Stockholms stad

GDPR Årsrapport

2023

Trafiknämnden

GDPR årsrapport
Januari 2024

Dnr: T2023-03449
Utgivningsdatum: 202X-MM-DD
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 ert Dataskyddsombud lämnar jag följande årsrapport.

Det är trafiknämnden som är personuppgiftsansvarig (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.

Sammanfattningsvis går arbetet med dataskyddsarbetet framåt på trafikkontoret främst på grund av de informationsklassningar som gjorts av IT-komponenter under året då många viktiga aspekter av dataskyddet fångas upp såsom säkerhetsåtgärder, incidenthantering, de registrerades rättigheter och pubavtal.

Trafikkontoret arbetar med att ta fram en ny förvaltningsmodell och processmodell, Vintergatan 2.0, där roller som förut var organiserade inom pm3 har förändrats och det är i nuläget osäkert hur ansvar och uppgiftsfördelning kommer att se ut när det kommer till dataskyddsarbetet.

Ingen handlingsplan gjordes för 2023 men flera av de punkter som togs upp i handlingsplanen för 2022 kvarstår. Däribland vissa frågor rörande kamerabevakning och rutiner för ostrukturerade personuppgifter.

Rutiner för konsekvensbedömning bör ses över eftersom dataskyddsombudet inte kan leda dem eftersom det står i strid med dess granskande roll.

3 Handlingsplan

3.1 Handlingsplan för 2023

Ingen handlingsplan upprättades utifrån årsrapporten för 2022.

3.2 Handlingsplan för 2024

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

4 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som 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?	117 poster i Records 151 förtecknade IT-komponenter
Har nödvändiga uppdateringar gjorts?	Delvis
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Delvis

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 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.

Trafikkontoret använder registerverktyget från Visma, Draftit Privacy Records (Records) samt förteckningen över IT-komponenter på trafikkontorets samarbetsyta för pm3, som har fält för de obligatoriska uppgifterna för personuppgiftsregister enligt dataskyddsförordningen.

Records uppdateras av DSO i samarbete med utsedda Ansvariga i Records, det är oftast Objektledare/Produktledare /Enhetschef eller Specialist/lämplig handläggare. IT-komponentförteckningen uppdateras av Objektledare för respektive objekt.

4.1.3 Resultat

Trafikkontoret har för närvarande 117 registrerade behandlingar i Records samt 151 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, Objektledare/Produktledare och Specialister för att komplettera registret.

Trafikkontoret har beslutat att avveckla Records under 2024 som registerverktyg eftersom det är besvärligt att använda för verksamheten och det är svårt att få bra överblick och det tenderar att bli för mycket information att hantera. Trafikkontoret kommer att istället börja använda en Sharepointlösning som kommer att publiceras på samarbetsytan för informationshantering.

Trafikkontoret har under 2023 gjort stora förändringar av modellen och strukturen inom pm3 och det är oklart på vilket sätt det kommer att påverka ansvar och roller när det kommer till registerföringen. Ansvars- och uppgiftsfördelning kommer att anpassas efter strukturen i Vintergatan 2.0.

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 har ingått i den övergripande modellen för dataskyddsarbetet inom pm3. Behandlingar med hög risk är väl dokumenterade i registret. De kontinuerliga informationsklassningarna pekar ut att behandlingar ska registerföras, det ingår då med i den handlingsplan som följer av klassningen. Hur uppföljningen kommer att se ut i Vintergatan 2.0 återstår att se.

4.1.5 DSO ger råd och rekommendationer till PUA

Det är prioriterat att fälten i förteckningen över IT-komponenter kompletteras av Objektledare eller Produktledare. Objektledare och Produktledare kan ta kontakt med DSO för att få stöd och hjälp i att fylla i fälten.

Trafikkontoret kommer att föra registret i Sharepoint på samarbetsytan för informationshantering. Där kan kontaktpersoner själva gå in och redigera, vilket underlättar. Detta register kommer endast att innehålla de obligatoriska uppgifterna för ett register enligt artikel 30. DSO stödjer verksamheten i detta arbete.

4.2 Styrdokument

4.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Nej
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 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 dataskyddsarbetet. Objektägare har det övergripande ansvaret för att de är på plats. Objektledare, Produktledare och informationssäkerhetssamordnare (ISAM) 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 2022 skulle trafikkontorets stab arbeta in formuleringar om dataskydd och personuppgiftsbehandling i en ny delegationsordning. Delegationsordningen är ännu inte klar men kommer troligen inte att innehålla några formuleringar om dataskydd och personuppgiftsansvar eftersom delegationsordningen enbart kommer att ta upp beslut som tas på delegation. Beslut inom dataskyddet fattas med verkställighet av trafikkontoret. Ansvar och roller formuleras därför i ett särskilt dokument, en beslutsordning eller en rollfördelning inom Vintergatan 2.0.

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

4.2.3 Resultat

Många viktiga riktlinjer och rutiner är bra. Men det saknas fortfarande rutiner för vissa områden och vissa kan vara utdaterade 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* med en *Tillämpningsanvisning.*
- *Lokal anvisning för informationssäkerhet på trafikkontoret* är inte på plats men är under arbete
- Systemdokumentation för system ska finnas, vilket inte har kontrollerats. Det är ett pågående arbete inom Vintergatan 2.0.
- Objektplaner för samtliga objekt tas fram inom Vintergatan 2.0. DSO har inte granskat dessa.

Dokument särskilt för viktiga områden inom dataskyddet

- **Rutin för personuppgiftsincident**. En rutin finns och är uppdaterad. 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 inom staden när de agerar biträden åt varandra.
- **Rutin för konsekvensbedömning**. Trafikkontoret använder verktyget DPIA från Visma, 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 registerutdrag**. Det finns en rutin för registerutdrag, men den behöver uppdateras.
- **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 utan detta sköts i verksamheten anpassat efter respektive system/process i samråd med DSO.
- **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. Objektledare/Produktledare 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.

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:

- Beslutsordning för trafikkontoret
- Lokal anvisning för informationssäkerhet
- 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
- 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?	• 57 aktuella informationsklassningar finns diarieförda • Av 117 behandlingar i Records anges 55 ha informationsklassats • Enligt ISAM:s klassningslista finns 55 genomförda klassningar
Är klassade personuppgiftsbehandlingar aktuella?	Delvis

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/system. Flera behandlingar sker i stadsgemensamma system som klassas 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. Det är osäkert om uppgifter om hur många klassningar som gjorts stämmer.

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

All information har ännu inte klassats. DSO rekommenderar därför att trafikkontoret fortsätter att arbetet med informationsklassning. Protokoll ska diarieföras så att de går att hitta. Uppgifter om infoklassning ska läggs in i förteckningen över IT-komponenter för pm3 med diarienummer.

4.4 Konsekvensbedömningar

4.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Ja, det finns 17 aktiva konsekvensbedömningar
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Ja
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 använder ett verktyg från Visma, DPIA för att genomföra konsekvensbedömningar. Trafikkontoret har fortfarande svårt att få igång en fungerande rutin för att 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 Visma som stöd för konsekvensbedömningar, DPIA.
- SLK har tagit 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 dataskyddsförordningens krav på att DSO ska närvara och övervaka konsekvensbedömningar.

Det saknas 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 lång sikt.

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

Trafikkontoret kommer att avveckla verktyget DPIA under 2024 för att gå över till att använda stadens mall. Protokollen kommer att diarieföras och bevaras i Public 360.

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 registerutdrag
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. Verksamheten kan be DSO att stödja dem de få fall som förekommer.

4.6 Personuppgiftsincidenter

4.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	• Registrerade kontaktar pua om brist • Verksamheten upptäcker brister
Hur många personuppgiftsincidenter har dokumenterats?	5
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	2
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	2

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 viss

osäkerhet hos delar av trafikkontoret hur en personuppgiftsincident ska rapporteras. Av pubavtal framgår personuppgiftsbiträdens ansvar, men det har visat sig inte alltid fungera tillfredsställande.

De incidenter som rapporterats till IMY har inte föranlett några åtgärder från deras sida.

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.

Det behöver säkerställas och följas upp att personuppgiftsbiträden har kunskap om hur personuppgiftsincidenter ska rapporteras. Detta gäller även stadeninterna biträden.

5 Övrigt att rapportera

5.1 Tredjelandsöverföringar

Hela kontoret

Överföring till USA har inte haft har tillräckligt skydd i och med Schrems II-domen och att Privacy Shield-avtalet inte längre gav tillräckligt skydd för personuppgifter på grund av amerikansk lagstiftning. Det räckte att det var ett bolag med amerikanska ägare som behandlade uppgifter för att personuppgifter skulle bedömas inte vara tillräckligt skyddade.

Nu finns ett ramverk mellan USA och EU, *Data Privacy Framework*. De mottagare som omfattas av ramverket anses ha adekvat skyddsnivå och personuppgiftsansvariga behöver inte vidta ytterligare skyddsåtgärder. SLK manar ändå fortsatt till försiktighet när det gäller överföring till USA och att stadens verksamheter ska utreda överföringar till USA.

5.2 Gatuvyer

Stadsmiljöavdelningen, projektutveckling.

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

I samband med ny upphandling av leverantör till Gatuvyer utreds frågan om hur en bättre maskning kan genomföras samt om bilderna ska upphandlas med nyttjanderätt eller äganderätt, vilket påverkar frågan om personuppgiftsansvar.

5.3 Kameror

Infrastrukturavdelningen, teknik.

Kameror i stadsmiljön innebär personuppgiftsbehandling i stor omfattning och av medborgare. Trafikkontoret har ett antal kameror av olika typer fördelade på olika avdelningar och enheter.

Infrastrukturavdelningen och trafikplaneringsavdelningen har genomfört ett projekt för inventering och ansökningar av kameratillstånd tillsammans med Governo.

Inventeringen har resulterat i en förteckning över samtliga kameror som förvaltas och drivs av trafikkontoret, med en rad uppgifter om varje kamera, samt kameratillståndsavsökningar till tillsynsmyndigheten (IMY).

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

Trafikkontoret har sökt och fått tillstånd för multisensorer för styrning av trafiksignaler runtom i staden.

Trafikkontoret, Trafikverket och Trafik Stockholm utreder personuppgiftsansvar och informationsägaskap för de kameror som nyttjas av Trafik Stockholm men som driftas av Trafikkontoret.

5.4 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 samt inskickade bilder. Att lämna kontaktuppgifter är frivilligt och krävs bara om man vill ha olika typer av feedback. Möjligheten att lämna geografisk position är för att lättare visa platsen för det ärendet gäller. Fritextfältet används för att göra en mer detaljerad beskrivning av det som ärendet gäller, det räcker oftast inte med rubrikerna. I fritextfältet kan anmälaren skriva in alla möjliga uppgifter, även känsliga. Bilder är också frivilligt att lämna men skickas in för att underlätta för utföraren.

Synpunkter, frågor, klagomål som leder till ett ärende gallras inte utan ska bevaras, därför finns idag ingen möjlighet att ta bort enbart kontaktuppgifter. Det nuvarande ärendehanteringssystemet i synpunktshanteringen kommer att ersättas av ett nytt system, Artvise, där anpassningar kommer att göras för att minimera personuppgifter som går till utförare. Ett AI-verktyg kommer att användas för att maska bilder.