Stockholms stad

Vägledning för inventering av personuppgifter

Första steget mot anpassningen till den nya dataskyddsförordningen

Stadsledningskontoret
Avdelningen för digital utveckling
Hantverkargatan H3D
104 22 Stockholm
stockholm.se

Innehåll

1. Inledning

Dataskyddsförordningen kommer att gälla som lag i alla EU:s medlemsländer från och med den 25 maj 2018. Förordningen kommer att ersätta personuppgiftslagen (1998:204), PuL, och vara direkt tillämplig i Sverige. Många av de bestämmelser som framgår av förordningen går att återfinna i PuLs bestämmelser. Om verksamheten redan idag har väl genomarbetade åtgärder och rutiner för att säkerställa att PuL följs, finns sannolikt en bra grund att utgå från.

För mer läsning kring de förändringar som dataskyddsförordningen innebär hänvisas till det PM som tagits fram av juridiska avdelningen.

Enligt dataskyddsförordningen artikel 30 har personuppgiftsansvariga en skyldighet att upprätta register över samtliga personuppgiftsbehandlingar. Tidigare låg detta ansvar på personuppgiftsombudet.

2. Syfte och innehåll

2.1 Vägledningens uppbyggnad

Denna vägledning som Stadsledningskontoret har tagit fram syftar till att hjälpa personuppgiftsansvariga att uppfylla kravet att upprätta ett register enligt artikel 30. Som ett stöd i detta arbete har en mall tagits fram för att hjälpa verksamheterna att utföra kartläggningen.

Vägledningen består av följande dokument:

PM - Vägledning för inventering av personuppgifter (detta dokument)
Bilaga 1 - Presentation - Inventeringsprocess
Bilaga 2 - Mall för inventering
Bilaga 3 - Mall för personuppgiftsbiträdesavtal

De dokument som tillhandahålls ska främst ses som en vägledning och ett stöd för inventeringen. Målet med bilaga 2 Mall för inventering är att den ska vara enkel att fylla i med valbara alternativ där så är möjligt. Mallen är emellertid generiskt utformad och behöver därför justeras och anpassas

till den specifika verksamheten. Rullgardins-menyerna kan behöva kompletteras eller i vissa fall ändras helt. Det framgår av Excel-filen vilka menyer som behöver kompletteras av den ansvarige.

2.2 Kartläggning av information

För att kunna ta fram ett nuläge och upprätta en registerförteckning krävs att varje verksamhet kartlägger samtliga personuppgiftsbehandlingar som förekommer i verksamheten. Det gäller således både nya och gamla behandlingar som stora IT-system eller enkla Excel-filer. I praktiken innebär inventeringen en detaljerad kartläggning av alla register, system och dokument där personuppgifter förekommer.

All personal bör därmed se över sina digitala enheter och undersöka vilken information som lagras lokalt eller vad som lagras på externa lagringsenheter som exempelvis USB-stickor, externa hårddiskar samt molnbaserade lagringstjänster, men även fysiskt material som datautskrifter. Övrigt material som förvaras i pärmar m.m. där personuppgifter inte är sökbara omfattas inte av lagen.

I samband med inventeringen bör säkerställas att det finns ett ändamål med personuppgiftsbehandlingen, att behandlingen följer de allmänna principerna (avsnitt 8), samt att personuppgiftsbehandlingarna är lagliga (avsnitt 7) m.m. En utvärdering ska därefter göras på allt insamlat material. Genom att dokumentera personuppgiftsbehandlingen säkerställs uppfyllnad av dataskyddsförordningens krav på att kunna visa att förordningens bestämmelser följs.

Det åligger därför varje nämnd/bolag att genomföra en inventering av de personuppgifter som hanteras i dess verksamhet samt att säkerställa korrekt hantering och implementering i enlighet med den nya dataskyddsförordningen. Kartläggning av alla personuppgiftsbehandlingar är en tidskrävande process och kan komma att kräva ett flertal resurser. Därför är det av stor vikt att kartläggningen påbörjas så snart som möjligt.

Beroende på hur väl PuL efterlevs idag kommer arbetet med anpassningen till dataskyddsförordningen att variera mellan verksamheterna. För den verksamhet som idag har god

kännedom och kontroll över sina personuppgiftsbehandlingar kommer gapet inte att vara lika stort som för den verksamhet som tidigare inte efterlevt PuL fullt ut.

2.3 Registerförteckning

Registerförteckningen uppfyller flera funktioner. Genom att upprätta en registerförteckning skapas god kontroll över personuppgifternas livscykel och denna kan ligga till grund för verksamhetens processer och utvecklingen av dessa, samt vilka säkerhetsåtgärder som behöver vidtas om behandlingen exempelvis rör känsliga uppgifter. Förteckningen bör innehålla information om vilka uppgifter som samlas in, varifrån uppgifterna samlas in, till vem uppgifterna lämnas ut, vart uppgifterna lagras, i vilka system används uppgifterna och för vilka ändamål dessa används.

Utöver att ge en god överblick syftar en registerförteckning även till att säkerställa att det finns en laglig grund för personuppgiftsbehandlingen. Förteckningen kan även användas för att visa upp för Datainspektionen vid ett eventuellt tillsynsärende, för uppföljning av efterlevnad, för att användas i samband med registerutdrag, för att hitta personuppgiftsbiträdesavtal som behöver uppdateras samt för att hitta dokumenterade åtgärder, t.ex. konsekvensbedömningar.

Registerförteckningen ska innehålla en s.k. registerbeskrivning över varje behandling av personuppgifter i verksamheten. En registerförteckning ska innehålla minst följande uppgifter:

- Namn och kontaktuppgifter för den personuppgiftsansvarige, den personuppgiftsansvariges företrädare samt dataskyddsombudet
- Ändamål med behandlingen
- Kategorier av registrerade
- Kategorier av personuppgifter
- Kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut
- Överföringar av personuppgifter till tredje land eller en internationell organisation
- Förutsedda tidsfrister för radering av de olika kategorierna av uppgifter, om möjligt

- Allmän beskrivning av de tekniska och organisatoriska skyddsåtgärder, om möjligt

Varje verksamhet bör utse ägarskap för registerförteckningen då det är ett levande dokument som ska uppdateras regelbundet. Vid varje ny personuppgiftsbehandling eller när en behandling upphör bör förteckningen uppdateras. Enligt dataskyddsförordningen ska registerförteckningen göras tillgänglig för Datainspektionen om en sådan begäran framställs.

Registret ska upprättas skriftligen inbegripet i elektronisk form.

En väl dokumenterad personuppgiftsbehandling bidrar till:

- Säkerställande av de registrerades rättigheter
- Lägre risk för personuppgiftsincidenter
- Säkerställande av regelefterlevnad
- Effektiva och tydliga verksamhetsprocesser

3. Process för inventering av personuppgifter

Inventeringen utgår ifrån verksamhetsprocesser och varje nämnd/bolag bör därför fundera på vilka personuppgiftsbehandlingar som förekommer i samband med respektive process, samt i vilka behandlingssystem som personuppgifterna kan förekomma i. Med behandlingssystem avses bärare av information, det kan exempelvis vara IT-system, lokalt sparade filer på digitala enheter (datorer, surfplattor, mobiltelefoner), register/listor, fysiskt material (utskrifter, akter), mail, löpande text på hemsidor, nätverkskomponenter m.m.). Inventeringen avser därmed såväl strukturerad som ostrukturerad data.

Processen för hur en inventering av data ska ske beskrivs nedan (se även sid 9 i bilaga 1 Presentation - Inventeringsprocess).

Steg 1 – Utse en huvudansvarig person som har det yttersta ansvaret för att tillse att kartläggningen blir genomförd. Detta kan exempelvis vara VD/vice VD eller en förvaltningschef. Därefter utses en samordnare för kartläggningsprojektet. Det bör vara en person som har tillräckligt god kännedom om de verksamhetsprocesser som finns inom nämnden/bolaget och som har erforderlig kompetens för att kunna justera bilaga 2 Mall för inventering utifrån de särskilda krav som den egna verksamheten har.

Steg 2 – Samordnande person ansvarar för att bilaga 2 Mall för inventering justeras utifrån den specifika verksamheten innan denna skickas ut för ifyllnad. Samordnaren ska kategorisera valen i rullgardinsmenyer där det behövs. Tänk utifrån verksamhetsprocesser.

I den bifogade mallen ska kolumn ”B-Z” fyllas i. Under fliken ”1.Basinformation” finns en allmän beskrivning för hur mallen ska fyllas i samt en beskrivning av innehållet i samtliga flikar.

Genom att ha förvalda kategorier underlättar det för den som ska fylla i mallen. Det underlättar även för den samordnare som sedan ska sammanställa det insamlade materialet. Rekommendationen är att ha så få fritextfält som möjligt för att minimera överflödig information.

Steg 3 – Utse personer som har bra kunskap om vilken information som hanteras i de olika behandlingssystemen och som kan fylla i mallen. Det kan vara ansvarig systemägare, systemförvaltare eller någon annan informationsägare. Det viktiga är att den/de personer som fyller i mallen har god kännedom om vilka personuppgiftsbehandlingar som görs i verksamheten.

Steg 4 – Samordnaren sammanställer samtliga insamlade uppgifter och upprättar ett en registerförteckning. I den bifogade mallen framgår det vilken information som är obligatorisk enligt artikel 30. Underlaget bör analyseras i syfte att identifiera områden som eventuellt behöver åtgärdas, exempelvis om laglig grund för en viss personuppgiftsbehandling saknas. Sådana personuppgifter bör i sådant fall gallras bort.

Steg 5 – Samordnaren måste även kartlägga vilka externa leverantörer som nämnden/bolaget anlitat för utförande av

olika tjänster. Eftersom leverantörer hanterar personuppgifter för nämnden/bolagets räkning är det av stor vikt att parterna reglerat behandlingen av personuppgifter i ett s.k. personuppgiftsbiträdesavtal. Det är alltid nämnden/bolaget som har det yttersta ansvaret för behandlingen av personuppgifter.

I bilaga 2 Mall för inventering kolumn ”Y” fylls i om personuppgiftsbiträdesavtal finns mellan parterna. Om ett sådant personuppgiftsbiträdesavtal saknas bör ett avtal upprättas så snart som möjligt. Även befintliga avtal behöver sannolikt uppdateras för att möta dataskyddsförordningens krav. Till vägledningen finns en mall för personuppgiftsbiträdesavtal bifogat, se bilaga 3 – Mall för personuppgiftsbiträdesavtal. Mallen är generisk och behöver anpassas till den specifika avtalssituationen.

Steg 6 – Huvudansvarig ska återkoppla till informationssäkerhetsansvarig på Stadsledningskontoret när en registerförteckning har upprättats. Observera att det inte är registerförteckningen som ska översändas, utan endast ett meddelande om att kartläggningen är genomförd och att en fullständig registerförteckning har upprättats. Syftet är att informationssäkerhetsansvarig på övergripande nivå ska ha möjlighet att följa stadens arbete med anpassningen till dataskyddsförordningen.

3.1 Centrala verksamhetssystem

Vad gäller stadens centrala och gemensamma verksamhetssystem finns i staden ett centralt ägandeskap, främst inom stadsledningskontoret och utbildningsförvaltningen.

Som tidigare nämnts i detta dokument ansvarar varje nämnd/bolag för de personuppgifter som nämnden/bolaget behandlar i sin verksamhet. Samtliga nämnder/bolag äger och ansvarar därmed för den information som behandlas i de olika verksamhetssystemen oavsett om det gäller ett centralt/gemensamt eller lokalt system.

För att underlätta kartläggningen har inventeringen delats upp på centrala/gemensamma verksamhetssystem samt lokala verksamhetssystem. Denna inventering fokuserar på lokala verksamhetssystem och därför behöver inte de

centrala/gemensamma verksamhetssystemen inventeras i detta skede, utan det görs centralt av ansvariga personer på stadsledningskontoret, utbildningsförvaltningen m.fl. I vissa fall kan dock kartläggningen av de centrala/gemensamma verksamhetssystemen behöva kompletteras med viss information. I sådant fall kommer respektive ansvarig person att ta kontakt med lämpliga personer i verksamheterna.

Med lokala verksamhetssystem avses system som används av en förvaltning/bolag och där driften sker i huvudsak av HCL inom ramen för avtalet för gemensam it-service (GSIT). Det kan emellertid även finnas lokala verksamhetssystem som inte driftas av HCL, så är exempelvis fallet vid användning av molntjänster. Även sådana verksamhetssystem ska omfattas av inventeringen.

Centrala system används i princip av alla verksamheter på staden och drift och förvaltning sker främst av Tieto inom ramen för SIKT-avtalet.

Frågor gällande den nya dataskyddsförordningen eller rörande ifyllandet av mallen skickas till: Funktion.GDPR.SLK@stockholm.se.

4. Definitioner

Nedan har ett antal centrala begrepp definierats.

4.1 Personuppgiftsansvarig

Definitionen av personuppgiftsansvarig är densamma som i PuL, dock har ansvaret för den personuppgiftsansvarige utökats i den nya förordningen. Personuppgiftsansvarig är ytterst ansvarig för att verksamheten behandlar personuppgifter på ett korrekt sätt och kan bli skadeståndsskyldig om överträdelse av dataskyddsförordningen sker. Höga sanktionsavgifter kan drabba den personuppgiftsansvarige som inte uppfyller kraven.

Inom Stockholms stad är varje nämnd/bolag personuppgiftsansvarig för de personuppgifter som

nämnden/bolaget behandlar i sin verksamhet, exempelvis är Kommunstyrelsen personuppgiftsansvarig för de uppgifter som Stadsledningskontoret behandlar och Fastighetsnämnden för de personuppgifter som Fastighetskontoret behandlar.

Detta innebär därmed att varje nämnd/bolag ansvarar för att hantering av personuppgifter sker i enlighet med dataskyddsförordningen.

4.2 Personuppgift

Med personuppgift avses all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet, dvs. kunder, medborgare, anställda m.fl. Definitionen är mycket bred och omfattar förutom exempelvis namn och personnummer även information som indirekt rör en person (exempelvis ett registreringsnummer för en bil eller målnummer för en dom) eller som kräver extra information för att kunna hänföras till en person.

Kan personen identifieras genom hänvisning till exempelvis ett identifikationsnummer, lokaliseringsuppgift eller till en eller flera faktorer som är specifika för hans eller hennes fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet är det således att betraktas som en personuppgift. Även bilder (foton) och ljudupptagningar på individer som behandlas i dator kan vara personuppgifter även om inga namn nämns.

Den personuppgiftsansvarige behöver inte själv förfoga över samtliga uppgifter som gör identifieringen möjlig. Det innebär att även krypterade uppgifter och olika slags elektroniska identiteter, som exempelvis olika nätidentifierare som lämnas av deras utrustning, exempelvis IP-adresser, cookies eller andra identifierare som radiofrekvensetiketter, räknas som personuppgifter om de kan göras läsbara och därmed identifiera fysiska personer. Sådana identifierare kan efterlämna spår som, särskilt i kombination med unika identifierare och andra uppgifter som tas emot av servrarna, kan användas för att skapa profiler för fysiska personer och identifiera dem.

Skyddet omfattar endast fysiska personer som är i livet. Juridiska personer, avlidna och ofödda omfattas inte.

4.3 Känsliga uppgifter

Dataskyddsförordningen ställer särskilda krav på behandling av personuppgifter som är av känslig karaktär. Därför är det viktigt att utreda om känsliga uppgifter behandlas i verksamheten.

Behandling av personuppgifter som avslöjar en känslig personuppgift ska som huvudregel vara förbjuden. Behandling av känsliga uppgifter kan vara tillåtet om något av de undantag som anges i artikel 9 (2) i dataskyddsförordningen är uppfyllda.

Nedan följer några exempel på vad som kan utgöra en känslig personuppgift.

- Etnicitet
- Politisk åsikt
- Sexuell läggning
- Religiös eller politisk övertygelse
- Hälso- och genetisk data
- Medlemskap i fackförening

4.4 Personuppgiftsbehandling

Med behandling avses varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat.

5. Missbruksregeln

Genom den s.k. missbruksregeln i 5 a § PuL undantas behandling av personuppgifter i s.k. ostrukturerat material från ett flertal av lagens hanteringsregler. De krav som ställs i den nya dataskyddsförordningen gäller emellertid även för ostrukturerad data, t.ex. löpande text i ordbehandlingsprogram, i e-post eller på internet samt ljud- och bildupptagningar. När missbruksregeln försvinner innebär det att samma regler som gäller för personuppgifter i databaser och ärendehanteringssystem, också ska användas för det som skrivs om personer i exempelvis e-post och på

webbplatser. Det kommer alltså inte att göras någon skillnad mellan ostrukturerat och strukturerat material. Det innebär att kraven avseende bland annat rättslig grund, information till de registrerade, skyldigheten att föra register m.m. gäller alla personuppgiftsbehandlingar oavsett form eller struktur.

För att det ska vara möjligt att uppfylla de krav som dataskyddsförordningen ställer krävs att samtliga nämnder/bolag har kontroll över sina verksamhetsprocesser samt har god kännedom om vilka personuppgifter som behandlas i verksamheterna och vart de finns lagrade.

6. Allmänna principer för behandling av personuppgifter

För att en verksamhet ska få behandla personuppgifter krävs enligt artikel 5 i dataskyddsförordningen att uppgifterna:

- behandlas på ett lagligt, korrekt och öppet sätt
- samlas in för ett uttryckligt angivet och berättigat ändamål och behandlas i enlighet med detta angivna ändamål
- är adekvata, relevanta och inte för omfattande i förhållande till ändamålen
- är korrekta och uppdaterade
- inte lagras längre än nödvändigt
- behandlas på ett sätt som säkerställer lämplig säkerhet

Den personuppgiftsansvarige ska ansvara för och kunna visa att ovan nämnda principerna efterlevs. Det är därför särskilt viktigt att register över samtliga personuppgiftsbehandlingar förs, och att data som inte är nödvändig, gammal och inaktuell identifieras och raderas. En grundläggande tanke med dataskyddsförordningen är uppgiftsminimering, dvs. att inte samla in fler uppgifter än nödvändigt.

7. Laglig behandling av personuppgifter

Varje behandling av personuppgifter måste vila på en rättslig grund enligt artikel 6 (1). I personuppgiftslagen framgår detta av 10 § PuL. De rättsliga grunder som idag anges i PuL återfinns även i dataskyddsförordningen. Den stora skillnaden är att dataskyddsförordningen har tagit bort möjligheten för myndigheter att använda intresseavvägning som en rättslig grund. Detta innebär att myndigheter inte längre kan göra en avvägning mellan den ansvariges berättigade intressen och den registrerades rättigheter och intressen vid behandlingen av personuppgifter. Detta torde gälla även kommunala bolag.

För att en behandling av personuppgifter ska vara laglig krävs enligt artikel 6 att något av följande villkor är uppfyllda:

- Den registrerade har lämnat sitt **samtycke**
- Behandlingen är nödvändig för att fullgöra ett **avtal** där den registrerade är part
- Behandlingen är nödvändig för att fullgöra **en rättslig förpliktelse**
- Behandlingen är nödvändig för att **skydda intressen** som är av grundläggande betydelse för den registrerade eller för en annan fysisk person
- Behandlingen är nödvändig för att utföra en uppgift **av allmänt intresse eller myndighetsutövning**
- Intresseavvägning. Observera att myndigheter inte längre har möjlighet att använda sig av denna lagliga grund. Detta torde gälla även kommunala bolag.

Observera att även om en behandling är laglig enligt denna artikel så måste personuppgiftsansvarige även uppfylla kraven i andra bestämmelser i förordningen, exempelvis de allmänna principerna som angetts ovan.

Sammanfattningsvis kan nämnas att minst en av de rättsliga grunder som anges i artikel 6 (1) måste vara tillämplig och samtliga principer som anges i artikel 5 måste följas!