

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12

Ärende/Dok. id.
TN 2026-0103

Infosäk. klass
K1 (Öppen)

Handläggare
Johanna Wallerström

Dataskyddsombudets övergripande kontroll av dataskyddsarbetet under verksamhetsåret 2025

Region Stockholm
Trafikförvaltningen
105 73 Stockholm

Leveransadress:
Lindhagensgatan 100
Godsmottagningen
112 51 Stockholm

Telefon: 08-123 316 00
Fax: 08-123 316 06
registrator.tf@regionstockholm.se

Säte: Stockholm
Org.nr: 232100-0016
www.regionstockholm.se

Besök oss: Lindhagensgatan 100. Kommunikationer: Stadshagen/Thorildsplan

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

Innehållsförteckning

1	Sammanfattning	3
2	Inledning.....	4
2.1	<i>Bakgrund</i>	4
2.2	<i>Syfte</i>	4
2.3	<i>Avgränsning</i>	4
3	Kontrollområden	5
3.1	<i>Organisation och ansvar</i>	5
3.2	<i>Styrande dokument</i>	11
3.3	<i>Registerförteckning</i>	13
3.4	<i>Konsekvensbedömningar och förhandssamråd</i>	17
3.5	<i>Registrerades rättigheter</i>	20
3.6	<i>Personuppgiftsincidenter</i>	26
3.7	<i>Tekniska och organisatoriska säkerhetsåtgärder</i>	31
3.8	<i>Personuppgiftsbiträden och avtal</i>	36
3.9	<i>Överföring av personuppgifter utanför EU/EES</i>	39
3.10	<i>Interna utbildningar och medvetenhet</i>	41

1 Sammanfattning

Dataskyddsombudets bedömning är att Trafiknämnden, AB Storstockholms Lokaltrafik ("AB SL") och Waxholms Ångfartygs AB ("WÅAB") har en väl fungerande struktur för dataskyddsarbetet. De grundläggande beståndsdelarna som krävs för att uppnå efterlevnad av dataskyddsförordningen¹ finns på plats, så som en dataskyddsorganisation, en registerförteckning samt processer och rutiner för att hantera registrerades rättigheter, personuppgiftsincidenter och andra dataskyddsfrågor. Det finns dock kvarvarande brister inom dataskyddsområdet. De brister som har bedömts allvarligast är:

- **Registerförteckningen är inte komplett**, dels eftersom dokumenterade personuppgiftsbehandlingar inte innehåller samtliga nödvändiga uppgifter, dels för att flera personuppgiftsbehandlingar saknas.
- **Registrerade informeras inte alltid om behandling av personuppgifter**, exempelvis saknas information för besökare vid spårvägmuseet, medarbetare på Trafikförvaltningen samt medarbetare hos trafikutövare och externa tjänsteleverantörer.
- **Dataskyddsfunktionen saknar förmåga att kontrollera folkbokföringsadress och förmåga att tillhandahålla registerutdrag i ett elektroniskt format på ett säkert sätt**, i samband med handläggning av registrerades rättigheter.
- **Det saknas övergripande styrning för inbyggt dataskydd och dataskydd som standard.**

Dataskyddsombudet vill även nämna ett par andra brister som i sig har bedömts som mindre allvarliga men som, på grund av sin återkommande karaktär, är allvarliga. Dessa är:

- **Rutiner för kontroll och uppföljning är bristande**, avseende exempelvis registerförteckningen, personuppgiftsincidenter, behörighetsrevidering, personuppgiftsbiträdesavtal och genomförda utbildningar.
- **Styrande dokument är inte giltiga, uppdaterade och lättillgängliga.**

Rapporten innehåller en närmare beskrivning av bristerna. Där framgår också andra brister och risker samt dataskyddsombudets rekommendationer.

¹ Europaparlamentets och rådets förordning (EU) 2026/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

2 Inledning

2.1 Bakgrund

Dataskyddsombudet har enligt dataskyddsförordningen i uppdrag att övervaka efterlevnaden av dataskyddsarbetet inom organisationen. Rollen innebär att självständigt och oberoende granska hur personuppgifter behandlas, ge råd till verksamheten samt fungera som kontaktpunkt för registrerade och Integritetsskyddsmyndigheten.

Som en del i detta uppdrag genomför dataskyddsombudet varje år en övergripande granskning av dataskyddsarbetet. Denna granskning har tidigare presenterats inom ramen för dataskyddsombudets årsrapport. I år redovisas denna granskning i en separat granskningsrapport som biläggs årsrapporten. Vidare har ett antal kontrollfrågor identifierats som är avsedda att användas varje år. Syftet är att underlätta jämförelser över tid.

2.2 Syfte

Granskningen syftar till att ge en samlad bild av organisationens dataskyddsarbete, hur efterlevnaden utvecklas över tid och om det finns områden som behöver förbättras.

Granskningen ska:

- belysa brister och risker som kan påverka skyddet av personuppgifter eller organisationens regelefterlevnad,
- synliggöra förbättringsbehov, och
- ge personuppgiftsansvariga underlag och rekommendationer för styrning och vidare utveckling av dataskyddsarbetet.

2.3 Avgränsning

Denna rapport omfattar Trafiknämnden (i de delar som Trafikförvaltningen utför på nämndens uppdrag), AB SL samt WÅAB. Om inte annat anges avser redovisningen samtliga tre personuppgiftsansvariga. Inom Trafiknämndens ansvarsområde ingår även "varumärkena" Färdtjänst och Spårvägmuseet. Dessa ingår därför i den del av rapporten som rör nämnden och kommenteras vid behov separat.

Samtliga kontrollfrågor har inte besvarats, eller endast besvarats delvis. Den främsta orsaken är att vissa kontroller av olika skäl har varit svåra att följa upp, i kombination med begränsad tid för att genomföra sådana kontroller. Frågorna behålls dock för att säkerställa spårbarhet och möjliggöra uppföljning över tid.

3 Kontrollområden

3.1 Organisation och ansvar

3.1.1 Bakgrund

Enligt dataskyddsförordningen ska den personuppgiftsansvarige kunna säkerställa och visa att personuppgifter behandlas i enlighet med regelverket. En grundläggande förutsättning för detta är att organisationen har en ändamålsenlig och tydligt utformad organisation. Detta följer av principen om ansvarsskyldighet i artikel 5.2, som innebär att den personuppgiftsansvarige inte bara ska följa principerna i förordningen utan också kunna visa hur de efterlevs i praktiken.

3.1.2 Kontrollfrågor och svar

Ref.	Kontrollfråga	Svar
A	<p>Har nödvändiga roller enligt dataskyddsförordningen identifierats?</p> <p><i>Enligt dataskyddsförordningen ska organisationer som behandlar personuppgifter säkerställa att vissa grundläggande roller finns. De centrala rollerna är:</i></p> <ul style="list-style-type: none"> • Personuppgiftsansvarig som är den organisation eller juridiska person som bestämmer ändamål och medel med personuppgiftsbehandlingen, dvs. varför och hur personuppgifter ska behandlas. • Personuppgiftsbiträde som är den organisation/juridiska person som behandlar personuppgifter för den personuppgiftsansvariges räkning och enligt dennes instruktioner. 	<p>Delvis.</p> <p>Personuppgiftsansvariga Trafiknämnden, AB SL och WÅAB är personuppgiftsansvariga. Det är dock inte alltid tydligt vem av dessa som ska vara personuppgiftsansvarig i olika sammanhang. I praktiken fattas de flesta besluten om ändamål och medel av Trafikförvaltningen.</p> <p>Vidare är det många gånger oklart vilken nämnd inom regionen som ska vara personuppgiftsansvarig. En vanlig situation är att Regionstyrelsen beslutar om att alla nämnder/förvaltningar ska använda ett visst it-system. Det talar för att det är de som beslutat om ändamål och medel och därmed ska ses som personuppgiftsansvariga. Ändå bedöms i regel respektive nämnd och bolag vara separat personuppgiftsansvariga.</p> <p>Sammanfattningsvis saknas det tydliga principer för hur personuppgiftsansvaret ska fördelas inom Region Stockholm och i</p>

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

	<ul style="list-style-type: none"> • Dataskyddsbud som är en roll som vissa organisationer måste utse, till exempel myndigheter och andra offentliga organ. Dataskyddsbudet ska vara oberoende och ge råd samt kontrollera att organisationen följer dataskyddsförordningen. Ombudet fungerar också som kontaktpunkt för de registrerade och Integritetsskyddsmyndigheten. <p>Av Reglementen för Regionstyrelsen och övriga nämnder² framgår att respektive nämnd ska utse ett dataskyddsbud.</p>	<p>synnerhet mellan Trafiknämnden och dess aktiebolag.</p> <p>Personuppgiftsbiträde Samtliga personuppgiftsansvariga upprättar personuppgiftsbiträdesavtal med sina leverantörer som behandlar personuppgifter för deras räkning. Grundläggande rutiner för att identifiera och ingå avtal med personuppgiftsbiträden finns.</p> <p>Dataskyddsbudet Trafiknämnden har utsett två dataskyddsbud. Ett för den verksamhet som Trafikförvaltningen utför och ett för den verksamhet som Förvaltning för utbyggd tunnelbana utför. Det dataskyddsbud som är utpekad för Trafikförvaltningen är även dataskyddsbud för AB SL och WÅAB.</p> <p>Dataskyddsbudet ska ha en oberoende ställning. Då det historiskt har varit få resurser som har arbetet med dataskydd har dataskyddsbudet varit den som i praktiken utfört många av de arbetsuppgifter som åligger personuppgiftsansvarig. Dataskyddsbudet har därför inte haft en oberoende ställning, utan har till stor del granskat sitt eget arbete.</p> <p>Under året har dock en dataskyddsfunktion skapats. Det har skapat bättre förutsättningar för dataskyddsbudet att framgent agera oberoende i rollen. Dataskyddsbudet är placerad i dataskyddsfunktionen.</p>
--	--	---

² Reglementen för regionstyrelsen och övriga nämnder, beslutad av regionfullmäktige 2022-12-06, RS 2022-0762 och RS 2022-0482.

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

B	<p>Har övriga roller (än de som följer direkt av lag) som behövs för att efterleva kraven i dataskyddsförordningen identifierats och definierats?</p>	<p>Ja. Av riktlinje för informationssäkerhet och dataskydd³ framgår att varje nämnd och bolag ska ha en funktion (en eller flera personer) som har i uppgift att samordna och följa upp arbetet med dataskydd inom den egna organisationen.</p> <p>Av Trafikförvaltningens arbetsordning⁴ framgår att it-avdelningen har funktionsansvar för informationssäkerhet och dataskydd. I it-avdelningens arbetsordning utvecklas vad funktionsansvaren innebär.</p> <p>Sedan i år finns en dataskyddsfunktion inom Trafikförvaltningen som stöttar Trafiknämnden, AB SL och WÅAB i utförandet av personuppgiftsansvaret.</p> <p>Av nu gällande arbetsordning framgår även att varje avdelning har tilldelats ett ansvarsområde och att ansvarsområden som ingår i uppdraget benämns <i>verksamhetsansvar</i>. Vidare framgår att verksamhetsansvaret innebär att leda, styra, följa upp och utveckla verksamheten i enlighet med gällande författningar och lagar, Trafikförvaltningens styrande dokument, gemensamma processer och rutiner samt uppdrag, fastställda mål och budget.</p> <p>I en rollbeskrivning rörande informationsägare fastslås även att Trafikförvaltningens information och informationstillgångar ska ha en informationsägare och att informationsägarskapet följer av verksamhetsansvaret så som det är</p>
---	---	--

³ Riktlinje för informationssäkerhet samt dataskydd, beslutad av regionfullmäktige den 9 december 2025, diarienummer RD 2025-0418.

⁴ Trafikförvaltningens arbetsordning, fastställd 2025-11-03, TN-S-3144190.

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		<p>definierat i förvaltningens övergripande respektive avdelningsvisa arbetsordningar. Vidare framgår det att informationsägaren är ytterst ansvarig för personuppgiftshanteringen inom sin verksamhet, vilket bland annat innebär att hen ansvarar för att dokumentera personuppgiftsbehandlingarna, upprätta och förvalta personuppgiftsbiträdesavtal, genomför konsekvensbedömningar och anmäla personuppgiftsincidenter till Integritetsskyddsmyndigheten.</p> <p>Det är alltså den som är verksamhetsansvarig som även är informationsägare och därmed ansvarig för personuppgiftsbehandlingen inom sitt verksamhetsområde.</p> <p>Vidare kan en informationsägare fördela det praktiska arbetet till en eller flera informationsförvaltare, som stödjer informationsägaren i det operativa arbetet.</p>
C	Har personer utsetts för nödvändiga roller?	<p>Delvis. Det saknas utpekade informationsägare och informationsförvaltare för vissa personuppgiftsbehandlingar.⁵ Detta gäller samtliga personuppgiftsansvariga. Se mer om detta under 3.3.2. Övriga roller är bemannade.</p>
D	Känner de personer som har utpekade ansvar inom dataskydd till sitt ansvar?	<p>Delvis. Under slutet av 2025 gjorde dataskyddsombudet en granskning rörande informationsägarna och informationsförvaltarnas kunskap och ansvarstagande enligt dataskyddsförordningen. Nästan hälften av respondenterna angav att de anser att det är ottydligt vad rollen som informationsägare och</p>

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		<p>informationsförvaltare inom dataskydd innebär.</p> <p>Dataskyddsfunktionen har uppgett att uppdraget är tydligt efter de förtydliganden som har gjorts i it-avdelningens arbetsordning. Dock upplever funktionen att det finns förväntningar inom organisationen att funktionen ska utföra fler uppgifter, som sträcker sig utanför dataskyddsområdet.</p> <p>Dataskyddsombudet anser att sitt ansvar är tydligt definierat, eftersom det följer direkt av lag.</p>
E	Är det delegerat vilka tjänstemän inom förvaltningen som får fatta beslut relaterat till dataskydd på uppdrag av nämnden och bolagen?	Nej. Det är inte delegerat vilka beslut som är delegationsbeslut och som får fattas av medarbetare på Trafikförvaltningen på uppdrag av nämnden och bolagen. Det pågår dock ett arbete med att ta fram en ny delegationsordning och det har föreslagits ändringar för att åtgärda detta.

3.1.3 Brister och risker

Inom detta kontrollområde har följande brister och risker identifierats:

- Att det är otydligt vilken/vilka nämnder och bolag som är personuppgiftsansvarig inom regionen innebär risk för felaktig tillämpning av dataskyddsförordningen. I vissa fall aktualiseras nämligen olika bestämmelser, beroende på om nämnden som myndighet eller aktiebolagen ska anses vara personuppgiftsansvariga. Felaktig tillämpning av dataskyddsförordningen kan leda till otillbörligt integritetsintrång, klagomål, tillsyn och sanktioner.
- Att dataskyddsombudet organisatoriskt är placerad inom dataskyddsfunktion innebär risk för att dataskyddsombudet inte kan agera tillräckligt oberoende i rollen. Det kan leda till att roller och ansvar blandas samman samt bristande uppfyllande av dataskyddsförordningens krav på att dataskyddsombudet ska vara oberoende.
- Att det saknas en tydlig koppling mellan verksamhetsansvaret och informationsägarskapet direkt i arbetsordningen innebär risk att ansvariga inte känner till och tar sitt ansvar för att efterleva kraven i dataskyddsförordningen.
- Att det saknas utpekade informationsägare och informationsförvaltare för flera personuppgiftsbehandlingar innebär risk för att ingen tar ansvar för sådana

personuppgiftsbehandlingar och säkerställer att kraven enligt dataskyddsförordningen efterlevs. Det innebär även risk för otillbörligt integritetsintrång, klagomål, tillsyn och sanktioner.

- Att det saknas tydlig delegation avseende vem som får fatta beslut i ärenden relaterat till dataskydd innebär risk för otydligt ansvar samt fördröjda beslut avseende exempelvis registrerades rättigheter och hantering av personuppgiftsincidenter.

3.1.4 Dataskyddsombudets sammanfattande bedömning och rekommendationer

	Allvarlig brist/hög risk Allvarlig brist/risk som kan leda till omfattande överträdelser av dataskyddsförordningen och betydande sanktions- eller förtroenderisk.
	Betydande brist/medelhög risk Brist/risk som kan påverka efterlevnaden av dataskyddsförordningen och skapa interna problem med att efterleva processen eller svårigheter att visa ansvarsskyldigheten.
X	Mindre brist/låg risk Mindre brist eller risk med begränsad påverkan på efterlevnaden, men som bör åtgärdas för att upprätthålla en konsekvent och korrekt tillämpning av dataskyddsreglerna.
	Inga brister/risker Inga identifierade brister/risker av nämnvärd betydelse.

Sammanfattningsvis bedömer dataskyddsombudet att det finns en grundläggande organisation och ansvarsfördelning som innebär goda förutsättningar för såväl Trafiknämnden som AB SL och WÅAB att efterleva kraven i dataskyddsförordningen.

Att det råder osäkerhet kring vilken organisation som är personuppgiftsansvarig i olika situationer medför dock en osäkerhet kring vilka bestämmelser i dataskyddsförordningen som är tillämpliga. Det utgör en risk som bör åtgärdas för att upprätthålla en konsekvent och korrekt tillämpning av dataskyddsreglerna.

För att åtgärda de brister och risker som ovan har identifierats rekommenderar dataskyddsombudet:

- Att frågan om vilken organisation som bör vara personuppgiftsansvarig utreds och att det tas fram styrande principer för att fördela personuppgiftsansvaret.
- Att dataskyddsombudets placering ses över och att det övervägas att placera dataskyddsombudet utanför dataskyddsfunktionen.
- Att arbetsordningen och/eller rollbeskrivning för informationsägare förtydligas, så att samma benämningar på rollen används.

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

- Att det säkerställs att det finns utpekade informationsägare och informationsförvaltare (eller motsvarande roll) för samtliga identifierade personuppgiftsbehandlingar.
- Att det tydliggörs vem som är behörig att fatta olika typer av beslut relaterat till dataskyddsförordningen i delegationsordningen.

3.2 Styrande dokument

3.2.1 Bakgrund

Enligt artikel 5.2 dataskyddsförordningen ska den personuppgiftsansvarige kunna visa att förordningens principer efterlevs vid all behandling av personuppgifter. För att detta ska vara möjligt krävs att organisationen har dokumenterade rutiner och processer i form av styrande och stödjande dokument. Genom sådana dokument säkerställs även att verksamheten har tydlig information och kunskap om vilka regler som gäller och vilka krav som måste följas i det dagliga arbetet.

3.2.2 Kontrollfrågor och svar

Ref.	Kontrollfråga	Svar
A	Finns det nödvändiga interna styrande dokument och processer beslutade för att efterleva kraven i dataskyddsförordningen?	<p>Delvis. Inom Trafikförvaltningen finns flera styrande och stödjande dokument som beskriver hur personuppgifter ska behandlas för att uppfylla kraven dataskyddsförordningen. Exempelvis finns det styrande dokument och processer för att hantera personuppgiftsincidenter⁶, registrerades rättigheter⁷, för att hantera e-post med personuppgifter⁸, hantera förteckning över personuppgiftsbehandlingar⁹ m.m.</p> <p>Dock har merparten av de styrande dokumentens giltighetstid löpt ut i Edit och vissa dokument saknas datum för beslut och beslutsfattare. Vidare noteras att flera styrande dokument saknar tydlighet och aktualitet.</p>
B	Är dessa dokument och processer uppdaterade i linje med gällande lagstiftning?	Ja. Inga direkta felaktigheter i relation till lag har identifierats. Däremot är dokumenten inte

⁶ Processspecifikation "Hantera personuppgiftsincidenter", fastställd 2023-07-07, TN-S-1360259.

⁷ Rutinen "Hantera inkommande förfrågningar baserat på den registrerades rättigheter", fastställd 2022-05-23, TN-S-1304931.

⁸ Rutinen "Hantera e-post med personuppgifter, fastställd 2023-03-29, TN-S-1215792.

⁹ Rutinen "Hantera förteckning av personuppgiftsbehandlingar", fastställd 2023-03-20, TN-S-1217246.

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		uppdaterade och korrekta utifrån interna bestämmelser och överenskommelser.
C	Är dokumenten och processerna tillgängliga för de målgrupper till vilka de riktar sig?	Delvis. De flesta styrande dokumenten är tillgängliga och sökbara i Edit, trots att de är ogiltiga. För den som inte känner till diarienumret eller titeln på dokumentet är de dock svåra att hitta.

3.2.3 Brister och risker

Inom detta kontrollområde har följande brister och risker identifierats:

- Om styrdokument inte är giltiga, uppdaterade och lättillgängliga för målgruppen ökar risken för felaktig eller inkonsekvent hantering av personuppgifter och bristande efterlevnad av dataskyddsförordningen. Det kan även försvåra för organisationen att uppfylla principen om ansvarsskyldighet.

3.2.4 Dataskyddsombudets sammanfattande bedömning och rekommendationer

	Allvarlig brist/hög risk Allvarlig brist/risk som kan leda till omfattande överträdelser av dataskyddsförordningen och betydande sanktions- eller förtroenderisk.
	Betydande brist/medelhög risk Brist/risk som kan påverka efterlevnaden av dataskyddsförordningen och skapa interna problem med att efterleva processen eller svårigheter att visa ansvarsskyldigheten.
X	Mindre brist/låg risk Mindre brist eller risk med begränsad påverkan på efterlevnaden, men som bör åtgärdas för att upprätthålla en konsekvent och korrekt tillämpning av dataskyddsreglerna.
	Inga brister/risker Inga identifierade brister/risker av nämnvärd betydelse.

Dataskyddsombudet bedömer att det finns relevanta styrande dokument inom de viktigaste områdena, men eftersom dokumenten inte är giltiga, uppdaterade och lättillgängliga innebär det en risk som bör åtgärdas för att upprätthålla en konsekvent och korrekt tillämpning av dataskyddsreglerna.

För att åtgärda de brister och risker som ovan har identifierats rekommenderar dataskyddsombudet:

- Att se över samtliga styrande dokument inom dataskyddsområdet och säkerställa att dessa är uppdaterade, giltiga och enkla att hitta för dem som bör ha kännedom och kunskap om dem.

3.3 Registerförteckning

3.3.1 Bakgrund

Enligt artikel 30 i dataskyddsförordningen ska den personuppgiftsansvarige föra en förteckning över alla behandlingar av personuppgifter. Förteckningen är ett centralt verktyg för att uppfylla ansvarsskyldigheten och ge en samlad överblick över bland annat ändamål, kategorier av uppgifter och registrerade, mottagare, lagringstider och säkerhetsåtgärder. En korrekt och uppdaterad förteckning är en grundläggande förutsättning för att kunna säkerställa efterlevnaden av dataskyddsförordningens krav samt för att kunna tillgodose de registrerades rättigheter.

3.3.2 Kontrollfrågor och svar

Ref.	Kontrollfråga	Svar
A	Finns en förteckning över personuppgiftsbehandlingar, enligt artikel 30 dataskyddsförordningen?	Ja. Region Stockholm har under 2025 upphandlat och implementerat ett nytt systemstöd för att föra förteckning över personuppgiftsbehandlingar. Det nya systemstödet heter Iris och används av alla tre personuppgiftsansvariga.
B	Uppfyller förteckningen kraven i dataskyddsförordningen?	Ja. Systemstödet som används för att föra förteckningen motsvarar kraven i artikel 30 dataskyddsförordningen och mer därtill. Förteckningen används inte bara för att uppfylla de grundläggande kraven på förteckningen, utan även för att dokumentera och visa att även övriga krav i dataskyddsförordningen är uppfyllda.
C	Är registerförteckningen komplett? Dvs. har alla personuppgiftsbehandlingar identifierats och dokumenterats?	<p>Nej. Ingen av registerförteckningarna är kompletta.</p> <p>Trafiknämnden</p> <p>Det kan konstaterats att flera personuppgiftsbehandlingar saknas. Bland identifierade saknade personuppgiftsbehandlingar kan nämnas sådana som sker för att upptäcka och utreda oegentligheter, logguppföljning och visselblåsarkanal.</p> <p>Överlag saknas många personuppgiftsbehandlingar som rör medarbetare. Bland identifierade saknade personuppgiftsbehandlingar kan nämnas behandlingar relaterat till den digitala arbetsplatsen.</p>

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		<p>Vidare har det under året konstaterats att vissa personuppgiftsbehandlingar är dokumenterade på en alltför övergripande nivå – så att det är svårt att utläsa vad det närmare ändamålet med personuppgiftsbehandlingen är. Detta gäller exempelvis inom HR-området.</p> <p>Det har också konstaterats att spårvägmuseet saknar flera personuppgiftsbehandlingar i registerförteckningen.</p> <p>AB SL Även inom AB SL:s personuppgiftsansvar är det många personuppgiftsbehandlingar som saknas. Exempelvis saknas dokumenterade behandlingar rörande köp av resor och biljetter, förmåner och inom trygghetsområdet. Det saknas även behandlingar relaterat till medarbetare hos externa tjänsteleverantörer.</p> <p>Vidare har det konstaterats att många behandlingar är dokumenterade på en övergripande nivå – så att det är svårt att utläsa vad det närmare ändamålet med personuppgiftsbehandlingen är. Detta gäller framför allt inom SL:s kundtjänst där det finns ett övergripande ändamål för all kontakt med kundtjänst.</p> <p>WÅAB Inom WÅABs personuppgiftsansvar saknas fler personuppgiftsbehandlingar, exempelvis avseende köp av biljett och kundtjänst. Det saknas även behandlingar relaterat till medarbetare hos externa tjänsteleverantörer.</p>
D	Hur många behandlingar har respektive personuppgiftsansvarig dokumenterat?	<p>Trafiknämnden 87 registrerade personuppgiftsbehandlingar.</p> <p>AB SL 97 registrerade personuppgiftsbehandlingar.</p> <p>WÅAB</p>

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		10 registrerade personuppgiftsbehandlingar.
E	Finns det utpekade ansvariga för respektive behandling?	<p>Nej. Det saknas i vissa fall utpekade ansvariga för personuppgiftsbehandlingar inom samtliga personuppgiftsansvariga organisationer.</p> <p>Trafiknämnden Trafiknämnden saknar informationsägare för 7 personuppgiftsbehandlingar.</p> <p>AB SL AB SL saknar informationsägare för 17 personuppgiftsbehandlingar.</p> <p>WÅAB WÅAB saknar informationsägare för 1 personuppgiftsbehandling.</p> <p>Gemensamt för samtliga personuppgiftsansvariga Eftersom samtliga personuppgiftsbehandlingar inte är dokumenterade finns det ytterligare personuppgiftsbehandlingar som rör respektive personuppgiftsansvarig som inte har en utpekad informationsägare.</p>
F	Finns det rutiner för att dokumentera nya och löpande uppdatera befintliga personuppgiftsbehandlingar?	<p>Delvis. Det finns en rutin som heter "Hantera förteckning av personuppgiftsbehandlingar"¹⁰ som reglerar hur personuppgiftsbehandlingar ska hanteras i förteckningen dvs. upprättas, uppdateras och avvecklas. Av den framgår att det är informationsägaren och informationsförvaltaren som ansvarar för detta. Det dokumentet är dock ogiltigt i Edit och inte uppdaterat. Vidare framgår det av rollbeskrivningen för informationsägare¹¹ att det är denne som ansvar för att dokumentera personuppgiftsbehandlingar i registerförteckningen.</p> <p>Det följer även av it-avdelningens anpassade version av åtgärds- och initiativprocessen att vid</p>

¹⁰ Rutinen "Hantera förteckning av personuppgiftsbehandlingar", fastställd 2023-03-20, TN-S-1217246.

¹¹ Rollbeskrivning "Informationsägare". Fastställd 2024-12-19, TN-S-2088249.

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		nya initiativ/projekt ska det säkerställas att en informationsägare utses och att dokumentation av ev. personuppgiftsbehandling genomförs/uppdateras.
--	--	---

3.3.3 *Brister och risker*

Inom detta kontrollområde har följande brister och risker identifierats:

- Att samtliga personuppgiftsbehandlingar inte är dokumenterade eller inte är korrekta/uppdaterade i förteckning över personuppgiftsbehandlingar innebär risk för bristande regelefterlevnad samt ofullständig kontroll över organisationens personuppgiftsbehandlingar och eventuella risker som pågående behandlingar kan innebära. Det innebär även risk för att registrerades rättigheter inte kan tillvaratas på en fullständig vis.
- Att vissa personuppgiftsbehandlingar är dokumenterade på en för övergripande/generell nivå innebär risk för att kraven enligt dataskyddsförordningen inte kan bedömas eller följas upp på ett tillfredställande sätt. Det försvårar även möjligheten att lämna korrekt information till registrerade.
- Att det saknas utpekade informationsägare och informationsförvaltare för flera personuppgiftsbehandlingar innebär risk för att registerförteckningen inte hålls aktuell och uppdaterad.
- Att rutinen kring dokumentation i registerförteckningen inte är uppdaterad och giltig innebär risk för att personuppgiftsbehandlingar inte förtecknas på ett korrekt sätt.

3.3.4 *Dataskyddsombudets sammanfattande bedömning och rekommendationer*

X	Allvarlig brist/hög risk Allvarlig brist/risk som kan leda till omfattande överträdelser av dataskyddsförordningen och betydande sanktions- eller förtroenderisk.
	Betydande brist/medelhög risk Brist/risk som kan påverka efterlevnaden av dataskyddsförordningen och skapa interna problem med att efterleva processen eller svårigheter att visa ansvarsskyldigheten.
	Mindre brist/låg risk Mindre brist eller risk med begränsad påverkan på efterlevnaden, men som bör åtgärdas för att upprätthålla en konsekvent och korrekt tillämpning av dataskyddsreglerna.
	Inga brister/risker Inga identifierade brister/risker av nämnvärd betydelse.

Dataskyddsombudet bedömer att det finns en bra grundstruktur avseende registerförteckningen och att det finns goda förutsättningar för informationsägare att ta sitt ansvar. Det kan dock konstateras att ingen av registerförteckningarna är kompletta. Dels behöver många redan dokumenterade personuppgiftsbehandlingar färdigställas och/eller uppdateras, dels saknas flera personuppgiftsbehandlingar.

De brister som finns relaterat till registerförteckningarna har bedömts som allvarliga. Det beror på att det bland de saknade personuppgiftsbehandlingarna finns flera integritetskänsliga personuppgiftsbehandlingar. Om dessa inte dokumenteras finns risk för överträdelser av dataskyddsförordningen samt risk för sanktioner och förtroendeskador.

För att åtgärda de brister och risker som ovan har identifierats rekommenderar dataskyddsombudet:

- Att det säkerställs att alla personuppgiftsbehandlingar dokumenteras i registerförteckningen.
- Att det säkerställs att registerförteckningen hålls aktuell och uppdaterad.
- Att det säkerställs att alla ändamål är tydliga och precisa så att det går att utläsa vad ändamålet med personuppgiftsbehandlingen är.
- Att det säkerställs att det finns utpekade informationsägare och informationsförvaltare (eller motsvarande roll) för samtliga identifierade personuppgiftsbehandlingar.
- Att det säkerställs att styrande dokument rörande registerförteckningen är uppdaterade, giltiga, och tillgängliga.

3.4 Konsekvensbedömningar och förhandssamråd

3.4.1 Bakgrund

Enligt artikel 35 i dataskyddsförordningen ska den personuppgiftsansvarige genomföra en konsekvensbedömning avseende dataskydd när en personuppgiftsbehandling sannolikt leder till en hög risk för de registrerades rättigheter och friheter. En konsekvensbedömning är ett verktyg för att i förväg identifiera, analysera och hantera risker utifrån den registrerades perspektiv innan behandlingen påbörjas. Om konsekvensbedömningen visar att det kvarstår höga risker trots planerade skyddsåtgärder, ska enligt artikel 36 dataskyddsförordningen ett förhandssamråd genomföras med Integritetsskyddsmyndigheten innan behandlingen får påbörjas.

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

3.4.2 Kontrollfrågor och svar

Ref.	Kontrollfråga	Svar
A	Finns det rutiner för att identifiera när en konsekvensbedömning behöver genomföras?	<p>Delvis. De bedömningskriterier som europeiska dataskyddsstyrelsen (EDPB) har tagit fram för att avgöra om en konsekvensbedömning behövs eller inte behövs har tidigare varit inkorporerad i anmälan till förteckning över personuppgiftsbehandlingar. Under slutet av 2025 ersattes dock systemstödet för att föra förteckningen. Efter systembytet saknas dessa kriterier i systemstödet. Det finns dock ett övergripande fält för att ange diarienummer för genomförd konsekvensbedömning. Enligt uppgift från Regionledningskontoret håller de på att ta fram en separat modul för att bedöma behovet av konsekvensbedömning och genomförande av sådana. Enligt uppgift från dem kommer dessa funktioner finnas på plats under september 2026.</p> <p>I väntan på att ovanstående kommer på plats bevakar dataskyddsfunktionen frågan.</p>
B	Finns det nödvändiga processer och mallar för att genomföra konsekvensbedömningar och uppfyller de kraven i dataskyddsförordningen?	<p>Delvis. Det finns en rutin gällande att genomföra konsekvensbedömningar.¹² Dokumentet är dock ogiltigt i Edit. Vidare finns det mallar för att genomföra konsekvensbedömningar. Dataskyddsombudet har dock, utifrån dialog med verksamheten, fått uppfattningen att dessa kan upplevas som svåra att tillämpa. I början av 2025 publicerade Integritetsskyddsmyndigheten mallar för att genomföra konsekvensbedömningar. Dessa har använts ett fåtal gånger efter dialog med dataskyddsfunktionen, istället för de mallar som är internt framtagna.</p> <p>Regionledningskontoret håller på att utveckla nya mallar som ska finnas i Iris.</p>

¹² Rutinen "Konsekvensbedömning av dataskydd på Trafikförvaltningen", fastställd 2024-01-17, TN-S-1282290.

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

C	Har konsekvensbedömningar genomförts och dokumenterats för behandlingar som innebär hög risk för individers rättigheter och friheter?	<i>Detta har inte kontrollerats under året på grund av att det nya systemstödet (Iris) inte möjliggör sådana kontroller samt att andra arbetsuppgifter har prioriterats.</i>
D	Har organisationen åtgärdat riskerna som identifierats i konsekvensbedömningen?	<i>Detta har inte kontrollerats under året på grund av att det nya systemstödet (Iris) inte möjliggör sådana kontroller samt att andra arbetsuppgifter har prioriterats.</i>

3.4.3 Brister och risker

Inom detta kontrollområde har följande brister och risker identifierats:

- Att det nya systemstödet Iris idag saknar fält för att bedöma om en konsekvensbedömning behövs eller inte innebär risk för att denna bedömning inte kommer att genomföras.
- Att rutinen för att genomföra konsekvensbedömningar inte är giltig och att det inte är fastslaget vilka mallar som ska användas innebär risk för att konsekvensbedömningar inte genomförs på ett korrekt sätt.
- Att det nya systemstödet Iris inte möjliggör kontroll av huruvida konsekvensbedömningar har genomförts i de fall verksamheten har kommit fram till att det behövs försvårar möjligheten till kontroll och uppföljning.

3.4.4 Dataskyddsombudets sammanfattande bedömning och rekommendationer

	Allvarlig brist/hög risk Allvarlig brist/risk som kan leda till omfattande överträdelser av dataskyddsförordningen och betydande sanktions- eller förtroenderisk.
	Betydande brist/medelhög risk Brist/risk som kan påverka efterlevnaden av dataskyddsförordningen och skapa interna problem med att efterleva processen eller svårigheter att visa ansvarsskyldigheten.
X	Mindre brist/låg risk Mindre brist eller risk med begränsad påverkan på efterlevnaden, men som bör åtgärdas för att upprätthålla en konsekvent och korrekt tillämpning av dataskyddsreglerna.
	Inga brister/risker Inga identifierade brister/risker av nämnvärd betydelse.

Dataskyddsombudet gör bedömningen att det finns brister och risker kopplat till systemstöd och mallar för att genomföra konsekvensbedömningar. Identifierade brister och risker bedöms dock ha begränsad påverkan på efterlevnad, men bör åtgärdas för att upprätthålla en konsekvent och korrekt tillämpning av dataskyddsreglerna. Att

dataskyddsfunktionen granskar all ny dokumentation och bevakar denna fråga särskilt minskar risken.

Under året har dataskyddsombudet inte kontrollerat om verksamheten har genomfört och dokumenterat konsekvensbedömningar för personuppgiftsbehandlingar som innebär hög risk för registrerades rättigheter och friheter och om verksamheten har åtgärdat sådana risker som har identifierats. Det saknas därför förutsättningar för att bedöma eventuella brister och risker i övrigt kopplat till detta kontrollområde.

För att åtgärda de brister och risker som ovan har identifierats rekommenderar dataskyddsombudet:

- Att det säkerställs att det finns systemstöd för att bedöma om en konsekvensbedömning behövs eller inte.
- Att det säkerställs att det går att kontrollera om verksamheten har bedömt att en konsekvensbedömning behövs eller inte behövs.
- Att rutinen för att genomföra konsekvensbedömningar ses över så att det är tydligt vilka mallar som ska användas och att rutinen är korrekt och giltig.

3.5 Registrerades rättigheter

3.5.1 Bakgrund

Enligt artiklarna 12–22 dataskyddsförordningen har registrerade ett antal rättigheter, såsom rätt till tillgång, rättelse, radering, begränsning, dataportabilitet och invändning mot behandling. Dessa rättigheter är grundläggande för att den enskilde ska kunna ha kontroll över sina personuppgifter och för att upprätthålla förtroendet för hur organisationen behandlar dem. För att uppfylla förordningens krav måste den personuppgiftsansvarige ha tydliga och fungerande rutiner för att ta emot, bedöma och besvara begäranden inom lagstadgade tidsfrister.

3.5.2 Kontrollfrågor och svar

Ref.	Kontrollfråga	Svar
A	Finns det rutiner för att hantera registrerades rättigheter?	Delvis. Det finns en rutin dokumenterad gällande att hantera registrerades rättigheter. ¹³ Den rutinen är dock ogiltig i Edit. Vidare har det konstaterats att den inte korrekt beskriver processen så som den faktiskt fungerar. Den är inte heller tillräckligt utförligt dokumenterad – så att nya medarbetare enkelt kan förstå processen. Det pågår ett arbete

¹³ Rutinen ”Hantera inkommande förfrågningar baserat på den registrerades rättigheter”, fastställd 2022-05-23, TN-S-1304931.

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		<p>hos dataskyddsfunktionen med att uppdatera rutinen.</p> <p>Det kan dock konstateras att såväl dataskyddsfunktionen som färdtjänst och kundtjänst hanterar ett stort antal ärenden varje år och att majoriteten av dessa ärenden hanteras inom lagstadgande tidsfrister (se nedan). Det tyder på att de rutiner och processer som finns på plats, fungerar på det stora hela.</p>
B	Hur många ärenden har hanterats under året?	<p>Trafiknämnden 39 ärenden. Varav:</p> <ul style="list-style-type: none"> • 38 ärenden rörande begäran om registerutdrag. • 0 ärenden rörande begäran om radering. • 1 ärenden rörande begäran om information. <p>Av dessa ärenden har 3 hanterats av dataskyddsfunktionen och 36 ärenden har hanterats av färdtjänst.</p> <p>0 ärenden har överklagats.</p> <p>AB SL 194 ärenden. Varav:</p> <ul style="list-style-type: none"> • 144 begäran om registerutdrag. • 44 begäran om radering • 5 begäran om information. • 1 begäran om begränsning. <p>Av dessa ärenden har 161 ärenden hanterats av dataskyddsfunktionen och 33 ärenden har hanterats självständigt av kundtjänst.</p> <p>2 ärenden har överklagats.</p> <p>WÅAB 1 ärende. Varav:</p> <ul style="list-style-type: none"> • 1 begäran om registerutdrag.

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		<p>Detta ärendehar hanterats självständigt av kundtjänst.</p> <p>o ärenden har överklagats.</p>
C	Hanteras inkomna begäran enligt lagstadgade tidsfrister?	<p>Ja, med undantag för ett fall.</p> <p>I dagsläget är det tre grupperingar som handlägger dessa typer av ärenden. Av ärendeloggarna framgår att både färdtjänst och kundtjänst har hanterat samtliga ärenden inom lagstadgade tidsfrister och att dataskyddsfunktionen har hanterat samtliga ärenden, utom ett, inom lagstadgade tidsfrister.</p>
D	Säkerställer verksamheten att den som begär att utöva sina rättigheter enligt dataskyddsförordningen verkligen är den person som begäran avser?	<p>Delvis. Vid begäran om bild/videomaterial inhämtas ID-handling i syfte att säkerställa att uppgifter inte lämnas ut till annan person än den personuppgifterna rör.</p> <p>I andra ärenden sker som huvudregel ingen ID-kontroll eller annan kontroll för att fastställa identitet. Endast om det finns rimliga skäl att ifrågasätta att någon annan än den registrerade själv gör begäran görs sådana kontroller. Enligt rutinen för hantering av registrerades rättigheter ska dock svar alltid skickas till folkbokföringsadressen. På så sätt säkerställs att uppgifter aldrig skickas till någon annan än den uppgifterna rör – även om det skulle vara någon annan som begär uppgifterna. Färdtjänst och Kundtjänst har uppgett att de följer denna rutin. Dataskyddsfunktionen saknar dock förmåga att kontrollera folkbokföringsadressen och skickar därför uppgifterna till den adress som den registrerade har uppgett.</p>
E	Tillhandahålls registerutdrag i ett allmänt använt elektroniskt format när den registrerade gör sin begäran elektroniskt, om inte den registrerade uttryckligen begär ett annat format?	<p>Delvis. För närvarande finns begränsade möjligheter att erbjuda registerutdrag elektroniskt, då tekniska förutsättningar saknas för att överföra dem på ett säkert sätt. De format som idag kan erbjudas är för de flesta registrerade för komplicerat. Endast i de situationer där skyddsvärdet på informationen bedöms lågt kan</p>

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		svar till de registrerade tillhandahållas via e-post. I vissa fall erbjuds även USB-minne.
F	Informeras de registrerade om deras rättigheter på ett begripligt och tydligt sätt?	<p>Delvis.</p> <p>Trafiknämnden</p> <p>Färdtjänstresenärer informeras om behandling av personuppgifter på hemsidan. Informationen uppfyller de grundläggande kraven. Samtidigt noteras att personuppgiftsbehandlingarna beskrivs på en relativt övergripande nivå. Den nuvarande strukturen, där informationen redovisas per rubrik snarare än per specifik personuppgiftsbehandling, kan i vissa fall försvåra för den registrerade att förstå vad som gäller för en specifik personuppgiftsbehandling. Strukturen kan påverka graden av tydlighet och transparens för den registrerade. Vidare saknas det information om vilka skyddsåtgärder som används i samband med överföring till länder utanför EU/EES.</p> <p>När det gäller besökare vid spårvägmuseet, medarbetare vid Trafikförvaltningen och medarbetare hos externa tjänsteleverantörer saknas sammanhållna informationstexter (informationspolicys) för dessa kategorier av registrerade. Information lämnas, enligt uppgift, ibland i samband med insamling, exempelvis i blanketter och it-system. Det är dock svårt för dessa kategorier av registrerade att ta reda på hur deras personuppgifter behandlas. <i>Av samma anledning har närmare kontroller inte genomförts av sådana informationstexter.</i></p> <p>AB SL</p> <p>SL-resenärer informeras om behandling av personuppgifter på hemsidan. När det gäller kamerabevakning lämnas även viss information på plats genom skyltar. Informationen uppfyller de grundläggande kraven. Dock har det noterats att flera ändamål kan uppfattas som alltför allmänna och övergripande. Det saknas även vissa ändamål och vissa ändamål anger fel laglig grund.</p>

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		<p>När det gäller medarbetare vid Trafikförvaltningen och medarbetare hos externa tjänsteleverantörer saknas sammanhållna informationstexter (informationspolicys) för dessa kategorier av registrerade. Information lämnas, enligt uppgift, ibland i samband med insamling, exempelvis i blanketter och it-system. Det är dock svårt för dessa kategorier av registrerade att ta reda på hur deras personuppgifter behandlas. <i>Av samma anledning har närmare kontroller inte genomförts av sådana informationstexter.</i></p> <p>WÅAB</p> <p>Waxholmsbolagets resenärer informeras på hemsidan. Informationen är dock inte fullständig och uppfyller inte de grundläggande kraven. Flera personuppgiftsbehandlings saknas. Vidare bör informationen presenteras per specifik personuppgiftsbehandling. Se vad som anges under Trafiknämnden.</p> <p>När det gäller medarbetare vid Trafikförvaltningen och medarbetare hos externa tjänsteleverantörer saknas sammanhållna informationstexter (informationspolicys) för dessa kategorier av registrerade. Information lämnas, enligt uppgift, ibland i samband med insamling, exempelvis i blanketter och it-system. Det är dock svårt för dessa kategorier av registrerade att ta reda på hur deras personuppgifter behandlas. <i>Av samma anledning har närmare kontroller inte genomförts av sådana informationstexter.</i></p> <p>Allmänt för samtliga personuppgiftsansvariga</p> <p>Under 2025 har dataskyddsfunktionen initierat ett arbete med att se över och uppdatera samtliga informationstexter.</p> <p>Föregående år rapporterade dataskyddsombudet om att registrerade inte informeras om rätten till överklagbart beslut. Detta är nu åtgärdat.</p>
--	--	---

3.5.3 Brister och risker

Inom detta kontrollområde har följande brister och risker identifierats:

- Att rutinen för handläggning av registrerades rättigheter inte är giltig och tillräckligt utförligt dokumenterad innebär risk för att sådana ärenden inte hanteras korrekt och inom rätt tid. Idag är det ett fåtal medarbetare som handlägger dessa ärenden och om någon av dem är frånvarande är det svårt för annan medarbetare att fortsätta handläggningen.
- Att dataskyddsfunktionen saknar förmåga att kontrollera folkbokföringsadressen i samband med handläggning av registrerades rättigheter innebär risk för att personuppgifter lämnas ut till fel person eller raderas på begäran av någon annan än den uppgifterna rör.
- Att det saknas tekniskt stöd för att tillhandahålla registerutdrag på ett säkert elektroniskt sätt, innebär risk för att kravet på att lämna informationen i ett allmänt använt elektroniskt format inte uppfylls. Det medför också risk för att överföringar sker på ett osäkert sätt och att uppgifter därför kommer obehöriga tillhanda.
- Att registrerade inte informeras tillräckligt om behandling av deras personuppgifter utgör risk för bristande transparens och kränkning av registrerades rättigheter, vilket kan leda till att de inte kan tillvarata sina rättigheter enligt förordningen.

3.5.4 Dataskyddsombudets sammanfattande bedömning och rekommendationer

X	Allvarlig brist/hög risk Allvarlig brist/risk som kan leda till omfattande överträdelser av dataskyddsförordningen och betydande sanktions- eller förtroenderisk.
	Betydande brist/medelhög risk Brist/risk som kan påverka efterlevnaden av dataskyddsförordningen och skapa interna problem med att efterleva processen eller svårigheter att visa ansvarsskyldigheten.
	Mindre brist/låg risk Mindre brist eller risk med begränsad påverkan på efterlevnaden, men som bör åtgärdas för att upprätthålla en konsekvent och korrekt tillämpning av dataskyddsreglerna.
	Inga brister/risker Inga identifierade brister/risker av nämnvärd betydelse.

Dataskyddsombudet bedömer att handläggningen rörande registrerades rättigheter över lag fungerar bra. Det finns dock risker kopplat till att registrerade inte alltid tillhandahålls registerutdrag i ett elektroniskt format och att dataskyddsfunktionen saknar förmåga att kontrollera folkbokföringsadressen (så att det säkerställs att

uppgifterna inte kommer obehöriga tillhanda). Riskerna bedöms medelhöga, eftersom de kan påverka efterlevnaden av dataskyddsförordningen.

Vidare innebär avsaknaden av information till vissa kategorier av registrerade allvarliga brister, eftersom det finns integritetskänsliga personuppgiftsbehandlingar som registrerade inte får information om.

För att åtgärda de brister och risker som ovan har identifierats rekommenderar dataskyddsombudet:

- Att rutinen för handläggning av registrerades rättigheter uppdateras så att den beskriver processen på ett tillräckligt och korrekt sätt i syfte att säkerställa att sådana ärenden hanteras korrekt och inom rätt tid.
- Att det säkerställs att dataskyddsfunktionen kan kontrollera folkbokföringsadressen i syfte att säkerställa att svar i ärenden rörande registrerades rättigheter inte skickas till fel personer. Alternativt säkerställ att dataskyddsfunktionen på annat sätt kan vara säker på att uppgifterna inte kommer obehöriga tillhanda.
- Att det säkerställs att det finns tekniskt stöd för att tillhandahålla registerutdrag elektroniskt på ett säkert sätt.
- Att det säkerställs att samtliga kategorier av registrerade informeras om behandling av personuppgifter.

3.6 Personuppgiftsincidenter

3.6.1 Bakgrund

Enligt artiklarna 33-34 i dataskyddsförordningen ska den personuppgiftsansvarige ha rutiner för att upptäcka, bedöma, hantera och rapportera personuppgiftsincidenter. En tydlig och fungerande incidenthanteringsprocess är en förutsättning för att säkerställa att personuppgiftsincidenter dokumenteras, att rapporteringsskyldigheten till Integritetsskyddsmyndigheten uppfylls samt att berörda registrerade informeras när så krävs. En väl fungerande incidenthantering bidrar även till att minska riskerna för de registrerades rättigheter och friheter och stärka organisationens informationssäkerhet.

3.6.2 Kontrollfrågor och svar

Ref.	Kontrollfråga	Svar
A	Finns det rutiner på plats för att upptäcka, anmäla och åtgärda personuppgiftsincidenter?	Delvis. Det finns flera styrande dokument som beskriver hantering av personuppgiftsincidenter. Dels finns det en rutin för informationssäkerhetsincidenter ¹⁴ som även innehåller skrivningar rörande

¹⁴ Rutin för informationssäkerhetsincidenter, fastställd 2024-07-02, TN-S-2980752.

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		personuppgiftsincidenter. Dels finns en processbeskrivning ¹⁵ och en checklista ¹⁶ . De senare dokumenten är dock ogiltiga i Edit. Vidare har det konstaterats att de inte korrekt beskriver processen så som den faktiskt fungerar. Därutöver finns en säkerhetsbestämmelse rörande styrning av informationssäkerhetsincidenter. ¹⁷
B	Hur många incidenter har rapporterats under året? Hur många av dessa har anmälts till Integritetsskyddsmyndigheten?	<p>De nedan redovisade uppgifterna baseras på dataskyddsfunktionens och färdtjänstsektionens loggar över inträffade personuppgiftsincidenter. Innan en personuppgiftsincident registreras i dessa loggar anmäls den via Service Desk, varför viss kompletterande information även har hämtats därifrån. Vid jämförelse mellan källorna kan det konstateras att statistiken inte är fullt ut samstämmig. Varken dataskyddsfunktionen eller dataskyddsombudet har kunnat fastställa orsaken till dessa avvikelser. De presenterade siffrorna bör därför tolkas med försiktighet och kan inte betraktas som helt tillförlitliga.</p> <p>Trafiknämnden 80 personuppgiftsincidenter (där 40 rörde färdtjänstverksamheten). Varav 0 anmälades till IMY.</p> <p>AB SL 28 personuppgiftsincidenter. Varav 1 anmäld till IMY.</p> <p>WÅAB 3 personuppgiftsincidenter. Varav 1 anmäld till IMY.</p>
C	Innehåller loggen över personuppgiftsincidenter nödvändiga uppgifter?	Delvis. I dagsläget finns det två loggar över personuppgiftsincidenter. En som rör färdtjänsts personuppgiftsincidenter och en som

¹⁵ ¹⁵ Processspecifikation ”Hantera personuppgiftsincidenter”, fastställd 2023-07-07, TN-S-1360259.

¹⁶ Checklista vid personuppgiftsincidenter, fastställd 2024-04-04, dokumentid: 1264535.

¹⁷ SÄB Styrning av informationssäkerhetsincidenter, fastställd 2024-12-19, TN-S-3127532.

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		<p>rör alla andra personuppgiftsincidenter. Den senare loggen omfattar Trafiknämnden, AB SL och WÅAB.</p> <p>Båda loggarna bedöms i stort uppfylla de grundläggande kraven enligt dataskyddsförordningen. Dock saknas uppgift om när beslut om att anmäla eller inte anmäla en personuppgiftsincident till Integritetsskyddsmyndigheten gjorts. Färdtjänstens logg saknar även fält för att motivera beslutet.</p>
D	<p>Registreras och dokumenteras alla personuppgiftsincidenter korrekt, inklusive vidtagna åtgärder och beslut?</p>	<p>Nej. Informationen i loggarna är bristande. Många gånger är det svårt att utläsa vad som har hänt och sällan framgår en motivering till varför incidenten inte bedöms medföra en risk för registrerades fri- och rättigheter. Sällan går det direkt av loggarna att utläsa vilka åtgärder som har vidtagits. En trolig förklaring till detta är att incidenterna handläggs av informationsägare och informationsförvaltare men loggas i efterhand av dataskyddsfunktionen. Detta gäller alla verksamhetsdelar förutom personuppgiftsincidenter relaterat till färdtjänstverksamheten. Även deras logg redogör sällan för vilka åtgärder som har vidtagits. Enligt uppgift kan dock ytterligare information, i vissa fall, finnas i andra it-system. <i>Detta har inte närmare kontrollerats.</i></p>
E	<p>Har personuppgiftsincidenter hanterats inom lagstadgade tidsfrister?</p> <p>Av dataskyddsförordningen framgår att alla personuppgiftsincidenter ska anmälas till Integritetsskyddsmyndigheten inom 72 h, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter.</p>	<p>Loggen saknar information om när beslut fattas om att anmäla eller inte anmäla en personuppgiftsincident till Integritetsskyddsmyndigheten. Det går därför inte att kontrollera om incidenterna har hanterats inom lagstadgade tidsfrister.</p> <p>Av Service Desk loggar går det att utläsa när en personuppgiftsincident har rapporterats och när den har stängts, men av dessa uppgifter går det inte att dra slutsatser kring om incidenten har hanterats inom rätt tid eller inte.</p>

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

F	Har de personuppgiftsincidenter som ska anmälas till Integritetsskyddsmyndigheten anmälts?	<i>Detta är inte kontrollerat under året på grund av andra prioriterade arbetsuppgifter.</i>
G	Är de anställda utbildade i att upptäcka och rapportera personuppgiftsincidenter?	Delvis. Information om hantering av personuppgiftsincidenter har ingått i den grundläggande utbildningen rörande dataskydd som riktar sig till alla medarbetare inom Region Stockholm samt i den målgruppsanpassade utbildningen för informationsägare och informationsförvaltare.
H	Finns det rutiner för intern uppföljning och lärande från personuppgiftsincidenter för att förhindra upprepning?	Delvis. Dataskyddsfunktionen, it-säkerhet och informationssäkerhet har haft månadsvisa möten för uppföljning och utveckling av incidenthanteringsprocessen i stort. Det har dock varit ett litet fokus på hantering av personuppgiftsincidenter och på sista tiden har antalet möten varit färre.

3.6.3 Brister och risker

Inom detta kontrollområde har följande brister och risker identifierats:

- Att styrande dokument för handläggning av personuppgiftsincidenter inte är giltiga och inte korrekt beskriver hur incidenter hanteras i praktiken innebär risk för felaktig hantering och att personuppgiftsincidenter inte hanteras inom lagstadgade tidsfrister (72 h).
- Att det finns flera styrande dokument rörande hantering av personuppgiftsincidenter medför att det är svårt för medarbetare att förstå och följa processen för hantering av personuppgiftsincidenter.
- Att incidentloggarna inte stämmer överens med informationen från Service Desk innebär risk för att alla personuppgiftsincidenter inte har loggats.
- Att det inte alltid framgår av loggarna vilka bedömningar som har gjorts och att det inte går att följa upp om personuppgiftsincidenter har hanterats inom lagstadgade tidsfrister innebär risk för att nödvändiga kontroller inte kan genomföras.
- Att det saknas rutiner för intern uppföljning och lärande från personuppgiftsincidenter innebär risk för återkommande incidenter och försvårar möjligheten att upptäcka systematiska brister och risker.

3.6.4 Dataskyddsombudets sammanfattande bedömning och rekommendationer

Allvarlig brist/hög risk

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

	Allvarlig brist/risk som kan leda till omfattande överträdelser av dataskyddsförordningen och betydande sanktions- eller förtroenderisk.
	Betydande brist/medelhög risk Brist/risk som kan påverka efterlevnaden av dataskyddsförordningen och skapa interna problem med att efterleva processen eller svårigheter att visa ansvarsskyldigheten.
X	Mindre brist/låg risk Mindre brist eller risk med begränsad påverkan på efterlevnaden, men som bör åtgärdas för att upprätthålla en konsekvent och korrekt tillämpning av dataskyddsreglerna.
	Inga brister/risker Inga identifierade brister/risker av nämnvärd betydelse.

Dataskyddsombudets samlade bedömning är att personuppgiftsincidenter hanteras och dokumenteras. Loggen över personuppgiftsincidenter har under 2025 förbättrats och innehåller nu de grundläggande kraven och lite mer. Dock bör kvarvarande brister relaterat till loggen omhändertas, liksom brister relaterat till de styrande dokumenten

för att upprätthålla en konsekvent och korrekt tillämpningen av dataskyddsförordningen.

För att åtgärda de brister och risker som ovan har identifierats rekommenderar dataskyddsombudet:

- Att styrande dokument gällande handläggning av personuppgiftsincidenter ses över så att de är giltiga och korrekta. Det bör även övervägas att minska antalet styrande dokument, så att det blir enklare att överblicka hur personuppgiftsincidenter ska hanteras.
- Att den som handlägger personuppgiftsincidenten bör vara den som loggar personuppgiftsincidenterna, eftersom det är svårt för någon annan att göra det på ett korrekt sätt i efterhand.
- Att loggen för personuppgiftsincidenter kompletteras med fält för att ange när beslut fattas om att anmäla eller inte anmäla incidenten till Integritetsskyddsmyndigheten, samt en motivering till beslutet. Syftet är att det i efterhand ska gå att följa upp och avgöra om personuppgiftsincidenter har hanterats enligt lagstadgade tidsfrister.
- Att det införs en rutin för att löpande kontrollera och följa upp hanteringen av personuppgiftsincidenter i syfte att säkerställa att dessa hanteras och dokumenteras på ett korrekt sätt.
- Att det tas fram rutiner för intern uppföljning och lärande av personuppgiftsincidenter i syfte att minska risken för återkommande incidenter och upptäckta systematiska brister och risker.

3.7 Tekniska och organisatoriska säkerhetsåtgärder

3.7.1 Bakgrund

Enligt artikel 32 i dataskyddsförordningen ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att säkerställa en skyddsnivå som är anpassad till de risker som är förknippade med behandlingen av personuppgifter. Åtgärderna ska skydda personuppgifter mot bland annat obehörig åtkomst, förlust, förstöring, ändring och otillåten spridning. Ett systematiskt och riskbaserat arbete med tekniska och organisatoriska säkerhetsåtgärder är avgörande för att upprätthålla informationssäkerhet, säkerställa efterlevnad av dataskyddsförordningen och minska risken för personuppgiftsincidenter som kan leda till negativa konsekvenser för både registrerade och organisationen.

3.7.2 Kontrollfrågor och svar

Ref.	Kontrollfråga	Svar
A	Finns dokumentation över vilka tekniska och organisatoriska åtgärder som har vidtagits för att skydda personuppgifter?	Delvis. I förteckning över personuppgiftsbehandlingsprocesser finns det fält för att dokumentera tekniska och organisatoriska säkerhetsåtgärder. I ett stort antal fall har det dock inte antecknats i registerförteckningen vilka tekniska och organisatoriska åtgärder som har vidtagits. Det är möjligt att tekniska och organisatoriska säkerhetsåtgärder har vidtagits trots att det inte är dokumenterat. <i>Närmare kontroller inom detta område har inte gjorts.</i>
B	Finns det rutiner för att regelbundet och systematiskt kontrollera och följa upp de tekniska- och organisatoriska säkerhetsåtgärderna?	Delvis. Vissa tekniska säkerhetsåtgärder följs regelbundet upp inom säkerhetsforum, exempelvis: <ul style="list-style-type: none"> • system/servers som är med i auto-patchning (vilket är mer än 80%) • sårbarhetsskanningar av servers, infrastruktur och nät, samt • konfiguration/hårdning av servermiljö kopplat till standard. Rutiner för uppföljning av organisatoriska säkerhetsåtgärder och ytterligare uppföljning av tekniska säkerhetsåtgärder kan även finnas för respektive it-system och/eller personuppgiftsbehandling. <i>Närmare kontroller inom området har inte gjorts.</i>

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

C	Ställs det krav på tekniska och organisatoriska åtgärder vid inköp och upphandling av nya it-system och tjänster?	Ja. I mallen för personuppgiftsbiträdesavtal ¹⁸ finns ett stycke som rör tekniska och organisatoriska säkerhetsåtgärder. Där i hänvisas även till informationssäkerhets- och it-säkerhetsbilagan som innehåller ytterligare krav. Vilka krav som ställs baseras på genomförd informationssäkerhetsklassning.
D	Finns det styrande dokument som reglerar loggning och logguppföljning avseende it-system som innehåller känsliga och integritetskänsliga personuppgifter?	<p>Ja. Av Regionstyrelsens riktlinjer för informationssäkerhet- och dataskydd¹⁹ framgår krav rörande säkerhetsloggning. Bland annat framgår att ägare av it-system ansvarar för att händelser som kan ha betydelse för säkerheten i it-systemet eller it-miljön loggas och att det finns rutiner för hantering av it-systemets loggar och händelser som kan påverka säkerheten i it-systemet.</p> <p>Vidare följer det av Trafikförvaltningens säkerhetsbestämmelser för Säkerhetsloggning och spårbarhet²⁰ bland annat att informationsägaren/verksamhetsansvarig har huvudansvaret för att identifiera och specificera krav på loggning av händelser och aktiviteter i och kring sin verksamhets it-tjänster och att säkerhetsloggning av Trafikförvaltningens it-miljö ska ske via en Central loggfunktion.</p> <p>De styrande dokumenten gäller för it-system generellt och innehåller inga särskilda krav avseende it-system som innehåller känsliga eller integritetskänsliga personuppgifter.</p>
E	Sker regelbunden logguppföljning för att upptäcka avvikelser?	Det finns en central säkerhetslogg med tillhörande säkerhetsövervakning (SOC/Security Operations Center), för it-system som driftas av CGI. I dagsläget driftar CGI 48 % av våra it-system. Av dessa är 79 % anslutna till den centrala säkerhetsloggen.

¹⁸ Finns i mallbiblioteket i word.

¹⁹ Riktlinje för informationssäkerhet samt dataskydd, beslutad av regionfullmäktige den 9 december 2025, diarienummer RD 2025-0418.

²⁰ SÄB Säkerhetsloggning och spårbarhet, fastställd 2025-08-28, TN-S-2958518.

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		<p>Vid identifierade avvikelser tillämpas etablerade rapporteringsrutiner för vidare hantering inom Trafikförvaltningen. Rutinen omfattar såväl it-säkerhetsincidenter som större incidenter enligt processen för MIM (Major Incident Management).</p> <p>Om ett it-system inte driftas av CGI finns det ingen central säkerhetslogg att ansluta till. Loggning ska dock ske ändå. <i>Närmare kontroller av om det sker har inte gjorts.</i></p>
F	Finns det styrande dokument som reglerar behörighetshantering för it-system?	<p>Ja. Av Regionstyrelsens riktlinjer för informationssäkerhet- och dataskydd²¹ framgår krav relaterat till åtkomstkontroll och informationstillgångar. Vidare framgår det regler för åtkomstkontroll i säkerhetsbestämmelsen Styrning av åtkomst.²² Av båda dokumenten följer att behörighet till informationstillgångar ska baseras på användarens aktuella arbetsuppgifter och organisatoriska tillhörighet för att endast ge åtkomst till de informationstillgångar som behövs för att lösa arbetet.</p> <p>En administrativ bestämmelse är under framtagning. Den kommer ytterligare att konkretisera ovan styrande dokument och beskriva hur identiteter och åtkomster ska och får hanteras inom Trafikförvaltningens verksamhet.</p>
G	Tilldelas behörigheter enligt principen om minsta privilegium och fastställda behörighetsroller?	<p>Delvis. Inom Trafikförvaltningen finns ett system för behörighetshantering, Omada. Om ett it-system är anslutet till Omada har systemroller definierats. Syftet med dessa är att medarbetare inte ska ha tillgång till och ha högre behörigheter än de behöver för att kunna utföra sina arbetsuppgifter.</p>

²¹ Riktlinje för informationssäkerhet samt dataskydd, beslutad av regionfullmäktige den 9 december 2025, diarienummer RD 2025-0418.

²² SÄB Styrning av åtkomst, fastställd 2024-12-19, TN-S-3126486.

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		<p>Dock är inte alla it-system anslutna till Omada. I vissa fall beror det på att en manuell rutin för behörighetshantering har tagits fram istället. I andra fall beror det på att systemet inte har anslutit än. <i>Det har inte kontrollerats om de icke anslutna it-systemen används för omfattande personuppgiftsbehandling eller behandling av känsliga och/eller integritetskänsliga personuppgifter.</i></p> <p>Det saknas i dagsläget övergripande verksamhetsroller, exempelvis för chefer eller andra grupper med gemensamma och återkommande arbetsuppgifter. Tilldelning av behörigheter sker därmed huvudsakligen på systemnivå. Det finns dock en ambition om att införa verksamhetsroller.</p>
G	Sker det regelbundna och systematiska behörighetsrevideringar?	<p>Nej, åtminstone inte på en övergripande och strukturerad nivå. Det är dock möjligt att det finns exempel där så sker.</p> <p>I Omada finns funktioner för att genomföra regelbundna och strukturerade behörighetsrevideringar. Det sker dock inte idag, men det finns en ambition om att införa det framåt. Det bygger dock på att olika verksamhetsroller har definierats och tillämpas.</p> <p>För dem som är rollägare för ett specifikt it-system finns det möjlighet att kontrollera och revidera behörigheter i Omada. Detta förutsätter dock att rollägaren själv tar ansvar för det. Samma sak gäller om ett it-system inte är anslutet till Omada utan använder helt manuella behörighetsrutiner.</p> <p>Frågan om behörighetsrevidering har ställts till informationsägare och informationsförvaltare i en enkätundersökning under 2025. Nästan en fjärdedel av respondenterna uppgav att det finns väl fungerande rutiner för behörighetsrevidering inom verksamhetsområdet. Ungefär en tredjedel</p>

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		angav att rutinerna endast delvis fungerar, medan resterande uppgav att rutiner saknas eller att de inte känner till om det finns några rutiner.
H	Finns rutiner för att säkerställa inbyggt dataskydd och dataskydd som standard?	Nej. Det saknas rutiner för att säkerställa inbyggt dataskydd och dataskydd som standard.

3.7.3 Brister och risker

Inom detta kontrollområde har följande brister och risker identifierats:

- Att förteckningen över personuppgiftsbehandlingar i flera fall saknar information om vilka tekniska och organisatoriska säkerhetsåtgärder som har vidtagits, innebär risk för bristande regelefterlevnad, otillräckligt skydd av personuppgifter samt försvårad uppföljning och kontroll.
- Att det saknas rutiner för att regelbundet och systematiskt revidera behörigheter innebär risk för att medarbetare har obehöriga åtkomster, vilket kan leda till risk för personuppgiftsincidenter och bristande regelefterlevnad.
- Att det saknas rutiner för att säkerställa inbyggt dataskydd och dataskydd som standard innebär risk för att integritetsskyddet inte beaktas i tillräckligt hög utsträckning vid utveckling och inköp av nya eller förändrade it-system och personuppgiftsbehandlingar. Det kan medföra en ökad risk för integritetsintrång för de registrerade.

3.7.4 Dataskyddsombudets sammanfattande bedömning och rekommendationer

	Allvarlig brist/hög risk Allvarlig brist/risk som kan leda till omfattande överträdelser av dataskyddsförordningen och betydande sanktions- eller förtroenderisk.
X	Betydande brist/medelhög risk Brist/risk som kan påverka efterlevnaden av dataskyddsförordningen och skapa interna problem med att efterleva processen eller svårigheter att visa ansvarsskyldigheten.
	Mindre brist/låg risk Mindre brist eller risk med begränsad påverkan på efterlevnaden, men som bör åtgärdas för att upprätthålla en konsekvent och korrekt tillämpning av dataskyddsreglerna.
	Inga brister/risker Inga identifierade brister/risker av nämnvärd betydelse.

Dataskyddsombudets sammanfattande bedömning är att det finns grundläggande styrande dokument på området och rutiner för att krävställa tekniska och organisatoriska åtgärder i samband med inköp och upphandling.

Samtidigt konstateras det att det saknas styrning för att säkerställa inbyggt dataskydd och dataskydd som standard vid utveckling samt inköp och upphandling. Denna brist har bedömts som medelhög, eftersom den kan påverka efterlevnaden av dataskyddsförordningen.

Vidare har det noterats att det saknas rutiner för att systematiskt och regelbundet revidera behörigheter. Denna brist har bedömts som låg. Rutiner bör dock tas fram för att säkerställa en korrekt tillämpning av dataskyddsreglerna.

För att åtgärda de brister och risker som ovan har identifierats rekommenderar dataskyddsombudet:

- Att det säkerställs att förteckning över personuppgiftsbehandlingar innehåller nödvändiga uppgifter om vilka tekniska och organisatoriska åtgärder som har vidtagits,
- Att det säkerställs att behörigheter till it-system som innehåller personuppgifter revideras systematiskt och regelbundet för att säkerställa att inga medarbetare har obehöriga åtkomster, och
- Att det tas fram rutiner och krav för att säkerställa inbyggt dataskydd och dataskydd som standard vid utveckling och inköp av nya eller förändrade it-system.

3.8 Personuppgiftsbiträden och avtal

3.8.1 Bakgrund

Enligt artikel 28 i dataskyddsförordningen får ett personuppgiftsbiträde endast behandla personuppgifter enligt den personuppgiftsansvariges dokumenterade instruktioner. När ett biträde anlitas ska detta regleras i ett personuppgiftsbiträdesavtal, som bland annat beskriver behandlingen, ställer krav på säkerhet, reglerar underbiträden och anger hur uppgifterna ska hanteras när uppdraget avslutas. Ett tydligt och korrekt utformat avtal, tillsammans med löpande uppföljning, är en förutsättning för att säkerställa att biträdet behandlar personuppgifter på ett säkert sätt och i enlighet med den personuppgiftsansvariges instruktioner.

3.8.2 Kontrollfrågor och svar

Ref.	Kontrollfråga	Svar
A	Finns det rutiner för att upptäcka när personuppgiftsbiträdesavtal behöver tecknas?	Ja. Dels innehåller förteckning över personuppgiftsbehandlingar fält gällande personuppgiftsbiträden och personuppgiftsbiträdesavtal. Det innebär att om verksamheten har identifierat en ny eller förändrad personuppgiftsbehandling så kommer

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		<p>det utredas tillsammans med dataskyddsfunktionen om ett personuppgiftsbiträdesavtal behöver tecknas eller uppdateras.</p> <p>Vidare framgår det av handbok för inköp och upphandling²³ att dataskyddsombudet²⁴ ska kontaktas för att utreda om personuppgifter kommer att hanteras av lösningen och att personuppgiftsbiträdesavtal i sådana fall ska tecknas. I praktiken innebär det att det ofta är i detta skede av upphandlings- eller inköpsprocessen som det identifieras att ett personuppgiftsbiträdesavtal behöver tecknas och att kraven i dataskyddsförordningen i övrigt behöver beaktas.</p>
B	Finns det mallar för att teckna personuppgiftsbiträdesavtal som uppfyller kraven i dataskyddsförordningen?	Ja. Det finns mallar för att teckna personuppgiftsbiträdesavtal och de uppfyller de grundläggande kraven enligt dataskyddsförordningen.
C	Har personuppgiftsbiträdesavtal ingåtts med alla personuppgiftsbiträden som hanterar personuppgifter för organisationens räkning?	Oklart. Det ska framgå av förteckning över personuppgiftsbehandlingar om det finns personuppgiftsbiträden och om personuppgiftsbiträdeavtal har tecknats. Det kan dock konstateras att förteckningen i många fall saknar uppgifter om detta. Det är möjligt att personuppgiftsbiträdesavtal i vissa fall finns, trots att uppgiften saknas i förteckningen. <i>Inga ytterligare kontroller har genomförts för att undersöka detta.</i>
D	Finns det rutiner och processer för att granska och följa upp att personuppgiftsbiträden hanterar personuppgifter korrekt och i enlighet med våra instruktioner?	Nej. Det pågår dock ett arbete med att ta fram en process för att följa upp trafikavtalen. Där ingår uppföljning av personuppgiftsbiträdesavtal. I övrigt saknas det rutiner och processer för att granska och följa upp personuppgiftsbiträden på ett systematiskt sätt.

²³ Handbok för inköp och upphandling på Trafikförvaltningen, fastställd 2025-04-23, TN-S-2992285.

²⁴ Det borde hänvisas till dataskyddsfunktionen istället.

3.8.3 Brister och risker

Inom detta kontrollområde har följande brister och risker identifierats:

- Att det saknas uppgifter om personuppgiftsbiträden och personuppgiftsbiträdesavtal i förteckning över personuppgiftsbehandlingar innebär en risk för bristande kontroll och överblick av externa parter behandling av våra personuppgifter. Det kan i förlängningen innebära risk för bristande efterlevnad avseende exempelvis ansvarsskyldighet och öka risken för oidentifierade risker och avvikelser.
- Att behovet av personuppgiftsbiträdesavtal många gånger identifieras sent i upphandlings- och inköpsprocessen försvårar möjligheten att integrera dataskydd i planering och kravställning. Det kan leda till bristande dataskyddskrav, tidsmässig press i avtalsfasen samt risk för att behandling inleds utan att kraven i dataskyddsförordningen efterlevs.
- Att det saknas rutiner och processer för att följa upp och granska personuppgiftsbiträden systematiskt innebär risk för bristande kontroll och styrning över hur personuppgiftsbiträden och deras underbiträden behandlar våra personuppgifter.

3.8.4 Dataskyddsombudets sammanfattande bedömning och rekommendationer

	Allvarlig brist/hög risk Allvarlig brist/risk som kan leda till omfattande överträdelser av dataskyddsförordningen och betydande sanktions- eller förtroenderisk.
	Betydande brist/medelhög risk Brist/risk som kan påverka efterlevnaden av dataskyddsförordningen och skapa interna problem med att efterleva processen eller svårigheter att visa ansvarsskyldigheten.
X	Mindre brist/låg risk Mindre brist eller risk med begränsad påverkan på efterlevnaden, men som bör åtgärdas för att upprätthålla en konsekvent och korrekt tillämpning av dataskyddsreglerna.
	Inga brister/risker Inga identifierade brister/risker av nämnvärd betydelse.

Dataskyddsombudets sammanfattande bedömning är att det finns rutiner för att upptäcka när det behöver tecknas personuppgiftsbiträdesavtal och att det finns mallar för att teckna sådana avtal.

Det har dock noterats att uppgifter om personuppgiftsbiträden och personuppgiftsbiträdesavtal saknas i förteckningen, samt att det saknas rutiner och processer för att följa upp och kontrollera personuppgiftsbiträden och dess

underbiträden. Detta medför risker som bör åtgärdas för att upprätthålla en konsekvent och korrekt tillämpning av dataskyddsreglerna.

För att åtgärda de brister och som ovan har identifierats rekommenderar dataskyddsombudet:

- Att förteckning över personuppgiftsbehandlingar kompletteras med personuppgiftsbiträden och hänvisningar till personuppgiftsbiträdesavtal.
- Att det säkerställs att det tidigt identifieras om ett personuppgiftsbiträdesavtal behöver tecknas.
- Att det införs rutiner och processer för att regelbundet och systematiskt följa upp och kontrollera att personuppgiftsbiträden och dess underbiträden efterlever våra krav och instruktioner.

3.9 Överföring av personuppgifter utanför EU/EES

3.9.1 Bakgrund

Överföring av personuppgifter till länder utanför EU/EES regleras särskilt i dataskyddsförordningen. Enligt artiklarna 44–49 får sådana överföringar endast ske om den personuppgiftsansvarig säkerställer att mottagarlandet eller mottagaren erbjuder en skyddsnivå som är likvärdig den inom EU/EES. Detta kan till exempel säkerställas genom att EU-kommissionen har fattat ett beslut om adekvat skyddsnivå, eller genom att lämpliga skyddsåtgärder vidtas innan överföringen genomförs. Syftet är att garantera att skyddet för de registrerades rättigheter följer med uppgifterna även utanför EU/EES.

Enligt principen om ansvarsskyldighet i artikel 5.2 och artikel 24 måste organisationer därför göra en bedömning av mottagarlandets rättsliga och praktiska skyddsnivå och vidta nödvändiga tekniska, organisatoriska och avtalsmässiga skyddsåtgärder. Ett strukturerat och riskbaserat arbetssätt minskar risken för otillräckligt skydd, personuppgiftsincidenter och intrång i den personliga integriteten.

3.9.2 Kontrollfrågor och svar

Ref.	Kontrollfråga	Svar
A	Finns det intern styrning för överföring av personuppgifter till länder utanför EU/EES säkerställer att tillämpliga dataskyddskrav beaktas?	Delvis. Det finns en stödjande vägledning från regionsledningskontoret gällande anskaffning av molntjänster och andra it-tjänster för Region Stockholm. ²⁵ Den innehåller vägledning gällande överföring till länder utanför EU/EES. Av den följer

²⁵ Vägledning för anskaffning av molntjänster och andra it-tjänster för Region Stockholm, daterad 2024-06-19, RS 2022-0265.

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		att molntjänster får användas när personuppgifter behandlas, men att utgångspunkten är att uppgifter inte ska behandlas utanför EU/EES vid behandling av skyddsvärda och känsliga personuppgifter. Det kan dock vara möjligt om tillräckligt långtgående skyddsåtgärder vidtas. Det framgår även att lagstiftning som kan ge myndigheter i andra länder rätt att ta del av informationen behöver beaktas.
B	Om överföring utanför EU/EES görs, finns det dokumentation över vilka uppgifter som överförs och till vilka mottagare? Har den rättsliga grunden för överföringen dokumenterats?	<p>Delvis. Det ska antecknas i förteckning över personuppgiftsbehandlingar om uppgifter överförs utanför EU/EES. I ett stort antal fall har dock frågan inte besvarats. I de fall frågan har besvarats ja, är inte alltid den rättsliga grunden för överföringen dokumenterad.</p> <p>Om en överföring utanför EU/EES sker ska även en tredjelandsöverföringsbedömning (Transfer Impact Assessment/TIA) dokumenteras. <i>Det har inte närmare kontrollerats om sådana har gjorts, i de fall det framgår att en överföring sker utanför EU/EES.</i></p>
C	Finns det mallar för att genomföra tredjelandsöverföringsbedömningar (Transfer Impact Assessment/TIA) och bedöms de vara tillräckliga för att uppfylla kraven i artiklarna 44-46 dataskyddsförordningen?	Ja. Det finns mallar för att genomföra tredjelandsöverföringsbedömning ²⁶ och de bedöms uppfylla kraven i artikel 44-46 dataskyddsförordningen.

3.9.3 Risker och brister

Inom detta kontrollområde har följande brister och risker identifierats:

- Att förteckning över personuppgiftsbehandlingar inte alltid besvarar frågan om uppgifter behandlas utanför EU/EES och att den rättsliga grunden för överföringen inte alltid framgår innebär risk för att tredjelandsöverföringar sker utan tillräcklig kännedom, styrning och kontroll. Det kan medföra bristande

²⁶ Finns i mallbiblioteket i word.

efterlevnad av dataskyddsförordningen samt att personuppgifter behandlas utan adekvata skyddsåtgärder.

- Att vägledningen för anskaffning av molntjänster är stödjande och inte styrande medför risk för otydlig kravbild och ett ökat tolkningsutrymme, vilket kan leda till en ojämnh och icke systematisk tillämpning av dataskyddskraven.

3.9.4 Dataskyddsombudets sammanfattande bedömning och rekommendationer

	Allvarlig brist/hög risk Allvarlig brist/risk som kan leda till omfattande överträdelser av dataskyddsförordningen och betydande sanktions- eller förtroenderisk.
	Betydande brist/medelhög risk Brist/risk som kan påverka efterlevnaden av dataskyddsförordningen och skapa interna problem med att efterleva processen eller svårigheter att visa ansvarsskyldigheten.
X	Mindre brist/låg risk Mindre brist eller risk med begränsad påverkan på efterlevnaden, men som bör åtgärdas för att upprätthålla en konsekvent och korrekt tillämpning av dataskyddsreglerna.
	Inga brister/risker Inga identifierade brister/risker av nämnvärd betydelse.

Eftersom det inte har gjorts några närmare kontroller avseende om tredjelandsöverföringsanalyser har genomförts är det svårt att göra en heltäckande sammanfattande bedömning av detta kontrollområde. De brister och risker som har identifierats bedöms i nuläget som låga, men de bör åtgärdas för att upprätthålla en konsekvent och korrekt tillämpning av dataskyddsreglerna.

För att åtgärda de brister och risker som ovan har identifierats rekommenderar dataskyddsombudet:

- Att det säkerställs att förteckning över personuppgiftsbehandlingar kompletteras med uppgift om tredjelandsöverföring och där så sker uppgift om laglig grund för överföringen.
- Att det tas fram intern styrning kring behandling av personuppgifter utanför EU/EES som tydliggör huruvida det är tillåtet att överföra personuppgifter utanför tredje land och vad som i sådana fall krävs.

3.10 Interna utbildningar och medvetenhet

3.10.1 Bakgrund

Utbildning och medvetenhet är avgörande för att säkerställa att medarbetare förstår sitt ansvar och följer dataskyddsförordningens krav. Enligt principen om

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

ansvarsskyldighet i artikel 5.2 ska den personuppgiftsansvarige säkerställa att all personal som hanterar personuppgifter har tillräcklig kunskap för att personuppgifter ska behandlas på ett lagligt, korrekt och säkert sätt. Regelbunden utbildning och information bidrar till att minska risken för felaktig hantering av personuppgifter, stärker förmågan att upptäcka och agera vid personuppgiftsincidenter och ökar förståelsen för de säkerhetskrav som gäller i verksamheten.

3.10.2 Kontrollfrågor och svar

Ref.	Kontrollfråga	Svar
A	Genomförs regelbundna utbildningar inom dataskydd för medarbetare?	<p>Ja. Det finns flera utbildningar inom dataskydd.</p> <p>Hantera GDPR i Region Stockholm Utbildningen är en grundläggande digital utbildning som ägs av Regionledningskontoret och riktar sig till samtliga medarbetare inom Region Stockholm. Utbildningen är inte obligatorisk för medarbetare på Trafikförvaltningen.</p> <p>Informationssäkerhet och dataskydd för informationsägare och informationsförvaltare Utbildningen är en lärarledd, frivillig utbildning som riktar sig till informationsägare och informationsförvaltare. Utbildningen ägs av informationssäkerhets- och dataskyddsfunktionen.</p> <p>Nanolearningutbildning rörande informationssäkerhet och dataskydd samt kunskapstest Utbildningen är digital och skickas via e-post till nyanställda. Den är obligatorisk.</p> <p>En gång per år skickas även kunskapsfrågor ut till alla medarbetare. Om någon svarar fel får medarbetaren en lektion med information inom området. Lektionerna är desamma som ingår den obligatoriska utbildningen för nyanställda.</p>

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		Utbildningen och kunskapstestet ägs av informationssäkerhets- och dataskyddsfunktionen.
B	<p>Innehåller utbildningen/-arna grundläggande moment om dataskydd?</p> <p>För att utbildningen ska anses innehålla grundläggande moment bör åtminstone följande delar ingå i utbildningen: begrepp och definitioner, roller och ansvar, grundläggande principer, registrerades rättigheter och hantering av personuppgiftsincidenter.</p>	<p>Delvis.</p> <p>Hantera GDPR i Region Stockholm Utbildningen innehåller information om grundläggande begrepp och definitioner, roller och ansvar, grundläggande principer enligt dataskyddsförordningen, registrerades rättigheter, hantering av personuppgiftsincidenter m.m. Utbildningen bedöms innehålla grundläggande moment inom dataskydd.</p> <p>Informationssäkerhet och dataskydd för informationsägare och informationsförvaltare Utbildningen innehåller information om grundläggande begrepp och definitioner, roller och ansvar, förordningens grundläggande principer, registrerades rättigheter, hantering av personuppgiftsincidenter och information om att personuppgiftsbehandlingar ska dokumenteras.</p> <p>Utbildningen bedöms innehålla grundläggande moment inom dataskydd.</p> <p>Nanolearningutskick rörande informationssäkerhet och dataskydd samt kunskapstest Lektionerna som skickas till nyanställda och frågorna som skickas en gång per år rör definitionen av personuppgifter och hantering av personuppgiftsincidenter. Övrigt innehåll rör phishing, säker inloggning, sociala medier, desinformation m.m. vilket i första hand är informationssäkerhetsfrågor, men som är viktiga även ur ett dataskyddsperspektiv.</p>

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

		Utbildningen bedöms inte innehålla samtliga grundläggande moment inom dataskydd som nyanställda behöver känna till.
C	Finns det information på intranätet (eller motsvarande) och är innehållet fullständigt, aktuellt och korrekt i förhållande till gällande lag, styrdokument och rutiner?	Ja. Information finns publicerad på intranätet. ²⁷ Innehållet är på det stora hela korrekt i förhållande till gällande lagstiftning. Informationen behöver dock uppdateras för att fullt ut stämma överens med interna riktlinjer och processer. Innehållet är omfattande, vilket påverkar överskådligheten.
D	Finns det rutiner för att följa upp att medarbetare har genomfört obligatoriska utbildningar inom dataskydd?	Oklart. Det framgår av den framtagna beslutsprocessen för obligatoriska utbildningar och indirekt av medarbetarpolicyn att chefer ansvarar för att följa upp att sina medarbetare har genomfört obligatoriska utbildningar. <i>Det har inte närmare kontrollerats om chefer har följt upp detta.</i>
E	Utvärderas effekten av utbildningar genom t.ex. uppföljning och kunskapstester?	Ja. Under 2023 och 2024 genomförde dataskyddsombudet ett kunskapstest relaterat till dataskydd. Hela organisationen omfattades av testen. 2024 års testresultat visade att kunskapsnivån hos de flesta respondenterna är god till mycket god. Till exempel visade svaren att de flesta respondenterna kunde identifiera personuppgifter, hade kännedom om de grundläggande principerna inom dataskydd och förmåga att identifiera personuppgiftsincidenter. Däremot var kunskapen om ansvarsfrågor och var man ska anmäla inträffade eller misstänkta personuppgiftsincidenter lägre. Under 2025 skickade informationssäkerhets- och dataskyddsfunktionen ut frågor kopplat till nanolearningutbildningen. Hela organisationen omfattades av testet. Drygt hälften besvarade frågorna. Resultatet visade på bra till mycket bra kunskaper inom de olika områdena. Vidare genomförde dataskyddsombudet en enkätundersökning riktad till informationsägare och informationsförvaltare. Av svaren framgick att fler informationsägare och

²⁷ [Region Stockholm intranät - Dataskydd GDPR](#)

		informationsförvaltare själva anser att de saknar utbildning eller tillräcklig utbildning inom dataskydd och sin roll som informationsägare/informationsförvaltare.
--	--	---

3.10.3 Brister och risker

Inom detta kontrollområde har följande brister och risker identifierats:

- Att den utbildning som är obligatorisk för nyanställda medarbetare (det vill säga nanolearningsutbildningen) inte innehåller alla nödvändiga moment relaterat till dataskydd innebär risk för att medarbetare inte kommer att tillförska sig tillräcklig kunskap inom dataskydd. Det kan leda till bristande kunskap inom dataskyddsförordningen samt att interna rutiner och processer inte efterlevs.
- Att flera informationsägare och informationsförvaltare har uppgett att de saknar utbildning eller tillräcklig utbildning inom dataskydd och sin roll som informationsägare/informationsförvaltare innebär risk för att personuppgifter inte hanteras enligt lag och interna instruktioner.
- Att informationen på intranätet inte fullt ut stämmer överens med interna riktlinjer och gällande processer, samt att materialet är omfattande, innebär risk för att det är svårt för medarbetare att hitta rätt information. Det kan leda till att medarbetare agerar i strid med dataskyddsförordningen och interna styrdokument.

3.10.4 Dataskyddsombudets sammanfattande bedömning och rekommendationer

	Allvarlig brist/hög risk Allvarlig brist/risk som kan leda till omfattande överträdelser av dataskyddsförordningen och betydande sanktions- eller förtroenderisk.
	Betydande brist/medelhög risk Brist/risk som kan påverka efterlevnaden av dataskyddsförordningen och skapa interna problem med att efterleva processen eller svårigheter att visa ansvarsskyldigheten.
X	Mindre brist/låg risk Mindre brist eller risk med begränsad påverkan på efterlevnaden, men som bör åtgärdas för att upprätthålla en konsekvent och korrekt tillämpning av dataskyddsreglerna.
	Inga brister/risker Inga identifierade brister/risker av nämnvärd betydelse.

Sammanfattningsvis är dataskyddsombudets bedömning att organisationen har utbildningar inom dataskydd och att innehållet i dem i huvudsak omfattar de moment som krävs för att skapa grundläggande förståelse för dataskyddsförordningens krav.

Trafikförvaltningen
IT-avdelningen
Strategi och styrning

GRANSKNINGSRAPPORT
2026-03-12
Version
1.0

Ärende/Dok. id.
TN 2026-0103
Infosäk. klass
K1 (Öppen)

Detta utgör en viktig förutsättning för efterlevnad. Dock innehåller utbildningen som är obligatorisk för nyanställda inte alla nödvändiga moment.

De identifierade riskerna bedöms i nuläget ha begränsad påverkan på den faktiska efterlevnaden, men bör åtgärdas för att upprätthålla en konsekvent och korrekt tillämpning av dataskyddsreglerna.

För att åtgärda de brister och risker som ovan har identifierats rekommenderar dataskyddsombudet:

- Att det säkerställs att den obligatoriska utbildningen som riktar sig till nyanställda kompletteras med nödvändiga moment inom dataskydd.
- Att den utbildning som riktar sig till informationsägare och informationsförvaltare görs obligatorisk för de som innehar rollen.
- Att det införs en process för att kontrollera att de som ska ha genomgått utbildningen har gjort det.
- Att sidorna på intranätet rörande dataskydd uppdateras så att de korrekt återger interna processer och blir mer överskådliga.

Stockholm den 12 mars 2026.

Johanna Wallerström
Dataskyddsombud