Stockholms stad

Bilaga 5

GDPR Årsrapport

År 2023

Socialförvaltningen

GDPR årsrapport
Januari 2024

Dnr: SOF 2024/57
Utgivningsdatum: 2024-01-17
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 framgår det att av dessa sex områden så är det två område som har stora brister och det är registerförteckningen som behöver ses över såväl strukturen som uppdateringen av innehållet samt konsekvensbedömningarna som behöver bli tydligare kopplade till behandlingarna i registerförteckningen.

Inom området Tekniska och Organisatoriska åtgärder arbetas det ambitiöst med informationsklassningar. Däremot är uppfyllandet av stadens obligatoriska e-utbildningar på en för låg nivå (50%) för att passera utan anmärkning.

Övriga område är däremot utan större brister och bedöms vara på rätt väg i mot regelefterlevnad.

	Registerförteckning	Styrdokument	Tekniska och organisatoriska åtgärder	Konsekvensbedömningar	Individens rättigheter	Personuppgiftsincidenter
Allvarliga brister identifierade						
Brister identifierade som bedöms vara omfattande	X			X		
Brister identifierade som bör åtgärdas			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?	307
Har nödvändiga uppdateringar gjorts?	Nej, 81% av behandlingarna har inte uppdaterats de senaste tre åren.
Bedöms registerförteckningen vara fullständig?	Nej, ”ifyllandegraden” av formulären är mycket låg.
Har verksamheten lämpliga rutiner för registerföring?	Delvis

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 register-förteckning.

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 307 personuppgiftsbehandlingar registrerade i verktyget Draftit Privacy Records. Under året 2023 har 20 registreringar tillkommit och/eller 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.

	Senast ändrat	
2023	20	7%
2022	16	5%
2021	22	7%
2020	41	13%
2019	208	68%
	307	

Ovanstående tabell illustrerar att det gjordes ett stort arbete med registerförteckningen under 2019 men att det därefter har varit en betydligt lägre aktivitet. Dataskyddsombudet rekommenderar att verksamheten 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 personuppgifts-behandlingar 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, då det torde ha skett en del verksamhetsförändringar sedan 2019, och behöver ett fortsatt utvecklingsarbete.

DSO bedömer hur fullständig registerförteckningen är

DSO bedömer att registerförteckningen inte är att anse som fullständig.

	Ifyllandegrad	
0-10%	69	22%
10-20%	7	2%
20-40%	178	58%
40-60%	46	15%
60-100%	7	2%
	307	

Ovanstående tabell illustrerar ”ifyllandegraden” vilket är ett mått på hur många av formulärets frågor som har besvarats. Tabellen visar att 82% av behandlingarna har <40% besvarade frågor. Detta är ett tecken på att antingen så är formulären för omfattande eller så har de som skall besvara frågorna inte tillräcklig information. Med dagens frågeformulär med över 100 frågor för att registrera en behandling blir det är svårt att hålla registret relevant och uppdaterat med korrekt information.
Bedömningen är att registerförteckningen idag inte är helt fullständig och behöver ett fortsatt utvecklingsarbete.
I dataskyddsförordningen finns det sju obligatoriska frågor som man ska ha med i en registerförteckning. Genom att börja med dem

och enbart bygga ut med det som är relevant så skulle ett mer hållbart register att arbeta efter och hålla uppdaterat åstadkommas.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Förvaltningen har idag, 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.

I förvaltningens Draftit Privacy Records finns idag ett stort antal identiska formulär vilket kan bidra till en ökad administration.

Antal	Behörighet
63	Aktiva användare
38	Formuläradministratör
4	Standardanvändare
21	Ingen behörighet

Ovanstående tabell illustrerar behörigheten till Draftit Privacy Records.
Formuläradministratören har egna inloggningsuppgifter men begränsad insyn då de enbart kan se sitt formulär och granska/godkänna skapade behandlingar.
En standardanvändare är en registrant ute i organisationen som får möjlighet att skapa registreringar på begäran av formuläradministratören.
Ingen behörighet är som namnet säger, en person som inte kan logga in i produkten där denna behörigheten är satt.

Bedömningen är att behörigheterna och formuläranvändningen idag inte är helt optimal, med för många formulär och formuläradministratörer, och behöver ses över.

3.1.4 DSO anger hur allvarliga bristerna är på en skala

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

3.1.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet bedömer att förvaltningen inte har en optimal struktur avseende registerförteckningen.

Registreringarna vilka registrerats i Drafit Privacy Records år 2023 har dock en betydande större ”ifyllandegrad” än tidigare år vilket tyder på att det utvecklingsarbete som startade under året är på rätt väg.

De brister som idag finns i förvaltningens registerförteckning behöver åtgärdas. Främst behöver gamla registreringar ses över samt att antalet formulär bättre anpassas och 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 verk-samhet om vad som gäller och vad som förväntas av medarbetarna i fråga om hantering av personuppgifter.

Att styrdokument finns ned-tecknade, 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?	26 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 26 stycken personuppgiftsbehandlingar, och de är aktuella. Det innebär att det är rimligt att anta att lämpliga tekniska och organisatoriska åtgärder är vidtagna för behandling. 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 2023 har hälften av medarbetarna genomfört dessa e-kurser, vilket inte kan anses vara godkänt då det är obligatoriskt genomförandekrav.

Status	Grundutbildning i dataskydd	Informationssäkerhet för medarbetare i staden
Certifierad	648	623
Ej certifierad	574	583
Pågår	45	65
	1267	1271
Genomförandegrad	51%	49%

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 obligatoriska utbildningar. Genomförandet i Ledningsgruppen under 2023 på 50% skickar signalen 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.

Antal	Risknivå
6	Hög risk
10	Medelhög risk
38	Låg risk
253	Ingen risknivå angiven

Ovanstående tabell illustrerar de angivna risknivåerna i registerförteckningen. Då det finns 253 behandlingar som inte har fått en angiven risknivå måste svaret på rubrikens fråga bli ett nej.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?
Det finns sex stycken personuppgiftsbehandlingar i Draftit Privacy Records som har en risknivå Hög risk. Inga av dessa sex har en genomförd konsekvensbedömning i Draftit Privacy DPIA.

Är de genomförda konsekvensbedömningarna aktuella?
Det har under 2023 genomförts fyra stycken konsekvensbedömningar, varav tre stycken tröskelanalyser.

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 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?	16 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. Denna blankett om begäran om registerutdrag berör socialförvaltningens verksamhet men den bör ses över och mer efterlikna stadens blankett som finns på intranätet. 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

Kravet på underskrift och kontaktuppgifter bör tas bort från blanketten. Det finns i artikel 15 inget formellt krav på underskrift och beträffande adress bör rutinen vara att det skickas till folkbokföringsadressen (inte den som den sökande ev uppger).

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?	17 stycken
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	6 stycken
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	5 stycken

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?

Rapportering till IMY har under 2023 skett i tid (utom en). Det som behöver förstärkas inom förvaltningen är förmågan att upptäcka och/eller identifiera en personuppgiftsincident. Funktionsbrevlådan för Dataskyddsombud bevakas dagligen vilket innebär att anmälda incidenter behandlas brådskande. Det finns rutiner, blanketter och vägledande dokument som stöd vid ovan nämnda hantering.

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

Det finns idag en etablerad struktur inom förvaltningen avseende rapportering av personuppgiftsincidenter och en dialog med Dataskyddsombudet sker vid behov.

Dataskyddsombudets bedömning har visat att det idag inte alltid är helt klart i ärendets gång avseende när en personuppgiftsincident uppmärksammats, när Dataskyddsombudet kopplas in samt när en bedömning om incidentens art och allvar genomförs.
Förtydliganden behöver ske avseende ansvarsfördelning mellan ansvarig chef och Dataskyddsombudet vid utredning och rapportering av personuppgiftsincidenter.

4 Genomförda granskningar under året

4.1 Sammanfattning

Den 21 april 2023 utnämnde Socialnämnden en medarbetare på Socialförvaltningen till Dataskyddsombud. På grund av den intressekonflikt som uppstått genom att en och samma person innehade rollerna som Dataskyddsombud och förvaltningsjurist, entledigade Socialnämnden medarbetaren från sitt uppdrag som Dataskyddsombud.

Med anledning av nämnda intressekonflikt som förelegat under året har det inte genomförts några granskningar under 2023.

4.2 DSO ger råd och rekommendationer till PUA

Socialnämnden beslutade att från och med den 12 december 2023 enligt ovan entlediga Dataskyddsombudet och utnämna en externt anlitad konsult till uppdraget som Dataskyddsombud.
Därmed är den tidigare intressekonflikten inte längre kvar så under 2024 kommer granskningar att vara en del i Dataskyddsombudets uppdrag.

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, 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 våra personuppgiftsbehandlingar. Det räcker inte bara att göra rätt, vi måste också kunna visa att vi gör rätt.

Det gör vi genom att dokumentera våra överväganden. Därför är det viktigt att detta genomförs 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 behandlingarna i registerförteckningen kommer dataskyddsarbetet att fungera i praktiken.
Dataskyddsarbetet måste bli en naturlig del av det löpande arbetet vilket då kommer leda till att dataskyddsfrågor inte känns lika

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

5.4 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att ledningsgruppen aktivt stödjer det arbete som har inletts med att bygga upp en fungerande dataskyddsorganisation som får de resurser som behövs för att integrera dataskyddsarbetet fullt ut i verksamheten.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Registerförteckningen
- Konsekvensbedömningar

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. Därav 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 2023 till 2024 samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.

6.3 Planerade granskningar

Granskning 1

Registerförteckning och bedömda risknivåer samt allmän överblick över vilka behandlingar som görs, enligt artikel 30

Granskning 2

Konsekvensbedömningar och överblick över hur risker identifieras, vilka åtgärder som vidtas och hur riskerna hanteras samt bedöma om behandlingen är proportionerlig i förhållande till de risker som behandlingen medför enligt artikel 35.