

Uppföljning av dataskyddsarbetet i Enskede-Årsta-Vantör 2020

Årsrapport från
dataskyddsombudet

Dnr EÅV **2021/37**

Uppföljning av dataskyddsarbetet i Enskede-Årsta-Vantör 2020
Årsrapport från dataskyddsombudet

Dnr: 2021/37

Kontaktperson: Hiba Hilali

Sammanfattning

Enskede-Årsta-Vantör stadsdelsnämnd är personuppgiftsansvarig för de personuppgifter som nämnden behandlar. Stadsdelsnämnden ska ha ett dataskyddsombud vars främsta uppgift är att övervaka att nämnden följer tillämplig dataskyddslagstiftning samt att ge information och råd till nämnden.

Stadsdelsnämndens dataskyddsombud har sammanställt sina granskningar och iakttagelser avseende Enskede-Årsta-Vantör stadsdelsnämnds efterlevnad av dataskyddsförordningen och brottsdatalagen under 2020 i en rapport.

Rapporten visar följande:

- *Stadsdelsnämnden kan undvika att en del personuppgiftsincidenter inträffar i framtiden om nämnden implementerar Stockholms stads Riktlinjer för informationssäkerhet i organisationen. Nämnden har en bra rutin för hantering av personuppgiftsincidenter som uppdateras årsvis.*
- *Stadsdelsnämnden kan bli bättre på att genomföra de obligatoriska webbutbildningarna för GDPR och Informationssäkerhet.*
- *Stadsdelsnämnden har blivit bättre på att uppdatera befintliga och registrera nya personuppgiftsbehandlingar i förteckningen men kan bli ännu bättre. En ny rutin för Inventering av personuppgiftsbehandlingar har tagits fram och kommer att implementeras år 2021.*
- *Stadsdelsnämnden har en bra rutin för registrerades rättigheter. Under år 2020 har det inte inkommit några begäranden där de registrerade åberopar sina rättigheter.*
- *Stadsdelsnämnden har implementerat brottsdatalagen i berörda verksamheter och har tagit fram rutiner som kommer att implementeras år 2021.*
- *Stadsdelsnämnden har varit bra på att informera om EU-domen i Schrems II-målet samt kartlagt samtliga tredjelandsoverföringar på förvaltningen och vidtagit de åtgärder som krävts och varit möjliga.*

Innehåll

Sammanfattning	3
Inledning	6
Definitioner	7
Personuppgiftsincidenter.....	8
Registrerades rättigheter	10
Registerförteckning	11
Brottsdatalagen	13
EU-domen i Schrems II-målet	15

Inledning

Enskede-Årsta-Vantör stadsdelsnämnd är personuppgiftsansvarig för de personuppgifter som nämnden behandlar. Den personuppgiftsansvarige ansvarar för efterlevnaden av EU:s dataskyddsförordning och brottsdatalagen, och ska kunna visa att bestämmelserna i dessa regelverk efterlevs.

Den personuppgiftsansvarige ska utse ett dataskyddsombud.¹ Dataskyddsombudets roll är främst att övervaka att den personuppgiftsansvarige följer tillämplig dataskyddslagstiftning samt att ge information och råd till den personuppgiftsansvarige i frågor som rör skyddet av personuppgifter.² Dataskyddsombudet ska inte driva eller utföra det operativa dataskyddsarbetet. Dataskyddsombudet ska inte heller fatta beslut avseende dataskydd. Dataskyddsombudet har inget eget ansvar för att organisationen följer dataskyddsförordningen. Det ansvaret ligger alltid hos den personuppgiftsansvarige.

Dataskyddsombudet ska rapportera till den personuppgiftsansvarige på högsta förvaltningsnivå.³ Ett exempel på rapportering är att dataskyddsombudet upprättar en årsrapport som lämnas till den personuppgiftsansvarige.⁴ I den här rapporten redogör dataskyddsombudet för de granskningar och iakttagelser som gjorts avseende den personuppgiftsansvariges efterlevnad av dataskyddsförordningen och brottsdatalagen under 2020.

Stockholm 2021-01-18

Hiba Hilali
Dataskyddsombud

¹ Art. 37 dataskyddsförordningen och 13 § brottsdatalagen.

² Art. 39 dataskyddsförordningen och 14 § brottsdatalagen.

³ Art. 38 dataskyddsförordningen.

⁴ Riktlinjer om dataskyddsombud, Artikel 29-arbetsgruppen för skydd av personuppgifter, 2016-12-13, sida 18.

Definitioner

Behandling av personuppgifter: Varje åtgärd som vidtas beträffande personuppgifter, till exempel insamling, registrering, lagring, bearbetning, ändring, spridning eller radering.

Personuppgifter: Varje upplysning som direkt eller indirekt kan identifiera en fysisk person ("registrerad"), till exempel namn, personnummer, e-postadress, fastighetsbeteckning, fotografi eller ljudinspelning.

Personuppgiftsansvarig: Den som bestämmer ändamålen och medlen för behandlingen av personuppgifter. I en kommun är varje nämnd personuppgiftsansvarig för de personuppgifter som nämnden behandlar eller som behandlas under nämndens ledning.

Personuppgiftsincident: En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust, ändring, obehörigt röjande eller obehörig åtkomst till personuppgifter.

Personuppgiftsincidenter

Sammanfattning

Under 2020 har det rapporterats 24 personuppgiftsincidenter i stadsdelen. 8 av dessa har anmälts till tillsynsmyndigheten. Dataskyddsombudet bedömer att en del personuppgiftsincidenter kan undvikas om nämnden implementerar *Stockholms stads Riktlinjer för informationssäkerhet* i organisationen.

Om en personuppgiftsincident inträffar ska den personuppgiftsansvarige inom 72 timmar efter att ha fått vetskap om personuppgiftsincidenten, anmäla den till tillsynsmyndigheten. Anmälan behöver inte göras om det är osannolikt att personuppgiftsincidenten medför en risk för personers rättigheter och friheter. Alla personuppgiftsincidenter, oavsett om de anmäls till tillsynsmyndigheten eller inte, ska dokumenteras.⁵ Om en incident sannolikt leder till en hög risk för personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål även informera de drabbade om incidenten.⁶

Under 2020 har det rapporterats totalt 24 personuppgiftsincidenter i stadsdelen. 8 av dessa har anmälts till Integritetsskyddsmyndigheten.⁷

Stadsdelsnämnden har en väl förankrad rutin för att hantera personuppgiftsincidenter. Rutinen uppdateras årsvis. Dataskyddsombudet bedömer dock att en del personuppgiftsincidenter kan undvikas om organisationen implementerar Stockholms stads riktlinjer för informationssäkerhet. Den obligatoriska webbutbildningen i GDPR behöver utföras i mycket högre utsträckning. Dataskyddsombudet kommer att följa upp antal utförda webbutbildningar i GDPR på avdelningsnivå under år 2021.

⁵ Art. 33 dataskyddsförordningen och 3 kap. 9 § brottsdatalagen. Med risker menas t.ex. att personer förlorar kontrollen över sina personuppgifter, att rättigheter inskränks, att personer utsätts för diskriminering, identitetsstöld eller bedrägeri, finansiell förlust, skadlig ryktesspridning eller brott mot sekretess eller tystnadsplikt.

⁶ Art. 34 dataskyddsförordningen och 3 kap. 10 § brottsdatalagen.

⁷ Integritetsskyddsmyndigheten är tillsynsmyndighet. Integritetsskyddsmyndigheten hette tidigare Datainspektionen.

Lista över personuppgiftsincidenter som har anmälts till
Integritetsskyddsmyndigheten

Typ av incident	Berörd avdelning	Anmald till IMY* inom 72	Beslut från IMY*
Klient har fått fel beslut i samma kuvert som sitt egna beslut.	Social omsorg äldre	Nej.	IMY har beslutat att avsluta ärendet.
Beslut har skickats till fel brukare.	Social omsorg vuxen	Ja.	IMY har beslutat att avsluta ärendet.
Sekretessuppgifter har skickats okrypterat.	Social omsorg vuxen	Ja.	IMY har beslutat att avsluta ärendet.
Verksamheten har använt sig av en okrypterad e-postadress som funktionsbrevlåda för verksamheten.	Social omsorg vuxen	Ja.	IMY har beslutat att avsluta ärendet.
Obehörig åtkomst för användare i Skolplattformen.	Förskola	Ja	IMY har beslutat att avsluta ärendet.
Bortkommen post till CSN.	Social omsorg barn och unga	Ja.	IMY har beslutat att avsluta ärendet.
Anställd har med privat telefon fotat brukare och delat bilden vidare.	Social omsorg äldre	Nej.	IMY har beslutat att avsluta ärendet.
E-post utskick till vårdnadshavare utan att dölja mailadresser.	Förskola	Ja.	IMY har beslutat att avsluta ärendet.

* IMY = Integritetsskyddsmyndigheten. Datainspektionen bytte namn
2021-01-01

Registrerades rättigheter

Sammanfattning

Under 2020 har det kommit in 0 begäranden där registrerade åberopar sina rättigheter. Nämnden har en bra rutin för registrerades rättigheter.

Fysiska personer har ett antal rättigheter enligt dataskyddsförordningen och brottsdatalagen.⁸

En person kan begära följande enligt dataskyddsförordningen:

- Ett registerutdrag där det framgår vilka personuppgifter vi behandlar om personen och hur vi behandlar uppgifterna
- Rättelse av felaktiga personuppgifter
- Radering av personuppgifter
- Begränsning av en behandling av personuppgifter
- Hjälp med att flytta personuppgifter (dataportabilitet)
- Invända mot en behandling av personuppgifter

En person kan begära följande enligt brottsdatalagen:

- Ett registerutdrag där det framgår vilka personuppgifter vi behandlar om personen och hur vi behandlar uppgifterna
- Rättelse av felaktiga personuppgifter
- Radering av personuppgifter
- Begränsning av en behandling av personuppgifter

När en begäran kommer in ska den personuppgiftsansvarige bedöma om begäran ska bifallas eller avslås. En begäran enligt dataskyddsförordningen ska hanteras inom en månad och en begäran enligt brottsdatalagen ska hanteras utan onödigt dröjsmål.

Under 2020 har det inte kommit in några begäranden om registerutdrag eller begäranden om radering.

⁸ Art. 15-21 dataskyddsförordningen och 4 kap. 3, 9 och 10 §§ brottsdatalagen.

Registerförteckning

Sammanfattning

Dataskyddsombudet bedömer att stadsdelsnämnden har blivit bättre på att uppdatera befintliga och inventera sina personuppgiftsbehandlingar men kan bli ännu bättre. Under hösten 2020 har förvaltningen tagit fram en rutin för inventering av personuppgiftsbehandlingar i syfte att få bättre styrning på detta område. Rutinen kommer att beslutas och implementeras år 2021.

Den personuppgiftsansvarige ska föra ett register över de behandlingar av personuppgifter som utförs under dess ansvar, en så kallad "registerförteckning".⁹ Stadsdelsnämnden använder systemstödet Draftit för sin registerförteckning.

Varje avdelning inom organisationen ansvarar för att lägga in de personuppgiftsbehandlingar som sker på avdelningen i registerförteckningen och att hålla dessa uppdaterade. I december 2020 finns totalt 526 personuppgiftsbehandlingar i registerförteckningen för hela förvaltningen.

I april 2020 följde dataskyddsombudet upp via mail om alla avdelningar hade sett över och vid behov uppdaterat sina personuppgiftsbehandlingar i registerförteckningen under det senaste halvåret. Uppföljningen visade att *administrativa avdelningen, avdelningen för förskola* samt *avdelningen för lokaler och stadsmiljö* hade sett över och uppdaterat alla sina personuppgiftsbehandlingar. Övriga fyra avdelningar hade sett över vissa men inte alla personuppgiftsbehandlingar. Orsaken till detta uppgavs främst bero på tidsbrist hos chefer och avdelningarnas dataskyddssamordnare.

Avdelning	Kommentar
Staben	Har sett över nästan alla sina personuppgiftsbehandlingar. Några nya personuppgiftsbehandlingar behöver registreras i Draftit.
Administrativa avdelningen	Har sett över alla sina personuppgiftsbehandlingar.
Avdelningen för förskola	Har sett över alla sina personuppgiftsbehandlingar.

⁹ Art. 30 dataskyddsförordningen och 3 kap. 3 § brottsdataförordningen.

Avdelningen för lokaler och stadsmiljö	Har sett över alla sina personuppgiftsbehandlingar.
Avdelningen för social omsorg barn och unga	Har sett över vissa personuppgiftsbehandlingar.
Avdelningen för social omsorg vuxen	Beställarenheten har sett över alla sina personuppgiftsbehandlingar. Övriga enheter har sett över vissa av sina personuppgiftsbehandlingar.
Avdelningen för social omsorg äldre	Beställarenheten har inte uppgett om de har sett över sina personuppgiftsbehandlingar eller inte. Övriga enheter har sett över alla sina personuppgiftsbehandlingar.

Det är viktigt att stadsdelsnämnden har en systematik för att regelbundet inventera sina personuppgiftsbehandlingar, registrera personuppgiftsbehandlingarna i registerförteckningen och vid behov uppdatera registerförteckningen.

Under 2019 granskade stadsrevisionen stadsdelsnämndens följsamhet till dataskyddsförordningen. I stadsrevisionens årsrapport för 2019 rekommenderade stadsrevisionen stadsdelsnämnden bland annat att regelbundet och systematiskt inventera sina personuppgiftsbehandlingar.¹⁰ I dataskyddsombudets årsrapport för 2019 bedömde även dataskyddsombudet att stadsdelsnämnden behövde bli bättre på att se över och uppdatera personuppgiftsbehandlingar i registerförteckningen.¹¹

Utifrån den granskning som dataskyddsombudet genomförde i april 2020 (se ovan) står dataskyddsombudet fast vid sin bedömning att stadsdelsnämnden behöver bli bättre på att se över och uppdatera personuppgiftsbehandlingar i registerförteckningen. Under 2020 har förvaltningen tagit fram en rutin för inventering av personuppgiftsbehandlingar i syfte att få bättre styrning på detta område. Rutinen kommer att implementeras år 2021 och dataskyddsombudet kommer under 2021 att följa upp att förvaltningen följer rutinen.

¹⁰ Årsrapport 2019 Enskede-Årsta-Vantörs stadsdelsnämnd, rapport från stadsrevisionen, nr 21, 2020, dnr 3.1.4-25/2020.

¹¹ Uppföljning av dataskyddsarbetet i Enskede-Årsta-Vantör 2019, årsrapport från dataskyddsombudet, dnr EÅV 2020/39.

Brottsdatalagen

Sammanfattning

Dataskyddsombudet bedömer att stadsdelsnämnden har implementerat brottsdatalagen i berörda verksamheter samt tagit fram rutiner som kommer att implementeras år 2021.

Brottsdatalagen började gälla den 1 augusti 2018. Brottsdatalagen bygger på EU:s dataskyddsdirektiv.¹² Dataskyddsdirektivet är en parallell lagstiftning till dataskyddsförordningen.

Brottsdatalagen gäller när en myndighet behandlar personuppgifter för att förebygga, förhindra eller upptäcka brottslig verksamhet, att utreda eller lagföra brott, att verkställa straffrättsliga påföljder eller att upprätthålla allmän ordning och säkerhet.¹³ När en myndighet behandlar personuppgifter för något annat syfte gäller dataskyddsförordningen.

Brottsdatalagen är tillämplig när stadsdelsnämnden behandlar personuppgifter för att verkställa:

- ungdomsvård som ska verkställas inom socialtjänsten
- vård enligt socialtjänstlagen eller lagen med särskilda bestämmelser om vård av unga, som är beslutad av allmän domstol som påföljd för ett brott
- när påföljden för ett brott blir att den enskilde överlämnas av allmän domstol till socialnämnden för vård enligt lagen om vård av missbrukare i vissa fall

Enligt stadsdelsnämndens verksamhetsplan för 2020 ska förvaltningen under 2020 implementera brottsdatalagen i berörda verksamheter samt ta fram och förankra rutiner och information i enlighet med brottsdatalagen.

Under 2020 har förvaltningen genomfört följande aktiviteter kopplat till brottsdatalagen:

- Dataskyddsombudet har haft ett informationsmöte med berörda enhetschefer och dataskyddssamordnare inom avdelningen för social omsorg barn och unga samt avdelningen för social omsorg vuxen. Dataskyddsombudet informerade om brottsdatalagen, när lagen är tillämplig och vad berörda enheter behöver tänka på eller göra för att följa lagen.

¹² 2016/680/EU.

¹³ 1 kap. 2 § brottsdatalagen.

- Frågorna i registerförteckningen i Draftit har uppdaterats så att de uppfyller kraven i 3 kap. 3 § brottsdataförordningen.
- Berörda enheter har registrerat de personuppgiftsbehandlingar som utförs med stöd av brottsdatalagen i registerförteckningen i Draftit.
- Delegationsordningen har uppdaterats utifrån brottsdatalagen.
- En informationstext har tagits fram så att berörda enheter kan informera de registrerade i enlighet med 4 kap. 2 § brottsdatalagen.
- Nya rutiner har tagits fram och kommer att implementeras år 2021 inom dataskyddsområdet. Rutinerna omfattar både dataskyddsförordningen och brottsdatalagen. Det gäller rutiner för inventering av personuppgiftsbehandlingar, hantering av personuppgiftsincidenter, hantering av registrerades rättigheter, konsekvensbedömning och personuppgiftsbiträdesavtal.

Dataskyddsombudet bedömer att stadsdelsnämnden har implementerat brottsdatalagen i berörda verksamheter samt tagit fram information i enlighet med brottsdatalagen samt rutiner som kommer att implementeras år 2021.

EU-domen i Schrems II-målet

Sammanfattning

Stadsdelsnämnden har varit bra på att kartlägga sina tredjelandsöverföringar och följa de rekommendationer och restriktioner i staden till följd av EU-domen i Schrems II-målet. Nämnden bör avstå från att införa nya tredjelandsöverföringar.

EU-domstolen fastställde den 16 juli 2020 i det så kallade Schrems-II målet C-311/18 att Privacy Shield-avtalet inte ger ett tillräckligt skydd för personuppgifter när dessa förs över till eller ges åtkomst till mottagare i USA. Ogiltigförklaringen innebär att det inte längre är tillåtet för stadsdelsnämnden att på laglig grund föra över eller ge åtkomst till personuppgifter till mottagare i USA.

Dataskyddsombudet har under hösten 2020 gjort följande utifrån de rekommendationer som kommit i staden efter EU-domen:

- Avdelningarna har kartlagt sina lokala avtal och tredjelandsöverföringar och rapporterat till dataskyddsombudet.
- Avdelningarna har även tagit Storbritannien i beaktande i sin kartläggning då Storbritannien blev ett tredjeland från årsskiftet 2020/2021.
- I det fall tredjelandsöverföring har identifierats har behandlingen stoppats och kontakt tagits med leverantör för diskussion om åtgärder för upphörande eller flytt av behandling från tredjeland.
- Restriktioner på sociala medier har införts och det är inte längre tillåtet för verksamheterna att lägga ut personuppgifter på sina sociala mediekonton såsom; Facebook mm.
- I staden pågår ett övergripande arbete och vi följer och bevakar utvecklingen i frågan.

Kartläggningen av tredjelandsöverföringar på förvaltningen visade följande:

Avdelning	Kommentar
Staben	Har kartlagt alla sina avtal och register och meddelat att inga tredjelandsöverföringar förekommer.
Administrativa avdelningen-Ekonomi	Har kartlagt alla sina avtal och register och meddelat att inga tredjelandsöverföringar förekommer.
Administrativa avdelningen-Digitalt verksamhetsstöd	Har kartlagt alla sina avtal och register och meddelat att inga tredjelandsöverföringar förekommer.
Administrativa avdelningen-HR	HR identifierade en tredjelandsöverföring hos friskvårdsleverantören Actiway. Behandlingen stoppades av HR i september 2020 och Actiway vidtog åtgärder och flyttade sin behandling från tredjeland. HR återupptog efter utredning och uppdaterat avtal personuppgiftsbehandlingen i november 2020.
Avdelningen för förskola	Har kartlagt alla sina avtal och register och meddelat att inga tredjelandsöverföringar förekommer.
Avdelningen för lokaler och stadsmiljö	Har kartlagt alla sina avtal och register och meddelat att inga tredjelandsöverföringar förekommer.
Avdelningen för social omsorg barn och unga	Har kartlagt alla sina avtal och register och meddelat att inga tredjelandsöverföringar förekommer.
Avdelningen för social omsorg vuxen	Har kartlagt alla sina avtal och register och meddelat att inga tredjelandsöverföringar förekommer.

Avdelningen för social omsorg äldre	Har kartlagt alla sina avtal och register och meddelat att inga tredjelsöverföringar förekommer.
-------------------------------------	--