Stockholms stad

Bilaga 5

GDPR Årsrapport

År 2025

Socialförvaltningen

GDPR årsrapport
December 2025

Dnr: SOF XXXXX/XX
Utgivningsdatum: 2025-12-11
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 Socialnämnden ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för nämnden att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

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

Innehåll

2 Sammanfattning

I egenskap av Socialförvaltningens Dataskyddsombud lämnar jag följande årsrapport. Tabellen på nästa sida 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 **två områden som har stora brister**, och behöver få en fokusering under det kommande verksamhetsåret, det är registerförteckning och konsekvensbedömningar.

Arbetet med registerförteckningen, som under slutet av 2024 och början av 2025, genomgick ett större förändringsarbete av såväl struktur som uppdatering av innehåll, och därför flyttades från en ”orange” till ”gul” risk har nu under 2025 dock tappat styrfart och förankring i verksamheten och återgår till en tidigare och högre risknivå.

Arbetet med konsekvensbedömningarna som under flera år fått anmärkningar då de behöver bli betydligt fler och tydligare kopplade till behandlingarna i registerförteckningen har inte fokuserats under året och bedöms därför fortsatt vara ett område med omfattande brister.

Inom området Tekniska och Organisatoriska åtgärder pågår arbete med informationsklassningar men de har fortfarande för liten koppling och påverkan på dataskyddet då tekniska åtgärder ofta förutsätter även organisatoriska åtgärder för att åtgärden ska ge det dataskydd som behövs.

Inom område Styrdokument och Personuppgiftsincidenter har det inte, rapporterats om, något nämnvärt utvecklingsarbete under året och dessa områden bedöms vara utan större brister och därmed leva upp till 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		X	
Inga brister av nämnvärd betydelse identifierade		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 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?	634
Har nödvändiga uppdateringar gjorts?	Nej
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Nej

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.

Socialförvaltningens 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

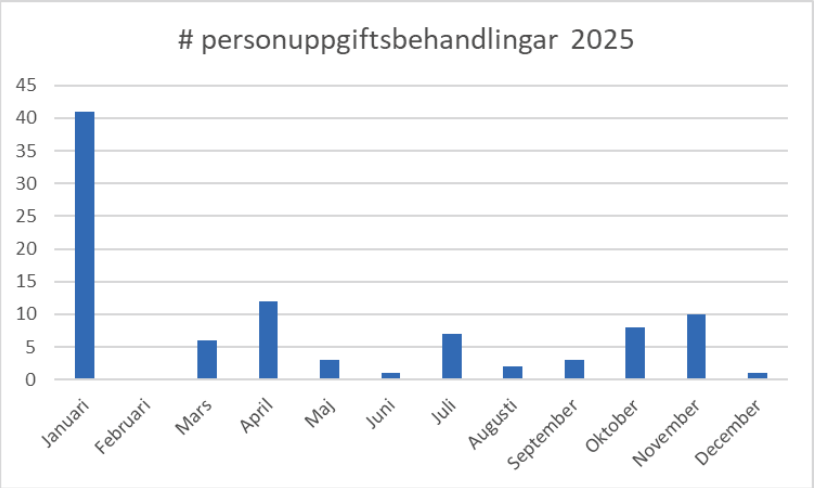
Socialförvaltningen startade under slutet av 2024 ett ambitiöst initiativ för att få en tydligare koppling till hanteringsanvisningarna, som kopplar redovisningsplanens processer till de handlingstyper som skapas i processerna, och personuppgiftsbehandlingarna.

Tyvärr har detta initiativ tappat fart och inriktning under 2025.

Av de 154 processer som är beskrivna i Hanteringsanvisningar har idag 74 stycken, en eller flera, personuppgiftsbehandlingar dokumenterade och resterande processer saknar aktuella personuppgiftsbehandlingar.

DSO kontrollerar hur många behandlingar som registrerats
Det finns idag 634 personuppgiftsbehandlingar registrerade i verktyget Draftit Privacy Records varav dock flertalet är obsoleta.

Denna rapport fokuserar på 2025 och under innevarande år har 94 nya registreringar tillkommit.



Bilden ovan visar antalet påbörjade personuppgiftsbehandlingar per månad under 2025. Under januari månad var det en hög aktivitet men den minskade betydligt under kommande månader.

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.

Status	#	
Under bearbetning	46	49%
Godkänd	40	43%
Komplettering begärd	6	6%
Under granskning	2	2%
	94	

Ovanstående tabell illustrerar att av de 94 startade personuppgifts-behandlingarna så är det mindre än hälften som har blivit godkända och klara.

DSO bedömer hur fullständig registerförteckningen är
DSO bedömer att registerförteckningen i dagsläget inte är att anse som fullständig och att det trots att det under hösten 2024 togs fram ett nytt gemensamt, nedbantat formulär så behövs det kraftfulla insatser i verksamheten för att uppnå en fullständighet under 2026.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Föregående års påpekande i årsrapporten att behörigheterna och formuläranvändningen inte var optimal, med för många formulär och formuläradministratörer, ledde till en mycket bättre behörighetsstyrning och en stor bantning i formulärsfloran. Trots dessa positiva åtgärder så har det ännu inte lett till någon övergripande större förbättring.

Det finns ett ambassadörsnätverk som består av dataskydds-intresserade medarbetare från olika delar av verksamheten som har träffats ett antal gånger under året men antalet deltagare på dessa träffar har succesivt minskat under året.

Som nedanstående bild visar så är det väldigt få organisations-entiteter (avd, enhet, stab, område) som har producerat en godkänd personuppgiftsbehandling under året.

Detta tyder på att det finns för få (inga) drivkrafter för verksamhets-chefer att ta fram kompletta och godkända personuppgifts-behandlingar för den egna verksamheten.

Enhet	#	(%)	Godkänd	Under bearbetning	Komplettering begärd
Socialförvaltningen (alla enheter)	23	25%	13	4	4
Kompetenscenter Vuxna	4	4%	3	1	0
Intro Stockholm	3	3%	3	0	0
Omr de hälso- och sjukv rd	3	3%	3	0	0
Resursteamen barn oc...	3	3%	3	0	0
Staben vid socialtjä...	3	3%	3	0	0
Omr det för tillstån...	4	4%	2	2	0
Enheten för digital verksamhetsutveckling	3	3%	2	1	0
Omr de öppenv rd	3	3%	2	1	0
Jour- och Familjehem...	4	4%	1	3	0
Korttidshemmet Drömm...	1	1%	1	0	0
LSS kollo	1	1%	1	0	0
Omr de stöd och skydd	1	1%	1	0	0
Upphandling och Före...	1	1%	1	0	0
Avdelningen för strategi och utveckling	9	10%	0	9	0
Kompetenscenter Funk...	4	4%	0	4	0
Enheten för samordning och uppföljning	4	4%	0	3	1
Omr de Hemlöshet	3	3%	0	3	0
Stockholms stad Soci...	3	3%	0	3	0
Ekonomiskt bistånd	2	2%	0	2	0
Staben	2	2%	0	2	0
Tillst ndsenheten	2	2%	0	2	0
Administrativa enhet...	1	1%	0	1	0
Boendeenheten	2	2%	0	1	1
Boutredningsenheten	1	1%	0	1	0
Enheten för sociala system	1	1%	0	1	0
Kompetenscenter Barn och unga	1	1%	0	1	0
Stockholms ungdomstj...	1	1%	0	1	0
	93		39	46	6

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.
Tidigare påpekande gällande ett förändringsarbete med färre formulär och färre frågor per formulär har genomförts men har inte räckt till utan det måste till ett betydligt större engagemang från chefer i verksamheten.
Gör en omstart av ambassadörsnätverket och säkerställ att ambassadörerna har tillräckligt med tid för att utföra sitt uppdrag.

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 dataskydds-arbete 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?	31 system är klassade, 26 finns i DraftIT och kan alltså kopplas till aktuella personuppgifts-behandlingar.
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

31 system är klassade, 26 finns i DraftIT och kan alltså kopplas till aktuella personuppgiftsbehandlingar.

Det finns dessutom 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

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 helt tydlig och bör förbättras så att det i registerförteckningen enklare går att se om det har genomförts en klassning för behanlingen.

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 register-förteckningen 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	69	73%
Låg risk	19	20%
Medelhög risk	2	2%
Hög risk	4	4%
	94	

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

Är de genomförda konsekvensbedömningarna aktuella?
Det har under 2025 inte genomförts några konsekvensbedömningar, vilket måste bedömas som anmärkningsvärt.

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 behovet av att genomföra en konsekvensbedömning i Draftit Privacy DPIA.

Rekommendationen blir därför att konsekvent bedöma risknivån på personuppgiftsbehandlingarna och utifrån denna bedömning gå vidare och göra första steget i en konsekvensbedömning (Tröskelanalys).
Denna tröskelanalys kommer då ge svar på om en mer omfattande Konsekvensbedömning skall genomföras.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	27 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

Den registrerade, det vill säga den vars personuppgifter behandlas, har ett antal rättigheter enligt dataskyddsförordningen. Som personuppgiftsansvarig har Socialförvaltningen ett ansvar för att ha rutiner på plats för att hantera begäranden om att utöva dessa rättigheter när någon begär det.

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

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.

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

Däremot visar dokumentationen i personuppgiftsbehandlingarna (nedanstående tabell) att förståelsen för vad de registrerades rättigheter innebär behöver förbättras då rättigheterna endast uppfylls i 60-70% av behandlingarna.

Rätten till rättelse endast uppfylls i 12% (finns en snarlik kopia på denna rättighet). Rätten till automatiserade beslut är inte medtagen i formuläret som rättighet.

Vilka av de registrerades rättigheter uppfylls?		%)	Artikel
Rätten till information om behandlingen	62	66%	Artikel 12
Rätten till registerutdrag	60	64%	Artikel 15
Rätten till rättelse av felaktiga uppgifter	12	13%	Artikel 16
Rätten till radering (Rätten att bli glömd)	66	70%	Artikel 17
Rätten till begränsning	69	73%	Artikel 18
Rätten till dataportabilitet	60	64%	Artikel 20
Rätten att göra invändningar	65	69%	Artikel 21
Rätten att f felaktiga uppgifter korrigerade	65	69%	Artikel 16

Rätt till information; Den registrerade har rätt att få information när hens personuppgifter behandlas. Information om personuppgiftsbehandlingen ska lämnas av förvaltningen både när uppgifterna samlas in och när den registrerade annars begär det.

Rätt till tillgång; Den registrerade har rätt att vända sig till förvaltningen för att få veta om hens personuppgifter behandlas eller inte. Om den registrerades personuppgifter behandlas måste förvaltningen tillhandahålla en kopia på uppgifterna (Registerutdrag).

Rätt till rättelse; Den registrerade har rätt att vända sig till förvaltningen och be att få felaktiga uppgifter rättade.

Rätt till radering; Den registrerade har rätt att vända sig till förvaltningen och be att uppgifterna om honom eller henne raderas.

Rätt till begränsning av behandling; Den registrerade har i vissa fall rätt att kräva att behandlingen av personuppgifter begränsas.

Rätten att invända; gäller när personuppgifter behandlas för att utföra en uppgift av allmänt intresse, som ett led i myndighetsutövning.

Rätt till dataportabilitet; Den registrerade har rätt att få ut och använda sina personuppgifter på annat håll, gäller bara sådana personuppgifter som den registrerade själv har lämnat.

Automatiserade beslut; Den registrerade har rätt att inte bli föremål för ett beslut som enbart grundas på någon form av automatiserat beslutsfattande.

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

3.5.5 DSO ger råd och rekommendationer till PUA

Genom dataskyddsförordningen garanteras registrerade både insyn och möjlighet att påverka användandet av sina personuppgifter. Detta ställer krav på förvaltningen: den ska både kunna förstå innebörden av dessa rättigheter och kunna hantera dem korrekt. Gör förvaltningen fel kan både dryga sanktionsavgifter och skadestånd aktualiseras.

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

Dessutom behöver kunskapsnivån höjas inom detta område så att personuppgiftsbehandlingarna på ett korrekt vis tydliggör vilka rättigheter som gäller i respektive personuppgiftsbehandling.

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?	27 stycken
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	2 stycken
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Alla

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.

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 behöver dock formaliseras och dokumenteras i en rutin samt göras känd för verksamheten.

4 Risker inom dataskydd

4.1 Sammanfattning

Den största risken inom dataskydd för Socialförvaltningen är de rådande brister som finns dokumentationen av verksamhetens behandlingsaktiviteter och de risker som kan finnas kopplade till personuppgiftsbehandlingen.

Chefer i verksamheten har idag svårigheter i att få en överblick över vilka behandlingar och riskbedömningar som finns eller som saknas i deras verksamheter då det är brister i dokumentationen.

Det som utgör basen i ett effektivt dataskydd är att ha fullständig insyn och kontroll över alla behandlingsaktiviteter. Ett behandlingsregister är inte bara ett lagkrav utan också en kritisk resurs för riskhantering. Det register ska detaljerat dokumentera syftet med att behandla datan, behandlingens laglighet, datatyper, och vem som har tillgång. Detta register kräver kontinuerlig uppdatering och granskning, särskilt när nya dataströmmar introduceras eller när befintliga processer ändras. Det skall fungera som ryggraden i förvaltningens dataskyddsstrategi, möjliggöra snabba åtgärder vid potentiella risker och säkerställa regelefterlevnad.

En avsaknad av dokumentation över alla behandlingsaktiviteter medför även brister i förmågan att göra en riskbedömning innan påbörjan av en ny behandling av personuppgifter.

Anledningen till att en riskbedömning ska göras är att den ger svar på vilka åtgärder som behöver vidtas för att skydda person-uppgifterna i verksamheten. Det måste genomföras lämpliga tekniska och organisatoriska åtgärder för att säkerställa – och även kunna visa – att behandlingen utförs enligt dataskyddsreglerna. Åtgärderna som vidtas måste regelbundet ses över och uppdateras vid behov.

Att arbeta med dessa områden kräver en sammanhållen strategi och ett löpande förbättringsarbete.

Genom att förstå och åtgärda ovanstående brister kan Socialförvaltningen inte bara undvika potentiella sanktioner utan också bygga ett starkare förtroende hos sina intressenter.

4.2 Syfte

Skapa en tydlig koppling mellan verksamhetens utförande av sina uppgifter (Hanteringsanvisningar) och dokumenterade personuppgiftsbehandlingar med tillhörande riskbedömningar.

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

4.3 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att ledningsgruppen initierar ett verksamhetsintegrerat projekt som mycket mer aktivt involverar verksamhetschefer i det dokumentationsarbete som inleddes under slutet av 2024 men tyvärr avstannade under början av 2025.

Ett sådant initiativ behövs för att få en genomförandekraft i dataskyddsorganisation och som då kan få det genomslag som behövs för att integrera dataskyddsarbetet fullt ut i verksamheten.