

Uppföljning av dataskyddsarbetet i Enskede-Årsta-Vantör 2019

**Årsrapport från
dataskyddsombudet**

Dnr EÅV 2020/39

Uppföljning av dataskyddsarbetet i Enskede-Årsta-Vantör 2019
Årsrapport från dataskyddsombudet

Dnr: EÅV 2020/39

Kontaktperson: Emma Ekelund

Sammanfattning

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

Stadsdelsnämndens dataskyddsombud har sammanställt sina granskningar och iakttagelser avseende Enskede-Årsta-Vantörs stadsdelsnämnds efterlevnad av dataskyddsförordningen under 2019 i en rapport. Rapporten visar följande:

- Stadsdelsnämnden kan bli bättre på att i god tid involvera dataskyddsombudet i alla frågor som rör skyddet av personuppgifter.
- De flesta personuppgiftsincidenter som har rapporterats under året beror på den mänskliga faktorn. Om stadsdelsnämnden implementerar Stockholms stads *riktlinje för informationssäkerhet* i organisationen bedömer dataskyddsombudet att nämnden kan undvika en del personuppgiftsincidenter i framtiden.
- Stadsdelsnämnden är bra på att lägga till nya personuppgiftsbehandlingar i registerförteckningen i Draftit. Nämnden kan dock bli bättre på att se över och uppdatera befintliga personuppgiftsbehandlingar i förteckningen.
- Stadsdelsnämnden kan bli bättre på att informera på sociala mediekonton om hur personuppgifter behandlas. Nämnden kan även bli bättre på att inhämta skriftliga samtycken för fotografier och filmer där personer visas och som publiceras på sociala mediekonton.
- Stadsdelsnämnden behöver teckna personuppgiftsbiträdesavtal med leverantören för tjänsten *Speed up*.

Innehåll

Sammanfattning.....	3
Inledning	5
Definitioner	6
Dataskyddsombudets deltagande i alla dataskyddsfrågor.....	7
Hantering av personuppgiftsincidenter	9
De registrerades rättigheter	13
Register över behandlingar av personuppgifter	14
Sociala medier	16
Personuppgiftsbiträdesavtal	18

Inledning

Enskede-Årsta-Vantörs stadsdelsnämnd är personuppgiftsansvarig för de personuppgifter som nämnden behandlar. Den personuppgiftsansvarige ansvarar för efterlevnaden av dataskyddsförordningen och ska kunna visa att bestämmelserna i dataskyddsförordningen efterlevs.

Den personuppgiftsansvarige ska utse ett dataskyddsombud.¹ Dataskyddsombudets roll är främst att övervaka att den personuppgiftsansvarige följer dataskyddsförordningen 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 under 2019.

Denna rapport omfattar inte efterlevnaden av brottsdatalagen, utan bara dataskyddsförordningen. Detta beror på att dataskyddsombudet inte utsågs till dataskyddsombud enligt brottsdatalagen förens den 21 november 2019.

Stockholm den 20 januari 2020

Emma Ekelund
Dataskyddsombud

¹ Artikel 37 dataskyddsförordningen.

² Artikel 39 dataskyddsförordningen.

³ Artikel 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.

Personuppgiftsbiträde: En fysisk eller juridisk person som behandlar personuppgifter för den personuppgiftsansvariges räkning, till exempel en systemleverantör.

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

Dataskyddsombudets deltagande i alla dataskyddsfrågor

Sammanfattning

Dataskyddsombudet bedömer att stadsdelsnämnden kan bli bättre på att i god tid involvera dataskyddsombudet i alla frågor som rör skyddet av personuppgifter.

Den personuppgiftsansvarige ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.⁵

Under 2019 finns det flera exempel där dataskyddsombudet inte har blivit involverad i frågor som rör skyddet av personuppgifter eller där dataskyddsombudet har blivit involverad för sent, bland annat:

- Dataskyddsombudet fick aldrig möjlighet att lämna synpunkter på förslaget till *Stockholms stads säkerhetsprogram 2020-2023*. I förslaget till program fanns det delar som handlade om dataskydd. Dataskyddsombudet borde därför ha blivit involverad i remissvaret.
- Dataskyddsombudet fick i ett mycket sent skede reda på att systemet Boss, som används av budget- och skuldrådgivarna, skulle uppgraderas och att den personuppgiftsansvarige behövde teckna ett nytt personuppgiftsbiträdesavtal med systemleverantören. Om dataskyddsombudet hade involverats i god tid hade dataskyddsombudet kunnat uppmana den personuppgiftsansvarige att genomföra en konsekvensbedömning och hjälpt den personuppgiftsansvarige att granska personuppgiftsbiträdesavtalet innan det skrevs på.
- Dataskyddsombudet fick först i efterhand kännedom om att personuppgiftsbiträdesavtal hade tecknats med en leverantör för parkskötsel. Om dataskyddsombudet hade involverats i god tid hade dataskyddsombudet haft möjlighet att hjälpa den personuppgiftsansvarige att bedöma om det föreligger en biträdessituation och att granska personuppgiftsbiträdesavtalet innan det skrevs på.

⁵ Artikel 38 dataskyddsförordningen.

- Dataskyddsombudet fick i ett mycket sent skede information om att en central konsekvensbedömning skulle genomföras inom försörjningsstöd gällande Mina meddelanden i Paraplysystemet (det var i Mina meddelanden som det skedde en stor personuppgiftsincident i staden i december 2018). Dataskyddsombudet ska involveras i genomförandet av konsekvensbedömningar och det är därför viktigt att dataskyddsombudet får kännedom om planerade konsekvensbedömningar i god tid.

Dataskyddsombudet bedömer att den personuppgiftsansvarige kan bli bättre på att i god tid involvera dataskyddsombudet i alla frågor som rör skyddet av personuppgifter.

Hantering av personuppgiftsincidenter

Sammanfattning

Stadsdelsnämnden har en väl förankrad rutin för att hantera personuppgiftsincidenter. Dataskyddsombudet bedömer dock att nämnden kan undvika att en del personuppgiftsincidenter inträffar i framtiden om nämnden implementerar Stockholms stads *riktlinjer för informationssäkerhet* i organisationen.

Om en personuppgiftsincident inträffar ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inom 72 timmar efter att ha fått vetskap om incidenten, anmäla den till tillsynsmyndigheten, såvida det inte är osannolikt att incidenten medför en risk för personers rättigheter och friheter. Alla personuppgiftsincidenter, oavsett om de anmäls till tillsynsmyndigheten eller inte, ska dokumenteras.⁶ 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.⁷

Under 2019 har det rapporterats totalt 43 personuppgiftsincidenter i stadsdelen. 15 av dessa har anmälts till Datainspektionen (som är Sveriges tillsynsmyndighet enligt dataskyddsförordningen). En incident har inledningsvis anmälts till Datainspektionen men sedan dragits tillbaka då bedömningen har varit att det är osannolikt att incidenten medfört risker för personers rättigheter och friheter.

Dataskyddsombudet bedömer att den personuppgiftsansvarige har en väl förankrad rutin för att hantera personuppgiftsincidenter. Att den personuppgiftsansvarige rapporterar många personuppgiftsincidenter behöver inte vara någonting dåligt. Så här skrev Datainspektionen nyligen i ett nyhetsbrev: *”Att en organisation eller en bransch anmäler många incidenter behöver inte vara en indikation på bristande säkerhet. Tvärtom kan det tyda på att verksamheten har bra rutiner på plats för att upptäcka och rapportera personuppgiftsincidenter.”*⁸

De flesta personuppgiftsincidenter, oavsett om de har anmälts till Datainspektionen eller inte, har inträffat på grund av den mänskliga

⁶ Artikel 33 dataskyddsförordningen.

⁷ Artikel 34 dataskyddsförordningen.

⁸ Datainspektionens nyhetsbrev ”Offentlig sektor allt bättre på att anmäla personuppgiftsincidenter”, 2019-11-11.

faktorn. Det handlar bland annat om att behörigheter inte har tagits bort vid avslutad anställning, att personuppgifter har skickats till fel mottagare, att personuppgifter har skickats på ett osäkert sätt eller att personuppgifter inte har varit tillräckligt skyddad genom till exempel skalskydd eller förvaring i säkra skåp.

Dataskyddsombudets slutsats av detta är att den personuppgiftsansvarige inte har implementerat Stockholms stads *riktlinje för informationssäkerhet* i organisationen. I riktlinjen står det bland annat hur information ska skickas på ett säkert sätt och i övrigt skyddas. Dataskyddsombudet bedömer att den personuppgiftsansvarige kan undvika att en del personuppgiftsincidenter inträffar i framtiden om den personuppgiftsansvarige implementerar riktlinjen för informationssäkerhet. Under 2020 ska förvaltningen påbörja ett projekt kring informationssäkerhet. Projektet syftar till att bygga upp ett ledningssystem för informationssäkerhet. Förhoppningsvis kommer detta att leda till att stadens riktlinje för informationssäkerhet implementeras i organisationen.

Lista över incidenter som har anmälts till Datainspektionen

Typ av incident	Berörd avdelning	Anmäld till DI* inom 72	Beslut från DI*
Handling har kommit bort med posten.	Individ- och familjeomsorg barn och unga	Ja.	DI har beslutat att avsluta ärendet.
Handling har kommit bort med posten.	Individ- och familjeomsorg barn och unga	Ja.	DI har beslutat att avsluta ärendet.
Handling har kommit bort med posten.	Individ- och familjeomsorg barn och unga	Ja.	DI har beslutat att avsluta ärendet.
Uppgifter har spridits felaktigt via röstbrevlåda.	Individ- och familjeomsorg vuxen	Ja.	DI har beslutat att avsluta ärendet.
Dokumentskåp har brutits upp i samband med inbrott.	Förskola	Nej.	Inväntar beslut från DI.

Vid utlämnande av handling till brukare följde ett beslut som rör en annan brukare med.	Individ- och familjeomsorg vuxen	Ja.	DI har beslutat att avsluta ärendet.
Uppgifter har spridits felaktigt via röstbrevlåda.	Individ- och familjeomsorg vuxen	Nej.	DI har beslutat att avsluta ärendet.
En utredning om en brukare har av misstag skickats till en annan brukare.	Äldreomsorg	Nej.	DI har beslutat att avsluta ärendet.
Behörighet har inte tagits bort i ett system vid avslutad anställning vilket lett till att personen kommit åt uppgifterna efter avslutad anställning.	Förskola	Nej.	DI har beslutat att avsluta ärendet.
Boendelista har hittats utanför ett vård- och omsorgsboende.	Äldreomsorg	Ja.	Inväntar beslut från DI.
USB-minne har tappats bort.	Individ- och familjeomsorg barn och unga	Nej.	Inväntar beslut från DI.
Beslut har skickats till fel mottagare.	Äldreomsorg	Nej.	Inväntar beslut från DI.
Telefon har blivit stulen.	Förskola	Nej.	Inväntar beslut från DI.
Några medarbetare med skyddade uppgifter har saknat sekretessmarkering i LISA på grund av att ansvariga chefer inte har skickat in beslut till serviceförvaltningen eller medarbetarna inte har meddelat att de har skyddade uppgifter.	Förskola, HR	En första anmälan gjordes inom 72 timmar. Några dagar senare, efter vidare utredning, drogs anmälan tillbaka.	Inväntar beslut från DI.

Uppföljning av dataskyddsarbetet i Enskede-Årsta-Vantör 2019
12 (18)

Brev har skickats till fel adress.	Individ- och familjeomsorg barn och unga	Nej.	Inväntar beslut från DI.
Fel namn har angetts i handling som skickats till brukare.	Äldreomsorg	Ja.	Inväntar beslut från DI.

* DI = Datainspektionen.

De registrerades rättigheter

Sammanfattning

Under 2019 har det kommit in tre begäran om registerutdrag. I alla tre fall har registerutdrag lämnats ut.

Fysiska personer har rätt att begära ett registerutdrag över vilka personuppgifter den personuppgiftsansvarige behandlar om personen.⁹ Fysiska personer har även rätt att begära att få sina personuppgifter rättade och raderade, begära begränsning av behandlingen av sina personuppgifter, begära överflyttning av sina personuppgifter och invända mot behandlingen av sina personuppgifter.¹⁰ När en begäran kommer in ska den personuppgiftsansvarige bedöma om begäran ska bifallas eller avslås.

Under 2019 kom det in tre begäran om registerutdrag till den personuppgiftsansvarige. I alla tre fall har begäran bifallits och registerutdrag har lämnats ut. Inga övriga begäran har kommit in till den personuppgiftsansvarige under året.

⁹ Artikel 15 dataskyddsförordningen.

¹⁰ Artikel 16-21 dataskyddsförordningen.

Register över behandlingar av personuppgifter

Sammanfattning

Stadsdelsnämnden är bra på att lägga in nya personuppgiftsbehandlingar i registerförteckningen. Dataskyddsombudet bedömer dock att nämnden kan bli bättre på att se över och uppdatera befintliga personuppgiftsbehandlingar i registerförteckningen.

Den personuppgiftsansvarige ska föra ett register över de behandlingar av personuppgifter som utförs under dess ansvar,¹¹ en så kallad "registerförteckning". Den personuppgiftsansvarige 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. Dataskyddsombudet granskar löpande de personuppgiftsbehandlingar som läggs in i registerförteckningen i syfte att kontrollera att de uppfyller kraven i dataskyddsförordningen. Om dataskyddsombudet bedömer att en behandling uppfyller kraven i dataskyddsförordningen markerar dataskyddsombudet behandlingen som "godkänd". Om dataskyddsombudet är osäker om en behandling uppfyller kraven i dataskyddsförordningen förs en dialog med berörd avdelning.

Den 2 december 2019 gjorde dataskyddsombudet ett utdrag ur registerförteckningen i Draftit för att se hur många registreringar varje avdelning hade lagt in förteckningen och hur många av dessa som var markerade som "godkänd".

Utdrag ur registerförteckningen den 2 december 2019

Avdelning	Totalt antal registreringar	Antal "godkända" registreringar
Administrativa avdelningen	42	31 (74 %)
Staben	48	47 (98 %)

¹¹ Artikel 30 dataskyddsförordningen.

Funktionsnedsättning och socialpsykiatri	90	78 (87 %)
Äldreomsorg	101	55 (54 %)
Förskola	37	32 (86 %)
Individ- och familjeomsorg barn och unga	78	73 (94 %)
Individ- och familjeomsorg vuxen	78	53 (68 %)
Kultur, fritid och demokrati	41	41 (100 %)
Utveckling, lokaler och stadsmiljö	20	20 (100 %)

Att en avdelning har ett lågt antal godkända registreringar kan bero tre olika saker:

- Avdelningen är inte klar med registreringen.
- Avdelningen har gjort ändringar i registreringen och dataskyddsombudet har inte hunnit granska ändringarna.
- Dataskyddsombudet har begärt att avdelningen ska komplettera registreringen med uppgifter.

Personuppgiftsbehandlingar tillkommer och förändras ständigt. Det är därför viktigt att den personuppgiftsansvarige har en systematik för att löpande lägga in nya personuppgiftsbehandlingar i registerförteckningen samt för att se över och uppdatera de personuppgiftsbehandlingar som lagts in i registerförteckningen. Att en avdelning har ett högt antal godkända registreringar behöver inte betyda att avdelningen löpande ser över och uppdaterar befintliga registreringar.

Dataskyddsombudet bedömer att den personuppgiftsansvarige är bra på att lägga in nya personuppgiftsbehandlingar i registerförteckningen. Den personuppgiftsansvarige kan dock bli bättre på att se över och uppdatera befintliga personuppgiftsbehandlingar i registerförteckningen.

Sociala medier

Sammanfattning

Dataskyddsombudet bedömer att stadsdelsnämnden kan bli bättre på att informera på sociala mediekonton om hur personuppgifter behandlas. Dataskyddsombudet bedömer även att nämnden kan bli bättre på att inhämta skriftliga samtycken för fotografier och filmer där personer visas och som publiceras på sociala mediekonton.

I mars genomförde dataskyddsombudet en granskning av sex sociala mediekonton som den personuppgiftsansvarige har. Granskningen skedde genom granskning av själva kontot (i de fall kontot var publikt) samt genom att ställa följande frågor till redaktörerna för kontona:

- Finns det information på kontot om hur personuppgifter behandlas?
- Finns det dokumenterade samtycken för bilder och filmer där personer visas?
- Hur ofta bevakas kontot?

Granskningen visade att bara ett konto hade information om hur personuppgifter behandlas. I ungefär hälften av fallen fanns det dokumenterade samtycken för bilder och filmer där personer visas. Samtliga konton bevakades regelbundet.

Dataskyddsombudet bedömer att den personuppgiftsansvarige kan bli bättre på att informera på sociala mediekonton om hur personuppgifter behandlas samt på att inhämta skriftliga samtycken för fotografier och filmer där personer visas.

Kontots namn	Avdelning	Info. om GDPR	Dokumenterade samtycken	Bevakning av kontot
Hagsätra fritidsgård (Facebook)	Kultur, fritid och demokrati	Nej.	Ja.	En gång i veckan.
Bandängens parklek (Facebook)	Kultur, fritid och demokrati	Nej.	För vissa bilder.	Ungefär en gång om dagen.
Enskede-Årsta-Vantörs stadsdelsförvaltning (Facebook)	Övergripande, staben	Ja.	Ja.	Dagligen.

eavsdf (Instagram)	Över- gripande, staben	Nej.	Ja.	Dagligen.
igelkotten_ haren.arken (Instagram)	Förskola	Nej.	Nej.	Ungefär en gång om dagen.
snosatraforskolor (Instagram)	Förskola	Nej.	Har bara en bild och personen på den bilden kan inte identifieras. I det fallet inhämtades muntligt samttycke.	Minst en gång i veckan.

Personuppgiftsbiträdesavtal

Sammanfattning

Dataskyddsombudet bedömer att stadsdelsnämnden behöver ingå ett personuppgiftsbiträdesavtal med leverantören för tjänsten *Speed up*.

Om ett personuppgiftsbiträde behandlar personuppgifter för den personuppgiftsansvariges räkning ska den personuppgiftsansvarige reglera detta i ett personuppgiftsbiträdesavtal eller annan rättsakt.¹²

I april granskade dataskyddsombudet om den personuppgiftsansvarige hade ingått personuppgiftsbiträdesavtal i de fall där den personuppgiftsansvarig är skyldig att göra det. Granskningen skedde genom ett utdrag av uppgifter från Draftit. Granskningen baserades alltså bara på de uppgifter som avdelningarna hade lagt in i registerförteckningen i Draftit.

Granskningen visade att den personuppgiftsansvarige saknade personuppgiftsbiträdesavtal för tre tjänster: *Insyn*, *Ai-Ai* och *Speed up*. Efter granskningen har personuppgiftsbiträdesavtal tecknats för *Insyn* och *Ai-Ai*. Personuppgiftsbiträdesavtal saknas fortfarande för *Speed up*.

Dataskyddsombudet bedömer att den personuppgiftsansvarige behöver teckna ett personuppgiftsbiträdesavtal med leverantören för tjänsten *Speed up*.

¹² Artikel 28 dataskyddsförordningen.