Stockholms stad

Dnr ÖST 2022/38 Bilaga 8

GDPR Årsrapport

2021

Östermalms stadsdelsnämnd

GDPR årsrapport 2021

Dnr: ÖST 2022/38
Utgivningsdatum: 2022-01-21
Kontaktperson: Ulrika Josephson Westberg

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). Dataskyddsombudet har till uppgift att övervaka verksamhetens integritets- och dataskyddsregelefterlevnad samt att ge rekommendationer och rapportera direkt till högsta förvaltningsnivå. Dataskyddsombud för Östermalms stadsdelsnämnd är Ulrika Josephson Westberg.

Denna årsrapport är ett medel för nämnd och styrelse att ta emot de råd och rekommendationer som dataskyddsombudet är skyldig att ge till ansvarig enligt dataskyddsförordningen samt för att få insyn i dataskyddsombudets 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 och rekommendation

Under året har arbetet med att genomföra klassning av stadsdelens informationstillgångar fortsatt. Förvaltningen har även tillsammans med övriga stadsdelar deltagit i utvecklingsarbete kring att genomföra normerande informationsklassningar. Resultatet från klassningarna kommer att ligga till grund för förvaltningens fortsatta arbete med hantering av informationstillgångarna.

Avdelningarna har gått igenom sina behandlingar av personuppgifter i stadsdelens registerförteckning och har vid behov reviderat uppgifterna. Under året har ett arbete påbörjats för att föra över informationen i registerförteckningen från exel-listor till ett digitalt verktyg som underlättar överblick och uppdateringar.

Förvaltningens chefer och medarbetare har uppmanats att digitalt genomföra stadens webbutbildning gällande informationssäkerhet, och antalet medarbetare som har genomgått utbildningen har ökat påtagligt under året.

Förvaltningen har applicerat ett allt mer systematiskt informationssäkerhets- och dataskyddaarbete genom att identifiera risker och koppla ihop internkontroll, löpande identifiering av risker och planering för kommande aktiviteter i årshjul och verksamhetsplan.

Ett större fokus i samhället på informationssäkerhetsfrågor har skapat en allt större medvetenhet i förvaltningen kring dataskyddsfrågor, och det finns en vilja hos chefer och medarbetare att göra rätt. Dataskyddsfrågorna kan dock upplevas som komplexa och inte helt enkla att applicera i verksamheten. Inte minst är detta tydligt när det gäller de begränsningar som finns kring överföring av personuppgifter till tredje-land vilket påverkat förvaltningens hantering av till exempel sociala medier.

Mycket arbete är genomfört eller påbörjat, men det återstår åtgärder för att förvaltningen i ännu högre grad ska uppnå kraven i dataskyddsförordningen. Utifrån rapportens resultat rekommenderas nämnden att ge förvaltningen i uppdrag att upprätta en handlingsplan för att åtgärda de brister som påtalats. Handlingsplanen föreslås anmälas till nämnden i samband med

tertialrapport 1 och följas upp i tertialrapport 2 och verksamhetsberättelsen för 2022.

Handlingsplanen bör ta i beaktande följande:

- Förvaltningen bör utveckla sin organisation för dataskyddsfrågorna. Det är först när dataskyddsarbetet sprids från den centrala förvaltningen till verksamheterna som efterlevnad och åtgärder får ordentligt genomslag och de rekommendationer som har getts i denna rapport kan genomföras
- Uppgifterna i registerförteckningen behöver kompletteras och det påbörjade arbetet med överföringen av förteckningen till digitalt verktyg slutförs under 2022. De funktioner som fortsättningsvis ska arbeta med att hålla förteckningarna uppdaterade får utbildning i verktyget.
- Att medarbetare har en grundläggande kunskap om informationssäkerhet inklusive dataskyddsförordningen är centralt för att förvaltningen ska kunna uppnå och upprätthålla en god informationssäkerhet. Förvaltningens utbildningsinsatser bör därför fortsätta.
- Det systematiska informationssäkerhetsarbetet bör fortsätta och utvecklas genom att följa upp informationsklassningar och genomföra övriga analyser som syftar till att nämndens information omfattas av den säkerhet informationen kräver.
- Förvaltningen bör ytterligare uppmärksamma att det kan finnas behov av att genomföra konsekvensbedömningar och informera om stadens webbutbildning om konsekvensbedömningar.
- Flertalet personuppgiftsincidenter beror på att medarbetare skickat papperspost eller e-post till fel mottagare. Förvaltningen bör påminna om stadens e-postregler och vikten av korrekt hantering av utskick

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

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	524
Har nödvändiga uppdateringar gjorts?	Ja
Bedöms registerförteckningen vara fullständig?	Registerförteckningen bedöms i allt väsentligt vara fullständig
Har verksamheten lämpliga rutiner för registerföring?	Rutiner kan utvecklas

3.1.2 Syfte

Dataskyddsförordningens artikel 30 ställer krav på att inventera alla personuppgifter som hanteras och dokumentera dem i en så kallad registerförteckning.

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.

3.1.3 Resultat

Registerförteckningen upprättades inför införandet av Dataskyddsförordningen i maj 2018. Sedan dess har förteckningen uppdaterats löpande. Förteckningen är upprättad i en exel-fil som togs fram av staden inför införandet av dataskyddsförordningen. Under hösten 2020 och våren 2021 har samtliga avdelningar gått igenom sina behandlingar i registerförteckningen och vid behov reviderat uppgifterna.

Totalt har 524 granskningar registrerats i förteckningen. Granskning av förteckningen visar att det i vissa fall finns behov av kompletterande information kring till exempel säkerhetsåtgärder, personuppgiftsbiträdesavtal m.m.. Registerförteckningen bedöms

dock i allt väsentligt omfatta de personuppgifter som hanteras och innehålla de obligatoriska uppgifterna.

Under året har ett arbete påbörjats för att föra över informationen från exel-listor till ett digitalt verktyg kallat Draftit som används av staden. En liten del av informationen är än så länge överförd. Systemet består av ett frågeformulär för varje personuppgiftsbehandling och fungerar därmed även som en checklista att alla krav i GDPR dokumenteras korrekt. Eftersom förteckningen i Draftit inte är komplett har granskningen skett av uppgifternas som är registrerade i exel-filerna.

3.1.4 Dataskyddsombudet anger hur allvarliga bristerna är på en skala

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

3.1.5 Dataskyddsombudet ger råd och rekommendationer till personuppgiftsansvarig

Arbetet med registerförteckningen behöver vara ett ständigt pågående arbete. Granskningen visar att det finns behov av att komplettera uppgifterna i förteckningen. Kraven på dokumentation har utvecklats sedan den initiala förteckningen togs fram vilket medför att informationen om varje behandling kommer att behöva utvecklas jämfört med den nuvarande förteckningen. Förteckningen behöver kompletteras med uppgifter om bland annat vem som är ansvarig för respektive behandling, förekomst av personuppgiftsbiträdesavtal, kontroll av ev. tredje-landsöverföringar, informationsklassningar och skyddsåtgärder.

Sammanställningen är uppbyggd utifrån de processer som beskrivs i stadsdelarnas gemensamma hanteringsanvisningar vilket är bra. Det skapar ett logiskt samband med avdelningarnas informationshantering och ger möjligheter till samordning med till

exempel årlig översyn av hanteringsanvisningarna som styr förvaltningens hantering av dokumentation. Förteckningen innehåller dock flera registreringar av samma typ av behandlingar vilket bör samordnas för att minska antalet registrerade behandlingar, och därmed skapa bättre överblick i förteckningen.

Av förvaltningens rutiner framgår att varje chef ansvarar för att anmäla nya, uppdaterade och avslutade personuppgiftsbehandlingar. I samband med att verktyget Drafit tas i drift kommer det finnas behov av att varje avdelning utser en funktion som kan registrera och uppdatera avdelningens personuppgiftsbehandlingar i verktyget. Därigenom bör förvaltningen kunna säkerställa att den löpande uppdateringen av registerförteckningen fungerar tillfredställande.

Registerförteckningen är ett grundläggande verktyg för verksamheterna att ha överblick över sina personuppgifts-behandlingar och att i samband med uppdateringar värdera och se över sina behandlingar och säkerhetsåtgärder. Det är därför av stor vikt att arbetet med att överföra och komplettera informationen slutförs under 2022, samt att de funktioner som fortsättningsvis ska arbeta med att hålla förteckningarna uppdaterade får utbildning i verktyget.

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?	Nej

3.2.2 Syfte

Genom styrdokument kommunicerar personuppgiftsansvarig 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).

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

3.2.3 Resultat

På intranätet finns en sida med rubriken GDPR på Östermalm med samlad information för chefer och medarbetare. Utöver informationen som är sammanställd för förvaltningens chefer och medarbetare finns länkar till stadens övergripande information och styrande dokument. Ett urval av dokumentationen:

- Rutin för hantering av personuppgiftsincident samt checklista

- Checklista för rensning av e-post
- Vägledning vid de registrerades begäran om tillgång, rättelse och radering av personuppgift
- Mallar för konsekvensbedömning, riskbedömning

Utöver rutindokument finns utförligt informationsmaterial på intranätet med instruktioner för vad verksamheten bör uppmärksamma och utföra. Till exempel kan nämnas informationsmaterialet ”GDPR i korthet för dig som chef” och ”GDPR i korthet för dig som medarbetare”. Det finns även hänvisningar till stadens gemensamma information på intranätet.

Sammanfattningsvis bedöms det finnas grundläggande styrdokument och informationsmaterial lättillgängligt på intranätet. Överlag är texterna anpassade till målgruppen. Inom områdena konsekvensbedömningar och riskbedömningar finns dock behov av kompletterande material för att underlätta för verksamheterna att genomföra dessa aktiviteter när behov finns av dessa.

Det framgår dock inte ägare på alla styrdokument vilket det bör göra för att dessa ska hållas uppdaterade över tid.

3.2.4 Dataskyddsombudet anger hur allvarliga bristerna är på en skala

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

3.2.5 Dataskyddsombudet ger råd och rekommendationer till personuppgiftsansvarig

Det finns relevanta och uppdaterade styrdokument. Det bör dock utses ägare till respektive styrdokument och anges på dokumenten när de senast reviderades.

Under 2021 har återkommande påminnelser gjorts i förvaltningens informationsbrev till samtliga chefer om vikten av att ta del av och sprida information om rutiner m.m. till sina medarbetare. Arbetet med att informera om rutiner m.m. behöver ständigt pågå.

Det behöver också tas höjd för att alla inom verksamheterna inte har åtkomst till datorer och intranät regelbundet och att information inte når fram till alla medarbetare den vägen. Det är viktigt att nå ut med relevant information även till dessa grupper och där bör lämpliga åtgärder övervägas i dialog med verksamheterna.

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?	7
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av Sveriges kommuner och regioners verktyg KLASSA. Stadsdelsförvaltningen ansvarar för att informationssäkerhetsklassa alla sina informationsmängder. Utan informationsklassningen har

verksamheten inte förutsättningar att välja rätt åtgärder för att skydda sin information. Det är därför av stor betydelse för dataskyddsarbetet att personuppgiftsansvarig ges en uppdaterad bild varje år av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar.

Eftersom informationsklassning är ett arbete som görs inom ramen för informationssäkerhetsarbetet, har denna del av granskningen utförts i samarbete med informationssäkerhetssamordnaren.

3.3.3 Resultat

Förvaltningen har informationsklassat 7 behandlingar. Klassningarna är inte mer än två år gamla. Under året har förvaltningen medverkat i stadens gemensamma klassningsarbete inom ramen för de behandlingar som kan ha kopplingar till NIS-direktivet där flertalet normerande klassningar har genomförts. Genom att genomföra normerande klassningar samarbetar stadsdelsförvaltningarna i syfte att underlätta klassningsarbetet för behandlingar som ser liknande ut i staden. Stadsdelarna kan använda varandras klassningar som utgångspunkt vid sin egen informationsklassning vilket innebär en effektivare hantering än att alla gör samma omfattande arbete.

Granskningen visar att förvaltningen har påbörjat ett arbete med att informationsklassa sina behandlingar, men att det återstår mycket arbete med att utföra klassningar.

Det finns inte utsedda informationsägare för behandlingarna vilket sannolikt påverkar antalet genomförda klassningar.

3.3.4 Dataskyddsombudet 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 Dataskyddsombudet ger råd och rekommendationer till personuppgiftsansvarig

Förvaltningen bör ta fram en plan för de klassningar som ska genomföras fortsättningsvis och i vilken ordning de ska prioriteras. Av planen behöver framgå vem som är informationsägare för respektive behandling. Informationsägarens ansvar blir att tillse att rätt kompetens deltar vid klassningar och att klassningarna blir genomförda. Arbetet med att genomföra klassningar bör intensifieras under året. Förutom att klassningarna ger underlag för åtgärder för att skydda information ger de också värdefull information om eventuella behov av justerade rutiner, sätt att registrera och använda information, behörighetskontroller med mera.

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?	

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 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

Konsekvensbedömning är ett område där kunskapen behöver ökas bland berörda medarbetare. För att bli ett effektivt verktyg behöver kravet på konsekvensbedömning fångas upp tidigt i berörda processer som exempelvis upphandling. Stadsdelsförvaltningen har deltagit i stadsdelsgemensamma konsekvensbedömningar som har genomförts för delar av skolplattformen samt delar av sociala system.

3.4.4 Dataskyddsombudet 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

3.4.5 Dataskyddsombudet ger råd och rekommendationer till personuppgiftsansvarig

I samband med kompletteringen av registerförteckningen bör även tydliggöras om konsekvensbedömningar behöver genomföras för behandlingarna.

Informationen på stadsdelens intranätsida har under året uppdaterats med underlag för genomförande av konsekvensbedömningar, och staden erbjuder även webbutbildning i att genomföra dessa bedömningar. Förvaltningen bör ytterligare uppmärksamma att det kan finnas behov av att genomföra konsekvensbedömningar och informera om stadens webbutbildning inom området.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	0
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	

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 är 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 dock 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.

3.5.3 Resultat

Under året har ingen begäran om registerutdrag, begränsning eller radering inkommit. Förvaltningen har rutiner för hur begäran ska hanteras. Via stadens hemsida hänvisas medborgare att kontakta dataskyddsombudet vid dataskyddsrelaterade frågor. Dataskyddsombudet förmedlar därefter ev. frågor om registerutdrag med mera vidare i organisationen för hantering.

3.5.4 Dataskyddsombudet anger hur allvarliga bristerna är på en skala

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

3.5.5 Dataskyddsombudet ger råd och rekommendationer till personuppgiftsansvarig

Stadsdelsförvaltningen har tydliga rutiner på intranätet för hur individens rättigheter ska omhändertas för registerutdrag. Kunskapen om rättigheterna och befintliga rutiner bör dock säkerställas bland berörda medarbetare.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Vanligtvis genom anställd eller utomstående/registrerad informerar förvaltningen
Hur många personuppgiftsincidenter har dokumenterats?	12
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?	7

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.”

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 Integritetsskyddsmyndigheten (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.

3.6.3 Resultat

Under året har 12 incidenter rapporterats i förvaltningen varav 9 incidenter har anmälts till Integritetsskyddsmyndigheten (IMY). Av de 9 incidenterna har 7 incidenter anmälts i tid (inom 72 timmar

från upptäckt av incidenten). När det gäller de två incidenter som inte anmäldes i tid berodde fördröjningen i den ena fallet på att det inledningsvis var oklart om det hade inträffat en incident och i det andra fallet berodde det på att verksamheten inte hade uppmärksammat att anmälan skulle göras inom 72 timmar från upptäckt av incidenten.

Tre av incidenterna berör socialtjänsten, tre berör äldreomsorgen, två berör förskolorna och en incident berör den centrala förvaltningen.

En av incidenterna är systemrelaterad medan övriga incidenter handlar om bristande rutiner eller handhavandefel. I dessa fall handlar merparten om att handlingar har skickats till fel motpart eller att e-post har skickats till fel mottagare.

Samtliga incidenter utom en bedöms som begränsade i allvarlighetsgrad i anmälningarna till IMY. Incidenterna har berört få personer och åtgärder har snabbt vidtagits för att minimera effekterna. En av incidenterna är systemrelaterad och berör flera förvaltningar och har bedömts som mer betydande i allvarlighets-grad. Även här har åtgärder vidtagits för att snabbt minimera effekterna och att incidenten inte ska upprepas. I de fall det har bedömts relevant har registrerade informerats om det inträffade.

Integritetsmyndigheten har beslutat att avsluta 7 anmälningar utan åtgärd. För 2 anmälningar har myndigheten ännu inte fattat något beslut.

Det finns information på intranätet om hur verksamheterna ska gå tillväga för att utreda och anmäla personuppgiftsincidenter. En checklista vägleder verksamheten om vilken information som behöver tas fram för att hantera incidenten. Av delegationsordningen framgår vilken funktion som anmäler personuppgiftsincidenter.

De tre incidenter som dokumenterats men inte anmälts till IMY har bedömts vara mycket begränsade och inte medföra någon skada för registrerade. Dokumentation har skett i syfte att uppmärksamma behov av översyn av rutiner.

3.6.4 Dataskyddsombudet anger hur allvarliga bristerna är på en skala

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

3.6.5 Dataskyddsombudet ger råd och rekommendationer till personuppgiftsansvarig

Kunskapsnivån hos chefer och nyckelpersoner bedöms som relativt god. Vid inträffade incidenter vidtas åtgärder snabbt och verksamheterna genomför aktiviteter för att minska risken att incidenterna inträffar igen. Kunskap om vad som betraktas som en personuppgiftsincident och hur man hanterar dessa är dock en färskvara och förvaltningen bör kontinuerligt arbeta med att höja kunskapsnivån hos alla medarbetare. Det kan till exempel göras genom att samtliga medarbetare genomgår informationssäkerhets-utbildningen på intranätet. För medarbetare som inte har kontinuerlig tillgång till intranätet bör alternativ lättillgänglig information om att upptäcka och anmäla personuppgiftsincidenter övervägas.

Flertalet incidenter beror på att medarbetare skickat papperspost eller e-post till fel mottagare. Förvaltningen bör påminna om stadens e-postregler och vikten av korrekt hantering av utskick.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- *Registerförteckning*
- *Styrdokument*
- *Kunskapsnivå*

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 personuppgiftsansvarig 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 resultat

4.3.1 Granskning 1 Registerförteckning

Granskningen visar att det finns behov av att komplettera uppgifterna i registerförteckningen med uppgifter om bland annat informationsklassningar och skyddsåtgärder. Förteckningen innehåller flera registreringar av samma typ av behandlingar vilket bör samordnas för att minska antalet registrerade behandlingar, och därmed skapa bättre överblick i förteckningen. Det är av stor vikt att arbetet med att överföra och komplettera informationen i verktyget Draftit slutförs under 2022, samt att de funktioner som fortsättningsvis ska arbeta med att hålla förteckningarna uppdaterade får utbildning i verktyget.

Se ytterligare beskrivning och bedömning i avsnitt 3.1.

	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

4.3.2 Granskning 2 Styrdokument

Granskning visar att styrdokument för dataskydd och informationssäkerhet har uppdaterats och kompletterats under året.

Se ytterligare beskrivning och bedömning i avsnitt 3.2.

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

4.3.3 Granskning 3 Kompetensutveckling

Stockholms stad erbjuder i sin utbildningsportal på intranätet en grundläggande informationssäkerhetsutbildning där även dataskyddsfrågor berörs. Utbildningen är obligatorisk för att anställda att genomgå. I oktober månad har 43 % av medarbetarna påbörjat eller genomgått den obligatoriska grundutbildningen om informationssäkerhet vilket kan jämföras med 11 % i mars. Det har således skett en markant förbättring under året.

Förvaltningen skickar ut information till chefer med många anställda några gånger per år med statistik så att de vet vilka hos sig som har genomgått utbildningen. För de enheter med många

timanställda som inte kommer in i systemet uppmanar förvaltningen verksamheterna att gå igenom utbildningen tillsammans vid t ex arbetsplatsträffar.

	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

4.4 Dataskyddsombudet ger råd och rekommendationer till personuppgiftsansvarig

Arbetet med komplettering av registerförteckningen bör fortsätta och intensifieras vilket kommenterats vidare i avsnitt 3.1

Att medarbetare har en grundläggande kunskap om informationssäkerhet inklusive dataskyddsförordningen är centralt för att förvaltningen ska kunna uppnå och upprätthålla en god informationssäkerhet. Förvaltningens utbildningsinsatser bör därför fortsätta.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker som identifierats inom verksamheten:

- Informationsklassificering – digitala system hanteras inte på ett säkert sätt
- Personuppgiftsincidenter - inträffad personuppgiftsincident har inte identifierats och rapporterats inom 72 timmar vilket kan medföra att åtgärder inte sätts in och händelsen upprepas.
- Registerförteckning – personuppgifter hanteras felaktigt
- Behörighetsadministration – personer har felaktiga behörigheter till olika verksamhetssystem och gruppdiskar

- Konsekvensbedömningar – personuppgiftsbehandlingar inleds utan att alla konsekvenser utifrån GDPR är kartlagda och hanterade.
- Personuppgiftsbiträdesavtal – risk att personuppgifterna hanteras utan att ansvarsfrågan för hanteringen är reglerad.

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

Risker inom dataskydd och informationssäkerhet har analyserats i det systematiska internkontrollarbetet och för 2022 har följande risker identifierats och dokumenterats i förvaltningens risk- och väsentlighetsanalys. Sannolikheten bedöms i en femgradig skala från mycket sannolik till osannolik, och konsekvenserna bedöms på en femgradig skala från mycket allvarlig till försumbar.

Risk 1
Informationsklassificering – bristande kontroll över vilken information som hanteras och hur den ska skyddas.
Risken har bedömts som mindre sannolik och konsekvensen som kännbar. Risken tas om hand i arbetet med egenkontroller i den systematiska interkontrollen.

Risk 2
Personuppgiftsincidenter - inträffad personuppgiftsincident har inte identifierats och rapporterats inom 72 timmar vilket kan medföra att åtgärder inte sätts in och händelsen upprepas.
Risken har bedömts som mindre sannolik att den inträffar och konsekvensen som kännbar. Risken tas om hand i arbetet med egenkontroller i den systematiska interkontrollen.

Risk 3

Registerförteckning – personuppgifter hanteras felaktigt
Risken har bedömts som mindre sannolik att den inträffar och konsekvensen som kännbar. Risken tas om hand i arbetet med egenkontroller i den systematiska interkontrollen.

Risk 4
Behörighetsadministration – personer har felaktiga behörigheter till olika verksamhetssystem och gruppdiskar. Risken har bedömts som möjlig och konsekvensen som kännbar. Risken tas om hand i arbetet med egenkontroller i den systematiska interkontrollen

Risk 5
Konsekvensbedömningar – personuppgiftsbehandlingar inleds utan att alla konsekvenser utifrån GDPR är kartlagda och hanterade. Risken har bedömts som möjlig och konsekvensen som kännbar. Risken tas om hand i arbetet med egenkontroller i den systematiska interkontrollen

Risk 6
Personuppgiftsbiträdesavtal – risk att personuppgifterna hanteras utan att ansvarsfrågan för hanteringen är reglerad. Risken har bedömts som möjlig och konsekvensen som kännbar. Risken tas om hand i arbetet med egenkontroller i den systematiska interkontrollen

5.4 Dataskyddsombudet ger råd och rekommendationer till personuppgiftsansvarig

Förvaltningen bör fortsätta arbetet med att genomföra riskkartläggningar som en del i det systematiska dataskydds- och informationssäkerhetsarbetet. Genom att uppmärksamma dessa frågor i förvaltningens arbete med internkontroll blir de en naturlig del av verksamhetsutvecklingen.

För att riskerna ska kunna hanteras och minimeras är det centralt att förvaltningen utvecklar sin organisation för dataskyddsfrågorna. Det bör finnas en organisation med medarbetare inom respektive avdelning som på en del av sin arbetstid arbetar med dataskyddsfrågor. Det kan till exempel handla om att identifiera och registrera personuppgiftsbehandlingar, uppmärksamma behov av konsekvensbedömningar och personuppgiftsbitrrädesavtal. Det är först när dataskyddsarbetet sprids från den centrala förvaltningen till verksamheterna som efterlevnad och åtgärder får ordentligt genomslag och de rekommendationer som har getts i denna rapport kan genomföras. Frågan om organisation för dataskyddsfrågorna kan förslagsvis ingå i lokal informationssäkerhetsanvisning som ingår som en aktivitet i verksamhetsplanen för 2022.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Översyn av registerförteckning*
- *Konsekvensbedömningar*
- *Personuppgiftsbiträdes-avtal*

6.2 Syfte

En av uppgifterna i rollen som dataskyddsombud är att granska personuppgiftsansvarigs efterlevnad av dataskyddsförordningen. 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.

Följande granskningar planeras att genomföras under 2022. Utifrån kontinuerlig riskbedömning kan planering och prioritering av granskningar förändras under året.

Granskning 1 Översyn av registerförteckningen
Kontroll av att samtliga avdelningar har reviderat sin registerförteckning enligt årsplanering och kompletterat med uppgifter enligt beskrivning i kapitel 3.1.

Granskning 2 Konsekvensbedömningar
Kontroll av att konsekvensbedömning har genomförts av behandling av känsliga personuppgifter. Kontroll genomförs i samband med översyn av registerförteckningen.

Granskning 3 Personuppgiftsbiträdesavtal
Kontroll att personuppgiftsbiträdesavtal har tecknats i de fall detta ska göras. Kontroll genomförs i samband med översyn av registerförteckningen och avtalsuppföljning.