Avdelningen Verksamhetsstöd
Moon Carlbring

Styrelsen för Stockholm Vatten AB

Dataskyddsombudets årsrapport 2025

FÖRSLAG TILL BESLUT

Styrelsen föreslås besluta

att anta årsrapporten från bolagets dataskyddsombud

att ge bolaget i uppdrag att vidta åtgärder i enlighet med rekommendationerna

Christian Rockberger
Verkställande direktör

Niklas Björkman
Avdelningschef
Verksamhetsstöd

Bilaga: Dataskyddsombudets årsrapport 2025 SVOA

Stockholms stad

GDPR årsrapport

År 2025

Stockholm Vatten och Avfall AB

GDPR årsrapport
Januari 2025

Dnr: 2026 SVOA41
Utgivningsdatum: 2026-01-07
Kontaktperson: Moon Carlbring

Sammanfattning

Dataskyddsförordning (General Data Protection Regulation, GDPR) 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 Stockholm Vatten och Avfalls (SVOA) dataskyddsarbete samt lämnar rekommendationer på åtgärder för att ytterligare stärka dataskyddet.

Årsrapporten består av sex olika obligatoriska riskområden med frågor som Stockholms stad har bestämt samt ett antal bolagsspecifika risker. Samtliga riskområden redovisas med riskbeskrivning, riskvärde och rekommenderade åtgärder som personuppgiftsansvarig behöver ta ställning till och fatta beslut.

De tre största riskerna enligt dataskyddsombudets bedömning:

Fråga/kontroll/Risk	Risk/risknivå	Kommentarer/Rekommenderad åtgärd/åtgärder
Olika personuppgiftsansvariga Komplexiteten i gränsdragningen av personuppgiftsansvaret medför att kontroll och ansvar försvåras och i händelse av tillsyn kommer SVOA ha svårt att redogöra för detta.		Risken innebär ingen omedelbar konsekvens. Personuppgiftsansvarig rekommenderas tillsammans med övriga personuppgifts-ansvarig inom koncernen tillämpa en strategi för att hantera risken eller acceptera risken.
Säkerhet i leverantörskedjan Komplexitet i den långa leverantörskedjan försvårar ansvar och kontroll för personuppgifter.		Risken innebär ingen omedelbar konsekvens. Risken bedöms ha flera gränsytor där fel hantering kan uppstå. Personuppgiftsansvarig rekommenderas att upprätta en strategi och arbetssätt för att hantera risken eller acceptera risken.

Tredjelandsöverföringar SVOA har idag inget systematiskt arbetssätt för att identifiera, och dokumentera tredjelandsöverföringar.		Risken innebär ingen omedelbar konsekvens. Risken bedöms ha flera gränsytor där fel hantering kan uppstå. Personuppgiftsansvarig rekommenderas att upprätta en strategi och arbetssätt för att hantera risken eller acceptera risken.

Innehållsförteckning

Inledning

Dataskyddsförordningen (fortsättningsvis benämns som GDPR i detta dokument) syftar till att skydda individers grundläggande rättigheter och friheter.

I det digitala samhället registreras, lagras och vidareutnyttjas information mer än någonsin både med rättsligt stöd och för kommersiella intressen. Personuppgifter nyttjas dessvärre även i olagliga sammanhang till exempel i nätbedrägerier, vilket gör att det är extra viktigt för varje personuppgiftsansvarig att skydda enskilda individers personuppgifter.

Varje juridisk person är enligt GDPR personuppgiftsansvarig. På SVOA är det styrelsen som är personuppgiftsansvarig.

Dataskyddsombudets uppgift

Varje personuppgiftsansvarig ska utse ett dataskyddsombud enligt art. 37 i dataskyddsförordningen och säkerställa att dataskyddsombudet kan utföra sina arbetsuppgifter enligt art. 38-39. Det omfattar bland annat att stötta personuppgiftsansvarig och ha en strategi för att skydda registrerades personuppgifter och ansvarstilldelning för att behandla personuppgifter på korrekt sätt samt ge råd, stöd och information till verksamheten. Dataskyddsombudet ska även utbilda och granska verksamheten i dataskyddsarbetet efter behov.

Bedömning av riskområden

Årsrapporten redovisar sex riskområden med tillhörande frågor enligt Stockholms stads anvisningar. De sex riskområdena har identifierats genom att staden har genomfört en analys av kraven i GDPR om hur verksamheter bör arbeta systematiskt med dataskydd.

Dessa riskområden 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 enligt stadens anvisning. Modellen hjälper dataskyddsombudet att visa vilken bedömning som görs av verksamhetens dataskyddsrisker.

Övrigt att rapportera

I avsnittet om *Övrigt att rapportera* redovisas de risker som dataskyddsombudet har identifierat utöver stadens obligatoriska riskområden. Riskerna utgår ifrån samma rapporteringsstruktur och modell.

Hänvisningar och begrepp

Samtliga artikel-, avsnitt- och kapitelhänvisningar refereras till Dataskyddsförordningen.

Inom arbetet för dataskydd finns det ett antal centrala begrepp som används regelbundet. Nedan finns en utförligare förklaring vad var och ett betyder enligt GDPR.

Personuppgiftsansvarig	*Är en juridisk person som bestämmer ändamål och medel för en personuppgiftsbehandling, och som har ansvaret för att GDPR efterlevs.*

Personuppgiftsbehandling	*När registrerade personuppgifter används för ett särskilt ändamål, till exempel när ett flertal personuppgifter behandlas för att möjliggöra en löneutbetalning som är en personuppgiftsbehandling.*
Personuppgiftsbiträde	*Är en annan juridisk person som behandlar personuppgifterna på uppdrag av en personuppgiftsansvarig. (Det har ingen betydelse om juridiska personer är inom samma koncern eller är en offentlig aktör.)*
Registrerade	*Enskilda individers personuppgifter som en personuppgiftsansvarig behandlar.*

Granskning av dataskyddsarbetet 2025

Kontroll av obligatoriska områden

Dataskyddsombudet har granskat verksamhetens dataskyddsarbete 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 dataskyddsarbete. 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 som görs av verksamhetens dataskyddsrisker utifrån de iakttagelser som gjorts i granskningen.

Följande risknivåer finns:

Risknivå	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 centrala 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

Under 2025 beslutade SVOA att ha ett internt dataskyddsombud i egen regi. Utöver en granskande roll arbetar dataskyddsombudet strategiskt och systematiskt med att komma närmare verksamheten med bland annat utbildning och registrering av personuppgifter. Målet är att alla dataskyddsfrågor ska hanteras löpande inom linjeverksamheten.

Nedan följer bedömning av risknivå och rekommendationer från dataskyddsombudet.

Fråga/kontroll	Risk	Rekommendationer
Antal behandlingar som är registrerade?		137 registrerade personuppgiftsbehandlingar. Dataskyddsombudet har inga brister att rapportera avseende denna del.
Har verksamheten ändamålsenliga rutiner för att registrera nya/förändrade behandlingar?		Dataskyddsombudet har inga brister att rapportera avseende denna del.
Registreras/uppdateras behandlingar i den omfattning som krävs för att registret ska innehålla de behandlingar som personuppgiftsansvarig utför?		Dataskyddsombudet har inga brister att rapportera avseende denna del.
Har de uppgifter som är obligatoriska enligt artikel 30 besvarats kopplat till de registrerade behandlingarna?		Dataskyddsombudet har inga brister att rapportera avseende denna del.

Säkerhet i samband med behandlingen

Sammanfattning

Säkerhet i samband med personuppgiftsbehandlingar är komplex och hanteras av olika aktörer i skilda processer. Att arbeta med säkerhet i personuppgiftsbehandlingar är ett löpande arbete i alla arbetsflöden. SVOA arbetar kontinuerligt med att förbättra processen för att säkerställa säkerheten i personuppgiftsbehandlingar

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Efter ett antal stickprov på genomförda informations-klassningar, bedömer DSO att resultatet i genomförda informationsklassningar i tillräcklig utsträckning tar hänsyn till olika kategorier av personuppgifter?		Inga stickprov är genomförda, då samtliga informationsklassningar genomfördes på nytt under 2025. Dataskyddsombudet har inga brister att rapportera avseende denna del.
Avseende de styrande dokument och rutiner om dataskydd (som finns skriftligt), bedömer DSO att det finns tillräckligt mycket reglerat och tillräckligt stöd?		Dataskyddsombudet har inga brister att rapportera avseende denna del.
Avseende de skriftligt styrande dokument och rutiner som finns, bedömer DSO att de är tillräckligt implementerade och kända?		Dataskyddsombudet har inga brister att rapportera avseende denna del.

Konsekvensbedömning avseende dataskydd

Sammanfattning

Konsekvensbedömning utgör del i hantering av registerförteckning, vilket innebär att en bedömning alltid görs i samband med registerförteckning huruvida personuppgiftsbehandlingen innebär en hög risk enligt art. 35.

Bedömning av risknivå och rekommendationer från dataskyddsombudet.

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga rutiner för att vid nya/förändrade personuppgiftsbehandlingar genomföra tröskelanalys?		Dataskyddsombudet har inga brister att rapportera avseende denna del.
Genomförs tröskelanalyser vid nya/förändrade personuppgifts-behandlingar?		Under 2025 har inga tröskelanalyser genomförts, då samtliga personuppgifts-behandlingar registrerades på nytt. Förändringar i personuppgiftsbehandlingar kommer omhändertas framgent i det systematiska dataskyddsarbetet.
Finns det en ändamålsenlig mall samt rutiner för genomförande av konsekvensbedömning avseende dataskydd?		Dataskyddsombudet har inga brister att rapportera avseende denna del.
Genomförs konsekvens-bedömning avseende dataskydd i de fall det krävs?		Dataskyddsombudet har inga brister att rapportera avseende denna del.
Har personuppgiftsansvarig identifierat samtliga personuppgiftsbehandlingar som kräver att en konsekvens-bedömning avseende dataskydd görs samt genomfört detta?		Dataskyddsombudet har inga brister att rapportera avseende denna del.

Den registrerades rättigheter

Sammanfattning

Personuppgiftsansvarig kan omhänderta registrerades rättigheter. Utveckling pågår inom ramen för linjeorganisationen för att etablera nya och tydligare arbetssätt för att effektivare bemöta registrerade rättighetsförfrågningar enligt kap. 3 i GDPR.

Bedömning av risknivå och rekommendationer från dataskyddsombudet.

Fråga/kontroll	Risk	Rekommendationer
Finns det ändamålsenliga mallar samt rutiner för besvarande av begäran från den registrerade?		Dataskyddsombudet har inga brister att rapportera avseende denna del.
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har under året inkommit från de registrerade?		Två begäran har inkommit under 2025. Dataskyddsombudet har inga brister att rapportera avseende denna del.
Hur många av de inkomna begärandena har besvarats av verksamheten inom en månad?		Samtliga besvarades inom en månad. Dataskyddsombudet har inga brister att rapportera avseende denna del.
Baserat på ett antal stickprov genomförda av dataskydds-ombudet, uppfyller svaren till de registrerade lagkraven?		Inga stickprov är genomfördes, då endast två begäran inkom under året. Dataskyddsombudet har inga brister att rapportera avseende denna del.

Personuppgiftsincidenter

Sammanfattning

Utmaningen i granskningsområde *Personuppgiftsincidenter* hör ihop med granskningsområde *Säkerhet i samband med behandling*. Personuppgiftsbehandlingar sker i flera olika konstellationer. Vissa personuppgiftsbehandlingar hanteras av personuppgiftsbiträden, vissa i stadsgemensamma system och vissa av SVOA själva. Det innebär att krav för att upptäcka och alarmera om en personuppgiftsincident behöver ställas mot alla parter och samtliga processer.

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 ska agera vid en personuppgiftsincident?		SVOAs medarbetare genomgår årligen den stadsgemensamma obligatoriska utbildning inom dataskydd. Under 2025 har SVOA prioriterat att utbilda särskilda målgrupper/nyckelpersoner. Utbildningsinsatserna kommer att fortsätta även under 2026.
Finns det ändamålsenliga rutiner för att hantera händelser som kan utgöra potentiella personuppgiftsincidenter? Följs dessa?		Ja, det finns ändamålsenliga rutiner, men det krävs ett kartläggningsarbete för att identifiera i vilka arbetsflöden personuppgiftsincidenter kan uppstå. Arbetet har påbörjats under 2025 och kommer att fortgå under 2026.
Hur många personuppgiftsincidenter har dokumenterats under året?		Fyra personuppgiftsincidenter dokumenterades under 2025. Dataskyddsombudet har inget att rapportera avseende denna del.
Hur många personuppgiftsincidenter har anmälts till IMY under året?		Tre personuppgiftsincidenter anmäldes till IMY under 2025. Dataskyddsombudet har inget att rapportera avseende denna del.

Överföring till tredje land

Sammanfattning

Samma komplexitet som finns i granskningsområdet *Säkerhet i samband med personuppgiftsbehandling*, är att all form av extern (utkontraktering) lagring och behandling av personuppgifter innebär en leveranskedja där tredjelandsöverföringar kan förekomma och är bortom all kontroll trots att bolaget har personuppgiftsanvaret.

Bedömning av risknivå och rekommendationer från dataskyddsombudet

Fråga/kontroll	Risk	Rekommendationer
Har personuppgiftsansvarig identifierat de tredjelands-överföringar som utförs?		Det finns en komplexitet att identifiera tredjelandsöverföringar då det kan förekomma långt ner inom leverantörskedjan. För att identifiera tredjelandsöverföringar krävs att personuppgiftsansvarig kravställer inrapportering från personuppgiftsbiträden i samband med upphandling. En del av dessa avtal avropas av SVOA från staden centralt och Adda inköpscentral, vilket innebär att SVOA inte är med och ställer krav om tredjelands-överföringar. Identifiering av tredjelandsöverföringar kommer hanteras löpande i framtida inköp/upphandlingar i samband med arbetet *informationssäkerhet i upphandlingsförfarande.*
Tillämpar personuppgiftsansvarig ett överföringsverktyg på de tredjelandsöverföringar som utförs?	NA	Inga nya kända tredjelandsöverföringar under 2025 har identifierats och därav har användning av överföringsverktyg ej bedömts.
Har personuppgiftsansvarig gjort en nödvändig bedömning, ”Transfer Impact Assessment” (TIA), avseende tredjelandsöverföringar?	NA	Inga nya kända tredjelandsöverföringar under 2025 har identifierats och därav har ingen TIA genomförts.

Övrigt att rapportera

I tidigare årsrapporter har även informationssäkerhetsrisker identifierats och rapporterats. Dataskydd utgör del av informationssäkerhetsarbetet. Rollen dataskyddsombud är fristående och bör därför särskiljas från informationssäkerhet som inte berör personuppgifter.

Dataskyddsförordningen trädde i kraft år 2018. Tidigare har dataskyddsombudets uppdrag huvudsakligen bestått i att granska den personuppgiftsansvariges dataskyddsarbete och därefter återrapportera resultaten. Några särskilda insatser för kunskapshöjning inom området har tidigare inte genomförts. Dataskyddsarbetet har inte varit integrerat i verksamhetens ordinarie arbetsprocesser.

Under 2025 har SVOA genomfört omfattande insatser inom dataskyddsområdet. Dessa har bland annat innefattat kartläggning och genomlysning av samtliga personuppgifts-behandlingar i verksamhetens system, genomförande av konsekvensbedömningar samt upprättande av personuppgiftsbiträdesavtal. Därutöver har stödmaterial, såsom avtals- och analysmallar tagits fram och utbildningsinsatser har genomförts för flera olika målgrupper.

Därutöver vill dataskyddsombudet uppmärksamma ett antal risker utöver de sex obligatoriska områdena. Ingen omedelbar åtgärd krävs, men det bedöms ändå viktigt att uppmärksamma riskerna till personuppgiftsansvarig.

Nedan redovisas övriga risker utöver ovan obligatoriska kontrollfrågor från staden.

Risk	Risknivå	Kommentarer
Risk 1 - Olika personuppgiftsansvariga SVOA består av tre juridiska personer: Stockholm Vatten och Avfall AB, Stockholm Vatten AB och Stockholm Avfall AB. Enligt GDPR tolkas SVOA som tre personuppgiftsansvariga. Flertal personuppgiftsbehandlingar ansvaras dessutom av SVOA, men där det är Stockholms stad som styr ändamål och medel som är ytterligare en egen personuppgiftsansvarig. Komplexiteten i gränsdragningen av personuppgiftsansvaret medför att kontroll och ansvar försvåras. I händelse av tillsyn kommer SVOA ha svårt att redogöra för detta.		Risken bedöms inte försvåra SVOAs löpande personuppgiftshantering utan att det är administrativt svårt att redogöra för vem som är personuppgiftsansvarig för vilka personuppgiftsbehandlingar samt ger en förhöjd risk för reprimand och/eller sanktion i samband med tillsyn. Personuppgiftsansvarig rekommenderas att ha en strategi och inriktning för att åtgärda risken eller acceptera den. Dataskyddsombudet rekommenderar att acceptera risken eller att personuppgifts-ansvarig tillsammans med övriga bolag och förvaltningar inom kommun-koncernen beslutar om en viljeriktning hur det gemensamma eller separata personuppgiftsansvaret ska se ut.

Risk 2 - Geopolitisk omvärld Den geopolitiska omvärlden innebär att enskilda personuppgiftsansvariga behöver förhålla sig till både teknokratin och den politiska viljan från Stockholms stad, Sverige och EU. Ett digitalt beroende kan skapa inlåsningseffekter utan möjlighet till anpassning av dataskyddet vid förändringar i geopolitiken.		Personuppgiftsansvarig rekommenderas att acceptera risken eller ha en strategi och plan för plötsliga förändringar som ska inkludera olika typfall av förändringar och hur förändringar/anpassningar kan aktiveras.
Risk 3 - Leverantör- och systeminlåsningar Personuppgifter (och även annan information) är oftast bunden till system eller leverantör. Det finns en risk att SVOA är beroende av externa parter för att bedriva verksamhet och att skydda personuppgifter på rätt sätt.		Personuppgiftsansvarig rekommenderas att acceptera risken eller att kartlägga och identifiera hur leverantörsberoenden ser ut. Analysera risker och konsekvenser vad leverantörs- och systeminlåsningar innebär för SVOA och redovisa ett förslag till åtgärdsplan för personuppgiftsansvarig att besluta om.
Risk 4 – Säkerhet i leverantörskedjan Personuppgifter (och även annan information) lagras och hanteras internt, externt, i licensformat och i stadsgemensamma tjänster. One-size-fit-all-principen där personuppgiftsansvarig köper, nyttjar/avropar system/ licenser/tjänster innebär många gånger effektivisering. Dock innebär det också en förhöjd risk att skyddet av personuppgifter inte är tillräcklig eller utgått ifrån grundbehovet.		I nuläget bedöms risken inte utgöra några direkta hot. Det är däremot en risk där det finns flera gränsytor där incidenter kan inträffa och det innebär också en gränsyta där tillsyn kan ske som in sin tur ger reprimander och tillsyn. Personuppgiftsansvarig rekommenderas upprätta en plan och strategi för att omhänderta risken, eller att acceptera risken.