Handläggare
Trafikkontoret
Ann-Marie Nyberg
Administrativa avdelningen
Telefon: 08-508 27 095

Exploateringskontoret
Ann-Charlotte Bergqvist
Administrativa avdelningen
Telefon: 08-508 27 125

Till
Trafiknämnden
2018-04-19
Exploateringsnämnden
2018-04-19

Dataskyddsförordningen. Information och anmälan av dataskyddsombud för trafiknämnden och exploateringsnämnden

Förslag till beslut

1. Trafiknämnden godkänner kontorets förslag till dataskyddsombud/anmälan av dataskyddsombud i enlighet med kontorets tjänsteutlåtande.

2. Exploateringsnämnden godkänner kontorets förslag till dataskyddsombud/anmälan av dataskyddsombud i enlighet med kontorets tjänsteutlåtande.

Jonas Eliasson
Förvaltningschef
Trafikkontoret

Håkan Falk
Förvaltningschef
Exploateringskontoret

Sammanfattning

Den 25 maj 2018 ersätter EU:s dataskyddsförordning den svenska personuppgiftslagen och skapar ett enhetligt regelverk inom EU för behandling av personuppgifter.

Dataskyddsförordningen gäller alla verksamheter som behandlar personuppgifter och alla personuppgiftsbehandlingar oavsett form.

Respektive nämnd i Stockholms stad kommer även fortsättningsvis att vara personuppgiftsansvarig på samma sätt som idag gäller för personuppgiftslagen.

Trafikkontoret
Administration

Fleminggatan 4
Box 8311
104 20 Stockholm
Telefon 08-508 27 095
Växel 08-508 27 200
ann-marie.nyberg@stockholm.se
trafikkontoret@stockholm.se
Org nr 212000-0142
stockholm.se

Många av dataskyddsförordningens begrepp och principer finns också i personuppgiftslagen men förordningen innebär en del förändringar och ökade krav på öppenhet, integritetsskydd och hur den registrerades rättigheter tas tillvara.

Alla personuppgiftsansvariga myndigheter och offentliga organ måste utse ett dataskyddsombud men det finns inget som hindrar att ett gemensamt dataskyddsombud utses för exempelvis flera nämnder. Dataskyddsombudet har en central och utökad roll då det gäller personuppgiftsbehandlingar och ska bland annat informera och ge råd till personuppgiftsansvarig, personuppgiftsbiträde och de anställda, vara kontaktperson mot tillsynsmyndighet och de registrerade samt övervaka efterlevnaden av dataskyddsförordningen.

Trafikkontoret och exploateringskontoret föreslår att kontoren har ett gemensamt dataskyddsombud. Kontorens bedömning är att detta är ett lämpligt åtagande som även möjliggör andra arbetsuppgifter för ombudet.

Till dataskyddsombud föreslås arkivarie Sara Helling Broström som arbetar på trafikkontorets administrativa avdelning.

Bakgrund

Den 25 maj 2018 ersätter EU:s dataskyddsförordning den svenska personuppgiftslagen och skapar ett enhetligt regelverk inom EU för behandling av personuppgifter. Förordningen innehåller regler om hur myndigheter, företag och andra får behandla personuppgifter. Som komplement till förordningen föreslås en dataskyddslag på nationell nivå.

Dataskyddsförordningen gäller alla verksamheter som behandlar personuppgifter och alla personuppgiftsbehandlingar oavsett form. Respektive nämnd i Stockholms stad kommer även fortsättningsvis att vara personuppgiftsansvarig på samma sätt som har gällt för personuppgiftslagen.

Förändringar jämfört med personuppgiftslagen

Många av dataskyddsförordningens begrepp och principer finns sedan tidigare i personuppgiftslagen, men förordningen innebär en del förändringar och ökade krav på öppenhet, integritetsskydd och hur den registrerades rättigheter tas tillvara.

Några tydliga förändringar är:

- ökade krav på hantering av personuppgifter
- krav att kunna visa vilka personuppgifter som samlas in och med vilket lagstöd
- ökat ansvar för personuppgiftsansvariga
- ökat ansvar för personuppgiftsbiträden
- dataskyddsombud, en ny och stärkt roll
- den registrerades rättigheter förstärks
- strängare sanktioner införs

Personuppgifter/känsliga personuppgifter

En personuppgift är en uppgift som direkt eller indirekt kan hänföras till en fysisk person. Exempel på personuppgifter är namn, personnummer, e-postadress, bild, registreringsnummer och ip-adress. Vissa personuppgifter är känsliga som uppgifter om etnicitet, politisk åsikt, sexuell läggning, religiös eller politisk övertygelse, hälso- och genetisk data och medlemskap i fackförening. Utgångspunkten är att känsliga personuppgifter inte får behandlas, men undantag finns som i vissa fall möjliggör behandling av känsliga personuppgifter.

Personuppgifter återfinns i såväl strukturerad form (IT-system, register etc.) som ostrukturerad form (löpande text etc.). Förordningen gäller till skillnad från personuppgiftslagen även personuppgifter i ostrukturerad form såsom löpande text i e-post, dokument, sms etc.

Tillåten personuppgiftsbehandling

För att en organisation ska få behandla personuppgifter krävs att allmänna principer för behandling av personuppgifter är uppfyllda och att behandlingen vilar på laglig grund.

Allmänna principer

Vid behandling av personuppgifter ska följande gälla:

- uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt
- uppgifterna ska samlas in för ett uttryckligt angivet och berättigat ändamål och behandlas i enlighet med detta angivna ändamål
- uppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålen
- uppgifterna ska vara korrekta och om nödvändigt uppdaterade

- uppgifterna ska inte lagras längre än nödvändigt
- uppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet

Laglig grund

Minst ett av nedan angivna kriterier måste föreligga för att laglig grund ska vara uppfyllt:

- Samtycke
- Avtalsrelation
- Rättslig förpliktelse
- Skydda grundläggande intressen
- Myndighetsutövning/allmänt intresse

Även intresseavvägning är en laglig grund men ej tillämpbar för myndigheter.

Personuppgiftsansvaret

Personuppgiftsansvarig

Personuppgiftsansvarig är den organisation, i Stockholms stad nämnd eller bolagsstyrelse, som bestämmer för vilket ändamål uppgifterna ska behandlas och hur behandlingen ska gå till. Den som är personuppgiftsansvarig kan överlåta den faktiska behandlingen av personuppgifter, men personuppgiftsansvaret kan aldrig överlåtas. Den personuppgiftsansvarige måste se till att behandlingen sker i enlighet med dataskyddsförordningens samtliga bestämmelser.

Säkerhet och skydd för personuppgifter

Dataskyddsförordningen ställer tydliga krav på inbyggt dataskydd (privacy by design) och dataskydd som standard (privacy by default). I detta inbegrips bland annat att lämpliga tekniska och organisatoriska åtgärder genomförs som uppgiftsminimering, att endast uppgifter som är nödvändiga för ett speciellt ändamål samlas in, att mängden insamlade uppgifter begränsas och att tiden för deras lagring begränsas samt att tillgängligheten begränsas.

Konsekvensbedömning

En konsekvensbedömning ska göras innan en behandling utförs som sannolikt medför hög risk för fysiska personers fri- och rättigheter. Konsekvensbedömningen bör utföras i samverkan med dataskydds-ombudet av den enhet som planerar att utföra personuppgifts-behandlingen.

Registerförteckning
Samtliga personuppgiftsbehandlingar ska finnas i den registerförteckning som ska föras. Registerförteckningen förs förslagsvis av dataskyddsombudet.

Anmälan av personuppgiftsincident till tillsynsmyndigheten
Vid en personuppgiftsincident ska anmälan göras till tillsyns-myndigheten. Anmälan ska ske utan onödigt dröjsmål och om möjligt senast 72 timmar efter det att incidenten upptäckts. Detta gäller om det inte är osannolikt att incidenten medför risk för personers rättigheter och friheter. Om incidenten sannolikt leder till hög risk ska den registrerade informeras om incidenten. Vid en personuppgiftsincident är troligtvis flera parter involverade som IT-driftsleverantör, stadsledningskontoret, respektive IT-funktion på kontoren samt dataskyddsombudet. Processen för incident-hanteringen är inte klar men troligt är att dataskyddsombudet hanterar anmälan till tillsynsmyndigheten.

Personuppgiftsbiträde
Den som behandlar personuppgifter för den personuppgifts-ansvariges räkning kommer, i likhet med vad som gäller för personuppgiftslagen, att vara personuppgiftsbiträde. Personuppgiftsbiträden är till exempel kontorens respektive IT-leverantörer och driftsleverantörer. I dataskyddsförordningen förändras denna roll så att personuppgiftsbiträdet får nya skyldigheter och ett betydligt utökat eget ansvar för personuppgifts-behandlingen. I ett flertal situationer kommer även person-uppgiftsbiträden att omfattas av samma skyldigheter som gäller för personuppgiftsansvariga.

Dataskyddsombud
Alla personuppgiftsansvariga myndigheter och offentliga organ måste utse ett dataskyddsombud. Det finns inget som hindrar att ett gemensamt dataskyddsombud utses för exempelvis flera nämnder. Det går även att anlita ett externt dataskyddsombud. Dataskyddsombudet har en utökad roll gentemot de krav som ställdes på personuppgiftsombudet i personuppgiftslagen. Personuppgiftsansvarig ska säkerställa att dataskyddsombudet deltar i frågor som rör skyddet av personuppgifter, och tillhandahålla de resurser som ombudet behöver. Dataskydds-ombudet rapporterar direkt till personuppgiftsansvarigs högsta ledningsnivå och får inte avsättas eller bli föremål för sanktioner för att ha utfört sina uppgifter.

Dataskyddsombudet ska bland annat:

- informera och ge råd till personuppgiftsansvarig, personuppgiftsbiträdet och de anställda som behandlar personuppgifter
- 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
- vara kontaktperson mot registrerade

Dataskyddsombudets kontaktuppgifter ska anmälas till Datainspektionen.

Den registrerades rättigheter

De viktigaste rättigheterna för de registrerade är:

- vid begäran få tillgång till sina personuppgifter
- få felaktiga uppgifter rättade
- kunna få sina personuppgifter raderade (här finns omfattande undantag för myndigheter)
- ha möjlighet att invända mot att personuppgifterna används för automatiserat beslutsfattande och profilering

Sanktionsavgifter

Dataskyddsförordningen ger en möjlighet att ta ut administrativa sanktionsavgifter för den som bryter mot reglerna. De föreslagna beloppen är höga och enligt dataskyddslagens förslag ska även myndigheter omfattas.

Tillsynsmyndighet

En tillsynsmyndighet i varje EU-land ska övervaka att de som behandlar personuppgifter följer dataskyddsförordningen. Tillsynsmyndigheten ska vara fullständigt oberoende i utförandet av sina uppgifter och utövandet av sina befogenheter. Datainspektionen föreslås att få detta uppdrag i Sverige.

Ärendets beredning

Ärendet har beretts inom trafikkontorets administrativa avdelning och i samråd med exploateringskontorets administrativa avdelning.

Trafikkontorets och exploateringskontorets analys

Kontorens förberedelser inför övergången till Dataskyddsförordningen

Kontoren har arbetat med förberedelser inför övergången till Dataskyddsförordningen genom att personuppgiftsbehandlingar har kartlagts och registerförteckning upprättats. Personuppgifts-behandlingarna har analyserats och den rättsliga grunden för respektive behandling har angivits. Kontoren har ett antal personuppgiftsbehandlingar i form av IT-system och även i ostrukturerad form som dokument, e-post etc. Kontoren har även med staden gemensamma behandlingar inom bland annat ekonomi och HR.

En översyn av befintliga personuppgiftsbiträdesavtal med kontorens IT-leverantörer har inletts och en inventering har påbörjats av behovet att teckna ytterligare personuppgiftsbiträdesavtal.

Workshoppar och möten har hållits med bland annat kontorens verksamheter som har speciella behandlingar. Kontoren planerar för informationsinsatser och material för detta håller på att tas fram. Översyn och framtagande av rutiner och instruktioner pågår.

Många frågeställningar är gemensamma med övriga förvaltningar och bolag inom staden och där så är möjligt sker en samverkan med stadsledningskontoret. Detta gäller bland annat stadsgemensamma system och leverantörer, incidentrapportering och modeller och metoder för informationsklassning och riskanalyser.

Ett antal frågor återstår dock att hantera och arbetet med dataskyddsförordningen är inte en engångsinsats utan ska efterlevas över tid. Rättsliga prövningar och praxis som i dagsläget saknas kommer också framöver att kunna ge ytterligare vägledning.

Trafikkontorets och exploateringskontorets förslag

Trafikkontoret och exploateringskontoret föreslår att kontoren har ett gemensamt dataskyddsombud. Kontorens bedömning är att detta är ett lämpligt åtagande som möjliggör även andra arbetsuppgifter för ombudet. Kontoren har närliggande verksamheter, ett gott samarbete och delar vissa IT-system. Exploateringskontoret föreslås köpa tjänsten från trafikkontoret på samma sätt som med andra administrativa tjänster för bland annat registratur, arkiv och IT-stöd.

Till dataskyddsombud föreslås arkivarie Sara Helling Broström som arbetar på trafikkontorets administrativa avdelning. Vid eventuell

långvarig frånvaro får tjänsten som dataskyddsombud köpas externt eller hanteras genom stöd från till exempel stadsledningskontoret.

Slut