Stockholms stad

GDPR Årsrapport

2022

Socialförvaltningen

1 Bakgrund

Dataskyddslagstiftningen och skyddet för individens personliga integritet har sin grund i de mänskliga rättigheterna i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, Europakonventionen. Den mänskliga rättighet som avses är individens rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Individen ska inte behöva utsättas för godtyckliga eller olagliga inskränkningar i sitt privatliv.

Europeiska unionen har antagit EU-stadgan om de grundläggande rättigheterna. Skyddet för individens personliga integritet föreskrivs i rättigheten att var och en har rätt till respekt för sitt privat- och familjeliv, sin bostad och sina kommunikationer. EU-stadgan innehåller även individens rätt till skydd för personuppgifter.

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

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 och obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som Personuppgiftsansvarig, i fortsättningen kallad 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.

I årets rapport kommer skyldigheterna nedan att beskrivas:
- att föra ett behandlingsregister,
- att ta fram styrdokument, rutiner och instruktioner avseende hur personuppgifter får behandlas,
- att implementera tekniska och organisatoriska skyddsåtgärder för personuppgifter,
- att utföra konsekvensbedömning avseende dataskydd,
- att kunna ta emot och hantera individens rättigheter,
- att ha förmåga att upptäcka, hantera och förebygga personuppgiftsincidenter.

Genomförda granskningar samt rekommendationer i fråga om obligatorisk e-utbildning avseende dataskydd och informationssäkerhet återfinns i årsrapporten. Årsrapporten kommer även behandla implementeringen av nya forumet för GDPR och informationssäkerhet.

Nedan redogörs för nämndens status. Vidare presenteras slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter genomförd uppföljning och granskning för året 2023.

3 Registerförteckning

3.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	292 registreringar.
Har nödvändiga uppdateringar gjorts?	Ja.
Bedöms registerförteckningen vara fullständig?	Delvis.
Har verksamheten lämpliga rutiner för registerföring?	Ja.

3.2 Syfte

Det följer i klartext av dataskyddsförordningen (artikel 30) att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas, i fortsättningen kallat personuppgiftsbehandlingar, i verksamheten och dokumentera dem i en så kallad registerförteckning. Förvaltningens registerförteckning återfinns i verktyget Draftit Privacy Records. När registerförteckningen är upprättad skapar den en intern synlighet och förståelse för personuppgiftsbehandlingar vilka finns och hur de hanteras. Registerförteckningen säkerställer att verksamheten beaktar att det ska finnas en laglig grund inom ramen för all personuppgiftsbehandling.

3.3 Resultat

Det finns idag 292 personuppgiftsbehandlingar registrerade i verktyget Draftit Privacy Records, sex av dem är riskregistreringar. Sammanfattningsvis är det fyra registreringar fler än under år 2021. Dataskyddsombudet ser det som positivt att flertalet personuppgiftsbehandlingar är registrerade, att förvaltningen börjat använda verktyget Draftit Privacy Records i stor utsträckning och att det idag finns en större kunskap inom förvaltningen huruvida nya personuppgiftsbehandlingar ska införas i registerförteckningen. Dataskyddsombudet bedömer dock att registerförteckningen inte är helt fullständig och att utvecklingsområdet från tidigare år, år 2021, till viss del kvarstår.

Samtliga registreringar vilka återfinns i systemet behöver återge korrekt och efterfrågad information exempelvis genom att personuppgiftsbehandlingar sker i enlighet med GDPR och gällande lagstiftning. Det bör fortsatt pågå ett löpande arbete med att implementera arbetet med risk- och konsekvensanalys i samband med registreringar i systemet Draftit Privacy Records. Vidare behövs fortsatt inventering av de äldsta registerförteckningarna utföras i förhållande till riskbehandlingar. Vidare ska dessa vid behov kompletteras med gällande PUB-avtal. Förvaltningen har sedan tidigare tagit fram ett dokument som fastställer roller och ansvarsfördelning avseende dataskyddsarbetet. En av rollerna är dataskyddssamordnarna och de har behörighet till Draftit Privacy Records. De har som uppgift att kontinuerligt se över och uppdatera befintliga, lägga till nya eller radera inaktuella personuppgiftsbehandlingar. Ett behandlingsregister över personuppgiftsbehandlingar behöver även löpande ses över allteftersom förutsättningarna hos en verksamhet förändras. Att ha en korrekt och uppdaterad registerförteckning är nödvändigt. Dataskyddsombudet rekommenderar att verksamheten fortsätter att löpande inventera vilka personuppgiftsbehandlingar som utförs, då personuppgiftsbehandling är rörlig över tid på grund av exempelvis nya uppdrag och förändrade förutsättningar. Det är viktigt att behandlingsregistret kompletteras med personuppgiftsbehandlingar om/när verksamheten identifierar att en personuppgiftsbehandling inte finns i behandlingsregistret. Det underlättar och utgör underlag för det systematiska och löpande dataskyddsarbetet.

Verktyget Draftit Privacy Records erbjuder vägledning för användarna i systemet både kring hur systemet är uppbyggt och fungerar. Systemet erbjuder även juridisk vägledning utifrån GDPR. Behörigheter till verktyget Draftit Privacy Records uppdateras kontinuerligt av Dataskyddsombudet och begränsar användarnas tillgång till uppgifter utöver deras egen enhet. Dessa har uppdaterats löpande under året 2022.

3.3.1 DSO bedömning och rekommendationer

	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

Dataskyddsombudet bedömer att förvaltningen har en bra och övergripande struktur avseende registerförteckningen. Registreringarna vilka registrerats i Drafit Privacy Records år 2022 har vid majoriteten av fallen varit fullständiga där behandlingen, ändamål samt övriga nyckeluppgifter är kompletta. De brister som idag finns i förvaltningens registerförteckning behöver dock åtgärdas, dock inte skyndsamt. Främst behöver gamla registreringar fortsatt ses över samt att ändamål i förhållande till gällande laglig grund behöver förtydligas med tillhörande riskbedömningar.

Samtliga registreringar behöver även ske i Draftit och inte i annat system eller genom s.k. manuell hantering utanför systemet Draftit. Med hänsyn till den verksamhet som bedrivs av förvaltningen inom till exempelvis socialtjänst och den mängd känsliga personuppgifter vilka hanteras gör Dataskyddsombudet bedömningen att antalet angivna riskbehandlingar för år 2022 är lågt. Den sammanfattande bedömningen utgår från att registerförteckningen idag fortfarande inte är helt fullständig och är ett fortsatt utvecklingsarbete

4 Styrdokument avseende dataskydd

4.1 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?	Ja.

Är dokumenten uppdaterade?	Till stor del.
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja.

4.2 Syfte

Området syftar till att PUA bedriver ett systematiskt dataskyddsarbete och styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar PUA till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna i fråga om hantering av 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.

4.3 Resultat

På förvaltningens intranät finns en egen flik för dataskyddsfrågor dit alla medarbetare har åtkomst. På fliken finns till exempel vägledande dokument inom incidentrapportering, mallar för upprättande av PUB-avtal med vägledning och instruktion, information och blanketter för samtycke, begäran om registerutdrag, rättelse och radering samt blanketter för risk- och konsekvensbedömning. Under fliken finns även generell information om dataskyddslagstiftning, kontaktuppgifter till Dataskyddsombudet, information om hur dataskyddsorganisationen är uppbyggd, hur ansvarsfördelningen ser ut samt rollförteckning. Fliken hänvisar vidare till en webbutbildning inom dataskydd och informationssäkerhet vilken varje medarbetare uppmanas att genomföra. Dataskyddsombudet uppdaterar blanketter och information löpande och följer rekommendationer från exempelvis tillsynsmyndighet. Blanketter för incidentrapportering är uppdaterade utifrån den anmälan som görs till Integritetskyddsmyndigheten, IMY. Detta för att fånga relevant information och minska på komplettering av uppgifter mellan Dataskyddsombudet och den som upprättar en incidentanmälan.

4.3.1 DSO bedömning och rekommendationer

	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

Fortsatt arbete krävs löpande i fråga om att tydliggöra information inom förvaltningen och påminna medarbetare i det dagliga arbetet. Blanketter och rutiner finns tillgängligt men fortsatt arbete om ansvarsfördelningen och fördelning av arbetsuppgifter behöver förankras inom hela förvaltningen löpande. Fortsatt informationsspridning bör även ske ut i verksamheterna avseende intranätet och relevanta styrdokument inom området. I och med att det idag finns en tidsfrist för att anmäla allvarliga personuppgiftsincidenter till Integritetsskyddsmyndigheten bör ökad kunskap om vilka incidenter vilka ska anmälas eller inte tydliggöras. I samband med registerförteckningen har chefers och medarbetares kunskap om ett lokalt behov av anvisningar, rutiner, instruktioner och metodstöd avseende dataskydd och personlig integritet ökat då allt fler tar kontakt med Dataskyddsombudet med ifyllda dokument för granskning och med allmänna frågor. Utöver det sker god samverkan med dataskyddsombudet avseende registerförteckning och personuppgiftsincidenthantering. En fungerande incidenthantering minskar konsekvenser för verksamheter och individer, åtgärdar fel samt bidrar till att informationshanteringen ständigt förbättras genom utvärdering och lärande. Det fortsatta arbetet enligt ovanstående rekommenderas att samrådas med Dataskyddsombudet. En instruktion som särskilt bör prioriteras är hur personuppgifter får hanteras i e-post internt och externt.

5 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna vilka finns i verksamheten har informationsklassats?	Nio under år 2022.
Är klassade personuppgiftsbehandlingar aktuella?	Ja.

5.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. 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.

5.3 Resultat

Under året har informationsklassaning skett i KLASSA och har därmed aktuella klassningsprotokoll. Totalt klassades nio system under år 2022 och utöver det har delaktighet i klassningar skett i tre integrationer/e-tjänster inom sociala system. Vidare är ett antal pågående klassningar på gång. Sedan innan har 27 klassningar genomförts (år 2021). Bakgrunden till att antalet klassningar minskat något under år 2022 i förhållande till år 2021 är för att tid lagts ner på att förändra processer för att öka kvaliteten inom ramen för klassningarna samt synkronisera våra processer med det utvecklingsarbete vilket bedrivs inom staden. Handbok och stadens riktlinjer för klassningsarbetet återfinns enligt nedan.

Handbok för Informationsklassning

5.3.1 Bedömning och rekommendationer

	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

Dataskyddsombudet tillsammans med informationssäkerhetssamordnare rekommenderas stödja verksamheterna med workshops i kompetenshöjande syfte i vart fall en gång per år. Främst rör det sig om områdena informationsklassning och personuppgiftsincidenter. Informationssäkerhetsklassningar genomförs enligt stadens riktlinje för informationssäkerhet i verktyget KLASSA. Generellt behöver förmågan att informationsklassa och implementera informationsklassningen förbättras. Medarbetare behöver även utbildas gällande informationsklassning och dataskydd i större utsträckning än idag samt i en mer återkommande form.

6 Konsekvensbedömningar

6.1 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.

6.2 Syfte

Syftet med risk- och konsekvensbedömningen är att förebygga risker innan de uppkommer, ta fram rutiner och åtgärder för att hantera

eventuella risker och kunna visa att vi följer dataskyddsförordningens krav.

6.3 Resultat

Förvaltningen använder idag verktyget Draftit Privacy Records som förteckning för sina personuppgiftsbehandlingar. Året 2022 har förvaltningens Dataskyddsombudet fortsatt, genom ny licens, fått tillgång till fler funktioner i Draftit genom Draftit Expert. Det innebär bland annat att tillgång och behörigheter utökats genom möjlighet till rättsdata, dokument och andra processer inom ramen dataskyddslagstiftningen samt dataskyddsarbetet. Syftet har främst varit att hålla staden uppdaterat på dataskyddsområdet samt ha rätt verktyg för att sköta dataskyddsarbetet på ett optimalt vis. I Draftit Privacy Records finns idag sex riskregistreringar. Detta är samma antal vilka fanns registrerade även året innan vilket innebär att inga direkta förändringar har skett på området under år 2022. Sex riskregistreringar bedömer Dataskyddsombudet som ett lågt antal med tanke på de känsliga personuppgifter som behandlas inom förvaltningen. För de sex riskregistreringar som finns angivna har inte en risk- och konsekvensanalys genomförts vilka behöver åtgärdas. Vissa brister vilka har uppmärksammats är ofullständiga personuppgiftsbehandlingar, d.v.s. att de inte är fullständigt ifyllda avseende säkerhetsåtgärder, syfte och ändamål, eller ansvarig kontaktperson. Dessa har därmed klassats till högre risk på grund av att informationen inte är fullständig. En generell förbättring är att Dataskyddsombudet och informationssäkerhetssamordnare tillfrågats kring bedömning av risker och konsekvenser innan uppstart av nya personuppgiftsbehandlingar i mycket större utsträckning än året 2021.

6.3.1 Bedömning och rekommendationer

	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

Det är ett lågt antal riskregistreringar i Draftit i förhållande till den verksamhet förvaltningen bedriver. Samtidigt har funktionen Draftit Privacy DPIA börjat användas och mer fokus har riktats till risk- och

konsekvensbedömningar under hela året 2022. Det finns ett ökat intresse och kunskap inom förvaltningen vilket är en bra utgångspunkt i det fortsatta arbetet. Det är av vikt att samtliga personuppgiftsbehandlingar värderas utifrån risker innan dessa startas upp eller genomförs. I nuläget är bedömningen från Dataskyddsombudet att riskbedömningar genomförs men att ett fortsatt arbete med de registreringar som är gjorda fortlöper och att det antal riskregistreringar vilka idag finns säkerställs och överensstämmer mellan verksamhet och registerförteckning.

7 Individens rättigheter

7.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	9.
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Samtliga.

7.2 Syfte

Ett registerutdrag är en sammanställning över den registrerades personuppgifter som behandlas. Syftet med registerutdraget är att den registrerade ska få medvetenhet om att personuppgiftsbehandling sker och på vilken laglig grund. Individen har även rätt att begära begränsning av sin personuppgiftsbehandling och att invända mot personuppgiftsbehandlingen. När den personuppgiftsansvarige hanterar rättigheterna, ska informationen vara tydlig och i lättillgänglig form med användning av ett klart och tydligt språk.

7.3 Resultat

Förvaltningen har rutiner avseende registerbegäran från enskild. Samtliga inkomna begäran om registerutdrag har under året behandlats inom utsatt tid. Dataskyddsombudet hanterar administrationen kring inkomna begäran om registerutdrag. Blanketten för begäran om registerutdrag finns tillgänglig för medborgare på Stockholm.se Denna blankett om begäran om registerutdrag berör socialförvaltningens verksamhet men när den inkommit har Dataskyddsombudets utredning visat att det oftast rör sig om efterfrågan av uppgifter

från socialtjänsten inom stadsdelarna eller till och med andra kommuner. Dataskyddsombud har initialt kontaktat den enskilde för att stämma av syftet med begäran för att sedan, vid behov, vidarebefordra eller hänvisa till rätt primärkälla eller avdelning.

Fler inkomna begäran om registerutdrag vilka inkommit till förvaltningen har varit ställda till fel instans. Dataskyddsombudet har lyft detta inom stadens nätverk för Dataskyddsombud även under 2022 men frågan har inte uppmärksammats ytterligare. Detta samarbete inom staden behöver förbättras och en struktur för begäran om registerutdrag bör struktureras tydligare mellan stadsdelar och förvaltningar. Vad förvaltningen behöver göra är att förtydliga rutiner för mottagen registerbegäran, hur man först kan kontrollera om den är rätt ställd till oss, vad vi kan bistå med för information och hur den hanteras.

9 inkomna begäran om registerutdrag vilka är riktade till Socialförvaltningen har behandlats på förvaltningen genom att göra slagningar på personen enligt enskilds önskemål och enligt rutinerna vilka finns satta på förvaltningen. Samtliga frågor och enskildas begäran om rättighet som har inkommit till Socialförvaltningen har hanterats inom föreskriven lagstadgad tidsram om trettio dagar.

7.3.1 Bedömning och rekommendationer

	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

Rekommendationen är att fortsatt utöka samarbetet och dialogen inom staden kring just begäran om registerutdrag. Det kommer fortfarande in många registerutdrag som är ställda till fel aktör vilka tar administrativ tid i anspråk. Det innebär att registerförfrågningar behöver skickas av Dataskyddsombudet till rätt stadsdel eller förvaltning och vilken tidvis aldrig blir aktuell inom Socialförvaltningen. En dialog kring aktuella blanketter och tillgänglighet för medborgaren bör diskuteras och upprättas. Likaså bör samarbetet inom staden förbättras vad gäller att hänvisa den enskilde rätt. Fortsättningsvis, i

syfte att öka digitalisering och individens säkerhet, bör möjligheter att se över huruvida den enskilde kan skicka in begäran om registerutdrag per säkra meddelanden eller därmed jämförbart arbetssätt. Utöver det bedömer Dataskyddsombudet att mognadsgraden avseende den interna hanteringen av registrerades rättigheter är hög och att hanteringen efterlever gällande lagstiftning. Om klagomål från individ avseende dataskydd inkommer bör verksamheten involvera Dataskyddsombudet.

8 Personuppgiftsincidenter

8.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Enskild meddelar felaktighet, medarbetare anger felaktighet.
Hur många personuppgiftsincidenter har dokumenterats?	10 incidenter.
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	1 har rapporterats till IMY.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Samtliga.

8.2 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.” Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering. Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter.

8.3 Resultat

Rapportering till IMY har under 2022 skett i tid. Det som behöver förstärkas inom förvaltningen är förmågan att upptäcka och/eller

identifiera en personuppgiftsincident. Den andra delen som kan förstärkas är att rapporteringen till eller kontakten med Dataskyddsombudet och informationssäkerhetssamordnaren dröjer något, dock har detta förbättrats sedan året 2022. Funktionsbrevlådan för Dataskyddsombud bevakas dagligen vilket innebär att anmälda incidenter behandlas brådskande. Det finns rutiner, blanketter och vägledande dokument som stöd vid ovan nämnda hantering.

8.3.1 DSO bedömer och rekommenderar

	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
x	Inga brister av nämnvärd betydelse identifierade

Det finns idag en god kompetens inom förvaltningen avseende rapportering av personuppgiftsincidenter och en dialog med Dataskyddsombudet sker ofta, men inte alltid i tidigt skede. Konsekvensen av detta kan bli att incidenter riskerar att rapporteras för sent till IMY.

Dataskyddsombudets bedömning har visat att det idag inte alltid är helt klart i ärendets gång avseende när en personuppgiftsincident uppmärksammats, när Dataskyddsombudet kopplas in samt när en bedömning om incidentens art och allvar genomförs. Förtydliganden behöver ske avseende ansvarsfördelning mellan ansvarig chef och Dataskyddsombudet vid utredning och rapportering av personuppgiftsincidenter. Detta behöver främst ske i de fall där incidenten anmäls till tillsynsmyndighet, IMY, då finns en tidsfrist att förhålla sig till. Det är även av vikt att varje incident har en tillhörande handlingsplan för att undvika fortsatta risker inom ramen för incidenter. Ansvarig chef ska utreda och tillgodose anmälan relevant information medan Dataskyddsombudet ska tillgodose vägledning och ansvara för att själva anmälan skickas in till IMY. Dataskyddsombudet har i sin bedömning sett att det finns behov av förtydliganden hur informationsutbytet och dialogen mellan ansvarig chef, inblandad medarbetare och Dataskyddsombudet bör se ut. I den granskande rol-

len ser även Dataskyddsombudet att det till viss del finns personuppgiftsincidenter dokumenterade i systemet, men att samtliga kategorier av incidenter behöver kontrolleras för att få fram informationen. Framtagna personuppgiftsincidentrutiner måste fungera i praktiken när en personuppgiftsincident uppkommer. Det innebär att rutinerna måste testas och övas av verksamheten. Vid testning och övning bör rutinerna vid behov justeras för att främja skyddet för individ och regelefterlevnad. Med anledning av ovanstående markeras riskerna i dels gula dels gröna kolumnen.

9 Genomförda granskningar och nya forum för GDPR och informationssäkerhet

9.1 Tredjelansöverföringar

Juridiska avdelningen har reviderat och uppdaterat mallar inom ramen för tredjelandsöverföringar. För nya avtal som ingås från den 27 september 2021 ska de nya standardavtalsklausulerna användas. De nya klausulerna innehåller en avtalsmall för olika situationer beroende på parternas rollfördelning för personuppgiftsansvaret. Det är inga färdiga avtal att hänvisa till såsom de tidigare klausulerna. Viss information behöver fyllas i för att avtalet ska bli fullständigt. Det har vidare utförts ett arbete med att uppdatera mallen för standardavtalsklausul, mallar för konsekvensbedömning samt mallen för personuppgiftsbiträdesavtal. Mallarna har publicerats på Intranätet (under området/fliken GDPR).

Dataskyddsförordningen (GDPR) och personuppgiftsbehandling - Stockholms stads intranät

Juridiska avdelningen har sammanställt en särskild sida på intranätet vilken beskriver bakgrunden till tredjelandsöverföringar samt därmed tillhörande omständigheter vilka är bra att ha kännedom om i samband med tredjelandsöverföringar.

Frågor och svar om Privacy Shield och Schrems II - Stockholms stads intranät

9.2 E-utbildningar

Som medarbetare i staden förväntas du bidra till ett säkert Stockholm i ditt dagliga arbete. Därför har alla medarbetare ett eget ansvar att informera sig om vilka regler som gäller för att skydda den information som hanteras i det dagliga arbetet. I Stockholms stad är det obligatoriskt för alla medarbetare att genomföra stadens informations-

säkerhetsutbildning och den grundläggande utbildningen i dataskydd. För att kunna säkerställa ett fullgott dataskyddsarbete behöver verksamhetens medarbetare ha kunskap om hur de ska hantera personuppgifter på rätt sätt. Förvaltningen behöver därför även fortsättningsvis ge medarbetarna möjlighet att delta i både interna och externa utbildningsinsatser för att höja den allmänna kunskapsnivån om dataskydd. Rekommendationerna är vidare att samtliga medarbetare genomför E-utbildningarna inom dataskydd i vart fall en gång per år.

Grundkurs i dataskyddsförordning: Grundkurs i dataskydd (stockholm.se)

Fördjupning i dataskydd - Överföring till tredje land (stockholm.se)
Detta är en helt ny påbyggnadskurs inom dataskydd.

9.3 Forum för GDPR och informationssäkerhet

Anställda vars uppgifter handlar om att samordna och utveckla dataskyddet och informationssäkerheten i kommunen har behov av att utbyta erfarenhet, kunskap och dela med sig av andra viktiga frågor. Forum för GDPR och informationssäkerhet ska utgöra forum för kontakt- och erfarenhetsutbyte, kompetensutveckling, informationsspridning samt diskussioner om det systematiska kvalitetssäkerhetsarbetet. Forumet ger möjlighet till diskussion och fördjupning i aktuella frågor ur ett både praktiskt och akademiskt (teoretiskt) perspektiv. Forumet ska främst bestå av nyckelpersoner på avdelningen där bland annat dataskyddsombudet och informationssäkerhetssamordnaren ingår. Vid behov kan externa eller interna tjänstepersoner och andra viktiga aktörer bjudas in. Nätverksträffarna utgår ifrån en fast agenda, men deltagarna ges ett stort utrymme att diskutera fritt inom ramen för agendan. Vid vissa tillfällen ges forumet även möjlighet att utgå ifrån valda teman. Forumet för GDPR och informationssäkerhet har som vision att träffas en gång varannan månad.

Syftet med forumet är att ge en övergripande förståelse och utbyte av huruvida avdelningen bedriver ett ändamålsenligt arbete med dataskyddsförordningen och informationssäkerhet samt hur man uppfyller de krav och åtgärder som förordning samt lagstiftning stipulerar. Vidare är syftet att ge tydlighet och skapa konsensus i fråga om hur förvaltningen organiserar och bedriver dataskydds- och informationssäkerhetsarbetet.

Mål med forumet är följande:

- Det primära målet är att skydda människors fri- och rättigheter samt minimera riskerna vid sådana behandlingar av personuppgifter som innebär en hög risk med stöd av forumet.
- Skapa en dynamisk mötesplats med erfarenhets- och informationsutbyte i syfte att stärka det systematiska kvalitetsarbetet.
- Målet är att öka kunskaper om regelverk, juridisk praxis och praktisk hantering av dataskydds- och informationssäkerhetsfrågor.
- Skapa diskussioner och kontaktytor som lever över tid samt utveckla kompetensen inom förvaltningen.
- Konkreta verktyg för att förbättra och effektivisera implementering, förankring samt uppföljning av gällande styrdokument och rutiner.
- Forumet kan användas i syfte att inventera behov av kunskap inom förvaltningen samt samordna regelbunden information i dessa frågor.

9.2.1 Bedömning och rekommendationer

Förvaltningen har fortsatt arbetat med att få ett enhetligt och uppdaterat personuppgiftsregister vilket är grundförutsättning för att lyckas med dataskyddsarbetet. Parallellt har förvaltningen satt en tydlig organisation kring hur dataskyddsfrågorna ska omhändertas och slagit fast en anvisning hur förvaltningen ska arbeta med dataskydd. Detta skall göras med stöd av styrning genom riktlinjer och anvisningar samt uppföljning av status och lyfta risker.

Dataskyddsarbetet på förvaltningen behöver ske mer proaktivt för att exempelvis registerförteckningar ska vara kompletta eller förhindra att incidenter sker. Förbättringsarbetet behöver förtydligas och genomföras med en större systematik. Ett frekvent förekommande önskemål från medarbetare är utökade informationsinsatser och utbildningar till följd av regelverkets komplexitet. Dataskyddsombudet rekommenderar därför att samtliga medarbetare genomför E-utbildningar inom området, vilka tillhandahålls på intranätet, *se punkten 9.2.*

Vikten av att dataskydd ska in tidigt i processerna kan inte nog betonas och ställer även krav på att dataskydd omhändertas vid upphandling, exempelvis för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår exempelvis hur verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster. Att tillse att Dataskyddsombudet deltar i planeringsstadiet inför personuppgiftsbehandling och

ges möjlighet att granska dataskyddsstrategin i Socialförvaltningen i rollen som personuppgiftsansvarig och personuppgiftsbiträde höjer även mognadsgraden och är linje med Dataskyddsombudets lagreglerade ställning och uppgifter.

I denna årsrapport framkommer att det genomförs regelbundna uppföljningar över hur väl kommunen uppfyller de lagkrav som finns vilket resulterat i ett medvetande om vissa brister och behovet av åtgärder. Att säkerställa förvaltningens efterlevnad av GDPR är ett pågående arbete där kontinuerligt arbetet kvarstår för att efterleva lagen fullt ut. Sammanfattningsvis bör nämnden och förvaltningsledningen säkerställa att

- Informationssäkerhetssamordnare och Dataskyddsombud involveras och rådfrågas i *samtliga större frågor* vilka omfattas av skyddet av personuppgifter, i synnerhet vid process- och projektstart.
- Fortsatt arbete med risk- och konsekvensbedömningar.
- Fortsatt löpande uppföljning av registreringar i Draftit, verktyget för risk och konsekvensbedömningar.
- Dataskyddsombudet tillsammans med informationssäkerhetssamordnare rekommenderas stödja verksamheterna med workshops i kompetenshöjande syfte i vart fall en gång per år.
- Medarbetare och chefer ska genomföra E-utbildningarna i informationssäkerhet och dataskydd då dessa är *obligatoriska* och nödvändiga för att medvetenheten om hantering av personuppgifter ska vara tillräcklig.
- Dataskyddsombudet vill i samband med årets rapport synliggöra att dataskydds- och informationssäkerhetsutbildningar finns på Stockholms stads utbildningsplattform för chefer och/eller medarbetare.[1]
- Fortsatt hantering samt inventering av biträdessituation samt nyteckning av biträdesavtal inom respektive nämnd/verksamhet.
- Undersöka möjligheter för implementering av tekniska lösningar vid den enskildes begäran om registerutdrag.
- Kvalitetsgranskningar bör utföras med start år 2023 av främst registerförteckningar.
- Dataskyddsombudet kommer att granska att samtliga uppdaterade mallar används korrekt, främst avseende PUB-avtal och att tredjelandsöverföringar hanteras enligt gällande EU-vägledningar.
- En instruktion som särskilt bör prioriteras är hur personupp-

[1] https://utbildning.stockholm.se/

gifter får hanteras i e-post internt och externt.

- Dataskyddsombudet kommer under år 2023 att granska hur dataskyddsombudets råd i denna rapport hanterats.