GDPR och upphandling

Inledning

Den 25:e maj 2018 börjar Europaparlamentets och Rådets förordning (EU) 2016/679) att gälla i Sverige och hela EU. I Sverige ersätter den personuppgiftslagen (1998:204), PUL. Förordningen kallas ibland för GDPR, en förkortning för General Data Protection Regulation. GDPR är direkt tillämplig och dess bestämmelser är tvingande. GDPR innehåller en hel del nyheter jämfört med PUL. I den här skriften redogörs översiktligt för GDPR:s betydelse vid offentliga upphandlingar. För fler nyheter och mer utförlig information om de centrala delarna i GDPR hänvisas till SKL:s PM om nya dataskyddsförordningen, som finns på SKL:s webbplats.

Missbruksregeln upphör

En viktig nyhet i GDPR jämfört med PUL är att den s.k. missbruksregeln försvinner. Missbruksregeln, som alltså gäller fram till och med den 24 maj 2018, innebär att enklare regler gäller för personuppgifter i ostrukturerat material. Enligt PUL är det exempelvis tillåtet att behandla personuppgifter i e-post, på internet eller i enkla listor som man sparar på datorn om behandlingen inte innebär en kränkning av den registrerades integritet. När missbruksregeln försvinner kommer det bl.a. att krävas en rättslig grund för personuppgiftsbehandling även när det gäller personuppgifter i e-post, på internet och i enkla listor, och detta gäller även i upphandlingssituationer. Det är därför bra att kontrollera att det finns tydliga rutiner och instruktioner i organisationen om vad som gäller för den personuppgiftsbehandling som tidigare utfördes med stöd av missbruksregeln, och att dessa instruktioner överensstämmer med GDPR.

Sveriges Kommuner och Landsting

Konsekvensbedömning

Om en behandling av personuppgifter sannolikt leder till hög risk för de registrerades fri- och rättigheter måste den som är ansvarig för personuppgiftsbehandlingen (den personuppgiftsansvarige) alltid göra en konsekvensbedömning (artikel 35 i GDPR). Den som underlåter att göra en konsekvensbedömning riskerar att drabbas av en sanktionsavgift. Det är alltså nödvändigt att göra en konsekvensbedömning om en upphandlande myndighet anser att ett köp av exempelvis en tjänst eller en IT-produkt kan medföra hög risk för registrerades fri och rättigheter. Det finns ingenting som hindrar att en konsekvensbedömning görs även om behandlingen inte leder till en hög risk för de registrerades fri- och rättigheter.

Personuppgiftsbiträdesavtal

Det är vanligt att företag eller myndigheter upphandlar leverantörer som exempelvis ska sköta driften av databaser eller utföra arbete som innebär en behandling av personuppgifter som myndigheten har ett personuppgiftsansvar för. En leverantör som behandlar personuppgifter för någon annans räkning är att anse som ett personuppgiftsbiträde. För att en upphandlande myndighet ska få anlita en sådan leverantör krävs att personuppgiftshanteringen regleras genom ett avtal eller en annan rättsakt enligt unionsrätten eller nationell rätt. Det vanliga är att myndigheten tecknar ett avtal med biträdet, ett s.k. personuppgiftsbiträdesavtal. En sådan skyldighet finns redan i PUL men i GDPR ställs mer detaljerade krav på avtalets innehåll. Vad avtalet ska innehålla framgår av artikel 28 punkten 3 i GDPR. De nya reglerna kommer även att omfatta avtal som ingåtts innan den 25 maj 2018. Det är därför viktigt att se över befintliga avtal för att säkerställa att de uppfyller reglerna i GDPR. Det är förstås också viktigt att upphandlande myndigheter redan nu, vid upphandlingar av avtal som löper över ikraftträdandet av GDPR, ställer krav på att vinnande leverantörer som ska agera personuppgiftsbiträden ingår personuppgiftsbiträdesavtal som uppfyller GDPR:s krav.

SKL har tagit fram ett exempel på ett personuppgiftsbiträdesavtal. Exemplet, inklusive en redigerbar mall, finns på SKL:s webbplats under 10 informationsinsatser punkt 6.

För det fall en upphandlande myndighet (exempelvis en nämnd) behandlar personuppgifter åt en annan upphandlande myndighet i samma kommun är det SKL:s tolkning att det inte behövs personuppgiftsbiträdesavtal dem emellan. Däremot krävs instruktioner för behandlingen som uppfyller kraven enligt artikel 28 punkten 3. Instruktionerna ska återges i ett reglemente eller dylikt (t ex ett beslut i kommunfullmäktige). Ett reglemente är nämligen att se som en ”annan rättsakt” enligt nationell rätt som är bindande för personuppgiftsbiträdet med avseende på den personuppgiftsansvarige. Se SKL:s förtydligande angående interna biträdesavtal på SKL:s webbplats.

Inbyggt dataskydd och dataskydd som standard

En annan nyhet som kan få stor betydelse för framförallt IT-upphandlingar är att det uttryckligen framgår av GDPR att den personuppgiftsansvarige, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, ska genomföra lämpliga tekniska och organisatoriska åtgärder så att kraven i förordningen uppfylls och den registrerades rättigheter skyddas (artikel 25 punkten 1). Detta kallas inbyggt dataskydd eller privacy by design. Enligt artikel 25 punkten 2 ska den personuppgiftsansvarige dessutom genomföra lämpliga tekniska och organisatoriska åtgärder för att i standardfallet säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Detta kallas dataskydd som standard eller privacy by default.

På upphandlingsområdet innebär dessa regler att en myndighet som upphandlar exempelvis ett IT-system bör ställa sådana krav i

förfrågningsunderlaget att IT-systemet uppfyller GDPR:s krav vid personuppgiftsbehandling.

Kravställning som rör inbyggt dataskydd och dataskydd som standard
Vilka krav som ska ställas för ett visst IT-system får avgöras i varje enskilt fall, men principerna i artikel 5 (laglighet, korrekthet och öppenhet, ändamålsbegränsning, uppgiftsminimering, korrekthet, lagrings-minimering, integritet och konfidentialitet samt ansvarsskyldighet) och övriga regler i GDPR bör beaktas vid kravställningen.
Datainspektionen har tagit fram en checklista för IT-projekt utifrån begreppet inbyggd integritet på sin webbplats (www.datainspektionen.se). Checklistan kan vara bra att utgå ifrån vid bedömningen av vilka krav som ska ställas.