Stockholms stad

GDPR Årsrapport

2021

Skärholmens stadsdelsnämnd

GDPR årsrapport
Januari 2022

Dnr: SKHLM 2022/37
Utgivningsdatum: 2022-01-17
Kontaktperson: Sabina Toromanovic

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.

Årsrapporten syftar till att täcka in de grundläggande och obligatoriska aktiviteter som en PUA bör hålla sig informerad om

för det gångna året. Det är obligatoriskt för PUA att efterfråga denna årsrapport.

Områdena i mallen för DSO:s årsrapport gör inte anspråk på att täcka in allt som möjligtvis kan och ska granskas och rapporteras om av ett dataskyddsombud i en verksamhet, utan är ett stöd och en basnivå utifrån vilken viktiga dataskyddsslutsatser kan dras *av PUA för att underlätta PUA:s styrning av det faktiska dataskyddsarbetet*. För att DSO ska hålla sina slutsatser i årsrapporten överblickbara, någorlunda rimliga i sin omfattning, relevanta för en ledningsperson och med ett fokus på något av det viktigaste, krävs att rapporten hålls koncis. Förslagsvis kan andra former och forum användas av DSO för att dokumentera och rapportera fördjupande eller bredare avseende dataskyddsfrågor som är relevanta för verksamheten. Det är annars lätt att tappa bort syftet med årsrapporten, vilket är att skapa förståelse hos PUA för dataskyddsfrågorna samt skapa förutsättningar för PUA att fatta beslut om dataskyddsåtgärder för nästa verksamhetsår.

Sekretess
Årsrapporten kommer visa på de risker och förbättringsområden som verksamheten har att arbeta med. Det ska i normalfallet inte vara skäl för sekretess enligt t.ex. kap 18:8 i OSL eftersom beskrivningarna till PUA bör vara på en övergripande nivå och därmed inte avslöja sådana detaljer som kräver sekretess.

Om DSO trots allt finner det nödvändigt att kommunicera sådana detaljer att rapporten bör beläggas med sekretess, så har DSO ett ansvar att lyfta ut detaljerna från den offentliga rapporten till ett annat dokument eller på annat sätt maska detaljerna innan rapporten blir offentlig som en bilaga till Verksamhetsberättelsen. Det är således den version som blir offentlig som kan behöva ses över på det här sättet.

Förkortningar
- **DSO:** dataskyddsombud.
- **PUA:** personuppgiftsansvarig, den som bestämmer ändamålen och medlen för en behandling av personuppgifter.
- **IMY:** Integritetsskyddsmyndigheten, från den 1 januari 2021 byter Datainspektionen namn till Integritetsskyddsmyndigheten.
- **IA:** stadens verktyg för incidentrapportering.
- **PuB:** personuppgiftsbiträdesavtal

Innehåll

1 Bakgrund ... 3
2 Sammanfattning ... 6
3 Obligatoriska rapporteringsområden ... 8
3.1 Registerförteckning ... 9
3.2 Styrdokument ... 13
3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar ... 16
3.4 Konsekvensbedömningar ... 20
3.5 Individens rättigheter ... 24
3.6 Personuppgiftsincidenter ... 26
4 Genomförda granskningar under året ... 32
4.1 Sammanfattning ... 32
4.2 Syfte ... 32
4.3 Genomförda granskningar och deras resultat ... 32
4.4 DSO ger råd och rekommendationer till PUA ... 36
5 Risker inom dataskydd ... 37
5.1 Sammanfattning ... 37
5.2 Syfte ... 37
5.3 Resultatet av riskkartläggningen ... 37
5.4 DSO ger råd och rekommendationer till PUA ... 38
6 Planerade granskningar under det nya verksamhetsåret ... 38
6.1 Sammanfattning ... 38
6.2 Syfte ... 39
6.3 Planerade granskningar ... 39
7 Övrigt att rapportera ... 40
7.1 Sammanfattning ... 40
7.2 Syfte ... 40
7.3 Övriga observationer ... 40
7.4 DSO ger råd och rekommendationer till PUA ... 41

2 Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

År 2021 har präglats av att återuppta delar av aktiviteter inom dataskydd som skjutits upp under år 2020 på grund av pandemi då fokus har varit att upprätthålla de samhällsviktiga funktionerna i förvaltningen, ibland med hård ansträngd personalstyrka.

Jag som DSO vill lyfta fram några av de viktiga punkter som har genomförts.

Det har påbörjats aktivt arbete med registerförteckning i systemet Draftit tillsammans med DSO och utsedda GDPR ombud per enhet. Det genomförs utbildning, vägledning för GDPR ombud för att fortsättningsvis underhålla registerförteckning och hålla den aktuell.

Efter att Privacy Shield har ogiltigförklarats i det så kallade ”Schrems II-fallet det har genomförts inventering och kartläggning av tjänster som används i förvaltningen som leder till att personuppgifter överförs till tredje land.

Förvaltningens rutiner för dataskyddsförordning och behandling av personuppgifter har uppdaterats.

Uppdatering av delegationsordning utifrån GDPR har genomförts.

Inventering och kartläggning om det förekommer eventuella kameror i förvaltningens verksamheter.

Utbildning och information om Brottsdatalagen har genomförts med berörda verksamheter.

Förvaltningens DSO har medverkat i informationsklassning av hälso-sjukvårdssystemet VODOK tillsammans med Enskede-Årsta-Vantör stadsdelsförvaltning och Stadsledningskontoret.

Det har utförts konsekvensbedömning avseende digital avisering om utbetalning av ekonomiskt bistånd genom förmedlingsväxel Mina meddelanden tillsammans med stadens samtliga DSO på förvaltningsnivå och Stadsledningskontoret.

Det har upprättats samarbete med Socialförvaltningen för att tillsammans hitta säkert arbetssätt i kommunikation mellan förvaltningen och LSS hälsan för att skydda de registrerades personuppgifter.

De har utförts riskanalys och informationsklassning tillsammans med förvaltningens DSO , informationssäkerhetssamordnare,

verksamheters ansvariga och leverantören gällande användning av tjänsten Embrace som främjar trygghet och förebygger brott.

Det har utförts arbete tillsammans med förvaltningens DSO, informationssäkerhetssamordnare, verksamhetsansvarig och leverantör för tjänsten Digidem Lab , digital plattform för medborgardialog i förvaltningen för att säkerställa att leverantör uppfyller informationssäkerhet och GDPR krav.

Det har utförts informationsklassning och konsekvensbedömning gällande ekonomi och verksamhetsuppföljning.

Det har utförts riskanalys och tagits fram ett nytt arbetssätt i samarbete mellan förskola och kö handläggare gällande kommunikation i kö handläggning. Förvaltningens DSO och informationssäkerhetssamordnare involverades och deltog i arbete.

Förvaltningens DSO och informationssäkerhetssamordnare genomförde dialog med företaget Amibotic innan ett eventuellt pilotprojekt Robot för distanssamtal i Äldreomsorgen för att säkerställa att projektet fungerar utifrån informationssäkerhet och GDPR krav.

Avdelning för Socialtjänst i förvaltningen har tillsammans med förvaltningens DSO och informationssäkerhetssamordnare genomfört förhandssamoråd inför eventuell ny personuppgiftsbehandling gällande samrådsmöte inom avdelningen.

De har utförts flertal riskanalyser utifrån GDPR avseende tredjelandsöverföring.

Förvaltningens medarbetare är nyfikna och bra på att identifiera personuppgiftsincidenter och vågar fråga om lösningar och se GDPR som en möjlighet.

Därför är min rekommendation att:

- Fortsätta med goda arbetet med att utbilda och informera
- Informera, komplettera och implementera styrdokument
- Att vara bättre på att involvera förvaltningens DSO och informationssäkerhetssamordnare i samband med upphandling av tjänster, system
- Att förstå vikten av konsekvensbedömning av personuppgiftsbehandlingar samt utse vem som ska hålla i konsekvensbedömningar.

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:

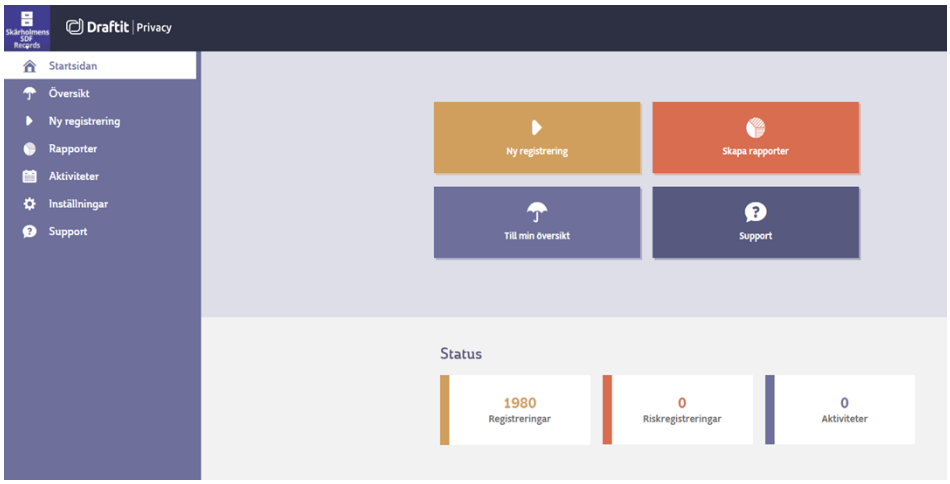
- registerförteckning,
- styrdokument,
- tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar,
- konsekvensbedömningar,
- individens rättigheter
- personuppgiftsincidenter.

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

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	1980
Har nödvändiga uppdateringar gjorts?	Aktiv uppdatering påbörjades från mitten av år 2021 och fortsätter under år 2022 med anledning av pandemi ,ändring av mallen i Draftit (slutet av 2020), och omorganisation i förvaltningen.
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).

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 inventering av personuppgifter i sig är avgörande för allt 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

Registerförteckning finns i ett digitalt verktyg kallat Draftit Records och består av ett frågeformulär per personuppgiftsbehandling vilket i sin tur blir funktionen av en checklista att alla krav i GDPR dokumenteras korrekt.

Skärholmens stadsdelsförvaltning har register förtecknat personuppgiftsbehandlingar i Draftit någon vecka innan GDPR trädde i kraft 25 maj 2018 utifrån Excellmall som framtogs av Stadsledningskontoret.
Under 2019 upptäcktes kunskapsluckor i befintliga Excellmallen som var grund för registerförteckningen då den initiala Excellmallen inte var så utförlig jämfört mot de tillkomna krav som vuxit fram på dokumentation sedan dataskyddsförordnings införande i maj 2018. När arbetet skulle återupptas efter uppdatering av Draftit Records mallen/frågeformulär kom pandemi som en försvårande faktor och arbetet med registerförteckning sköts framåt.

DSO redovisar 1980 personuppgiftsbehandlingar registrerade i Draftit Recordcs. Stor antal av personuppgiftsbehandlingar är under bearbetning då det pågår uppdatering av personuppgiftsbehandlingar inom samtliga verksamhetsområde som behöver kompletteras ,kontrolleras eller på annat sätt bearbetas. Vid den pågående arbete kommer dessa kunskapsluckor att fyllas på enligt plan.

Registerförteckningen är upprättad internt inför dataskyddsförordnings införande i maj 2018.
Registerförteckningens arbete har en skriven rutin som uppdaterades i augusti 2021 och ska förmedlas till verksamheter.
Stadsledningskontoret har skapat en utbildning med filmer där medarbetare guidas genom varje steg i verktyget Draftit Records. Utbildningen finns i stadens utbildningsplattform.

Uppdatering av personuppgiftsbehandlingar har startat i mitten av 2021 samt omregistreringar av befintliga personuppgiftsbehandlingar i nya mallen som Stockholms stad har tagit fram tillsammans med Draftit Records i slutet av 2020.

Registerförteckningen kan aldrig anses som fullständig. Det ska vara ett ständigt levande dokument.

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

3.1.5 DSO ger råd och rekommendationer till PUA

Varje enhet har utsett en GDPR ansvarig och det pågår utbildning i verktyget Darftit Records.
Rådet från DSO är att verksamhetsansvariga tillsammans med GDPR ansvarig ska genomgå personuppgiftsbehandlingarna enligt årshjulet och det systematiska arbetet. Detta påverkar starkt bedömningen av bristerna till orange. När detta är genomförs är bristen minimerad till grönt.

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?	Ja
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 DSO bedöma om verksamheten har de styrdokument antagna och på plats, dels ska rapporteringen visa om dokumentationen innehållsmässigt håller en lämplig kvalitet, i vilket ingår bl.a. att dokumentationen ska vara uppdaterad och aktuell.

En brist inom detta område bör förstås ses som en brist i förhållande till direkta lagkrav, men det finns fler nyanser av detta som bör lyftas fram till PUA. 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

Vid dataskyddsförordningen införande så fördes ett central GDPR projekt vid SLK som skulle ta fram gemensamma dokument för hela staden. Detta projekt levererade aldrig sina dokument och staden har således tagit fram centrala dokument på en gemensam intranätssida.

Finns lämplig styrande dokumentation på plats?
Baserad på stadens centrala styrdokument och dataskyddsföordningens krav ska stadsdelar ha lokalt antagna styrdokument och rutinbeskrivningar.
Stadens centrala informationssäkerhetspolicy inte uppdaterad sedan 2014och det inte finns central beslutad policy eller motsvarande som innefattar en särskild del tillägnade personuppgifter. En tillämpningsanvisning till stadens riktlinjer för informationssäkerhet är dock för närvarande enbart utkast.
En avsaknad av en särskild policy kan bidra till stadsdelsledning inte prioriterar dataskydd.

Skärholmens stadsdelsförvaltning har följande dokumentation på plats:

- Handbok för hantering av personuppgifter enligt GDPR
- Information om hantering av personuppgifter
- Rutiner för inventering av personuppgiftsbehandlingar
- Rutin för hantering av personuppgiftsincidenter
- Rutin för konsekvensbedömning
- Rutin för personuppgiftsbiträdesavtal

- Rutin för hantering av begäran om registerutdrag, rättelse, radering
- Samtyckesblanketter
- Arkiv och gallring i förhalande till GDPR
- Offentlig upphandling och GDPR
- E-utbildning i Dataskyddsförordningen
- Infofolder/brev till de registrerade gällande behandling av personuppgifter
- Arbetsbeskrivning och årshjul för enheternas GDPR-ombud

Samtliga rutiner/grundläggande styrdokument är uppdaterade i november 2021 och är för närvarande på delegation för godkännande och beslut .DSO bedömer att innehållet i existerande/uppdaterande dokument håller lämplig kvalitet.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

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

3.2.5 DSO ger råd och rekommendationer till PUA

Styrdokument
Texten som finns i stadsgemensamma dokument på intranätet kan ibland vara svår att förstå för medarbetarna.

Skärholmens stadsdelsförvaltning har en gemensamgruppdisk med styrdokument och rutiner. I och med att förskoleverksamheter ligger på en annan IT-plattform och inte har tillgång längre till gemensamma gruppdisken behöver Skärholmens stadsdelsförvaltning skapa en egen intranätssida med styrande dokument och rutiner och utvecklas med länkar till både lokal och

centrala dokument. Detta behöver göras efter att uppdaterade och kompletterande styrdokument är godkända och att ägare till styrdokument är utsedd.
Skärholmens stadsdelsförvaltning rekommenderas att fortsätta driva arbetet med att ta fram lokala instruktioner för personuppgiftshantering för respektive verksamhetsområde. Vidare rekommenderas stadsdelsförvaltning att genom detta arbete se till att det bildas en logisk kedja av beslut, ansvarsfördelning samt instruktioner som samtliga medarbetare förstår, så att processerna kan ske i enlighet med vad som är tänkt från centralt håll samt från dataskyddsförordningens krav. Slutligen rekommenderas stadsdelsförvaltning att införa tydligare rutiner för att kontinuerligt granska samt uppdatera styrdokument kring informationssäkerhet (med förutsättning att det finns aktuell styr dokument på central nivå) samt personuppgiftshantering, för att säkerställa dess aktualitet till rådande lagstiftning.

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?	Samtliga verksamhetssystem är informationsklassade. I samband med genomgång av registerförteckning kommer övriga personuppgiftsbehandlingar att ses över informations klassas
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.

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

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

Eftersom informationsklassning är ett arbete som görs inom ramen för informationssäkerhetsarbetet, bör DSO samråda och planera uppföljningen tillsammans med informationssäkerhetssamordnare. Enligt stadens metodik klassas personuppgifter och övrig information i samma workshop, och slutsatserna kring klassningen dokumenteras i samma protokoll.

3.3.3 Resultat

Stockholms stad/Skärholmens stadsdelsförvaltning använder sig av SKR:s verktyg KLASSA för att klassificera verksamhetens IT-system samt ta fram tillhörande skyddsåtgärder utifrån dataskyddsförordningens krav.

KLASSA har vidareutvecklas som verktyg av SKR och GDPR har blivit obligatoriskt segment med uppmaningen att kontakta DSO om det framkommer att det finns personuppgifter. Detta underlättar också för DSO:s arbete att få löpnade information om KLASSA-aktiviteter och eventuell behov om konsekvensbedömning behöver utföras.

Stadsdelsförvaltning har informations klassat samtliga verksamhetssystem samt nya personuppgiftsbehandlingar som tillkommit under året 2021. Stadsdelsförvaltningen och enheternas GDPR ombud genomgår registerförteckningar i Draftit och efter genomgång så ska man se över vilka övriga/gamla personuppgiftsbehandlingar som behöver informations klassas.

Stadsdelsförvaltningens informationssäkerhetssamordnare och DSO har nära samarbete gällande informationsklassning och konsekvensbedömning.

Via stadsdelsförvaltningens intranät distribueras information kring dataskydd- och informationssäkerhetsfrågor till medarbetarna.

Stadsdelsförvaltningen genomför regelbundna utbildningar utifrån verksamhetens behov med medarbetarna inom dataskyddsfrågor.

I stadens e-utbildnings plattformen finns två utbildningarna – informationssäkerhetsutbildning och den grundläggande utbildningen i dataskydd – är obligatoriska för alla medarbetare.

Utöver de två obligatoriska utbildningar finns även :

- Informationssäkerhet- fördjupning
- Fördjupning i dataskydd – offentlighet och sekretess
- Fördjupning i dataskydd – Känsliga personuppgifter
- Fördjupning i dataskydd – rättslig grund
- Fördjupning i dataskydd - webbpublicering och e-post
- Fördjupning i dataskydd – diarier
- Fördjupning i dataskydd – personalfrågor
- Fördjupning i dataskydd – registerutdrag
- Fördjupning i dataskydd – e-förvaltning
- Fördjupning i dataskydd – registerförteckning i Privacy Records (Draftit)
- Konsekvensbedömning avseende dataskydd.

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

3.3.5 DSO ger råd och rekommendationer till PUA

Samtlig information har inte klassificerats. Informationsklassning har skett för delar av befintliga system som har identifierats som kritiska, men inte alla. Ytterligare arbete kvarstår för att täcka i samtliga relevanta system.

Metod och rutin för att genomföra klassificering finns och arbete med klassificering leds av stadsdelens informationssäkerhetssamordnare.

Stadsdelsförvaltningen behöver regelbundet utbilda medarbetare i första hand ansvariga chefer i informationsklassningsarbete.

När personuppgiftsbehandlingarna i Draftit har inventerats och uppdaterats av enheternas GDPR- ombud så är det naturliga steg att dessa också kan KLASSA:s för de system som är aktuella samt genomföra konsekvensbedömning. DSO:s rekommendation är att detta följs upp och påbörjas när inventering och uppdatering av personuppgiftsbehandlingar i Draftit är klar.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Delvis, 2021 årskontroll med registerförteckningen är inte helt klart d v s kontrollera vilka behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter”
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Delvis, 2021 årskontroll med registerförteckningen är inte helt klart d v s kontrollera vilka behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter”
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). Notera att IMY på sin webbplats har publicerat en förtydligande förteckning över när personuppgiftsbehandlingar kräver en konsekvensbedömning. Det är viktigt att PUA genom årsrapporten får en uppdaterad bild av hur fullständig verksamhetens situation är i fråga om konsekvensbedömningar avseende dataskydd.

3.4.3 Resultat

Stadsdelsförvaltningen har deltagit vid flera konsekvensbedömningar under året. Under 2020 genomfördes konsekvensbedömning vid införandet av elektroniska körjournaler som har lett till ett förhandssamråd med Integritetsskyddsmyndigheten, IMY. Efter IMY:s yttrande så ska varje stadsdel genomföra egen konsekvensbedömning för införandet av körjournaler. Stadsdelsförvaltningens DSO har lämnat ut samtlig underlag till ansvarig verksamhet med uppmaning att konsekvensbedömningen ska genomföras. I skrivande stund så är konsekvensbedömningen fortfarande inte genomförd.

Det har utförts konsekvensbedömning avseende digital avisering om utbetalning av ekonomiskt bistånd genom förmedlingsväxel Mina meddelanden tillsammans med stadens samtliga DSO på förvaltningsnivå och Stadsledningskontoret. Stadsdelsförvaltningens DSO har skickat ut konsekvensbedömning till ansvarig verksamhet för granskning och godkännande av konsekvensbedömningen. I skrivande stund så är konsekvensbedömningen inte godkänd än.

Stadsdelen har genomfört flertal riskanalyser och konsekvensbedömningar vid införandet av nya personuppgiftsbehandlingar.

Stadsdelen har även genomför flertal riskanalyser gällande överföring av personuppgifter till tredje land.

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

Oftast är det stadelens DSO och informationssäkerhetssamordnare som har identifierat nya behandlingar som verksamheterna ska införa och konsekvensbedömning och informationsklassning har genomförts. Men ansvaret för konsekvensbedömning ska genomföras och bjuda in DSO och informationssäkerhetssamordnare ligger på verksamheter.

Verksamheternas mognad är väldigt låg när det gäller den delen av ansvar.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Delvis, 2021 årskontroll med registerförteckningen är inte helt klart d v s kontrollera vilka behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter”. Fortsatt arbete av kontroll av registerförteckning.

Är de genomförda konsekvensbedömningarna aktuella?

Konsekvensbedömningar som är genomförda är aktuella.

3.4.4 DSO anger hur allvarliga bristerna är på en skala

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

Kvalitet på konsekvensbedömningar som är genomförda är kompletta och utförliga.
Enligt dataskyddsförordningen artikel 35.2 *ska* den personuppgiftsansvariga/ansvarig verksamhet ”rådfråga dataskyddsombudet vid genomförande av en konsekvensbedömning”, men så är inte fallet, mognad för det i verksamheter är väldigt låg och i nästan alla konsekvensbedömningar så är stadsdelens DSO som har tagit initiativ för att verksamheterna ska genomföra konsekvensbedömningen.

3.4.5 DSO ger råd och rekommendationer till PUA

Konsekvensbedömningar är idag beroende av individers kunskap och metoden.
Då konsekvensbedömningar inte genomförs löpande för samtliga behandlingar är viktigt att vidareutveckla konsekvensbedömningsprocessen, dokumentera och informera om rutiner enligt arbete som stadsdelsförvaltningen genomförde under hösten 2021:

- stadsdelsförvaltningen har i hösten 2021 sett över och fastställt delegationsordning för vem ansvarar att konsekvensbedömningen ska genomföras, vem får godkänna eller avslå dataskyddsombudets rekommendationer samt godkänna eller avslå de åtgärder som tas fram i konsekvensbedömningen.
- Stadsdelsförvaltningen har också under hösten 2021 uppdaterat rutiner och vägledning för genomförandet av konsekvensbedömning.

- Fortsätta informera och utbilda ansvariga verksamheter om vikten av genomförandet av konsekvensbedömning. På stadens E-utbildning portalen finns även webbutbildning för konsekvensbedömning i form av mer detaljerade instruktioner för de olika stegen i processen.

- Fastslå granskningsplan eller internkontrollfunktion som följer upp att stadsdelsförvaltningens verksamheter hanterar personuppgifter i enlighet med dataskyddsförordningen.

- Fortsätta med utbildning av GDPR ombud på enhetsnivå som har hand om enheternas registerförteckning och utveckla/utbilda dem i konsekvensbedömning.

3.5 Individens rättigheter

3.5.1 Sammanfattning

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

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.)

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

Om verksamheten inte klarar av att hantera en begäran från en registrerad person i enlighet med dataskyddsförordningens krav, kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter. Det kan även leda till tillsynsärenden från

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?

Verksamheten har förutsättningar att hantera registrerades rättigheter inom föreskriven tid. Stadsdelsförvaltningen har tydliga rutiner för hantering av begäran från registrerade. Men mognad i verksamheten är inte på önskad nivå. Verksamheterna förväntar sig att stadsdelens DSO ska i helhet hantera begäran från de registrerade. Av den anledningen så har stadsdelen under hösten 2021 uppdaterat rutiner, vägledning inklusive mallar för hantering av begäran från 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
	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

Bristen berör på att verksamheternas mognads grad av hantering av begäran från registrerade. Verksamheterna har yttersta ansvar att hantera inkomna begäran, involvera stadsdelsförvaltningen DSO.

3.5.5 DSO ger råd och rekommendationer till PUA

Fortsätt uppdatera rutiner och informera verksamheter och medarbetare löpande om hantering av begäran från de registrerade.

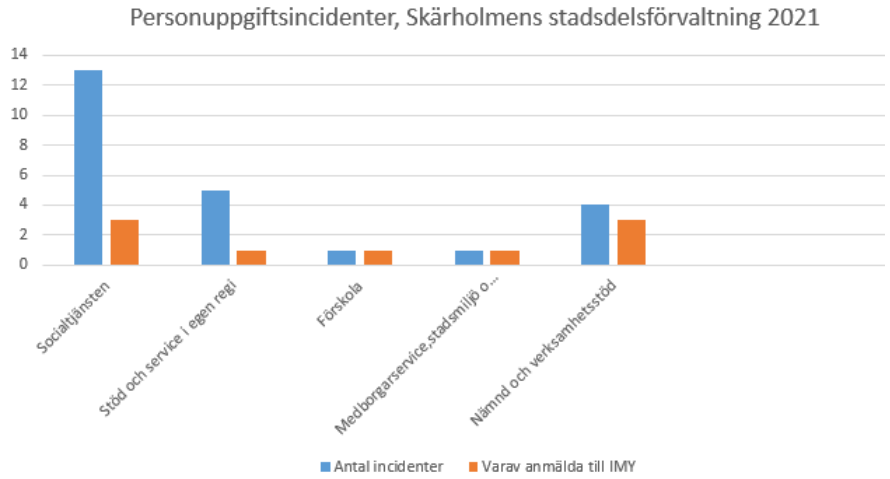
Fortsätta involvera stadsdelens DSO i hantering av inkomma begäran då DSO för in register över hur många begäran inkommit

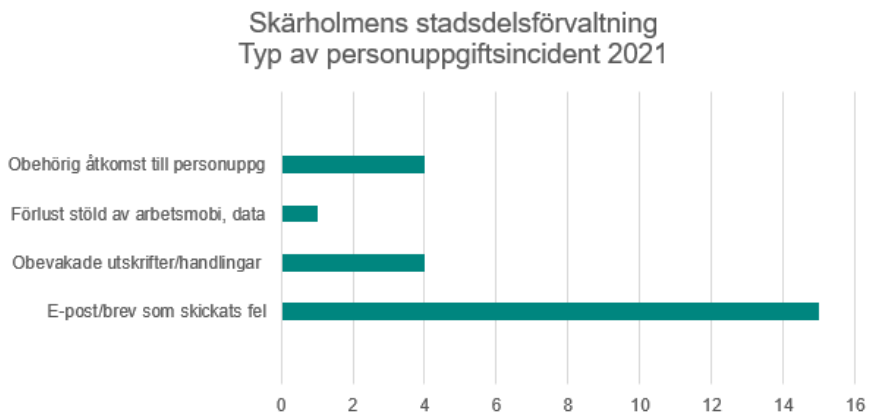
under året. Anledningen att DSO för register är att kunna följa upp att inkomna begäran hanterades inom föreskrivna trettiodagarsfristen samt att kunna rapportera om inkomna begäran i årsrapporten

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Genom att medarbetare, kunder (de registrerade), leverantör
Hur många personuppgiftsincidenter har dokumenterats?	24
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	9
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	5





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.”

I en verksamhet kan förekomma många andra typer av incidenter, som inte involverar personuppgifter. Det är viktigt att hålla den saken i åtanke, så att årsrapporteringen inte omfattar annat än just personuppgiftsincidenter. Vidare är det en grundförutsättning för hanteringen av personuppgifter att incidenter över huvud taget upptäcks, samt att verksamheten förstår att hantera incidenter som rör personuppgifter på det särskilda sätt som dataskyddsförordningen kräver.

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 DSO:s årsrapport är avsedd att fokusera på rapporteringen.

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se artikel 33). Detta innebär att de flesta personuppgiftsincidenter ska rapporteras till IMY, inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter, ska rapportering även ske till de

berörda registrerade personerna, utan dröjsmål. Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till IMY samt rapportering till de berörda personerna.

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

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

3.6.3 Resultat

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

Skärholmens stadsdelsförvaltning har väldokumenterade rutiner som beskriver vad en personuppgiftsincident är, roller och ansvar i rapporteringsprocessen samt hur man ska gå till väga för att rapportera. Skärholmens stadsdelsförvaltning i regel anmäler personuppgiftsincidenter till IMY i tid, avvikelse för år 2021 med 4 incidenter av 9 inte är rapporterade i tid är på grund av att vissa verksamheter inte följer fullt ut rutiner för arbete på distans.

Personuppgiftsincidenter som har anmälts till IMY handlar om e-post eller brev som har skickats till felmottagare, obehörig åtkomst till personuppgifter, utskrift/handlingar som har legat obevakade, förlust/stöld av arbetsmobil, data.

Skärholmens stadsdelsnämnd har beslutat i samband med införandet av Dataskyddsförordningen 2018 att :

Verksamheter anmäler personuppgiftsincident till stadsdelens dataskyddsombud

Verksamheten registyrrar personuppgiftsincident i Stockholms stads incidentrapporteringssystem IA.

Dataskyddsombud ansvarar för att upprätta dokumentation i form av utredningsrapport som innehåller dokumentation/logg över händelse, rekommendationer för åtgärder som verksamheten behöver vidta för incidenten ska inte inträffa igen samt att verksamhetsansvariga i samråd med dataskyddsombud beslutar om personuppgiftsincident ska anmälas till Integritetsskyddsmyndighet (IMY).Dataskyddsombud anmäler personuppgiftsincident till Integritetsskyddsmyndighet (IMY)

Samtliga personuppgiftsincidenter hanteras och dokumenteras på samma sätt (med viss skillnad som beskrivs nedan) oavsett om incident hanteras internt inom stadsdelsförvaltningen eller om den anmäls vidare till Integritetsskyddsmyndighet (IMY).

Skillnader mellan intern hantering av personuppgiftsincident och personuppgiftsincident som anmäls till Integritetsskyddsmyndighet (IMY)

Intern hantering av personuppgiftsincident:

Verksamheten skickar anmälan till stadsdelens dataskyddsombud

Verksamheten registrerar personuppgiftsincident i IA

Dataskyddsombud hanterar dokumentation i form av utredningsrapport som innehåller dokumentation/logg över händelse, rekommendationer för åtgärder som verksamheten behöver vidta för incidenten ska inte inträffa igen.

Dataskyddsombudet utredningsrapport skickas till berörd verksamhet, till medarbetare som är berörda av inträffad incident samt till dataskyddshandläggare och informationssäkerhetssamordnare. Vid hantering av interndokumentation som inte diarieförs uppstår begränsningar i dataskyddsombudets uppdrag utifrån arkivlagen. I stadsarkivets hanteringsanvisningar står det att handlingstypen ”Utredningar rörande incidenter som ligger utanför IA” håller på att utredas. Stadsarkivet informerar om att Turordningen är att först ska en strategi för incidentrapportering tas fram (SLK) och därefter ska St

Erik Försäkring skriva instruktioner för IA. Beslut för informationen som ligger utanför systemet kommer när vi vet hur systemet ska användas dvs vad som då faller utanför. Anledningen till turordningen är att man inom staden använt IA olika, en del har hanterat nästan allt där och andra inte.” Av den anledning och inväntan på tydliga riktlinjer från SLK, St Erik försäkring och stadsarkivet stadsdelens dataskyddsombud sparar alla utredningar i dataskyddsförordnings gruppdisk där få personer har tillgång till (dataskyddsombud, dataskyddsombudets chef)

Hantering av personuppgiftsincident som anmäls till Integritetsskyddsmyndighet (IMY):

Verksamheten skickar anmälan till stadsdelens dataskyddsombud

Verksamheten registrerar personuppgiftsincident i IA

Dataskyddsombud hanterar dokumentation i form av utredningsrapport som innehåller dokumentation/logg över händelse, rekommendationer för åtgärder som verksamheten behöver vidta för incidenten ska inte inträffa igen.

Dataskyddsombudet utredningsrapport skickas till berörd verksamhet, till medarbetare som är berörda av inträffad incident samt till dataskyddshandläggare och informationssäkerhetssamordnare.

Personuppgiftsincident som anmäls till Integritetsskyddsmyndighet (IMY) diarieförs i e-Dok och anmäls till stadsdelsnämndens sammanträdde som anmälningsärende.

Stadsdelens dataskyddsombud upprättar och ansvarar för personuppgiftsregister, register finns i dataskyddsförordnings gruppdisk.

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

Brister som är identifierade under 2021 är att fanns incidenter som inte anmäldes till IMY i tid. Bristen beror på att rutiner för arbete på distans följs inte fullt ut.

3.6.5 DSO ger råd och rekommendationer till PUA

Mognadsgraden hos medarbetarna är i hantering av personuppgifter är relativt hög.

Det är viktigt att fortsätta fokusera på ökad medvetenhet och kunskap hos verksamheter om anmälningsskyldigheten.

Viktigt att fortsätta jobba med samma budskap att det viktiga inte är vem som gjorde fel utan varför felet uppkom vid inträffad incident och att medarbetarna vågar anmäla personuppgiftsincidenter för att kunna lära va det inträffande och bli bättre framöver.

Skärholmens stadsdelsförvaltning har tagit fram ett förslag i januari 2021 på en gemensam process för hantering av utredningar inom respektive funktion, dataskyddsombud, informationssäkerhetssamordnare, lex Sarah utredare samt utredare för säkerhetsskydd för att bygga upp en gemensam process för hantering av utredningar/incidenter inom dessa områden.

Rekommendationen är att Skärholmens stadsdelsförvaltning fastställer förslag och skapar en gemensam process för hantering av utredningar/incidenter.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- ***Granskning 1*** Granskning/kontroll gällande hantering av samtyckesblanketter i samband med region Stockholms planering av vaccinationen mot Covid -19.
- ***Granskning 2*** Granskning/kontroll av hantering av personuppgifter i e-post
- ***Granskning 3*** Granskning/kontroll av behörighetshantering
- ***Granskning** 4* Granskning Efterlevnad av Schrems II/Privacy shield
- ***Granskning 5*** Granskning av att personuppgiftsbiträdesavtal (PuB)

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 1 *Granskning/kontroll gällande hantering av samtyckesblanketter i samband med region Stockholms planering av vaccinationen mot Covid -19.*

	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

Granskningen avser verksamheternas hantering av
- hur samtycket inhämtades,
- när samtycke inhämtades
- vilken information som gavs den registrerade
- registrering av inkomna samtycke i systemet
- förvaring av inkomna samtycke

Stockholms stad har tagit fram en samtyckesblankett som enskilda inom riskgrupper skulle ha möjlighet att skriva på. Den enskilde ger då sitt samtycke till att staden lämnar uppgifter om namn, adress och vilken insats enskilde har. Skärholmens stadsdelsförvaltning var behjälplig med att inhämta samtycke från enskilda som tillhör Skärholmens stadsdelsförvaltning.
Inhämtade samtyckeblanketter har levererats till beställarenheten för journalföring i Sociala system. Original påskrivna blanketter har skickats vidare till region Stockholm.

Granskningen påvisar brister i hantering då det är flera som är inblandade i inhämtning av samtycke. Skärholmens stadsdelsförvaltning var ”mellanhand” för inhämtning.
Stockholms stad behöver ha mer tydligt information och rutiner vid denna typ av inhämtning av samtycket. Se över vad ligger personuppgiftsansvar för hantering av samtyckesblankett och tydligt beskriva vad som gäller, hur samtycke ska dokumenteras, hanteras, förvaras.

Granskning 2 *Granskning/kontroll av hantering av personuppgifter i e-post*

	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

Granskningen har påvisat att verksamheter skickar olika bifogade filer via e-post som innehåller personuppgifter. Hantering av filer som innehåller personuppgifter är inte unik för en specifik verksamhet. Filer i stort sätt hanteras på samma sätt i övriga verksamheter. Filer vars åtkomst är behörighetsstyrd och som innehåller personuppgifter ska aldrig mailas ut, utan eventuell uppdatering som är gjord i filer ska hänvisas till filenslagringplats med rätt behörighet.

Efter granskningen och utredningen DSO rekommenderar att

- Avdelningsansvariga behöver se över /utreda gränsdragning mellan avdelningar, medarbetarnas uppdrag och ansvar i samband med hantering av personuppgifter
- Verksamheterna ser över arbetssätt
- Ha tydlig beskrivning av syfte för behandling av personuppgifter där verksamheterna anser att de måste ha i olika uppföljningsfiler och inte maila dessa filer.

Berörd verksamhet har vidtagit följande åtgärder

- Verksamheten har granskat behörighet till filer/gruppdiskar och åtgärdat felaktiga behörigheter
- Verksamheten har även strukturerat filer/gruppdiskar på ett annat sätt som uppfyller dataskyddsförordningens krav

Verksamheten har genomfört konsekvensbedömning för personuppgiftsbehandling/filer/gruppdisk

Granskning 3 *Granskning/kontroll av behörighetshantering*

	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

En central del i arbetet med informationssäkerhet och dataskydd handlar om behörighetsstyrning. Alla verksamheter som hanterar personuppgifter behöver ha stabila rutiner för att säkerställa att

behörigheter tilldelas korrekt, att behörigheterna löpande kontrolleras och följs upp samt att åtkomstkontroller genomförs.

I granskning av behörighetshantering framkom tydligt att det är väldigt många medarbetare som tilldelas behörigheter ”i fall att” och ” det är bra att ha”. Behörighetshantering är en personuppgiftsbehandling och ovan nämnda orsaker till tilldelning av behörigheter är inte tillåtna.
Efter genomförd granskning stadsdelens dataskyddsombud skickade mail till samtliga chefer om hantering av behörigheter samt uppmaning att:
-ansvariga ser över behörighetshantering
-tilldela behörigheter enbart till personer som tillhör enheten och utifrån uppdrag aktivt jobbar i systemet, gruppdiskar m m
-behörighet beställs/godkänns av ansvarig chef och inte av medarbetare själv
- man får inte ha stående behörigheter som t ex ersättare vid frånvaro, utan man lägger in ersättare/tillfälligt behörighet under tiden en chef eller medarbetare är frånvarande.
-man ska ta bort behörigheter för medarbetare som har slutat sin anställning inom en specifik verksamhet eller i stadsdelen.
-ha regelbundna kontroller av behörighetshantering inom verksamheter.

Granskning 4 *Efterlevnad av Schrems II/Privacy shield*

	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

Privacy Shield är ett avtal mellan EU-kommissionen och den amerikanska handelskammaren som tillåtit överföringar av personuppgifter till mottagare i USA.

Ogiltigförklarandet innebär att Privacy Shield inte ger ett tillräckligt skydd för de personuppgifter som förs över till USA – en sådan överföring bryter nu mot Dataskyddsförordningen (GDPR).

Under 2021 genomförde Skärholmens stadsdelsförvaltning kartläggningen av tjänster som används i verksamheter och identifierat vilka tjänster som för över eller behandlar personuppgifter i USA/tredjeland. Verksamheterna har fått granskningsresultat och DSO.S rekommendation för åtgärder.

Flertal verksamheter genomförde riskanalys över personuppgiftsbehandlingar där överföring till tredjeland förekommer.

Granskning 5 *Granskning av att personuppgiftsbiträdesavtal (PuB)*

	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

Under 2021 genomförde Skärholmens stadsdelsförvaltning kartläggning av leverantörer och personuppgiftsbiträdesavtal (PuB). Granskningen påvisar oklarhet vem som ska huvudansvar för uppföljning av PuB avtal. Yttersta ansvaret enligt dataskyddsförordningen för PuB avtal ligger hos ansvarig verksamhet, men samtidigt har stadsdelen strateg för uppföljning av avtal och där uppkom oklarhet om stadsdelen ska ha strategen ska ha uppföljnings ansvar av samtliga PuB avtal.
Granskningen lede till att uppdatera och skriva nya PuB avtal med instruktioner.

4.4 DSO ger råd och rekommendationer till PUA

- Skärholmens stadsdelsförvaltning har kommit långt i implementation av rutiner för säker personuppgiftshantering.

Nästa steg för att stärka säker personuppgiftshantering är

- Att granskning av behörighetshantering sker regelbundet i verksamheter och att granskningen blir en del av verksamheternas internkontroll.
- Att fortsätta arbeta med efterlevnad av Schrem II , genomföra riskanalyser av personuppgiftsbehandlingar vid förekomst av överföring av personuppgifter till tredje land.
- Att fortsätta med regelbunden kontroll av PuB avtal och besluta vem som ansvarar för uppföljningen/kontroll

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- ***Risk 1*** Brist på kunskap om konsekvensbedömning och 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 *Brist på kunskap om konsekvensbedömning och konsekvensbedömning*

	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

Identifierande brister i kunskap om konsekvensbedömningen och informationsklassning anses som risk då verksamheterna inte har tydligt bild av kravet på att utföra konsekvensbedömning och informationsklassning. Verksamheterna brister i att genomföra konsekvensbedömning och informationsklassning vid införandet av nya tjänster och system. Konsekvensbedömningen och informationsklassning bör påbörjas så tidigt som det är praktiskt möjligt vid utformningen av behandlingen, även om vissa delar av behandlingen fortfarande är okända.
Det saknas tydligt definiering om roller och skyldigheter i samband med konsekvensbedömning och informationsklassning.

5.4 DSO ger råd och rekommendationer till PUA

Konsekvensbedömningen och informationsklassning bör påbörjas så tidigt som möjligt vid utföringen av behandlingen, även om vissa delar av behandlingen förfarande är okända och att genomförandet av en konsekvensbedömning och informationsklassning är pågåendeprocess, inte ett förfarande som vid ett enda tillfälle.

Trots tydliga rutiner så behövs fortsatta information och utbildningar för konsekvensbedömningar och informationsklassningar. PuA ska se till att det finns tydlig dokumentation med beskrivning av roller och skyldigheter, verksamheternas ansvar för genomförandet av konsekvensbedömningar och informationsklassningar.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- ***Område 1*** Kontroll av genomförda (obligatoriska) webbutbildningar i dataskydd och informationssäkerhet

- ***Område 2*** Genomföra kartläggning av mognadsgrad i dataskyddsfrågor på alla nivåer i organisationer

6.2 Syfte

Som nämnts ovan är det granskande arbetet en av dataskyddsombudets viktigaste uppgifter. Eftersom dataskyddsombudet ofta har begränsat med tid, behöver granskningsplanen för det nya året utformas med eftertanke. Som en tumregel bör två-tre granskningar ses som en rimlig granskningsinsats under ett verksamhetsår. Granskningsområdena bör lämpligen väljas utifrån ett *riskbaserat synsätt*, det vill säga att fokus bör ligga på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Därigenom åstadkoms 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 *Kontroll av genomförda (obligatoriska) webbutbildningar i dataskydd och informationssäkerhet*

Grundkurs i dataskydd är obligatoriskt för Stockholms stads medarbetare. E-utbildning finns på stadens utbildningsplattform. Grundkursen fokuserar på det allra viktigaste om personuppgiftsbehandlingen.
Eftersom utbildningen är obligatoriskt så har Stockholms stad tagit fram ett underlag till samtliga stadsdelsförvaltningar för att kunna följa upp medarbetarnas genomförande av utbildningen. Skärholmens stadsdelsförvaltnings DSO har följt upp medarbetarnas genomförande av utbildningen samt rapporterat till verksamhetsansvariga lägesrapporter. Uppföljning har skett regelbundet under 2018 och 2019 tills det har uppstått problem med underlag och då rapporterna inte levererandes till stadsdelsförvaltningen. Rapporter slutade levereras i slutet av 2020 till och med november 2021. Underlag och rapporter har uppdaterats och utskick av rapporter underlag påbörjades igen i december 2021. Rekommendationen är att återuppta uppföljningen då leverans av rapporter/underlag har uppdaterats.

Granskning 2 Genomföra kartläggning av mognadsgrad i dataskyddsfrågor på alla nivåer i organisationer

Stadsdelens DSO hade plan under 2021 att genomföra kartläggning av mognadsgrad i dataskyddsfrågor på alla nivåer i organisationer i form av en enkät, men arbetet blev inte genomförd på g a den rådande situationen med pandemi.

Enkäten borde ha några frågeställningar om dataskydd och personuppgiftsbehandlingar inom respektive verksamhet.

Samanställningen av enkät borde göras på avdelnings- och enhetsnivå. Återapporteringen till stadsdelsförvaltningens ledning.

7 Övrigt att rapportera

7.1 Sammanfattning

- ***Observation 1*** Skärholmens stadsdelsförvaltning bedöms delvis arbeta ändamålsenligt för att uppfylla de krav och regleringar som införts i och med dataskyddsförordningen.

- ***Observation 2*** Ändamålsenlig kontroll och uppföljning av arbetet med dataskyddsförordningen

7.2 Syfte

Avsikten med denna punkt i årsrapportmallen är att ge möjlighet att komplettera bilden av statusen i dataskyddsarbetet. Under denna rubrik kan anges sådant som inte på ett naturligt sätt tas upp under någon av punkterna i rapporteringsstrukturen ovan, eller som inte heller ryms i den inledande sammanfattningen (som ju enbart bör innehålla de två-tre allra mest centrala observationerna eller händelserna från det gångna året).

7.3 Övriga observationer

Observation 1 *Skärholmens stadsdelsförvaltning bedöms delvis arbeta ändamålsenligt för att uppfylla de krav och regleringar som införts i och med dataskyddsförordningen.*

Skärholmens stadsdelsförvaltning uppvisar stor kunskap samt höga ambitioner inom arbetet med dataskyddsförordningen. Mognadsgraden beskrivs som genomsnittlig då återstår vissa komponenter innan arbetet kan beskrivas som ändamålsenligt, exempelvis bättre implementering av genomförande av konsekvensbedömning och informationsklassning samt ännu bättre uppföljning av leverantörer och PuB avtal.

***Observation 2** Ändamålsenlig kontroll och uppföljning av arbetet med dataskyddsförordningen*

Skärholmens stadsdelsförvaltning bedöms inte ha en ändamålsenlig kontroll och uppföljning med avseende dataskyddsförordningen. Det återstår visstarbete med att skapa en strukturerad granskningsplan på verksamhetsnivåer och att dataskyddskontroll bör vara en naturlig del i stadsdelens internkontrollplan. Men Skärholmen utför ambitiöst arbete och är på god väg att helt uppfylla de krav och regleringar som införs.

7.4 DSO ger råd och rekommendationer till PUA

Skärholmens stadsdelsförvaltning har en genomsnittlig mognadsgrad i dataskyddsförordningen. Överlag bedöms mognadsgraden vara högst inom hantering av personuppgiftsincidenter.

Den viktigaste förbättringspunkten är att upprätta mer formaliserade rutiner för granskning av efterlevnad. Syftet är att minska risker för otillbörlig behandling av personuppgifter på grund av att man missat efterlevnad.

Rekommendationer är att Skärholmens stadsdelsförvaltning ska fortsätta jobba vidare med inom området utbildning och medvetenhet, samt med rutinerna för att genomföra konsekvensbedömningar och informationsklassningar på befintliga personuppgiftsbehandlingar.

Tydliggöra att dataskyddsombud inte själv ska implementera arbetet utan kontrollera och ge råd och stöd. Detta är sällan fullt ut praktiskt då denna funktion oftast har bäst insyn i själva frågeställningarna

och sett behoven av en åtgärd. För at få ett bra dataskyddsarbete och att den blir en del av vardagliga arbetet krävs dock att fler blir involverade i hela organisationen.

DSO rekommenderar att när krisen med pandemi är över att återuppta informationsspridning till stadsdelsförvaltningens ledningsgrupp och chefsforum. Även kortare utbildningar hållna av DSO behöver genomföras löpande under året.

DSO rekommenderar också att nämnden, som är formellt personuppgiftsansvarig, får utbildning årligen i dataskyddsförordningen. Det är lämpligt om detta finns som schemalagt ärende i nämndens årshjul så att det sker med kontinuitet.