

GDPR Årsrapport

2023

Överförmyndarnämnden

GDPR Årsrapport 2023

Januari 2024

Dnr: Klicka här för att ange Dnr

Utgivningsdatum: Klicka här för att ange utgivningsdatum

Kontaktperson: Kristofer Gisslén

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 *dokumenteringsskyldighet*. Årsrapporten är även ett medel för nämnds/bolagsstyrelsens uppföljning och styrning av verksamhetens systematiska integritets- och dataskyddsarbete.

Innehållsförteckning

Bakgrund	3
Innehållsförteckning	4
Sammanfattning	5
1. Obligatoriska rapporteringsområden	7
1.1. Registerförteckning	8
1.2. Styrdokument	11
1.3. Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar	13
1.4. Konsekvensbedömningar.....	15
1.5. Individens rättigheter	18
1.6. Personuppgiftsincidenter.....	20
2. Genomförda granskningar	23
2.1. Sammanfattning	23
2.2. Syfte	23
2.3. Genomförda granskningar och deras resultat.....	23
2.4. DSO ger råd och rekommendationer till PUA	24
3. Risker inom dataskydd	25
3.1. Sammanfattning	25
3.2. Syfte	25
3.3. Resultat av riskkartläggningen	25
3.4. DSO ger råd och rekommendationer till PUA	26
4. Planerade granskningar under det nya verksamhetsåret...	27
4.1. Sammanfattning	27
4.2. Planerade granskningar	27
5. Övrigt att rapportera	29
5.1. Sammanfattning	29
5.2. Övriga obeservationer	29
5.3. DSO ger råd och rekommendationer till PUA	29

Sammanfattning

I egenskap av ert Dataskyddsombud (DSO) lämnar jag följande årsrapport.

Jag har sedan våren 2021 innehaft uppdraget som DSO och har sedan dess verkat för att stärka den interna kontrollen över de personuppgifter som behandlas, samt bevaka att incidenter rapporteras i stadens incidenthanteringssystem.

Jag kan konstatera att medvetenheten inom överförmyndarnämndens verksamhetsområde är fortsatt god vad gäller dataskyddet. En bidragande 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.

I föregående årsrapport rekommenderades överförmyndarnämnden att åtgärda ett antal redovisade brister. 2023 har präglats av övergången mellan två verksamhetssystem (Wärna och LEX) vilket menligt påverkat förmågan att aktivt arbeta med dataskyddet. I denna rapport redogör jag för de upptäckter jag gjort under året vid uppföljningen av föregående års uppdrag.

Jag kan konstatera att jämte medarbetarnas kunskap om skyldigheten att anmäla incidenter till Integritetsskyddsmyndigheten, brister det alltså i kunskapen om skyldigheten att rapportera och dokumentera alla former av personuppgiftsincidenter. Alldeles för få ärenden inrapporteras i incidenthanteringssystemet i förhållande till löpande avvikelser som torde uppstå i verksamheten. Bristen härleds helt till bristande utrymme för utbildning i dataskyddet för såväl nyanställd som befintlig personal. Stärkt medvetenhet om att alla medarbetare är skyldiga att meddela sin närmsta chef om incidenter och själva anmäla in det i incidenthanteringssystemet är nyckeln till att eliminera denna brist.

Vidare finns det alltså brister rörande överförmyndarnämndens avsaknad av rutiner för konsekvensbedömningar i enlighet med dataskyddsförordningen. I föregående års rapport lyftes särskilt vikten att sådana rutiner skulle inrättas under 2023 och att samtliga informationsbehandlingar skulle inventeras i syfte att avgöra om och i så fall vilka behandlingar som måste konsekvensbedömas. Under 2023 har inventeringen genomförts och all informationsbehandling har därefter informationssäkerhetsklassats. En följd av detta är att all information nu också kan registerföras i enlighet med dataskyddsförordningen. Med detta bedöms

överförmyndarförvaltningen ha tagit ett stort steg framåt i sin informationshantering och arbetet med att säkerställa säkerheten kring informationsmaterian.

1. 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.

1.1. Registerförteckning

1.1.1. Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	23 behandlingar är upptagna i ett excelark, varav 9 stycken uppdaterats i verksamhetssystemet Visma Draftit Privacy Records.
Har nödvändiga uppdateringar gjorts?	Nej.
Bedöms registerförteckningen vara fullständig?	Delvis. Den fysiska registerförteckningen bedöms vara fullständig. Visma Draftit Privacy Records är inte fullständig.
Har verksamheten lämpliga rutiner för registerföring?	Uppfylls.

1.1.1. 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.

1.1.2. Resultat

Antalet registrerade behandlingar

Den ursprungliga registerförteckningen som upprättades i ett Excel-ark innehåller 23 behandlingar grundande i de processer som verksamheten arbetar med. Nio av dessa har förts över till det

digitala stödet Visma Draftit Privacy Records och i samband med detta också 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 har i de tidigare årsrapporterna bedömts vara komplett om än inte uppdaterad, utifrån den kunskap som då fanns. Efter att informationssäkerhetsklassningen genomförts under 2023 kan det konstateras att den ursprungliga registerförteckningen varit långt ifrån komplett. Först när den klassade informationen överförs till Visma Draftit Privacy Records kan överförmyndarförvaltningen anses ha en komplett registerförteckning.

Rutiner för registerföring

Det finns tydliga rutiner för hur registerföringen ska gå till och instruktionen om hur mallen för registerföring ska ifyllas bedöms pedagogisk. Visma Draftit Privacy Records innehåller tydliga instruktioner och rutiner som vägledning för den som ska genomföra registreringen i systemet.

1.1.3. 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

Överförmyndarförvaltningens samlade hantering av registerförteckningen bedöms uppfylla alla ställda krav även om den ännu inte är registrerad i Visma Drafit Privacy Records. Informationssäkerhetsklassningen innebär att upprättandet av registerförteckningen endast är en formaliafråga. Förteckningen behöver dock ställas under årlig översyn. Av stadsledningskontorets mall för dataskyddsombudet årsplan framgår det att "[d]ataskyddsombudet bör genomföra en årlig genomgång av behandlingsregistret i syfte att kontrollera att uppgifterna är uppdaterade och aktuella". En gång per år bör således räcka för att säkerställa aktualiteten i registerförteckningen.

1.1.4. DSO ger råd och rekommendationer till PUA

Överförmyndarnämnden rekommenderas att under 2024 säkerställa att informationssäkerhetsklassningen i sin helhet överförs till det digitala stödet Visma Drafit Privacy Records så att en fullgod registerförteckning färdigställs.

1.2. Styrdokument

1.2.1. 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

1.2.2. 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.

1.2.3. 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.

Förvaltningen rekommenderades i föregående årsrapport att åtgärda denna brist. Bristen konstateras fortfarande råda och måste prioriteras under 2024.

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.

1.2.4. 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

1.2.5. DSO ger råd och rekommendationer till PUA

Överförmyndarnämnden rekommenderas att under 2024 säkerställa att rutindokumentationen separeras från mallar och informationsmaterial för att förenkla för medarbetarna att hitta dessa.

1.3. Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingar

1.3.1. Sammanfattning

Fråga/kontroll	Svar
Hur många av personuppgiftsbehandlingarna som finns i verksamheten har informationsklassats?	Samtliga
Är klassade personuppgiftsbehandlingar aktuella?	Ja.

1.3.2. 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 informationsklassning 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.

1.3.3. Resultat

Eftersom all information som förekommer i verksamheten blivit informationssäkerhetsklassad under året har också samtliga brister på området undanröjts. I förra årsrapporten rapporterades allvarliga brister som krävde omgående insatser. Vid denna granskning bedöms samtliga brister vara åtgärdade på detta område.

1.3.4. 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

1.3.5. DSO ger råd och rekommendationer till PUA

Överförmyndarnämnden bedöms ha förmågan att kunna bedriva ett gott dataskyddsarbete. DSO har inga rekommendationer att lämna till detta avsnitt.

1.4. Konsekvensbedömningar

1.4.1. 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?	-

1.4.2. 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.

1.4.3. Resultat

Inga konsekvensbedömningar har genomförts under 2023. Under 2023 övergick verksamheten i ett nytt digitalt verksamhetssystem (LEX) som inneburit delvis nya arbetssätt i informationsbehandlingen – arbetssätt som skulle kunna medföra att en konsekvensbedömning blir nödvändig. Redan under 2022 framkom det att just denna kunskap, det vill säga den om vikten av att *alltid* överväga om ett nytt arbetssätt innebär nya former eller typer av behandlingar, brister i verksamheten. Många ser övergången som ett byte av ett digitalt system, där information endast byter lagringsplats, inte som ett sådant förändrat arbetssätt som kan få konsekvenser för personuppgiftsbehandlingen.

Verksamheten bör därför ha som utgångspunkt att *alla* nya behandlingar ska 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

Informationssäkerhetsklassningen genomförs i form av en inventering av information utifrån de arbetsprocesser som verksamheten identifierat. På så sätt bör verksamheten i dagsläget vara väl förtrogen med såväl befintliga som nya arbetssätt. Under 2024 bör därför konsekvensbedömningar göras utifrån denna kunskap.

Konsekvensbedömningar för alla potentiella högriskbehandlingar av personuppgifter?

Inga konsekvensbedömningar har genomförts under 2023.

Är de genomförda konsekvensbedömningarna aktuella?

Inga konsekvensbedömningar har genomförts under 2023.

1.4.4. 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
X	Brister identifierade som bör åtgärdas men ej bedöms vara brådskande, omfattande eller allvarliga
	Inga brister av nämnvärd betydelse identifierade

1.4.5. DSO ger råd och rekommendationer till PUA

Riskenivån bedöms ha sänkts under 2023 från omfattande med krav på omgående åtgärder till brister som inte bedöms omfattande, med hänvisning till att informationssäkerhetsklassningen inneburit en större medvetenhet inom verksamheten för de informationsmängder som behandlas. Möjligheterna att kunna genomföra konsekvensbedömningar bedöms bättre inför 2024 än 2023. Överförmyndarnämnden rekommenderas därför att under 2024 säkerställa att nödvändiga behov av konsekvensbedömningar identifieras och att eventuella konsekvensbedömningar genomförs.

1.5. Individens rättigheter

1.5.1. 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?	-

1.5.2. 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 Integritetsskyddsmyndighetens sida, med sanktioner som följd.

1.5.3. 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. En förfrågan har ställts till stadens övriga DSO om att skapa ett enhetligt kontrollsystem för att säkerställa att den som begär ett registerutdrag verkligen är vem den utger sig för att vara. Processen för att handlägga en begäran bedöms dock vara fullgod.

1.5.4. 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

1.5.5. 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.

1.6. Personuppgiftsincidenter

1.6.1. Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Anmälan av enskilda medarbetare.
Hur många personuppgiftsincidenter har dokumenterats?	10
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	1
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	0

1.6.2. 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.

1.6.3. Resultat

Verksamhetens förmåga att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten?

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. Medvetenheten saknas dock fortfarande inom förvaltningen om vad som ska betraktas vara en personuppgiftsincident och var sådana incidenter ska anmälas.

Under året har en incident inträffat som anmälts till IMY. På grund av missar i den interna kommunikationen anmäldes den inte inom 72-timmars fristen utan först en och en halv vecka för sent. Dataskyddsombudet ser allvarligt på det inträffade, men bedömer inte att det beror på ett systemfel utan på missar i det enskilda fallet.

1.6.4. 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

1.6.5. DSO ger råd och rekommendationer till PUA

Överförmyndarnämnden bedöms ha en god förmåga att kunna anmäla personuppgiftsincidenter till tillsynsmyndigheten inom föreskriven tid. Nämnden rekommenderas dock att under 2024 säkerställa att medvetenheten kring dokumentationsskyldigheten i stadens incidentrapporteringssystem stärks hos samtliga medarbetare. Nämnden rekommenderas också säkra att dataskyddsombudet har en designerad backup som träder i dess ställe vid frånvaro för att undvika brister i rapporteringsskyldigheten.

2. Genomförda granskningar

2.1. Sammanfattning

Förvaltningen skulle under 2023 genomföra tre granskningar:

- **Granskning 1:** Finns all behandling (inklusive ev. förändringar som gjorts i behandlingen eller dess ändamål) dokumenterad i registerförteckningen [enligt kraven i artikel 30]?
- **Granskning 2:** När uppgifter samlas in, finns och efterlevs rutiner som ger den registrerade information enligt kraven i artikel 14?
- **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)

2.2. 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.

2.3. Genomförda granskningar och deras resultat

Granskning 1

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

Under 2023 har granskning av registerförteckningen inte genomförts. Målet har istället varit att upprätta en helt ny registerförteckning utifrån informationssäkerhetsklassningen, då *alla* informationsmängder som behandlas i verksamheten

inventerats och därför med enkelt handgrepp kan registreras i registerförteckningen. Under 2024 ska den befintliga registerförteckningen ersättas av en helt ny.

Granskning 2

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

Granskningen har inte hunnit genomföras under 2023.

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 har inte hunnit genomföras under 2023.

2.4. DSO ger råd och rekommendationer till PUA

Överförmyndarnämnden rekommenderas att under 2024 säkerställa att alla verksamhetens blanketter tillförs information om syftet med insamlingen av personuppgifter, bevarandetid och hänvisning till var man kan läsa mer om överförmyndarnämndens behandling av personuppgifter. Därtill rekommenderas nämnden att behålla samma granskningsområden för 2024 för att säkerställa att dessa grundläggande områden hanteras korrekt.

3. Risker inom dataskydd

3.1. Sammanfattning

Relevanta risker inom verksamheten:

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

3.2. 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 personuppgiftsbehandlings.

3.3. Resultat 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.

Under 2023 har det inte funnits utrymme att erbjuda utbildningar inom området. Bristen kvarstår därför från föregående års rapport och måste prioriteras under 2024. Under 2023 har förvaltningen istället fokuserat på att bygga upp ett stabilt informationssäkerhetsarbete genom att klassa all den information som behandlas i verksamheten. Med den på plats, och med ett upprättat årshjul för informationssäkerhetsarbetet går det under 2024 att planera in interna utbildningar i dataskydd.

	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

3.4. DSO ger råd och rekommendationer till PUA

Överförmyndarnämnden rekommenderas att under 2024 säkerställa att alla anställda erbjuds utbildningar inom dataskydd för att stärka medvetenheten om dataskyddsarbetet. Därtill rekommenderas förvaltningen att under 2024 ta fram rutiner och mallar för konsekvensbedömningar som verksamheten kan använda vid införandet av nya personuppgiftsbehandlingar.

4. Planerade granskningar under det nya verksamhetsåret

4.1. Sammanfattning

Relevanta granskningsområden inom verksamheten för 2024:

- Registerförteckningen
- Uppgiftsinsamling
- Bevarande av uppgifter

4.2. Planerade granskningar

Förvaltningen rekommenderas att under 2024 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 2024 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 ställföreträderskap
- lämnar klagomål mot ställföreträderskap
- ansöker om tillstånd att sälja eller köpa fastighet
- ansöker om tillstånd för underårig att bedriva näring.

Granskningen utförs under andra kvartalet 2024.

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 verksamhetssystemet. 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 tredje halvåret 2024.

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

5. Övrigt att rapportera

5.1. Sammanfattning

Verksamheten handlägger ärenden som uteslutande behandlar personuppgifter av olika slag och därför är medvetenheten generellt god hos medarbetarna vad beträffar hanteringen av känslig information. 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, men rörande detta område har DSO redan lämnat rekommendationer enligt ovan.

5.2. Övriga obeservationer

Inga övriga obeservationer har gjorts under 2023.

5.3. DSO ger råd och rekommendationer till PUA

DSO har inga rekommendationer att lämna till detta avsnitt.