Stockholms stad

Bilaga 10

GDPR Årsrapport

2022

Norrmalms Stadsdelsnämnd

GDPR årsrapport
Januari 2023

Dnr: YYYY
Utgivningsdatum: 2023-01-05
Kontaktperson: Pedro Bentancour Garin

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.

År 2022 har präglats av återgången till det normala efter pandemin och Norrmalms stadsdelsförvaltning har under detta år tagit tag i dataskyddsfrågorna med nya krafter.

Jag som DSO vill lyfta fram några av de viktiga punkter som genomförts under året: registerförteckningen har skrivits klar samt en ny mall uppställts för registrera processer.

Stadsdelsförvaltnings personal är bra på att identifiera personuppgiftsincidenter. De två DSO som finns på förvaltningen kontaktas ofta med frågor rörande dataskyddsfrågor.

Min rekommendation inför 2023 är att:

- Fortsätta komplettera och korrigera registerförteckningen
- Fortsätta granskningen av rutiner
- Fortsätta arbetet med infoklassningar av de olika systemen
- Fortsätta komplettera och implementera styrdokument
- Fortsätta arbetet med att utbilda och informera
- Granska PUB-avtal

Pedro Bentancour Garin
Dataskyddsombud

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?	624
Har nödvändiga uppdateringar gjorts?	Registerförteckningen är uppdaterad just nu och kommer att fortsätta uppdateras löpande.
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Ja och de utvecklas löpande

3.1.2 Syfte

Artikel 30 anger krav på att inventera alla personuppgifter som behandlas. Registerförteckningen utgör dokumentationen av inventeringen. När registerförteckningen är upprättad skapar den en intern synlighet och förståelse för vilka personuppgifter som behandlas samt hur de hanteras. Därmed är registerförteckningen dataskyddsarbetets centrala utgångspunkt och bas samt säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling.

3.1.3 Resultat

Varje avdelning ansvarar för sin egen registerförteckning. Under 2022 har en ny mall för att registrera processer tagits fram, liksom en stor genomgång av registerförteckningen gjorts där denna har uppdaterats fullständigt. Registerförteckningen omfattar till stor del de personuppgifter som hanteras. Det krävs nu att registerförteckningen uppdateras löpande. Att utveckla den rättsliga grunden, förståelsen för när konsekvensbedömning behöver genomföras samt ställningstagande till nödvändiga säkerhetsåtgärder är också ett fortlöpande arbete.

Ett nätverk (ID-nätverket) för informationssäkerhet och dataskydd har startats upp på förvaltningen med representanter (dataskyddshandläggare) från varje avdelning samt ISAM och DSO.

Dataskyddshandläggarna är inblandade och involverade i alla delar av infosäkerhetsarbetet nu. Kunskapen och kompetensen ökar. Fokus under 2022 har varit arbetet med ny registerförteckning, befintliga rutiner, att delta och lära sig av informationsklassningar, följa upp rapporterade incidenter och informationssäkerhet i upphandlingsförfarandet. Det fortsätter även under 2023 med vissa prioriterade frågor.

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

Det krävs nu att registerförteckningen uppdateras löpande. Att utveckla den rättsliga grunden, förståelsen för när konsekvensbedömning behöver genomföras samt ställningstagande till nödvändiga säkerhetsåtgärder är också ett fortlöpande arbete.

Förvaltningen bör i samråd med DSO bereda för att dataskyddshandläggarna får relevanta utbildningar o.s.v. särskilt när en ny dataskyddshandläggare tillträder. Fortsatt arbete med vissa prioriterade frågor inom IDnätverket.

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

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.

3.2.3 Resultat

På intranätet finns det en sida som sammanfattar rutinerna på så sätt att det är tydligt vilka krav som ställs på verksamheterna och vad de ska tänka på.

I övrigt finns det rutiner för:

Hantering av en personuppgiftsincident
Inventering av personuppgifter
Risk- och konsekvensanalyser
Begäran om registerutdrag
Övergripande rutiner om nämndens dataskyddshantering och ansvarsfördelning

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

3.2.5 DSO ger råd och rekommendationer till PUA

Rutiner finns upprättade. Arbetet fortsätter med att säkerställa att dokumenten är kända och tillämpas.

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?	13
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.

3.3.3 Resultat

Fem klassningar har genomförts under året. Sammanlagt har 13 klassningar gjorts, där samhällsviktiga och lokala system prioriterats. Arbetet kommer att fortsätta under 2023.

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
X	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

Arbetet med informationsklassning har pågått under 2022 och kommer att fortsätta under 2023.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Nej
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Nej
Är de genomförda bedömningarna aktuella?	Ja

3.4.2 Syfte

Kravet på konsekvensbedömning är 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

Arbetet med konsekvensbedömningar har påbörjats under 2022, med bl.a. en konsekvensbedömning av systemet ” Nyckelfri hemtjänst” och arbetet med att identifiera behandlingar som behöver konsekvensbedömmas av kommer att fortsättas under 2023.

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

3.4.5 DSO ger råd och rekommendationer till PUA

Chefer och berörda medarbetare behöver öka sina kunskaper om kravet på konsekvensbedömningar. Det kan uppnås genom att chefer och berörda medarbetare tar del av utbildningar om dataskydd. Arbetet fortsätter med att identifiera i vilka behandlingar som konsekvensbedömningar behöver genomföras och att ta fram en plan för det.

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?	0

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.

3.5.3 Resultat

Det finns vägledning och rutiner till stöd för att på ett säkert sätt för att efterleva kravet på enskildas rättigheter. Kunskapen om rättigheterna och befintliga rutiner behöver upprätthållas bland berörda medarbetare.

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

Det finns rutiner för att hantera begäran av registerutdrag. Under 2021 och 2022 kom det inte in någon begäran.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Medborgare eller personal informerar förvaltningen.
Hur många personuppgiftsincidenter har dokumenterats?	6
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	4 har rapporterats till IMY
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	1

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.”

3.6.3 Resultat

Under året har 6 incidenter rapporterats vara 4 har bedömts att de ska anmälas till IMY. Det finns rutiner för hur incidenter ska hanteras och i samtliga fall har det vidtagits åtgärder för att minimera konsekvenserna samt underrätta de drabbade.

Anledningarna till att 3 incidenter rapporterats senare än de 72 timmar som IMY begär har varit i ett fall att det var osäkert om underleverantören hos vilken incidenten inträffade var biträde till förvaltningen eller inte, ket tog viss tid att utreda. I två fall handlade det om att respektive handläggare inte hade kännedom att anmälan ska göras omedelbart.

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
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

3.6.5 DSO ger råd och rekommendationer till PUA

Trots att kravet på anmälan av personuppgiftsincidenter (som ska göras inom 72 timmar till IMY) är en del av dataskyddet där kunskapen är relativt väl etablerad, är det nödvändigt att all personal regelbundet påminns om detta krav, liksom att kravet upprätthålls och att nödvändiga rutiner är kända och uppdaterade.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- *Registerförteckning*
- *Incidentrapportering*
- *Rutiner*

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

Det har tagits fram en ny registerförteckning som omfattar samtliga processer som stadsdelsförvaltningen använder sig av samt kopplar ihop den med informationssäkerheten. Det ger en samlad överblick och möjliggör för ett systematiskt dataskyddsarbete.

	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

Granskning 2

Incidentrapportering sker löpande under året och stäms av en gång i kvartalet tillsammans med dataskyddshandläggarna och informationssäkerhetssamordnaren.

	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

Granskning 3

Rutinerna har börjat gås igenom, detta arbete fortsätter under 2023.

	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

4.4 DSO ger råd och rekommendationer till PUA

Fortsätta arbetet med informationssäkerhet- och dataskyddsnätverket. Nätverket innebär ett systematiskt dataskyddsarbete och håller frågorna levande hos avdelningarna. Tänk på att se till att rutiner finns på plats.

5 Planerade granskningar under det nya verksamhetsåret

5.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Konsekvensbedömningar
- Infoklassningar
- Personuppgiftsincidenter
- Rutiner
- PUB-avtal
- Kompletteringar och ändringar av registerförteckningen

5.2 Syfte

Granskningsområdena har valts utifrån ett *riskbaserat synsätt*, det vill säga att fokus ska ligga på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Detta är för att åstadkomma en röd tråd i dataskyddsarbetet från innevarande verksamhetsår till nästa samtidigt som de största riskerna elimineras eller åtminstone sänks till en mer acceptabel nivå.