Stockholms stad

Bilaga 8

# GDPR Årsrapport

2021

Skönhetsrådet

**GDPR årsrapport**
Januari 2022

**Dnr:** KS 2021/1557
**Datum:** 2022-01-13
**Kontaktperson:** Skönhetsrådets dataskyddsombud

# Innehåll

**1 Bakgrund ..... 4**

**2 Sammanfattning ..... 5**

**3 Obligatoriska rapporteringsområden ..... 6**

3.1 Registerförteckning ..... 7

3.2 Styrdokument ..... 8

3.3 Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar ..... 10

3.4 Konsekvensbedömningar ..... 11

3.5 Individens rättigheter ..... 12

3.6 Personuppgiftsincidenter ..... 13

**4 Genomförda granskningar under året ..... 14**

**5 Risker inom dataskydd ..... 14**

5.1 Sammanfattning ..... 14

**6 Planerade granskningar under det nya verksamhetsåret ..... 14**

# 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 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 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.

Skönhetsrådet har 2018 utnämnt ett dataskyddsombud som är anmält till tillsynsmyndigheten. Av denna anledning upprättas denna GDPR årsrapport. I egenskap av dataskyddsombud lämnar jag följande årsrapport.

# 2 Sammanfattning

Skönhetsrådet behandlar inga känsliga personuppgifter förutom de som tillhör ledamöter utsedda av politiska partier. Enligt artikel 9 i dataskyddsförordningen kan undantag göras för dessa behandlingar om den registrerade uttryckligen lämnat sitt samtycke till behandlingen av dessa personuppgifter för ett eller flera specifika ändamål med mera.

I de fall sekretessbelagda bygglov remitteras till rådet diarieförs dessa i eDok som sekretessbelagt ärende enligt Offentlighets- och sekretesslagen (OSL) 18 kap. 8§. Beträffande inkommande e-post och skrivelser från privatpersoner rörande stadsmiljöärenden registreras personuppgifter såsom namn och e-postadress.

Ett nytt inslag sedan mars 2020 är att rådet pga. pandemin haft digitala sammanträden via Skype. Detta har inte registrerats eller riskbedömts.

Riskbedömningen nedan speglar den personuppgiftsbehandling som Skönhetsrådet utför. Därför kan riskbedömningarna skilja sig från stadsledningskontorets.

# 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? | 22 |
| Har nödvändiga uppdateringar gjorts? | Se nedan |
| Bedöms registerförteckningen vara fullständig? | Nej |
| Har verksamheten lämpliga rutiner för registerföring? | Eftersom endast DSO arbetar med frågan så skulle en skriftlig rutin behöva formuleras i det fall arbetet överlämnades till någon annan. |

Verksamheten har registerfört **22** behandlingar, dessa utgår från Skönhetsrådets klassificeringsstruktur vilken även hänger ihop med eDok. Det finns några ytterligare behandlingar som behöver registerföras.

### 3.1.2 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 |

Nivå gul har valts eftersom det finns obesvarade frågor i registerförteckningen som ska besvaras under 2022.

## 3.2 Styrdokument

### 3.2.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Finns lämplig styrande dokumentation på plats? | Skönhetsrådet kan tillämpa de styrdokument som stadsövergripande avdelningen för informationssäkerhet har tagit fram. Samtidigt finns inga instruktioner och rutiner för t.ex. hantering av epost. Rutiner har tagits fram av KS för fritextfält i system. Det finns dokument men inte på den nivå som GDPR kräver. |
| Håller innehållet i de existerande dokumenten lämplig kvalitet? | Kan ej bedöma. |
| Är dokumenten pedagogiska och ger de ett tillräckligt stöd? | Ibland svåra att förstå. Mer konkretion i instruktionerna skulle behövas. |
| Är dokumenten uppdaterade? | Ej säker på om de innehåller adekvat information om digitala möten. |
| Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov? | Ja |

### 3.2.2 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 |

Skönhetsrådet behandlar inga känsliga personuppgifter förutom de som tillhör ledamöter utsedda av politiska partier. Enligt artikel 9 i dataskyddsförordningen kan undantag göras för dessa behandlingar om behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.

### 3.2.3 DSO ger råd och rekommendationer till PUA

Det är angeläget att kommunstyrelsen tar fram ytterligare tydliga och enkla instruktioner för hur personuppgifter får behandlas inom olika områden.

## 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? | Systemägare och förvaltningsägare av eDok och eVald har säkerställt att informationsklassning är utförd. |
| Är klassade personuppgiftsbehandlingar aktuella? | Ovan nämnda system har enligt uppgift uppdaterats |

### 3.3.2 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 |

Se sammanfattning s. 5

Skönhetsrådet kommer under 2022 att informationsklassa sina egna personuppgiftsbehandlingar.

## 3.4 Konsekvensbedömningar

### 3.4.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av? | Efter bedömning finns inte några sådana behandlingar. |
| Har alla potentiella högriskbehandlingar konsekvensbedömts? | Vi hanterar inga högriskbehandlingar. |
| Är de genomförda bedömningarna aktuella? | Ja |

### 3.4.2 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 Individens rättigheter

### 3.5.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer? | Under 2021 inkom en (1) person med begäran om utdrag ur Skönhetsrådets diarium. |
| Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar? | En (1) |

Eftersom personen inte tidigare varit i kontakt med Skönhetsrådet skulle själva förfrågan om utdrag innebära en registrering av personen. Med anledning av detta kom man överens om att förfrågan kunde gallras.

### 3.5.2 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 Personuppgiftsincidenter

### 3.6.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Hur upptäcks personuppgiftsincidenter? | Inväntar information om stadsledningskontorets rutin för personuppgiftsincidenter, vilket Skönhetsrådet kommer att utgå ifrån. |
| Hur många personuppgiftsincidenter har dokumenterats? | 0 |
| Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte? | 0 |
| Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten? | 0 |

Inga kända incidenter under 2021 har kunnat upptäckas.
Vi välkomnar utbildning avseende personuppgiftsincidenter och hantering av dessa.

### 3.6.2 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 |
| | Inga brister av nämnvärd betydelse identifierade |

Eftersom vi inte haft någon incident så lämnas ovanstående tomt.

# 4 Genomförda granskningar under året

Den granskning som gjorts utgörs av föreliggande årsrapport. DSO arbetar idag operativt med dataskydd och kan därför inte granska sig själv. Kommunstyrelsens dataskyddsombud kommer under 2022 att granska de personuppgiftsbehandlingar som Skönhetsrådets kansli utför.

# 5 Risker inom dataskydd

## 5.1 Sammanfattning

Det finns vissa ärenden som behandlas enligt Offentlighets- och sekretesslagen 18 kap. 8§ (OSL). Majoriteten av ärenden omfattar dock inte känsliga och/eller integritetskänsliga personuppgiftsbehandlingar.

# 6 Planerade granskningar under det nya verksamhetsåret

Kommunstyrelsens dataskyddsombud kommer under 2022 att granska personuppgiftsbehandlingar som Skönhetsrådets kansli utför.