Stockholms stad

GDPR Årsrapport

2021

Farsta stadsdelsnämnd

GDPR årsrapport
Januari 2022

Dnr: FAR 2022/8
Utgivningsdatum: 2022-01-24
Kontaktperson: Medea Sandbladh

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

Årsrapporten spänner över sex obligatoriska rapporteringsområden. Det har identifierats brister i varje rapporteringsområde under framtagandet av årsrapporten. Den största bristen rör rapporteringsområdet *registerförteckning* som visar på att både mallen för registerförteckningen behöver ses över och uppdateras samt att ett större arbete kring ifyllandet av registerförteckningen behöver genomföras omgående för att uppfylla kraven i dataskyddsförordningen. Registerförteckningen utgör en grund för att dataskyddsarbetet i övrigt ska kunna genomföras.

Vidare har det identifierats att väldigt få informationsklassningar har genomförts. Informationsklassningar behöver genomföras omgående för att säkerställa att rätt tekniska- och organisatoriska säkerhetsåtgärder finns på plats. Detta är framför allt viktigt i personuppgiftsbehandlingarna där känsliga personuppgifter behandlas. Vid genomförandet av informationsklassningar kommer det bli tydligt vilka åtgärder som krävs för att uppfylla kraven kring informationssäkerhet och dataskydd.

I arbetet med att genomföra granskning och ta fram årsrapporten har förvaltningen tagit hjälp av leverantören Knowit Insight. Stadsdelsförvaltning har kompletterat underlaget samt gjort bedömningarna om bristernas allvar och behov av åtgärder i dialog med leverantören.

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 slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter genomförd uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	369
Har nödvändiga uppdateringar gjorts?	Nej
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Delvis

3.1.2 Syfte

För att något ska gå att skydda måste det först vara synligt för verksamheten. Det följer därför i klartext av dataskyddsförordningen (artikel 30) att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas i verksamheten, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde, och dokumentera dem i en så kallad registerförteckning (även kallat behandlingsregister).

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 PUA 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 PUA 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 PUA behöver förstå och ta ställning till inför det planerade åtgärdsarbetet under nästa verksamhetsår.

3.1.3 Resultat

Kontroller av hur många behandlingar som registrerats

Det finns totalt 364 registrerade behandlingar i registerförteckningen. I samband med registrering av en behandling får man även besvara frågan ”Är du klar med registerbeskrivningen?”. Av de registrerade behandlingarna är 107 registrerade behandlingar markerade som klara, 13 stycken har skrivit att de inte är färdiga och återkommer. I övriga 240 behandlingar har frågan lämnats obesvarad. Av registerförteckningen framgår inte vad som saknas för att de olika registreringarna ska bli godkända eller anledningen till att de inte godkänts under året.

Kontroller av om nödvändiga uppdateringar gjorts

Registerförteckningen har formellt uppdaterats under verksamhetsåret för att förtydliga och förenkla frågorna. Innehållsmässigt har uppdateringar inte skett i den utsträckning som varit nödvändig. Majoriteten av de registrerade behandlingarna är fortfarande inte fullständigt registrerade i registerförteckningen.

Bedömning av hur fullständig registerförteckningen är

En stickprovskontroll har gjorts bland de registreringar som är markerade som klara. I stickprovskontrollerna har en kvalitetsbedömning avseende huruvida obligatoriska fält fyllts i gjorts, korrekt laglig grund och att informationen som anges i registreringarna i övrigt är korrekt kontrollerats.

Det har gjorts totalt 15 stycken slumpmässiga stickprovskontroller. De obligatoriska frågorna är besvarade i samtliga. Den rättsliga grunden är korrekt i majoriteten av behandlingarna men det finns

anledning att se över registreringarna och gå igenom dessa tillsammans med DSO för att säkerställa att laglig grund är rätt i samtliga registreringar. I övrigt bör informationen, utifrån det DSO har berättat, i registreringarna vara korrekt.

De behandlingar som finns beskrivna i registerförteckningen saknar däremot till stor del information, i de behandlingar som är klara är framförallt de obligatoriska frågorna besvarade däremot inte övriga frågor. Den information som finns är många gånger också bristfälligt beskriven, oaktat om frågan är obligatorisk eller inte. Detta gäller särskilt frågan om ändamål. Frågan besvaras ibland väldigt kort till exempel anges ”avtal”, ”lätt tillgängligt” och ”administration” som ändamål vilket inte beskriver ändamålet med personuppgiftsbehandlingen tillräckligt.

Med beaktande av den kännedom som finns om verksamheten, bör också fler behandlingar finnas registrerade i registerförteckningen.

Bedömning av om verksamheten har lämpliga rutiner för registerföring

Tydliga och lämpliga rutiner på plats är nödvändigt för att registreringen av behandlingar ska ske strukturerat och att informationen i de registrerade behandlingarna är komplett och korrekt.

Det finns ett utbildningsmaterial, *Dataskyddsförordningen och registerförteckning* för hur registerförteckningen ska fyllas i och vad den bör innehålla för att uppfylla kraven i dataskyddsförordningen. Utbildningsmaterialet bör kompletteras med en rutin som innehåller information om vad som ska anges i varje kolumn för att säkerställa att all information registreras samt att arbetssättet med registerförteckningen blir enhetligt. Detta för att säkerställa att registerförteckningen uppfyller samtliga krav i artikel 30.

Utöver utbildningsmaterialet för registerförteckningen finns en vägledning *GDPR för dig som chef* som redogör för chefernas ansvar enligt dataskyddsförordningen. Cheferna ska, enligt den, säkerställa att de personuppgiftsbehandlingar som görs ska registreras i systemverktyget Draftit och att alla obligatoriska frågor ska besvaras för varje behandling. Utöver det ska cheferna ansvara för att registerförteckningen hålls uppdaterad och att alla nya personuppgiftbehandlingar registreras samt att registerförteckningen minst en gång om året kontrolleras för att säkerställa att den är

komplett och korrekt. Det finns även en lathund för hur systemet Draftit ska användas vid en registrering.

3.1.4 Uppskattning av hur allvarliga bristerna är på en skala

X	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
	Inga brister av nämnvärd betydelse identifierade

De identifierade bristerna är omfattande och kräver omgående åtgärder. Grunden för fastställandet är både registerförteckningens kvalité och omfattning men även en bedömning av de obligatoriska frågorna i registerförteckningen.

PUA behöver ha kontroll över vilka behandlingar som utförs i verksamheterna, särskilt vilka behandlingar som omfattar känsliga personuppgifter, för att kunna vidta rätt skyddsåtgärder och i övrigt leva upp till kraven i dataskyddsförordningen.

3.1.5 Råd och rekommendationer till PUA

Frågorna i registerförteckningen är många till antalet och tar lång tid att besvara. Arbetet med registerförteckning kan därför uppfattas som övermäktigt för medarbetarna som väljer att prioritera sina andra arbetsuppgifter. DSO kommer därför att se över samtliga frågor i registerförteckningen dels för att minska antalet frågor för att underlätta för medarbetarna att besvara frågorna, dels för att se till att de obligatoriska frågorna motsvarar minimikraven i artikel 30.

Eftersom registerförteckningen är en grundförutsättning för allt annat dataskyddsarbete är rekommendationen att arbetet med registerförteckningen prioriteras högst.

En årlig uppmaning från PUA bör gå ut till samtliga medarbetare för att uppmana samtliga medarbetare till att uppdatera registerförteckningen och hålla den uppdaterad med eventuella nya

personuppgiftsbehandlingar som tillkommit under det gångna verksamhetsåret. PUA bör säkerställa att särskilda personer har utsetts för att ha ett huvudsakligt ansvar för registerförteckningen, så att det finns en tydlig kontaktperson för medarbetarna avseende registerförteckningen. Den årliga uppmaningen bör även uppmuntra till att repetera den obligatoriska grundkursen i dataskydd.

De underlag som finns kring registerförteckningen kan med fördel samlas i ett dokument eller ett utbildningsmaterial för att minimera risken kring vad medarbetarna väljer att läsa eller var de kan söka svar på sina frågor. En tydlig rutin bör underlätta arbetet med registerförteckningen.

Dessa åtgärder kommer att förbättra kvalitén på registerförteckningen avsevärt och motivera medarbetarna till att fullfölja registreringarna av samtliga personuppgiftsbehandlingar.

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?	Delvis
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Delvis
Är dokumenten uppdaterade?	Delvis
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja

3.2.2 Syfte

Området syftar till att PUA genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den 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, 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 det bedömas om verksamheten har de styrdokument antagna och på plats, dels ska rapporteringen visa om dokumentationen innehållsmässigt håller en lämplig kvalitet, i vilket ingår bland annat att dokumentationen ska vara uppdaterad och aktuell.

Bristande styrning på grund av att lämplig styrande dokumentation saknas leder exempelvis ofta till *bristande kvalitet* i hur verksamheten utför aktiviteterna, men även till att verksamheten *slösar värdefulla resurser* när exempelvis för många personer blir involverade i en incidenthantering eller för att en analys behöver göras om från grunden varje gång istället för att man återanvänder redan uppfunnen kunskap. Dessa effekter drabbar verksamheter ur ett vidare perspektiv och är något som ligger i PUA:s intresse att förstå för att fatta rätt beslut om.

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?

Det finns en del dokument på plats:

- Handboken för personuppgiftsbehandling innefattar information om hur verksamheten hanterar information till den registrerade samt information om den registrerades rättigheter,
- Integritetspolicy Farsta Stadsdelsnämnd,
- Hantering av anställdas personuppgifter,
- Mall för hur redovisning av personuppgiftsbehandling ska utformas (Registerutdrag),
- Handbok för informationsklassning,
- Rutin för hantering av personuppgiftsincidenter,
- Vägledning för personuppgiftsincidenter,
- Checklista och mall för konsekvensbedömning

- Stockholms stads policy används för instruktioner om publicering på sociala medier, samt
- Arkiv och gallring i förhållande till GDPR.
- Mall för personuppgiftsbiträdesavtal (PuB-avtal) (Stadens)
- Instruktion till personuppgiftsbiträdesavtalet (Stadens)
- Checklista för inbyggt dataskydd samt dataskydd som standard (Stadens)

Det saknas tillräckliga rutiner för hur verksamheten arbetar med:

- Personuppgiftsbiträdesavtal (PuB-avtal). Eftersom verksamheten är personuppgiftsansvarig för de behandlingar som utförs är det viktigt att det finns en rutin för och kunskap om när det behövs PuB-avtal med parter som bidrar i behandlingen. Det finns ett standardiserat PuB-avtal och instruktioner för avtalet, men det saknas rutin för hur man går till väga och när det ska användas.

Punktlistan ska inte ses som uttömmande.

Bedömning av om innehållet i existerande dokument håller lämplig kvalitet

Dokumentation som finns på plats bedöms vara lättillgänglig för verksamheten genom att all dokumentation finns samlad på samma plats på intranätet (se dokumentbiblioteket – GDPR och personuppgiftsbehandling). Dokumentationen är tydligt strukturerad genom uppdelningen i underrubriker. Genom att dokumentationen är samlad på samma plats blir det enkelt för medarbetarna att veta var de ska leta efter rätt information. Vissa dokument behöver uppdateras då de fortfarande hänvisar till Datainspektionen.

Information till den registrerade samt om dennes rättigheter
I handboken för personuppgiftsbehandling redogörs för den registrerades rättigheter. Information i handboken är utförligt och tydligt förklarad vilket gör det enkelt för användaren att ta till sig informationen. Informationen är dock generellt formulerad och kan tjäna på att konkretiseras med exempel från verksamheterna.

Avseende den registrerades rättigheter finns även en integritetspolicy, vilken riktas till stadsdelsförvaltningens invånare. I policyn ges en kortfattad bakgrund till dataskyddsförordningen, där bland annat information om vad som utgör en personuppgift innefattas. Det ges dessutom en generell beskrivning över hur verksamheten behandlar personuppgifter, där det bland annat

beskrivs att verksamheten behandlar personuppgifter för ändamålet att utföra myndighetsutövning. Integritetspolicyn uppfyller inte kraven i artikel 13 avseende information om rättslig grund, information om mottagare av personuppgifterna och information om överföringar till tredjeland. Eftersom integritetspolicyn riktar sig till stadsdelsförvaltningens invånare bör den även uppfylla kraven i artikel 14. PUA måste tillhandahålla särskild information om personuppgifterna inte har erhållits från den registrerade själv, detta görs bäst i en integritetspolicy som finns publicerad på hemsidan för samtliga att nå. Integritetspolicyn uppfyller i dagsläget inte kraven i artikel 14 och bör därför ses över och kompletteras med information.

Det finns även en information om hantering av anställdas personuppgifter. Detta dokument är strukturerat på samma sätt som ovan nämnda integritetspolicy, detta gör att ovan nämnda brister även återfinns i aktuellt dokument. Informationen om hantering av anställdas personuppgifter uppfyller inte kraven i artikel 13 avseende information om rättslig grund, information om mottagare av personuppgifterna och information om överföringar till tredjeland, och bör därför uppdateras.

Informationsklassning
Det finns en väldigt omfattande handbok för informationsklassning på 28 sidor som föredömligt beskriver hur informationsklassning ska genomföras steg för steg. Handboken anses heltäckande och är enkel för användaren att följa. Utöver handboken finns även två olika mallar för “Informations-klassningsprotokoll” som stöd i arbetet och är tydliga i vad och hur man ska göra. Dessa dokument anses vara fullt tillräckliga för användare att följa för att kunna fullgöra informationsklassningar.

Personuppgiftsincident
Det finns en rutin för hantering av personuppgiftsincident samt en blankett för anmälan av personuppgiftsincident. Rutinen för hantering av personuppgiftsincident saknar instruktioner för hur incidenter ska bedömas, analyseras och utredas. Detta uppfylls till viss del av stadens vägledning vid händelse av personuppgiftsincident, där förutsättningarna för personuppgiftsincident beskrivs mer utförligt. Detta dokument är dock generellt formulerad för alla verksamheter i staden. Det hade gynnat verksamheten att ge några exempel och på ett tydligare och mer konkret sätt förklara vad som utgör en incident och hur medarbetarna ska gå till väga vid en incident, genom exempelvis en checklista.

Konsekvensbedömning
Det finns en mall för konsekvensbedömning och en checklista för konsekvensbedömning. Mallen för konsekvensbedömning kommer från Stockholms stad och fungerar som en stödmall i processen för konsekvensbedömningar. Farsta stadsdelsnämnds checklista för konsekvensbedömningar tar snarare sikte på att fungera som ett stöd för organisationen vid bedömningen om en konsekvensbedömning behöver genomföras. Checklistan är tydligt strukturerad och formulerad med exempel på varje bedömningsdel. I checklistan stadgas att rutinen för konsekvensbedömningen är att den ska dokumenteras och att DSO ska kontaktas.

Gallring och GDPR
Det finns ett kort dokument; Arkiv och gallring i förhållande till GDPR som redogör för principen i dataskyddsförordningen om att personuppgifter inte ska sparas längre än nödvändigt. Dokumentet tydliggör vidare att radering (gallring) enbart får ske enligt gallringsbeslut fattade av Stadsarkivet. Detta dokument bör ses över för att det ska bli tydligt för medarbetarna när gallring ska ske och vilka gallringsrutiner som finns, detta kommer också vara till hjälp för att kunna besvara frågan om gallring i registerförteckningen. Svaren kring gallring i registerförteckningen är bristfälliga.

3.2.4 Uppskattning av 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

Flertalet av de styrdokument som finns på plats är för allmänt formulerade och ger inte tillräcklig vägledning för organisationens användare. De flesta dokumenten, däribland integritetspolicyn och rutinen för personuppgiftsincidenter, bör förtydligas med exempel från verksamheten och instruktioner bör beskrivas mer utförligt.

Utan tydlig dokumentation och rutiner kan det leda till att medarbetarna inte vet hur de ska gå tillväga för att uppfylla kraven som ställs i dataskyddsförordningen. Ett annat exempel är rutinen för hantering av de registrerades rättigheter. Om det inte på ett tydligt sätt i rutinen beskrivs vad den registrerade har rätt till eller om det saknas en rutin för vem den registrerade ska kontakta för att tillvarata sina rättigheter kan det leda till att organisationen inte uppfyller kraven i dataskyddsförordningen.

Verksamheten ska i första hand hänvisa till Stockholm stads integritetspolicy, men det finns en specifik integritetspolicy för personuppgiftsbehandling i Farsta stadsdelsnämnd. Denna finns dock för tillfället inte öppet tillgänglig för de registrerade vilket är problematiskt då själva syftet med informationen är att informera de registrerade om deras rättigheter. Tidigare fanns Farstas integritetspolicy tillgänglig under stadsdelsområdets dokument på stadens hemsida, men togs bort när Stockholm ändrade domän. På stadens nya hemsida listas de områden som stadsdelsförvaltningen ansvarar över, men dessa överensstämmer inte med de områden som listas i integritetspolicyn. Problemet med att hänvisa till stadens policy är därmed att den inte är anpassad efter stadsdelsförvaltningens olika verksamhetsområden och är heller inte komplett utformad. Det leder dessutom till att det är svårt för den registrerade att få en helhetsbild över verksamhetens behandlingar.

Utöver avsaknaden på publicering är det en brist att det inte tydligt framgår ur integritetspolicyn hur personuppgifterna behandlas. Ett exempel på detta är om lagring av uppgifter där det framkommer av policyn att uppgifter inte lagras längre än vad som är nödvändigt för ändamålet. Då ändamålet för behandlingen beskrivs vara myndighetsutövning är det svårt för den registrerade att skapa sig en uppfattning om hur länge uppgifterna i praktiken lagras.

3.2.5 Råd och rekommendationer till PUA

Först och främst bör den dokumentation som finns i dokumentbiblioteket uppdateras för att uppnå en högre kvalité. Ett exempel på något som skulle kunna förbättras är handboken för personuppgiftsbehandling där det skulle vara bra att lägga till konkreta exempel för att öka förståelsen för hur den registrerades rättigheter ska tillgodoses i praktiken. Formuleringarna som finns med i handboken är för allmänt formulerade och knyter inte på ett tydligt sätt an till verksamheten i sig. Detsamma gäller för integritetspolicyn där det inte på ett tydligt och klart sätt framgår

vilka typer av personuppgifter som faktiskt behandlas, för vilka ändamål och under vilken tid. Avseende integritetspolicyn rekommenderas även att denne publiceras och görs tillgänglig för de registrerade då verksamheten är personuppgiftsansvariga för behandlingarna som utförs.

Dokumenten bör ses över och om möjligt slås ihop för att minimera risken för fel i arbetet med konsekvensbedömningar. Det ska vara tydligt vilket syfte varje dokument har och var medarbetaren kan hitta hjälp. För vissa dokument stämmer inte dokumentnamnet med huvudrubriken i dokumentet, till exempel ”Information om personuppgiftsbehandling till anställda i Farsta stadsdelsnämnd” där huvudrubriken i dokumentet är ”Information om hantering av anställdas personuppgifter”. Detta bör prioriteras först efter att samtliga dokument har gåtts igenom och det har säkerställts att all dokumentation uppfyller kraven i dataskyddsförordningen. PUA bör även ta fram egna rutiner och/eller styrdokument i de fall detta inte finns till exempel en policy för sociala medier.

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?	6
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 PUA ges en uppdaterad bild varje år av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar.

3.3.3 Resultat

Informationsklassning sker efter protokoll framtaget av SLK. Denna har börjat användas under hösten 2021. Dokumentet ger en första bedömning och stöd innan den större aktiviteten med verktyget KLASSA.

Det finns 6 stycken *system* klassade. Dock ska man beakta att samtliga personuppgiftsbehandlingar klassas utifrån vilken typ av personuppgifter som behandlas och lämpligt skydd vidtas för respektive behandling. Detta kan vara behörighetsbegränsning, skydd av lösenord på dokument osv. Detta ska dokumenteras i Draftit, men är i majoriteten av de registrerade behandlingarna inte ifylld

En handlingsplan finns framtagen för organisationens arbete med både informationssäkerhet och dataskydd samt en inventeringsplan.

I Draftit har uppgifter om genomförd informationsklassning inte rapporterats för någon behandling i registerförteckningen. Det finns en personuppgiftsbehandling som är registrerad i registerförteckningen som är informationsklassad, enligt KLASSA, av extern part som tillhandahåller tjänsten. Kolumnen för tekniska och organisatoriska åtgärder är i majoriteten av de registrerade behandlingarna inte ifylld, vilket också beror på att frågorna om tekniska- och organisatoriska säkerhetsåtgärder inte är obligatoriska. DSO kommer att uppdatera registerförteckningen så att frågorna om säkerhetsåtgärder är obligatoriska, då de utgör ett krav i registerförteckningen enligt artikel 30.

3.3.4 Uppskattning av hur allvarliga bristerna är på en skala

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

Bedömningen är att bristerna som identifieras kräver åtgärder, vilket beror på att väldigt få informationsklassningar har genomförts. Informationsklassningar behöver genomföras för att säkerställa att rätt tekniska- och organisatoriska säkerhetsåtgärder finns på plats. Detta är framför allt av vikt i de personuppgiftsbehandlingar där känsliga personuppgifter behandlas.

3.3.5 Råd och rekommendationer till PUA

Till att börja med behöver organisationen för informationssäkerhet förtydligas då uppfattningen idag är oklar om vem som ansvarar för att driva arbetet med informationssäkerhet framåt. I Stockholms stads “Riktlinjer informationssäkerhet” finns stöd i hur förvaltningarna bör organisera sig. Det har tidigare saknats organisatoriska resurser att bedriva ett effektivt arbete med informationssäkerhet i förvaltningen. Under året har

kompetensresurser tillsatts för att ha bättre möjlighet att stötta informationsägarna i deras arbete med informationsklassningar samt att få in all information som är nödvändig i registerförteckningen.

Informationsägare är formellt sett utsedda (förvaltningens chefer) det är oklart (se granskning nedan) om dessa har kännedom om vilket ansvar detta innebär och vad de förväntas göra så det bör förankras omgående. Detta kan även vara en anledning till att så få informationsklassningar har genomförts.
Det är även otydligt vilka förväntningar som Stockholm Stad har gällande hastigheten på arbetet med informationsklassningarna och när man förväntas vara klar med arbetet.

Man bör uppdatera registerförteckningen med informationsklassning så att det på ett enklare sätt är möjligt att avgöra hur många behandlingar som har klassats.

Arbetet med att informationsklassa IT-systemen fortsätter för 2022 och idag är planen att genomföra klassning av ytterligare tio IT-system. Denna plan bör förankras med Stockholm Stad för att säkerställa ett godkännande om att samtliga informationsklassningar försenas och är färdigställda till utgången av 2023.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Nej
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Nej
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 dataskyddsförordningen. och ska utföras för alla behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1).

3.4.3 Resultat

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

Verksamheten har inte identifierat alla behandlingar som det borde upprättas konsekvensbedömningar av. Verksamheten har endast rapporterat fyra genomförda konsekvensbedömningar, varav en utförts av Konsumentverket. De bedömningar som gjorts, utöver Konsumentverkets, har varit av smarta lås i hemtjänsten,

familjestödet samt en påbörjad om anställdas användning av tjänstebil. Det är endast konsekvensbedömningen om smarta lås i hemtjänsten som gjorts tillgänglig inför framtagandet av denna årsrapport.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Genom att utföra ett stickprov ur registerförteckningen kan det konstateras att det inte gjorts konsekvensbedömningar av alla behandlingar där det finns ett behov att göra en sådan. Mot bakgrund av att det är flera behandlingar som innefattar känsliga personuppgifter, uppgifter om barn, äldre, funktionsnedsatta och andra personer som befinner sig i underläge eller beroendeställning samt personuppgifter i stor omfattning bör fler konsekvensbedömningar gjorts. För att exemplifiera behandlingar som saknar konsekvensbedömning men där det finns ett behov för en sådan är:

1) Behandling ”Personakt barn” och ”Personakt ungdom” om handläggning av biståndsbehov och myndighetsutövning av barn och ungdomar.
2) Behandling ”Klientadministrativa dokument” om dokument i enskilda ärenden som beslut, beslutsunderlag mm.
3) Behandling ”Dokumentation av barn i behov av särskilt stöd” om dokumentation och beslut som rör stöd till barn i behov av särskilt stöd.

På grund av att registerförteckning i flera delar är bristfälligt ifylld går det visserligen att konstatera att det saknas konsekvensbedömningar, men det är inte möjligt att besvara i vilken omfattning.

Är de genomförda konsekvensbedömningarna aktuella?

Den konsekvensbedömning som finns tillgänglig avser säkra lås i hemtjänsten. Konsekvensbedömningen har tagits fram i juni 2019 och det finns inte någon information om behandlingen förändrats sedan upprättandet av bedömningen. Avseende de övriga två konsekvensbedömningarna är det inte möjligt att bedöma aktualiteten då de inte gjorts tillgängliga.

3.4.4 Uppskattning av hur allvarliga bristerna är på en skala

X	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
	Inga brister av nämnvärd betydelse identifierade

Då verksamheten behandlar en stor mängd personuppgifter, däribland känsliga personuppgifter, är det viktigt att den har utrett de potentiella riskerna som finns med behandlingen ur ett integritetsperspektiv. Detta görs bland annat genom en konsekvensbedömning.

Av det som framgår av underlagen inför denna granskning saknas det konsekvensbedömningar på majoriteten av de behandlingar som utförs i verksamheten, inklusive högriskbehandlingar.

3.4.5 Råd och rekommendationer till PUA

Respektive avdelning rekommenderas att omedelbart initiera arbete med att ta fram de konsekvensbedömningar som saknas. I denna rapport ges endast exempel på behandlingar som behöver konsekvensbedömningar, men det finns sannolikt fler behandlingar där konsekvensbedömningar behöver genomföras. Det är viktigt att komma ihåg att kravet på konsekvensbedömning inte endast gäller för nya behandlingar, utan även gäller för behandlingar som verksamheten genomfört innan dataskyddsförordningen trädde ikraft.

För att underlätta arbetet med konsekvensbedömningar har Farsta stadsdelsförvaltning till 2022 kompletterat Draftit med verktyget DPIA, där konsekvensbedömningar kan göras direkt i systemet och kopplas till registerförteckningen.

3.5 Individens rättigheter

3.5.1 Sammanfattning

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

3.5.2 Syfte

Registrerade personer har enligt dataskyddsförordningen (artikel 12–22) ett antal rättigheter som på olika sätt ska garantera 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 verksamhet som enligt förordningen är att se som personuppgiftsansvarig – dvs. i stadens fall nämnder och bolag – 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 verksamheter 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 dock att det finns undantagssituationer angivna i artikel 12.3, där fristen kan förlängas till mer än en månad.)

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 Intetgritetsskyddsmyndighetens (”IMY”) sida, med sanktioner som följd. Det är därför viktigt att PUA 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?

Den registrerade har ett antal rättigheter enligt dataskyddsförordningen. Några av dem är rätten till information, rätten att bli glömd och rätten att få felaktiga uppgifter korrigerade. I rätten till information innefattas flera olika delar, så som rätt att ta del av information om personuppgiftsbehandling och rätt till registerutdrag.

Den interna processen är uppbyggd så att en begäran om registerutdrag går till DSO, som sedan vidarebefordrar frågan till utsedda funktioner med behörighet att genomsöka systemen. Invånare informeras i första hand om att de kan kontakta DSO för detta, men den registrerade ska dock kunna kontakta vem som helst i organisationen med en begäran och ansvariga chefen ska se till så att begäran hanteras korrekt. Det ställer höga krav på medarbetare och chefers kunskap om den registrerades rättigheter. För att säkerställa medarbetarnas kunskap krävs utbildningar och tydliga styrdokument och rutiner.

I handboken för personuppgiftsbehandlingen beskrivs alla rättigheter på ett utförligt sätt vilket är positivt. Det ges dock inga konkreta exempel och beskrivs heller inte hur hanteringen av begäran ska gå till. I dokumentet ”GDPR för dig som chef” beskrivs rutinen för registerutdrag, men de övriga rättigheterna nämns inte. Detta avspeglas även i de svar från de intervjuer med chefer som DSO utförde under året där det framhävdes att den registrerades rättigheter garanterades genom rätten till information.

Den här typen av process ökar risken för att hanteringen sker på ett felaktigt sätt eller att begäran inte hanteras överhuvudtaget. Det ökar även riskerna för att hanteringen inte dokumenteras på ett korrekt sätt, vilket kan vara orsaken till att inga begäran registrerats under året.

En förutsättning för att den registrerade ska inkomma med begäran är att den har information om dennes rättigheter och hur verksamheten behandlar den registrerades personuppgifter. Genom att inte erbjuda tillräcklig information till den registrerade garanteras därmed inte heller dennes rättigheter. Avsaknaden av en separat integritetspolicy för verksamheten utgör en av bristerna,

men det kan även röra sig om övrig kommunikation med de registrerade.

3.5.4 Uppskattning av 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

Otydligheter i rutin för hanteringen av begäran från registrerade är en risk som kan leda till att de registrerade i praktiken inte har möjlighet att utnyttja sina rättigheter

3.5.5 Råd och rekommendationer till PUA

Verksamheten bör ta fram en tydligare rutin för hur hanteringen av begäran från registrerade ska gå till. Denna rutin skulle förslagsvis kunna bygga på att alla begäran inkommer till en funktions- eller gruppmail. Utöver detta bör medarbetarna fortsätta vidareutbildas inom dataskyddsförordningen och de registrerades rättigheter för att öka förståelsen om verksamhetens skyldigheter gentemot de registrerade.

Verksamheten bör dessutom tillgängliggöra integritetspolicyn där den registrerades rättigheter på ett tydligt sätt bör beskrivas samt rutinen för hur den registrerade kan tillvarata sina rättigheter.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Vanligtvis genom information från anställd, utomstående eller registrerad.
Hur många personuppgiftsincidenter har dokumenterats?	Fem stycken*
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Fyra stycken incidenter har rapporterats till IMY och i samtliga fall har man informerat de berörda
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Tre stycken

**under verksamhetsåret 2021.*

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 sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering. Stadens mall för 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, 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. 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 tillsynsmyndigheten att kontrollera efterlevnaden och bristande dokumentering är sanktionsgrundande.

3.6.3 Resultat

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

Verksamheten förmår att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten. Majoriteten av personuppgiftsincidenterna har dessutom hanterats i tid. En incident anmäldes sent på grund av bristande kunskap kring vad en personuppgiftsincident faktiskt är.

Ett stort ansvar läggs på cheferna gällande personuppgiftsincidenter. I ”GDPR för dig som chef” anges att den som är chef för den verksamhet där en personuppgiftsincident har inträffat ska utreda och dokumentera incidenten. Chefen uppmanas att följa förvaltningens rutin för hantering av personuppgiftsincidenter.

Huruvida en incident därför upptäckts och anmäls i tid beror också på chefernas agerande.

3.6.4 Uppskattning av 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

Det finns alltid en risk att PUA inte upptäcker alla personuppgiftsincidenter som inträffar i verksamheten. Kunskap om vad och hur man hanterar personuppgiftsincidenter är en färskvara. Det finns till exempel en tydlig korrelation mellan att personalen haft utbildning i dataskyddsförordningen och en ökad benägenhet att anmäla personuppgiftsincidenter. Under året har en incident som inträffat har inte rapporterats i tid på grund av att verksamheten inte direkt uppfattade att det var en personuppgiftsincident. Det är också av vikt att rutiner är tydliga och väl kända och rutinen för hantering av personuppgiftsincidenter behöver utvecklas.

3.6.5 Råd och rekommendationer till PUA

Det fortsatta arbetet bör främst fokusera på att utbilda samtliga medarbetare om vad som utgör en personuppgiftsincident för att dessa ska ha möjlighet att identifiera eventuella personuppgiftsincidenter. Den obligatoriska utbildningen ”Grundkurs i dataskydd (obligatorisk för alla medarbetare)” rekommenderas att skickas ut till samtliga medarbetare på nytt. Avsnittet gällande personuppgiftsincidenter bör särskilt lyftas. Det är positivt att utbildningen avslutas med ett kunskapstest. Medarbetare som har gått utbildningen har upptäckt incidenter i större utsträckning än de som inte gjort det.

Eftersom ett stort ansvar läggs på cheferna bör dessa årligen få möjlighet att delta i en workshop kring personuppgiftsincidenter för

att lära sig vilka personuppgiftsincidenter som är vanligast i verksamheten och hur dessa hanterats samt vad som förväntas av dem i de fallen. Eftersom cheferna i sin vägledning hänvisas till rutinen för hantering av personuppgiftsincidenter är det viktigt att den ses över och förtydligas för att möjliggöra för cheferna att hantera dessa enligt förväntade krav.

I IA-systemet rapporteras alla incidenter som sker i verksamheten, som till exempel att någon skadar sig fysiskt. Det rekommenderas därför att man ser över hur man i systemet kan tydliggöra när en personuppgiftsincident ska rapporteras. Vidare rekommenderas att löpande kontrollera huruvida övriga rapporterade incidenter också utgör en personuppgiftsincident.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Granskning av registerförteckningen
- Uppföljning av de som gått utbildning i dataskydd
- Intervjuer med enhetschefer om utmaningar för att kunna besvara registerförteckningen

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 PUA 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 av registerförteckningen

Under året har DSO granskat registreringarna i registerförteckningen. DSO har gått igenom registreringar och begärt in kompletteringar. Eftersom registerförteckningen i slutet på

verksamhetsåret fortfarande är bristfällig är det dock svårt att se hur den utförda granskningen givit något märkbart resultat.

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

Uppföljning av de som gått utbildning om dataskydd

Under året har DSO granskat hur många som gått den obligatoriska utbildningen om dataskydd. Granskningen har inte lett till önskat resultat eftersom det under granskningen framkommit att data över hur många som gått den obligatoriska utbildningen försvunnit till följd av ändringar i utbildningen. När ändringar i utbildningen genomförts har antalet som genomfört utbildningen nollställts. Den kontinuerliga personalomsättningen påverkar också andel medarbetare som genomfört utbildningen.

	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

Intervjuer med chefer om utmaningar för att kunna besvara registerförteckningen

Under året har DSO intervjuat ett antal enhetschefer för att utreda vilka utmaningar som finns för att de ska kunna besvara registerförteckningen. Av intervjurapporten framkommer att cheferna har allvarliga kunskapsbrister om både dataskyddsförordningen och systemet för registerförteckning,

Draftit. Samtliga av de intervjuade svarar att de inte vet om registerförteckningen är fullständigt ifylld, trots att det är samma personer som ansvarar för registerförteckningen. Utöver detta har de intervjuade bristfällig kunskap om laglig grund, tredjelandsöverföringar, behovet av personuppgiftsbiträdesavtal samt de registrerades rättigheter.

X	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
	Inga brister av nämnvärd betydelse identifierade

4.4 Råd och rekommendationer till PUA

Mot bakgrund av bristerna i registerförteckningen bör en mer utförlig granskning utföras under kommande verksamhetsår, där det säkerställs att samtliga enheter fyller i förteckningen.

Då enhetscheferna är ansvariga för ifyllandet av registerförteckningen, och det både mot bakgrund av förteckningens brister samt chefernas kunskapsbrister, bör vidare utbildning vidtas för att garantera att cheferna vet vad som förväntas av dem.

Den obligatoriska utbildningen bör skickas ut till samtliga medarbetare, oaktat om medarbetare gått den tidigare, detta för att i första hand repetera utbildningen och säkerställa att den når fler än vad man har kännedom om idag.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- Ofullständig registerförteckning
- Bristfälliga interna rutiner
- Avsaknad av informationsklassning

5.2 Syfte

Verksamheten har ansvar för att göra vissa typer av riskanalyser, så som konsekvensbedömningar och informationsklassningar, men dessa ger inte en heltäckande bild av personuppgiftsriskerna i verksamheten. Dataskyddsombudet behöver som underlag för sin egen planering och sitt löpande arbete ha kontinuerlig överblick över dessa risker, i 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 - Ofullständig registerförteckning

För att verksamheten ska kunna garantera de registrerades rättigheter och se till så att dataskyddsarbetet sker på ett riktigt och rätt sätt är det viktigt att verksamhetens registerförteckning är korrekt ifylld. Utan en fullständig registerförteckning är det inte möjligt för verksamheten att hålla koll på de olika behandlingar som görs. Registerförteckningen utgör dessutom grunden för den interna kontrollen och speglar verksamhetens kunskap om sina behandlingar. En bristfällig registerförteckning tyder därmed på att verksamheten inte har koll på de behandlingar som utförs, vilket i sin tur leder till risker som avsaknad av konsekvensbedömningar och personuppgiftsbiträdesavtal avseende de behandlingar som kräver det.

Det är svårt att besvara hur allvarliga konsekvenser som skulle kunna uppstå om den aktuella risken skulle realiseras, men då flera andra risker är nära anknutna till den aktuella risken bör det kunna antas att konsekvenserna kan bli allvarliga. De identifierade

bristerna bör därför anses som omfattande och kräver omedelbara insatser.

X	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
	Inga brister av nämnvärd betydelse identifierade

Risk 2 – Bristfälliga interna rutiner

Tydliga interna rutiner är grunden för ett effektivt dataskyddsarbete. I en tydlig intern rutin har ansvarsroller delats ut och alla i organisationen vet vad som gäller vid bland annat incidenter eller begäran från registrerade. Om det däremot saknas en tydlig intern rutin avseende dataskyddsarbetet finns en betydande risk att den registrerades rättigheter inte tillvaratas.

Granskningen av verksamheten har visat att flera interna rutiner är bristfälliga. I rapporten har både rutinen för hantering av begäran från registrerade och för personuppgiftsincidenter tidigare tagits upp. Risken med otydliga och bristfälliga rutiner är att verksamheten inte vet vad som ska utföras vid olika händelser och att den därmed inte uppfyller de krav som ställs på den.

	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 – Avsaknad av informationsklassningar

Informationsklassning är en grundläggande del av verksamhetens dataskyddsarbete. Det krävs för att verksamheten har koll på sina system för att förstå vilka tekniska och organisatoriska säkerhetsåtgärder som krävs för att skydda de personuppgifter som behandlas. Utan informationsklassning är det inte möjligt för verksamheten att veta om de åtgärder som de vidtagit är tillräckliga och risken för att åtgärderna är felaktiga är påtaglig.

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

5.4 Råd och rekommendationer till PUA

Dessa risker bör hanteras inom ramen för planerade granskningar under det nya verksamhetsåret, se därför nästa kapitel 6.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Registerförteckning
- Individens rättigheter
- Informationsklassning

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 med fokus på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Dessa har valt för att åstadkomma en röd tråd i dataskyddsarbetet från ett verksamhetsår till nästa samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.

6.3 Planerade granskningar

Granskning 1 – registerförteckning

Syftet med granskningen är att komplettera den nuvarande registerförteckningen. Utgångspunkten kan med fördel vara den granskning som gjorts i denna rapport där slutsatsen är att registerförteckningen varken är fullständig eller uppfyller kraven enligt artikel 30.

Granskningen bör ledas av DSO som ger samtliga ansvariga för behandlingar i uppdrag att säkerställa att deras behandlingar är uppdaterade och korrekta och sedan återkoppla det till DSO. Återkopplingen till DSO bör således innehålla information huruvida alla behandlingar finns med i förteckningen samt om dokumentationen är komplett, korrekt och uppdaterad. Denna granskning rekommenderas först efter att mallen för registerförteckningen har granskats och uppdaterats. Mallen för registerförteckningen behöver motsvara minimikraven i artikel 30, detta kan säkerställas genom att frågorna som motsvarar kraven blir obligatoriska. Om mallen för registerförteckningen inte motsvarar

kraven eller i övrigt är bristfällig kommer ingen typ av granskning av registerförteckningen att leda till ett tillfredsställande resultat.

Granskning 2 – individens rättigheter

Syftet med granskningen är att förbättra den interna rutinen för säkerställande av de registrerades rättigheter. DSO bör leda granskningen och inventera styrdokument samt rutinbeskrivningar. I granskningsarbetet bör DSO ta hjälp av ansvariga för behandlingarna för att utreda huruvida rutinerna bör vara avdelningsspecifika. En del av granskningen bör innefatta att rutinerna dokumenteras och görs tillgängliga för organisationen.

Då det inte inkommit någon begäran från registrerade under året skulle det även vara en fördel för verksamheten att testa sina rutiner för exempelvis begäran om registerutdrag. Detta för att se hur väl rutinerna uppfyller kraven i dataskyddsförordningen.

Granskning 3 – avsaknad av informationsklassningar

Eftersom det finns en avsaknad av informationsklassningar bör en granskning av huruvida informationsklassningar har genomförts och om lämpliga tekniska och organisatoriska säkerhetsåtgärder har vidtagits i enlighet med kraven i artikel 32 granskas i slutet av verksamhetsåret 2022. Granskningen bör ledas av DSO tillsammans med informationssäkerhetsansvarig. Efter att informationsklassning genomförts bör en analys av vilka tekniska och organisatoriska säkerhetsåtgärder som är lämpliga upprättas och uppdateras i registerförteckningen.

7 Övrigt att rapportera

7.1 Sammanfattning

I de övriga observationerna har det framkommit att ett tydligare samarbete och ansvarsfördelning med Stockholm stad hade underlättat det löpande dataskyddsarbetet på stadsdelsförvaltningen. Dataskyddsarbetet kräver även fler resurser med beaktande av resultaten som framkommit i de obligatoriska rapporteringsområdena ovan men även med beaktande av rättsläget i omvärlden gällande tredjelandsöverföring.

7.2 Syfte

Avsikten med denna punkt i årsrapportmallen är att ge möjlighet att komplettera bilden av statusen i dataskyddsarbetet. Under denna rubrik anges därför sådant som inte på ett naturligt sätt kunde tas upp under någon av punkterna i rapporteringsstrukturen ovan.

7.3 Övriga observationer

Observation 1

Stödet till informationsklassningar har pausats från centralt håll vilket gör att Farsta stadsdelsnämnd påverkas avsevärt eftersom Stockholm stad har en samordnande roll, och också förvaltar och ansvarar för de centrala systemen. Det är också viktigt i detta arbete att tydliggöra vilken roll stadsdelsförvaltningen har. Otydlighet i ansvar och mandat mellan staden och stadsdelsnämnden avseende informationssäkerhet och dataskydd leder till risker för Farsta stadsdelsnämnd

Observation 2

Dataskyddsarbetet är, i allmänhet, mycket krävande och i dagsläget, vilket framkommer ovan, har flera allvarliga brister identifierats. Eftersom bristerna är omfattande förutsätter det fortsatta arbetet att det finns resurser som kan arbeta med det löpande dataskyddsarbete för att minimera riskerna. Detta särskilt eftersom det inte ingår i DSO:s arbetsuppgifter att arbeta med det operativa arbetet. Det är viktigt att PUA möjliggör för DSO att utföra sin granskande roll.

Dataskyddsarbetet kräver även fler resurser med beaktande av rättsläget i omvärlden särskilt på grund av Schrems II-domen[1] och de krav som efter den ställts på PUA. PUA behöver kartlägga samtliga tredjelandsöverföringar för att kunna identifiera var personuppgifterna finns och vilka skyddsåtgärder som behöver tillämpas. Detta förutsätter att det grundläggande arbetet kring dataskydd såsom en fullständig registerförteckning finns.

7.4 Råd och rekommendationer till PUA

[1] Mål C-311/18 Data Data Protection Commissioner/Maximillian Schrems och Facebook Ireland.

Den slutliga rekommendationen är därför att tillsätta fler resurser för dataskyddsarbetet i stadsdelsförvaltningen för att säkerställa att riskerna minimeras och att dataskyddsarbetet sker löpande. Detta är viktigt för att få det grundläggande dataskyddsarbetet på plats såsom registerförteckningen men också för att det ska finnas möjlighet att anpassa dataskyddsarbetet löpande efter rättsläget. En särskild resurs bör utses gentemot Stockholm stad. Detta för att säkerställa ett gott samarbete och samsyn på dataskyddsfrågorna som berör stadsdelsförvaltningen. Det är viktigt att Stockholm stad är insatt i stadsdelsförvaltningarna arbete och hur de påverkas av det övergripande dataskyddsarbetet som sker hos Stockholm stad men också att Farsta stadsdelsförvaltning får möjlighet att jobba med de rutiner och mallar som kommer från Stockholm stad på rätt sätt.

PUA bör också granska samtliga system utifrån tredjelandsperspektivet. Detta för att säkerställa att inga olagliga tredjelandsöverföringar finns pågående men också för att säkerställa att rätt åtgärder vidtagits i de fall tredjelandsöverföringar sker. I dessa fall är det också viktigt att dokumentation som krävs såsom konsekvensbedömningar eller Transfer Impact Assessment har tagits fram och att dessa följt de rekommendationer som finns från bland annat IMY. Detta borde göras omgående särskilt med beaktande av att Farsta Stadsdelsförvaltning redan har en förteckning över de system som behandlar personuppgifter.

8 Bilaga 1

Specifikation över underlag som ligger till grund för granskningen.

Underlag	**Kommentar**
Registerförteckning 211206 Farsta	Utdrag ur Draftit
Dataskyddsförordningen och registerförteckning	Dokumentbibliotek Farsta, GDPR – personuppgifts-hantering
Checklista inventering personuppgiftsbehandlingar	Dokumentbibliotek Farsta, GDPR – personuppgifts-hantering
Lathund Draftit Privacy records	Dokumentbibliotek Farsta - GDPR– personuppgifts-hantering

GDPR för dig som chef	Dokumentbibliotek Farsta - GDPR– personuppgifts-hantering
Handbok för personuppgiftsbehandling Farsta	Dokumentbibliotek Farsta - GDPR– personuppgifts-hantering
Registerutdrag – mall för redovisning av personuppgiftshantering	Dokumentbibliotek Farsta - GDPR– personuppgifts-hantering
Handbok för informationsklassning och mallar för ”Informations-klassningsprotokoll”	Dokumentbibliotek Farsta - GDPR– personuppgifts-hantering
Riktlinje informationssäkerhet	Intranätet
Rutin för hantering personuppgiftsincident	Dokumentbibliotek Farsta - GDPR– personuppgifts-hantering
Blankett Anmälan av personuppgiftsincidenter	Dokumentbibliotek Farsta - GDPR– personuppgifts-hantering
Vägledning för personuppgiftsincidenthantering – SLK mall	Dokumentbibliotek Farsta - GDPR– personuppgifts-hantering
Policy sociala medier	Intranätet
Integritetspolicy Farsta stadsdelsnämnd	Dokumentbibliotek Farsta - GDPR– personuppgifts-hantering
Information om personuppgiftsbehandling till anställda i Farsta stadsdelsnämnd	Dokumentbibliotek Farsta - GDPR– personuppgifts-hantering
Mall och checklista konsekvensbedömning personuppgiftsbehandlingar	Dokumentbibliotek Farsta - GDPR– personuppgifts-hantering
Mall för konsekvensbedömning	Dokumentbibliotek Farsta - GDPR– personuppgifts-hantering
Arkiv och gallring i förhållande till GDPR	Dokumentbibliotek Farsta - GDPR– personuppgifts-hantering
Grundkurs i Dataskydd	Utbildningsplattformen Stockholm stad
Personuppgiftsbiträdesavtal Mall	Dokumentbibliotek Farsta - GDPR– personuppgifts-hantering

Konsekvensbedömning Farsta smarta lås i hemtjänsten	
Intervju enhetschefer checklista GDPR 2021	Blankett för rapport av kontroll
Förteckning system med personuppgiftsbehandling	Dokumentbibliotek Farsta – GDPR– personuppgifts-hantering