Handläggare
Maria Wedenlid
Telefon: 08-508 11 837

Till
Servicenämnden
2018-06-19

Dataskyddsombud för Servicenämnden

Förvaltningens förslag till beslut

Servicenämnden utser Maria Wedenlid till dataskyddsombud för servicenämnden.

Anna-Karin Sandén
Tf. förvaltningschef

Sammanfattning

Dataskyddsförordningen (GDPR) ersatte den 25 maj 2018 personuppgiftslagen (PuL). Detta ärende beskriver principer och ansvar för dataskyddsarbetet inom servicenämndens ansvarsområde. Förvaltningen föreslår att nämnden utser Maria Wedenlid till dataskyddsombud.

Serviceförvaltningen
Stab

Palmfeltsvägen 5
Box 7005
12107 Stockholm
Telefon 08-508 11 837
maria.wedenlid@stockholm.se
stockholm.se

Bakgrund

Från och med den 25 maj 2018 gäller Europaparlamentets och rådets förordning om skydd för fysiska personer med avseende på behandling av personuppgifter. Dataskyddsförordningen (GDPR) ersätter personuppgiftslagen (PuL). Förordningen gäller för i princip all automatiserad behandling av personuppgifter och i vissa fall även manuell behandling av personuppgifter. Personuppgifter är varje upplysning som avser en identifierad eller identifierbar fysisk person.

Många av dataskyddsförordningens begrepp och principer återfinns i personuppgiftslagen med tillhörande bestämmelser. Förordningen innebär även förändringar som är viktiga att känna till. Några tydliga förändringar är

- ökade krav på hantering av personuppgifter,
- ökat ansvar för personuppgiftsansvariga,
- ökat ansvar för personuppgiftsbiträden,
- dataskyddsombud – stärkt roll,
- den registrerades rättigheter förstärks,
- strängare sanktioner

Dataskyddsförordningen medför bland annat att dataskyddsombud ska utses och rapporteras till Datainspektionen.

Ärendet

Serviceförvaltningen har inför GDPR följt stadens mall för inventering av hantering av personuppgifter. Förvaltningen fortsätter följa stadens gemensamma arbete och planerar för att implementera kommande riktlinjer och rutiner i nämndens verksamheter.

Personuppgiftsansvarig

Definitionen av personuppgiftsansvarig är densamma som i personuppgiftslagen. Personuppgiftsansvarig ansvarar för att principerna för behandling av personuppgifter efterlevs. Servicenämnden är personuppgiftsansvarig för all behandling av personuppgifter inom nämndens ansvarsområde. Varje chef är ansvarig för att personuppgifter hanteras på ett lagligt och korrekt sätt inom sitt verksamhetsansvar.

Dataskyddsprinciper

Dataskyddsförordningen fastställer principer för behandling av personuppgifter. Syftet med principerna är att styra behandlingen av personuppgifter så att kraven i förordningen uppfylls och den

registrerades rättigheter respekteras. Följande principer gäller för behandling av personuppgifter:

1. Personuppgifter ska behandlas på ett **lagligt, korrekt och öppet sätt** i förhållande till den registrerade.

   Med öppet sätt menas att det för de registrerade bör vara klart och tydligt hur uppgifter som gäller dem insamlas och används samt i vilken utsträckning personuppgifterna behandlas eller kommer att behandlas. Öppenhetsprincipen kräver att all information och kommunikation i samband med behandlingen av personuppgifter är lättillgänglig och lättbegriplig.

2. Insamlingen av personuppgifter ska vara begränsad till ändamålet och ske för **särskilda, uttryckligt angivna och berättigade ändamål.** Uppgifterna får inte senare användas för ett ändamål som inte är bundet till ändamålet med de insamlade uppgifterna.

   Ändamålsbegränsningen hindrar inte att uppgifterna används för arkivändamål eller för historiska forskningsändamål eller för statistiska ändamål.

3. Insamlingen av personuppgifter ska vara **uppgiftsminimerad,** dvs. inte vara för omfattande i förhållande till de ändamål för vilka uppgifterna behandlas, och uppgifterna ska vara adekvata och relevanta.

   Personuppgifter bör behandlas endast om syftet med behandlingen inte rimligen kan uppnås genom andra medel.

4. Personuppgifterna ska vara **korrekta** och om nödvändigt **uppdaterade**. Den personuppgiftsansvarige ska med rimliga åtgärder säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.

   Den personuppgiftsansvarige ska till exempel med hjälp av fastställda tidsfrister, säkerställa att personuppgifter inte förvaras längre än nödvändigt.

5. Personuppgifter ska förvaras i en form som möjliggör identifiering av den registrerade endast under den tid som är nödvändig för de ändamål för vilka personuppgifterna behandlas. Uppgifter får dock förvaras längre, om de endast

behandlas för arkivändamål av allmänt intresse, eller används för historiska forskningsändamål eller statistiska ändamål.

6. Personuppgifter ska behandlas på ett sätt som **säkerställer lämplig säkerhet** för uppgifterna. Uppgifterna ska skyddas mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Då ska lämpliga tekniska eller organisatoriska åtgärder användas.

Varje chef ansvarar för att kraven i förordningen uppfylls inom sitt ansvarsområde.

Arkiv och gallring utifrån dataskyddsförordningen

En allmän princip i dataskyddsförordningen (GDPR) är att personuppgifter inte ska sparas längre än nödvändigt. GDPR slår samtidigt fast att uppgifter får sparas för arkivändamål av allmänt intresse. Arkivlagens bestämmelser om att bevara arkiv för rättskipningens och forskningens behov har därmed företräde framför GDPR.

Regelverket för bevarande av arkiv och gallring av allmänna handlingar hos stadens verksamheter ändrades därmed inte när GDPR infördess, utan det som gäller för staden är samma som tidigare.
Bevarande av allmänna handlingar är huvudregel. Radering (gallring) får endast ske enligt gallringsbeslut fattade av stadsarkivet. Om det helt saknas bestämmelser om hur länge handlingar ska finnas kvar måste en informationsvärdering göras och förvaltningen behöver ansöka om ett gallringsbeslut hos Stockholms stadsarkiv.

Registerförteckning

Den personuppgiftsansvariga är skyldig att föra ett register eller en förteckning över behandlingar av personuppgifter. Registret ska upprättas skriftligen, vara tillgängligt i elektronisk format och hållas uppdaterat. På begäran ska registret göras tillgängligt för Datainspektionen.

Registret ska innehålla följande uppgifter:

- Namn och kontaktuppgifter för den personuppgiftsansvarige, den personuppgiftsansvariges företrädare samt dataskyddsombudet.
- Ändamålen med behandlingen.
- En beskrivning av kategorierna av registrerade och kategorierna av personuppgifter.

- De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut.
- I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation.
- Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.
- Om möjligt, en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder.

Varje chef ansvarar för att registerförteckningen är aktuell och uppdaterad inom sitt ansvarsområde.

Dataskyddsombud

När en myndighet behandlar personuppgifter ska personuppgiftsansvarig utse ett dataskyddsombud (tidigare personuppgiftsombud). Dataskyddsombudet ska utses utifrån yrkesmässiga kvalifikationer och sakkunskap om lagstiftning och praxis samt förmåga att utföra ett dataskyddsombuds uppgifter. Ombudet får ingå i den personuppgiftsansvariges ordinarie personal eller utföra uppgifterna enligt särskilt tjänsteavtal. Ett dataskyddsombud får utses för flera myndigheter med hänsyn till organisationsstruktur och storlek. Det finns inget hinder mot att flera personer utses till dataskyddsombud. Personuppgiftsansvarig ska offentliggöra dataskyddsombudets kontaktuppgifter och meddela tillsynsmyndigheten.

Personuppgiftsansvarig ska säkerställa att dataskyddsombudet deltar i alla frågor som rör skyddet av personuppgifter, och tillhandahålla de resurser ombudet behöver för sina uppgifter och för upprätthållande av sin sakkunskap.

Dataskyddsombudet ska

- informera och ge råd till personuppgiftsansvarig, personuppgiftsbiträdet och de anställda som behandlar personuppgifter om skyldigheter,
- övervaka efterlevnaden av dataskyddsförordningen och av den personuppgiftsansvariges strategi för dataskydd, inbegripet bland annat information, granskning och kontroller,
- ge råd till personuppgiftsansvarig om konsekvensbedömning
- samarbeta med och vara kontaktpunkt för tillsynsmyndigheten och vara kontaktperson mot registrerade

Konsekvensbedömning och förhandssamråd

Om behandlingen av personuppgifter sannolikt är förknippad

med stora risker, ska den personuppgiftsansvarig göra en konsekvensbedömning av dataskyddet. Då bedöms riskerna i anslutning till behandlingen och också metoderna för att möta dessa risker.

Konsekvensbedömning ska göras särskilt om det används ny teknik eller om det gäller omfattande behandling av personuppgifter eller särskilda kategorier av personuppgifter. Med särskilda kategorier avses det som enligt personuppgiftslagen definieras känsliga personuppgifter, d.v.s. uppgifter om etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, uppgifter om hälsa eller uppgifter om en persons sexualliv eller sexuella läggning. Vid en konsekvensbedömning ska dataskyddsombudet rådfrågas. Visar konsekvensbedömningen att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken ska förhandssamråd ske med Datainspektionen.

Varje chef svarar för att dataskyddsombudet rådfrågas om en konsekvensbedömning av dataskyddet behöver göras.

Rapportering av personuppgiftsincident

Personuppgiftsansvarig ska utan onödigt dröjsmål och om möjligt senast 72 timmar efter att ha fått vetskap anmäla en personuppgiftsincident till tillsynsmyndigheten om det inte är osannolikt att incidenten medför risk för personers rättigheter och friheter.

En personuppgiftsincident är en säkerhetshändelse som har påverkat sekretessen, integriteten eller tillgängligheten till personuppgifter. En personuppgiftsincident har inträffat om personuppgifter har

- förstörts, oavsiktligt eller olagligt
- gått förlorade eller ändrats
- röjts till någon obehörig.

Personuppgiftsincidenter ska dokumenteras, inklusive dess effekter och vilka åtgärder som vidtagits, i syfte att möjliggöra kontroll att bestämmelsen har följts.

Om det är sannolikt att personuppgiftsincidenten leder till hög risk för personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade.

Anmälan av personuppgiftsincidenter inom servicenämndens ansvarsområde görs till dataskyddsombudet som i sin tur gör anmälan till Datainspektionen som är tillsynsmyndighet.

För närvarande pågår ett arbete på stadsövergripande nivå med att ta fram riktlinjer och rutiner för rapportering av personuppgifts-incidenter. Riktlinjer och rutiner implementeras och anpassas vid behov i samtliga verksamheter.

Varje chef ansvarar för att berörda medarbetare känner till rutiner för anmälan av personuppgiftsincidenter.

Styrning och uppföljning

För att säkerställa att principerna för behandling av personuppgifter efterlevs bör genomgång av instruktioner och rutiner ingå i introduktion för nya medarbetare och chefer. Internkontrollplanen kompletteras för att säkerställa att dataskyddsförordningen följs över tid.

Ärendets beredning

Ärendet har beretts inom staben.

Förvaltningens förslag

Förvaltningen föreslår att servicenämnden utser Maria Wedenlid till dataskyddsombud.