Stockholms stad

Årsrapport över arbetsmarknadsförvaltningens arbete med skydd av personuppgifter 2020

Mars 2021

stockholm.se

Årsrapport över arbetsmarknadsförvaltningens arbete med skydd av personuppgifter 2020
Mars 2021

Dnr: AMF 2021/17
Utgivningsdatum: 2021-03-11
Kontaktperson: Amanda Broman

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 ett medel för arbetsmarknadsnämnden att få information om eller 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. Detta i syfte att arbetsmarknadsnämnden ska kunna fatta beslut om prioriteringar, resurser och initiativ framåt. Samspelet resulterar i att det blir enklare för ansvarig nämnd 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.

Innehåll

2 Sammanfattning

I egenskap av arbetsmarknadsnämnden Dataskyddsombud lämnas följande årsrapport, där vart och ett av de obligatoriska rapporteringsområdena finns upptagna.

Sammanfattningsvis är bedömningen att arbetsmarknadsförvaltningen i och med granskningar och väsentlighets- och riskanalys uppmärksammat ett antal utvecklingsområden för 2021 och att aktiviteter planerats i syfte att hantera de risker som framkommit. Här är några exempel på behov som finns, samt aktiviteter som planerats för dessa:

- Behov av fortsatt genomgång och uppdatering av förteckning av behandlingar. Arbetet med förteckningen inleddes 2020 och fortsätter under 2021.
- Behov av översyn och uppdatering av befintliga infoklassningar, samt behov av uppdaterade rutiner för processen. Arbete med båda dessa aktiviteter är planerade att genomföras under 2021.
- Behov av uppdatering av rutin för konsekvensbedömning av behandling av personuppgifter. Arbetet med att uppdatera rutinen är planerat att genomföras under 2021 och kommer att genomföras som en del av översyn av rutinen för infoklassningar.
- Behov av översyn av konsekvensbedömningar för behandlingar. Arbetet sker i samband med översyn av registerförteckningen.

Det finns även behov av att säkerställa medarbetares kunskap gällande hantering av personuppgifter, och som ett steg för att kunna följa upp medarbetarnas kunskap kommer arbetsmarknadsförvaltningens verksamheter att 2021 redovisa hur stor andel av medarbetarna som deltagit i stadens obligatoriska utbildning i dataskydd.

Det finns också ett behov av att på en övergripande nivå undersöka vilket stöd verksamheten behöver för att kunna ta fram rutiner och arbeta för en säker hantering av personuppgifter på lokal nivå. I syfte att kunna planera för framtida stödinsatser kommer arbetsmarknadsförvaltningens verksamheter att genomföra en inventering av sin egen hantering, som därefter kommer att sammanställas i en förvaltningsövergripande rapport. Rapporten kommer att färdigställas under hösten 2021 och finnas som underlag inför verksamhetsplaneringen för 2022.

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 arbetsmarknadsnämndens status och DSO:s information, 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?	15
Har nödvändiga uppdateringar gjorts?	Arbete pågår med att förändra och uppdatera hela registerförteckningen. Arbetet är prioriterat och beräknas bli klart under 2021.
Bedöms registerförteckningen vara fullständig?	Nej. Med anledning av att det genomgripande arbete med registerförteckningen som pågår saknas behandlingar. Detta kommer dock att prioriteras och åtgärdas under 2021.
Har verksamheten lämpliga rutiner för registerföring?	Ja, men de rutiner som finns behöver uppdateras utifrån nytt arbetssätt i samband med att registerförteckningen har omarbetats.

3.1.2 Syfte

För att något ska gå att skydda måste det först vara synligt för verksamheten. Det följer därför i klartext 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. Det är därför viktigt att arbetsmarknadsnämnden (som PUA) får information om hur komplett verksamhetens förteckning är. 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.

Att ha en registerförteckning på plats leder till att verksamheten kan arbeta mer resurs- och kostnadseffektivt med sitt systematiska och riskbaserade dataskyddsarbete. Man kan styra insatserna där de gör störst nytta.

Syftet med detta rapporteringsområde är att rapportera till arbetsmarknadsnämnden (som PUA) gällande hur väl förvaltningen har lyckats inventera sina personuppgifter och de personuppgifter som behandlas för annans räkning och 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 arbetsmarknadsnämnden (som PUA) får information om inför som grund för planering inför nästkommande år.

3.1.3 Resultat

DSO kontrollerar hur många behandlingar som registrerats
I dagsläget finns 15 personuppgiftsbehandlingar införda i förteckningen. Det låga antalet anmälda behandlingar härrör till att förvaltningen påbörjat ett genomgripande förändringsarbete av hela förteckningen. Syftet med förändringsarbetet är att skapa en bättre struktur och få en ökad korrekthet i de behandlingar som är anmälda och återfinns i förteckningen. Tidigare har otydligheteter i ansvarsfördelning, vilka behandlingar som ska anmälas samt hur anmälan ska ske skapat en förteckning som inte har varit korrekt.

Förändringsarbetet av förteckning och anmälda behandlingar påbörjades hösten 2020 och kommer att prioriteras och slutföras under 20201. I samband med årsrapporten från DSO för 2021 borde således antalet behandlingar ha ökat och förteckningen vara, så långt det är möjligt, komplett.

DSO kontrollerar om nödvändiga uppdateringar gjorts
I samband med förändringsarbetet gällande förteckningen så gås samtliga behandlingar igenom för att kontrolleras gällande om det finns behov av uppdateringar eller kompletteringar.

DSO bedömer hur fullständig registerförteckningen är
Då förteckningen genomgår ett grundläggande förändringsarbete är bedömningen att den i nuläget är långt ifrån komplett, men ett aktivt arbete pågår för att förbättra struktur och information i förteckningen.

Bakgrunden till förändringsarbetet med registerförteckningen, och rutinerna för anmälan till förteckningen, är otydligheteter i ansvarsfördelning, vilka behandlingar som ska anmälas samt hur anmälan ska ske. Detta har lett till att det har skapats en förteckning som inte har varit korrekt.

Som komplement eller nära sammanlänkad till registerförteckningen finns förvaltningens hanteringsanvisningar. I detta dokument anges vilken information som hanteras inom förvaltningen, och hur den informationen hanteras. En av informationspunkterna som framgår av hanteringsanvisningarna är om informationen innehåller personuppgifter.

Detta sammantaget gör att, trots att det finns behov av att omarbeta och komplettera registerförteckningen, det finns en bra överblick och kunskap kring var personuppgifter hanteras inom förvaltningen/nämnden.

DSO bedömer om verksamheten har lämpliga rutiner för registerföring
Bedömningen är att rutinerna för att hantera anmälan av behandling av personuppgifter och uppdatering av behandlingar behöver förtydligas och förenklas. Detta i syfte att göra det enklare för verksamheterna och förvaltningen att anmäla, uppdatera och få insyn i vilka behandlingar som finns samt hur behandlingar ska hanteras.

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

Med anledning av den pågående förändringsarbete gällande registerförteckningen, och med anledning av otydliga rutiner för hur

anmälan och uppdatering av behandlingar ska gå till, så skattas allvarligheten enligt ovan. Utifrån skattningen är förteckningen en prioriterad fråga att hantera under 2021.

3.1.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet har lämnat rekommendationer till arbetsmarknadsförvaltningen gällande att prioritera omarbetningen och uppdatering av förteckningen 2021, och detta har tagits i beaktande och återfinns som en aktivitet för administrativa staben att genomföra under 2021. Arbetet har redan inletts.

Dataskyddsombudet har också lämnat rekommendationen att förvaltningen ska se över och uppdatera de rutiner som finns för att anmäla och uppdatera behandlingar i förteckningen, i syfte att göra det tydligt och enkelt att genomföra. Även detta har tagits i beaktande och återfinns som en aktivitet för administrativa staben att genomföra under 2021.

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, men uppdateringar och kompletteringar med ytterligare stöddokument (rutiner och mallar) kommer att genomföras under 2021.
Är dokumenten pedagogiska och ger de ett tillräckligt stöd?	Osäkert, men det kommer att genomföras en översyn av dokumenten under 2021.
Är dokumenten uppdaterade?	Ja, men det kommer att genomföras en översyn av dokumenten under 2021.
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 dokumenterade. Detta följer bland annat av kravet på att den personuppgiftsansvarige måste kunna *visa* att dataskyddsförordningens principer för behandling av personuppgifter efterlevs (artikel 5).

Rapporteringen av området är tvådelad: dels ska DSO bedöma om verksamheten har de styrdokument antagna och på plats, dels ska

rapporteringen visa om dokumentationen innehållsmässigt håller en lämplig kvalitet, i vilket ingår bl.a. att dokumentationen ska vara uppdaterad och aktuell.

Bristande styrning på grund av att lämplig styrande dokumentation saknas leder exempelvis ofta till *bristande kvalitet* i hur verksamheten utför aktiviteterna, men även till att verksamheten *slösar värdefulla resurser* när exempelvis för många personer blir involverade i en incidenthantering eller för att en analys behöver göras om från grunden varje gång istället för att man återanvänder redan uppfunnen kunskap.

3.2.3 Resultat

Finns lämplig styrande dokumentation på plats?
Ja, de styrande dokument som krävs, och behövs, finns på plats. Exempel på styrande dokument som finns är:

- Integritetspolicy för arbetsmarknadsnämnden
- Riktlinjer gällande hantering av personuppgifter
- Anvisningar för generell hantering av skyddade personuppgifter inom arbetsmarknadsnämndens verksamheter
- Ansvarsfördelning gällande hantering av personuppgifter
- Rutin för hantering av personuppgiftsincidenter inom arbetsmarknadsförvaltningen
- Rutin för hantering av begäran av registerutdrag
- Rutin för hantering av rättelse och radering, begränsning samt invändning gällande behandling av personuppgifter
- Rutin för konsekvensbedömning gällande behandling av personuppgifter

DSO bedömer om innehållet i existerande dokument håller lämplig kvalitet
Flera av styrdokumenten och rutinerna är i behov av uppdateringar, bland annat med anledning av att arbetssätten gällande hantering av personuppgifter har förändrats och förbättras under den senaste tiden.

När det gäller hanteringen av den övergripande frågan om informationssäkerhet, där hanteringen av personuppgifter är en del, behöver styrdokumenten och rutinerna en särskild översyn i syfte att hitta samordningsfördelar och effektiviseringsvinster i såväl förståelighet och arbetssätt. Allt i syfte att göra frågorna så lätta att hantera som möjligt. Ett av de aktuella områdena att se över är hanteringen av konsekvensbedömning.

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

Dataskyddsombudet har rekommenderat arbetsmarknadsförvaltningen att genomföra en inventering och uppdatering av styr- och stöddokument gällande hantering av personuppgifter. Detta har tagits i beaktande och finns som en aktivitet för administrativa staben att genomföra under 2021.

Dataskyddsombudet har även rekommenderat arbetsmarknadsförvaltningen att genomföra en översyn av gemensamma processer inom informationssäkerhetsområdet, där hanteringen av personuppgifter är en del. Administrativa staben och it- och kommunikationsstaben kommer under 2021 att genomföra ett gemensamt arbete med att se över dessa processer, till exempel vad gäller informationsklassning och 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?	Oklart
Är klassade personuppgiftsbehandlingar aktuella?	Till viss del

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 arbetsmarknadsnämnden (som PUA) genom årsrapporten 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.

Enbart sådan informationsklassning som avser behandling eller system som omfattar *personuppgifter* är av intresse för denna årsrapport.

3.3.3 Resultat

DSO bedömer att det finns en osäkerhet kring vilka behandlingar som är del av förvaltningens befintliga informationsklassningar, samt kring vilka behandlingar som har behov av informationsklassning. Det är också svårt att bedöma om de

klassningar som finns är i behov av uppdatering. Med anledning av detta kommer en inventering av informationsklassningar att genomföras under 2021.

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

Med anledning av osäkerheten gällande om samtliga behandlingar som behöver informationsklassats har det samt om eventuella uppdateringar i informationsklassningar behöver göras, så görs bedömningen enligt ovan.

3.3.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet har rekommenderat arbetsmarknadsförvaltningen att genomföra en inventering av befintliga informationsklassningar, samt utifrån den genomföra en behovsanalys gällande kompletteringar och uppdateringar. Detta har tagits i beaktande och en aktivitet finns för administrativa staben och it- och kommunikationsstaben att genomföra 2021.

Utifrån ovanstående osäkerheter har förvaltningen även planerat att 2021 se över arbetssättet för hantering av informationsklassningar och uppdatera eventuella rutiner för hanteringen. Ansvaret för denna aktivitet ligger på administrativa staben och it- och kommunikationsstaben.

3.4 Konsekvensbedömningar

3.4.1 Sammanfattning

Fråga/kontroll	Svar
Har man identifierat alla behandlingar som det borde göras konsekvensbedömningar av?	Osäkert
Har alla potentiella högriskbehandlingar konsekvensbedömts?	Osäkert
Är de genomförda bedömningarna aktuella?	Ja

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). IMY har på sin webbplats en förteckning över när personuppgiftsbehandlingar kräver en konsekvensbedömning.

Arbetsmarknadsnämnden (som PUA) får genom årsrapporten en uppdaterad bild av hur fullständig verksamhetens situation är i fråga om konsekvensbedömningar avseende dataskydd.

3.4.3 Resultat

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

Det är osäkert om konsekvensbedömningar genomförts för alla behandlingar som behöver det. Detta innebär att en översyn av behov av konsekvensbedömningar behöver göras i samband med uppdateringen av registerförteckningen.

I samband med att information framkommit vad gäller nya behandlingar, eller förändringar av annan art som påverkar behandling av personuppgifter, så har frågan gällande konsvensbedömning lyfts, och vid behov även genomförts.

Har konsekvensbedömning gjorts för alla potentiella högriskbehandlingar av personuppgifter?
Även gällande högriskbehandlingar finns en osäkerhet kring om nödvändiga konsekvensbedömningar genomförts, och därför behövs en översyn av behovet även för dessa behandlingar.

I samband med att information framkommit gällande ny eller befintlig hantering av högriskbehandlingar så har konsekvensbedömning genomförts.

Är de genomförda konsekvensbedömningarna aktuella?
De konsekvensbedömningar som tagits fram bedöms som aktuella, viss osäkerhet finns dock gällande hantering av rutin för uppdatering av 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
	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

Osäkerheten gällande om konsekvensbedömning finns där det krävs handlar till stor del om att verksamheten ibland saknar kunskap om hanteringen av processen och därigenom bristande följsamhet om gällande rutiner. Dataskyddsombudet bedömning är att det finns en bra rutin för hantering av nya konsekvensbedömningar. Bedömningen är dock att verksamheten kan behöva få ytterligare information och stödmaterial gällande ansvar och hantering, att rutinen kan förenklas och förtydligas samt att en inventering av konsekvensbedömningar kan behöva göras.

3.4.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet har rekommenderat arbetsmarknadsförvaltningen att göra en inventering och uppdatering av samtliga styrdokument och rutiner. Förvaltningen har planera för att genomföra denna uppdatering under 2021, och i det arbetet ingår även en översyn av hantering av konsekvensbedömning. Administrativa staben ansvarar för att aktiviteten genomförs 2021.

Konsekvensbedömningen ingår även som en del av den planerade översynen av de processer som finns inom det övergripande informationssäkerhetsområdet (tillsammans med till exempel informationsklassningar). För den sistnämnda aktiviteten ansvarar administrativa staben och it- och kommunikationsstaben.

I samband med översynen av registerförteckningen kommer behovet av att genomföra konsekvensbedömningar för behandlingar att ses över. Administrativa staben ansvarar för översynen av registerförteckningen.

3.5 Individens rättigheter

3.5.1 Sammanfattning

Fråga/kontroll	Svar
Hur många begäran (om registerutdrag, begränsning, radering etc.) har inkommit från registrerade personer?	2
Hur många av dessa begäran har hanterats av verksamheten inom 30 dagar?	Samtliga har behandlats inom 30 dagar.

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 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?
Dataskyddsombudets bedömning är att verksamheten har förutsättningarna att hanterade registrerades rättigheter.

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

Dataskyddsombudet bedömer att tillräckliga rutiner och stöddokument finns för att kunna hantera registrerades rättigheter utifrån vad som anges ovan.

3.5.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet har utifrån nuvarande situation inga särskilda råd och rekommendationer gällande detta område. Arbetsmarknadsförvaltningen kommer i sin översyn av samtliga styrdokument och rutiner även att genomföra en översyn gällande rutiner för hantering av registrerades rättigheter.

3.6 Personuppgiftsincidenter

3.6.1 Sammanfattning

Fråga/kontroll	Svar
Hur upptäcks personuppgiftsincidenter?	Verksamheten som drabbas av incident genomför en incidentrapportering i systemet IA samt kontaktar Dataskyddsombudet.
Hur många personuppgiftsincidenter har dokumenterats?	6
Hur många av dessa har ansetts behöva rapporteras (till IMY resp. till berörda personer) och inte?	1 (av 6) har rapporterats till IMY 1 (av 6) har rapporteras till berörd person
Hur många av incidenterna har rapporterats i tid till tillsynsmyndigheten?	Den som anmälts till IMY har anmälts i tid.

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. Denna rapport hanterar endast personuppgiftsincidenter. Det är 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. Incidenthanteringen består av två huvudsakliga moment – dokumentering respektive

rapportering. I den här rapporten ligger fokus på hantering av 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 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. Årsrapporten är därför avsedd att kartlägga detta, samtidigt som det finns möjlighet att redovisa vilka typer av personuppgiftsincidenter som inträffat, incidenternas allvarsgrad etc.

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?
Dataskyddsombudets bedömning är att rapportering till Integritetsskyddsmyndigheten sker i tid i de fall där rapportering är aktuell.

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

Dataskyddsombudets bedömning är att den rapportering som har skett gällande personuppgiftsincidenter har skett på ett korrekt sätt. Bedömningen är dock att verksamheterna behöver ytterligare information gällande hur en incident ska hanteras.

3.6.5 DSO ger råd och rekommendationer till PUA

Dataskyddsombudet har rekommenderat arbetsmarknadsförvaltningen att säkerställa att medarbetarnas kunskaper gällande hantering av incidenter är tillräckligt. Denna rekommendation har tagits i beaktande och ingår som en del i det arbete som förvaltningen planterat att genomföra under 2021. Bland annat kommer uppföljning att ske gällande medarbetares genomförande av utbildning i dataskydd, samt en inventering av verksamhetens hantering av personuppgifter (där rutiner för incidentrapportering är en del).

4 Genomförda granskningar

4.1 Sammanfattning

Genomförda granskningar:

- *Internkontrollsbesök vid fem verksamheter inom förvaltningen*

Arbetsmarknadsförvaltningen genomför årligen internkontrollsbesök hos ett visst antal verksamheter. Under besöket kontrolleras flera olika frågor, varav hantering av personuppgifter i en. En sammanfattning gällande bedömning utifrån besöken 2020 återfinns nedan.

- *Genomgång och omarbetning av personuppgiftsförteckning (påbörjad)*

2020 påbörjade arbetsmarknadsförvaltningen en genomgång och omarbetning av förteckningen över behandlingar av personuppgifter. Genomgång och omarbetning påbörjades med syftet att säkerställa att rätt och tillräcklig information finns om respektive behandling, samt att säkerställa att alla behandlingar finns upptagna i förteckningen. Arbetet med förteckningen kommer att fortsätta under 2021.

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

Internkontrollsbesök vid fem verksamheter inom förvaltningen

Den sammanfattande bedömningen är att verksamhetens kunskap att personuppgifter behöver hanteras på ett särskilt sätt är från medel till hög. Medvetenheten om GDPR och hantering av personuppgifter upplevs ha ökat sedan förändringen av lagstiftningen och förvaltningens ökade arbete med frågan.

Det finns dock en del oklarheter och brister vad gäller hur personuppgifter ska hanteras, t.ex. i verksamhetssystem och

e-post.

För att höja kunskapsläget vad gäller behandling av personuppgifter uppmanas verksamheterna att genomgå stadens centrala e-utbildningar ” Grundkurs i dataskydd” och ”Informationssäkerhet i staden”.

Anmälan av nya behandlingar av personuppgifter i förvaltningens förteckning (DraftIT) är bristfällig eller obefintlig. Detta beror dels på svårighet hos verksamheterna att avgöra när en behandling ska anmälas, dels på att det pågår ett centralt arbete hos förvaltningen med utformningen av förteckningen. Detta har orsakat en otydlighet för verksamheterna om hur anmälan av personuppgiftsbehandlingar ska göras.

Kunskap finns hos de kontrollerade verksamheterna hur de ska agera vid en personuppgiftsincident.

Rutiner för egenkontroll inom området saknas eller är bristfälliga.

	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

Genomgång och omarbetning av personuppgiftsförteckning
2020 påbörjade arbetsmarknadsförvaltningen en genomgång och omarbetning av förteckningen över behandlingar av personuppgifter.

Vid genomgången upptäcktes bland annat att vissa anmälningar var att behandlingar fanns som dubbletter både på lokal och central nivå (t ex behandlingar i HR-system och andra centrala processer som gäller hela verksamheten), behandlingar saknade i förteckningen nödvändig information och behandlingar som inte fanns inte anmälda.

För att säkerställa såväl kvalitet som korrekthet i förteckningen så påbörjades en genomgång och omarbetning med syftet att säkerställa att rätt och tillräcklig information finns om respektive

behandling, samt att säkerställa att alla behandlingar finns upptagna i förteckningen. Arbetet med förteckningen kommer att fortsätta under 2021.

Bedömningen nedan är densamma som bedömningen under rubriken ”Registerförteckning”, och där finns även information om förslag till åtgärder samt vidtagna åtgärder för 2021.

	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

4.3 DSO ger råd och rekommendationer till PUA

Verksamhetens behandling av personuppgifter (utifrån internkontrollsbesök)
Utifrån internkontrollsbesöken har dataskyddsombudet gjort bedömningen att verksamheterna behöver ökat och mer pedagogiskt stöd vad gäller deras egen hantering av personuppgifter. Det gäller bland annat säkerställande av medarbetarnas kunskap om lagstiftning och rutiner, säkerställande av egna rutiner samt anmälan till registerförteckningen.

Utifrån den samlade bilden gällande verksamhetens behov av stöd och rutiner för hantering av personuppgifter föreslogs i rapporten ett antal förbättringsområden och åtgärder. Detta har arbetsmarknadsförvaltningen tagit i beaktande och därefter vidtagit ett flertal åtgärder 2021, vilka några anges nedan.

- Enheterna ska följa upp och redovisa hur stor andel av medarbetarna som genomfört obligatorisk utbildning i dataskydd.
- Enheterna ska följa upp och redovisa hur stor andel av medarbetarna som genomfört obligatorisk utbildning i informationssäkerhet.
- Enheterna ska genomföra en inventering av verksamhetens hantering av personuppgifter, vad gäller t ex egna rutiner och anmälan av behandlingar. Förvaltningen kommer utifrån

inlämnade inventeringar att göra en sammanställning över hur personuppgifter hanteras i verksamheten
- Enheterna ska i sin lokala intern kontrollplan redogöra för hur vissa utvalda risker gällande hantering av personuppgifter kontrolleras och hanteras.
- Administrativa staben ska genomföra en översyn av styr- och stöddokument inom området
- Administrativa staben ska uppdatera registerförteckningen och ta fram en ny rutin för anmälan till registerförteckningen
- Administrativa staben och it- och kommunikationsstaben ska göra en översyn av och uppdatera rutiner för hantering av informationsklassning och konsekvensbedömning.

5 Risker inom dataskydd

Risker inom dataskydd framgår av och hanteras i förvaltningens *Väsentlighets- och riskanalys samt internkontrollplan 2021*, vilken återfinns som bilaga till arbetsmarknadsnämndens verksamhetsplan 2021.

6 Planerade granskningar under det nya verksamhetsåret

6.1 Sammanfattning

Relevanta granskningsområden inom verksamheten:

- *Genomgång och omarbetning av registerförteckning*
- *Översyn och uppdatering av infoklassningar*
- *Inventering och översyn av att konton i sociala medier följer gällande styrdokument*
- *Verksamheternas inventering av hantering av personuppgifter, samt sammanställning av resultatet*
- *Interkontrollsbesök*

6.2 Syfte

Det granskande arbetet en del av dataskyddsombudets uppgifter. Granskningsområdena bör lämpligen väljas utifrån ett riskbaserat synsätt, det vill säga att fokus bör 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 mer acceptabel nivå.

Arbetsmarknadsförvaltningens planering av granskningar utgår från föregående års granskningar och de risker som framkommer av väsentlighets- och riskanalysen (som återfinns som bilaga till verksamhetsplanen).

6.3 Planerade granskningar

Genomgång och omarbetning av registerförteckning

Arbetet med att se över och göra om arbetsmarknadsnämndens registerförteckning påbörjades 2020 och fortsätter under 2021. I arbetet ingår dels att kontrollera, dels att komplettera information i anmälda behandlingar, samt att tillföra de behandlingar som saknas i förteckningen.

Granskningen och omarbetningen genomföras av administrativa staben. I samband med omarbetningen kommer även nya rutiner för anmälan till förteckningen att tas fram, och i samband med att rutinerna är färdigställda sker en särskild informationsinsats, gällande anmälan till förteckningen, riktad mot förvaltningens verksamheter.

Översyn och uppdatering av infoklassificeringar

Arbetsmarknadsförvaltningen kommer under 2021 att genomföra en översyn och eventuella uppdateringar av befintliga informationsklassningar, samt planera för genomförande av saknade informationsklassningar. I samband med detta kommer även befintlig rutin för genomförande och hantering av infoklassningar uppdateras.

Administrativa staben och it- och kommunikationsstaben är ansvariga för att genomföra arbetet gällande informationsklassningar.

Inventering av konton i sociala medier

Med anledning av att arbetsmarknadsförvaltningen tar fram nya tillämpningsanvisningar och rutiner för konton i sociala medier, kommer en inventering och genomgång att genomföras av förvaltningens konton i sociala medier. Det ger en möjlighet att upptäcka och åtgärda eventuella risker och brister i hanteringen av förvaltningens konton i sociala medier.

Administrativa staben och it- och kommunikationsstaben ansvarar för att genomföra inventeringen.

Verksamheternas inventering av hantering av personuppgifter, samt sammanställning av resultatet

2021 ska arbetsmarknadsförvaltningens verksamheter genomföra en inventering av sin egen verksamhets hantering av personuppgifter. Inventeringen genomförs via ett frågeformulär i systemet IA. Verksamheterna ska ha genomfört inventeringen/besvarat frågorna i formuläret senast i samband med tertialrapport 2.

Efter att verksamheterna genomfört inventeringen kommer en sammanställning över resultatet att tas fram. Administrativa staben ansvarar för att ta fram den förvaltningsövergripande rapporten.

Internkontrollsbesök

Arbetsmarknadsförvaltningen genomför årligen ett visst antal internkontrollsbesök där vissa övergripande frågor kontrolleras. Hanteringen av personuppgifter är ett av de områden som kontrolleras i samband med besöket, och besök genomförs hos fem verksamheter.

Efter besöken sammanställs en rapport som delges verksamheten, där resultatet av granskningen samt eventuella förslag till förbättringar tas upp. När samtliga besök genomförts sammanställs

en förvaltningsövergripande rapport som redovisar det övergripande resultatet inom respektive område. Om det finns ett behov förbättringar lyfter rapporten upp förslag till förbättringsåtgärder på dels förvaltningsnivå, dels avdelningsnivå.

Administrativa staben ansvarar för att vid dessa besök, och i sammanställning i rapporterna, kontrollera och föreslå förbättringar gällande hantering av personuppgifter.