskanalyser och DPIA. De uppdateringar som genomförts under året har påbörjat implementeras.

Nämnden arbetar även med att genomföra de åtgärder som identifierats tidigare, till exempel har arbetet med att ta fram en förvaltningsövergripande rutin för regelbunden granskning av användarbehörigheter påbörjats i syfte att säkerställa att åtkomst till information sker enligt behörighetsprincipen och att obehörig åtkomst förebyggs. Detta bidrar till att upprätthålla konfidentialitet, riktighet och tillgänglighet. Utöver detta har användarvillkor tagits fram för nyttjande av digitala enheter inom nämnden. Dessa villkor är utformade för att säkerställa att personuppgiftsbehandling sker i enlighet med GDPR och att informationssäkerhet upprätthålls.

3.10.3 Nämndens efterlevnad av kraven

Nämnden har fortsatt att initiera och genomföra identifierade åtgärder för informationssäkerhet och dataskydd. Arbetet är löpande och bör regelbundet förankras.

En årsplan har fastställts för år 2026 avseende samordningsfunktionen för informationssäkerhet och dataskydd. Planen syftar till att tydliggöra hur funktionen bör uppnå de fastställda målen och ge en översikt över planerade aktiviteter.

3.10.4 DSO ger råd och rekommendationer till PuA

Nämnden har under året visat engagemang och högt medvetande för att uppfylla kraven inom informationssäkerhet och dataskydd.

Genom strukturerade åtgärder, uppdaterade styrdokument och en tydlig årsplan för 2026 har grunden lagts för ett fortsatt systematiskt och riskbaserat arbete. För att ytterligare stärka efterlevnaden och skapa långsiktig hållbarhet föreslås följande rekommendationer:

- stärkt styrning och ansvarsskyldighet genom till exempel årlig förankring av styrdokument till identifierade målgrupper och upprätta/uppdatera korrekt dokumentation,
- inför en harmoniserad DPIA-process som konsekvent säkerställer identifiering och hantering av risker för de registrerade. Detta är avgörande för att undvika högriskbehandlingar utan adekvata skyddsåtgärder.
- formalisera behörighetsgranskning genom till exempel regelbunden granskning av användarbehörigheter, förebygga obehörig åtkomst och stärka informationssäkerhet.

4. Operativt arbete av dataskyddsombudets rekommendation

DSO rekommenderar att nämnden vidtar åtgärder för att förstärka det systematiska dataskyddsarbetet i enlighet med GDPR. Rekommendationen innefattar att en åtgärdsplan upprättas baserad på ledningens genomgång samt att en ansvarsplan tas fram som tydliggör ansvarsfördelningen för de olika kontrollpunkternas rekommendationer. Det föreslås att detta arbete görs inom samordningsfunktionen för informationssäkerhet och dataskydd i syfte att säkerställa en enhetlig och effektiv implementering av nämndens skyldigheter enligt art 24 och 39 GDPR.