Stockholms stad

Bilaga 03

Dataskyddsombudets årsrapport 2021

Dataskyddsombudets årsrapport
Januari 2022

Dnr: SÖD 2021/1253
Utgivningsdatum: 2022-02-25
Kontaktperson: Anna Remmets

Innehåll

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. För 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.

2 Sammanfattning

Dataskyddsombudet lämnar följande årsrapport.

Utifrån stadens centrala mall för årsrapportering har de obligatoriska rapporteringsområdena registerförteckning, styrdokument, tekniska och organisatoriska säkerhetsåtgärder för personuppgiftsbehandlingar, konsekvensbedömningar, individens rättigheter och personuppgiftsincidenter granskats.

I ett försök att intensifiera arbetet med registerförteckningen (här också kallad personuppgiftsförteckningen då det inte bara är register som ska redovisas) har dataskyddsredogörare utsetts på respektive avdelning. Deras arbete och förutsättningar behöver dock vidare utvärderas och personuppgiftsförteckningen innehåller fortfarande brister.

Ett annat område där brister har identifierats är i arbetet med konsekvensbedömningar, varför en satsning på detta behöver göras under 2022.

Det har vidare skett en märkbar ökning av inrapporterade personuppgiftsincidenter, vilket dock med stor sannolikhet kan tolkas positivt som att kunskapen om rapporteringsskyldigheten har ökat. Men då ett antal av dessa inte kommit till DSO:s kännedom i tid för rapportering till Integritetsskyddsmyndigheten inom de föreskrivna 72 timmarna efter upptäck behövs kunskap om befintlig rutin öka ytterligare.

De övriga granskningar som genomförts under 2021 var, förutom personuppgiftsförteckningen, tredjelandsöverföringar och behörighetskontroll. Vad gäller tredjelandsöverföringar bedöms efter informationsinsatser under året att medvetenheten på avdelningarna är relativt god. Frågan behöver dock fortsatt stå högt upp på dagordningen för dataskyddsarbete. Granskningen av behörighetskontroll visade att de flesta enheter har rutiner för att lägga till och ta bort behörigheter när medarbetare slutar men att man behöver arbeta mer med rutiner för kontinuerliga och övergripande kontroller.

Till 2022 års granskningsområden har DSO valt ut personuppgiftsförteckningen som också var bland 2021 års granskningsområden (då denna utgör grund för förvaltningens övriga dataskyddsarbete och fortsatt har brister), konsekvensbedömningar och information till registrerade.

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

3.1 Registerförteckning

3.1.1 Sammanfattning

Fråga/kontroll	Svar
Antal behandlingar som är registrerade?	Ca 313
Har nödvändiga uppdateringar gjorts?	Se kommentarer nedan
Bedöms registerförteckningen vara fullständig?	Nej
Har verksamheten lämpliga rutiner för registerföring?	Nya rutiner har införts men dessa behöver utvärderas.

3.1.2 Syfte

Det följer av dataskyddsförordningen (artikel 30) att stadens alla förvaltningar och bolag måste inventera alla personuppgifter som behandlas i verksamheten, både i rollen som personuppgiftsansvarig och personuppgiftsbiträde, och dokumentera dem i en så kallad registerförteckning (även kallat behandlingsregister).
När registerförteckningen är upprättad skapar den en intern synlighet och förståelse för vilka personuppgifter som behandlas samt hur de hanteras. Registerförteckningen är därför dataskyddsarbetets centrala utgångspunkt och bas samt säkerställer att verksamheten beaktar att det ska finnas en laglig grund för all personuppgiftsbehandling. Att ha en registerförteckning på plats leder till att verksamheten kan arbeta mer resurs- och kostnadseffektivt med sitt systematiska och riskbaserade dataskyddsarbete.

Syftet med detta rapporteringsområde är således att rapportera till PUA hur väl verksamhetens har lyckats inventera sina personuppgifter och de personuppgifter som behandlas för annans räkning samt upprätta en registerförteckning.
Eftersom inventeringen av personuppgifter i sig är avgörande för allt det fortsatta dataskyddsarbetet inom verksamheten, är denna lägesbild en av de viktigaste slutsatserna som PUA behöver förstå och ta ställning till inför det planerade åtgärdsarbetet under nästa verksamhetsår.

3.1.3 Resultat

Under 2021 har förvaltningen tillsatt dataskyddsredogörare vars huvudsakliga uppgift ska vara att flytta in och föra in nya personuppgiftsbehandlingar i systemstödet Draftit. Ledningen har beslutat att arbetet som dataskyddsredogörare ska utgöra 10 % av en heltid. Tanken med dataskyddsredogörare är att dessa, som jobbar mot specifika avdelningar, ska vara ett verksamhetsnära, operativt stöd som underlättar en kontinuerlig uppdatering av personuppgiftsförteckningar.

Det dröjde dock en bit in på året innan alla dataskyddsredogörare var utsedda och en del har inte haft möjlighet att komma igång och efterlyst ytterligare introduktion. Under 2022 behöver det utvärderas hur väl arbetssättet fungerar.

DSO kontrollerar hur många behandlingar som registrerats

Sedan 2020 har 13 behandlingar registrerats i Draftit. Alla dessa är inte nya, utan en del har förts över från de tidigare Excelförteckningarna.

DSO kontrollerar om nödvändiga uppdateringar gjorts

DSO bedömer att arbetat med att förteckna inte riktigt har kommit igång än.

DSO bedömer hur fullständig registerförteckningen är

De flesta enheter har tidigare lämnat in förteckningar över personuppgiftsbehandlingar, men merparten bedöms inte vara fullständiga och få uppdateringar har gjorts.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring

Arbetssättet med dataskyddsredogörare behöver utvärderas under 2022.

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
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

3.1.5 DSO ger råd och rekommendationer till PUA

Dataskyddsredogörarna är nu på plats och DSO kommer att ge dem ytterligare stöd. Det är dock viktigt att de i samråd med sina respektive chefer verkligen får möjlighet att avsätta de 10 % för dataskyddsarbete som ledningen tidigare har beslutat om. Varje avdelning/enhet behöver också upprätta en fungerande rutin för att underrätta dem om nya/ändrade personuppgiftsbehandlingar så att de kan registrera dessa.

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?	I stort sett
Finns ägare till dokumenten utpekade, så att uppdateringar kan bli gjorda vid behov?	Ja

3.2.2 Syfte

Genom styrdokument kommunicerar PUA till medarbetare i sin verksamhet 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 dokumenterade. Detta följer bland annat av kravet på att den personuppgiftsansvarige måste kunna visa att dataskyddsförordningens principer för behandling av personuppgifter efterlevs (artikel 5).

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?

Ja. Staden har på en central sida på intranätet samlat relevanta dokument.

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet

De dokument som finns håller lämplig kvalitet och uppdateras.

3.2.4 DSO anger hur allvarliga bristerna är på en skala

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

3.2.5 DSO ger råd och rekommendationer till PUA

Det är viktigt att de stadsgemensamma dokument som finns på intranätet är kända av ledningen och görs kända för medarbetare vid nyanställning och i olika sammanhang som arbetsplatsträffar (APT) eller liknande.

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?	8
Är klassade personuppgiftsbehandlingar aktuella?	Personuppgiftsförteckningarna behöver uppdateras för att kunna svara på det avseende äldre klassningar.

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. Notera att enbart sådan informationsklassning som avser behandling eller system som omfattar personuppgifter är av intresse för DSO:s årsrapportering. Förvaltningens informationssäkerhetssamordnare finns som stöd i detta arbete.

3.3.3 Resultat

Under 2021 har ett intensivt arbete med att utföra informationsklassningar inletts. Dessa är dock relativt tidskrävande och arbetet behöver fortsätta under 2022.

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

Det är viktigt att verksamheterna vet om att de vid anskaffning av nya system/tjänster eller inledande av nya processer behöver ta informationssäkerhet och dataskydd i beaktande och kontakta informationssäkerhetssamordnare och DSO innan arbetet inleds.

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?	Behöver fortsatt ses över med anledning av domen i Schrems II-målet.

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 registerförteckning 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

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

Då personuppgiftsförteckningarna inte är fullständiga eller uppdaterade går det inte att säkerställa den överblick som krävs för att identifiera behovet av konsekvensbedömningar av befintliga behandlingar. Vad gäller nya behandlingar så har DSO informerat

om behovet av att ta ställning till detta, samt skrivit in det i checklistan för direktupphandling.

Observera att svaret har ändrats sedan 2020 års rapport utifrån en ny analys av läget och inte på grund av att situationen har förändrats till det sämre.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?

Se resonemanget ovan.

Är de genomförda konsekvensbedömningarna aktuella?

Verksamheterna behöver utifrån sin inventering av tredjelandsöverföringar bedöma om det behöver göras nya konsekvensbedömningar.

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

För att kunna leva upp till dataskyddsförordningens krav att genomföra konsekvensbedömningar av vissa behandlingar behöver dels förvaltningens personuppgiftsförteckningar vara uppdaterade och dels behöver det finnas rutiner för att kontakta DSO inför upphandling eller införande av ny process som innebär personuppgiftsbehandlingar.

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 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.)
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 (IMY) sida, med sanktioner som följd.

3.5.3 Resultat

Har verksamheten förutsättningar att hantera registrerades rättigheter inom föreskriven tidsfrist?

Ja, verksamheten har förutsättningar men medarbetare bör kontinuerligt påminnas om dessa rättigheter för att kunna handlägga och/eller kontakta DSO inom föreskriven tidsfrist.

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

Det är viktigt att medarbetarna (t ex via informationssidan på intranätet) påminns om att registrerade kan inkomma med dessa förfrågningar och att de då ska kontakta DSO om de själva inte är säkra på handläggningen av dessa ärenden.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Oftast genom att någon i verksamheten upptäcker en händelse och kontaktar DSO. I vissa fall när DSO granskar IA eller får information från Lex Sarah-handläggare.
Hur många personuppgiftsincidenter har dokumenterats?	26
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	16 har rapporterats till IMYoch10 har inte rapporterats. Registrerade har blivit informerade om 6 av de incidenter som rapporterats till IMY och inga av de som inte rapporterats.
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	8

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.”

Det är en grundförutsättning för hanteringen av personuppgifter att incidenter 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. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive rapportering. Stadens mall för DSO:s årsrapport är avsedd att fokusera på rapporteringen.

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 IMY, 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 IMY samt rapportering till de berörda personerna.
Bristande förmåga att rapportera personuppgiftsincidenter i tid kan leda till sanktioner från IMY:s sida. Notera att enligt dataskyddsförordningen artikel 33.5 ska alla personuppgiftsincidenter dokumenteras, det vill säga även i de fall då incidenten inte ska rapporteras till IMY. Bristande dokumentering står i strid med Dataskyddsförordningen och leder även 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

Hur väl förmår verksamheten att rapportera personuppgiftsincidenter i tid till Integritetsskyddsmyndigheten?
Att antalet inrapporterade incidenter ökat under 2021 beror med stor sannolikhet på att förståelsen för vad en personuppgiftsincident är och hur den ska hanteras har ökat. Det förekommer dock fortfarande att DSO kontaktas för sent eller inte alls utan i efterhand upptäcker personuppgiftsincidenter i IA- och Lex Sarah-rapporter.

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

3.6.5 DSO ger råd och rekommendationer till PUA

Chefer på respektive enhet bör säkerställa att rutinen för hantering av personuppgiftsincidenter är känd. I dataskyddsredogörarnas uppdrag ingår också att påminna om gällande rutin.

4 Genomförda granskningar under året

4.1 Sammanfattning

Genomförda granskningar:

- Tredjelandsöverföringar
- Personuppgiftsförteckningar
- Behörighetsstyrning

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

Tredjelandsöverföringar

Efter utbildnings- och informationsinsatser bedöms medvetenheten om att tredjelandsöverföringar behöver ses över som relativt god. Enheterna behöver dock fortsatt påminnas så att frågan hålls levande och tas i beaktande inför varje ny upphandling/behandling av personuppgifter.

	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

Personuppgiftsförteckningar

De flesta enheter har tidigare lämnat in redogörelser över personuppgiftsbehandlingar i Excelfiler. Merparten av dessa är dock ofullständiga och innehåller felaktigheter. Under 2021 har dataskyddsredogörarna inlett arbete med att förteckna gamla och nya behandlingar i systemet Draftit. Detta upplevs dock som krångligt och svårt att komma igång med och arbetssättet behöver utvärderas.

	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

Behörighetsstyrning

Av de enheter som i skrivande stund svarat genomför några regelbundna kontroller av behörigheter i de system de använder.

Svaren från enheterna tyder dock på att det hos vissa saknas rutiner för att regelbundet granska behörigheter, och att detta istället görs på individnivå när en medarbetare slutar/börjar och en behörighet ska tas bort/läggas till. Kontrollen har också visat att kunskapen hos de som bör känna till rutiner kring behörigheter behöver säkerställas samt att enheterna behöver se över behovet av lokala och uppdaterade rutiner.

En risk som särskilt behöver tas i beaktande är hanteringen av skyddade personuppgifter då en säker behandling av dessa bygger på att så få personer som möjligt på myndigheten har tillgång till dessa och att åtkomst loggas. Enligt svaren finns skyddsåtgärd i paraplysystemet, men skyddade personuppgifter kan förekomma även i andra system.

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

4.4 DSO ger råd och rekommendationer till PUA

Enheterna behöver inventera vilka skriftliga rutiner som finns för behörighetsstyrning av de system/ytor de använder och vid behov upprätta lokala rutiner. Dessa rutiner bör inkludera regelbunden kontroll av behörigheter för att hindra att gamla behörigheter felaktigt ligger kvar. Det behöver också finnas rutiner för behörighetsstyrning när skyddade personuppgifter förekommer eftersom utgångspunkten är att så få medarbetare och chefer som möjligt ska ha tillgång till dessa uppgifter och att åtkomst ska loggas.

5 Risker inom dataskydd

5.1 Sammanfattning

Relevanta risker inom verksamheten:

- *Personuppgiftsförteckningen är inte uppdaterad*
- *Konsekvensbedömningar genomförs inte*
- *Personuppgifter överförs till tredje land utan lagligt stöd och fullgott skydd*

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: Personuppgiftsförteckningen är inte uppdaterad

Under 2021 har ambitionen varit att genom inrättande av dataskyddsredogörare intensifiera arbetet med förteckning. Detta arbete kom dock igång relativt sent och ännu inte gett önskvärda resultat. Samtidigt är personuppgiftsförteckningen en förutsättning för allt dataskyddsarbete på förvaltningen. En ofullständig personuppgiftsförteckning står därmed kvar som en risk.

	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: Konsekvensbedömningar genomförs inte

För att kunna vidta tillräckliga skyddsåtgärder krävs dels en fullständig och uppdaterad överblick över personuppgiftsbehandlingar via personuppgiftsförteckningen, dels att konsekvensbedömningar genomförs på vissa särskilt riskfyllda behandlingar. Antalet genomförda konsekvensbedömningar är dock, att döma av vad som finns i diariet och de kontakter som tagits med DSO (vilket är obligatoriskt vid en konsekvensbedömning), få.

	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: Personuppgifter förs över till tredje land utan lagligt stöd och fullgott skydd

Under 2021 har kunskapen om vad som behöver göras avseende överföringar av personuppgifter till land utanför EU/EES ökat. Eftersom domen som ligger till grund för situationen fortfarande är ny och överföringar sker via många olika typer av tjänster som dessutom är dominerande på marknaden (till exempel amerikanska molntjänster) bedöms dock risken fortsatt vara relativt hög.

	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

5.4 DSO ger råd och rekommendationer till PUA

Under 2021 har enheterna arbetat med dataskydd, bland annat utifrån 2020 års granskningsrapport och ökat sina kunskaper. Ännu återstår dock arbete, framförallt med förvaltningens personuppgiftsförteckning och arbete med konsekvensbedömningar. Båda dessa områden är centrala delar av dataskyddsarbetet och förutsättningar för att kunna skydda personuppgifter på rätt sätt.

Under 2022 behöver arbetssättet med dataskyddsredogörare (vars huvudsakliga uppgift är att uppdatera avdelningarnas personuppgiftsförteckningar) fortsätta och därefter utvärderas. Det är viktigt att dataskyddsredogörarna får chefsstöd så att de kan avsätta de 10% som förvaltningsledningen tidigare har beslutat om.

DSO har i checklistan för direktupphandlingar beskrivit behovet av att bedöma nödvändighet av konsekvensbedömning inför upphandling och förhoppningen är att rutinen därigenom blir mer känd på förvaltningen. Det är dock inte bara vid upphandlingar som konsekvensbedömningar kan behöva genomföras, och enheterna behöver därför regelbundet påminnas. Detta kan ske genom deltagande på de utbildningar som förvaltningens DSO regelbundet håller och genom att stadens sida om GDPR lyfts fram i olika sammanhang, till exempel på APT.

Då den dom som ligger till grund för det delvis nya förhållningssättet till tredjelandsöverföringar är relativt ny och många tjänster på marknaden idag innebär överföring behöver enheterna även fortsatt jobba med frågan och säkerställa att inga överföringar sker utan lagligt stöd. Även här personuppgiftsförteckningen en förutsättning då det bara är när den personuppgiftsansvariga vet vilka behandlingar den utför som kan bedöma om tredjelandsöverföring förekommer.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Personuppgiftsförteckningen*
- *Konsekvensbedömningar*
- *Information till registrerade*

6.2 Syfte

Det granskande arbetet är en av dataskyddsombudets viktigaste uppgifter. Granskningsområdena väljs utifrån ett riskbaserat synsätt, det vill säga att fokus ska ligga på områden där verksamhetens mest relevanta risker har identifierats i riskanalysen och i de övriga rapporteringspunkter i årsrapporten som visar på brister. Därigenom åstadkoms en röd tråd i dataskyddsarbetet från ett verksamhetsår till nästa samtidigt som de största riskerna elimineras eller åtminstone sänks till en tillräcklig nivå.

6.3 Planerade granskningar

Granskning 1: Personuppgiftsförteckningen

Förvaltningens personuppgiftsförteckning var ett granskningsområde 2021 också, men då den är central dataskyddsarbetet och fortfarande har brister behöver den följas upp ytterligare. Dessutom behöver arbetssättet med dataskyddsredogörare utvärderas.
Granskningen sker genom att DSO kontrollerar vad som lagts in i Draftit.

Granskning 2: Konsekvensbedömningar

Såsom framgår i denna rapport behöver arbetet med konsekvensbedömningar intensifieras och kunskapen behöver öka. Att så har skett behöver granskas i slutet av 2022. Då det är obligatoriskt att bjuda in DSO till konsekvensbedömningar är det lätt för DSO att ha kontroll över när de genomförs, men kontroll av kunskapsläge kan även ske genom intervjuer med utvalda personer på enheterna.

Granskning 3: Information till registrerade

Att som personuppgiftsansvarig vara transparent gentemot de registrerade är en viktig del i efterlevnaden av GDPR. De registrerade ska via lättillgänglig och begriplig information på förvaltningens blanketter och kommunikationskanaler kunna förstå hur och varför deras personuppgifter behandlas. De ska också kunna vända sig till förvaltningen och begära information om och var deras personuppgifter behandlas.

Vid en granskning kontrollerar DSO bland annat blanketter, webbsidor och annan information. Många av dessa är centralt framtagna, men det är varje personuppgiftsansvarig som ansvarar för att uppfylla GDPR:s krav på information till registrerade.