Stockholms stad

GDPR Årsrapport

2021

Kyrkogårdsförvaltningen

GDPR årsrapport
Januari 2022

Dnr: 2022-01-10
Utgivningsdatum: 2022-01-DD
Kontaktperson: Göran Höglund

1 Bakgrund

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

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

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

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

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

Innehåll

2 Sammanfattning

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

Verksamheten i Kyrkogårdsförvaltningen har fungerande rutiner för persondataskydd och medarbetare är väl insatta i vilka rutiner som ska tillämpas i olika situationer.

Under året har två personuppgiftsincidenter hanterats inom förvaltningen, dessa relateras bägge till utskick av brev där två brev hamnade hos fel mottagare. Incidenterna åtgärdades så snart det blivit känt. Incidenterna är loggade men bedömdes inte bli föremål för anmälan till IMY (Integritetsskyddsmyndigheten). Rutiner för brevutskick har setts över i samband med de inträffade incidenterna.

Under 2021 har inga begäran om registerutdrag kommit in till Kyrkogårdsförvaltningen.

Under året har två möten hållits mellan verksamheten och förvaltningschefen, där uppfyllanden av har krav enligt GDPR stämts av, eventuella avvikelser diskuterats samt förteckningen över personuppgiftsbehandlingar kvalitetssäkrats. Not: Kyrkogårdsförvaltningen har valt att hantera behandlingsregistret med stöd av Excel, vilket bedöms vara fullt tillräckligt för en god kontroll över personuppgiftsbehandlingarna.

Under det kommande året genomförs fortsatt kvalitetssäkring av hantering av personuppgifter i verksamheten. Dataskyddsombudet är sammankallande till dessa möten. Dessutom kommer fortsatt bevakning och hantering av ev. personuppgiftsincidenter att ske.

Dataskyddsombudet har uttryckt viljan av att i alla händelser av incidenter, oavsett om de ska anmälas eller inte till IMY (Integritetsskyddsmyndigheten), bli informerad. Detta så att gemensamma bedömningar gällande ev. incidenters allvarlighetsgrad kan göras.

En intern GDPR-utbildning genomfördes under hösten 2021 där samtliga medarbetare på huvudkontoret deltog. Kompetensutvecklingen genomfördes av dataskyddsombudet och syftade till att ge alla en för verksamheten anpassad utbildning och med tid för frågor och gemensamma ställningstaganden.

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 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?	18 st.
Har nödvändiga uppdateringar gjorts?	Ja, bevakning sker löpande
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Ja

3.1.2 Syfte

Syftet är att rapportera till PUA hur väl verksamhetens har lyckats inventera och upprätthålla behandlingen av sina personuppgifter inkluderat att upprätta en registerförteckning.

Registerförteckningen ger en grund för ett arbete med resurs- och kostnadseffektivt samt stöd för systematiska riskbedömningar. Man kan styra insatserna där de gör störst nytta.

3.1.3 Resultat

Verksamheten har registerfört 18 behandlingar. Det bedöms i nuläget inte finnas några ytterligare behandlingar som behöver registerföras. Fungerande rutiner för registerföring finns på plats.

Bevakning av registerförteckningen har skett löpande och översyn har gjorts vid 2 tillfällen under året. DSO har vid dessa tillfällen kontrollerat hur många behandlingar som finns registrerade och om några nya har uppstått.

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
	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

3.1.5 DSO ger råd och rekommendationer till PUA

Inga rekommenderade åtgärder från DSO lämnas avseende registerförteckningen.

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Nej, 1 rutin var inte tillgänglig vid tillfället för årsrapporteringen, se nedan.
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Ja
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Behov av revidering av rutin för incidenthantering finns, se nedan.
Är dokumenten uppdaterade?	Uppdatering/revidering av rutin för incidenthantering ska göras.
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja

3.2.2 Syfte

Syftet är att visa om rutiner finns på plats samt om dokumentationen innehållsmässigt håller en lämplig kvalitet, inkl. att dokumentationen ska vara uppdaterad och aktuell.

3.2.3 Resultat

- Vid tillfället för årsrapporteringen saknade DSO rutin för begäran om registerutdrag. DSO önskar få en genomgång av detta. Dock konstateras att ett praktiskt arbetssätt för detta finns kommunicerat och används i förekomna fall.
- DSO önskar får en översyn av dokumentet ”Vägledning vid händelse av en personuppgiftsincident”, viss information gällande DSO:s engagemang behöver ses över. Dessutom behöver dokumentet uppdateras med nytt namn för tidigare Datainspektionen (IMY, Integritetsskyddsmyndigheten).

Övriga styrande dokument är på plats, och bedöms vara användbara.

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

Ovan beskrivna åtgärder (se 3.2.3) rekommenderas genomföras snarast under 2022 och återrapporteras till PUA.

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?	Ja, alla har informationsklassats
Är klassade personuppgiftsbehandlingar aktuella?	Ja

3.3.2 Syfte

Utred med Göran. 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.

3.3.3 Resultat

Samtliga personuppgiftsbehandlingar har informationsklassats. Noteringar om detta finns gjort i förteckningen över personuppgiftsbehandlingar.

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
	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

3.3.5 DSO ger råd och rekommendationer till PUA

Inga rekommendationer ges.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Ja
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Ja. Inga högriskbehandlingar har identifierats.
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 kan/ska riskförebyggande åtgärder vidtas.

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

Bedömningen är att Kyrkogårdsförvaltningen inte har några personuppgiftsbehandlingar där brister gällande konfidentialitet (bristande behörighetsstyrning), riktighet (korrekt information) samt tillgänglighet (åtkomst till information i rätt omfattning) leder till allvarliga konsekvenser för enskild individ.

De personuppgiftsbehandlingar där skyddad identitet gäller hanteras kontrollerat och etablerade rutiner. Konsekvensbedömningar av dessa har gjorts i tidigare sammanhang.

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
	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

3.4.5 DSO ger råd och rekommendationer till PUA

Frågan om konsekvensbedömningar lyfts av DSO i samband med kontroller och avstämningar under 2022. Inga ytterligare åtgärder rekommenderas.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	Inga begäran har tagits emot under 2021.
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Se ovan.

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.)

3.5.3 Resultat

Verksamheten har förutsättningar att på ett så skyndsamt sätt som möjligt ta emot och hantera registrerades rättigheter. Detta sker senast inom föreskriven tidsfrist.

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

3.5.5 DSO ger råd och rekommendationer till PUA

Inga rekommendationer eller förslag till förbättringar lämnas.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Genom information från individen
Hur många personuppgiftsincidenter har dokumenterats?	2
Hur många av dessa har ansetts behöva rapporteras (till IMY) och inte?	0
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	--- se ovan.

3.6.2 Syfte

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

Verksamheten har under 2021 identifierat 2 st. personuppgiftsincidenter, bägge dessa orsakades av fel i utskick av brev till individer. Två brev hamnade hos fel mottagare, vilket åtgärdades så snart det blivit känt. Incidenterna loggades men bedömdes inte bli föremål för anmälan till IMY (Integritetsskyddsmyndigheten).

Dokumentation en av dessa personuppgiftsincidenter bifogas årsrapporten, se bilagt dokument med ärendenummer: KYF 2021/1017

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

3.6.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet vill i alla lägen bli informerad då en informationssäkerhetsincident inträffar, en gemensam bedömning ska göras gällande innehållet i incidenten samt om anmälan till IMY ska göras.

PUA rekommenderas läsa dokumentationen av de två incidenterna, för att ha kunskap om dem. Incidenterna ligger i diariet. Inga övriga åtgärder rekommenderas.

4 Genomförda granskningar under året

4.1 Sammanfattning

4.2 Syfte

Dataskyddsombudet har till uppgift att övervaka verksamhetens efterlevnad av dataskyddsförordningen. En 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

4.3.1 Granskning 1, 2021-03-19

- Allmän avstämning, genomgång av centrala dokument inkl. registerförteckningen. Inga allvarliga brister noterades. Arbetet med persondataskyddet fortsätter med gällande rutiner.

	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

4.3.2 Granskning 2, 2021-11-26:

- Avstämning/genomgång av GDPR-status. Inga stora avvikelser loggades förutom de två inträffade personuppgiftsincidenterna, se ovan.

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

4.4 DSO ger råd och rekommendationer till PUA

Inga särskilda rekommendationer lämnas. Inom Kyrkogårdsförvaltningen fortsätter arbetet med persondataskyddet.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

Risk 1-Risk för onödig behörighet i det gravadministrativa systemet

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.

5.3 Resultatet av riskkartläggningen

Risk 1-Risk för onödig behörighet i det gravadministrativa systemet

Att samtliga medarbetare har samma behörighet, förutom två medarbetare med administrationsbehörighet, kan leda till onödig åtkomst av personuppgifter för medarbetare. Principer för s k ”Least privilege” kan inte uppfyllas, d v s man ska bara ha åtkomst till de personuppgifter som är nödvändiga för uppgiften man har.

	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

5.4 DSO ger råd och rekommendationer till PUA

Se under avsnitt 2 Sammanfattning ovan.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Registerförteckning personuppgiftsbehandlingar
- Rutiner för incidenthantering personuppgiftsincidenter
- Rutin vid begäran om registerutdrag
- Hantering av ändringar, de områden som inte förhindras av övriga regelverk

6.2 Syfte

Det granskande arbetet är en av dataskyddsombudets viktigaste uppgifter. 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, genomförs kvartal 1 2022: Granskning och kvalitetssäkring av hela arbetssättet avseende persondataskydd.
- Granskning 2, genomförs under kvartal 3 2022: Genomgång av avvikelser och förbättringsåtgärder med utgångspunkt från erfarenheter från arbetet hittills under året.
- Granskning 3, genomförs vid behov under december 2022. För översyn och avstämning av tidigare identifierade förbättringsåtgärder.

7 Övrigt att rapportera

7.1 Sammanfattning

- Arbete pågår med löpande översyn och kvalitetssäkring av blanketter som används i administrationen.
- Rättelser av fel i personuppgifter hanteras omgående vid anmälan av detta.
- Rensning av personuppgifter görs i enlighet med regelverk och lagstiftning efter 10 år.

7.2 Syfte

7.3 Övriga observationer

7.4 DSO ger råd och rekommendationer till PUA

Se ovan.