Stockholms stad

Bilaga 10

GDPR Årsrapport

År 2022

Farsta stadsdelsnämnd

GDPR årsrapport
Januari 2023

Dnr: YYYY
Utgivningsdatum:
Kontaktperson:

1 Bakgrund

Dataskyddsförordningen trädde i kraft som lag i Sverige den 25 maj 2018. Syftet med förordningen var att skapa enhetliga dataskyddsregler inom EU avseende respekt för privatlivet och rätten till skydd av personuppgifter enligt artikel 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Dataskyddsförordningen syftar även till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna i EU.

Enligt dataskyddsförordningen är varje nämnd och bolagsstyrelse inom Stockholms stad ansvarig för att verksamheten följer dataskyddslagstiftningen vid hantering av personuppgifter. Det innebär att nämnd och bolagsstyrelse behöver informera sig, styra och följa upp sin verksamhet avseende behandlingen av personuppgifter.

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

Denna årsrapport är således ett medel för nämnd och styrelse att ta emot de råd och rekommendationer som DSO:n är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i vad DSO:ns granskande arbete av verksamhetens status avseende integritet och dataskydd visar. Årsrapporten syftar till att nämnd/bolagsstyrelse ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Detta samspel resulterar i att det blir enklare för ansvarig nämnd/bolagsstyrelse att visa hur de som personuppgiftsansvarig efterlever dataskyddslagstiftningen.

Dataskyddsförordningen bygger på grundläggande principer och en av dessa principer är ansvarsskyldigheten. Den innebär att nämnd eller bolagsstyrelse ska kunna *visa* att verksamheten efterlever dataskyddsförordningen. Årsrapporten är en mycket viktig del av denna *dokumenteringsskyldighe*t. Årsrapporten är även ett medel för nämnds/bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehåll

2 Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport. Årsrapporten spänner över sex obligatoriska rapporteringsområden. Det har identifierats brister i varje rapporteringsområde under framtagandet av årsrapporten.

Den största bristen rör liksom föregående år rapporteringsområdet *registerförteckning*, som visar på att arbetet som påbörjades förra året kring ifyllande och komplettering av registerförteckningen behöver fortsätta och genomföras för att uppfylla kraven i dataskyddsförordningen. Registerförteckningen utgör en grund för att dataskyddsarbetet i övrigt ska kunna genomföras.

I rapporten för 2021 identifierades att väldigt få informationsklassningar hade genomförts. Vid genomförandet av informationsklassningar tydliggörs vilka åtgärder som krävs för att uppfylla kraven kring informationssäkerhet och dataskydd. Under 2022 har ett antal nya informationsklassningar gjorts, men fler behöver genomföras för att säkerställa att rätt tekniska- och organisatoriska säkerhetsåtgärder finns på plats. Detta är framför allt viktigt i personuppgiftsbehandlingarna där känsliga personuppgifter behandlas.

3 Obligatoriska rapporteringsområden

Denna årsrapport spänner över sex obligatoriska rapporteringsområden som Personuppgiftsansvarig (”PUA”) som ett minimum ska informera sig om årligen för att kunna anses leda och styra dataskyddsarbetet så som dataskyddsförordningen avser.

De obligatoriska rapporteringsområdena är registerförteckning, styrdokument, tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter.

Nedan redogörs för nämndens status och DSO:ns slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:ns genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	386
Har nödvändiga uppdateringar gjorts?	Delvis
Bedöms registerförteckningen vara fullständig?	Delvis
Har verksamheten lämpliga rutiner för registerföring?	Ja

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).

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.

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.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

Det finns totalt 386 registrerade behandlingar i registerförteckningen, 17 fler än föregående år. I samband med registrering av en behandling får man även besvara frågan ”Är du klar med registerbeskrivningen?”. Av de registrerade behandlingarna är 153 registrerade behandlingar markerade som klara jämfört med föregående år då 107 var klarmarkerade. 17 stycken har markerats som inte färdiga och återkommer. I övriga behandlingar har frågan lämnats obesvarad.

Många behandlingar är registrerade av flera olika verksamheter. Dessa behandlingar behöver registreras samlat och övergripande för att minska antalet dubbletter, göra registerförteckningen mer översiktlig och minska administrationstrycket på enheterna.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Innehållsmässigt har uppdateringar inte skett i den utsträckning som varit nödvändig. Majoriteten av de registrerade behandlingarna är fortfarande inte fullständigt registrerade i registerförteckningen.

DSO bedömer hur fullständig registerförteckningen är

I registerförteckningen saknas till stor del de behandlingar som görs i centrala system. En anledning till detta är att behandlingarna i dessa system inte rimligast registreras för varje enskild enhet, utan ett samlat gemensamt arbete behöver göras.

I rapporten för 2021 konstaterades att de behandlingar som finns beskrivna i registerförteckningen många gånger också är bristfälligt beskriven, oaktat om frågan är obligatorisk eller inte. Detta gäller särskilt frågan om ändamål. Frågan besvaras väldigt kort till exempel anges ”avtal”, ”lätt tillgängligt” och ”administration” som ändamål vilket inte beskriver ändamålet med

personuppgiftsbehandlingen tillräckligt. Dessa brister kvarstår även 2022.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Det finns ett utbildningsmaterial, *Dataskyddsförordningen och registerförteckning* för hur registerförteckningen ska fyllas i och vad den bör innehålla för att uppfylla kraven i dataskyddsförordningen.

Utöver utbildningsmaterialet för registerförteckningen finns en vägledning ”GDPR för dig som chef” som redogör för chefernas ansvar enligt dataskyddsförordningen. Enligt vägledningen ska cheferna säkerställa att de personuppgiftsbehandlingar som görs i deras verksamhet 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.

PUA kan utöver detta komplettera styr- och stöddokumentationen 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.

3.1.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten
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

De identifierade bristerna är omfattande och kräver omgående åtgärder. Grunden för fastställandet är både registerförteckningens

kvalitet 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 DSO ger råd och rekommendationer till PUA

PUA bör prioritera att sammanhållna registreringar görs på övergripande förvaltningsnivå för att komplettera registerförteckningen med alla personbehandlingar i centrala system så som LISA, Sociala System etc.

De behandlingar som å andra sidan är registrerade av flera olika verksamheter, exempelvis vissa typer av protokoll eller faktureringar, skulle även dessa behöva registreras samlat och förvaltningsövergripande för att minska antalet dubbletter och göra registerförteckningen mer översiktlig och korrekt.

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.

För att säkerställa att det finns en tydlig kontaktperson för både medarbetarna och DSO avseende registerförteckningen bör PUA utse särskilda personer för att ha ett huvudsakligt ansvar för registerförteckningen.

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 kvaliteten 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?	Ja
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Ja
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?

Lista över befintliga styr- och stöddokument:

- Handbok för personuppgiftsbehandling.
  Omfattar information om hur verksamheten hanterar information till den registrerade samt information om den registrerades rättigheter.
- Integritetspolicy Farsta Stadsdelsnämnd
- Hantering av anställdas personuppgifter
- Mall(-ar) för information om hantering av personuppgifter (Stadens, nämndens och verksamhetsspecifika utformningar)
- 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
- 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)

DSO bedömer 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 i förvaltningens dokumentbibliotek, tillgängligt för alla

medarbetare via intranätet. 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.

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 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 fungerar som generell information till invånarna med hänvisning vidare för mer information och uppfyller inte kraven i artikel 13 avseende information om rättslig grund, information om mottagare av personuppgifterna och information om överföringar till tredjeland, eller 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. Detta är svårt att åstadkomma med nuvarande utformning av stadens hemsida.

För att uppfylla artikel 13 och 14 finns Mall för information om hantering av personuppgifter. Den grundläggande utformningen av mallen är framtagen av staden, men används sedan i nämndens verksamheter, som kan anpassa mallen med aktuella personuppgiftbehandlingar inom verksamhetsområdet och hanteringen av dessa, som information till invånare i kontakt med stadsdesförvaltningen.

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 DSO anger hur allvarliga bristerna är på en skala

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

Många dokument, till exempel integritetspolicyn och rutinen för personuppgiftsincidenter, kan kompletteras med exempel från verksamheten och instruktioner bör beskrivas mer utförligt.

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 DSO ger råd och rekommendationer till PUA

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 knyter inte på ett tydligt sätt an till verksamheten i sig. En tydlig rutin för tillvaratagande av de registrerades rättigheter skulle minska risken för att inte uppfylla Dataskyddsförordningens krav

En tydlig rutin för arkiv och gallring i förhållande till dataskyddsförordningen behöver tas fram.

Dokumenten bör kontinuerligt ses över och om möjligt slås ihop för att minimera risken för fel i arbetet. Det ska vara tydligt vilket syfte varje dokument har och var medarbetaren kan hitta hjälp. PUA bör även ta fram egna rutiner och/eller styrdokument i de fall detta inte finns.

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?	10
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. Dokumentet ger en första bedömning och stöd innan den större aktiviteten med verktyget KLASSA. Ett flertal klassningar har genomförts under 2022, men många kvarstår att göra.

Det finns 10 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 DSO anger 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 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 DSO ger 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, initiera klassningsarbete och ansvara vid införande av nya system.

Informationsägare är formellt sett utsedda (förvaltningens chefer), men de har bristande 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.

Registerförteckningen har under 2022 uppdaterats med en fråga om informationsklassning så att det på ett enklare sätt ska vara möjligt att avgöra vilka och hur många behandlingar som har klassats.

Arbetet med att informationsklassa IT-systemen fortsätter för 2023 i så snabb takt som är möjligt.

Den årliga uppmaningen bör även uppmuntra till att repetera den obligatoriska grundkursen i dataskydd.

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. Det finns en funktion i Draftit där risknivån för personuppgiftsbehandlingar anges (låg/mellanhög/hög), men den används i mycket liten utsträckning.

De konsekvensbedömningar som genomförts under 2022 har gjorts i samband med informationsklassningar och på initiativ av informationssäkerhetssamordnare och DSO. Verksamheterna saknar i stor utsträckning kunskap och processer för att själva kunna identifiera och bedöma behov av konsekvensbedömningar.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Genom att utföra ett stickprov ur registerförteckningen kan det konstateras att det gjorts några fler riskbedömningar sedan 2021, men 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.

Då registerförteckningen i vissa delar är bristfälligt ifylld, särskilt i detta fall med avseende på risknivå, går det visserligen att konstatera att det saknas konsekvensbedömningar men det är inte möjligt att besvara i vilken omfattning.

Är de genomförda konsekvensbedömningarna aktuella?

De konsekvensbedömningar som finns är aktuella och i de flesta fall genomförda under 2022.

3.4.4 DSO anger 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.

Konsekvensbedömningar saknas för majoriteten av de behandlingar som utförs i verksamheten, inklusive högriskbehandlingar.

3.4.5 DSO ger 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?

Ett av huvudsyftena med dataskyddsförordningen är att värna om enskilda individers rättigheter i sammanhang där deras personuppgifter behandlas och registreras. Därför måste alla organisationer vara medvetna om att man endast kan behandla personuppgifter om man respekterar individens fri- och rättigheter, och har rutiner för att bemöta och uppfylla dessa rättigheter när det blir aktuellt. Några av dessa rättigheter 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.

I handboken för personuppgiftsbehandlingen beskrivs alla rättigheter på ett utförligt sätt vilket är positivt. Det saknas dock konkreta exempel och beskrivning av 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 endast en 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 DSO anger 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

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 DSO ger 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.

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?	9
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Sju incidenter har rapporterats till IMY och de berörda har i samtliga fall informerats.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Fem incidenter har rapporterats i tid.

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 hanterats i tid. 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. Chefen har också ett ansvar att säkerställa att medarbetare genomgått stadens e-utbildning för grundläggande dataskydd. Huruvida en incident därför upptäckts och anmäls i tid beror också på chefernas agerande.

Under 2022 har fler personuppgiftsincidenter rapporterats och en högre andel har rapporterats korrekt. Detta är förmodligen en följd av att utbildningen i dataskydd genomförts i större utsträckning samt att alla chefer och nyckelpersoner fått två särskilda utbildningstillfällen kring chefsansvaret för dataskyddsarbetet i praktiken.

3.6.4 DSO anger hur allvarliga bristerna är på en skala

	Allvarliga brister identifierade som omgående kräver insatser av ledning och/eller övriga verksamheten

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

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.

3.6.5 DSO ger råd och rekommendationer till PUA

Arbetet med att kontinuerligt utbilda samtliga medarbetare om grundläggande dataskydd och vad som utgör en personuppgiftsincident behöver fortsätta och upprätthållas för att eventuella personuppgiftsincidenter ska identifieras och hanteras på korrekt sätt. Den obligatoriska utbildningen ”Grundkurs i dataskydd” bör skickas ut årligen till alla medarbetare och det bör säkerställas att den är en del av introduktionen för alla nya medarbetare. 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..

I IA-systemet rapporteras alla incidenter som sker i verksamheten, som till exempel att någon skadar sig fysiskt. Ibland sker felregistreringar av händelsetyp, vilket kan leda till att identifiering av personuppgiftsincidenter fördröjs eller inte hanteras på rätt sätt. En rekommendation är att löpande kontrollera huruvida övriga rapporterade incidenter också utgör en personuppgiftsincident.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- *Granskning av registerförteckningen*
- *Granskning av incidentrapporteringssystemet*
- *Granskning av utbildning dataskydd*
- *Granskning av avsaknaden av informationsklassningar*

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

Ansvariga chefer har under året fått i uppdrag att säkerställa att deras behandlingar är uppdaterade och korrekta. För att stödja dem i detta genomförde DSO under våren två utbildningstillfällen där samtliga chefer och nyckelpersoner uppmanades att delta.

En kontroll har efter det gjorts i registerförteckningen avseende huruvida obligatoriska fält fyllts i gjorts, korrekt laglig grund och att informationen som anges i registreringarna i övrigt är korrekt kontrollerats. De obligatoriska frågorna är besvarade även i de registreringar som inte är markerade som klara, förutom frågan om huruvida informationsklassning har gjorts. Den frågan har gjorts obligatorisk under året, vilket kan vara en av anledningarna till att den inte besvarats, men också att kunskapsnivån är låg i

verksamheterna och många känner inte till vad en informationsklassning är, hur och när det görs, eller om det gjorts. Den rättsliga grunden är korrekt i majoriteten av behandlingarna men det finns anledning för verksamheterna att gå igenom sina registreringar tillsammans med DSO för att säkerställa att laglig grund är rätt i samtliga registreringar.

	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

Granskning av utbildning om dataskydd

Under året har DSO följt upp genomförandet av den obligatoriska utbildningen om dataskydd. Samtliga verksamheter rapporterar att de genomfört aktiviteten i 2022 års verksamhetsplan om att medarbetarna ska genomföra utbildningarna i dataskydd och informationssäkerhet. Vid stickprov varierar andelen av medarbetarna som genomfört utbildningen mellan olika verksamheter men ligger på ungefär 70-80%. Det kan vara fler än så som vid något tillfälle genomfört utbildningen eftersom antalet som nollställs när ändringar i utbildningen gjorts. Den kontinuerliga personalomsättningen påverkar också andel medarbetare som genomfört utbildningen. De verksamheter där andelen är lägre, exempelvis där medarbetare inte har åtkomst till dator på samma sätt som i mer administrativa verksamheter, rekommenderas att ha gemensamma genomgångar.

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

	Inga brister av nämnvärd betydelse identifierade

Granskning av incidentrapporteringssystemet IA

Under året har DSO granskat rapporteringen av personuppgiftsincidenter i incidentrapporteringssystemet IA med avseende på:

- om korrekt incidenttyp rapporterats
- om någon personuppgiftsincident felregistrerats och därför inte identifierats.
- Om utredning dokumenterats i IA
- Om utredning av incidenterna avslutats.

Vid genomgång av samtliga övriga avvikelser i IA har ingen oidentifierad personuppgiftsincident upptäckts. En incident har dock en rubrik som gör att det kan vara svårt att uppfatta att det rör sig om en personuppgiftsincident. Däremot har några avvikelser felregistrerats som personuppgiftsincidenter trots att de har att göra med helt orelaterade händelser, som till exempel skada på person. Detta kan indikera bristande kunskap hos de rapporterande medarbetarna om vad en personuppgiftsincident är.

Samtliga nio identifierade misstänkta personuppgiftsincidenter finns registrerade i IA enligt rutin. Av dessa nio är det dock bara fem som är helt avslutade. I två av fallen är ingen egentlig utredning av händelsen dokumenterad och det går inte att utläsa i IA-systemet om anmälan gjorts till IMY.

Granskning om avsaknad av informationsklassningar

Granskningen gällande avsaknaden av informationsklassningar genomfördes inte helt så som planerades i årsrapport 2021. Istället konstaterades att informationsklassningsarbetet hade så klara brister att åtgärder vidtogs omgående. Under ledning av DSO och informationssäkerhetssamordnare genomfördes därför en översikt och prioritering av nödvändiga informationsklassningar och etablerande av processer för det arbetet. Klassning av prioriterade informationsmängder påbörjades och i samband med detta även analys av vilka tekniska och organisatoriska säkerhetsåtgärder som är lämpliga, samt tillhörande bedömning och genomförande av nödvändiga konsekvensbedömningar. Ett stort arbete kvarstår dock inom detta område.

	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

4.4 DSO ger råd och rekommendationer till PUA

Mot bakgrund av bristerna i registerförteckningen bör granskning fortsätta under följande år, där det följs upp 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 fortsätta att 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, specifikt inom säkerställandet av individens rättigheter
- Avsaknad av informationsklassning och konsekvensbedömningar

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

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.

	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

Risk 2

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
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

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 DSO ger 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.

Då samma identifierade risker kvarstår sedan föregående år som de mest prioriterade kommer granskningarna under 2023 att beröra samma områden.

6.3 Planerade granskningar

Granskning 1 – registerförteckning

Syftet med granskningen är att komplettera den nuvarande registerförteckningen. 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.

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. Granskningen bör omfatta chefernas kunskap om de olika rättigheterna och verksamheternas ansvar och verksamheternas rutiner för att hantera förfrågningar från de registrerade.

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 2023.

7 Övrigt att rapportera

7.1 Sammanfattning

I de övriga observationerna har det framkommit att en tydligare organisation och mer ansvarsfördelning hade underlättat det löpande dataskyddsarbetet på stadsdelsförvaltningen. Dataskyddsarbetet kräver även kontinuerlig kommunikation, prioritering och utbildning med beaktande av resultaten som framkommit i de obligatoriska rapporteringsområdena.

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

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.

Observation 2

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

Då enhetscheferna är ansvariga för ifyllandet av registerförteckningen, och det både mot bakgrund av förteckningens brister samt chefernas kunskapsbrister, genomförde DSO vidare utbildning och ”GDPR för chefer” kommunicerades för att garantera att cheferna vet vad som förväntas av dem.

Utbildningarna i dataskydd och informationssäkerhet gjordes till obligatorisk aktivitet i verksamhetsplanen för samtliga verksamheter och medarbetare, oaktat om medarbetare gått den tidigare, för att både repetera utbildningen och säkerställa att den når fler än vad man har kännedom om idag.

Resultatet av detta är att registreringar i registerförteckningen förbättrats något, samt att fler personuppgiftsincidenter identifierats, rapporterats och dokumenterats korrekt. Det visar också att denna typ av insatser måste fortsätta och att mycket arbete kvarstår för att komma tillrätta med brister och leva upp till dataskyddsförordningens krav och intentioner.

7.4 DSO ger råd och rekommendationer till PUA

Den slutliga rekommendationen är att organisera fler resurser för dataskyddsarbetet i stadsdelsförvaltningen för att säkerställa att riskerna minimeras och att dataskyddsarbetet sker löpande. För att sköta det praktiska ansvaret för dataskyddsarbetet behövs grupper och nätverk som har kompetens både att identifiera vad som behöver göras och att genomföra det. Ett ensamt dataskyddsombud räcker inte till, särskilt då dataskyddsombudet har andra arbetsuppgifter samt ska ha en granskande roll, vilket försvårar att också vara en projektledare för implementation och framtagande av styrdokument.

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 och ha ett gott samarbete och samsyn på dataskyddsfrågorna i förvaltningen.