Stockholms stad

GDPR Årsrapport

2021

Norrmalms stadsdelsnämnd

GDPR årsrapport
Januari 2022

Dnr: NORR 2021/373
Utgivningsdatum: 2022-02-10
Kontaktperson: Christer Bergman

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

Årsrapporten omfattar de obligatoriska rapporteringsområdena enligt dataskyddsförordningen.

Registerförteckning

Styrande dokument

Tekniska och organisatoriska åtgärder

Konsekvensbedömningar

Personuppgiftsincidenter

Individens rättigheter

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?	308
Har nödvändiga uppdateringar gjorts?	En del avdelningar har gjort det, några inte.
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Rutinen kan utvecklas

3.1.2 Syfte

Artikel 30 anger krav på att inventera alla personuppgifter som behandlas. Registerförteckningen utgör dokumentation av inventeringen. Därmed är registerförteckningen dataskyddsarbetets centrala utgångspunkt och bas samt säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling.

Resultat

Varje avdelning ansvarar för sin egen registerförteckning. Genomgång har gjorts av registerförteckningarna som till stor del har reviderats och uppdaterats. Registerförteckningen till stor del omfatta de personuppgifter som hanteras. Delar som kan utvecklas är rättslig grund och förståelsen för när konsekvensbedömning behöver genomföras samt ställningstagande till nödvändiga säkerhetsåtgärder.

3.1.3 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

3.1.4 DSO ger råd och rekommendationer till PUA

En ny mall för registerförteckningarna håller på att tas fram för att bättre kunna registrera processer. Ett nätverk för informationssäkerhet och dataskydd startas upp på förvaltningen med representanter (dataskyddshandläggare) från varje avdelning. Det är viktigt att förvaltningsledningen utser dataksyddshandläggare som är villiga att sätta sig in i frågorna och göra det arbete som krävs samt ser till att de har tid att utföra sitt dataskyddsarbetet.

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).

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 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?	8
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

Gemensamma system och digitala plattformar som delar av skolplattformen, sociala system och ekonomisystemet Agresso har klassats på systemförvaltningsnivå. Under 2021 påbörjades arbetet med att klassa behandlingar som omfattas av NIS-direktivet. Arbetet kommer att fortsätta under 2022.

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 2021 och kommer att fortsätta under 2022.

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 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 vara en del av berörda processer som exempelvis upphandling. En konsekvensbedömning är planerad för digital läkemedelssignering.

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. Arbete 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

[Se Instruktion för Årsrapportmallen kap. 9 för vägledning om hur risken kan beskrivas.]

3.5.5 DSO ger råd och rekommendationer till PUA

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

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Medborgare informerar förvaltningen.
Hur många personuppgiftsincidenter har dokumenterats?	14
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	7
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.”

3.6.3 Resultat

Under året har 14 incidenter rapporterats vara 7 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.

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

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

3.6.5 DSO ger råd och rekommendationer till PUA

Kravet på anmälan av personuppgiftsincidenter är en del av dataskyddet där kunskapen är relativt väl etablerad. Det är nödvändigt att den upprätthålls och att nödvändiga rutiner är kända och uppdaterade.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

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

4.2 Syfte

En av dataskyddsombudets viktigaste uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten kan fatta i fråga om dataskyddsåtgärder.

4.3 Genomförda granskningar och deras resultat

Granskning 1

Samtliga verksamheter har gått igenom registerförteckningen och gjort nödvändiga uppdateringar.

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

Granskning 2

Lämpliga rutiner finns på plats.

	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

Incidenter har hanterats korrekt, rapporterats i IA och registrerats i diariet.

	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

Förra årets granskningar har visat at arbetet med nämndens förteckningar över personuppgiftshantering behöver utvecklas under 2022.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker 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

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. Risker inom dataskydd och informationssäkerhet har analyserats i det systematiska internkontrollarbetet

5.3 Resultatet av riskkartläggningen

Risk 1

Risken har bedömts som möjlig och allvarlig.

	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

Risk 2

Risken har bedömts som mindre trolig men med alvarliga konsekvenser.

	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

Risk 3

Risken har bedömts som möjlig och allvarlig.

	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

Det är en fördel att risker inom dataskydd inventeras och analyser i samband med upprättande av internkontrollplan och den sammanhängande väsentlighets- och riskanalysen.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Samtycken för bildpublicering inom förskola*
- *Personuppgiftsbirädesavtal*
- *Registerförteckningar*

6.2 Syfte

Avsikten med att välja ut två områden för granskning är för att kunna planera och avsätta tid för detta under det kommande året. Att det upprättas personuppgiftsavtal och inhämtas samtycken för bildpublicering är krav i dataskyddslagen och det är av stor vikt att dessa krav efterlevs. Årets granskning har visat att registerförteckningarna behöver utvecklas och kompletteras.

6.3 Planerade granskningar

Granskning 1

Förskoleavdelningen är den avdelning som till störst del använder samtycken för bildhantering. Det kommer att ske en kontroll av att samtycken finns vid aktualitet samt att dessa gallrats vid inaktualitet.

Granskning 2

När nämnden använder sig av ett biträde för att hantera personuppgifter krävs det att det upprättas ett personuppgiftsbiträdesavtal som reglerar hanteringen. Under 2022 kommer det att kontrolleras att det finns personuppgiftsbiträdesavtal på plats där detta är ett krav.

Granskning 3

Kontroll av att samtliga enheter har reviderat sin registerförteckning enligt årsplanering.