Stockholms stad

GDPR Årsrapport

2021

Servicenämnden

GDPR årsrapport
Januari 2021

Dnr: SF 2022/35
Utgivningsdatum: 2022-01-21
Kontaktperson: Ann-Marie Svärd

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.

Innehåll

2 Sammanfattning

I egenskap av servicenämndens dataskyddsombud lämnar jag följande årsrapport.

Under året har person som innehar rollen som dataskyddsombud förändrats så sent som under senare delen av oktober månad. Rapporteringen har därför i stora delar skett genom avrapportering från nämndens tidigare dataskyddsombud. Då rollen som dataskyddsombud kräver såväl kompetens inom juridik inom offentlig sektor, dataskyddsförordningen samt kunskap inom IT har förvaltningen gjort bedömningen att förvaltningen behöver göra en förstärkning. Förvaltningen har därför påbörjat dialog om gemensam lösning av dataskyddsombud. Tillsammans med fem andra facknämnder inom staden har förvaltningen avsikt att tillsammans genomföra en gemensam lösning av dataskyddsombud.

En fråga som ännu inte är klarlagd är vem som är personuppgiftsansvarig, personuppgiftsbiträde och eventuellt underbiträde för de personuppgifter som behandlas inom de processer som förvaltningen utför för andra nämnders räkning. Frågan är komplex och förvaltningens tidigare dataskyddsombud och juridiska avdelningen inom Stadsledningskontoret samarbetar för att komma fram till svaren.

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. Servicenämnden är personuppgiftsansvarig.

De obligatoriska rapporteringsområdena är

- behandlingsregister (benämns även som 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 mina och min företrädares genomförda uppföljningar och granskning.

3.1 Behandlingsregister

3.1.1 Sammanfattning

För att något ska gå att skydda måste det först vara synligt för verksamheten. För att följa dataskyddsförordningen ska därför stadens alla förvaltningar och bolag inventera alla personuppgifter som behandlas i verksamheten, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde, och dokumentera dem i ett så kallat behandlingsregister.

Behandlingsregistret skapar en intern synlighet och förståelse för vilka personuppgifter som behandlas samt hur de hanteras. Behandlingsregistret är därför dataskyddsarbetets centrala utgångspunkt och bas samt säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling

3.1.2 Syfte

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	91 behandlingar för över 800 handlingstyper[1] finns registrerade
Har nödvändiga uppdateringar gjorts?	Ja, uppdaterat 2021-10-18, uppdateras kontinuerligt.
Bedöms registerförteckningen vara fullständig?	Delvis. Förteckningen bedöms i stort som fullständig men för ett tjugotal handlingstyper saknas information om rättslig grund och/eller typ av personuppgift som behandlas.
Har verksamheten lämpliga rutiner för registerföring?	Ja

[1] Behandlingstyp kan förklaras som viss typ av information/dokument, var dessa förvaras och gallringsfrister för dessa enligt Stadsarkivets beslut.

Förvaltningen har inkluderat behandlingsregistret i förvaltningens hanteringsanvisningar. Hanteringsanvisningarna utgår från stadsarkivets informationsklassificering utifrån dataskyddsförordningen och offentlighets- och sekretesslagen. Det innebär att majoriteten av de personuppgiftsbehandlingar som förekommer inom förvaltningen finns dokumenterade.

Registret är uppdaterat under året med undantag av Kontaktcenters enhet för samhällsbyggnadsfrågor, samt förvaltningens förvaltning av systemstöd för nytt ärendehanteringssystem. Uppdatering för dessa är planerat att genomföras under våren år 2022. Bedömningen är dock att det inte bör vara någon förändring av personuppgiftsbehandlingarna i sak med anledning av införandet av förvaltningens gemensamma ärendehanteringssystem.

De mest väsentliga systemen ingår, till exempel ekonomisystem, personalsystem och förvaltningens gemensamma ärendehanteringssystem. Andra system och personuppgiftsbehandling i dessa saknas i behandlingsregistret.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats

I behandlingsregistret finns över 800 olika typer av handlingstyper för 91 processer med personuppgiftsbehandlingar.

DSO kontrollerar om nödvändiga uppdateringar gjorts

Uppdateringar har skett för majoriteten av förvaltningens verksamheter. Kvar att uppdatera är de personuppgiftsbehandlingar som sker inom Kontaktcenters enhet för samhällsbyggnadsfrågor, samt förvaltningens förvaltning av systemstöd för nytt ärendehanteringssystem. Dessa uppdateringar är planerade att göras under våren 2022. I sak bör förändringen från ett ärendehanteringssystem till ett annat inte innebära några större förändringar från det som finns sedan tidigare i behandlingsregistret.

DSO bedömer hur fullständig registerförteckningen är

Min bedömning är att behandlingsregistret i princip är fullständigt.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Bedömningen är att verksamheten till största delen har lämpliga rutiner för registerföring.

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

Förvaltningens behandlingsregister är tydligt strukturerat och utgår från förvaltningens processer och stadsarkivets informationsklassificering. Det finns en organisation inom förvaltningen som arbetar med att hålla hanteringsanvisningar och behandlingsregister uppdaterat. I och med införande av förvaltningens gemensamma ärendehanteringssystem har uppdatering skett av såväl hanteringsanvisningar som behandlingsregister. Detta gäller med undantag av behandlingar som registreras inom Kontaktcenter samhällsbyggnadsfrågor samt förvaltningens förvaltning av det nya ärendehanteringssystemet. Bedömningen är dock att behandlingarna i sak inte bör skilja sig åt mellan det nya och det tidigare ärendehanteringssystemet. För ett tiotal handlingstyper i behandlingsregistret saknas information om vilken typ av personuppgifter som behandlas och eller rättslig grund för handlingstypen.

De mest väsentliga informationstillgångarna som finns i IT-system med personuppgiftsbehandling finns i behandlingsregistret.

3.1.5 DSO ger råd och rekommendationer till PUA

PUA bör ge förvaltningen i uppdrag att:

- utreda om behandlingsregistret ska kompletteras med vilken nivå för klassning som gjorts enligt samma principer som systemet KLASSA. Detta för att snabbt få en bild av klassningen av samtliga personuppgiftsbehandlingar
- uppmana berörda verksamheter att komplettera behandlingsregistret med typ av personuppgifter som registreras samt rättslig grund där uppgift saknas

3.2 Styrdokument

3.2.1 Sammanfattning

Fråga/kontroll	Svar
Finns lämplig styrande dokumentation på plats?	Delvis
Håller innehållet i de existerande dokumenten lämplig kvalitet?	Delvis
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Delvis
Är dokumenten uppdaterade?	Delvis
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja.

3.2.2 Syfte

Området syftar till att PUA genom styrdokument ska kunna visa att den bedriver ett systematiskt dataskyddsarbete och att den styr sina medarbetares hantering av personuppgifter. Genom styrdokument kommunicerar PUA till medarbetare i sin verksamhet om vad som gäller och vad som förväntas av medarbetarna, när de hanterar personuppgifter. Att styrdokument finns nedtecknade, beslutade och kommunicerade medför att medarbetaren får dataskyddsinformation och kan behålla kunskapen över tid och tillämpa den på ett konsekvent sätt. En röd tråd i Dataskyddsförordningen är att viktiga arbetssätt och rutiner ska vara dokumente-

rade. Detta följer bland annat av kravet på att den personuppgifts-ansvarige måste kunna visa att dataskydds-förordningens principer för behandling av personuppgifter efterlevs (artikel 5).

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?
Information och styrande dokument finns samlade på förvaltningens samarbetsyta. Samarbetsytan är uppdelad i olika områden. Ansvarig för respektive område framgår av samarbetsytan. Ansvarig för information och styrande dokument kan därmed sägas ha utpekade ägare. På samarbetsytan finns också länkar till stadens styrande dokument.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet
Rutin för hur verksamheten hanterar den registrerades rättigheter (artikel 15-21).
Det finns risk att medarbetare gör fel när de ska distribuera information via brev till medborgare och har inträffat tidigare år.

Rutin för behörighethetstilldelning, förändring och avslut finns men rutinen omfattar inte samtliga system.

Personuppgiftsincidentrutin finns. Rutinen beskriver hur personuppgiftsincidenter ska utredas, analyseras, rapporteras och dokumenteras. Rutinen anger tydligt vilken roll som ansvarar för vad i detta förfarande

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

PUA bör ge förvaltningen i uppdrag att:

- Ta fram rutin för konsekvensbedömning

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?	11
Är klassade personuppgiftsbehandlingar aktuella?	Delvis

3.3.2 Syfte

För att kunna skydda information (inklusive personuppgifter) med rätt slags skydd så ska verksamheten informationsklassa sin information. Stadens riktlinjer för informationssäkerhet föreskriver att alla stadens informationstillgångar ska vara klassade med stöd av SKR:s verktyg KLASSA. Utan informationsklassningen har verksamheten inte förutsättningar att välja rätt åtgärder för att skydda sin information. Det är därför av stor betydelse för dataskyddsarbetet att PUA ges en uppdaterad bild varje år av huruvida informationsklassning är genomförd för personuppgifter som verksamheten hanterar.

Ansvaret för att informationsklassning genomförs ligger på den del av verksamheten som är informationsägare. En första kontrollpunkt måste därför vara om en informationsägare eller en informationsägarrepresentant med ansvar för klassning är identifierad i verksamheten. Om en ansvarig för klassningen inte har pekats ut och känner till sitt ansvar för klassning, minskar sannolikheten avsevärt att en klassning faktisk initieras.

Notera att enbart sådan informationsklassning som avser behandling eller system som omfattar *personuppgifter* är av intresse för DSO:s årsrapportering.

Eftersom informationsklassning är ett arbete som görs inom ramen för informationssäkerhetsarbetet, bör DSO samråda och planera uppföljningen tillsammans med informationssäkerhetssamordnare. Enligt stadens metodik klassas personuppgifter och övrig information i samma workshop, och slutsatserna kring klassningen dokumenteras i samma protokoll.

3.3.3 Resultat

I KLASSA finns i december månad 11 system informationsklassats. Flertalet av dessa system används inte längre eller är på väg att avvecklas.

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

KLASSA bör uppdateras genom att de system som inte längre används märks upp/tas bort i KLASSA och kompletteras med eventuellt saknade system.

3.3.5 DSO ger råd och rekommendationer till PUA

PUA bör ge

- förvaltningen i uppdrag att utse ansvarig person för informationsklassning för de system som används och där behandling finns.
- alla chefer i uppdrag att kontrollera att alla ansvariga för informationsklassning har undersökt behovet av klassning och/eller uppdatering samt vid behov genomfört klassning/uppdatering under det kommande året.

3.4 Konsekvensbedömningar

Att göra en konsekvensbedömning är obligatoriskt endast om behandlingen sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Konsekvensbedömning ska göras både för befintliga behandlingar och innan en verksamhet börjar med en ny personuppgiftsbehandling.

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 anses liksom behandlingsregister och informationsklassning som ett viktigt verktyg för verksamhetens dataskyddsarbete. Kravet på konsekvensbedömning är dessutom ett uttryckligt krav enligt dataskyddsförordningen. och ska utföras för alla behandlingar som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter” (artikel 35.1).

3.4.3 Resultat

Förvaltningen saknar dokumenterad rutin för hur konsekvensbedömning ska dokumenteras och registreras samt vem som ansvarar för att konsekvensbedömning sker.

Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?
Nej.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?
Nej.

Är de genomförda konsekvensbedömningarna aktuella?
-

3.4.4 DSO anger hur allvarliga bristerna är på en skala

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

3.4.5 DSO ger råd och rekommendationer till PUA

PUA bör ge

- förvaltningen i uppdrag att tillse att rutin, som inkluderar roller, ansvarsfördelning och hur dokumentation av gjorda konsekvensbedömningar ska förvaras tas fram och implementeras inom förvaltningen under kommande år.
- alla chefer i uppdrag att till slutet av år 2022 tillse att verksamheten har kontrollerat behovet av konsekvensbedömningar och/eller uppdatering samt vid behov genomfört konsekvensbedömning/uppdatering.

3.5 Individens rättigheter

Fråga/kontroll	Svar
Hur många har inkommit med begäran om registerutdrag, begränsning, radering etc.?	Ingen begäran om registerutdrag finns
Hur många av dessa begäranden har hanterats av verksamheten inom 30 dagar?	-

3.5.1 Sammanfattning

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 personuppgiftsansvarig – dvs. i stadens fall nämnder och bolag – 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. (Notera dock att det finns undantagssituationer angivna i artikel 12.3, där fristen kan förlängas till mer än en månad.)

Dataskyddombudet har en roll i att granska efterlevnaden, identifiera brister samt ge råd och stöd hur processer och rutiner för att tillgodose rättigheterna bör utformas.

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 personuppgif-

ter. Det kan även leda till tillsynsärenden från Intetgritetsskyddsmyndighetens (”IMY”) sida, med sanktioner som följd. Det är därför viktigt att PUA regelbundet ges en bild av i vilken mån verksamheten klarar av att leva upp till regelverkets krav på att hantera begäran inom föreskriven tidsfrist.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

Rutin och stöddokument för verksamheterna vid begäran av registerutdrag finns på förvaltningens samarbetsyta. Bedömningen är därför att verksamheten har förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist. Enligt förvaltningens hanteringsanvisning ska handlingen gallras efter två månader. Detta innebär att frågan om antal inkomna begäran inte går att besvara. Då ingen begäran om registerutdrag, rättelse eller radering finns sparad går det alltså inte med säkerhet att säga om bedömningen är korrekt.

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

PUA bör ge

- alla chefer i uppdrag att årligen informera anställda om för begäran om registerutdrag och var förvaltningens rutin och stöddokument finns. Aktiviteten bör följas upp av dataskyddsombud genom att verksamheterna tillfrågas om information registerutdrag har tagits upp på APT under året.

- förvaltningen i uppdrag att rutin för registrator uppdateras med hur förvaltningen ska kunna ta fram uppgift om antal inkomna begäran.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	I de fall som registrerats under året upptäcktes incidenterna av mottagare av faktura/mejl.
Hur många personuppgiftsincidenter har dokumenterats?	Två incidenter under år 2021 finns loggat den 7 december 2021.
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	Ingen av dessa incidenter har bedömts behöva rapporteras till integritetsskyddsmyndigheten. I ett av fallen har rapportering skett till berörd person.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Ingen av incidenterna har rapporterats till tillsynsmyndighet

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.”

I en verksamhet kan förekomma många andra typer av incidenter, som inte involverar personuppgifter. Det är viktigt att hålla den saken i åtanke, så att årsrapporteringen inte omfattar annat än just personuppgiftsincidenter. Vidare är det en grundförutsättning för hanteringen av personuppgifter att incidenter över huvud taget upptäcks, samt att verksamheten förstår att hantera incidenter som rör personuppgifter på det särskilda sätt som dataskyddsförordningen kräver.

Hantering av personuppgiftsincidenter är en viktig och obligatorisk komponent bland dataskyddsförordningens olika verktyg för att åstadkomma en sund personuppgiftshantering.

3.6.3 Resultat

Hur väl förmår verksamheten att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten?

Min bedömning är att verksamheten har tillräcklig förmåga att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten.

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

PUA bör ge

- alla chefer i uppdrag att årligen informera anställda om rutin för rapportering av personuppgiftsincident och var förvaltningens rutin och stöddokument finns. Aktiviteten bör följas upp av dataskyddsombud genom att verksamheterna tillfrågas om information personuppgiftsincident har tagits upp på APT under året.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Granskning av behandlingsregister
- Granskning av rutin för registerutdrag
- Granskning av rutin för personuppgiftsincident

4.2 Syfte

En av dataskyddsombudets viktigaste uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen. En central del av det arbetet är att göra återkommande granskningar av hur väl dataskyddsförordningen efterlevs. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten kan fatta i fråga om dataskyddsåtgärder. För PUA är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och vad resultaten av granskningarna är.

4.3 Genomförda granskningar och deras resultat

Granskning av behandlingsregister

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

Granskning av rutin för registerutdrag

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

Granskning av rutin för personuppgiftsincident

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

4.4 DSO ger råd och rekommendationer till PUA

-

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- Att kommunikation som innehåller känsliga eller skyddade personuppgifter inte sker via säkra kanaler
- Att skyddade personuppgifter röjs

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. Dataskyddsombudet behöver som underlag för sin egen planering och sitt löpande arbete ha kontinuerlig överblick över dessa risker, i verksamhetens samtliga personuppgiftsbehandlingar. Exempelvis krävs en sådan överblick för att kunna välja ut vilka områden som bör granskas under det kommande året eller för att avgöra vilka råd som dataskyddsombudet behöver lämna till verksamheten om dataskyddsåtgärder som behöver vidtas.

5.3 Resultatet av riskkartläggningen

Risk 1 Att kommunikation som innehåller känsliga eller skyddade personuppgifter inte sker via säkra kanaler

	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

Risk 2 Att skyddade personuppgifter röjs

Risk finns att skyddade personuppgifter röjs. Förvaltningen bör fortsätta sitt arbete med att utveckla rutiner och att sekretessmarkering kan göras i system kravställs.

	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

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- Att behandlingsregistret hålls uppdaterat och ger en rättvisande bild av verksamhetens personuppgiftsbehandlingar.
- Kontroll av att rutiner för personuppgifter, känsliga och skyddade personuppgifter finns framtagna och efterlevs.
- Uppföljning av att det finns utpekade personer som är informationsägare inom förvaltningen
- Uppföljning av att de viktigaste informationsmängderna finns klassificerade och dokumenterade
- Uppföljning av kontroll av behörigheter
- Att kommunikation som innehåller känsliga eller skyddade personuppgifter sker via säkra kanaler
- Att dokumenterad rutin finns för hur konsekvensbedömning ska dokumenteras och registreras samt vem som ansvarar för att konsekvensbedömning sker.

Flertalet av dessa granskningar finns med i nämndens plan för intern kontroll 2022.

6.2 Syfte

En av dataskyddsombudets viktigaste uppgifter är att övervaka verksamhetens efterlevnad av dataskyddsförordningen. En central

del av det arbetet är att göra återkommande granskningar av hur väl dataskyddsförordningen efterlevs. Resultaten av granskningarna påverkar i stor utsträckning vilka beslut verksamheten kan fatta i fråga om dataskyddsåtgärder. För personuppgiftsansvarig är det därför av stor betydelse att få rapportering om vilka granskningar som gjorts under det gångna året och vad resultaten av granskningarna är.