Stockholms stad

Bilaga

GDPR Årsrapport

År 2023

Kungsholmens stadsdelsnämnd

GDPR årsrapport 2023

Dnr: KUNG 2023/478
Utgivningsdatum: 2023-12-27
Kontaktperson: Christin Bjuggren

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:s 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.

I egenskap av ert Dataskyddsombud lämnar jag följande årsrapport.

Årsrapporten omfattar de obligatoriska rapporteringsområdena enligt dataskyddsförordningen.

- Registerförteckning
- Styrande dokument
- Tekniska och organisatoriska åtgärder
- Konsekvensbedömningar
- Individens rättigheter
- Personuppgiftsincidenter

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:s slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter DSO:s genomförda uppföljning och granskning.

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	400
Har nödvändiga uppdateringar gjorts?	Ja
Bedöms registerförteckningen vara fullständig?	Ja
Har verksamheten lämpliga rutiner för registerföring?	Ja

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.

3.1.3 Resultat

Genomgång har gjorts av registerförteckningen som därmed har reviderats och uppdaterats. Registerförteckningen bedöms i allt väsentligt omfatta de personuppgifter som hanteras.

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

Avdelningarnas dataskyddshandläggare samordnar arbetet med att hålla registerförteckningen aktuell och uppdaterad. Detta arbetssätt säkerställer kvalitet och kontinuitet.

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 en sida med rubriken Informationssäkerhet och dataskydd med samlad information för chefer och medarbetare. I stadsdelsförvaltningens övergripande rutin för dataskydd fastställs vad chefer och medarbetare behöver tänka på när personuppgifter hanteras. Rutinen finns tillgänglig på intranätsidan. Förutom den övergripande rutinen finns även:

- Dokument för inledande utredning av personuppgiftsincident
- Checklista för rensning av e-post
- Checklista vid begäran om registerutdrag
- Vägledning vid begäran om tillgång, rättelse och radering av personuppgifter
- Hantering av tjänstekort

På intranätet finns även en sida med vägledning om de bestämmelser som gäller enligt NIS-direktivet (Nätverks- och informationssäkerhet inom vissa samhällsviktiga verksamheter). Där redogörs för de särskilda bestämmelser om incidentrapportering som följer av NIS-direktivet. Rutiner finns framtagna för incidentrapportering.

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 och checklistor 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?	25
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

Informationsklassning har genomförts av bland annat system som har anknytning till HR och som omfattar personuppgifter om anställda. Den kommunala hälso- och sjukvården inom äldreomsorgen omfattas av de särskilda bestämmelser som följer av NIS-direktivet (Nätverks- och informationssäkerhet i vissa samhällsviktiga tjänster). Klassningar av system och digitala tjänster som påverkar den kommunala hälso- och sjukvården har prioriterats.

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

Arbetet med att genomföra informationsklassificeringar fortsätter enligt verksamhetsplan 2024.

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
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

Konsekvensbedömning är ett område som fortsatt behöver prioriteras. Konsekvensbedömning har genomförts av delar av skolplattformen, delar av sociala system samt digitala system inom äldreomsorgen

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

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?	Tre
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Tre

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

Kunskapen om rättigheterna och befintliga rutiner säkerställs bland berörda medarbetare.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Huvudsakligen av användare, dvs medarbetare och chefer.
Hur många personuppgiftsincidenter har dokumenterats?	14
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	En har anmälts till IMY
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Samtliga har rapporterats i tid.

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 personuppgiftsincidenter rapporterats varav en har föranlett anmälan till Integritetsskyddsmyndigheten. I samtliga incidenter vidtogs åtgärder omedelbart för att minimera skadan samt säkerställa att det inte sker igen. Antalet rapporterade incidenter är fler än föregående år (tio). 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

3.6.4 DSO ger råd och rekommendationer till PUA

Sett till antalet personuppgiftsbehandlingar är antalet rapporterade incidenter förhållandevis lågt. Det låga antalet rapporterade personuppgiftsincidenter kan innebära att incidenter inte identifieras. Kompetensen inom dataskydd behöver säkerställas bland samtliga användare.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Styrdokument
- Registerförteckning
- Informationsklassningar
- Kompetensutveckling

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

Styrdokument för dataskydd och informationssäkerhet har reviderats.

	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

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

Granskning 3

Informationsklassning av bland annat system som har anknytning till HR och som omfattar personuppgifter om anställda. Därutöver har klassningar av system och digitala tjänster som påverkar den kommunala hälso- och sjukvården har prioriterats.

	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 4

340 av förvaltningens medarbetare genomgått den obligatoriska grundkursen i dataskydd och 420 har genomgått den obligatoriska grundutbildningen om informationssäkerhet. Det är en låg andel av förvaltningens totalt över 1000 användarkonton.

	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 DSO ger råd och rekommendationer till PUA

Arbetet med dataskydd och informationssäkerhet behöver prioriteras enligt verksamhetsplan och plan för internkontroll.

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

Samtliga risker har identifierats och analyserats i det systematiska internkontrollarbetet. De identifierade riskerna graderas utifrån sannolikhet och konsekvens. Riskerna dokumenteras i en matris som bygger på en femgradig skala enligt följande:

	Sannolikhet	**Konsekvens**
5	Mycket sannolikt	Mycket allvarlig
4	Sannolikt	Allvarlig
3	Möjlig	Kännbar
2	Mindre sannolikt	Lindrig
1	Osannolikt	Försumbar

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

Behörighetshantering – om behörigheter inte avslutas kan obehöriga användare komma åt konfidentiell information. Personuppgifter hanteras därmed felaktigt.

Risken har bedömts som sannolik och kännbar. Risken tas med i internkontrollplanen.

Risk 2

Informationssäkerheten upprätthålls inte vilket kan leda till skador för enskilda personer, skadat förtroende och ekonomiska konsekvenser.

Risken har bedömts som mindre sannolik och kännbar. Risken tas om hand i uppföljning av internkontrollen.

Risk 3
Incidenthantering – inträffad personuppgiftsincident har inte identifierats och rapporterats inom 72 timmar vilket kan medföra att åtgärder inte sätts in och att händelsen upprepas.

Risken har bedömts som möjlig och konsekvensen som allvarlig. Risken har tagits med internkontrollplanen.

Risk 4
Informationsklassning – att digitala system inte hanteras på ett säkert sätt.

Risken har bedömts som mindre sannolik och konsekvensen som allvarlig. Risken tas om hand i uppföljning av internkontrollen.

5.4 DSO ger råd och rekommendationer till PUA

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

6 Planerade granskningar under det nya verksamhetsåret

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

Översyn av aktuella informationsklassificeringar
Kontroll av att planerade informationsklassningar har genomförts.

Deltagande i stadens webbutbildningar om dataskydd och informationssäkerhet
Kontroll av deltagande genomförs i samband med tertialrapporter och verksamhetsberättelse.

Uppdatering av rutiner och andra styrande dokument
Kontroll av att rutiner och andra styrande dokument för dataskyddsarbete är aktuella. Stödmaterial till chefer tillhandahålls.

Kontroll av att stödmaterial används.

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

Personuppgiftsincidenter
Kontroll av rapporterade personuppgiftsincidenter görs i samband med tertialrapporter och verksamhetsberättelse.

Individens rättigheter
Vägledning och rutiner hålls aktuella. Chefer och medarbetare informeras om betydelsen av rättigheterna.