Stockholms stad

GDPR Årsrapport

2021

Trafiknämnden

GDPR årsrapport
Januari 2022

Dnr: T2021-03531
Utgivningsdatum: 2021-12-21
Kontaktperson: Patrik Stensson

1 Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnd och bolagsstyrelse behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

Varje nämnd och bolagsstyrelse i Stockholms stad har i enlighet med dataskyddsförordningen utnämnt ett Dataskyddsombud (”DSO”). DSO:n har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå.

Denna årsrapport är således ett medel för nämnd och styrelse att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnd eller bolagsstyrelse ska kunna *visa* att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna *dokumenteringsskyldighe*t. Årsrapporten är även ett medel för nämnds/bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

2 Sammanfattning

I egenskap av DSO för trafiknämnden lämnar undertecknad följande årsrapport avseende trafiknämndensdataskyddsarbete och hantering av personuppgifter för år 2021.

Det är trafiknämnden som är personuppgiftsansvarig, men samtidigt är det trafikkontoret som utför uppgifterna inom dataskyddsarbetet, därför kommer trafikkontoret fortsättningsvis att vara den beteckning som används för personuppgiftsansvarig i denna rapport.

DSO:s årsrapport för år 2020 överlämnades endast till trafikkontoret (dnr T2021-00060). Hädanefter kommer rapporten även att tillgängliggöras för trafiknämnden genom verksamhetsberättelsen.

Årsrapporten består av två delar:

- Uppföljning av den handlingsplan trafikkontpret upprättade som svar på DSO:s årsrapport för verksamhetsåret 2020. I handlingsplanan har trafikkontoret beskrivit vilka åtgärder som planerades under 2021
- Uppföljning av trafikkontorets dataskyddsarbete för verksamhetsåret 2021 enligt stadens mall

3 Handlingsplan

Med utgångspunkt från DSO:s årsrapport för 2020 upprättade trafikkontoret en handlingsplan över vilka åtgärder som skulle vidtas under 2021. I egeneskap av DSO har undertecknad nu följt upp denna. Nedan redovisas vilka åtgärder som trafikkontoret har genomfört och vilka som kvarstår.

Eftersom trafikkontoret fortfarande håller på att hitta formen för hur dataskyddsarbetet ska bedrivas handlar merparten av de åtgärder som kontoret vidtar främst om organisation, roller, ansvarsfördelning och arbetsuppgifter, snarare än konkreta personuppgiftsbehandlingar och konkreta granskningar av dem.

3.1 Handlingsplanens punkter

- Delegation
- Organisation, roller och ansvar
- Register över behandlingar

- Risker
- Tredjelandsöverföringar
- Tyck till/Synpunktsportalen
- Registerutdrag
- Konsekvensbedömningar
- Informationsklassningar och riskanalyser
- Personuppgiftsbiträdesavtal(pubavtal)
- Ostrukturerad personuppgiftsbehandling
- Fotografier till parkeringstillstånd för rörelsehindrade
- Utbildningar

3.2 Ansvarsfördelning för handlingpslanen

Avdelning	Enhet/funktion	Åtgärd	Status
Samtliga medarbetare på trafikkontoret		Att känna till hur man behandlar personuppgifter	Ingen uppföljning
DSO		Utföra granskning och revision	Delvis genomförd
Samtliga avdelningar		Bjuda in DSO till ledningsgruppsmöten för information	Delvis genomförd
Administration	Säkerhetssamordnare	Riktlinjer för kameror	Pågående
	Dokumentation	Rutin för pubavtal	Ej genomförd
		Rutin för ostrukturerad personuppgiftsbehandling	Ej genomförd
		Personuppgiftsbehandling i hanteringsanvisningarna	Påbörjad
		Integrationer mellan system	Ej genomförd
	IT	Ansvar och beslutsnivåer i pm3	Genomförd

		Register stående punkt på agenda nätverksträffar FL/FL IT	Genomförd
		Ansvar för informations-klassning i pm3	Genomförd
		Uppföljning av informations-klassningar i pm3	Genomförd
		Inventering av tredjelands-överföring	Genomförd
		Rutiner för pubavtal	Ej genomförd
		Riktlinjer för kameror	Pågående
	Servicecenter	Styra upp personuppgifts-hanteringen i systemstöd	Pågående
Ekonomi	Upphandling	Rutiner för pubavtal	Ej genomförd
Stab		Delegations-ordning	Pågående
Infrastruktur	Trafiksystem	Riktlinjer för kameror	Pågående
Tillstånd	Juridik och parkering	Konsekvens-bedömning för fotografier till PRH	Delvis genomförd
Stadsmiljö		Inget utpekat ansvar	N/A
Trafikplanering		Inget utpekat ansvar	N/A
Kom-munikation		Inget utpekat ansvar	N/A

3.3 Sammanfattning av handlingsplanen

3.3.1 Ej åtgärdat

- Dataskyddsombud ska utföra granskning och revision
- De avdelningar som ännu inte gjort det ska bjuda in dso till ledningsgruppsmöten för information om dataskydd
- Se över rutiner för ostrukturerad personuppgiftsbehandling
- Undersöka integrationer mellan system med personuppgiftsbehandlingar
- Rutin för pubavtal ska utformas av IT och Upphandling tillsammans med dso. Se avsnitt Styrdokument.

3.3.2 Pågående

- **Utarbeta riktlinje för kameror.** Infrastruktur/Trafiksystem och Trafikplanering/Teknik har initierat en utredning och inventering av samtliga kameror i ett projekt lett av Governo. Se avsnitt under Övriga observationer.
- **Lägga till personuppgiftsbehandling i hanteringsanvisningarna.** Revidering av hanteringsanvisningar är påbörjad. Se avsnitt under Styrdokument.
- **Inventering av tredjelandsöverföring.** Måste göras kontinuerligt, särskilt vid upphandling av nya system eller tjänster. Se avsnitt under Säkerhetsåtgärder.
- **Revidera delegationsordningen.** Staben har inlett ett arbete med detta. Personuppgiftsbehandlingar tas troligen upp i en beslutsordning utanför delegationsordningen. Se avsnitt under Styrdokument.
- **Genomföra en konsekvensbedömning för fotografier knutna till parkeringstillstånd för rörelsehindrade (PRH).** Konsekvensbedömningen är genomförd, men den måste följas upp. Se avsnitt under Övriga observationer

3.4 Organisation, roller och ansvar enligt pm3

Administrativ chef har tillsammans med chef för dokumentationsenheten och DSO tagit fram förslag på vilka roller som har ansvar för dataskyddsarbetet. Ansvar och uppgifter fördelas på objektägare, förvaltningsledare, förvaltningsledare it och objektspecialister.

Dataskyddsarbetet blir en stående punkt på agendan för Objektstyrgruppsmöte 1 i maj. Objektspecialister, förvaltningsledare och objektägare förväntas förbereda denna punkt under februari/mars med hjälp av den checklista som tagits fram och den handlingsplan som denna årsrapport mynnar ut i.

Det övergripande rådet och rekommendationen från dso är att trafikkontoret sätter sig in i detta arbetssätt och bekantar sig med de dokument som tagits fram som stöd för detta.

Denna övergripande rekommendation gäller samtliga av de obligatoriska rapporteringsområdena: register, styrdokumnet, individens (de registrerades) rättigheter, säkerhetsåtgärder, konsekvensbedömningar och personuppgiftsincidenter.

Objektägare, Förvaltningsledare och Objektspecialister bör sätta sig in i hur den nya rollfördelningen är tänkt att fungera och ta del av den stöddokumentation som tagits fram.

Objektägare/Avdelningschefer bör ha som stående punkt på Objektstyrmöten följa upp samtliga punkter enligt framtagen checklista i excelformat.

Förvaltningsledare/Förvaltningsledare IT bör ha som stående punkt på Förvaltningsgruppmöten att följa upp samtliga punkter enligt framtagen checklista rörande dataskydd.

4 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som Personuppgiftsansvarig (”PUA”) som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som dataskyddsförordningen avser.

De obligatoriska rapporteringsområdena är registerförteckning, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter.

Nedan redogörs för nämndens eller bolagets status och DSO:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

4.1 Registerförteckning

4.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	113
Har nödvändiga uppdateringar gjorts?	Nej
Bedöms registerförteckningen vara fullständig?	Delvis
Har verksamheten lämpliga rutiner för registerföring?	Nej

4.1.2 Syfte

Enligt Dataskyddsförordningen ska personuppgiftsansvarig föra ett register över samtliga personuppgiftsbehandlingar (artikel 30). Det är en viktig del av ansvarsskyldigheten, det vill säga att kunna visa att personuppgiftsansvarig följer Dataskyddsförordningen (artikel 5.2). Trafikkontoret använder ett registerverktyg från Draftit Privacy Records (Draftit).

Att föra register är ett av de viktigaste verktygen i dataskyddsarbetet och granskning av registret är en av de viktigaste delarna av DSO:s arbete med uppföljning av dataskyddet på trafikkontoret.

Enligt handlingsplanen för 2021 ska registerföringen vara en stående punkt på agendan för trafikkontorets nätverksmöten för förvaltningsledare och förvaltningsledare it.

4.1.3 Resultat

Trafikkontoret har för närvarande 113 registrerade behandlingar.

Registret är inte fullständigt. Det finns fortfarande behandlingar/registerposter som saknar obligatoriska uppgifter. Dataskyddsombudet förutsätter att det saknas behandlingar, men har kontinuerlig kontakt med avdelningar, enheter, förvaltningsledare för att komplettera registret.

Verksamheten har fortfarande inte någon tydlig fungerande rutin för registerföring.

4.1.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

Ett kontinuerligt arbete görs för att förbättra registret och uppföljning av registret ingår i den övergripande modellen för dataskyddsarbetet inom pm3 som framtagen och presenterad för avdelningschefer och förvaltningsledare. Behandlingar med hög risk är väl dokumenterade i registret. De kontinuerliga informationsklassningarna pekar ut att behandlingar ska registerföras, det kommer då med i den handlingsplan som följer på klassningen.

4.1.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar PUA att implementera den övergripande modell för dataskyddsarbetet enligt pm3 som är framtagen för trafikkontoret.

Detta innebär bland annat att inventera vilka behandlingar som förekommer i respektive objekt samt att utse ansvariga för varje behandling. Ansvariga kan ta kontakt med DSO för att få stöd och hjälp att fylla i uppgifter för sin behandling.

4.2 Styrdokument

4.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Ja
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Delvis
Är dokumenten uppdaterade?	Delvis
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Delvis

4.2.2 Syfte

Att ha styrdokument, riktlinjer och rutiner på plats är tillsammans med registret en viktig del av ansvarsskyldigheten, det vill säga att vi ska kunna visa att trafikkontoret följer Dataskyddsförordningen. Trafikkontoret har en handbok för GDPR i ärendehanteringssystemet Public 360 som kan nås via en länk på kontorets intranätssida för handböcker eller direkt i diariet, (handboksnummer 18-4, *Riktlinjer för personuppgiftshantering på trafikkontoret*. Handboken inehåller ett antal dokument som tilldelats olika dokumentnummer).

Det finns en rad rutiner som ska fungera i dataskyddsarbetet. Objektägare har det övergripande ansvaret för att de är på plats. Förvaltningsledare och informationssäkerhetsansvarig i samarbete med DSO ansvarar för att de uppdateras kontinuerligt, att de finns tillgängliga och att de som ska ha kunskap om rutinen verkligen har det.

Enligt handlingsplanen för 2021 ska trafikkontorets stab arbeta in formuleringar om dataskydd och personuppgiftsbehandling i en ny delegationsordning. Detta kommer troligen att ske i form av en beslutsordning utanför delegationsordningen.

En rutin för ostrukturerade personuppgiftsbehandlingar skulle enligt handlingsplanen tas fram, lilksom en ny rutin för pubavtal. Detta har ännu inte utförts.

4.2.3 Resultat

Många viktiga riktlinjer och rutiner är mycket bra. Men det saknas fortfarande rutiner för vissa områden och vissa kan vara föråldrade och behöver uppdateras.

Övergripande dokument

- Övergripande styrdokument för personuppgiftshantering på trafikkontoret finns i handboken *Riktlinjer för personuppgiftshantering* på trafikkontoret.
- Styrdokument för informationssäkerhet håller på att tas fram centralt i staden i form av riktlinjer. Dessa har ännu inte införts. Det finns en äldre riktlinje som fortfarande gäller. Den finns på stadens sida för informationssäkerhet och i handboken, dokumentnummer 19-395, *Riktlinje för informationssäkerhet.* Det finns även andra rutiner och riktlinjer för informationssäkerhetsarbetet på trafikkontoret som återfinns på intranätet på stadens sida för informationssäkerhet.
- Delegationsordning för trafiknämnden är under arbete, vilket samordnas av staben. Administrativ chef, informationssäkerhetsansvarig och DSO är involverade i detta arbete
- Systemdokumentation för system ska finnas, vilket inte har kontrollerats.
- Förvaltningsplaner för objekt ska finnas, vilket inte har kontrollerats.

Dokument särskilt för viktiga områden inom dataskyddet

- **Rutin för personuppgiftsincident**. En rutin finns men behöver uppdateras. Den finns i handboken, dokumentnummer 19-395
- **Rutiner för personuppgiftsbiträdesavtal och instruktionen till dessa**. Mallar för dettta återfinns på stadens intranätssida för GDPR. Dokumentation finns även i Handboken, dokumentnummer 19-395. Frågor som behöver besvaras är: hur sker hantering, utformning, underskrift, uppföljning, registrering och diarieföring. Trafikkontoret måste även tydliggöra ansvar.
- **Rutin för konsekvensbedömning**. Trafikkontoret använder verktyget DPIA från Draftit, men det finns ännu ingen bra rutin

för konsekvensbedömning. Den vägledning med dokumentnummer 18-113 som återfinns i handboken är äldre och behöver uppdateras. Stadsledningskontoret har ett förslag till rutin som kan hittas på stadens intranätssida för GDPR. Vidare håller stadsledningskontoret på att ta fram ett metodstöd, men det är ännu inte på plats.

- **Rutin för registerutdrag**. Det finns en rutin för registerutdrag, men den behöver uppdateras. Eftersom det är DSO som samordnar är det bara DSO som har tillgång till denna rutin. Trafikkontoret har ännu inte tagit fram e rutin för hur en begäran om registerutdrag ska hanteras när DSO inte är på plats. Just nu är det enhetschefen för dokumentationsenheten som går in som ersättare.
- **Rutin och mall för information till de registrerade**. Rutin och mall finns i handboken, dokumentnummer 18-336. Information till anställda återfinns i Public 360: *Behandling av personuppgifter vid anställning på trafikkontoret, PM* dnr T2018-01634-1. Information om hur trafikkontoret behandlar personuppgifter finns på webbsida: *Behandling av personuppgifter på trafikkontoret - Stockholms stad*
- **Rutin för invändning, rättelse, radering, begränsning och dataportabilitet**. Just nu finns det inga skriftliga, fastställda rutiner kring detta.
- **Rutin för registerföring**. DSO arbetar med att ta fram en fungerande rutin. Objektägare har det yttersta ansvaret för att registret är uppdaterat och fullständigt för de behandlingar som finns i objektet. Förvaltningsledare för respektive objekt har det operativa ansvaret för att följa upp att behandlingar som ingår i objektet finns med i registret med alla obligatoriska uppgifter. Enhetschefer utser ansvariga som fyller i och uppdaterar uppgifter i registret.

4.2.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

4.2.5 DSO ger råd och rekommendationer till PUA

Trafikkontoret behöver tydligare svara på frågan vem det är som ansvarar för att kontorsövergripande styrdokument är uppdaterade, relevanta och kända av verksamheten. Dokumentation som behöver ses över är:

- Delegationsordning för trafikkontoret
- Beslutsordning för trafikkontoret
- Rutin för personuppgiftsincident
- Lokal rutin för pub-avtal
- Lokal rutin för konsekvensbedömning
- Lokal rutin för registerutdrag
- Lokal rutin för invändning, rättelse, radering, begränsning och dataportabilitet
- Lokal rutin för registerföring

4.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

4.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	Enligt Registerförteckningen är 45 av 113 klassade, 10 av 113 är inte klassade och för 57 av 113 har inget angivits.
Är klassade personuppgiftsbehandlingar aktuella?	11 av 45 är klassade inom föreskriven tidsram

4.3.2 Syfte

Informationsklassning är en metod för att bedöma risker och ge åtgärdsförslag för att säkerställa att stadens riktlinjer för informationssäkerhet följs. Bland de frågor som ställs i klassningen finns det specifika frågor som rör dataskyddet. Därför är det mycket viktigt att all information som ägs att trafikkontoret klassas. Då kommer dataskyddsfrågorna automatiskt att behandlas. Detta gäller bland annat frågan om det är nödvändigt med en konsekvensbedömning. Även frågor om registret och de registrerades rättigheter och säkerhetsåtgärder ställs här.

4.3.3 Resultat

Alldeles för få behandlingar uppges ha genomgått en informationsklassning. Det är svårt för DSO att avgöra om det beror på brist på information i registret. Flera av de klassningar som gjorts är inte längre aktuella enligt de regler för klassning som staden har.

4.3.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
X	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga

	Inga brister av nämnvärd betydelse identifierade

4.3.5 DSO ger råd och rekommendationer till PUA

Det finns fler utmaningar när det kommer till uppgifter om informationsklassningar. Registret har inte fyllts i tillräckligt, det verkar saknas informationsklassningar där det borde finnas och flera klassningar är inte längre aktuella.

Följande åtgärder bör vidtas:

- Registret måste uppdateras så att det klart framgår när en informationsklassning är gjord och när den inte är gjord
- Kontoret bör tydligt urskilja vilka behandlingar som behöver klassas och vilka som redan har klassats.
- Kontoret bör hålla genomförda klassningarna uppdaterad

4.4 Konsekvensbedömningar

4.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Delvis
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Delvis
Är de genomförda bedömningarna aktuella?	Ja

4.4.2 Syfte

Om risken för de registrerades fri- och rättigheter bedöms som hög utifrån de kriterier som dataskyddsförordningen anger (artikel 35 och 36) ska en konsekvensbedömning genomföras. Integritetsskyddsmyndigheten (IMY), som är tillsynsmyndighet inom dataskyddsområdet, ger detaljerad information om konsekvensbedömningar på sin webbsida.

Om det kvarstår risker efter en konsekvensbedömning ska IMY kontaktas för förhandssamråd. Detta görs via ett webbformulär på deras hemsida.

DSO ska alltid finnas med för övervakning av genomförandet och rådfrågning.

4.4.3 Resultat

Trafikkontoret har fortfarande svårt att få igång en fungerande rutin för initiera och genomföra konsekvensbedömningar. Det finns fortfarande en okunskap om vad det innebär, när de bör göras och vem som ska göra dem. Det finns en rad stöd för att arbetet med detta ska kunna bli bättre:

- Den modell för organisering av dataskyddsarbetet som avdelningschef administration tillsammans med enhetschef

dokumentation och DSO tagit fram. Förvaltningsledare är första hand de som ska initiera konsekvensbedömning med stöd av DSO och informationssäkerhetsansvarig.
- Informationsklassningar visar om det krävs en konsekvensbedömning och det ingår då i den handlingsplan som blir resultatet.
- Trafiknämnden använder ett verktyg från Draftit som stöd för konsekvensbedömningar, DPIA.
- SLK håller på att ta fram ett stöd för konsekvensbedömning.

Det är i nuläget trafikkontorets DSO som har bäst kunskap om vad en konsekvensbedömning innebär och är därför den som i praktiken leder genomgångarna. Detta är inte hållbart på lång sikt då det kommer i konflikt med DSO:s oberoende och datskyddsförordningens krav på att DSO ska närvara och övervaka konsekvensbedömningar.

Det finns fortfarande behandlingar som borde konsekvensbedömas men där detta inte gjorts. De konsekvensbedömningar som genomförts har i saknar i flera fall mer detaljerad dokumentation.

Det finns några högriskbehandlingar där konsekvensbedömningar ännu inte är helt och hållet genomförda.

Det saknas även uppföljning av redan genomförda konsekvensbedömningar.

4.4.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
X	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

4.4.5 DSO ger råd och rekommendationer till PUA

Enligt dataskyddsförordningen ska DSO rådfrågas vid en konsekvensbedömning och övervaka genomförandet. Det är därför inte lämpligt i längden att DSO leder konsekvensbedömningen, men

det är den lösning trafikkontoret har i nuläget. Detta förhållande bör utredas och åtgärdas på lång sikt.

Trafikkontoret bör fortsätta att genomföra informationsklassningar av all sin information. Då kommer det att visa sig om det krävs konsekvensbedömningar.

DSO rekommenderar PUA att implementera den rutin som är framtagen för trafikkontoret av administrativ chef och DSO.

Påbörjade konsekvensbedömningar bör skyndsamt slutföras och kompletteras så att PUA kan vara trygg med att alla risker har eliminerats eller minimerats. Redan genomförda konsekvensbedömningar bör följas upp på ett systematiskt sätt.

4.5 Individens rättigheter

4.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	1 begäran om radering
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	samtliga

4.5.2 Syfte

Dataskyddsförordningen ger de registrerade vissa rättigheter som formuleras i kapitel III, dessa är:

- Rätt till information
- Rätt till tillgång (registerutdrag)
- Rätt till radering
- Rätt till rättelse
- Rätt till invändning
- Rätt till begränsning
- Rätt till dataportabilitet

Den registrerade har rätt att få ett svar inom 30 dagar, om vi inte kan visa att vi behöver längre tid. Besluten kan överklagas till allmän domstol.

4.5.3 Resultat

Verksamheten har förutsättningar att hantera registrerades rättigheter inom föreksriven tidsfrist.

4.5.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

4.5.5 DSO ger råd och rekommendationer till PUA

Det som brister är att det inte finns tydliga, skriftliga rutiner för att tillmötesgå begäran om invändning, radering, begränsning och dataportabilitet. Det finns ingen stor kunskap om vad de registrerades innebär, särskilt gäller det rätten till invändning, begränsning och dataportabilitet.

PUA borde utarbeta rutiner för invändning, radering, begränsning eller dataportabilitet.

4.6 Personuppgiftsincidenter

4.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Den som upptäcker en incident rapporterar i IA-systemet
Hur många personuppgiftsincidenter har dokumenterats?	6
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Inga
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Ej tillämpbar, se ovan

4.6.2 Syfte

Enligt dataskyddsförordningen är en 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.”

Personuppgiftsincidenterna ska anmälas till tillsynsmyndigheten inom 72 timmar från upptäckt om trafikkontoret inte bedömer att det är en mycket liten risk för de registrerades rättigheter och friheter. Trafikkontoret ska ändå anmäla och dokumentera dessa lokalt enligt kontorets rutiner.

Det kan krävas att de registrerade måste informeras. Det är om incidenten sannolikt leder till hög risk för den registrerades rättigheter och friheter.

4.6.3 Resultat

Trafikkontoret har rutinen att rapportera i stadens IA-system samt enligt en lokalt framtagen rutin som återfinns i den handbok för personuppgiftsbehandling som ligger i Public 360. Rapporteringen i IA har visat sig opålitlig då inte alla anmälningar verkar registreras

så att ansvarig chef ser det. Det finns även en osäkerhet hos delar av trafikkontoret hur en personuppgiftsincident ska rapporteras.

4.6.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
	Brister identifierade som bedöms vara omfattande och/eller kräva omgående åtgärder
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

4.6.5 DSO ger råd och rekommendationer till PUA

Det finns en rutin som fungerar om den efterlevs, men den behöver uppdateras och förtydligas. Det finns fortfarande viss okunskap om hur rapportering går till, vilken rutin som gäller vid riskbedömning, utredning och anmälan till tillsynsmyndigheten.

DSO rekommenderar att PUA går igenom och uppdaterar rutinen för personuppgiftsincidenter och klargör roller och ansvar. På sikt behövs information till alla på kontoret om hur en incident ska rapporteras.

5 Övrigt att rapportera

5.1 Övriga observationer

Kameror

Trafikkontoret har ett antal kameror fördelade på olika avdelningar och enheter. Alla dessa har i dagsläget inte tillstånd till kamerabevakning. Trafikkontoret har inte gjort konsekvensbedömningar och det finns heller ingen samlad bild av vilka kameror som finns på kontoret. Kameror i stadsmiljön innebär personuppgiftsbehandling i stor omfattning och av medborgare.

Infrastrukturavdelningen och trafikplaneringsavdelningen har initierat ett projekt för inventering och ansökningar av kameratillstånd tillsammans med Governo. När det projektet har avslutats kommer trafikkontoret ha mycket större möjligheter att hantera sina kameror korrekt och då bör riskerna med dem ha minskat avsevärt. Arbetet med kameror och kameratillstånd måste förvaltas långsiktigt.

Synpunktshantering och felanmälan

Trafikkontorets verktyg för handläggning av synpunkter, frågor och klagomål och felanmälan, Tyck till/Synpunktportalen, tar emot en del personuppgifter, till och med känsliga personuppgifter i det fritextfält som är en del av lösningen. Verktyget har ingen bra funktion för behörighetsstyrning, sekretessmarkering eller känslighetsmarkering av personuppgifter. Eftersom de inkommande anmälningarna är allmänna handlingar som ska bevaras kan trafikkontoret heller inte ta bort uppgifter. Det finns därmed stora risker att uppgifter röjs. Detta verktyg kommer att på sikt ersättas av ett mer anpassat ärendehanteringssystem och ett projekt för att genomföra systembytet påbörjas 2022. Fram tills dess är det av stor vikt att det finns bra rutiner för det systemstöd trafikkontoret använder i nuläget för att minimera riskerna.