Checklista - Offentlig upphandling och GDPR

I denna checklista har vi samlat sådant som är viktigt att tänka på vid offentlig upphandling när det gäller integritetsskydd och personuppgifter.

En personuppgiftsansvarig myndighet har en skyldighet att endast anlita leverantörer och samarbetspartners som kan uppfylla kraven enligt dataskyddsförordningen. Integritetsskyddet ska förbli detsamma även när en myndighet genom upphandling uppdrar åt någon annan aktör att utföra uppgifter som inbegriper personuppgiftsbehandling.

- **Red ut rollfördelningen**. Ha koll på vilken part som får vilken roll redan från början. Vem är personuppgiftsansvarig och vilken/vilka aktörer blir biträden? Många upphandlingar innebär att en leverantör (eller leverantörer i flera led) ska behandla personuppgifter för en myndighets räkning. Det innebär att leverantören ofta får ställning som personuppgiftsbiträde, men det måste inte vara så. Förhållandet mellan myndigheten och leverantören måste vara klarlagt redan i förfrågningsunderlaget i upphandlingen.

- **Ha koll på vilka uppgifter som berörs**. Ingår behandling av personuppgifter inom ramen för den tjänst som upphandlas, och i vilket utsträckning i så fall? Vilka slags personuppgifter aktualiseras, dvs. vad ryms inom upphandlingens ”scope”? Hur känsliga är dessa uppgifter? Har ni gjort en riskanalys och klassat informationen? Vilka krav som är rimliga att ställa på en extern leverantör är helt beroende av integritetsriskerna i det aktuella fallet. Kraven och säkerhetsåtgärderna ska stå i proportion till detta.

- **Involvera dataskyddsombudet.** Precis som i alla frågor som rör personuppgifter och integritetsskydd är det i allra högsta grad relevant att involvera den eller de personer som är utsedda till dataskyddsombud i processen inför och under en upphandling som involverar personuppgifter.

- **Gör en riskanalys och ev. en konsekvensbedömning.** Det är mycket möjligt att det behövs en konsekvensbedömning avseende dataskydd vid upphandlingar, eftersom det kan innebära stora integritetsrisker att anlita externa leverantörer, använda molntjänster etc. Om upphandlingen omfattar känsliga personuppgifter är det extra viktigt med en ordentlig risk- och sårbarhetsanalys och eventuellt en regelrätt konsekvensbedömning som dokumenteras.

- **Kommunicera villkoren**. Leverantörer/biträden måste lämna tillräckliga garantier för att de genomför lämpliga tekniska och organisatoriska skyddsåtgärder, heter det i lagstiftningen. Detta innebär att den upphandlande myndigheten måste ställa krav på leverantörerna i detta avseende genom att kommunicera villkoren redan i förfrågningsunderlaget vid en upphandling. Se även följande punkter.

- **Planera för biträdesavtal.** Ett biträdesavtal är ett måste när man anlitar någon utomstående som ska hantera personuppgifter för den egna organisationens räkning. Ett sådant avtal reglerar i slutänden ansvaret mellan parterna och där ingår att det ska finnas instruktioner som tydliggör vad som gäller. Förslagsvis kan myndigheten lägga med ett utkast till biträdesavtal i förfrågningsunderlagen eller begära att ett sådant utkast skickas med från respektive leverantör i anbudet.

Observera att många av de övriga punkterna i denna checklista är sådant som ska framgå av just biträdesavtalet. Det finns uttryckliga krav på vad avtalet ska innehålla. Har man fått till ett bra biträdesavtal har man förmodligen ”automatiskt” täckt in många av kraven i GDPR.

Se även separat information i handboken samt vår checklista och avtalsmall som kan hjälpa till i avtalsskrivningen.

- **Gör rätt från början.** Underskatta inte vikten av att göra en förstudie/noggrant förarbete inför att en upphandlingsförfrågan tas fram. Det kan ställa till problem om ett biträdesavtal exempelvis behöver ändras i efterhand. Har man otur och inte planerar ordentligt kan hela upphandlingen behöva göras om ifall det uppstår behov av att skriva om avtal i efterhand. Det gäller att vara medveten om vilka villkor och möjligheter som LOU ger avseende ändringar i avtal. Upphandlingsmyndigheten har mer information om detta på sin webbplats.

- **Ställ krav på dataskydd som standard och inbyggt dataskydd**. Kravställning som rör dessa GDPR-principer behöver finnas med i förfrågningsunderlaget för att säkerställa att leverantörer möter kraven och det inte uppstår problem senare. Exakt vad kravställningen ska innebära beror förstås på vad det är som ska upphandlas/vilket uppdraget är.

- **Ställ krav på incidenthantering.** Hur ska personuppgiftsincidenter och andra säkerhetsincidenter hanteras av leverantören?

- **Ställ krav gällande överföringar till tredjeland.** Vilka krav behöver ni ställa när det gäller ev. överföringar till tredjeland? Särskilt relevant för molntjänster och liknande, men även serverlagring, supporttjänster med mera. Om t.ex. lagring eller support sker i ett land utanför EU, så ska leverantören ha en laglig grund för en sådan tredjelandsöverföring. Detta gäller också i flera led. Kan leverantören redovisa för sina underleverantörer och visa att de säkerställer godkänd hantering? Det finns en hel del problem och svårigheter vad gäller just tredjelandsöverföringar och t.ex. molntjänster. Detta har diskuterats flitigt inom bland annat SKL, men tyvärr finns inga glasklara riktlinjer eftersom rättsläget just nu är osäkert.

- **Ska det krävas certifiering/standard?** Ska det ställas krav på att leverantören följer någon etablerad standard eller har en certifiering av något slag?

- **Tänk på informationsplikten gentemot de registrerade**. Som personuppgiftsansvarig bär man ansvaret för att informera alla registrerade personer, t.ex. medborgare, om hur deras personuppgifter behandlas. Detta inkluderar information och transparens kring exempelvis lagring hos externa leverantörer som behandlar personuppgifter.

Tips! MSB har tagit fram en mer utförlig vägledning som rör upphandling och informationssäkerhet – som täcker in betydligt mer än bara GDPR/personuppgiftshantering, men som tangerar samma områden. Ladda ner eller beställ MSB:s vägledning här.