REGIONREVISORERNA

Rapport nr 17/2025

Trafiknämndens kontroll över färdtjänstens efterlevnad av dataskyddsförordningen (GDPR)

Innehållsförteckning

1. Sammanfattande analys och rekommendationer

Revisionskontoret bedömer att trafiknämnden endast delvis har säkerställt en ändamålsenlig styrning och kontroll i efterlevnaden av dataskyddsförordningen i färdtjänstens verksamhet. Det finns grundläggande strukturer såsom en organisation med definierade roller, styrande dokument, rutiner för incidenthantering samt registerförteckning och hantering av registrerades rättigheter. Det finns även en process för årlig rapportering om dataskydd till nämnden. Granskningen visar dock att styrning, löpande kontroll och rapportering inte är fullt ändamålsenliga. Ansvarsfördelningen är delvis otydlig, vissa styrdokument saknar aktualitet och uppföljningen av underleverantörer är bristfällig. Den löpande kontrollen behöver utvecklas för att bli mer systematisk, bland annat genom granskning av registerförteckningen, redovisning av skyddsåtgärder vid tredjelandsöverföringar och uppföljning av medarbetarnas utbildningar. Vidare framgår det inte tydligt i den årliga rapporteringen hur färdtjänstens verksamhet omfattas, vilket innebär att nämnden inte har fullständig information för att säkerställa efterlevnad.

Sammantaget finns en grund för dataskyddsarbetet, men styrning, uppföljning och rapportering behöver stärkas för att minska risken för brister i hantering av personuppgifter.

Rekommendationer:

1. Trafiknämnden bör säkerställa att hantering av färdtjänstresenärernas personuppgifter är tydligt spårbara i alla led samt att personuppgiftsbiträden och underbiträden är tydligt dokumenterade.

2. Trafiknämnden bör säkerställa att resenärer i färdtjänstens verksamhet tydligt informeras om behandling av personuppgifter i tredje land samt redogör för vilka skyddsåtgärder som tillämpas.

3. Trafiknämnden bör säkerställa att registerförteckningen i färdtjänstens verksamhet regelbundet hålls uppdaterad.

2. Utgångspunkter för granskningen

2.1 Bakgrund

Dataskyddsförordningens syfte (GDPR, General Data Protection Regulation) är att skydda enskildas personuppgifter. Alla organisationer och myndigheter inom EU som hanterar personuppgifter måste säkerställa att den personliga integriteten skyddas genom att samla in, behandla och lagra personuppgifter på ett säkert och lagligt sätt. För färdtjänstens personuppgifter är trafiknämnden personuppgiftsansvarig.

År 2021 visade en granskning, som genomfördes av trafikförvaltningens dataskyddsombud, att färdtjänsten i Region Stockholm inte uppfyllde dataskyddsförordningens krav på dokumentation. Ett grundläggande krav är att alla behandlingar av personuppgifter ska dokumenteras. Trafiknämnden hade inte säkerställt att skydd och kontroll av personuppgifter var dokumenterade.

Enligt lagen om färdtjänst är färdtjänst ett kommunalt ansvar med möjlighet att överlåta uppgifterna till region. Kommunerna i Region Stockholm har överlåtit färdtjänstuppgifterna till Region Stockholm. Färdtjänsten i Region Stockholm hanterar enskildas personuppgifter och ansvarar bland annat för att handlägga färdtjänsttillstånd, genomföra beställning av färdtjänstresor och erhålla kundservice för de resenärer som beviljats färdtjänst. Färdtjänsten hanterar också känsliga personuppgifter eftersom det angår resenärernas hälsa. Region Stockholm har organiserat verksamheten under trafiknämndens ansvar, och nämnden har delegerat beslut om upphandling till färdtjänstutskottet.

Revisorerna har, utifrån en riskanalys, beslutat i sin revisionsplan för år 2025 att granska trafiknämndens kontroll över personuppgifter i färdtjänstverksamheten i Region Stockholm. Om personuppgifter inte hanteras korrekt finns det risk att personuppgifter hamnar i orätta händer, det vill säga blir tillgängliga för obehöriga personer eller aktörer som inte har rätt att ta del av dem. Det finns även en risk att Integritetsskyddsmyndigheten (IMY) utfärdar en varning eller en sanktionsavgift till trafiknämnden.

2.2 Syfte och revisionsfrågor

Syftet med granskningen är att bedöma om trafiknämnden avseende verksamheten gällande färdtjänst säkerställt en tillräcklig styrning och kontroll i efterlevnaden av dataskyddsförordningen.

För att besvara syftet har följande revisionsfrågor formulerats:

2.1.1. Styrning

Har trafiknämnden för färdtjänsten säkerställt en tillräcklig styrning, dvs att det finns:

- En ändamålsenlig dataskyddsorganisation?
- Ändamålsenliga policys, riktlinjer och rutiner för dataskydd?

2.1.2. Löpande kontroll

Har trafiknämnden för färdtjänsten säkerställt en tillräcklig löpande kontroll, dvs att det finns:

- En organisation för incidenthantering utifrån kraven i dataskyddsförordningen?
- En registerförteckning över personuppgiftsbehandlingar i färdtjänstverksamheten som är upprättade i enlighet med dataskyddsförordningen?
- Rutiner för hantering av de registrerades rättigheter med fokus på rättelse, radering och begränsning i färdtjänstverksamheten i enlighet med dataskyddsförordningen?

- Åtgärder som vidtagits för att säkerställa att de krav som följer av dataskyddsförordningen är välkända hos medarbetarna inom trafiknämndens förvaltning som ansvarar för färdtjänsten?

2.1.3. **Uppföljning**

Har trafiknämnden säkerställt en tillräcklig uppföljning?

2.3 Avgränsningar och ansvarig nämnd

Granskningen är övergripande och avgränsad till trafiknämndens styrning, kontroll och uppföljning av hanteringen av personuppgifter i färdtjänstverksamheten i nuläget. Granskningens iakttagelser bygger på dokumentationsstudier av styrande dokument, rutiner, policyer, incidentrapporter, registerförteckning, aktuella leverantörsavtal (för taxi med fem leverantörer, rullstolstaxi med fyra leverantörer, kundservice och beställningscentral) samt information från intervjuer.

2.4 Revisionskriterier

Revisionskriterierna utgör de bedömningsgrunder som bildar underlag för granskningens analyser, slutsatser och bedömningar. Revisionskriterier för denna granskning är:

- **Kommunallagen 6 kap. 6 §** som anger att nämnder och styrelser ska se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har beslutat om samt bestämmelser i lag eller annan författning som gäller för verksamheten. De ska också se till att den interna kontrollen är tillräcklig för att förebygga fel och oegentligheter i verksamheten, och att verksamheten bedrivs på ett i övrigt tillfredsställande sätt.
- **Kommunallagen 10 kap. 8 §** som anger att när skötseln av en kommunal angelägenhet genom avtal har lämnats över till en privat utförare, ska kommunen eller regionen kontrollera och följa upp verksamheten.

- **Europaparlamentets och rådets förordning (EU)** 2016/679 av den 27 april 2016 som anger skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter. (Allmän dataskyddsförordning)
- **Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning kap 3. § 3 (Dataskyddslagen)** som anger att myndigheter får behandla integritetskänsliga uppgifter om behandlingen är nödvändig för handläggningen av ett ärende. Lagen kompletterar dataskyddsförordningen för offentlig verksamhet i myndighetsutövning.
- **Riktlinjer för informationssäkerhet (RS 2020–0148)** anger att i de fall nämnder och bolag uppdrar åt andra att hantera information ska avtalet om denna hantering omfatta sådana krav att informationen hanteras i enlighet med

dessa riktlinjer. Den nämnd eller det bolag som avtalar med annan om hantering av information ansvarar också för en uppföljning av utförandet och de avtal som ligger till grund för utförandet, så att informationen ges ett avtalsenligt skydd.

2.5 Metod och kvalitetssäkring

Granskningen har genomförts med följande steg:

- Granskning av styrande dokument, rutiner, dagordningar från färdtjänstutskottet och trafiknämndens sammanträden, leverantörsavtal samt dataskyddsombudets rapportering. Dagordningarna i färdtjänstutskottet har granskats i syfte att avgöra om utskottet respektive nämnden har berett eller behandlat ärenden med anknytning till dataskydd/ dataskyddsförordningen.
- Granskning av registerförteckning respektive rapporter för personuppgiftsbehandlingar avseende färdtjänstresenärer. Valda kontrollpunkter framgår i bilaga 3.
- Granskning av incidentloggar för åren 2021–2025. Valda kontrollpunkter framgår i bilaga 3.
- Intervjuer med informationsägare/sektionschef Färdtjänst, informationsförvaltare, dataskyddsombud, två representanter från IT-avdelningen, chef för avtalsenheten på Sektion Färdtjänst samt tre affärsförvaltare på Sektion Färdtjänst.

Ett utkast av rapporten har faktakontrollerats med intervjupersoner och ledningen för trafikförvaltningen. I samband med kvalitetsgranskningen har det framkommit att trafikförvaltningen har uppdaterade dokument samt IT-system. Dessa kommenteras i fotnoter. Intern kvalitetssäkring har gjorts på revisionskontoret av revisionsdirektör Richard Norberg.

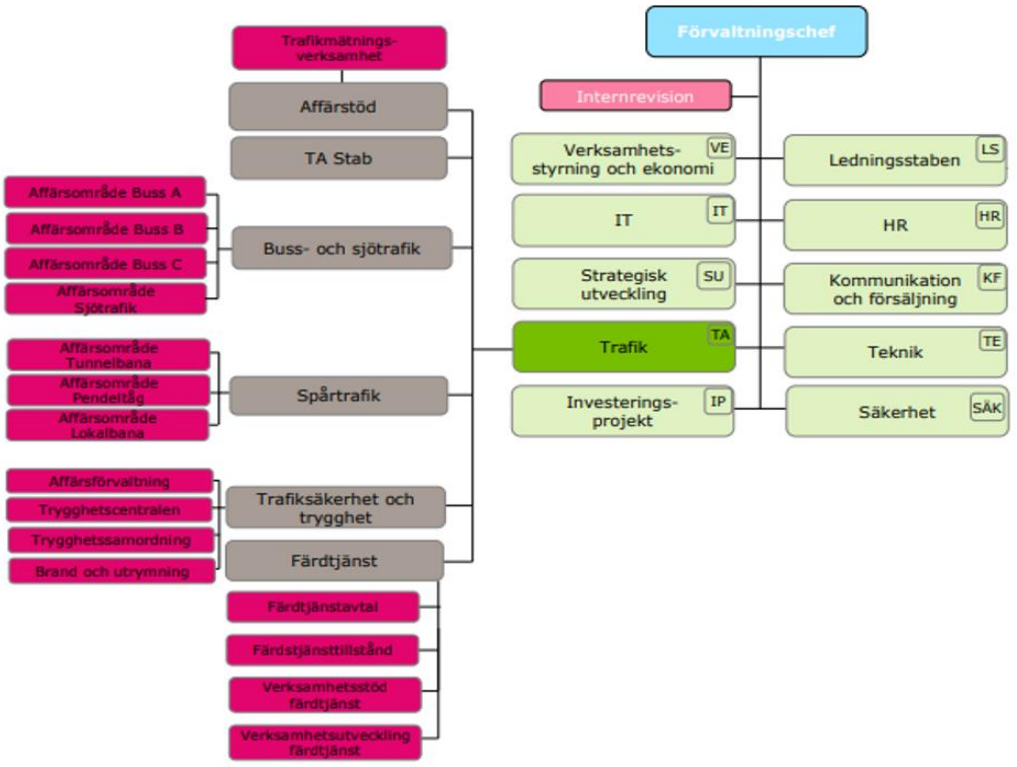
3. Resultat av granskningen

3.1 Styrning

Inledning:

Med ändamålsenlig avses att nödvändiga roller och ansvar är tydligt definierade i organisationen samt att det finns dokumenterade interna policys och rutiner. Principen om ansvarsskyldighet (artikel 5) i dataskyddsförordningen innebär att den personuppgiftsansvarige måste kunna visa att förordningen efterlevs. För myndigheter som behandlar personuppgifter, såsom färdtjänstens verksamhet, är det obligatoriskt att ett dataskyddsombud utses med en oberoende ställning, tillhandahålls tillräckliga resurser och kompetens (artikel 37).

3.1.1 Organisation och roller



Figur 3.1.1. Organisationsbild för trafikavdelningen

Färdtjänstverksamheten ligger under trafikavdelningen och benämns sektion Färdtjänst.[1] Sektionen omfattar fyra arbetsgrupper och har en sektionschef. Trafikförvaltningens arbetsordning anger att alla chefer har ett verksamhetsansvar som innebär att de har ansvar för verksamhet, ekonomi och medarbetare i enlighet med gällande lagar.

Trafikförvaltningens arbetsordning[2] reglerar att IT-avdelningen har ett övergripande och samordnat ansvar för informationssäkerhet och dataskydd för hela förvaltningen. Enligt intervjuer förvaltas IT-system för färdtjänsten av IT-avdelningen. Avdelningen bistår vid kravställning vid upphandlingar men följer inte upp leverantörernas efterlevnad av kraven.

Revisionskontoret noterar att varken arbetsordningen eller beslutsordningen uttryckligen nämner chefers ansvar för personuppgifter, men detta framgår i dokumentet *Informationsägare*. Personuppgiftshanteringen följer verksamhetsansvaret och att

[2] Ersatt efter tiden för granskning med ny arbetsordning.

informationsägaren, oftast en avdelnings- eller sektionschef, har det yttersta ansvaret för att personuppgifter hanteras korrekt. Dokumentet anger bland annat att:

- informationsägaren äger och förvaltar personuppgiftsbehandlingar
- ansvarar för att innehållet i personuppgiftsbehandlingen är korrekt över tid
- upprättar och förvaltar personuppgiftsbiträdesavtal
- leder hanteringen av personuppgiftsincidenter i sin verksamhet
- anmäler personuppgiftsincidenter inom sin verksamhet till (IMY) Integritetsskyddsmyndigheten

Inom Sektion Färdtjänst är sektionschefen informationsägare och har stöd av en informationsförvaltare. I intervjuer framkommer att informationsförvaltaren på Sektion Färdtjänst bedömer personuppgiftsincidenter tillsammans med informationsägaren regelbundet och handlägger samtliga begäran om registerutdrag som inkommer från resenärer. Informationsförvaltarens roll är central för all hantering av personuppgifter inom Sektion Färdtjänst.

Dataskyddsombudets roll

Fullmäktiges reglementen anger att trafiknämnden är personuppgiftsansvarig och ska utse ett dataskyddsombud. Trafiknämnden har genom delegationsbeslut utsett dataskyddsombud för trafiknämnden, AB Storstockholms Lokaltrafik samt Waxholms Ångfartygs AB gemensamt. Enligt arbetsordningen ansvarar dataskyddsombudet för att utbilda och informera verksamheten samt ge råd och rekommendationer i dataskyddsfrågor. Dataskyddsombudet ska även enligt arbetsordningen granska och följa upp att dataskyddsförordningen efterlevs vilket är i linje med lagstiftningen.

Dataskyddsförordningen kräver att ombudet är oberoende och kompetent. Trafiknämndens ombud är jurist och placerad på trafikförvaltningens IT-avdelning. Ombudet har deltagit i framtagande av styrande dokument, samordnat dataskyddsfrågor och genomfört konsekvensbedömningar. I praktiken innebär det att dataskyddsombudet i vissa fall granskar sina egna insatser.

Granskningen visar att arbetsordningen genomgår en revidering för att renodla ombudets roll, säkerställa oberoende och överlåta dataskyddsarbetet till dataskyddsfunktionen.

3.1.2 Styrande dokument och övriga interna dokument

Regionens styrdokument följer lagstiftning och sammanfattas i *Region Stockholms policy för verksamhetsskydd* samt *Riktlinjer för informationssäkerhet*[3]. Dessa reglerar skydd av informationstillgångar inom samtliga nämnder och bolag.

Revisionskontoret noterar att det är oklart hur befogenheter har delegerats från trafiknämnden till trafikförvaltningen. Den nuvarande delegationsordningen saknar delegerade befogenheter för beslut om registrerades rättigheter och anmälan av

[3] Ersatt efter tiden för granskning med ny riktlinje Riktlinjer för informationssäkerhet och dataskydd RS 2025-0418

personuppgiftsincidenter till tillsynsmyndigheten. Intervjuer bekräftar att ett arbete pågår för att förtydliga detta i en ny delegationsordning.

Trafikförvaltningen har gemensamma styrdokument, rutiner och checklistor för hantering av personuppgifter och incidenter samt särskilda rutindokument för färdtjänstsektionen. Revisionskontoret har granskat dokumenten och noterar att vissa dokument saknar datum för beslut, beslutsfattare och finns i flera versioner.

Riktlinjer för informationssäkerhet anger att incidenter som rapporteras till tillsynsmyndighet även ska rapporteras till regionstyrelsen. Granskningen visar att det i rutiner och rollbeskrivningar saknas tydliga instruktioner för hur rapporteringen till regionstyrelsen ska genomföras.

Färdtjänstens personuppgiftsbiträdesavtal med färdtjänstens leverantörer

Regionrevisorerna har genomfört en granskning med färdtjänstens leverantörer som hanterar personuppgifter.[4] Artikel 28.2 anger att personuppgiftsbiträdet inte får anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige. Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar.

Integritetsskyddsmyndigheten (IMY) uttrycker skyldigheterna så att innan ett underbiträde får anlitas måste det ursprungliga biträdet först få skriftlig tillåtelse av den personuppgiftsansvariga att anlita underbiträden. Därefter måste biträdet säkerställa att det finns ett avtal med underbiträdet med samma nivå av skydd för de registrerades personuppgifter som finns i avtalet mellan den personuppgiftsansvariga och personuppgiftsbiträdet.

Revisionskontorets granskning visar att samtliga avtal innehåller personuppgiftsbiträdesavtal som säkerställer efterlevnad av kraven i dataskyddsförordningen. Däremot framgår att de granskade avtalen, med undantag för avtalet som rör kundtjänst, saknar ett skriftligt förhandstillstånd hos trafikförvaltningen för underbiträden (underleverantörer) för avtalet med taxi och rullstolstaxi (enskilda åkare och åkeribolag) samt beställningscentralen.

Vid intervjuer har tjänstepersoner inom trafikförvaltningen uppgett att en analys har genomförts av jurist på trafikförvaltningen, vilken visat att underleverantörerna (enskilda åkare och åkeribolag) inte ska betraktas som underbiträden. Revisionskontoret har efterfrågat skriftliga underlag som bekräftar analysen. Detta underlag har inte kunnat tillhandahållas. Revisionskontoret konstaterar att det saknas underlag för trafiknämndens ställningstagande att enskilda åkare och åkeribolag inte är att betrakta som underbiträden.

[4] Ramavtal för vanlig taxi (5 avtal); Ramavtal för rullstolstaxi (4 avtal); Avtal för Kundtjänst samt Beställningscentralen

För de avtal som revisionskontoret granskat saknas dokumenterad och systematisk uppföljning av personuppgiftsbiträdesavtalen på färdtjänstsektionens avtalsenhet vilket inte är i enlighet med kommunallagen (KL 10 kap. 8 §). IT-avdelningen bistår vid upphandling med systemkrav på leverantörens IT-system men har ingen roll i kontrollen av att kraven på dataskydd är uppfyllda.

3.2 Bedömning styrning

Revisionskontoret bedömer att trafiknämnden kan visa en etablerad och grundläggande dataskyddsorganisation med utsett dataskyddsombud, en dataskyddsfunktion, informationsägare och rutiner för personuppgiftshantering. Det finns också styrande dokument som följer lagstiftningen. Granskningen visar dock att styrningen inte framstår som helt ändamålsenlig. Bedömningen grundas på följande iakttagelser:

- Den nuvarande delegationsordningen saknar delegerade befogenheter för beslut om registrerades rättigheter och anmälan av personuppgiftsincidenter till tillsynsmyndigheten.

- Vissa interna styrdokument saknar tydlighet och aktualitet, vilket riskerar att skapa osäkerhet kring vilka rutiner som gäller och hur de ska tillämpas.

- Det saknas dokumenterad och systematisk uppföljning av personuppgiftsbiträdesavtal, vilket innebär att nämnden inte följer kommunallagen och kan visa att leverantörer följer avtalade krav för dataskydd.

- Majoriteten av de granskade avtalen saknar förvaltningens skriftliga förhandstillåtelse för underbiträden. Detta innebär att kontrollen över kedjan av personuppgiftsbiträden inte är tillräckligt säkerställd, vilket i sin tur innebär en risk för att resenärernas personuppgifter inte hanteras på ett säkert sätt.

3.3 Löpande kontroll

Inledning:

Revisionskontoret har granskat färdtjänstverksamhetens kontroll utifrån dataskyddsförordningen med fokus på incidenthantering, registerhantering, de registrerades rättigheter samt åtgärder för att säkerställa att medarbetare får adekvat utbildning.

3.3.1 Incidenthantering

Trafikförvaltningen har en gemensam processbeskrivning för hantering av personuppgiftsincidenter vilken är i enlighet med dataskyddsförordningens artikel 33–34. Som tidigare nämnts finns flera styrande dokument. För personuppgiftsincidenter specifikt finns två identiska dokument som beskriver processen vid hantering av personuppgiftsincidenter, en checklista samt en rutin för informationssäkerhetsincidenter.

Revisionskontoret konstaterar att det vid tiden för granskning i samtliga dokument framgår att trafikförvaltningen ska säkerställa att incidenter kan upptäckas, rapporteras och åtgärdas så att anmälan till IMY görs inom rätt tid, det vill säga senast 72 timmar efter att incidenten upptäckts. Revisionskontoret noterar att det däremot inte framgår av dokumenten vilket dokument som är överordnat vilket, eller som nämns tidigare, hur rapportering av anmälningar till IMY ska rapporteras vidare till regionstyrelsen.

Intervjuer visar att på färdtjänstsektionen är det informationsförvaltaren, tillsammans med informationsägaren som bedömer misstänkta personuppgiftsincidenter löpande. Arbetet med att följa upp incidenter som inträffar hos personuppgiftsbiträdet utförs separerat från den ordinarie avtalsuppföljningen. Det leds av informationsägaren som biträds av informationsförvaltaren och gruppchefen för avtalsförvaltning. Vid behov konsulteras dataskyddsombudet.

Incidenter som inträffar i färdtjänstverksamheten kan inkomma via Kundtjänst, som vidarebefordrar ärendet till Service Desk som i sin tur informerar informationsförvaltaren. En incident kan även rapporteras direkt av ett personuppgiftsbiträde eller anställd vid förvaltningen. Revisionskontoret konstaterar att det finns definierade roller inom färdtjänstsektionen för att hantera personuppgiftsincidenter.

Revisionskontoret har granskat samtliga rapporterade incidentloggar under perioden 2021–2025, hämtade från arbetsytan Webforum. Revisionskontoret konstaterar att de tillhandahållna loggarna i huvudsak är upprättade i enlighet med dataskyddsförordningen artikel 32 och kan därmed läggas till grund för personuppgiftsincidentrapporteringen i enlighet med artikel 33-34. Loggarna saknar dock uppgifter om tidsangivelser och om informationsägaren genomfört bedömningar, vilket de styrande dokumenten anger ska registreras. Vidare framgår det inte om incidenten gäller en personuppgiftsbehandling som hanteras av anlitade personuppgiftsbiträden eller underbiträden.

3.3.2 Registerförteckning

Registerförteckningar innebär enligt dataskyddsförordningens artikel 30 att den personuppgiftsansvarige, personuppgiftsbiträdet och deras företrädare ska föra ett skriftligt register över vilka personuppgiftsbehandlingar som utförs. Det är den personuppgiftsansvarige som ska identifiera och dokumentera behandlingar av personuppgifter samt säkerställa att registerförteckningen hålls aktuell och korrekt. Revisionskontoret har granskat registerförteckningen över personuppgiftsbehandlingar som avser färdtjänstresenärer.

Förteckningen omfattar åtta behandlingar och dokumenteras i systemstödet Draftit[5] där varje behandling omfattar ett eget separat dokument. Granskningen visar att samtliga granskade behandlingar i huvudsak följer dataskyddsförordningens ansvarsskyldighet och innehåller information som krävs enligt artikel 30 för behandlingar av

[5] Draftit har efter tiden för granskning ersatts med Iris.

personuppgifter. Bland annat anges varför personuppgifterna behandlas, vilka personuppgifter som sparas och vem som får ta del av uppgifterna.

I granskningen har det framkommit att dataskyddsombudet inte har genomfört någon inventering av färdtjänstens personuppgiftsbehandlingar sedan denne tillträdde 2024 och att det saknas dokumenterade kontroller av behandlingarna. Dataskyddsfunktionen har dock initierat en dialog med färdtjänstsektionen om att utveckla informationen till registrerade avseende personuppgiftsbehandlingar. Enligt intervju pågår diskussion om att eventuellt dela upp behandlingar som bedömts vara för övergripande.

3.3.3 Registrerades rättigheter

Revisionskontoret har granskat om resenärerna får tydlig information om sina rättigheter i enlighet med artikel 12–23. Färdtjänstsektionen har tagit fram skriftlig information till resenärer som omfattar rättelse, radering, begränsning av behandling samt uttag av uppgifter vid ansökan om färdtjänst, resor och betalning för utförda färdtjänstresor. Trafikförvaltningen har också en gemensam rutin för hantering av förfrågningar baserade på den registrerades rättigheter som handläggs enligt rutinen på färdtjänstsektionen.

Relevant information om den registrerades rättigheter framgår på Färdtjänsts webbplats, i foldrar, och på ansökningsblanketter. Det framgår även hur resenären kan kontakta dataskyddsombudet, både via regionens och färdtjänsts webbplats.

På Färdtjänsts webbplats framgår att personuppgifter överförs till tredje land (utanför EU/EES) i samband med att resenären ringer beställningscentralen för att boka en resa. Intervjuer visar att leverantören hanterar samtalen i Senegal, Moldavien och Estland, med lokal personal som utbildats i svenska. Samtalen, som kan innehålla känsliga personuppgifter, lagras i tre månader i tredje land. Revisionskontoret konstaterar att det av informationen på Färdtjänstens webbplats inte framgår hur trafikförvaltningen redogör för resenärer om vilka skyddsåtgärder som används i samband med överföringen till tredje land, vilket är ett krav enligt dataskyddsförordningens artikel 13.

3.3.4 Utbildning

Som personuppgiftsansvarig behöver trafiknämnden säkerställa att personalen har tillräcklig kunskap om dataskydd och följer fastställda rutiner. Detta är viktigt eftersom dataskyddsförordningen ställer krav på ansvarstagande, riskbedömningar och lämpliga organisatoriska åtgärder (artikel 24, 32). Utbildning är en central åtgärd för att säkerställa att dessa krav efterlevs i praktiken.

Trafikförvaltningen tillhandahåller utbildning till medarbetarna genom de e-utbildningar som tillhandahålls via Region Stockholm centralt på Lärtorget[6]. I granskningen har det framkommit att det inte sker någon kontroll eller uppföljning av om medarbetare på färdtjänstsektionen har genomfört utbildningarna.

[6] Lärtorget har efter tiden för granskning ersatts med Kompetenstorget.

3.4 Bedömning kontroll

Revisionskontoret bedömer att trafikförvaltningen har en grund för kontroll av dataskyddsförordningen genom etablerade rutiner för incidenthantering, registerhantering och omhändertagande av registrerades rättigheter. Det finns processer och roller och incidenter kan rapporteras via flera kanaler. Trots detta kan trafiknämnden inte fullt ut visa att kontrollen är systematisk och kontinuerlig, vilket innebär en risk att centrala delar av dataskyddsarbetet inte följs upp på ett sätt som minskar risken för brister i hanteringen av personuppgifter. Bedömningen grundas på följande iakttagelser:

- Incidenthanteringsprocessen saknar tydlig prioriteringsordning, systematisk uppföljning av personuppgiftsbiträden eller underbiträdens incidenter samt rutiner för rapportering till regionstyrelsen.

- Registerförteckningen saknas dokumenterade kontroller av behandlingarna som säkerställer att förteckningen används aktivt och hålls uppdaterad.

- Vid överföring av personuppgifter till tredje land saknas redovisning av vilka skyddsåtgärder som används.

- Det sker ingen uppföljning av att medarbetarna har genomfört en dataskyddsutbildning.

3.5 Uppföljning

Inledning:

Enligt kommunallagen har nämnden det yttersta ansvaret för att verksamheten bedrivs i enlighet med lagar och fullmäktiges mål. Ansvarsskyldighet är även en av huvudprinciperna i dataskyddsförordningen (artikel 5).

3.5.1 Dataskyddsombudets årsrapportering

Trafiknämnden beslutar om en granskningsplan vilken dataskyddsombudet genomför med avrapportering i nämnd en gång per år. Syftet är att ge nämnden möjlighet att bli informerad, styra och följa upp behandlingen av personuppgifter inom verksamheten.

Revisionskontoret har tagit del av årsrapporterna för de senaste fyra åren (2021–2024) och konstaterar att rapportering sker till ansvarig nämnd för varje verksamhetsår. Rapporteringen sker genom ett tjänsteutlåtande som redovisar centrala delområden kopplade till uppföljning av dataskyddsförordningen.

För år 2021 redovisades färdtjänstens verksamhet separat till den dåvarande personuppgiftsansvariga färdtjänstnämnden. Från och med 2022 har redovisningen skett till trafiknämnden. Sedan färdtjänstnämnden upphörde 2023 finns ingen separat rapportering för färdtjänstens verksamhet som i stället ingår i den övergripande rapporteringen för de verksamheter som ingår i hela trafikförvaltningen.

I granskning av färdtjänstutskottets möteshandlingar för 2024–2025 har ingen rapportering eller beredning skett för personuppgifter i färdtjänstens verksamhet.

3.6 Bedömning uppföljning

Trafiknämnden har en etablerad process för årlig rapportering om dataskydd, men granskningen visar att det inte tydligt framgår hur färdtjänstens verksamhet omfattas, vilket innebär en risk att nämnden inte har fullständig information för att säkerställa efterlevnad. Eftersom det varken framgår tydligt i dataskyddsombudets rapportering till nämnden eller att dataskydd beretts i färdtjänstutskottet, finns en risk att nämnden inte har försäkrat sig om att färdtjänstens verksamhet uppfyller kraven i dataskyddsförordningen och sin ansvarsskyldighet.

4 Svar på syfte och revisionsfrågor

Syftet med granskningen är att bedöma om trafiknämnden som är personuppgiftsansvarig för resenärer inom färdtjänstverksamheten har säkerställt en tillräcklig styrning och kontroll i efterlevnaden av dataskyddsförordningen. Granskningen visar att grundläggande strukturer finns, men att styrning och kontrollen behöver stärkas för att säkerställa systematisk uppföljning och minska risken för brister i hantering av personuppgifter.

Revisionsfråga	Svar på revisionsfråga	Motiv för bedömning
En ändamålsenlig dataskyddsorganisation?	Ja	Det finns en grundläggande struktur för kontroll av färdtjänstverksamhetens personuppgiftshantering.
Ändamålsenliga policys, riktlinjer och rutiner för dataskydd?	Delvis	Det finns i huvudsak ändamålsenliga styrdokument men det saknas skriftligt förhandstillstånd hos trafikförvaltningen för underbiträden vilket innebär att kontrollen över kedjan av personuppgiftsbiträden inte är tillräckligt säkerställd.
En ändamålsenlig organisation för incidenthantering utifrån kraven i dataskyddsförordningen?	Ja	Det finns i huvudsak en ändamålsenlig organisation för incidenthantering.
Det finns register över personuppgiftsbehandlingar i färdtjänstverksamheten som är	Delvis	Det finns ett register för färdtjänstverksamheten men risk finns att registret inte är komplett eftersom trafikförvaltningen inte har en

upprättade i enlighet med dataskyddsförordningen?		systematisk och löpande uppföljning av aktuella behandlingar.
Rutiner för hantering av de registrerades rättigheter med fokus på rättelse, radering och begränsning i färdtjänstverksamheten i enlighet med dataskyddsförordningen?	Delvis	Det finns rutindokument och information på webben. Det framgår dock inte på webben hur skydd av den registrerades rättigheter till tredje land efterlevs.
Åtgärder som vidtagits för att säkerställa att de krav som följer av dataskyddsförordningen är välkända hos medarbetarna inom trafiknämndens förvaltning som ansvarar för färdtjänsten?	Delvis	Det finns intern utbildning. Det saknas dock dokumentation på genomförda utbildningar hos medarbetarna vilket är en brist.
Har trafiknämnden säkerställt en tillräcklig uppföljning med hjälp av återrapportering till nämnden?	Delvis	Det finns en etablerad process för årlig rapportering om dataskydd men färdtjänstens verksamhet redovisas inte separat i dataskyddsombudets rapportering till trafiknämnden.

Stockholm den 19 mars 2026

Caroline Palo
Sakkunnig

Richard Norberg
Revisionsdirektör

Revisionskontoret
Region Stockholm

Bilaga 1 – Begrepp och nyckelord se artikel 4

Behandling: Ett begrepp som omfattar "all hantering" av personuppgifter, oavsett om det sker automatiskt eller inte, exempelvis insamling, registrering, lagring, ändring, spridning, radering, utlämnande eller förstöring av uppgifter.

Personuppgifter: All slags information som direkt eller indirekt kan kopplas till en identifierad eller identifierbar, levande fysisk person, som namn, personnummer, adress, bilder, e-post, IP-adresser.

Personuppgiftsansvarig: En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.

Personuppgiftsbiträde: En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Personuppgiftsincident: En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Tillsynsmyndighet: En oberoende offentlig myndighet som är utsedd av en medlemsstat i enlighet med artikel 51, i Sverige är det IMY (Integritetsskyddsmyndigheten).

Personuppgiftsansvarig: En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.

Personuppgiftsbiträde: En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Register: En strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden.

Registrerad: Den enskilde vars personuppgifter behandlas.

Tredje land: Ett land som inte är medlem i EU eller EES. En överföring till tredje land är när personuppgifter som behandlas i ett EU- eller EES-land görs tillgängliga i ett land utanför EU/EES-området. Personuppgifter får föras över endast om det finns en adekvat skyddsnivå i mottagarlandet eller om det finns särskilda garantier för att uppgifterna och de registrerades rättigheter skyddas.

Underbiträde: En tredje part som ett personuppgiftsbiträde anlitar för att behandla personuppgifter för den ursprungliga personuppgiftsansvariges räkning.

Bilaga 2 - Granskade dokument

Avtal i färdtjänstens verksamhet:

Avtal avseende Beställningscentral för färdtjänstverksamhet TN 2023–0597

Ramavtal färdtjänsttaxi, FTN HaningeNynäs (HaningeNynäs Taxi TN 2023–0286; Taxi Stockholm 2023–0286; Haninge Nynäs TN FTN 2022–0012; Samtrans Omsorgsresor FTN 2022–0012)

Ramavtal om rullstolstaxi TN 2023-abcd

Uppdragsavtal Kundservice FTN 2019–0119

Trafikförvaltningens interna dokument:

Beslutsordning för trafikförvaltningen TN-S-993 215

Dataskyddsombudets årsrapport för verksamhetsåren 2021–2024; TN 2025–0463; TN 2023–0020; TN 2022–0008; FTN 2021–0057

Delegationsordning, TN 2014–0104

Delegationsbeslut Dataskyddsombud, TN 2 883 649/2 883 649

Hantera fysiskt skydd av personuppgifter, TN-S-1 215 793

Hantera inkommande förfrågningar baserat på den registrerades rättigheter, TN-S-1 304 931

Säker hantering av personuppgifter, TN-S-1 215 791

Hantera ostrukturerat material med personuppgifter, TN-S-1 363 459

Processpecifikation Hantera personuppgiftsincidenter, TN-S-1 360 259

Hantera personuppgiftsincidenter, TN-S-1 360 259

Hantera e-post med personuppgifter, TN-S-1 215 792

Checklista vid personuppgiftsincidenter (ej fastställt), 1 354 535

Rutin för informationssäkerhetsincidenter, TN-S-2 980 752

Informationsägare (ej fastställt), TN-S-2 088 249

SÄB Styrning av informationssäkerhetsincidenter, TN-S-2 980 752

Arbetsordning, TN-S-3 144 190

Hantering av underlag som skannas in, 1 190 082

Rutin Hantera rättningar av personuppgifter, 1 183 860

Rutin Hantering av ärenden utanför systemet, 1 176 535

Rutin Hantering av utskrivet material med personuppgifter, 1 176 530

Rutin säkerställa den registrerades identitet, 1 178 917

Personuppgiftsincidenter år 2021 – 2024: FTN 2021–0003; FTN 2022–0003; TN 2023–0018; 2024 saknar diarienummer

Säker hantering av personuppgifter (ej fastställt), TN-S-1 215 791

Regionfullmäktiges beslut:

Policy Verksamhetsskydd, RS 2020–0147

Riktlinjer för informationssäkerhet, RS 2020–0148

Övrigt:

Beslut om godkännande av bindande företagsbestämmelser. Integritetsmyndigheten; DI-2019-8136

Färdtjänstutskottets dagordningar, 2024–2025

Uppföljning av färdtjänstavtalet Kommunförbundet, TN 2013–0705

IMY: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsansvariga-och-personuppgiftsbitraden/personuppgiftsbitradesavtal/

Bilaga 3 Kontrollpunkter

Kontrollpunkter för personuppgiftsincidenter:

(artikel 33–34 dataskyddsförordningen)

a) Datum och tid för incidenten.

b) Beskrivning av incidenten.

c) Vilka personuppgifter som berörs.

d) Konsekvenser för de registrerade (risker för integriteten).

e) Vidtagna åtgärder.

f) Om incidenten anmälts till Integritetsskyddsmyndigheten (IMY) och/eller de registrerade.

Kontrollpunkter för personuppgiftsbehandlingar:

(artikel 30 dataskyddsförordningen)

a) Namn och kontaktuppgifter för den personuppgiftsansvariga, den personuppgiftsansvarigas företrädare samt dataskyddsombudet.

b) Ändamålen med behandlingen.

c) En beskrivning av kategorierna av registrerade och av kategorierna av personuppgifter.

d) De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut.

e) I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation.

Vad gör regionrevisorerna?

Regionrevisorerna granskar den verksamhet som bedrivs av regionens nämnder och bolagsstyrelser. Revisionsuppdraget är det största inom kommunal verksamhet.

Att vara revisor är ett förtroendeuppdrag vars syfte är att med oberoende, saklighet och integritet främja, granska och bedöma verksamheten. Den övergripande uppgiften för revisorerna är att granska hur nämnder och styrelser tar sitt ansvar. De förtroendevalda revisorerna är fullmäktiges och ytterst medborgarnas instrument för den demokratiska kontrollen. De har därmed en viktig funktion i den lokala självstyrelsen.

Ledamöter i nämnder och styrelser ansvarar inför fullmäktige för hur de själva, anställda och uppdragstagare genomför verksamheten. I ansvaret ingår att genomföra en ändamålsenlig verksamhet utifrån fullmäktiges mål, beslut och riktlinjer samt de föreskrifter som gäller för verksamheten, på ett ekonomiskt tillfredsställande sätt och med en tillräcklig intern kontroll samt att upprätta rättvisande räkenskaper.

I årsrapporter för nämnder och styrelser sammanfattar revisionskontoret den granskning som genomförts under det gångna året. Verksamhetsrevisionen redovisas löpande i projektrapporter. Publikationerna finns på www.regionstockholm.se. Det går även att prenumerera på regionrevisorernas nyhetsbrev genom att anmäla intresse via e-postmeddelande till regionrevisorerna.rev@regionstockholm.se.

Postadress: Box 22230, 104 22 Stockholm
Besöksadress: Hantverkargatan 25 b (T-bana Rådhuset)
Telefon: 08-737 25 00
E-post: regionrevisorerna.rev@regionstockholm.se
Hemsida: www.regionstockholm.se

Region Stockholm