Personuppgiftslagstiftningen förstärks och ersätts med nya regler från och med 25 maj 2018

Inledning

25 maj 2018 kommer lagstiftningen gällande personuppgifter att ändras. För att säkerställa att staden lever upp till de krav som ställs i den nya lagen är det viktigt att alla stadens verksamheter redan nu ser över sin hantering av personuppgifter. I och med den nya lagstiftningen kommer också kraven på leverantörer av moln- och outsourcingtjänster att öka. Sanktionerna för brott mot den nya lagstiftningen blir strängare och kan innebära högre böter.

Den nya Dataskyddsförordningen har kortfattat ett utökat krav på öppenhet, ett ökat fokus på integritetsskydd och innebär en förstärkning av den registrerades rättigheter. Samtidigt ges den personuppgiftsansvariga ett förtydligat och utökat ansvar och skyldigheter. Det innebär bland annat en större skyldighet i att kunna visa att förordningen följs, något som kan ställa krav på ökad dokumentation. Därför är det viktigt att stadens verksamheter som personuppgiftsansvariga har tydliga interna riktlinjer och styrning i hanteringen av personuppgifter. Även Datainspektionen kommer ha ett större ansvar att bland annat granska Dataskyddsförordningens efterlevnad, men även att stötta organisationer med riktlinjer och allmänna råd.

Med anledning av dessa förändringar har avdelningen för digital utveckling på stadsledningskontoret tagit fram denna information om hur de nya reglerna skiljer sig från nuvarande lagstiftning samt vad stadens verksamheter bör tänka på redan nu.

Bakgrund till nya lagstiftningen

Komplexiteten, gränser och gråzoner har ökat mellan teknik, juridik och ekonomi och det skydd vi hittills haft gällande hantering av personuppgifter räcker inte längre. Tekniken utvecklas ständigt och det blir allt mer vanligt med exempelvis molntjänster och sociala medier innehållande olika former av personuppgifter. Tillslut krävs en modernisering av lagstiftningen för att vara aktuell och tillämpbar i största möjliga mån. Det är även av intresse att ha en så enhetlig lagstiftning som möjligt inom EU:s medlemsstater.

Den nya lagen ”General Data Protection Regulation” (GDPR), på svenska ”Allmän dataskyddsförordning” (nedan ”Dataskyddsförordningen”) kommer att ersätta den nuvarande

personuppgiftslagen (nedan PUL) och ska implementeras och börja tillämpas i samtliga medlemsstater från och med den 25:e maj 2018. Dock behöver Dataskyddsförordningen kompletteras med vissa nationella regler och medlemsstaterna har också möjlighet att behålla eller införa egna krav eller undantag i vissa frågor.

Förberedelser inför 2018

Denna genomgång utgår framförallt från Datainspektionens vägledning till personsuppgiftsansvariga gällande föreberdelser inför EU:s nya dataskyddsförordning. Ytterligare nyheter och en mer kortfattad informationslista återfinns i slutet av dokumentet.

Generella principer gällande integritetsskydd är att:

- Inte samla in mer information än vad som kan anses nödvändigt
- Inte spara informationen längre än vad som behövs
- Inte använda informationen till annat än ändamålet med insamlingen

Det är i första hand viktigt att försäkra sig om att stadens beslutsfattare och övriga som hanterar personuppgifter, **har kunskap om det nya regelverket** och förståelse för hur dessa kan påverka den egna verksamheten. Det är vidare viktigt att stadens verksamheter har en effektiv policy för dataskydd samt tydliga rutiner för hantering av personuppgifter.

Stadens alla verksamheter bör göra en **inventering och dokumentera** vilka personuppgifter som hanteras, hur insamlingen av dessa görs samt till vem uppgifter lämnas. Det är även viktigt att ha en strukturerad dokumentation för detta. I de fall fel upptäcks är det viktigt att dessa rättas. Staden ska även kunna svara på eventuella frågor från Datainspektionen, varför det är viktigt att ha all dokumentation uppdaterad och tillgänglig.

Staden kommer vidare att behöva **visa på vilken rättslig grund** personuppgifterna behandlas, något som verksamheten ska informera om redan vid insamlingen av personuppgifterna. De rättsliga grunderna som i dag finns i PUL kommer vara oförändrade, varför staden redan nu kan börja kartlägga och dokumentera vilka behandlingar som utförs, för att på så sätt kunna visa att förordningens krav uppfylls. Det kommer vidare att finnas större möjlighet för den registrerade att motsätta sig en behandling som sker med stöd av en intresseavvägning. Observera att

formuleringen indikerar att myndigheter inte kommer kunna stödja sin behandling på enbart en intresseavvägning.

Tillsyn och utökade rättigheter

Tillsynsmyndigheten, i Sverige Datainspektionen, kommer att ges ett större ansvar med ökade befogenheter och skyldigheter med krav på att agera och sammarbeta. De kommer få mandat att granska efterlevnad, besluta om eventuella sanktioner samt samordna mellan medlemsstater. De ska även ta fram standardpolicyer som ger företag möjlighet att bli certifierade. De ska som tidigare även stötta organisationer med att utarbeta riktlinjer och allmänna råd inkluderat detaljerade tekniska och organisatoriska åtgärder som är nödvändiga för att skydda personuppgifter.

Den **registrerade individens rättigheter utökas** i och med förordningens införande och ett utökat krav ställs på vilken information som ska lämnas ut till den registrerade. Liksom i dagens lagstiftning har den personuppgiftsansvariga en skyldighet att på den registrerades begäran lämna ut information om vilka uppgifter om denne som behandlas. Enligt förordningen kommer även följande information att behöva lämnas ut; den rättsliga grunden för behandlingen, hur länge personuppgifterna lagras, rätten att få felaktiga uppgifter rättade samt möjligheten att lämna klagomål till tillsynsmyndigheten. Informationen i fråga ska vara kortfattad, lättförståelig och ett tydligt språk ska användas. Begäran ska kunna göras elektroniskt och informationen ska även kunna lämnas ut elektroniskt i ett allmänt använt format. Under ”Kortfattad lista” nedan, återfinns de enligt Datainspektionen viktigaste uppgifterna för den registrerade.

En inte ny, men i förordningen förtydligad, formulering för den registrerade gäller gallring och **rätten att bli ”bortglömd”**. Den registrerade har rätt att när som helst begära att få sina uppgifter raderade, *om* det inte längre föreligger en rättslig grund för behandlingen av personuppgifterna. Man vill på så sätt ge den registrerade ytterligare kontroll över vilka uppgifter om denne som behandlas samt att denne ska kunna invända mot sådan behandling. Det finns dock undantag, såsom exempelvis när personuppgifter behövs för bokföringsändamål, för att utöva rätten till yttrande- och informationsfrihet, som ett led i myndighetsutövning, vid allmänt intresse på folkhälsoområdet, för arkivändamål, statistiska ändamål och vid rättsliga anspråk. Men personuppgifterna får då endast användas för ändamålet i fråga.

Frågan om **samtycke** behandlas redan i dagens PUL och innebörden av ett ”giltigt samtycke” kommer vara densamma i Dataskyddsförordningen. Det ska vara fråga om frivillig, specifik och otvetydig viljeyttring, där den registrerade ska få tydlig information samt därefter välja att godta behandlingen eller inte. Datainspektionen ger exempel på att en i förväg ikryssad ruta på en webbplats inte är godtagbart, vilket inte heller ett tyst samtycke är. Det är därför viktigt, om verksamheten stödjer sin insamling på samtycke, att kraven i Dataskyddsförordningen är uppfyllda samt att man i efterhand ska kunna visa att sådant giltigt samtycke har lämnats.

Ett, för många av stadens verksamheter, intressant fråga rör den om **barns personuppgifter**. Vad gäller behandling av barns personuppgifter, en person under 16 år enligt Dataskyddsförordningen, krävs samtycke från vårdnadshavaren. Detta är inte något nytt, men skyddet har förstärkts i Dataskyddsförordningen, särskilt avseende kommersiella internettjänster som till exempel sociala nätverk. Medlemsstaterna kan välja en lägre åldersgräns, dock lägst 13 år. Liksom vid samtycke, krävs även här att ett giltigt samtycke från vårdnadshavaren kan visas upp i efterhand.

En (eventuellt) betydande förändring är att PUL:s nuvarande undantagsregel, den så kallade **missbruksregeln** (5a § PUL), för behandling av personuppgifter i ostrukturerat material, **inte längre kommer att finnas kvar** i det nya regelverket. Sådan behandling kan exempelvis vara personuppgifter i löpande text på internet, under förutsättning att den inte utgör en kränkning av den personliga integriteten. Därför bör varje verksamhet som behandlar personuppgifter göra en undersökning för att se om denna undantagsregel används, och i sådant fall finna nytt lagstöd för sådan användning genom att se huruvida verksamhetens nuvarande användning är förenlig med förordningens bestämmelser.

Nytt i Dataskyddsförordningen är rätten till **dataportabilitet**, vilket innebär att det ska bli lättare för den registrerade att få sina uppgifter flyttade från en verksamhet till en annan (exempelvis om man vill byta socialt nätverk). I den mån det är aktuellt i stadens verksamheter, är det viktigt att säkerhetsställa att en sådan flytt kan ske och att en sådan begäran verkligen kommer från den registrerade själv.

Tekniska aspekter och förändringar

Dataskyddsförordningen ställer särskilda krav på verksamheter som vill behandla personuppgifter som medför **stora integritetsrisker**. Behandling av personuppgifter som är förenliga med särskilda risker för enskildas fri- och rättigheter kräver att en konsekvensbedömning och noggrann analys görs, det vill säga en form av hotbilds-, sårbarhets- och riskanalys. Det kan exempelvis röra särskilt stora register med känsliga personuppgifter, profilering eller omfattande kameraövervakning på allmän plats. Visar analysen att risken är hög, måste verksamheten först samråda med tillsynsmyndigheten samt utse ett **dataskyddsombud** som ska ha stor kunskap om området. Stadsledningskontoret kommer under våren 2017 att utreda om staden bör ha ett centralt dataskyddsombud eller om det ska finnas ett för respektive förvaltning och bolag.

Stadens verksamheter måste se till att det finns **tillräckliga rutiner** för det fall en **personuppgiftsincident** sker, det vill säga om verksamheten blir utsatt för exempelvis dataintrång eller på annat sätt förlorar kontrollen över personuppgifterna som behandlas. Det måste bland annat finnas tillräckliga rutiner på plats för att kunna upptäcka, rapportera och utreda personuppgiftsincidenter, liksom att veta hur och när anmälan till tillsynsmyndigheten ska göras samt vem som bär ansvaret för att anmälan de facto görs. Alla sådana händelser måste dokumenteras och är det inte osannolikt att det kan medföra en risk för enskildas fri- och rättigheter, måste en **anmälan till tillsynsmyndigheten** göras inom loppet av 72 timmar (från det att incidenten har upptäckts i den normala rutinen). De **registrerade måste också underrättas** om ett sådant intrång, i de fall då det finns allvarliga risker för exempelvis id-stöld, diskriminering, bedrägeri med mer, så att denne själv också kan vida nödvändiga åtgärder. Redan idag finns krav på att rapportera in it-incidenter till Myndigheten för säkerhet och beredskap (MSB) och samma rutiner bör gå att återanvända som bas även för detta ändamål. Datainspektionen kommer att komma med riktlinjer om hur detta ska gå till.

Något som uttryckligen regleras i Dataskyddsförordningen är ”**Privacy by design**”, vilket innebär att det finns ett **inbyggt dataskydd** i systemet/en. Detta blir särskilt viktigt för leverantörer till staden att säkerställa och kunna argumentera för när de tar fram nya lösningar. Datainspektionen tar upp åtgärder som *pseudonymisering* (att uppgifterna som behandlas inte kan kopplas till enskild utan ytterligare information/nyckel som förvaras

avskild) eller *dataminimering* (endast behandla de uppgifter som är nödvändiga vid varje enskilt ändamål). Båda dessa begrepp behandlas i förordningen.

Sanktioner

Dataskyddsförordningen har nya **sanktioner** vilka beror av i vilken grad förordningen inte efterlevts. Vid mindre förseelse kan ett påpekande ges eller ett föreläggande om eventuella brister framhållas. Är det fråga om ett allvarligare avsteg mot förordningen, eller ovilja från verksamhetens sida att vidta nödvändiga åtgärder, kan det bli fråga om så kallade **administrativa böter** på upp till fyra procent av organisationens omsättning eller 20 miljoner Euro. För stadens vidkommande är det än så länge inte klart om omsättningen avser staden som en helhet eller respektive förvaltning och bolag. Det troliga är dock att det alltid avser organisationer som helhet för att undvika att koncerner lägger ansvaret för dessa frågor i ett bolag med lite resurser och omsättning. Observera också att det ännu inte är klart om de administrativa sanktionsavgifterna kommer att omfatta myndigheter eller inte.

Även en enskild individ som har drabbats av integritetsbrott, kan ha rätt till ersättning för skada denne lidit på grund av att dataskyddsförordningen inte följts. Dock har tillsynsmyndigheten rätt att utfärda böter oavsett om någon de facto lidit skada eller inte.

Ytterligare information

Datainspektionen har på följande sida samlat ihop bra information och checklistor gällande dataskyddsförordningen, som kan vara lämpliga att läsa igenom.

http://www.datainspektionen.se/fragor-och-svar/eus-dataskyddsreform/

Kortfattad lista över vad som bör göras nu

Utgångspunkt – vad bör staden göra/se över

- Försäkra sig om att verksamhetens nyckelpersoner är **medvetna** och har **nödvändig kunskap** om det nya regelverket.
- Planera för att utse **dataskyddsombud**, antingen internt eller genom tjänsteavtal
- Se över **vilka personuppgifter** som behandlas.
- **Inventera och dokumentera** nuvarande rutiner och policy gällande hantering av personuppgifter.
- **Anpassa** rutiner och **it-system** för att få korrelation med förordningen.
- Se över rutiner för hur ni **informerar** om behandlingen.
- Se över huruvida de **registrerades rättigheter** tillvaratas.
- Dokumentera på vilken **laglig grund** redan insamlade personuppgifter och kommande insamling av personuppgifter behandlas.
- Undersöka om undantagsregeln, den så kallade **missbruksregeln**, som inte kommer finnas kvar i förordningen, används och i sådant fall utreda om en ny rättslig grund för sådan behandling finns.
- Säkerhetsställa att **dataportabilitet** finns, det vill säga att flytt av personuppgifter från den egna verksamheten/ organisationen till annan kan ske.
- Säkerhetsställa att **begäran** om dataportabilitet verkligen kommer från den registrerade själv.
- Se över hur **samtycke** erhålls och uppdatera eventuella blanketter och rutiner.
- Ska ett **barns** (person under 16 år) personuppgifter behandlas, krävs samtycke från vårdnadshavaren.
- Särskilda krav ställs på behandling av personuppgifter som är förenliga med **särskilda risker för enskildas fri- och rättigheter** och kräver en föregående konsekvensbedömning och analys. Är risken hög, krävs först **samråd** med tillsynsmyndigheten
- Vissa kan som sagt behöva utse ett dataskyddsombud, men oavsett kan det vara bra att på verksamheten ha en person med ett **övergripande ansvar**.
- Se till att det finns tillräckliga rutiner för ev. **personuppgiftsincident**, som att kunna upptäcka, rapportera och utreda personuppgiftsincidenter, liksom

att veta hur och när anmälan till tillsynsmyndigheten görs samt av vem.
- **Anmälan till tillsynsmyndigheten** ska göras inom 72 timmar från det att incidenten har upptäckts i den normala rutinen. Det väntas mer utförliga instruktioner från Datainspektionen hur detta ska ske.
- Vid personuppgiftsincident som kan medföra **allvarliga risker** för exempelvis diskriminering, id-stöd, bedrägeri m.m. måste den registrerade meddela om det.
- ”**Privacy by design**”, regleras uttryckligen och innebär att det finns ett inbyggt dataskydd i systemet/en. Åtgärder som kan finnas är *pseudonymisering* eller *dataminimering*. Här måste även stadens personuppgiftsbiträden (HCL, Tieto med flera) beskriva hur de hanterar detta.
- Principerna om **inbyggt dataskydd** och dataskydd som standard bör också beaktas vid offentliga upphandlingar.
- Alla stadens verksamheter som behandlar personuppgifter är ansvariga att **vida tekniska och organisatoriska åtgärder**. Därför är det att föredra att ha ett it-system som kan ”hjälp till att göra jobbet” till exempel genom att det lätt ska gå att få fram rapporter ur systemet och liknande.
- Samtliga verksamheter som behandlar personuppgifter måste **svara inför *en* tillsynsmyndighet** och vilken som blir aktuell beror på var verksamheten har sin centrala förvaltning eller var beslut om personuppgiftsbehandlingen fattas.
- **Bredrivs verksamhet i flera olika EU-länder** med spridda ansvarsområden, kan olika behandlingar falla in under olika tillsynsmyndigheters behörighet, varför det är viktigt att ständigt kartlägga sådan information och beslutsrutiner i sin verksamhet.

Nyheter i Dataskyddsförordningen (ej uttömande)

- PUL är subsidiär, medan **Dataskyddsförordningen** kommer vara överordnad andra lagar, något som innebär att exempelvis befintliga registerlagar kommer behöva anpassas till förordningen.
- En del **nya begrepp** finns med i Dataskyddsförordningen, exempelvis: mottagare, profilering, personuppgiftsbrott, dataskyddsombud, pseudonymisering.
- Den **registrerade** individens rättigheter utökas.

- Ett inrättande av europeiska **dataskyddsstyrelsen**, som kommer ersätta art. 29-gruppen.
- Utökat krav på vilken **information** som ska lämnas ut till den registrerade, som:
    - Den rättsliga grunden för behandlingen
    - Hur länge personuppgifterna lagras
    - Att man har rätt att få felaktiga uppgifter rättade
    - Möjligheten att lämna klagomål til Datainspektionen.
- De viktigaste **uppgifterna för den registrerade** är enligt Datainspektionen:
    - Att få tillgång till sina personuppgifter
    - Att få felaktiga personuppgifter rättade
    - Att få sina personuppgifter raderade
    - Att kunna invända mot att personuppgifterna används för direktmarknadsföring
    - Att kunna invända mot att personuppgifterna används för automatiserat beslutsfattande och profilering
    - Att ha rätt att få sina personuppgifter flyttade (dataportabilitet).
- Vilken **rättslig grund** man behandlar personuppgifterna på, kommer behöva informeras om redan vid insamlingen av personuppgifterna.
- Förstärkt skydd för behandling av **barns** (person under 16 år) personuppgifter.
- Man har en **rätt att bli ”bortglömd”**, det vill säga rätt att få sina personuppgifter raderade när de inte längre behövs för ändamålet.
- Den nuvarande undantagsregeln, den så kallade **missbruksregeln**, kommer inte finnas kvar i dataskyddsförordningen.
- Det kommer finnas större möjlighet för den registrerade att motsätta sig en behandling som sker med stöd av en **intresseavvägning**.
- En **myndighet** kommer troligen inte kunna stödja sin behandling endast på en intresseavvägning.
- Rätten till **dataportabilitet** har införts, vilket ska göra det lättare för den registrerade att få sina personuppgifter flyttade från en verksamhet/organisation/leverantör till en annan (t.ex. om man vill byta socialt nätverk).

- Förordningen innehåller en del nya regler gällande vad verksamheten måste göra för det fall den blir utsatt för **dataintrång** eller på annat sätt förlorar kontrollen över de behandlade personuppgifterna.
- Ökade säkerhetskrav och en uttrycklig reglering gällande ”**Privacy by design**”.
- Kraven kommer öka på organisationer och leverantörer av **moln- och outsourcingtjänster** som behandlar personuppgifter.
- Krav för verksamheter/organisationer att göra en **konsekvensbedömning**, det vill säga en hotbilds-, sårbarhets- och riskanalys.
- **Tillsynsmyndigheten**, i Sverige Datainspektionen, får ett större ansvar med ökade befogenheter och skyldigheter samt mandat att granska efterlevnad, besluta om eventuella sanktioner samt att samordna mellan medlemsstater.
- En skyldighet att **anmäla och informera** tillsynsmyndigheten om personuppgiftsbrott skett.
- Obligatoriskt att ha **uppgiftsskyddsombud** för myndigheter eller andra verksamheter/organisationer som behandlar känsliga uppgifter eller bedriver övervakning på allmän plats med mer.
- Nya **sanktioner** har införts och en rimlighetsbedömning måste göras från fall till fall och hänsyn tas till hur allvarlig förseelsen är, hur villig man är att vidta nödvändiga åtgärder och förebygga brister. Vid allvarligare avsteg mot förordningen kan det bli fråga om så kallade *administrativa böter*, med en glidande skala, med böter upp till fyra procent av en organisations/företags globala omsättning eller upp till 20 miljoner euro.
- En **enskild individ som drabbats** av integritetsbrott, kan ha rätt till ersättning för skada. Tillsynsmyndigheten har dock rätt att utfärda böter, oavsett om någon lidit skada eller inte.
- **Överföring till tredje land** regleras i förordningen och EU-kommissonen har fattat beslut om adekvat skyddsnivå, lämpliga skyddsåtgärder och bindande företagsbestämmelser (med undantag i särskilt uppräknade fall).
- Verksamheter/organisationer har en skyldighet att ha en **företrädare i EU** för individer att vända sig till.