

GDPR årsrapport

År 2025

SDF Skärholmen




GDPR årsrapport
Januari 2026

Dnr: YYYY
Utgivningsdatum: 2026-01-20
Kontaktperson: Jonas Olsson

Sammanfattning

GDPR, eller Dataskyddsförordningen, syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. I Stockholms stad är varje nämnd och styrelse ansvarig för personuppgiftsbehandlingar som sker i den egna verksamheten. Ett dataskyddsombud har i uppdrag att oberoende granska verksamhetens efterlevnad av Dataskyddsförordningen. I denna rapport redovisar dataskyddsombudet årets granskning av Skärholmens stadsdelsförvaltnings dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

De tre största riskerna i Skärholmens stadsdelsförvaltning är, enligt dataskyddsombudets bedömning:

Fråga/kontroll	Risk	Rekommenderad åtgärd/åtgärder
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		<p><i>Nej det görs inte frekvent idag men kommer att kunna etableras under kommande år med ett nytt verktyg.</i></p> <p>Rekommenderad åtgärd: Ta beslut om (resurssatt och planerad) övergång till nytt verktyg som har tröskelanalys integrerad i personuppgiftsbehandlingen.</p>
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		<p><i>Det har skett positiva framsteg under året men de sitter fortfarande inte riktigt förankrade i verksamhetens linjärbete.</i></p> <p>Rekommenderad åtgärd: För att säkerställa att verksamheten har ändamålsenliga rutiner för att registrera nya personuppgiftsbehandlingar krävs en strukturerad process och ett tydligt system för att hantera nya behandlingar av personuppgifter. Det första steget är att skapa medvetenhet och utbilda alla chefer i verksamheten om betydelsen av dataskydd och deras viktiga roll i sammanhanget.</p>
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		<p><i>Det finns fortfarande förbättringsutrymme på ett antal viktiga områden:</i></p> <ul style="list-style-type: none">• Förståelsen för användning av rättslig grund• Hantering av leverantörer (PUB)• Hantering av känsliga personuppgifter <p>Rekommenderad åtgärd: Det bör inrättas en formell dataskyddsgrupp med en centralt ansvarig, exempelvis en DSA (Dataskyddsansvarig). Denna kan, med hjälp av DSO, utbilda, skapa rutiner, granska behandlingar och se till att alla lagkrav följs.</p>

Innehållsförteckning

Sammanfattning	1
Inledning.....	3
Dataskyddsombudets uppgift	3
Granskning av dataskyddsarbetet.....	4
Kontroll av obligatoriska områden	4
Resultatsammanställning och iakttagelser inom dataskyddsarbetet. 5	
<i>Register över personuppgiftsbehandlingar.....</i>	<i>5</i>
<i>Säkerhet i samband med behandlingen.....</i>	<i>7</i>
<i>Konsekvensbedömning avseende dataskydd.....</i>	<i>9</i>
<i>Den registrerades rättigheter.....</i>	<i>11</i>
<i>Personuppgiftsincidenter.....</i>	<i>13</i>
<i>Överföring till tredje land.....</i>	<i>15</i>

Inledning

GDPR, eller Dataskyddsförordningen, syftar till att skydda individers grundläggande rättigheter och friheter, med särskilt fokus på rätten till skydd av personuppgifter. Dataskyddsreglerna (*kallas GDPR fortsättningsvis*) sätter tydliga ramar för hur personuppgifter får behandlas för att minimera risken för skada och säkerställa att hanteringen sker ansvarsfullt och rättvist. GDPR har sin grund i de mänskliga rättigheterna, där varje individ har rätt till respekt för sitt privat- och familjeliv samt skydd av sina personuppgifter.

I Stockholms stad är varje nämnd och styrelse ansvarig för personuppgiftsbehandlingar som sker i den egna verksamheten.

Dataskyddsombudets uppgift

Varje personuppgiftsansvarig (nämnd eller styrelse) ska utse ett dataskyddsombud. Dataskyddsombudets uppgifter framgår direkt av lagstiftningen. Ombudets roll är att kontrollera att GDPR följs inom organisationen. Det innebär bland annat att ge råd, rekommendationer och informera om frågor som rör behandlingar av personuppgifter. Dataskyddsombudet har även i uppdrag att oberoende granska verksamheternas arbete med dataskyddsfrågor för att säkerställa att dataskyddslagstiftningen efterlevs. DSO ska rapportera direkt till högsta förvaltnings-/bolagsnivå. I Stockholms stad innebär det att dataskyddsombudet rapporterar till nämnder och styrelser.





Dataskyddsombudet lämnar årligen en rapport om verksamhetens dataskyddsarbete till varje nämnd och styrelse. Genom rapporten kan nämnd och styrelse ta emot de råd och rekommendationer som dataskyddsombudet lämnar. Årsrapporten syftar till att nämnd/styrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Årsrapporten är ett medel för nämnds/styrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Granskning av dataskyddsarbetet

Kontroll av obligatoriska områden

Dataskyddsombudet har granskat verksamhetens dataskyddarbete utifrån sex obligatoriska områden. De sex områdena har identifierats genom en analys av kraven i GDPR om hur verksamheter bör arbeta systematiskt med dataskydd. Varje område innehåller ett antal kontrollfrågor som ger en bild av verksamhetens dataskyddarbete. Dessa områden överensstämmer med de delar som enligt Integritetsskyddsmyndigheten (IMY) utgör grunden för en verksamhets systematiska och rättssäkra hantering av personuppgifter.

I rapporten används en riskmodell med fyra nivåer av risk. Modellen hjälper dataskyddsombudet att visa vilken bedömning hen gör av verksamhetens dataskyddsrisiker utifrån de iakttagelser som gjorts i granskningen.

Riskenivå	Beskrivning
Hög risk 	Iakttagelsen avser en brist som kan leda till betydande risker för de registrerades rättigheter och friheter. Bristen kräver omgående åtgärd och korrigering.
Medelhög risk 	Iakttagelsen avser en brist som kan leda till risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas skyndsamt, men kräver inte omedelbar korrigering.
Låg risk 	Iakttagelsen avser en brist som kan leda till mindre risker för de registrerades rättigheter och friheter. Bristen bör åtgärdas, men kräver inte omedelbar korrigering.
Inget att anmärka 	Dataskyddsombudet har inga brister att rapportera avseende denna del.
Notera att risken för att tilldelas en sanktion vid tillsyn är större desto högre risken är.	

Resultatsammanställning och iakttagelser inom dataskyddsarbetet

I detta avsnitt presenteras en sammanställning av den bedömda risknivån för verksamhetens dataskyddsarbete, grundat på kontrollfrågorna inom de sex obligatoriska områdena. Vidare redovisas dataskyddsombudets centrala iakttagelser, inklusive områden där verksamheten uppvisar goda resultat och bör upprätthålla sitt arbete, samt identifierade brister som kan utgöra dataskyddsrisker. Avsnittet innehåller även dataskyddsombudets rekommenderade åtgärder för att hantera dessa risker och stärka dataskyddsarbetet.

Register över personuppgiftsbehandlingar

Sammanfattning




Stadsdelsförvaltningen är, enligt Dataskyddsförordningen (artikel 30), som Personuppgiftsansvarig skyldig att föra ett register över alla personuppgiftsbehandlingar. Detta register ska innehålla information om alla de sätt på vilka personuppgifter behandlas inom organisationen. Syftet med registret är att säkerställa transparens och att verksamheten följer de krav som Dataskyddsförordningen ställer på hanteringen av personuppgifter.

Det finns idag 96 personuppgiftsbehandlingar registrerade i verktyget Draftit Privacy Records. Under året 2025 har 11 nya registreringar tillkommit och 33 äldre (skapade innan 2025) har ändrats.

Det har under året skett positiva framsteg inom förvaltningen avseende arbetssätt och kompetens för att hantera Registerförteckningen på ett korrekt sätt.

Ett förbättringsområde som kvarstår, och bör prioriteras kommande år, är att öka förståelsen och ansvarstagandet för Registerförteckningen hos förvaltningens linjechefer.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		<i>Under året 2025 har 11 nya registreringar tillkommit och 33 äldre (skapade innan 2025) har ändrats.</i>
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		<i>Det har skett positiva framsteg under året men de sitter fortfarande inte riktigt förankrade i verksamhetens linjearbete.</i>
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		<i>Nej inte fullt ut även om det har skett positiva framsteg under året så är det fortfarande inte riktigt förankrat i verksamhetens linjearbete.</i>

Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?



Det finns fortfarande förbättringsutrymme på ett antal viktiga områden:

- *Förståelsen för användning av rättslig grund*
- *Hantering av leverantörer (PUB)*
- *Hantering av känsliga personuppgifter*

Säkerhet i samband med behandlingen

Sammanfattning

Säkerhet i samband med behandlingen av personuppgifter är en av de viktigaste aspekterna inom dataskydd. I enlighet med Dataskyddsförordningen är alla som hanterar personuppgifter skyldiga att vidta lämpliga åtgärder för att skydda dessa uppgifter från oönskad åtkomst, förlust, förstörelse eller andra typer av intrång. Det handlar om både **tekniska** och **organisatoriska** åtgärder för att säkerställa att personuppgifterna behandlas på ett säkert sätt och för att minska riskerna för de registrerades integritet.

Det har under 2025 genomförts fyra stycken klassningar, varav tre stycken var kompletteringar av tidigare gjorda klassningar.



Inom stadsdelsförvaltningens verksamheter hanteras en stor mängd personuppgifter. Varav en del berör personer med skyddade personuppgifter. Stadsdelsförvaltningen bör göra en noggrann genomgång av sin verksamhet och upprätta anvisningar för hanteringen av skyddade personuppgifter inom den egna verksamheten då det krävs mer konkret dokumentation än vad den stadsövergripande policyn ger.

Det finns två e-utbildningar inom informationssäkerhet som är obligatoriska för alla medarbetare i stadsdelsförvaltningen och dessa utbildningar ska genomföras årligen för att hålla kunskaperna fräscha.

Tyvärr går det inte att presentera en rättvisande statistik då statistikverktyget inte ger en korrekt information. Det finns problem med att personer som blir certifierade sedan faller ut som ej certifierade trots detta. Många enheter har genomfört utbildningarna tillsammans på APT, med ett gemensamt formulär där man tillsammans fört en dialog om frågorna.

Den exakta statistiken kommer att presenteras i Verksamhetsberättelsen som då är baserad på en aktivitet för alla enheter att besvara.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Efter ett antal stickprov på genomförda informationsklassningar, bedömer DSO att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?		<i>Avsaknad av åtgärder för personer med skyddade personuppgifter.</i>
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att		<i>DSO bedömer att det finns tillräckligt med styrande dokument och rutiner om dataskydd.</i>

det finns tillräckligt mycket reglerat och tillräckligt stöd?

Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?



Den största utmaningen inom området är implementationen av de faktiska skyddsåtgärderna.

Konsekvensbedömning avseende dataskydd

Sammanfattning

Konsekvensbedömning avseende dataskydd (eller Data Protection Impact Assessment, DPIA) är ett viktigt verktyg för att säkerställa att personuppgifter hanteras på ett sätt som inte riskerar individens rättigheter och friheter. En konsekvensbedömning görs för att **identifiera** och **åtgärda** potentiella risker vid behandling av personuppgifter, särskilt när behandlingen är omfattande eller kan påverka individers integritet på ett allvarligt sätt.

Detta är ett område som länge varit eftersatt på Skärholmens stadsdelsförvaltning men har nu på senare delen av 2025 nått en viss insikt och förståelse i organisationen för att arbeta med riskbedömningar utifrån den registrerades perspektiv.

DSO ser positivt på denna utveckling för kommande år och tror även att en övergång till den senaste utgåvan av systemstöd för Registerförteckning/Konsekvensbedömning kan bidra positivt då hela processen – från behovsbedömning till dokumenterad riskanalys – då kommer att vara samlad i ett och samma verktyg.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		<i>Nej det finns inte riktigt på plats men det finns goda förutsättningar inför nästa år.</i>
Genomförs tröskelanalyser vid nya/förändrade personuppgiftsbehandlingar?		<i>Nej det görs inte frekvent idag men kommer att kunna etableras under kommande år med ett nytt verktyg.</i>
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		<i>Det finns ett systemstöd idag som har börjat användas men det är inte etablerat eller känt i organisationen.</i>
Genomförs konsekvensbedömning avseende dataskydd i de fall det krävs?		<i>Nej det görs inte frekvent idag men kommer att kunna etableras under kommande år med ett nytt verktyg.</i>
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvensbedömning		<i>Nej, men det kommer att kunna etableras för nya behandlingar under kommande år med ett nytt verktyg.</i>

avseende dataskydd görs samt genomfört detta?		
--	--	--

Den registrerades rättigheter

Sammanfattning

Stadsdelsförvaltningen har en fungerande rutin för att hantera inkommande begäranden av Registrerades rättigheter.

Däremot visar en genomgång av Personuppgiftsbehandlingarna på vissa kunskapsbrister i förståelsen av de Registrerade rättigheter.

De registrerades rättigheter under GDPR:





Rättighet	Betydelse	Kommentar till SDF
Rätt till information:	Den registrerade har rätt att få veta vilka personuppgifter som samlas in, varför de samlas in och hur länge de kommer att lagras.	SDF bör se över hur denna rättighet efterlevs då SDF inte finns med på stadens informationssida.
Rätt till tillgång:	Den registrerade har rätt att få en kopia på de personuppgifter som lagras.	SDF har idag en fungerande rutin för att lämna en kopia på personuppgifterna och information om hur de används.
Rätt till rättelse:	Den registrerade har rätt att få sina personuppgifter rättade om de är felaktiga eller ofullständiga.	De uppgifter om registrerade som behandlas av SDF ska vara korrekta och aktuella.
Rätt till radering ("Rätten att bli bortglömd"):	Den registrerade kan begära att få sina personuppgifter raderade, om de inte längre behövs för det syfte de samlades in för.	Den rättighet är inte absolut utan gäller vissa särskilda situationer exempelvis om SDF utför en uppgift av allmänt intresse och det saknas berättigade skäl som väger tyngre än den registrerades intresse.
Rätt till begränsning av behandling:	Den registrerade kan begära att behandlingen av sina personuppgifter begränsas (t.ex. om den registrerade anser att uppgifterna är felaktiga eller om behandlingen är olaglig).	Denna rättighet är inte absolut utan gäller vissa särskilda situationer.
Rätt till dataportabilitet:	Den registrerade har rätt att få sina personuppgifter i ett strukturerat, allmänt använt och maskinläsbart format och att överföra dessa till en annan tjänst, om det är tekniskt möjligt.	Denna rättighet gäller enbart om den registrerade själv har lämnat uppgifterna och samtyckt eller lämnat uppgifterna med anledning av ett avtal.
Rätt att invända:	Den registrerade har rätt att invända mot att sina uppgifter behandlas, till exempel om behandlingen sker för allmänintresse eller myndighetsutövning.	SDF är skyldig att informera den registrerade om sin rätt att invända. Det ska framgå senast vid första kontakttillfälle och informationen ska lämnas klart, tydligt och åtskilt från annan information.
Rätt att inte vara föremål för automatiserade beslut:	Den registrerade har rätt att inte vara föremål för beslutsfattande som uteslutande grundar sig på automatisk behandling, såsom profilering, och som har rättsverkningar för den registrerade. Det finns dock undantag till förbudet.	SDF arbetar fn inte med automatiserad beslut.

Nedanstående tabell visar hur de Registrerades rättigheter är dokumenterade i förvaltningens registerförteckning.

DSO ger korta och konkreta rekommendationer för att hantera bristerna och stärka dataskyddsarbetet utifrån de identifierade iakttagelserna.

Registrerades rättigheter	Andel av behandlingarna	Kommentar och förslag till åtgärd
[Inga rättigheter angivna]	4%	Komplettera behandlingarna
Rätten till information om behandlingen	89%	Borde vara nära 100% - se över
Rätten till registerutdrag	88%	Borde vara nära 100% - se över
Rätten till att göra invändningar	68%	
Rätten till begränsning	65%	
Rätten till dataportabilitet	58%	Borde inte vara så högt - se över
Rätten till radering (rätten att bli glömd)	64%	
Rätten att få felaktiga uppgifter korrigerade	90%	Borde vara nära 100% - se över
Rätt att inte vara föremål för automatiserade beslut	0%	Saknas i formuläret - komplettera

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		<i>Ja</i>
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		<i>Det har under året inkommit tre begäran om Registerutdrag</i>
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		<i>Samtliga har besvarats inom föreskriven tid.</i>
Baserat på ett antal stickprov genomförda av dataskyddsombudet, uppfyller svaren till de registrerade lagkraven?		<i>Inga anmärkningar</i>

Personuppgiftsincidenter

Sammanfattning

Att hantera personuppgiftsincidenter korrekt är en viktig del av dataskyddsarbetet och innebär att Stadsdelsförvaltningen ska vara förberedd på att hantera eventuella dataläckor eller säkerhetsincidenter som kan påverka personuppgifter.

En personuppgiftsincident är när det sker en säkerhetsöverträdelse som leder till att personuppgifter antingen förloras, förstörs, ändras eller obehörigen tillgängliggörs, t.ex. genom dataintrång, förlust av en enhet, felaktig hantering av information, eller obehörig åtkomst till system.

En omfattande personuppgiftsincident inträffade under hösten 2025 då IT-leverantören Miljödata, som för Stockholms stad testkörde ett rehabiliteringssystem (STELLA), drabbades av ett cyberangrepp, vilket ledde till att känsliga personuppgifter (namn, personnummer, adresser, hälsodata, etc.) för medarbetare som är eller varit anställda i Stadsdelsförvaltningen under perioden 2024 till augusti 2025, läcktes till Darknet.

Stadsdelsförvaltningen drabbades hårt då flera personer med skyddad identitet fick sina uppgifter röjda. Detta föranledde en anmälan till Integritetsskyddsmyndigheten (IMY), ett skadeståndsanspråk inkom från en drabbad person och Stadsdelsförvaltningen fick vidta åtgärder och löpande informera personalen.


Av denna anledning har DSO gått igenom **samtliga** rapporterade och dokumenterade personuppgiftsincidenter för att utvärdera om:

- 1) Personuppgiftsincidenterna har behandlats korrekt
- 2) Om någon personuppgiftsincidenten har inneburet en risk för individens rättigheter och friheter, då ska Personuppgiftsansvarig rapportera incidenten till Integritetsskyddsmyndigheten (IMY) inom 72 timmar från att den upptäcktes.

Status	Antal
Rapporterad	3
Under registrering	6
Klar	28
Under utredning	1
Under åtgärd	1
	39

Ovanstående tabell visar Stadsdelsförvaltningens status på rapporterade och dokumenterade personuppgiftsincidenter under 2025.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Hur säkerställs det att samtliga medarbetare har den kunskap som behövs för att veta hur denne		<i>Det är obligatoriskt för alla medarbetare att genomföra stadens informationssäkerhetsutbildning och den grundläggande utbildningen i dataskydd. Genomförandet har förbättrats</i>

ska agera vid en personuppgiftsincident?		<i>markant under året och kan bedömas som en mindre risk för de registrerades rättigheter och friheter.</i>
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		<i>Ja för att hantera personuppgiftsincidenter men det saknas en rutin för att hantera registrerade med Skyddade personuppgifter</i>
Hur många personuppgiftsincidenter har dokumenterats under året?		<i>39 st, se tabell.</i>
Hur många personuppgiftsincidenter har anmälts till IMY under året?		<i>3 st, se tabell.</i>

Överföring till tredje land

Sammanfattning

Stadsdelsförvaltningen hanterar och behandlar ett stort antal personuppgifter, inklusive känsliga uppgifter om invånare, elever, anställda och patienter. I vissa fall kan det vara nödvändigt att överföra dessa uppgifter till leverantörer eller system som är baserade utanför EU/EES, det vill säga till ett tredje land. Enligt Dataskyddsförordningen krävs det då att den Personuppgiftsansvarige vidtar särskilda åtgärder för att säkerställa att uppgifterna får ett adekvat skydd även i länder som inte har samma dataskyddsnivå som EU.

Av denna anledning har DSO gått igenom **samtliga** dokumenterade personuppgiftsbehandlingar för att utvärdera om:

- 1) personuppgifter behandlas i tredje land och om så är fallet
- 2) personuppgiftsbehandlingarna har ett adekvat skydd

Formulär	Överförs personuppgifter till tredjeland eller internationell organisation?		
	Ja	Nej	Vet ej
Direktörens Stab	0	2	0
HR, administration och nämnd	0	35	0
Individ och familj inklusive fritid	0	19	1
Förskola	0	12	0
Stöd och service	0	14	0
Medborgarservice och stadsmiljö	0	13	0
Ekonomi, lokal och upphandling	0	0	0

Genomgången av de dokumenterade personuppgiftsbehandlingarna visar att inga tredjelandsöverföringar förekommer.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelandsöverföringar som utförs?		<i>Ja och det finns inga dokumenterade tredjelandsöverföringar</i>
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?		<i>Det finns inga dokumenterade tredjelandsöverföringar</i>
Har personuppgiftsansvarig gjort en nödvändig bedömning, "Transfer Impact Assessment" (TIA), avseende tredjelandsöverföringar?		<i>Nej då det inte finns några dokumenterade tredjelandsöverföringar</i>