Stockholms stad

# GDPR Årsrapport

2021

Överförmyndarnämnden

**GDPR årsrapport 2021**
Januari 2021

**Dnr:** ÖFF 2022/8
**Utgivningsdatum:** 2022-01-12
**Kontaktperson:** Kristofer Gisslén

# 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 (DSO) lämnar jag följande årsrapport.

Jag tillträdde uppdraget som DSO under våren 2021 och har under perioden verkat för att bilda mig en uppfattning om nuläget i dataskyddsarbetet utifrån den dokumentation verksamheten upprättat.

Jag kan konstatera att medvetenheten inom överförmyndarnämndens verksamhetsområde är god vad gäller dataskyddet. Medarbetarna ifrågasätter själva riskerna med användningen av personuppgifter på ett sätt som tyder på att kunskapen är relativt hög. En gynnande faktor kan vara att verksamhetens huvuduppgift är att handlägga ärenden som rör enskildas hälso- och ekonomiska förhållanden och därför är redan medvetenheten av den anledningen hög. Överförmyndarnämnden bedöms också ha en god förmåga att tillvarata de registrerades rättigheter och skyldigheten att vid behov kunna anmäla incidenter till Integritetsskyddsmyndigheten.

Jag kan dock konstatera att det alltjämt finns brister som måste åtgärdas under 2022. Främst rör dessa överförmyndarnämndens avsaknad av rutiner för konsekvensbedömningar i enlighet med dataskyddsförordningen. Det är av yttersta vikt att sådana rutiner inrättas under 2022 och att samtliga behandlingar inventeras i syfte att avgöra om och i så fall vilka behandlingar som måste konsekvensbedömas. Överförmyndarnämnden behöver också säkerställa att all information som behandlas blivit informationsklassad. Utan relevant klassning kan verksamheten inte sägas ha full kontroll över sin information.

# 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 status och mina slutsatser samt rekommendationer gällande de obligatoriska rapporteringsområdena efter min genomförda uppföljning.

## 3.1 Registerförteckning

### 3.1.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Antal behandlingar som är registrerade? | 23 behandlingar är upptagna i ett Excel ark, varav 3 stycken uppdaterats i verksamhetssystemet Visma Draftit Privacy Records. |
| Har nödvändiga uppdateringar gjorts? | Delvis. Förvaltningen har under 2021 påbörjat övergången från den fysiska registerförteckningen till verksamhetssystemet Visma Draftit Privacy Records. |
| Bedöms registerförteckningen vara fullständig? | Delvis. Den fysiska registerförteckningen bedöms vara fullständig. Visma Draftit Privacy Records är inte fullständig. |
| Har verksamheten lämpliga rutiner för registerföring? | Det finns rutiner för hur uppgifter insamlas och registreras. Uppföljning av registerföringen sker två gånger om året i samband med internkontrollen genom stickprovskontroller. |

### 3.1.2 Syfte

Av artikel 30 i dataskyddsförordningen framgår det att verksamheten måste inventera alla personuppgifter som behandlas, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde och dokumentera dem i en så kallad registerförteckning. Med hjälp av registerförteckningen kan verksamheten synliggöra med vilka lagliga grunder personuppgiftsbehandlingen utförs, samt förvissa sig om att insamling av personuppgifter inte görs i onödan eller i strid med lagstiftningen. Om dokumenteringskravet uppfylls kan verksamheten arbeta effektivt, systematiskt och riskbaserat och samtidigt värna individens integritet, särskilt när känsliga och särskilt skyddsvärda personuppgifter behandlas av verksamheten.

### 3.1.3 Resultat

*Antalet registrerade behandlingar*
Den ursprungliga registerförteckningen som upprättades i ett Excel-ark innehåller 23 behandlingar grundande i de processer som verksamheten arbetar med. Tre av dessa har vid övergången till Visma Draftit Privacy Records uppdaterats.

*Registerförteckningens aktualitet*
Verksamheten bör löpande, gärna årligen, följa upp innehållet i registerförteckningen för att se om det skett förändringar som ska uppdateras. Förändringarna ska vara sådana att rådande behandlingar saknas i förteckningen eller att upptagna behandlingar inte längre utförs. Verksamheten ska endast ha en registerförteckning och inte flera som konkurrerar med varandra. Nämndens fysiska registerförteckning i form av ett Excel-ark bedöms inte vara uppdaterad. Nämndens digitala registerförteckning är inte uppdaterad, då den inte är komplett. Dess innehåll motsvarar heller inte den fysiska registerförteckningen. Att nämnden för närvarande har två konkurrerande registerförteckningar är inte tillfredsställande. Den sammanvägda bilden är därför att nämnden endast delvis har en nödvändigt uppdaterad registerförteckning.

*Omfattningen av registerförteckningens fullständighet*
Den ursprungliga registerförteckningen bedöms vara komplett. Den registrering som genomförts i Visma Draftit Privacy Records är dock för övergripande och måste brytas ned till samma nivå som den ursprungliga registerförteckningen.

*Rutiner för registerföring*
Det finns tydliga rutiner för hur registerföringen ska gå till och instruktionen om hur mallen för registerföring ska ifyllas bedöms pedagogisk. Nya rutiner och instruktioner måste dock upprättas för att beskriva hur registerförteckningen ska föras i Visma Draftit Privacy Records.

### 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 |

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

Överförmyndarförvaltningens samlade hantering av registerförteckningen bedöms vara god även om det finns två konkurrerande förteckningar. Förteckningen behöver dock överföras från det befintliga kalkylarket till det verktyg som är avsett att användas för registerförteckningen. Förteckningen behöver också ställas under årlig översyn. Av överförmyndarförvaltningens årshjul för dataskyddsarbetet framgår det att inventeringen av personuppgifter ska göras två gånger per år. Av stadsledningskontorets mall för dataskyddsombudet årsplan framgår det att ”dataskyddsombudet bör genomföra en årlig genomgång av behandlingsregistret i syfte att kontroller att uppgifterna är uppdaterade och aktuella”. En gång per år bör således räcka för att säkerställa aktualiteten i registerförteckningen.

### 3.1.5 DSO ger råd och rekommendationer till PUA

Överförmyndarnämnden rekommenderas att under 2022 säkerställa att registerförteckningen överförs till det digitala stödet Visma Draftit Privacy Records, samt att nya rutiner och instruktioner upprättas för detta.

## 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? | |
| 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. Genom att vara nedtecknade, beslutade och kommunicerade kan medarbetarna behålla kunskapen om dataskyddet över tid och tillämpa den på ett konsekvent sätt. Detta rapporteringsområde visar på dels en bedömning om verksamheten har antagit sådana styrdokument som krävs för att kunna efterleva Dataskyddsförordningens principer för behandling av personuppgifter, dels om dokumentationen innehållsmässigt håller en lämplig kvalitet.

### 3.2.3 Resultat

*Finns lämplig styrande dokumentation på plats?*

Det finns skriftliga rutiner samlade i en gemensam mapp dit medarbetarna kan vända sig för stöd i dataskyddsarbetet. Rutinerna är dock uppblandade med annan dokumentation runt dataskyddet vilket skapar otydlighet i överblicken av vilka rutiner som finns och till vad. Rutinerna skulle behöva separeras från annan dokumentation och samlas i en enhetlig rutinmapp.

*DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet*

Dokumentationen är utformad för att medarbetarna ska kunna tillgodogöra sig stödet utan förkunskaper. De är pedagogiskt utformade för att kunna användas när de behövs. Rutinerna spänner över ämnen såsom hur en personuppgiftsincident ska rapporteras, hur registerutdrag ska hanteras samt hur inventering av personuppgifter och konsekvensbedömningar ska utföras.

### 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

Överförmyndarnämnden rekommenderas att under 2022 säkerställa att rutindokumentationen separeras från mallar och informationsmaterial för att förenkla för medarbetarna att hitta dessa.

## 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? | Ytterst få. |
| Är klassade personuppgiftsbehandlingar aktuella? | De som klassats behöver ses över. |

### 3.3.2 Syfte

En förutsättning för att kunna bedriva ett gott dataskyddsarbete är att verksamheten informationsklassat all sin informationsbehandling. Informationsklassning är en metod som hjälper verksamheten att välja rätt åtgärder för att skydda information. Utan informationklassning saknar därför verksamheten förutsättningar att kunna välja rätt åtgärder för att skydda sin information. PUA behöver årligen ges en uppdaterad bild av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar. Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. Om en ansvarig för klassningen inte har pekats ut och känner till sitt ansvar för klassning, minskar sannolikheten avsevärt att en klassning faktisk initieras. Enbart sådan informationsklassning som avser behandling eller system som omfattar *personuppgifter* är av intresse för denna rapport.

### 3.3.3 Resultat

Verksamheten har informationsklassat de verksamhetssystem som används i handläggningen, men inte den information som lagrats i systemen. Det innebär att ytterst få informationsmängder blivit informationsklassade. De system som klassats behöver dessutom ses över eftersom det inte blivit gjort.

### 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 |

| | |
|---|---|
| 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 |

### 3.3.5 DSO ger råd och rekommendationer till PUA

Överförmyndarnämnden rekommenderas att under 2022 säkerställa att all information som behandlas inom verksamheten informationsklassas.

## 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? | - |

### 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. Konsekvensbedömningen är ett uttryckligt krav enligt Dataskyddsförordningen och ska alltid göras vid behandlingar av personuppgifter som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1). I förekommande fall ska en konsekvensbedömning också föregås av ett samråd med Integritetsskyddsmyndigheten.

### 3.4.3 Resultat

Inga konsekvensbedömningar har genomförts under 2021. En orsak bedöms vara att inga nya typer av behandlingar påbörjats som bedömts kräva en konsekvensbedömning. Det är dock inte tillfredsställande att inga konsekvensbedömningar alls gjorts. Det signalerar att verksamheten inte påbörjat några nya behandlingar alls under 2021. Verksamheten bör ha som utgångspunkt att *alla* nya behandlingar omfattas av en konsekvensbedömning för att säkerställa att kunskapen på området inte faller i glömska. Mängden av nya typer av behandlingar bedöms som pass begränsad årligen att en konsekvensbedömning inte bör vara allt för betungande för verksamheten.

*Identifierade behandlingar som det borde göras konsekvensbedömningar för*
Under 2022 planerar verksamheten att införa ett nytt verksamhetssystem. Även om sannolikheten för att dessa behandlingar skulle leda till stor risk för de registrerade bedöms vara liten så är det ett bra tillfälle för verksamheten att öva på konsekvensbedömningar. Därför bör verksamheten inför denna nya behandlingsform genomföra en konsekvensbedömning.
I övrigt bör verksamheten identifiera och vid behov genomföra nödvändiga konsekvensbedömningar.

*Konsekvensbedömningar för alla potentiella högriskbehandlingar av personuppgifter?*
Inga konsekvensbedömningar har genomförts under 2021.

*Är de genomförda konsekvensbedömningarna aktuella?*
Inga konsekvensbedömningar har genomförts under 2021.

### 3.4.4 DSO anger hur allvarliga bristerna är på en skala

| | |
|---|---|
| X | 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 |

### 3.4.5 DSO ger råd och rekommendationer till PUA
Överförmyndarnämnden rekommenderas att under 2022 säkerställa att nödvändiga konsekvensbedömningar identifieras och vid behov genomförs.

## 3.5 Individens rättigheter

### 3.5.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer? | 1 |
| Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar? | 1 |

### 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 PUA 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. I undantagssituationer kan denna tidsfrist förlängas.

Om verksamheten inte klarar av att hantera en begäran från en registrerad person i enlighet med dataskyddsförordningens krav, kan det skada allmänhetens förtroende för hur staden hanterar personuppgifter. Det kan även leda till tillsynsärenden från Intetgritetsskyddsmyndighetens sida, med sanktioner som följd.

### 3.5.3 Resultat

*Verksamhetens förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist*

Verksamheten har tydliga rutiner för hur en begäran om registerutdrag ska handläggas. Det finns också en ny

ansökningsblankett framtagen där den sökande tydligare kan ange för vem begäran avser (om minderårig eller huvudman). Verksamheten håller på att ta fram en rutin för hur den sökandes identitet kan styrkas i enlighet med dataskyddsförordningens bestämmelser. Processen för att handlägga en begäran bedöms dock vara fullgod.

### 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

Överförmyndarnämnden bedöms ha en god förmåga att kunna hantera de registrerades rättigheter inom föreskriven tid. Antalet system ur vilka de registrerades uppgifter ska hämtas är till antalet få och arbetsinsatsen som krävs för att kunna fullgöra nämndens skyldigheter inom ramen för dataskyddslagstiftningen bedöms vara begränsad.

## 3.6 Personuppgiftsincidenter

### 3.6.1 Sammanfattning

| Fråga/kontroll | Svar |
|---|---|
| Hur upptäcks personuppgiftsincidenter? | Anmälan av enskilda medarbetare. |
| Hur många personuppgiftsincidenter har dokumenterats? | 4 |
| 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 |

### 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.” En personuppgiftsincident skiljer sig från många andra typer av incidenter genom att innehålla just personuppgifter. Därför omfattar den här granskningen enbart personuppgiftsrelaterade incidenter, inte övriga former av rapporterade incidenter.

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering.

Rapporteringsskyldighet gäller som huvudregel för alla personuppgiftsincidenter. Undantag från rapporteringsskyldigheten gäller enbart om det är ”osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter” (se artikel 33). Detta innebär att de

flesta personuppgiftsincidenter ska rapporteras till Integritetsskyddsmyndigheten, inte senare än 72 timmar efter att verksamheten fått vetskap om incidenten.
Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter, ska rapportering även ske till de berörda registrerade personerna, utan dröjsmål. Dataskyddsförordningen delar alltså in personuppgiftsincidenter i tre kategorier: ingen rapportering, rapportering till Integritetsskyddsmyndigheten samt rapportering till de berörda personerna. Bristande förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner från Integritetsskyddsmyndigheten sida.

Enligt dataskyddsförordningen artikel 33.5 ska alla personuppgiftsincidenter dokumenteras, det vill säga även i de fall då incidenten inte ska rapporteras till Integritetsskyddsmyndigheten. Bristande dokumentation står i strid med Dataskyddsförordningen och leder också 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

*Verksamhetens förmåga att rapportera personuppgiftsincidenter i tid till Integritetsskydds-myndigheten?*
Verksamheten har en god beredskap för att kunna anmäla in incidenter till Integritetsskyddsmyndigheten. Rutinen är tydlig för hur anmälningsprocessen ska gå till och dataskyddsombudets möjligheter att snabbt kunna skaffa sig tillgång till nödvändig information för att kunna avgöra om en anmälan är nödvändig bedöms som mycket goda.

### 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

Överförmyndarnämnden bedöms ha en god förmåga att kunna anmäla personuppgiftsincidenter till tillsynsmyndigheten inom föreskriven tid.

# 4 Genomförda granskningar under året

## 4.1 Sammanfattning

Inga granskningar har genomförts under 2021.

## 4.2 Syfte

Granskningen är avsedd att säkerställa att verksamheten uppfyller skyldigheterna i Dataskyddsförordningen. En granskning kan därför innehålla kontroller av sådant som tidigare bedömts fungera för att säkerställa att dessa bedömningar fortfarande är giltiga.
Normalt sett bedöms tre granskningar vara en rimlig insats under ett verksamhetsår. Granskningsområdena väljs utifrån ett *riskbaserat synsätt*, det vill säga att fokus ligger på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkterna i årsrapporten som visar på brister. På så sätt 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.

## 4.3 Genomförda granskningar och deras resultat

Förvaltningen har under 2021 inte genomfört några granskningar. Det beror på att verksamheten under året tvingats avbryta ett stort införandeprojekt rörande nytt verksamhetssystem vilket lett till att mycket arbete fokuserats på att styra arbetet med en upphandling av ett nytt system. Hela organisationen har ägnat all tid åt att säkra processerna så att verksamheten inte blir lidande under kommande år, då det nya systemet ska driftsättas.

## 4.4 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet har inga rekommendationer att lämna till detta avsnitt.

# 5 Risker inom dataskydd

## 5.1 Sammanfattning

Relevanta risker inom verksamheten:

- Utbildningar inom GDPR/Dataskydd.
- Översikt av personuppgiftsbiträden som verksamheten använder (inklusive överföringar till tredjeland om relevant).

## 5.2 Syfte

Verksamheten ansvarar för att göra vissa typer av riskanalyser, så som konsekvensbedömningar och informationsklassningar, men dessa ger inte en heltäckande bild av personuppgiftsriskerna i verksamheten. Riskanalyserna ger en överblick över alla risker i verksamhetens samtliga personuppgiftsbehandlingar.

## 5.3 Resultatet av riskkartläggningen

*Utbildningar inom GDPR/Dataskydd*

Behovet av kunskap om hur ett gott dataskydd uppnås behöver stärkas inom verksamheten. Mängden information som verksamheten behandlar, graden av känslighet samt tiden som uppgifterna behandlas är viktiga riskfaktorer att omhänderta med hjälp av utbildning. I dagsläget erbjuder verksamheten de obligatoriska informationssäkerhets- och dataskyddsutbildningar som stadsledningskontoret tagit fram till samtliga anställda och särskilt till nyanställda. Därutöver bör verksamheten också erbjuda breda och fördjupade utbildningar inom dataskyddet för att öka medvetenheten kring dataskydd. I dagsläget erbjuds dock inte sådana utbildningar vilket är en brist som behöver åtgärdas.

| | |
|---|---|
| | 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 |

*Rutiner för konsekvensbedömningar*

Som tidigare nämnts har verksamheten inte genomfört några konsekvensbedömningar av personuppgiftsbehandlingarna. Det

saknas också mallar och rutiner för hur sådana konsekvensbedömningar ska genomföras.

| | |
|---|---|
| X | 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 |

## 5.4 DSO ger råd och rekommendationer till PUA

Överförmyndarnämnden rekommenderas att under 2022 säkerställa att alla anställda erbjuds utbildningar inom dataskydd för att stärka medvetenheten om dataskyddsarbetet. Därtill rekommenderas förvaltningen att under 2022 ta fram rutiner och mallar för konsekvensbedömningar som verksamheten kan använda vid införandet av nya personuppgiftsbehandlingar.

# 6 Planerade granskningar under det nya verksamhetsåret

## 6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten för 2022:

- Registerförteckningen
- Uppgiftsinsamling
- Bevarande av uppgifter

## 6.2 Planerade granskningar

Förvaltningen rekommenderas att under 2022 genomföra följande granskningar:

*Granskning 1*

**Finns all behandling (inklusive ev. förändringar som gjorts i behandlingen eller dess ändamål) dokumenterad i registerförteckningen [enligt kraven i artikel 30]?**

Registerförteckningen ska följas upp i samband med den årliga inventeringen av personuppgiftsbehandlingarna. Eftersom registerförteckningen över tid är ett levande register bör verksamheten därför rikta särskild uppmärksamhet mot att granska hur registerförteckningen är uppbyggd och uppdaterad. Om registerförteckningen uppdaterats ska det också framgå vad som ändrats och när.

Granskningen genomförs som en del av inventeringen, det vill säga kraven i artikel 30 jämförs med den upprättade registerförteckningen för att säkerställa att alla behandlingar är korrekt dokumenterade. Granskningen utförs under andra halvan av 2022 för att säkerställa att så många nyregistreringar som möjligt omfattas av granskningen.

Målet med granskningen är att måluppfyllnaden om en korrekt upprättad registerförteckning ska uppgå till 100%. Måluppfyllnaden ska visa på hur många korrekt dokumenterade behandlingar som finns i registerförteckningen.

*Granskning 2*

**När uppgifter samlas in, finns och efterlevs rutiner som ger den registrerade information enligt kraven i artikel 14?**

Granskningen görs mot de blanketter som verksamheten använder sig av när någon

- anmäler behov av ett ställföreträdarskap
- lämnar klagomål mot ställföreträdarskap
- ansöker om tillstånd att sälja eller köpa fastighet
- ansöker om tillstånd för underårig att bedriva näring.

Granskningen utförs under första kvartalet 2022.

Målet med granskningen är att måluppfyllnaden om väl fungerande rutiner med god efterlevnad uppgår till 100%.

*Granskning 3*

**Behandlas enbart uppgifter som faktiskt behövs för att uppnå de angivna ändamålen? (Uppgiftsminimering) och bevaras uppgifterna bara så länge som de är nödvändiga för det ändamål för vilket de samlades in? (Lagringsminimering)**

Granskningen görs genom stickprov bland kompletteringar till redovisningshandlingar i 20 avslutade akter samt i det befintliga verksamhetssystemet Wärna. Syftet är att kontrollera att enbart kompletteringar begärts som krävts för att kunna slutföra redovisningsgranskningen begärts in, samt att kontrollera att akterna gallrats från sådana personuppgifter som inte behöver arkivbevaras när akten upphört.

Granskningen utförs under första halvåret 2022.

Målet med granskningen är att måluppfyllnaden om korrekt insamlade och gallrade personuppgifter uppgår till 100%.

# 7 Övrigt att rapportera

## 7.1 Sammanfattning

Verksamheten handlägger ärenden som uteslutande behandlar personuppgifter av olika slag och därför är medvetenheten generellt god hos medarbetarna vad beträffar dataskydd. Dataskyddsarbetet påverkas dock av verksamhetens kunskap och förståelse för hur information ska handläggas på ett informationssäkert sätt. Här bedöms förvaltningen ha ett större behov av utveckling.

## 7.2 Övriga observationer

*Observation 1*

Dataskyddsombudet noterar att det i vissa fall råder osäkerhet kring hur eposten får användas vid kommunikation innehållande personuppgifter. En del externa myndigheter tillåter epostkommunikation innehållande personuppgifter med stöd av krypterad överföringsteknik. Andra saknar sådan teknik och tillåter därför inte sådan kommunikation. Det skapar osäkerhet hos medarbetarna om vad som egentligen gäller.

*Observation 2*

Dataskyddsombudet noterar också att det i vissa delar råder osäkerhet i hur verksamheten hanterar informationssäkerheten. Främst gäller detta hanteringen av inloggningen i datorerna och hanteringen av fysiska handlingar vid skrivbordsplatserna.

## 7.3 DSO ger råd och rekommendationer till PUA

Överförmyndarnämnden rekommenderas att under 2022 säkerställa att alla anställda erbjuds praktisk information om hur det vardagliga arbetet kan bedrivas på ett dataskyddssäkert sätt. Vidare bör alla anställda erbjudas praktiska tips på hur handläggningen kan ske på ett informationssäkert sätt.