Stockholms stad

GDPR Årsrapport

År 2022

Trafiknämnden

GDPR årsrapport
Januari 2023

Dnr: T2022-03049
Utgivningsdatum: 2023-01-10
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 *ansvarsskyldighe*t. Årsrapporten är även ett medel för nämnds/bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

1 Bakgrund ... 3

Innehåll ... 4

2 Sammanfattning ... 5

3 Handlingsplan ... 5

3.1 Uppföljning av handlingsplan ... 5

3.2 Kommentarer till handlingsplan för 2023 ... 7

4 Obligatoriska rapporteringsområden ... 8

4.1 Registerförteckning ... 9

4.2 Styrdokument ... 11

4.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar ... 15

4.4 Konsekvensbedömningar ... 17

4.5 Individens (de registrerades) rättigheter ... 20

4.6 Personuppgiftsincidenter ... 22

5 Övrigt att rapportera ... 24

5.1 Övriga observationer ... 24

2 Sammanfattning

I egenskap av Dataskyddsombud för trafiknämnden lämnar jag följande årsrapport avseende trafiknämndens dataskyddsarbete och hantering av personuppgifter för år 2022.

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

Årsrapporten består av två delar:

- Uppföljning av den handlingsplan som trafikkontoret upprättade som svar på DSO:s årsrapport för verksamhetsåret 2021.
- Uppföljning av trafikkontorets dataskyddsarbete för verksamhetsåret 2022 enligt stadens mall.

3 Handlingsplan

Med utgångspunkt från DSO:s årsrapport för 2021 upprättade trafikkontoret en handlingsplan över vilka åtgärder som skulle vidtas under 2022, dnr T2021-03531-2.

3.1 Uppföljning av handlingsplan

Flera punkter återkommer i rapporten och kommenteras mer i detalj där.

Åtgärder enligt tidigare årsrapport	**Tidigare status**	**Nuvarande Status**
De avdelningar som ännu inte bjudit in DSO till sina ledningsgruppsmöten för information om dataskydd ska göra det	Ej åtgärdat	Pågående
Se över rutiner för ostrukturerade personuppgifter	Ej åtgärdat	Ej åtgärdat
Undersöka integrationer mellan system med personuppgiftsbehandlingar	Ej åtgärdat	Ej åtgärdat
Rutin för personuppgiftsbiträdesavtal (pubavtal) ska utformas av IT och Upphandling tillsammans med DSO.	Ej åtgärdat	Pågående

Utarbeta riktlinjer för kameror	Pågående	Pågående
Lägga till personuppgiftsbehandling i hanteringsanvisningarna	Pågående	Åtgärdat
Inventering av tredjelandsöverföring	Pågående	Pågående
Revidera delegationsordningen	Pågående	Pågående
Genomföra en konsekvensbedömning för fotografier knutna till parkeringstillstånd för rörelsehindrade (PRH)	Pågående	Pågående

Implementering av den övergripande modellen för dataskyddsarbetet enligt pm3.	**Tidigare status**	**Nuvarande status**
Ansvars- och rollfördelning rörande personuppgiftsbehandling enligt pm3 utarbetades av administrativ chef tillsammans med chef för dokumentationsenheten och DSO	Planerad	Åtgärdat
Dataskyddsarbetet blir en stående punkt på agendan för Objektgruppstyrmöte	Planerad	Omarbetad
Trafikkontoret sätter sig in i arbetssättet och känner till de stöddokument DSO har tagit fram rörande samtliga obligatoriska rapporteringsområden: register, styrdokument, individens (de registrerades) rättigheter, säkerhetsåtgärder, konsekvensbedömningar och personuppgiftsincidenter	Planerad	Åtgärdat/ delvis omarbetad
Objektägare, Förvaltningsledare (FL) och Objektspecialister ska sätta sig in i hur rollfördelningen ska fungera	Planerad	Åtgärdat
Objektägare/Avdelningschefer ska ha som stående punkt på objektstyrmöten att följa upp samtliga punkter enligt framtagen checklista.	Planerad	Omarbetad
FL/FL IT ska ha som stående punkt på förvaltningsgruppmöten att följa upp samtliga punkter enligt framtagen checklista.	Planerad	Omarbetad

Åtgärder enligt rapporteringsområden	Tidigare status	Nuvarande status
Register: FL och objektspecialister ska registrera obligatoriska uppgifter om personuppgiftsbehandlingarna i IT-komponentlistan	Planerad	Pågående
Register: Med utgångspunkt från uppgifterna i IT-komponentlistan registrerar DSO motsvarande personuppgiftsbehandlingar i Draftit	Planerad	Pågående
Register: FL och objektspecialister ska se till att IT-komponentlistan kompletteras med uppgift om genomförd informationsklassning.	Planerad	Pågående
Styrdokument: DSO och avdelningschef administration diskuterar vem/vilka på trafikkontoret som ansvarar för kontorsövergripande styrdokument	Planerad	Åtgärdat
Konsekvensbedömning: DSO informerar om konsekvensbedömning på ett informationsmöte för FL	Planerad	Ej åtgärdat
Individens rättigheter: DSO och avdelningschef administration diskuterar vem/vilka på trafikkontoret som bör utarbeta rutiner för invändning, radering, begränsning och dataportabilitet	Planerad	Åtgärdat
Personuppgiftsincidenter: DSO och avdelningschef administration diskuterar vem/vilka på trafikkontoret som bör uppdatera rutinerna samt hur roller och ansvar ska fastställas	Planerad	Åtgärdat

3.2 Kommentarer till handlingsplan för 2023

Trafikkontoret kommer att upprätta en handlingsplan med åtgärder utifrån DSO:s rekommendationer med utpekade enheter och avdelningar.

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 (de registrerades) 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?	114 i Draftit 145 i IT-komponentförteckning
Har nödvändiga uppdateringar gjorts?	Kontinuerlig uppdatering
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Ja, delvis

4.1.2 Syfte

Enligt Dataskyddsförordningen ska PUA föra ett register över samtliga personuppgiftsbehandlingar (artikel 30). Det är en viktig del av ansvarsskyldigheten, det vill säga att kunna visa att PUA följer Dataskyddsförordningen (artikel 5.2).

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.

För att på ett smidigare sätt föra ett komplett register har Trafikkontoret två kompletterande register. Dels används registerverktyget Draftit Privacy Records (Draftit) och dels förteckningen över IT-komponenter på trafikkontorets samarbetsyta för pm3, som har fält för de obligatoriska uppgifterna för ett register enligt dataskyddsförordningen. De är delvis överlappande. Det är främst DSO som använder Draftit, medan IT-komponentförteckningen används i verksamheten. IT-komponentförteckningen används av DSO vid registerutdrag.

Draftit uppdateras av DSO i samarbete med utsedda Ansvariga i Draftit, det är oftast Förvaltningsledare (FL)/Enhetschef eller Objektspecialist/lämplig handläggare. IT-komponentförteckningen uppdateras av FL för respektive objekt.

4.1.3 Resultat

Trafikkontoret har för närvarande 114 registrerade behandlingar i Draftit samt 145 poster i förteckningen över IT-komponenter. Registret är inte fullständigt. Det finns fortfarande behandlingar/registerposter som saknar uppgifter. Dataskyddsombudet förutsätter att det även saknas behandlingar, men har kontinuerlig kontakt med avdelningar, enheter, FL och objektspecialister för att komplettera registret.

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 är framtagen och presenterad för avdelningschefer, FL och ledningsgrupp. Behandlingar med hög risk är väl dokumenterade i registret. De kontinuerliga informationsklassningarna pekar ut att behandlingar ska registerföras, och detta ingår då i den handlingsplan som följer av klassningen.

4.1.5 DSO ger råd och rekommendationer till PUA

Det har under 2022 varit prioriterat att fälten för personuppgifter i förteckningen över IT-komponenter kompletteras av FL. Detta bör prioriteras även under 2023. FL kan ta kontakt med DSO för att få stöd och hjälp i att fylla i fälten. När det gäller Draftit är det särskilt HR-enheten och enheten juridik och parkering som har processer som måste kompletteras. Detta bör slutföras under 2023. DSO stödjer verksamheten att fylla i uppgifter i Draftit.

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?	Ja

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 Public 360 som kan nås via en länk på trafikkontorets samarbetsyta för informationshantering, kontorets intranätssida för handböcker eller direkt i diariet (handboksnummer 18-4, *Riktlinjer för personuppgiftshantering på trafikkontoret*.). Handboken innehåller ett antal dokument som tilldelats olika dokumentnummer.

Det finns en rad rutiner som ska fungera i verksamhetens dataskyddsarbete. FL och informationssäkerhetssamordnare (ISAM) i samarbete med DSO ansvarar för att de uppdateras kontinuerligt, att de finns tillgängliga och att finns kunskap om rutinerna i verksamheten. Objektägare har det övergripande ansvaret för att de är på plats.

Enligt handlingsplanen för 2022 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. Denna är ännu inte färdigställd, men arbetet fortsätter under 2023.

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

4.2.3 Resultat

Många viktiga riktlinjer och rutiner är 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 har tagits fram centralt i staden i form av en Riktlinje. *Riktlinje för informationssäkerhet i Stockholms stad.*
- *Delegationsordning för trafiknämnden* är under arbete, vilket samordnas av staben. Administrativ chef, ISAM och DSO är involverade i detta arbete
- Systemdokumentation för system ska finnas, vilket inte har kontrollerats av DSO. Det är ett pågående arbete inom pm3. DSO har inte granskat några av dessa.
- Förvaltningsplaner för samtliga objekt tas fram inom pm3. DSO har inte granskat dessa.

Dokument särskilt för viktiga områden inom dataskyddet

- **Rutin för personuppgiftsincident**. En rutin finns men behöver uppdateras. ISAM ansvarar för detta. Den finns i handboken, dokumentnummer 19-395
- **Rutiner för personuppgiftsbiträdesavtal och instruktionen till dessa**. Aktuell mall för detta återfinns på stadens intranätssida för GDPR. Dokumentation finns även i Handboken, dokumentnummer 19-395. SLK har tagit fram en mall för instruktion för nämnder och bolag.
- **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 tagit fram ett metodstöd som återfinns på stadens intranätssida för GDPR.

- **Rutin för TIA, riskanalys för tredjelandsöverföring**. Mall för detta har tagits fram av SLK och återfinns hos ISAM. Det finns ännu inte någon officiell mall på intranätet, men det finns en mall att utgå ifrån i trafikkontorets handbok i Public 360.
- **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, denna kan behöva ses över. 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.* Kunskapen på trafikkontoret om information till de registrerade kan behöva uppdateras.
- **Rutin för invändning, rättelse, radering, begränsning och dataportabilitet**. Just nu finns det inga skriftliga, fastställda rutiner kring detta. En arbetsgrupp med jurist, DSO och IT tillsätts under 2023.
- **Rutin för registerföring**. DSO arbetar med att ta fram en fungerande rutin. Trafikkontoret har två kompletterande register, Draftit och IT-komponentlistan för pm3, se närmare detaljer under rubriken *Registerförteckning*. Objektägare har det yttersta ansvaret för att registret är uppdaterat och fullständigt för de behandlingar som finns i objektet. FL 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 med stöd av DSO fyller i och uppdaterar uppgifter i registret i Draftit.

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

Dokumentation som behöver ses över är:

- Delegationsordning för trafikkontoret
- Beslutsordning för trafikkontoret
- Rutin för personuppgiftsincident
- Mall med information till de registrerade samt utbildning om information till de registrerade
- 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
- Handboken i sin helhet måste uppdateras

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?	20 av 145 IT-komponenter har angetts som klassade c:a 45 av 114 behandlingar i Draftit har uppgetts vara klassade Enligt ISAM är 22 klassningar klara
Är klassade personuppgiftsbehandlingar aktuella?	Ja

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

Informationsklassningar pågår i stor omfattning på trafikkontoret av IT-komponenter inom pm3. Flera behandlingar sker även i stadsgemensamma system som klassas av staden centralt. En hel del behandlingar är analoga och infoklassas inte i nuläget. Det finns behandlingar som sker i inaktiva system och dessa klassas inte heller. Det framgår av förteckningen över IT-komponenter om klassning gjorts. ISAM har en egen lista över klassningar, planerade, pågående och genomförda.

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
	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

4.3.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att trafiknämnden fortsätter att infoklassa som den gör idag. Klassningsprotokoll bör diarieföras så att de går att hitta. Uppgifter om infoklassning bör läggs in i förteckningen över IT-komponenter på samarbetsytan för pm3.

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:

- 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 har tagit fram ett stöd för konsekvensbedömning som återfinns på stadens intranätssida för GDPR.

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 dataskyddsförordningens 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
	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

4.4.5 DSO ger råd och rekommendationer till PUA

Enligt dataskyddsförordningen ska DSO rådfrågas vid en konsekvensbedömning och övervaka genomförandet. Det är därför inte lämpligt att DSO leder konsekvensbedömningen, men det är den lösning trafikkontoret har i nuläget. Detta förhållande bör utredas och åtgärdas på längre sikt.

Trafikkontoret bör fortsätta att genomföra informationsklassningar. Då kommer det att visa sig om det krävs konsekvensbedömningar.

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 (de registrerades) 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 1 begäran om dataportabilitet
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 föreskriven 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

	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	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 rättigheter innebär, särskilt gäller det rätten till invändning, begränsning och dataportabilitet. Men det är dock enkelt att be DSO att hjälpa till i de få fall som förekommer.

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?	0
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 tillämpbart

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. Det finns 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

5.1.1 Tredjelandsöverföringar

Samtliga avdelningar och enheter

Överföring till USA har inte har tillräckligt skydd längre i och med Schrems II-domen och att Privacy Shield-avtalet därför inte längre ger tillräckligt skydd för personuppgifter på grund av amerikansk lagstiftning. Det räcker att bolag med amerikanska ägare inblandade i personuppgiftsbehandlingen för att personuppgifter ska bedömas inte vara tillräckligt skyddade.

Trafikkontoret har ett antal upphandlade leverantörer vars tjänster innefattar funktioner och verktyg som tillhandahålls av amerikanskägda bolag. Det kan vara t.ex. Google eller Amazon.

Det är mycket besvärligt att komma till rätta med problemet eftersom trafikkontoret behöver tjänsterna och de redan är upphandlade. Trafikkontoret gör så mycket det kan för att minimera riskerna för att personuppgifter ska föras över till dessa och att de ska vara av så liten känslighetsgrad som möjligt.

I ett fall har en process med standardavtalsklausuler inletts för att kunna använda en licenshantering. I framtida upphandlingar kommer tydligare krav i upphandlingar att olaglig tredjelandsöverföring inte ska förekomma.

5.1.2 Gatuvyer

Stadsmiljöavdelningen, projektutveckling.

Trafikkontorets verktyg Gatuvyer innehåller maskade bilder från gaturummet. Maskningen är tyvärr bristfällig i vissa situationer och lite för svag. Framtida bildinhämtning kommer att maskas fullständigare. Tidigare bilder kommer att maskas bättre i mån av upptäckt.

5.1.3 Kameror och sensorer

Infrastrukturavdelningen, teknik.

Kameror i stadsmiljön innebär personuppgiftsbehandling i stor omfattning och övervakning av medborgare och kräver kamerabevakningstillstånd. Trafikkontoret har ett antal kameror av

olika typer fördelade på olika avdelningar och enheter. Trafikkontoret har även ett antal sensorer/multisensorer med kamerateknik/kameraliknande teknik inbyggd, även dessa är tillståndspliktiga.

Infrastrukturavdelningen och trafikplaneringsavdelningen har genomfört ett projekt för inventering och ansökningar av kamerabevakningstillstånd med hjälp av konsultföretaget Governo.

Inventeringen har resulterat i en mycket djupare kunskap om trafikkontorets kameror bland annat tillståndsansökningar till tillsynsmyndigheten (IMY).

Viktigare tillståndsansökningar:
Trafikkontoret har sökt och fått tillstånd för projektet med multisensorer i Slussen.

Trafikkontoret har sökt tillstånd för multisensorer för styrning av trafiksignaler runtom i staden. Detta ärende ligger nu hos IMY och trafikkontoret har ännu inte fått något besked.

Trafikkontoret har sökt om tillstånd för kamerabevakning av trafikhinder som nyttjas av Trafik Stockholms trafikövervakningscentral.

5.1.4 Synpunktshantering och felanmälan

Administrativa avdelningen, servicecenter.

Synpunktshanteringen kan innehålla olika typer av personuppgifter som rör medborgare, även känsliga och integritetskänsliga eftersom det inte finns något bra sätt att filtrera det som allmänheten skickar in.

Det är främst kontaktuppgifter, position och fritextfält som innehåller personuppgifter. Att lämna kontaktuppgifter är frivilligt och krävs bara om man vill ha olika typer av feedback. Möjligheten att lämna uppgift om position är för att lättare visa platsen för ärendet. Fritextfältet används för att göra en mer detaljerad beskrivning av ärendet gäller, det räcker oftast inte med rubrikerna. I fritextfältet kan anmälaren skriva in alla möjliga uppgifter, även känsliga personuppgifter.

Synpunkter, frågor, klagomål och liknande gallras inte utan ska bevaras, därför finns idag ingen möjlighet att ta bort kontaktuppgifter eller andra personuppgifter. Ärendehanteringssystemet i synpunkthanteringen kommer att

ersättas av ett mer anpassat system. Fram tills dess är det av stor vikt att det finns bra rutiner för det systemstöd trafikkontoret använder i nuläget för att minimera riskerna för de registrerade.

5.1.5 Fotografier till parkeringstillstånd för rörelsehindrade

Tillståndsavdelningen, juridik och parkering

Trafikkontoret har en mycket stor samling fotografier som hör till parkeringstillstånd för rörelsehindrade (PRH) som lagras på en gruppdisk. Eftersom de kan knytas till uppgifter om funktionsnedsättningar, det vill säga uppgifter om hälsa, är det fråga om känsliga personuppgifter.

En konsekvensbedömning har genomförts och dokumenterats i DPIA från Draftit. De säkerhetsåtgärder som varit möjliga att vidta har vidtagits, men tyvärr finns ännu inte någon rimlig möjlighet att gallra inaktuella uppgifter, vilket vore att föredra eftersom trafikkontoret inte får behandla uppgifter utan ett tydligt ändamål. Det ska poängteras att den stora majoriteten hör till ärenden som fortfarande är aktiva.

5.1.6 Octavius, system för parkeringsvakter

Tillståndsavdelningen, juridik och parkering.

Trafikkontoret har ställt krav på att upphandlade parkeringsvakter ska rapportera i Octavius, ett verktyg för rapportering av parkeringsövervakning. Octavius innehåller en funktion med GPS som på ett mycket detaljerat sätt visar hur den enskilda p-vakten rör sig. Det går även att se hur p-vakten rör sig dels på sin privata tid på raster, dels även efter arbetet om vakten glömmer att logga ut.

Konsekvensbedömning har påbörjats men ej slutförts. Dataskyddsombudet har rekommenderat att försöka minska på detaljrapporteringen och försöka komma ifrån kartläggning på raster och fritid. Inga förändringar har skett av användningen efter genomgång och bedömning av systemet.