Stockholms stad

Bilaga 5

GDPR Årsrapport

År 2024

Socialförvaltningen

GDPR årsrapport
December 2024

Dnr: SOF XXXXX/XX
Utgivningsdatum: 2024-12-17
Kontaktperson: Jonas Olsson

1 Bakgrund

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

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnd och bolagsstyrelse behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett Dataskyddsombud (”DSO”). DSO:n har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för nämnd och styrelse att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

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

Innehåll

2 Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport. Nedanstående tabell visar en sammanställning över de 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.

Av tabellen nedan framgår det att av dessa sex områden så är det ett område som har stora brister och det är konsekvensbedömningarna som behöver bli fler och tydligare kopplade till behandlingarna i registerförteckningen. Arbetet med registerförteckningen, som genomgår ett större förändringsarbete av såväl struktur som uppdatering av innehåll, har därmed flyttats ner från en ”orange” till ”gul” risk.

Inom området Tekniska och Organisatoriska åtgärder pågår arbete med informationsklassningar om än i lägre grad än tidigare år. Däremot är uppfyllandet av stadens obligatoriska e-utbildningar på en för låg nivå (50% av medarbetarna) för att passera utan anmärkning.

Övriga område är däremot utan större brister och bedöms leva upp till regelefterlevnad.

	Registerförteckning	Styrdokument	Tekniska och organisatoriska åtgärder	Konsekvensbedömningar	Individens rättigheter	Personuppgiftsincidenter
Allvarliga brister identifierade						
Brister identifierade som bedöms vara omfattande				X		
Brister identifierade som bör åtgärdas	X		X			
Inga brister av nämnvärd betydelse identifierade		X			X	X

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 eller bolagets 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?	345
Har nödvändiga uppdateringar gjorts?	Nej, men det är ett pågående arbete för att uppdatera flera års försummelse.
Bedöms registerförteckningen vara fullständig?	Nej, inte på den totala mängden men på de behandlingar som har tillkommit/ändats under året.
Har verksamheten lämpliga rutiner för registerföring?	Delvis, det har inletts ett arbete för en översyn.

3.1.2 Syfte

Det följer i klartext av dataskyddsförordningen (artikel 30) att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas, i fortsättningen kallat personuppgiftsbehandlingar, i verksamheten och dokumentera dem i en så kallad registerförteckning.

Förvaltningens registerförteckning återfinns i verktyget Draftit Privacy Records. När registerförteckningen är upprättad skapar den en intern synlighet och förståelse för personuppgiftsbehandlingar vilka finns och hur de hanteras. Registerförteckningen säkerställer att verksamheten beaktar att det ska finnas en laglig grund inom ramen för all personuppgiftsbehandling.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

Det finns idag 345 personuppgiftsbehandlingar registrerade i verktyget Draftit Privacy Records. Under året 2024 har 46 nya registreringar tillkommit och 43 äldre har ändrats.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Ett behandlingsregister över personuppgiftsbehandlingar behöver löpande ses över allt eftersom förutsättningarna hos en verksamhet

förändras. Att ha en korrekt och uppdaterad registerförteckning är nödvändigt.

Nedanstående tabell illustrerar att det gjordes ett stort arbete med registerförteckningen under 2019 men att det därefter under flera år har varit en betydligt lägre aktivitet. Tabellen visar också att det under 2024 har blivit ett trendbrott med en betydligt högre aktivitet i arbetet med registerförteckningen.

	Senast ändrat	
2024	89	26%
2023	20	7%
2022	16	5%
2021	22	7%
2020	41	14%
2019	201	67%

Dataskyddsombudet rekommenderar att verksamheten fortsatt löpande inventerar vilka personuppgiftsbehandlingar som utförs, då personuppgiftsbehandling är rörlig över tid på grund av exempelvis nya uppdrag och förändrade förutsättningar. Det är viktigt att behandlingsregistret kompletteras med personuppgiftsbehandlingar om/när verksamheten identifierar att en personuppgiftsbehandling inte finns i behandlingsregistret. Det underlättar och utgör underlag för det systematiska och löpande dataskyddsarbetet.

Bedömningen är att registerförteckningen idag inte är helt uppdaterad, men att det är på rätt väg och med fortsatt samma aktivitet som har visats under andra halvåret 2024 så bedöms registerförteckningen under 2025 kunna nå målet att vara en aktuell registerförteckning.

DSO bedömer hur fullständig registerförteckningen är

DSO bedömer att registerförteckningen i dagsläget inte är att anse som fullständig men med det nya gemensamma och nedbantade formuläret på plats så bedöms detta vara uppnåeligt under 2025.

Med den tidigare stora floran av frågeformulär och över 100 frågor att besvara i respektive formulär för att registrera en behandling var det en mycket svår uppgift att hålla registret relevant och uppdaterat med korrekt information.

Med det under hösten 2024 framtagna nya gemensamma formuläret med cirka 50 frågor bedöms möjligheten att hålla ett aktuellt register som goda.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Förvaltningen hade tidigare, av oklar anledning, väldigt många aktiva formulär. Ett formulär behövs för att kunna skapa registreringar och innehåller ett batteri av frågor som syftar till att skapa en noggrann bild av registret eller behandlingen. Här har det som tidigare nämnts gjorts ett stort arbete för att skapa ett gemensamt formulär med betydligt färre frågor att fylla i.

Föregående års påpekande i årsrapporten att behörigheterna och formuläranvändningen idag inte är helt optimal, med för många formulär och formuläradministratörer, har alltså setts över och är nu på väg att anpassas efter verksamhetens krav och behov.

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

Dataskyddsombudet bedömer att förvaltningen ännu inte har en optimal struktur avseende registerförteckningen men att pågående förändringsarbete med färre formulär och färre frågor per formulär är på rätt väg.

Registreringarna vilka registrerats i Drafit Privacy Records år 2024 i det nya formuläret har en betydande större ”ifyllandegrad” än tidigare år vilket tyder på att det utvecklingsarbete som startade under året är på rätt väg.

De brister som tidigare har påtalats och ännu finns kvar i förvaltningens registerförteckning behöver åtgärdas. Främst behöver gamla registreringar flyttas till det nya formuläret samt att strukturen för godkännande av behandlingar inte göras av samma person som har fyllt i formuläret.

3.2 Styrdokument

3.2.1 Sammanfattning

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

Området syftar till att PUA bedriver ett systematiskt dataskyddsarbete och styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar PUA till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna i fråga om hantering av 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. En röd tråd i dataskyddsförordningen är att viktiga arbetssätt och rutiner ska vara dokumenterade.

3.2.3 Resultat

På stadens intranät finns en egen flik för dataskyddsfrågor dit alla medarbetare har åtkomst. På fliken finns till exempel vägledande dokument inom incidentrapportering, mallar för upprättande av PUB-avtal med vägledning och instruktion, information och blanketter för samtycke, begäran om registerutdrag, rättelse och radering samt blanketter för risk- och konsekvensbedömning. Under fliken finns även generell information om dataskyddslagstiftning, kontaktuppgifter till Dataskyddsombudet, information om hur

dataskyddsorganisationen är uppbyggd, hur ansvarsfördelningen ser ut samt rollförteckning.

Finns lämplig styrande dokumentation på plats?
Ja

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet
Ja

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
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

3.2.5 DSO ger råd och rekommendationer till PUA

Fortsatt arbete krävs löpande i fråga om att tydliggöra information inom förvaltningen och påminna medarbetare i det dagliga arbetet. Blanketter och rutiner finns tillgängligt men fortsatt arbete om ansvarsfördelningen och fördelning av arbetsuppgifter behöver förankras inom hela förvaltningen löpande. Fortsatt informationsspridning bör även ske ut i verksamheterna avseende intranätet och relevanta styrdokument inom området.

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?	27 st personuppgiftsbehandlingar
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd ska verksamheten informationsklassa sin information.
Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA.
Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. En första kontrollpunkt måste därför vara om en informationsägare eller en informationsägarrepresentant med ansvar för klassning är identifierad i verksamheten.

3.3.3 Resultat

Informationsklassning har genomförts för 27 stycken personuppgiftsbehandlingar, och de är aktuella. Det är dock en marginell ökning från föregående år vilket indikerar ett mindre fokus på detta viktiga område. Notera dock att granskningen inte omfattat stickprovskontroller för att verifiera detta i vidare bemärkelse.
Det finns två e-utbildningar inom informationssäkerhet som är obligatoriska för alla medarbetare och dessa skall genomföras årligen för att hålla kunskaperna fräscha.

- Informationssäkerhet för medarbetare i staden
- Grundkurs i dataskydd

Under 2024 har knappt hälften av medarbetarna genomfört grundutbildning i dataskydd och lite mer än hälften utbildning i informationssäkerhet, vilket inte kan anses vara godkänt då det är obligatoriskt genomförandekrav.

Status	Grundutbildning i dataskydd	Informationssäkerhet för medarbetare i staden
Certifierad	439	481
Ej certifierad	519	516
Pågår	83	106
	1041	1103
Genomförandegrad	42%	56%

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

Kopplingen mellan klassning och registerförteckningen är inte tydlig och bör förbättras så att det i registerförteckningen går att se om det har genomförts en klassning.

DSO rekommenderar ledningsgruppen att föregå med gott exempel och visa vägen med att genomgå båda dessa obligatoriska utbildningar. Under 2024 har endast hälften av medlemmarna i Ledningsgruppen genomfört dessa utbildningar vilket skickar en tydlig signal till verksamheten att detta inte är så viktigt.

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?	Nej

3.4.2 Syfte

Syftet med risk- och konsekvensbedömningen är att förebygga risker innan de uppkommer, ta fram rutiner och åtgärder för att hantera eventuella risker och kunna visa att vi följer dataskyddsförordningens krav.

3.4.3 Resultat

Förvaltningen använder idag verktyget Draftit Privacy DPIA som förteckning för sina konsekvensbedömningar.

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

När förvaltningen överväger att börja behandla personuppgifter för nya syften eller vill börja använda ny teknik där personuppgifter behandlas, så krävs enligt artikel 35 i dataskyddsförordningen att en konsekvensbedömning avseende dataskydd, en så kallad DPIA, genomförs. Med verktyget Draftit Privacy DPIA kan verksamheten snabbt avgöra om det behöver göras en DPIA och att genomföra en när det väl behövs. Verktyget dokumenterar resultatet av varje bedömning, som skall kunna visas upp för tillsynsmyndigheten. Detta verktyg har dock använts mycket sparsamt under året (3-4 gånger) av ett fåtal personer.

Det finns även en möjlighet att ange risknivån i registerförteckningen från ingen risk till hög risk.

Tabellen på nästa sida visar att denna funktion inte används vilket indikerar att riskbedömningskulturen i förvaltningen måste bedömas som mycket låg.

Risknivå	#	
Ingen risk angiven	68	76%
Låg risk	14	16%
Medelhög risk	6	7%
Hög risk	1	1%
	89	

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?
Nej, då det finns en personuppgiftsbehandlingar i Draftit Privacy Records som har en risknivå Hög risk och sex som har Medelhög risk. Inga av dessa sju har en genomförd konsekvensbedömning i Draftit Privacy DPIA.

Är de genomförda konsekvensbedömningarna aktuella?
Det har under 2023 genomförts fyra stycken konsekvensbedömningar, vilket måste bedömas som mycket lågt.

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
Det är av stor vikt att samtliga personuppgiftsbehandlingar värderas utifrån risker innan dessa startas upp eller genomförs. I nuläget är bedömningen från Dataskyddsombudet att det saknas en koppling mellan gjorda personuppgiftsbehandlingar i Draftit Privacy Records och konsekvensbedömningar i Draftit Privacy DPIA.

Rekommendationen blir därför att kompetensen i allmänhet inom området risk måste höjas i organisationen och i synnerhet förmågan att konsekvent bedöma risknivån på personuppgiftsbehandlingarna och utifrån detta gå vidare med konsekvensbedömningar.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	11 förfrågningar om registerutdrag under året.
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Samtliga har fått svar inom 30 dagar

3.5.2 Syfte

Ett registerutdrag är en sammanställning över den registrerades personuppgifter som behandlas. Syftet med registerutdraget är att den registrerade ska få medvetenhet om att personuppgiftsbehandling sker och på vilken laglig grund.

Individen har även rätt att begära begränsning av sin personuppgiftsbehandling och att invända mot personuppgiftsbehandlingen.

När den personuppgiftsansvarige hanterar rättigheterna, ska informationen vara tydlig och i lättillgänglig form med användning av ett klart och tydligt språk.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

Förvaltningen har rutiner avseende registerbegäran från enskild. Samtliga inkomna begäran om registerutdrag har under året behandlats inom utsatt tid. Dataskyddsombudet hanterar administrationen kring inkomna begäran om registerutdrag. En blankett för begäran om registerutdrag finns tillgänglig för medborgare på stockholm.se.

Samtliga frågor och enskildas begäran om rättighet som har inkommit till Socialförvaltningen har hanterats inom föreskriven lagstadgad tidsram om trettio dagar.

3.5.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

3.5.5 DSO ger råd och rekommendationer till PUA

Det saknas idag en samlad rutin över hur alla registrerades rättigheter (8 stycken) praktiskt skall hanteras. Denna rutin bör snarast tas fram.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Alla anställda i Stockholms stad kan rapportera en incident.
Hur många personuppgiftsincidenter har dokumenterats?	20 stycken
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	0 stycken
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	NA

3.6.2 Syfte

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

Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering. Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter.

3.6.3 Resultat

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

Socialförvaltningen har en dokumenterad rutin för hantering av personuppgiftsincidenter. På grund av tillfälliga ändringar i personalstyrkan har denna rutin behövt revideras mot slutet av året och den nuvarande arbetsgången är ännu inte ”officiellt” dokumenterad. Vad som gäller i skrivande stund är att den medarbetare som upptäckt en incident genast ska rapportera denna via ett standardiserat formulär. Rapporten skickas sedan till förvaltningens dataskyddsansvarig (DSA) som läser igenom och gör

en bedömning av hur allvarlig incidenten är. Vid behov kontaktar DSA förvaltningens DSO och rådgör med denna kring huruvida incidenten ska rapporterats till IMY eller ej. Därefter diarieförs incidentrapporten och bevaras för statistikändamål.

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
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

3.6.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudets bedömning är att det idag finns en fungerande rutin för hur personuppgiftsincidenter skall hanteras. Denna rutin behöver dock formaliseras och dokumenteras samt göras känd för verksamheten.

4 Genomförda granskningar under året

4.1 Sammanfattning

Socialförvaltningens DSO har under hösten 2024 granskat förvaltningens hantering av avtal med leverantörer eller samarbetspartners avseende personuppgiftsbehandling (PUB-avtal) och kunde då konstatera att det finns brister inom området.

Medskick till förvaltningen efter granskningen var att det finns brister inom framförallt tre områden:

- För alla avtal som finns i Stockholms Stads avtalskatalog, som innefattar personuppgiftsbehandling och som Socialnämnden bestämt ändamål och medel för, ska ett PUB-avtal upprättas. Detta gäller även gemensamt tecknade avtal avseende programvaror och tjänster.
- De avtal som Serviceförvaltningen upphandlar å Socialförvaltningens vägnar, och Socialförvaltningen är personuppgiftsansvarig för skall Socialförvaltningen säkerställa att det finns ett undertecknat PUB-avtal.
- Informationskravet gäller inte enbart leverantörer utan även alla aktuella underleverantörer.

Socialförvaltningen behöver omhänderta detta och hitta en hantering framöver för att själva eller tillsammans med andra förvaltningar hitta en fungerande lösning för att upprätta och inarbeta upprättade PUB-avtal inom ramen för förvaltningens dataskydd.

4.2 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet uppmanar förvaltningen att gå igenom avtalskatalogen för att se vilka avtal som är aktuella för Socialförvaltningen. Där kan finnas redan undertecknade personuppgiftsbiträdesavtal som undertecknats för hela staden vilket kan vara fallet då:

- KF har fattat ett beslut i t.ex. budget där det fastslås att en nämnd, som t.ex. kommunstyrelsen, ska genomföra upphandling och teckna avtal för ett visst ändamål (t.ex. GSIT)
- Nämnd som vill delta i en gemensam upphandling har lämnat fullmakt till upphandlande myndighet att teckna

avtal å dess räkning, vilket även omfattar personuppgiftsbiträdesavtal.

Dessa PUB-avtal måste då finnas med i aktuella behandlingar i förvaltningens registerförteckning.
Saknas PUB-avtal med aktuell leverantör så måste det snarast upprättas.

Vidare bör förvaltningen ta del av och beakta det yttrande som den europeiska dataskyddsdomstolen (EDPB) gjorde i oktober.

Yttrandet belyser att den personuppgiftsansvariga alltid bör ha tillgång till information om identiteten (dvs. namn, adress, kontaktperson) för alla personuppgiftsbiträden, underentreprenörer osv. så att de på bästa sätt kan fullgöra sina skyldigheter enligt artikel 28 i den allmänna Dataskyddsförordningen. Dessutom bör den personuppgiftsansvariges skyldighet att kontrollera om (under)personuppgiftsbiträdena uppvisar "tillräckliga garantier" gälla oberoende av risken för de registrerades rättigheter och friheter, även om omfattningen av en sådan kontroll kan variera, särskilt på grundval av de risker som är förknippade med behandlingen.

I yttrandet anges också att även om det ursprungliga personuppgiftsbiträdet bör se till att det föreslår underentreprenörer med tillräckliga garantier, ligger det slutliga beslutet och ansvaret för att anlita en specifik underentreprenör kvar hos den personuppgiftsansvarige.

Om överföring av personuppgifter utanför Europeiska ekonomiska samarbetsområdet äger rum mellan två (under)entreprenörer bör personuppgiftsbiträdet i egenskap av uppgiftsutförare dessutom utarbeta relevant dokumentation, t.ex. om den grund för överföring som används, konsekvensbedömningen av överföringen och eventuella kompletterande åtgärder. Eftersom den personuppgiftsansvarige fortfarande omfattas av de skyldigheter som följer av artikel 28.1 i Dataskyddsförordningen om "tillräckliga garantier", utöver de som anges i artikel 44 för att säkerställa att skyddsnivån inte undergrävs av överföringar av personuppgifter, bör den personuppgiftsansvarige bedöma denna dokumentation och kunna visa den för Integritetsskyddsmyndigheten (IMY) vid behov.

5 Risker inom dataskydd

5.1 Sammanfattning

De största riskerna inom dataskydd för Socialförvaltningen har redan beskrivits i denna rapport. Avsaknaden av en stabil grund att basera dataskyddsarbetet på, i form av en uppdaterad och väl anpassad registerförteckning, medför att övrigt dataskyddsarbete kan ”hänga lite löst” och inte ha den förankring som behövs.

Dataskyddsförordningen ställer dokumentationskrav på aktuella personuppgiftsbehandlingar. Det räcker inte bara att göra rätt, förvaltningen måste också kunna visa att den gör rätt.

Detta bör göras genom att dokumentera aktuella överväganden. Av den anledningen är det viktigt att dokumentation upprättas innan en ny behandling påbörjas och att pågående behandlingar, gås igenom, för att säkerställa att lagkraven uppfylls.

5.2 Syfte

Verksamheten har ansvar för att göra vissa typer av riskanalyser, så som **konsekvensbedömningar** och **informationsklassningar**, men dessa ger inte en heltäckande bild av personuppgiftsriskerna i verksamheten. Dataskyddsombudet behöver som underlag för sin egen planering och sitt löpande arbete ha kontinuerlig överblick över dessa risker, i verksamhetens samtliga personuppgifts-behandlingar. Exempelvis krävs en sådan överblick för att kunna välja ut vilka områden som bör granskas under det kommande året eller för att avgöra vilka råd som Dataskyddsombudet behöver lämna till verksamheten om dataskyddsåtgärder som behöver vidtas.

5.3 Resultatet av riskkartläggningen

Som tidigare nämnts bedrivs det på Socialförvaltningen inom flera delar av dataskyddsområdet ett bra arbeta som bidrar till regelefterlevnad.
Men grunden för att få ett fullt fungerande dataskyddsarbete är att insikten och kompetensen att dokumentera sina behandlingar finns i verksamheten och att detta integreras i den dagliga verksamheten och sköts löpande av såväl chefer som medarbetare. Först då, det sker en kontinuerlig uppdatering av riskbedömningarna och behandlingarna i registerförteckningen, kommer dataskyddsarbetet att fungera i praktiken.
Dataskyddsarbetet måste bli en naturlig del av det löpande arbetet. När så är fallet kommer dataskyddsfrågorna inte känns lika

främmande och svårhanterliga som det upplevs som att de på många håll i verksamheten gör idag.

5.4 DSO ger råd och rekommendationer till PUA

En otroligt viktig aktivitet i dataskyddsarbetet är att säkerställa att man har byggt upp en fungerande dataskyddsorganisation som är tydligt förankrad och fastställd och som specificerar vilka arbetsuppgifter och vilket ansvar respektive anställd i organisationen har i dataskyddsarbetet.

DSO rekommenderar ledningsgruppen att aktivt stödja det arbete som under året har inletts med att bygga upp en fungerande dataskyddsorganisation.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Registerförteckningen
- PUB-avtal

6.2 Syfte

Det granskande arbetet är en av Dataskyddsombudets viktigaste uppgifter. Eftersom Dataskyddsombudet har begränsat med tid, så måste granskningsplanen för det nya året utformas med eftertanke.

Av den anledningen har två granskningar ansetts som en rimlig granskningsinsats inför kommande verksamhetsår. Granskningsområdena är valda utifrån ett riskbaserat synsätt, det vill säga att fokus ligger på de områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Därmed åstadkoms en röd tråd i dataskyddsarbetet från verksamhetsår 2024 till 2025 samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.

6.3 Planerade granskningar

Granskning 1

Denna granskning av registerförteckning och bedömda risknivåer samt allmän överblick över vilka behandlingar som görs, enligt artikel 30 kommer inte vara vid ett specifikt tillfälle utan kommer att ske kontinuerligt under kommande år.

Granskning 2

Denna granskning avseende PUB-avtal och överblick över hur PUB-avtal identifieras kommer att ske vid ett specifikt tillfälle, troligtvis under hösten 2025.
Granskningen kommer då att inriktas på vilka åtgärder som vidtas och hur riskerna hanteras samt bedöma om förvaltningen har implementerat de aspekter som den europeiska dataskyddsdomstolen (EDPB) gjorde i sitt yttrande i oktober 2024.