
Styrelsehandling 12

Utfärdat 2025-05-08

Ärendenummer STJ-2025-00073

Handläggare

Louise Ternlind

Telefon: 031-7738382

E-post: louise.ternlind@storningsjouren.goteborg.se

Åtgärdsplan för dataskyddsarbetet 2025

Informationsärende

Styrelsen Störningsjouren i Göteborg AB

Åtgärdsplan för dataskyddsarbetet 2025 föreslås antecknas.

Sammanfattning

I Dataskyddsombudets årsrapport för dataskyddsarbetet 2024 lämnades två rekommendationer till bolaget. Med detta ärende informeras styrelsen om status på åtgärder för dataskyddsarbetet i 2024–2025 års kontrollplan samt åtgärdsplan för ett förstärkt dataskydd 2025 och Dataskyddsombudets kontrollplan för dataskyddsarbetet 2025–2026.

Bedömning ur ekonomisk, ekologisk och social dimension

Bolaget inte har funnit några särskilda aspekter på frågan utifrån dessa dimensioner.

Samverkan

Ärendet anses inte vara föremål för samverkan

Ärendet

Ärendet är en återkoppling till styrelsen om vilka åtgärder bolaget har planerat utifrån dataskyddsombudets rekommendationer i årsrapporten för 2024.

Beskrivning av ärendet

Dataskyddsombudet har inkommit med en årsrapport för år 2024 avseende bolagets dataskyddsarbete samt med bedömt nuläge. I årsrapporten ges bolaget rekommendationer och förslag på fokusområden för dataskyddsarbetet framöver.

Med detta ärende informeras styrelsen dels om status på de åtgärder som ingick i bolagets åtgärdsplan för dataskyddsarbetet 2024–2025, dels om de åtgärder bolaget har planerat för 2025 för ett förstärkt dataskydd samt Dataskyddsombudets kontrollplan för dataskyddsarbetet 2025–2026

Bilagor

1. Åtgärdsplan för dataskyddsarbetet 2025
2. Dataskyddsombudets kontrollplan för dataskyddsarbetet 2025-2026

Handläggarens namn

Louise Ternlind

Befattning

Dataskyddskontakt

Chefens namn

Sofia Gärdsfors

Befattning

Vd

Åtgärdsplan dataskyddarbetet 2025

Uppföljning av genomförda åtgärder i 2024–2025 års kontrollplan

Kontrollpunkt	DSO rekommendation i årsrapport 2023	Bolagets åtgärdsplan 2024–2025	Status och kommentar
4 Register över personuppgifts-behandlingar	Gör en översyn av befintligt register. Gå igenom hur de dokumenterade behandlingarna är definierade och för respektive behandling kontrollera att informationen uppfyller kraven enligt artikel 30 i GDPR. Kontrollpunkt 4 kommer att följas upp i årsrapport 2025.	Under 2024 påbörjade bolaget en översyn och omarbetning av behandlingsregistret. Dataskyddsombudet har i 2024 års granskning erhållit information om bolagets åtgärdsplanering. Pågår	Omarbetning av behandlingsregistret pågår. Bolaget har att ta hänsyn till det planerade införandet av kommungemensamt systemstöd för hanteringen. SLK:s dataskyddsfunktion, Intraservice Införandeprojektet för systemstöd samt den koncerngemensamma dataskyddsgruppen arbetar parallellt för att säkerställa enhetlig struktur och förutsättningar för import till nya systemstödet, vilket beräknas vara slutfört 2025-12-31 Pågår – beräknas klart 2026
7 Informationsplikt	Se över samtliga delar i den information som lämnas till de registrerade och de arbetssätt som tillämpas för att säkerställa att informationsplikten gentemot de registrerade uppfylls. I arbetet behöver de rekommendationer som tidigare lämnats kopplat till den specifika informationen i integritetspolicyn omhändertas. DSO följer bolagets arbete med kontrollpunkt 9 men kommer inte att särskilt följa upp i årsrapport 2025.	Behandlingsregistret ligger till grund för informationen till registrerade. I takt med att behandlingsregistret uppdateras kommer informationen till registrerade uppdateras. Pågår	Omhändertagandet av rekommendationen är försenad med hänsyn till kontrollpunkt 4 (se kommentar ovan) då översyn och uppdatering av behandlingsregistret är en förutsättning för att utveckla informationen till registrerade. Utveckling av enhetlig struktur och innehåll för information till registrerade pågår i den koncerngemensamma dataskyddsgruppen och beräknas vara slutfört 2025-12-31. Pågår - beräknas klart 2026

9 Konsekvens- bedömning/samråd	I takt med att behandlingsregistret uppdateras se över genomförda konsekvensbedömningar och ta fram en handlingsplan för hanteringen för arbetet med att uppdatera och/eller ta fram nya konsekvensbedömningar. Fokus på arbetet ska vara på de behandlingar som kan innebära höga risker för de registrerade. DSO följer bolagets arbete med kontrollpunkt 9 men kommer inte att särskilt följa upp i årsrapport 2025.	I takt med att behandlingsregistret uppdateras identifieras behandlingar som ska konsekvensbedömas. Bolagets kärnverksamhet och HR-området kommer att prioriteras. Pågår	Under 2024 har arbetet med konsekvensbedömningar av behandlingar i kärnverksamheten påbörjats. En första avstämning med DSO genomförs våren 2025. I takt med att behandlingsregistret uppdateras identifieras behandlingar som kan innebära höga risker för registrerade och som är föremål för konsekvensbedömning. Pågår
--------------------------------------	---	--	---

Åtgärdsplan för ett förstärkt dataskydd 2025

I tabellen nedan framgår de rekommendationerna som Dataskyddsombudet lämnar i årsrapporten 2024. I tabellen framgår hur bolaget bedömer statusen på aktiviteterna och vad som avses att ytterligare åtgärdas under 2025

Detta är områden som dataskyddsombudet särskilt kommer att följa upp 2025.

Kontrollpunkt	DSO rekommendation i årsrapport 2024	Status	Bolagets åtgärdsplan 2025
1 Dataskydds- organisationen	Se över hur verksamheten kan involvera dataskyddsombudet mer regelbundet i arbetet med dataskydd, med syfte att säkerställa att bolaget uppfyller kravet enligt artikel 38.1 i GDPR gällande att dataskyddsombudet ska involveras i alla frågor som gäller dataskydd.	Klart	Artikel 38.1 <i>Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.</i> I samband med genomgång av årsrapport 2024 träffades en överenskommelse att involvera dataskyddsombudet regelbundet för avstämningar om pågående dataskyddsarbete. Under våren är fokus på behandlingsregister och bedömning av risk för behandlingar i bolagets kärnverksamhet. Rekommendationen bedöms omhändertagen. Klart 2025

	I rekommendationen ingår det att säkerställa att det finns dokumenterade arbetssätt för hur dataskyddsombudet involveras.	Pågår	Under 2025 revideras bolagets styrande dokument avseende dataskyddsarbetet, inkluderat dokumenterade arbetssätt för hur bolaget involverar dataskyddsombudet. Pågår – beräknas klart 2025-12-31
4 Register över personuppgifts- behandlingar	Ta del av granskningsrapporten från dataskyddsombudets fördjupade kontroll och omhändertar rekommendationerna som framgår av granskningsrapporten	Pågår	Ett större omtag av behandlingsregistret pågår. SLK:s dataskyddsfunktion, Intraservice Införandeprojektet för systemstöd samt den koncerngemensamma dataskyddsgruppen arbetar parallellt för att säkerställa enhetlig struktur och förutsättningar för import till nya systemstödet, vilket beräknas vara slutfört 2025-12-31. Pågår - beräknas klart 2026

Bolagets bedömning

Bolaget bedömer att de åtgärder som bolaget redan åtgärdat och planerar för och som framgår i ovan åtgärdsplan för 2025 omhändertar de rekommendationer som dataskyddsombudet lämnat i årsrapporten för 2024. På sikt bedöms detta att bidra till ett förstärkt dataskydd.



Kontrollplan för dataskyddsarbetet 2025–2026

Förvaltningar och bolag i Göteborgs Stad

2025-02-26

Innehåll

1	Bakgrund.....	3
1.1	Ändrad utformning av den övergripande kontrollen 2025.....	3
2	Kontrollarbetet 2025–2026	4
2.1	Kontrollarbetets delar	4
2.1.1	Övergripande kontroll	4
2.1.2	Fördjupad kontroll.....	5
2.1.3	Uppföljning	5
2.2	Tidplan för kontrollarbetet 2025–2026	5
3	Rapportering.....	6
3.1	Årsrapport	6
3.2	Särskilt yttrande.....	6
Kontakt		7
	Bilaga 1 - Beskrivning av fasta kontrollpunkter	8

1 Bakgrund

Att få ta del av och hantera andra människors personliga uppgifter på ett sådant sätt som kommunala förvaltningar och bolag gör innebär att förvalta ett stort förtroende. Dataskyddsförordningen (GDPR) har tillkommit för att särskilt värna om den enskildes rätt till integritet och kontroll över vad som sker med ens personuppgifter. Att förvaltningar och bolag hanterar personuppgifter i enlighet med gällande lag bör vara en självklarhet i syfte att visa omsorg om det förtroende som givits den som har att hantera personuppgifter.

Det är varje nämnd och bolaget som är ytterst ansvarig för att dess verksamhet följer dataskyddslagstiftningen. För att stödja stadens nämnder och bolag i arbetet med dataskydd har ett dataskyddsombud utsetts. I Göteborgs Stad fullgör dataskyddsenheten på Intraservice uppdraget som dataskyddsombud. Dataskyddsombudet har särskild sakkunskap i dataskyddslagstiftning och arbetar bland annat för att hålla nämnden/bolaget informerade om hur verksamheten lever upp till dataskyddslagstiftningen. Vad som är dataskyddsombudets uppgifter framgår direkt av GDPR. En av dessa uppgifter är att övervaka att stadens förvaltningar och bolag följer dataskyddslagstiftningen. När dataskyddsombudet kontrollerar efterlevnaden av dataskyddslagstiftningen sker det bland annat genom att samla in information om hur personuppgifter behandlas inom en verksamhet och genom att kontrollera hur bestämmelser och interna styrdokument som styr dataskyddsarbetet efterlevs.

1.1 Ändrad utformning av den övergripande kontrollen 2025

Med anledning av den omorganisation som genomfördes hösten 2024, där tre tjänster flyttades från dataskyddsenheten till stadsledningskontorets dataskyddsfunktion, har dataskyddsenheten behövt arbeta om strukturen för kontrollarbetet. Under 2024 visades det genom ett ändrat upplägg för den fördjupade kontrollen, och under 2025 kommer det visas genom ändringar i utformningen av den övergripande kontrollen.

Den övergripande kontrollen kommer fortfarande att genomföras inom alla verksamheter under hösten 2025, men dess utformning och omfattning kommer att skilja sig från tidigare år. Ändringarna syftar till att öka kvaliteten i kontrollen och möjliggöra för mer systematisk uppföljning av verksamheternas dataskyddsarbete.

Dataskyddsenheten kommer innan kontrollen genomförs att skicka ut information om ändringarna till verksamheterna.

2 Kontrollarbetet 2025–2026

Den övergripande och viktigaste uppgiften för dataskyddsombudet är att övervaka att organisationen följer dataskyddsförordningen. I Göteborgs Stad innebär detta bland annat att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom förvaltningar och bolag. För dataskyddsombudet är kontrollarbetet ett sätt att få en bild av vilka risker och/eller brister som eventuellt föreligger inom en verksamhet. Genom kontroller kan dataskyddsombudet kartlägga verksamhetens dataskyddsarbete, och denna kartläggning kan sedan användas som ett stöd av verksamheten i dess fortsatta arbete med dataskydd. Dessa kontroller specificeras genom denna kontrollplan, som syftar till att informera personuppgiftsansvariga om upplägg och tidplan för kontrollarbetet åren 2025 och 2026. Dataskyddsombudets kontrollarbete löper över tvåårsperioder. En ny kontrollplan skickas ut årligen, vilken omfattar både innevarande och nästkommande kalenderår.

Syftet med att arbeta utefter en på förhand fastställd kontrollplan är att det ska bidra till att sätta fokus på verksamhetens dataskyddsarbete och därmed:

1. Säkerställa ett kontinuerligt dataskyddsarbete som skapar förutsättningar för efterlevnad av förordningen.
2. Uppmuntra ett riskbaserat arbetssätt och därigenom minimera risken för lagbrott.
3. Göra dataskyddsarbetet till en integrerad del i verksamhetens informationssäkerhetsarbete.

2.1 Kontrollarbetets delar

Kontrollarbetet består av tre delar som tillsammans syftar till att ge, såväl dataskyddsombud som personuppgiftsansvariga, en överblick över verksamhetens dataskyddsarbete och dess följsamhet gentemot GDPR.

2.1.1 Övergripande kontroll

Den övergripande kontrollen utgår från principerna om inbyggt dataskydd och dataskydd som standard (enligt artikel 25 i GDPR). Verksamhetens följsamhet mot förordningen beror till stor del på hur väl dessa principer har integrerats i ordinarie arbetsprocesser. Med principerna som utgångspunkt har tolv kontrollpunkter identifierats. Dessa är av både teknisk och organisatorisk karaktär och är gemensamma för alla verksamheter inom Göteborgs Stad.

Den övergripande kontrollen genomförs genom en enkät inom vilken verksamhetens dataskyddsarbete kartläggs. Resultaten från enkäten är tänkt att ge en generell ögonblicksbild för respektive kontrollpunkt och kan därför, förutsatt att enkäten är korrekt ifylld, användas som vägledning för verksamheten i sitt dataskyddsarbete. Syftet är att få till ett långsiktigt och systematiskt arbetssätt, samt åskådliggöra de förändringar som vidtas över tid.

För beskrivning av de olika kontrollpunkterna, se bilaga 1.

2.1.2 Fördjupad kontroll

I utformningen av den fördjupade kontrollen utgår dataskyddsombudet från de risker som identifierats, både inom enskilda verksamheter och på en övergripande nivå. Hänsyn tas även till vad som bedöms kunna få störst effekt för flest verksamheter inom Staden. Från och med 2024 är den fördjupade kontrollen utformad som en stickprovskontroll vilket innebär att inte alla verksamheter kontrolleras. I stället genomförs kontrollen inom ett antal förvaltningar och bolag som dataskyddsombudet anser utgör ett representativt urval för stadens verksamheter.

Resultaten från kontrollen redovisas dels på verksamhetsnivå genom en rapport till respektive deltagande verksamhet, dels på övergripande nivå genom en staden gemensam rapport. Den staden gemensamma rapporten är tänkt att kunna användas av flera verksamheter och genom denna kan även de verksamheter som ej varit med i kontrollen dra nytta av resultaten.

2.1.3 Uppföljning

Uppföljning av de rekommendationer som tidigare lämnats till verksamheten i samband med årsrapportering eller fördjupade kontroller genomförs årligen. Resultatet redovisas till styrelse eller nämnd i verksamhetens årsrapport.

2.2 Tidplan för kontrollarbetet 2025–2026

I tabellerna nedan anges huvuddragen i kontrollarbetet för åren 2025–2026 för stadens förvaltningar och bolag.

2025	Aktivitet
Februari	Kontrollplan för 2025–2026 lämnas till nämnder och styrelser.
September	Övergripande kontroll genomförs.
November – december	Genomgång av innehåll i årsrapport med respektive verksamhet.
December	Dataskyddsombudets årsrapport översänds till nämnd eller styrelse.

2026	Aktivitet
Februari	Kontrollplan för 2026–2027 lämnas till nämnder och styrelser.
April – Oktober	Fördjupad kontroll genomförs.
November – december	Genomgång av innehåll i årsrapport med respektive verksamhet.
December	Dataskyddsombudets årsrapport översänds till nämnd eller styrelse.

3 Rapportering

3.1 Årsrapport

Det är nämnd respektive bolag som har det yttersta ansvaret för att verksamheten följer dataskyddslagstiftningen och dataskyddsombudet ska enligt lag rapportera om detta till högsta förvaltningsnivå. Därför sammanställer dataskyddsombudet årligen en rapport om verksamhetens dataskyddsarbete. I rapporten redogörs för eventuella risker och brister som dataskyddsombudet har identifierat. I rapporten redogörs också för de råd och rekommendationer som dataskyddsombudet har lämnat. För att möjliggöra en direkt kommunikation mellan dataskyddsombud och högsta ansvarsnivå inom verksamheten ska årsrapporten tillhandahållas nämnd respektive bolagsstyrelse.

3.2 Särskilt yttrande

Dataskyddsombudet kan i vissa situationer komma att rikta ett särskilt yttrande till högsta ansvarsnivå. En sådan situation kan vara om dataskyddsombudet har identifierat höga risker för de registrerade som kräver omgående åtgärder från ansvarig nämnd/bolag. Det kan också vara om dataskyddsombudet uppmärksammar att det inom verksamheten fattats beslut som är oförenliga med dataskyddslagstiftningen och dataskyddsombudets råd.

Kontakt

Frågor avseende kontrollplanen hänvisas till dataskyddsenhetens funktionsbrevlåda; dso@intraservice.goteborg.se.

Bilaga 1 - Beskrivning av fasta kontrollpunkter

Kontrollpunkt 1: Dataskyddsorganisation

Kontrollpunkten avser verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete och omfattar bland annat verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet.

Kontrollpunkt 2: Personuppgiftsincidenter

Kontrollpunkten avser verksamhetens förutsättningar för att identifiera och hantera personuppgiftsincidenter. För att uppfylla ansvarsskyldigheten bör verksamhetens rutin för hanteringen vara dokumenterad. I de fall verksamheten är både personuppgiftsansvarig och personuppgiftsbiträde bör rutinen omfatta båda scenarier. I kontrollpunkten ingår även översyn av verksamhetens rutin för att bedöma incidenter, hantering av eventuell anmälan till tillsynsmyndigheten, samt hur rutinerna tillgängliggörs och kommuniceras inom verksamheten. Även efterlevnad av verksamhetens dokumentationsskyldighet, att alla inträffade personuppgiftsincidenter registreras, innefattas.

Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

Kontrollpunkten avser verksamhetens dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd och förutsätter att verksamheten har identifierat samt registrerat personuppgiftsbiträden i personuppgiftsregistret. Även verksamhetens rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas.

Kontrollpunkt 4: Register över personuppgiftsbehandlingar

Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med, och rutin för, att säkerställa ett uppdaterat och heltäckande register innefattas.

Kontrollpunkt 5: Övergripande styrning av dataskyddsarbetet

Kontrollpunkten avser verksamhetens övergripande styrning för att arbeta med dataskydd. Tydlig styrning sätter ramarna för arbetet med dataskydd och främjar ett riskbaserat arbetssätt. Kontrollpunkten innefattar även verksamhetens arbete för att integrera dataskyddsfrågorna i det övriga informationssäkerhetsarbetet, samt hur verksamheten arbetar med egna interna kontroller för att säkerställa att dataskyddslagstiftningen efterlevs.

Kontrollpunkt 6: Utbildning

Kontrollpunkten avser verksamhetens arbete med att utbilda och upprätthålla kunskapsnivån i dataskyddsfrågor hos anställda.

Kontrollpunkt 7: Informationsplikt

Kontrollpunkten avser hur väl verksamheten uppfyller principen om öppenhet och kravet på att lämna information till de registrerade om hur deras personuppgifter behandlas. Punkten omfattar även hur verksamheten säkerställer att informationen är uppdaterad.

Kontrollpunkt 8: E-post och dokumenthantering

Kontrollpunkten avser verksamhetens rutiner för e-post och dokumenthantering. I detta är en aktuell och fastställd dokumenthanteringsplan med gallringsbeslut en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddslagstiftningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Kontrollpunkt 9: Konsekvensbedömning/samråd

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras samt genomföra denna. Även verksamhetens rutiner för arbetet med konsekvensbedömningar samt hur dataskyddsombudet involveras i arbetet ingår. Därtill tillkommer verksamhetens rutin för att hantera de risker som identifieras i konsekvensbedömningen, samt hur genomförda konsekvensbedömningar följs upp och hålls aktuella.

Kontrollpunkt 10: IT-projekt och upphandling

Kontrollpunkten avser verksamhetens organisation och rutiner för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår till exempel hur verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster.

Kontrollpunkt 11: IT-system och digitala verktyg

Kontrollpunkten avser verksamhetens rutiner för att säkerställa att verksamhetens personuppgiftshantering inom ramen för IT-system och digitala verktyg är förenlig med dataskyddslagstiftningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår även.

Kontrollpunkt 12: Hantering av registrerades rättigheter

Kontrollpunkten avser verksamhetens förutsättningar för att hantera de registrerades rättigheter. En förutsättning för att verksamheten ska kunna hantera de registrerades rättigheter är att man har en process och rutiner för arbetet, så att den registrerades personuppgifter enkelt kan lokaliseras vid efterfrågan. Även verksamhetens rutin för att hantera ett tillbakadragande av samtycke ingår i kontrollpunkten.