Stockholms stad

Bilaga 7

GDPR Årsrapport

2021

Miljö- och hälsoskydds-nämnden

GDPR årsrapport
Januari 2022

Dnr: 2022-802
Utgivningsdatum: 2022-01-13
Kontaktperson: Mikael Nyberg

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 Dataskyddsombud i Stockholms stads Miljö- och hälsoskyddsnämnd lämnar jag följande årsrapport.

Under tillsynsåret har DSO involverats i verksamhetens dataskyddsarbete på ett aktivt och löpande sätt. DSO har således god insyn i verksamhetens förehavanden och upplever att samarbetet mellan verksamheten och DSO har lett till att nämnden utför dataskyddsarbete på en god nivå.

DSO konstaterar att verksamhetens dataskyddsarbete håller en förhållandevis hög nivå och att många av förra tillsynsårets föreslagna åtgärder har åtgärdats på ett bra sätt. Särskilt vad gäller arbetet kring verksamhetens registerförteckning.

DSO har granskat de sex obligatoriska granskningsområdena samt ett antal granskningar utöver de obligatoriska. Inledningsvis konstaterar DSO att verksamheten i god utsträckning uppfyller de krav som ställs enligt dataskyddsförordningen och enligt den aktuella rapporten. DSO återger däremot nedan de områden där vissa brister kan och behöver åtgärdas.

- DSO rekommenderar att informationsklassningsarbetet skiftas från ett systemorienterat, till ett behandlingsorienterat arbetssätt.
- DSO rekommenderar att verksamheten fortsätter med arbetet att upprätta styrdokument och komplettera de redan upprättade styrdokumenten.
- DSO rekommenderar att verksamheten upprättar blanketter som kan tillhandahållas till registrerade som vill lämna synpunkter och klagomål eller som vill utöva sina rättigheter enligt dataskyddsförordningen.
- DSO rekommenderar att verksamheten vidtar utbildningsinsatser i syfte att höja kunskapsnivån kring personuppgiftsincidenter.
- DSO rekommenderar att arbetet med att lösa de kommuninterna personuppgiftsansvarsproblemen fortsätter.

3 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 status och DSO:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	87
Har nödvändiga uppdateringar gjorts?	Ja, framförallt vad gäller komprimering och sammanslagning av personuppgiftsbehandlingar.
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

Det följer av dataskyddsförordningen art. 30 att varje personuppgiftsansvarig och personuppgiftsbiträde måste upprätta ett register över samtliga personuppgiftsbehandlingar som utförs under dess ansvar.

När registerförteckningen är upprättad skapar den en intern synlighet och förståelse för vilka personuppgifter som behandlas samt hur de hanteras. Registerförteckningen är därför dataskyddsarbetets centrala utgångspunkt och bas samt säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling. Det är därför viktigt att personuppgiftsansvarige får information om hur komplett verksamhetens förteckning är. Om dokumenteringskravet uppfylls kan verksamheten arbeta effektivt, systematiskt och riskbaserat och samtidigt värna individens integritet, särskilt när känsliga och särskilt skyddsvärda personuppgifter behandlas av verksamheten.

Att ha en registerförteckning på plats leder till att verksamheten kan arbeta mer resurs- och kostnadseffektivt med sitt systematiska och riskbaserade dataskyddsarbete. Man kan styra insatserna där de gör störst nytta.

Syftet med detta rapporteringsområde är således att rapportera till personuppgiftsansvarige hur väl verksamhetens har lyckats inventera sina personuppgifter och de personuppgifter som behandlas för annans räkning och upprätta en registerförteckning.

Eftersom inventeringen av personuppgifter i sig är avgörande för allt det fortsatta dataskyddsarbetet inom verksamheten, är denna lägesbild en av de viktigaste slutsatserna som personuppgiftsansvarige behöver förstå och ta ställning till inför det planerade åtgärdsarbetet under nästa verksamhetsår.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

87 st. personuppgiftsbehandlingar finns i nuläget registrerade i verksamhetens registerförteckning.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Vid förra årets tillsyn noterade DSO att verksamhetens registerförteckning var mycket omfattande och innehöll 1502 rader. DSO hade inga anmärkningar på registerförteckningens utformning, men innehållet ansågs alltför omfattande för att möjliggöra en god överblickbarhet. Av den anledningen anfördes en komprimering av den dåvarande registerförteckningen som en åtgärdspunkt.

DSO konstaterar att verksamheten åtgärdat åtgärdspunkten mycket väl genom att komprimera antalet rader från 1502 till 87.

DSO konstaterar att den senast uppdaterade versionen av registerförteckningen som tillhandahållits till DSO är daterad 21 oktober 2021, vilket indikerar att registerförteckningen hålls uppdaterad och levande. Uppfattningen om att registerförteckningen hålls uppdaterad understöds av uppgifter från de intervjuer som hållits i samband med tillsynsarbetet.

DSO bedömer hur fullständig registerförteckningen är

DSO bedömer att registerförteckningen är att anse som fullständig. Vid tillsyn framgår att verksamheten har arbetat rigoröst med sin registerförteckning och lagt ned ett stort arbete på att se till verksamhetens samtliga personuppgiftsbehandlingar ingår. DSO konstaterar att verksamhetens samtliga personuppgiftsbehandlingar

med största sannolikhet ingår i registerförteckningen. I vart fall finns en sådan ambition i verksamheten.

Registreringarna håller i regel en god kvalitet innehållsmässigt och exempelvis är fältet *Laglig grund* ifyllt i samtliga registreringar. I vissa fall saknas däremot information i registerförteckningen. Framförallt vad gäller fältet *(Om möjligt) Allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder*, som endast är ifyllt i 7 av de 87 registreringarna.

DSO noterar även att registerföringen i regel är utformad och strukturerad utefter behandlingar och inte efter system, i enlighet med vad Stockholm stad rekommenderar. I vissa fall är däremot system angivna som personuppgiftsbehandlingar, exempelvis vad gäller behandlingarna med namn *Fleetmanagement* och *Molntjänst-Antura projects*. Den angivna informationen i exempelvis *Fleetmanagement* har vissa brister innehållsmässigt, såsom att ett fält innehåller endast ett frågetecken. DSO noterar att verksamheten framöver fullständigt bör föra sin registerförteckning efter behandlingar och inte efter vilka system dessa sker i.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

DSO konstaterar att verksamheten har nedtecknade rutiner för arbetet med registerförteckningen. Det innebär att verksamheten arbetar med registerförteckningen som ett levande dokument på ett gott sätt.

3.1.4 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

3.1.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att verksamheten fokuserar registerföringen helt och hållet på ett behandlingsorienterat sätt, i motsats till ett systemorienterat sätt, och som ett led i detta raderar eller sammanfogar behandlingar med andra beskrivna behandlingar, såsom exempelvis *Fleetmanagement*.

DSO rekommenderar även att fältet *(Om möjligt) Allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder* fylls på i den utsträckning som är möjlig.

3.2 Styrdokument

3.2.1 Sammanfattning

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

3.2.2 Syfte

Området syftar till att personuppgiftsansvarige genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar personuppgiftsansvarige till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna, när de hanterar personuppgifter. Att styrdokument finns nedtecknade, beslutade och kommunicerade medför att medarbetaren får dataskyddsinformation och kan behålla kunskapen över tid och tillämpa den på ett konsekvent sätt. En röd tråd i Dataskyddsförordningen är att viktiga arbetssätt och rutiner ska vara dokumenterade. Detta följer bland annat av kravet på att den personuppgiftsansvarige måste kunna *visa* att dataskyddsförordningens principer för behandling av personuppgifter efterlevs (artikel 5).

Rapporteringen av området är tvådelad: dels ska DSO bedöma om verksamheten har relevanta styrdokument antagna och på plats, dels ska rapporteringen visa om dokumentationen innehållsmässigt håller en lämplig kvalitet, i vilket ingår bl.a. att dokumentationen ska vara uppdaterad och aktuell.

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?

DSO konstaterar att verksamhetens styrande dokumentation i dagsläget omfattar en stor del av dataskyddsområdet. Verksamheten har följande nedtecknade rutiner:

- Rutin för konsekvensbedömning
- Rutin för tillvaratagande av de registrerades rättigheter
- Rutin för begäran om registerutdrag
- Rutin för hantering av personuppgiftsincident
- Rutin för användning av nya molntjänster
- Rutin för elektronisk kommunikation (berör delvis GDPR)
- Rutin för att hålla artikel 30-registret uppdaterat

DSO bedömer att den styrande dokumentationen är godtagbart omfattande, men att det finns utrymme för fortsatt arbete med att upprätta än mer styrande dokumentation. De punkter som bör täckas in framöver är:

- Rutin för hur verksamheten hanterar inbyggt dataskydd och dataskydd som standard i verksamhetens processer och rutiner enligt art. 25. Syftet med en sådan rutin är att undersöka om verksamheten tagit höjd för och analyserat hur de grundläggande principerna i art. 5 ska beaktas i relevanta processer och rutiner. Exempel på sådana analyser är: används automatiska lösningar såsom raderings-funktioner och/eller textbegränsningar som främjar principen om uppgifts- och lagringsminimering? Hur stor är risken att medarbetarna gör manuella fel när de ska distribuera information via brev till medborgare?
- Rutin för publicering av handlingar och personuppgifter på sociala medier och på start.stockholm. DSO rekommenderar att denna dokumentation även innehåller rutiner för hur verksamheten använder sig av samtycke respektive modellavtal som laglig grund.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

DSO bedömer att innehållet i de tillhandahållna dokumenten håller god kvalitet. Rutinerna är överskådliga, lättillgängliga, omfattande och är utformade för att kunna användas av samtliga anställda.

DSO konstaterar att de tillhandahållna dokumenten saknar en uttryckligen angiven ägare. I en del av dem, exempelvis rutinen för tillvaratagande av de registrerades rättigheter, framgår vem som gjort den senaste uppdateringen i dokumentet. Huruvida den personen är ägare av dokumentet eller inte framgår inte. I rutinen för användning av molntjänster saknas ett sådant namn över huvud taget. DSO rekommenderar därför att verksamheten identifierar och anger en ägare för varje upprättat styrdokument.

DSO konstaterar att dokumenten förefaller vara relevanta och väl uppdaterade.

3.2.4 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

3.2.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att verksamheten fortsätter arbetet med att upprätta fler styrande dokument, förslagsvis rutin för inbyggt dataskydd och dataskydd som standard samt rutin för publicering av personuppgifter på sociala medier och på Stockholm stads hemsida, inbegripet en rutin för användande av samtycke respektive modellavtal som laglig grund.

DSO rekommenderar även att verksamheten identifierar och anger en ägare för varje upprättat styrdokument.

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

3.3.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	~65
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd så ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Utan informationsklassningen har verksamheten inte förutsättningar att välja rätt åtgärder för att skydda sin information. Det är därför av stor betydelse för dataskyddsarbetet att personuppgiftsansvarige ges en uppdaterad bild varje år av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar.

Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. En första kontrollpunkt måste därför vara om en informationsägare eller en informationsägarrepresentant med ansvar för klassning är identifierad i verksamheten. Om en ansvarig för klassningen inte har pekats ut och känner till sitt ansvar för uppdraget, minskar sannolikheten avsevärt att en klassning faktiskt initieras.

Notera att enbart sådan informationsklassning som avser behandling eller system som omfattar *personuppgifter* är av intresse för DSO:s årsrapportering.

3.3.3 Resultat

DSO konstaterar att verksamhetens informationsklassning i huvudsak har gjorts på systemnivå (och inte på behandlingsnivå, vilket är den uppdelning som Stockholms stad i andra sammanhang bedömer mest relevant att tillämpa):

2016-12-22 Miljödatabasen
2017-01-02 Miljöbarometern
2017-01-11 Kemikalieregistret
2017-07-03 Livsmedelskollen
2017-08-30 Ecos 1
2019-02-27 E-tjänst Värmepumpar
2019-03-26 Kemikalieregistret
2020-05-29 E-tjänst Brister
2020-05-29 REST
2020-06-25 Livsmedelskollen
2020-06-25 Livsmedelsinspektioner
2020-06-25 E-tjänst Matförgiftningar
2020-09-14 Elektronisk körjournal
2020-10-02 Elektronisk körjournal
2020-10-05 E-tjänst inomhusmiljö
2020-10-07 App luftkvalitet
2020-10-19 App luftkvalitet
2020-10-20 Flextidsystem
2020-10-28 Ecos 2
2020-11-24 Klimatpaktens kundhanteringssystem
2020-11-25 E-tjänst Registrera livsmedelsverksamhet
2020-12-01 Biodrivmedelskampanj
2021-01-27 Antura project
2021-01-28 E-tjänst inomhusmiljö
2021-02-09 Agresso
2021-02-10 Lisa självservice
2021-06-15 Lisa självservice
2021-10-25 Avista time

DSO har jämfört systemklassningarna mot de angivna system som anges i registerförteckningens fält ”Var finns personuppgifterna?”. DSO konstaterar att de genomförda informationsklassningarna täcker de allra flesta system som används vid de flesta av nämndens personuppgiftsbehandlingar.
Däremot anmärker DSO att de personuppgiftsbehandlingar som sker i exempelvis endast Outlook eller på verksamhetens servrar (t.ex. ”Outlook, N:” i personuppgiftsbehandling ”*Inom ramen för EKR-samarbetet: inbjudan till skolor- workshop*”, eller ”epost,

intranätet, fotografier sparas i mapp på U: [liksom namnskyltar]” i personuppgiftsbehandlingen ”*Hantera intern kommunikation*”) inte förefaller täckas av de systemövergripande informationsklassningar som gjorts.

Översyn av klassningarna sker årligen och anses vara någorlunda aktuella.

Det innebär att DSO bedömer att det är rimligt att anta att lämpliga tekniska och organisatoriska åtgärder är vidtagna för verksamhetens personuppgiftsbehandlingar.

3.3.4 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

3.3.5 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att verksamheten fortsätter med sitt informationsklassningsarbete i fråga om personuppgiftsbehandlingar som inte sker i de datorsystem som hittills informationsklassats. DSO noterar även att utformningen av SKR:s KLASSA i dagsläget är systemorienterat och att viss personuppgiftsbehandling därför kan vara svår att passa in i den mall som tillhandahålls av KLASSA.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

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

3.4.2 Syfte

Konsekvensbedömningen hjälper en organisation att identifiera och minimera integritetsriskerna för personuppgifter som behandlas i projekt eller linjeverksamhet. En konsekvensbedömning har till syfte att identifiera och dokumentera risker kopplade till en viss behandling, samt att bedöma sannolikheten och konsekvensen om riskscenariot skulle inträffa. Baserat på bedömningen kan/ska riskförebyggande åtgärder vidtas.

Konsekvensbedömningen anses liksom registerförteckning och informationsklassning som ett viktigt verktyg för verksamhetens dataskyddsarbete. Kravet på konsekvensbedömning är dessutom ett uttryckligt krav enligt GDPR och ska utföras för alla behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1). Det är viktigt att personuppgiftsansvarige genom årsrapporten får en uppdaterad bild av hur fullständig verksamhetens situation är i fråga om konsekvensbedömningar avseende dataskydd.

3.4.3 Resultat

Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?

Verksamheten har inte gjort någon faktisk retroaktiv inventering av redan pågående personuppgiftsbehandlingar som kan tänkas innebära hög risk för fysiska personers rättigheter och friheter och på så sätt föranleda en konsekvensbedömning. Däremot konstaterar DSO att kunskapsläget och medvetenheten kring dataskyddsfrågor bland de anställda är på så pass hög nivå att det enligt vår bedömning inte föreligger någon risk att någon högriskbehandling som inte konsekvensbedömts skulle pågå i dagsläget. Eftersom verksamhetens systemanvändande i stort styrs ovanifrån av Stockholms stads direktiv, så minimeras risken att nämnden i sig ensamt använder sig av ett system som skulle innebära en hög risk utan att ha konsekvensbedömts.

I sammanhanget kan även nämnas att verksamheten också har inlett ett arbete med en förstudie gällande anslutande till digitala myndighetsbrevlådor.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Verksamheten har under tillsynsåret genomfört två konsekvensbedömningar: en vad gäller ett körjournalssystem och en vad gäller ett flextids-system. Vad gäller körjournalssystemet så konstaterade verksamheten efter samråd med både DSO och IMY att det i dagsläget tycks saknas förutsättningar att använda sig av den del av körjournalssystemet som berör insamling och lagring av uppgifter om lagöverträdelser.

Vad gäller flextids-systemet så har verksamheten genomfört en upphandling baserad på konsekvensbedömningen, som nu ska uppdateras med information om den upphandlade tjänsten innan den godkänns.

Är de genomförda konsekvensbedömningarna aktuella?

DSO konstaterar att de genomförda konsekvensbedömningarna är genomförda i närtid och är aktuella. Personuppgiftsbehandlingarna som konsekvensbedömningarna avser har inte förändrats i någon mån och konsekvensbedömningarna har således inget behov av att uppdateras.

3.4.4 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
	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
X	Inga brister av nämnvärd betydelse identifierade

DSO bedömer att verksamhetens situation kring konsekvensbedömningsarbetet är så gott som fullständigt. Kunskapsläget är mycket bra, både hos ledningen och hos berörda anställda i stort. Av den anledningen föreligger en låg risk att verksamheten ägnar sig åt icke konsekvensbedömda personuppgiftsbehandlingar som innebär en hög risk för registrerades fri- och rättigheter.

De genomförda konsekvensbedömningarna där DSO involverats håller mycket god kvalitet.

3.4.5 DSO ger råd och rekommendationer till PUA

Som framhålls på annan plats i denna rapport, finns det enligt DSO skäl att klargöra ansvarsfördelningen mellan Stockholms stad centralt och miljö- och hälsoskyddsnämnden som personuppgiftsansvarig, när det gäller personuppgiftsbehandlingar som sker exempelvis i datasystem som upphandlats centralt och där användningen för nämndernas del är påbjuden från Fullmäktige eller SLK. En sådan översyn kommer sannolikt även att ge återverkningar för hur ansvaret för konsekvensbedömningar av system respektive behandlingar fördelas inom staden i framtiden.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäranden (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	2
Hur många av dessa begäranden har hanterats av verksamheten inom 30 dagar?	Samtliga

3.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt garanterar att den registrerade personen har insyn i hur dennes personuppgifter hanteras samt har en viss kontroll över personuppgiftsbehandlingen. Det är ett krav enligt förordningen att den personuppgiftsansvarige tillgodoser rättigheterna i fråga.

Rättigheterna medför en rätt att ställa krav på att verksamheten vidtar vissa åtgärder, som exempelvis att lämna ut ett så kallat registerutdrag eller att rätta vissa uppgifter. (Radering, den så kallade ”rätten att bli glömd”, är sällan aktuell i någon större mån eftersom stadens organ lyder under krav på bevarande till följd av offentlighetsprincipen.) Verksamheten har enligt dataskyddsförordningen artikel 12.3 en skyldighet att vidta åtgärder inom trettio dagar efter att ha mottagit begäran. (Notera även att det finns undantagssituationer angivna i artikel 12.3, där svarsfristen kan förlängas till mer än en månad.)

Dataskyddombudet har en roll i att granska efterlevnaden, identifiera brister samt ge råd och stöd hur processer och rutiner för att tillgodose rättigheterna bör utformas.

Om verksamheten inte klarar av att hantera en begäran från en registrerad person i enlighet med dataskyddsförordningens krav, kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter. Det kan även leda till tillsynsärenden från IMY:s sida, med sanktioner som följd. Det är därför viktigt att

personuppgiftsansvarige regelbundet ges en bild av i vilken mån verksamheten klarar av att leva upp till regelverkets krav på att hantera begäran inom föreskriven tidsfrist.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

Verksamheten har under tillsynsåret tagit emot en begäran om registerutdrag och en begäran om radering. Båda hanterades inom föreskriven tidsfrist på 30 dagar.

DSO konstaterar att verksamheten har goda förutsättningar för att hantera registrerades rättigheter på ett mycket gott sätt. Vid utbildningstillfällen gällande dataskyddsarbete inom verksamheten så har det lagts fokus både på hur de registrerades rättigheter ska hanteras samt hur gallring och radering ska ske på ett fullgott sätt med beaktande av såväl offentlighetsprincipen som GDPR. DSO bedömer också att de rutiner som finns nedtecknade för att tillvarata de registrerades rättigheter är mycket goda.

3.5.4 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

3.5.5 DSO ger råd och rekommendationer till PUA

Som ett nästa steg i arbetet med att tillvarata de registrerades rättigheter rekommenderar DSO att verksamheten upprättar blanketter att tillhandahålla till registrerade som vill utöva sina rättigheter. En sådan blankett underlättar både för den registrerade att lätt kunna ta tillvara på sina rättigheter, och för verksamheten som genom en väl ifylld blankett får den information de behöver för att tillmötesgå begäran redan i ett första skede.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Genom att anställda ute i verksamheten anmäler till behörig person, eller genom att ledning och dataskyddssamordnare plockar upp signaler om sådana incidenter.
Hur många personuppgiftsincidenter har dokumenterats?	12
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	1
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	0

3.6.2 Syfte

Med begreppet personuppgiftsincident avses enligt dataskyddsförordningen (artikel 4.12) ”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.”

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland dataskyddsförordningens olika verktyg för att åstadkomma en god personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering. Stadens mall för DSO:s årsrapport är avsedd att fokusera på rapporteringen.

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten

gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se artikel 33). Detta innebär att de flesta personuppgiftsincidenter ska rapporteras till IMY, och då inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter, ska rapportering även ske till de berörda registrerade personerna, utan dröjsmål. Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt rapportering till de berörda personerna.

Bristande förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner från IMY:s sida. DSO:ns årsrapportering är därför avsedd att kartlägga detta, samtidigt som det finns möjlighet att redovisa vilka typer av personuppgiftsincidenter som inträffat, incidenternas allvarsgrad etc.

Notera att enligt dataskyddsförordningen artikel 33.5 ska alla personuppgiftsincidenter dokumenteras, det vill säga även i de fall då incidenten inte ska rapporteras till IMY. Bristande dokumentering står i strid med Dataskyddsförordningen och leder även till problem med att ta fram korrekta siffror till årsrapporteringen avseende hur väl verksamheten lever upp till rapporteringsfristerna. Enligt artikel 33.5 är det ett krav att dokumentera omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för den egna organisationen att förbättra sin personuppgiftshantering genom systematiskt kvalitetsarbete och för tillsynsmyndigheten (IMY) att kontrollera efterlevnaden. Bristande dokumentation är sanktionsgrundande.

3.6.3 Resultat

Hur väl förmår verksamheten att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten?

De personuppgiftsincidenter som dokumenterats under tillsynsåret har samtliga inneburit en obetydlig risk för enskildas friheter och rättigheter och ingen av dem har därför rapporterats till IMY. DSO uppfattar, givet den information som funnits tillgänglig vid bedömningstillfällena, att bedömningen att de anmälda incidenterna varit av ringa betydelse varit korrekt. Gällande en av incidenterna har det dock uppdagats i efterhand att bedömningen av risken för

den enskilde kan ha gjorts utifrån delvis felaktiga uppgifter och att den därför kan behöva göras om.

3.6.4 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

3.6.5 DSO ger råd och rekommendationer till PUA

DSO noterar att tolv st. personuppgiftsincidenter under ett tillsynsår för en verksamhet av den aktuella storleken är ett förhållandevis lågt antal. Likväl det faktum att endast en av incidenterna har bedömts utgöra en sådan risk för enskildas fri- och rättigheter att en rapport ska göras till IMY är noterbart. Det kan finnas två anledningar till ett sådant förhållandevis lågt antal: antingen hanterar verksamheten sina personuppgifter på ett ovanligt tillfredsställande sätt, eller så sker det i praktiken fler incidenter, men som inte rapporteras eller anmäls till de ansvariga i organisationen. Det kan alltså finnas ett mörkertal som beror på exempelvis en låg kunskapsgrad i verksamheten om vad en personuppgiftsincident faktiskt är och hur en sådan incident ska hanteras när den befaras ha inträffat. DSO noterar däremot att verksamheten uppvisar att de nästintill omgående tagit till sig av den återkoppling som DSO gav under tillsyn och rapportförfattandet, och att verksamheten visar mycket goda förutsättningar för att fortsatt förbättra arbetet med hantering av personuppgiftsincidenter samt spridning av kunskap inom verksamheten.

Av den anledningen rekommenderar DSO att personuppgiftsansvarige lägger särskilt fokus på att sprida kunskap om personuppgiftsincidenter och hur de ska hanteras. En lämplig insats för att öka på denna kunskap kan vara obligatoriska utbildningstillfällen för ledning och personal.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- *Granskning 1 – Implementering av åtgärder från förra årets tillsynsrapport*
- *Granskning 2 – Samtycke som rättslig grund*
- *Granskning 3 – Agerande med anledning av Schrems II-domen*

4.2 Syfte

En av dataskyddsombudets viktigaste uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen. En central del av det arbetet är att göra återkommande granskningar av hur väl dataskyddsförordningen efterlevs. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten kan fatta i fråga om dataskyddsåtgärder. För personuppgiftsansvarige är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och vad resultaten av granskningarna är.

4.3 Genomförda granskningar och deras resultat

Granskning 1 – Implementering av åtgärder från förra årets tillsynsrapport

I förra årets tillsynsrapport rekommenderade DSO ett antal åtgärder, däribland: komplettering och komprimering av artikel 30-registret, placering av personuppgiftsansvar i stadsgemensamma personuppgiftsbehandlingar, upprättande av rutiner för tillvaratagande av registrerades rättigheter, systematisering av informationsklassning av informationstillgångar, upprättande av rutiner för genomförande av tröskelanalyser och konsekvensbedömningar.

DSO konstaterar att de flesta av de rekommenderade åtgärderna har implementerats väl av Miljönämnden. De åtgärder som ännu ej implementerats fullt ut är: placering av personuppgiftsansvar i stadsgemensamma personuppgiftsbehandlingar samt systematisering av informationsklassning av informationstillgångar.

Vad gäller placering av personuppgiftsansvar i stadsgemensamma personuppgiftsbehandlingar konstaterar DSO att verksamheten har inlett ett stadsgemensamt samarbete i avsikt att lösa frågan. Verksamheten har upprättat ett förslag/utkast och ärendet ligger vid rapportens upprättande på annan verksamhet i stadens organisation. DSO konstaterar givet detta att nämnden har gjort en ansats att försöka implementera den rekommenderade åtgärden så långt det går från eget håll.

DSO konstaterar att arbetet med att systematisera informationsklassning av informationstillgångar har framskridit men att vissa förbättringsområden återstår. Verksamheten har under tillsynsåret agerat utefter den kritik som framfördes av Stockholm stads Revisionskontor, vilken låg till grund även för den rekommenderade åtgärden från DSO. Således finns det nu upprättade rutiner vad gäller det specifika datasystemet. Det finns även uttryckliga instruktioner om att informationsklassning ska ske av nya system. Vad gäller informationsklassning av systemanvändning finns således en klar och tydligt upprättad rutin, dock inte vad gäller personuppgiftsbehandlingar som sker utanför användningen i de stora systemen. DSO rekommenderar att verksamheten i fortsättningen arbetar vidare med att systematisera informationsklassning av personuppgiftsbehandlingar som sker separat från systemanvändning.

	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

Granskning 2 – Samtycke som rättslig grund

DSO granskande verksamhetens användning av samtycke som rättslig grund för viss personuppgiftsbehandling. På grund av verksamhetens karaktär (kommunal nämnd och förvaltning) så används samtycke i mycket liten omfattning som rättslig grund för personuppgiftsbehandlingar. Verksamheten uppger att samtycke används vid publicering av fotografier, intervjuer och filmer. Det är

producenten/redaktören för den enskilda publiceringen som inhämtar samtycket från berörda enskilda. Den samtyckande kan återkalla sitt samtycke när som helst genom att höra av sig till verksamhetens funktionsbrevlåda för e-post. Verksamheten är även införstådd i de särskilt höga krav som ställs på informationsgivning i samband med inhämtande av samtycke, samt de höga krav som ställs vid inhämtande av samtycke från barn. DSO konstaterar att verksamhetens användning av samtycke som rättslig grund håller en godkänd nivå.

Verksamheten har tagit fram en blankettmall för samtycke. DSO noterar däremot att blankettmallen inte används i dagsläget. DSO noterar vidare att det saknas nedtecknade rutiner för hur verksamheten använder sig av samtycke som laglig grund och när andra lösningar, som exempelvis modellavtal, kan vara en lämpligare lösning. DSO konstaterar också att det i blankettmallen finns möjlighet för den samtyckande att ange en tidsrymd för när samtycket ska vara giltigt. Verksamheten tycks däremot sakna nedtecknade rutiner för att stämma av huruvida en sådan tidsangivelse förfallit. DSO rekommenderar därför verksamheten att implementera den upprättade blankettmallen samt upprätta rutiner för hur verksamheten ska använda sig av samtycke som rättslig grund, inbegripet en rutin för att kontinuerligt stämma av huruvida ett samtycke förfallit enligt den tidsrymd som den samtyckande kan ha angivit.

	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

Granskning 3 – Agerande med anledning av Schrems II

Under förra tillsynsåret kom avgörandet Schrems II från EU-domstolen. I avgörandet slog domstolen fast att Privacy Shield-avtalet mellan EU och USA inte gav ett tillräckligt skydd för personuppgifter när dessa förs över till USA. Ogiltigförklarandet innebär att verksamheter inte längre kan stödja sig på Privacy

Shield som grund för att överföra personuppgifter till USA. DSO har därför valt att granska verksamhetens agerande med anledning av Schrems II-avgörandet.

DSO konstaterar inledningsvis att verksamheten uppvisar god kunskap om avgörandet och de konsekvenser avgörandet har fått på dataskyddsområdet i stort. Det finns en tydlig förståelse i verksamheten om de problem som tredjelandsöverföring till USA innebär. Som exempel på den goda medvetenheten så ställer verksamheten numer ska-krav i nya upphandlingar av data- och molntjänter på att inga tredjelandsöverföringar av personuppgifter ska ske.

DSO noterar däremot att kommunikationsavdelningen i verksamheten använder sig av ett flertal olika sociala medier, exempelvis Facebook och LinkedIn. Där publicerar verksamheten exempelvis rekryteringsannonser eller information som har med verksamheten att göra. DSO konstaterar att verksamheten fortsättningsvis bör hålla personuppgiftsbehandling på sociala medier, i form av exempelvis publikation av bilder med identifierbara fysiska personer, på så låg nivå som möjligt.

	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

4.4 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att verksamheten arbetar vidare med systematiseringsarbetet vad gäller informationsklassning av informationstillgångar, särskilt i form av nedtecknade rutiner som täcker in personuppgiftsbehandling som sker utöver systemanvändning – exempelvis vid publiceringar på hemsida och sociala medie-plattformar.

DSO rekommenderar att verksamheten implementerar och använder sig av den blankettmall för inhämtning av samtycke, samt upprättar nedtecknade rutiner för användning av samtycke.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- *Risk 1 – Kommuninterna förhållanden*
  - *A) Kommunintern fördelning av personuppgiftsansvar*
  - *B) Skillnad i riskanalys på systemnivå respektive behandlingsnivå*
- *Risk 2 – Närvaro på sociala medier*
- *Risk 3 – Sannolikt att kunskapsnivå kring personuppgiftsincidenter behöver höjas*

5.2 Syfte

Nämnden ansvarar för att utföra vissa typer av riskanalyser, så som konsekvensbedömningar och informationsklassningar, men dessa ger inte en heltäckande bild av personuppgiftsriskerna i verksamheten. Såväl den personuppgiftsansvarige som dataskyddsombudet behöver ha kontinuerlig överblick över dessa risker som underlag för egen planering och löpande arbete. Detta gäller för verksamhetens samtliga personuppgiftsbehandlingar. Exempelvis krävs en sådan överblick för att kunna välja ut vilka områden som bör granskas under det kommande året eller för att avgöra vilka råd som dataskyddsombudet behöver lämna till verksamheten om dataskyddsåtgärder som behöver vidtas.

5.3 Resultatet av riskkartläggningen

Risk 1 – Kommuninterna förhållanden

A) DSO har i kommunikation med verksamheten redan tidigare identifierat en problematik vad gäller kommuninterna förhållanden. Problematiken består i att verksamhetens personuppgiftsansvar tillfaller miljö- och hälsoskyddsnämnden. Nämnden är däremot bunden till de beslut om exempelvis systemanvändning som i överensstämmelse med kommunernas reglering tas ovanifrån. Här har DSO identifierat en risk kan det uppkomma situationer där nämnden kan betraktas som ansvarig enligt GDPR för beslut som man inte själv förfogar över. DSO noterar att frågan lämpligen kan regleras genom exempelvis stadsinterna styrdokument eller reglementen, snarare än via personuppgiftsbiträdesavtal. DSO konstaterar att denna problematik inte på något sätt är unik för Stockholms Stad, utan är ett inherent problem i stort sett samtliga kommunala organisationer i Sverige.

DSO:s uppfattning är att problematiken har identifierats i Stockholms stad såväl som hos nämnden och att ett arbete för att lösa frågan har inletts under ledning av SLK, där nämnden genom miljöförvaltningen involverats för synpunkter och förslag. DSO uppmuntrar därför Stockholm stad, via miljö- och hälsoskyddsnämnden, att fortsätta arbetet.

B) DSO konstaterar att verksamhetens informationsklassningsarbete för närvarande sker i huvudsak på systemnivå. En anledning till detta är att SKR:s riskklassningsverktyg KLASSA, som Stockholm stad anmodat sina nämnder och bolag att använda i detta arbete, är utformat för ett mer systemorienterat arbete. En risk med ett sådant arbetssätt är att viss personuppgiftsbehandling inte träffas av de informationsklassningar som gjorts (på systemnivå), exempelvis i det fall personuppgiftsbehandlingen sker i form av pappershantering eller i mappstrukturen på de egna servrar som medarbetarna kommer åt genom sina persondatorer.

	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

Risk 2 – Närvaro på sociala medier

Med anledning av Schrems II-domen så har frågan om verksamheters närvaro på sociala medier ställts på sin spets, då nästintill alla sociala medier tillhandahålls av amerikanska leverantörer. Det innebär att rättsläget kring närvaro på sociala medier är i dagsläget oklart. Den norska dataskyddsmyndigheten Datatilsynet publicerade nyligen en riskbedömning där myndigheten kom fram till att skulle upphöra med sin närvaro på Facebook. DSO påpekar att DSO inte anmodar verksamheten att upphöra med all närvaro på sociala medier, men vill däremot uppmärksamma de risker som finns involverade med sådan närvaro. De möjligheter som GDPR ställer upp för personuppgiftsöverföring till tredje land (se kapitel V), som är möjliga att tillämpa när inget beslut om adekvat skyddsnivå föreligger för ett specifikt land eller territorium, är dock komplicerade att tillämpa och kräver noggrant dokumenterade förstudier och avvägningar. Såvitt DSO känner till är sådant varken på plats hos miljö- och hälsoskyddsnämnden eller hos Stockholms stad generellt.

	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

Risk 3 – Sannolikt att kunskapsnivån kring personuppgiftsincidenter behöver höjas

Som tidigare nämnt så anmärker DSO att antalet personuppgiftsincidenter under granskningsåret (12 st.) är ett lågt antal för en verksamhet av den aktuella storleken. DSO befarar att det låga antalet beror på att kunskapsnivån kring personuppgiftsincidenter hos personal och ledning är otillräcklig. En låg kunskapsnivå riskerar inte bara leda till att faktiska personuppgiftsincidenter förblir orapporterade, utan att personuppgiftshantering i stort riskerar att skötas på ett otillräckligt sätt, exempelvis när det uppstår orsak att gå utanför gängse arbetsrutiner för att utföra en uppgift.

5.4 DSO ger råd och rekommendationer till PUA

DSO rekommenderar att miljö- och hälsoskyddsnämnden uppmuntrar Stockholm stad, tillsammans med övriga berörda nämnder, att fortsätta arbetet med att klargöra och dokumentera de kommuninterna relationerna för personuppgiftshantering, främst i kommunövergripande datasystemen.

DSO rekommenderar verksamheten att skifta fokus i informationsklassningsarbetet från en systemorienterad inriktning till en bredare personuppgiftsbehandlingsorienterad inriktning.

DSO rekommenderar att verksamheten ser över sin närvaro på USA-kontrollerade sociala medieplattformer. DSO rekommenderar verksamheten att arbeta fram rutiner för närvaro på sociala medier, inbegripet rutin om användande av samtycke och modellavtal som laglig grund.

DSO rekommenderar att verksamheten lägger ytterligare fokus på att höja kunskapsnivån hos personalen i verksamheten gällande dataskyddsfrågor, särskilt vad gäller personuppgiftsincidenter.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Område 1 – hantering av klagomål och synpunkter från registrerade*
- *Område 2 – Stadsinterna förhållanden*

6.2 Syfte

Som nämnts ovan är det granskande arbetet en av dataskyddsombudets viktigaste uppgifter. Granskningsområdena har valts utifrån ett riskbaserat synsätt, det vill säga att fokus läggs på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister.

Granskning 1 – Hantering av klagomål och synpunkter från registrerade

I mars 2021 fattade IMY beslut om en ny tillsynspolicy (https://www.imy.se/nyheter/klagomal-i-fokus-for-kommande-tva-ars-granskningar/). I tillsynspolicyn uppger IMY att fokus i kommande två år kommer att ligga på klagomål och synpunkter från registrerade. Det innebär att myndighetens fokus för tillsynsärenden, från deras håll, kommer att ligga på klagomål från registrerade.

DSO noterar att enskildas klagomål och synpunkter inte bara är av stor betydelse i dataskyddsarbetet, utan även är ett av dataskyddsförordningens fundamentala syften, i fråga om tillvaratagande av enskildas rättigheter.

DSO väljer därför att i kommande tillsynsår granska hur väl verksamheten är rustad att hantera klagomål och synpunkter från enskilda. DSO uppmuntrar verksamheten att i förebyggande syfte exempelvis upprätta blanketter som kan tillhandahållas till registrerade som vill tillvarata sina rättigheter.

Granskning 2 – Kommuninterna förhållanden

DSO väljer att till nästa år granska hur verksamheten, och i förlängningen Stockholm Stad, arbetar för att lösa problematiken kring den kommuninterna personuppgiftsansvarsfördelningen. Som ovan nämnts känner DSO till att frågan leds av SLK och att miljö- och hälsoskyddsnämnden involverats i detta. Däremot finns ett stort värde i att arbetet fortskrider och DSO väljer därför att till nästa tillsynsår fördjupa granskningen av hur detta arbete fortskrider.

Stockholm 2022-01-13

Simon Jernelöv, Externt DSO för Miljö- och hälsoskyddsnämnden, Stockholms stad, och Anders Eriksson, dataskyddsjurist.