EUROPARÄTTSLIG TIDSKRIFT

Särtryck ur ERT 2018 2

LOU och GDPR – Kravställning om dataskydd i IT-upphandlingar

Av Pernilla Norman

LOU OCH GDPR – KRAV-STÄLLNING OM DATASKYDD I IT-UPPHANDLINGAR

Pernilla Norman*

1. INLEDNING

1.1 Rättsområdens samspel

Offentlig upphandling har historiskt betraktats ur något som kan beskrivas som ett stuprörsperspektiv, dvs. upphandlingsrätten har haft en tendens att hanteras självständigt utan att sättas i perspektiv och relation med andra rättsområden. Ett av de mest tydliga exempel på detta är överprövningsprocesser där domstolarna endast hanterar den överprövade upphandlingen ur ett upphandlingsrättsligt perspektiv, oberoende av huruvida andra rättsområden skulle kunna inverka på den totala bedömningen av överprövade upphandlingen.[1]

Offentlig upphandling är emellertid ett område där ett stort antal rättsområden behöver fungera i samverkan. Tydliga exempel på detta är avtalsrätten som har stor betydelse för de avtal som offentliga upphandlingar leder fram till. Konkurrensrättens tillämplighet på offentliga upphandlingar har fått ökat fokus genom det uttryckliga införandet av konkurrensprincipen i lagen om offentlig upphandling (LOU).[2] Även arbetsrättens betydelse har lyfts upp genom införandet i LOU av uttryckliga regler om arbetsrättsliga villkor.[3]

En stor och viktig del av de upphandlingar som genomförs avser IT i någon form. Upphandling av olika former av IT-system, licenser, tjänstelösningar, telekommunikation etc., utgör en stor och viktig del av myndigheters upphandlingar. I IT-upphandlingar berör upphandlingsföremålet ofta viktiga delar av myndigheternas kärnverksamhet. IT-rätten har därmed stor betydelse i offentlig upphandling. Såväl kravställning som avtalskonstruktion och innehåll i IT-upp-

* Pernilla Norman är advokat och delägare i Advokatfirman LexIT, samt doktorand vid juridiska institutionen vid Stockholms universitet.

1 20 kap. LOU, Lag (2016:1145) om offentlig upphandling.

2 4 kap. 2 § LOU.

3 4 kap. 3 § LOU.

handlingar görs med tillämpning av IT-rätt. Samspelet mellan upphandlingsrätten och IT-rätten är alltså av stor betydelse i IT-upphandlingar.

Precis nu, den 25 maj, börjar dataskyddsförordningen (ofta kallad GDPR, General Data Protection Regulation)[4] tillämpas. Den nya lagen ställer stora krav på hur myndigheter, organisationer och företag hanterar personuppgifter. Det ställer helt nya krav på kravställning och avtal i IT-upphandlingar. Dataskyddsförordningen måste beaktas i varje IT-upphandling från och med nu.

Denna artikel undersöker och analyserar hur samspelet mellan LOU och Dataskyddsförordningen kan och bör hanteras i IT-upphandlingar framöver.

1.2 Dataskydd och informationssäkerhet

Dataskyddsförordningen möter den ökade globaliseringen som digitaliseringen innebär genom att stärks skyddet för enskilda i hanteringen av personuppgifter och för att garantera den fria rörligheten av personuppgifter inom EU.

Dataskyddsförordningen har två utgångspunkter. Dels den fria rörligheten, att personuppgifter (information) ska kunna röra sig fritt inom EU. Dels mänskliga rättigheter med skydd för personlig integritet. Enkelt uttryckt kan man beskriva det som att Dataskyddsförordningen utgår från att personen själv ”äger” sina personuppgifter och har rätt att bestämma hur dessa används, och i fall där man inte har den bestämmanderätten har man i vart fall rätt att få information om och veta hur ens personuppgifter används.

En viktig del av att skydda data är informationssäkerhet. Med skydd avses att kunna upprätthålla rätt nivå av

- Konfidentialitet
- Riktighet
- Tillgänglighet
- Spårbarhet

Informationssäkerhet vid upphandling av IT-relaterade tjänster handlar därmed om att styra upphandlingsprocessen så att den levererade tjänsten eller systemet kan upprätthålla de krav på att informationen ska vara skyddad som har definierats i avtalet. I fall av köp av IT-tjänster, outsourcing mm behöver det allstå säkerställas att informationen är skyddad hos leverantören. Det innebär till exempel att informationen ska vara skyddad från obehörig insyn och förändring hos leverantören samt att informationen inte hanteras på annat sätt än vad som överenskommits. Beställaren ska också ha möjlighet att granska

[4] Förordning EU/2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

hur informationen har hanterats hos leverantören.[5] Bristerna avseende informationssäkerhet i såväl upphandling som avtal och avtalsuppföljning, illustreras tydligt av exemplet från Transportstyrelsen från förra sommaren.[6]

1.3 Säkerhetsskyddad upphandling

Av exemplet med Transportstyrelsens upphandling som ledde till att hemliga uppgifter fördes över till icke-säkerhetsklassad personal i andra länder, framgår att det vid IT-upphandlingar är viktigt att definiera vilken typ av information som behandlas i det system som är föremål för upphandlingen. I fallet med Transportstyrelsen var det fråga om att myndigheten outsourcade driften till hela sin IT-miljö.[7] Innan en myndighet påbörjar en IT-upphandling ska myndigheten pröva om upphandlingen helt eller delvis ska säkerhetsskyddas, dvs. att det ska genomföras en så kallad upphandling med säkerhetsskyddade avtal (SUA). Det som avgör om en upphandling ska säkerhetsskyddas eller inte är om företaget kan få del av hemliga uppgifter i förfrågningsunderlaget eller under uppdragets utförande.

Hemliga uppgifter avser uppgifter som är hemliga enligt säkerhetsskyddslagen (1996:627).

Med säkerhetsskydd avses:

- Skydd mot brott som kan hota rikets säkerhet
- Skydd av hemliga uppgifter som rör rikets säkerhet
- Skydd mot terrorism.

För upphandling som berör säkerhetsskyddad information, dvs. där leverantören kan få del av sådan information gäller särskilda regler. Bland annat ska myndigheten[8] träffa ett skriftligt säkerhetsskyddsavtal med leverantören om det säkerhetsskydd som behövs i det särskilda fallet.[9] På grund av att det är särskilda regler som gäller, behandlas säkerhetsskyddad upphandling inte ytterligare i denna artikel.[10]

---

5 Myndigheten för samhällsskydd och beredskap, Vägledning för informationssäkerhet i upphandling, 2013, s. 7.

6 Transportstyrelsens bristande hantering av säkerhetsskyddad information uppdagades under sommaren 2017 och ledde såväl till att generaldirektören avsattes, som till granskning av ”affären” i Konstitutionsutskottet under hösten 2017 och våren 2018.

7 Ds 2018:6 Granskning av Transportstyrelsen upphandling av it-drift, Regeringskansliet Näringsdepartementet.

8 Enligt 8 § Säkerhetsskyddslagen (1996:627).

9 Myndigheten för samhällsskydd och beredskap, Vägledning för informationssäkerhet i upphandling, 2013, s. 10.

10 Information om säkerhetsskyddad upphandling finns i Säkerhetspolisens vägledning för säkerhetsskyddad upphandling, www.sakerhetspolisen.se/sakerhetsskyddadupphandling.

2. TILLÄMPLIGA LAGAR

2.1 De aktuella lagarna

Vid upphandling av IT berörs ett antal olika regelverk inom olika rättsområden.[11] Avseende säkerställande av dataskydd i de IT-system som upphandlas, är det huvudsakligen LOU och Dataskyddsförordningen som är aktuella. Medan LOU styr upphandlingsförfarandet och upphandlingens genomförande, tillämpas Dataskyddsförordningen på kravställningen dvs. utformningen av kraven i upphandlingsdokumenten.[12]

Såväl LOU som Dataskyddsförordningen innehåller grundläggande rättsprinciper vilka ska genomsyra all hantering enligt respektive lagstiftning. Både vid genomförande av offentlig upphandling och vid hantering av personuppgifter, är det alltså viktigt att läsa och tolka specifika regler i ljuset av respektive lags allmänna principer. Vid sidan om de allmänna rättsprinciperna innehåller de båda lagarna ett antal stadganden som är av särskild betydelse vid kravställning i IT-upphandlingar.

2.2 LOU

De grundläggande upphandlingsrättsliga principerna stadgas numera i 4 kap. LOU.[13] Principerna har stort genomslag i upphandlingsrätten och har i allt väsentligt överförts från tidigare upphandlingslagar.[14] Endast konkurrensprincipen har en lite speciell historia.[15]

De grundläggande upphandlingsrättsliga principerna är följande.

Transparensprincipen – Principen om transparens, förutsebarhet och öppenhet innebär att det ska vara möjligt för en anbudsgivare att från förfrågningsunderlaget (upphandlingsdokumentationen) utläsa dels vad den upphandlade myndigheten efterfrågar (såväl avseende själva upphandlingsföremålets krav och kriterier, som i formaliahänseende), och dels att hur anbudet kommer att hanteras, prövas och värderas. Vidare innebär transparensprincipen att det efter upphandlingens genomförande ska vara möjligt att säkerställa att den upphandlande myndigheten faktiskt agerade och genomförde upphandlingen på det sätt som angavs i förfrågningsunderlaget.

I transparensprincipen kan också objektivitetsprincipen sägas ingå. *Objektivitetsprincipen* innebär att upphandlande myndighet ska vara oberoende i

[11] Punkt 1.1 ovan.
[12] Sedan nuvarande LOU:s införande i januari 2017 används begreppet upphandlingsdokument istället för förfrågningsunderlag, som är den term som tidigare har använts.
[13] 4 kap. 1 och 2 §§ LOU.
[14] Senast 1 kap. 9 § lagen (2007:1091) om offentlig upphandling.
[15] Fanns senast i 1 kap. 4 § lagen (1992:1528) om offentlig upphandling.

upphandlingen och inte ta ovidkommande hänsyn, dvs. inte tillmäta någon betydelse annat än de faktorer som beskrivits i förfrågningsunderlaget.[16]

Likabehandlingsprincipen – Likabehandlingsprincipen är nära sammankopplad med icke-diskriminering, och innebär att alla anbudsgivare ska behandlas på ett likvärdigt sätt. Ingen anbudsgivare ska sättas i en bättre eller sämre situation än övriga. Detta gäller exempelvis vad gäller tillgång till information, men också själva behandlingen av anbudsgivare och deras anbud. Bland annat innebär principen att i fall där den upphandlande myndigheten har ett avtal för samma eller liknande avtalsföremål som upphandlingsföremålet, kan extra information behöva ges i förfrågningsunderlaget för att den befintliga avtalsparten inte ska ha tillgång till mer information än övriga anbudsgivare.

Likabehandlings- och icke-diskrimineringsprincipen innebär att alla anbud ska hanteras på ett likvärdigt sätt, att likheter ska bedömas och hanteras likadant, men också att olikheter ska uppmärksammas och hanteras på olika sätt. Det kan således strida mot likabehandlingsprincipen att exempelvis i utvärderingshänseende sätta upp en nivå (en ribba) och tilldela alla anbudsgivare som överstiger den nivån samma poäng, oavsett hur mycket nivån överstigs.

Proportionalitetsprincipen – Proportionalitetsprincipen innebär att varje åtgärd som vidtas i en upphandling ska stå i rimlig proportion till syftet med åtgärden. Vidare måste åtgärden ha ett naturligt samband med det ändamål som ska uppnås. Det är alltså inte tillåtet att ställa alltför långtgående krav i en upphandling. Kraven ska vara både lämpliga och nödvändiga och upphandlande myndigheten ska alltid välja det minst ingripande alternativet som står till buds.

Ömsesidigt erkännande – Upphandlingsrätten innehåller också den mer utpräglat EU-rättsliga principen om ömsesidigt erkännande. Principen innebär att examina, intyg, certifikat med mera som har utfärdats i ett medlemsland ska erkännas och godkännas och därmed vara gällande i samtliga EU-länder.[17]

Konkurrensprincipen – Konkurrensprincipen innebär att upphandlingar inte får utformas på ett sätt så att konkurrensen inte begränsas på ett konstgjort (i syfte att begränsa) sätt (eng.: artificially narrowing competition). En upphandling anses syfta till att begränsa konkurrensen om leverantörer otillbörligen gynnas eller missgynnas av det sätt på vilket upphandlingen har utformats. Stadgandet tar sikte på det sätt på vilket den upphandlande myndigheten utformar själva upphandlingen. Detta kan exempelvis gälla hur upphandlingsföremålet formuleras, eller hur enskilda villkor i förfrågningsunderlaget eller avtalet utformas.[18]

De allmänna principerna har stor betydelse för hur krav kan formuleras och hanteras i offentliga upphandlingar. Vid sidan om dessa principer finns speci-

[16] Norman Pernilla och de Jounge Malin, Offentlig upphandling En handbok, Norstedts Juridik, supplement 33 2017, s. 43.
[17] Norman och de Jounge, s. 44.
[18] Norman och de Jounge, s. 48.

fika regleringar i kap. 9 LOU. Dessa regler tar främst sikte på att tillse att handeln mellan EU-länderna inte förhindras, exempelvis genom att föreskriva att standarder ska användas i största möjliga utsträckning[19] och att olika former av märkningar (såsom miljömärkningar) hanteras på ett konkurrensneutralt sätt.[20]

Till skillnad från de allmänna rättsprinciperna i LOU kan man säga att reglerna kring tekniska krav för en undanskymd tillvaro. De beaktas endast i begränsad omfattning i upphandlande myndigheters praktiska arbete med framtagande av upphandlingsdokument och hantering av inkomna anbud.

2.3 GDPR

Precis som LOU innehåller Dataskyddsförordningen ett antal grundläggande rättsprinciper. Dessa principer ska genomsyra all hantering av personuppgifter och övriga regler i Dataskyddsförordningen ska tolkas och tillämpas i ljuset av dessa principer. De grundläggande dataskyddsprinciperna är följande.

Laglighet, korrekthet och öppenhet/ lawfulness, fairness and transparency – Personuppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.

Ändamålsbegränsning/Purpose limitation – Alla personuppgifter ska enligt dataskyddsförordningen samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

Uppgiftsminimering/Data minimisation – Personuppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

Korrekthet/Accuracy – Alla personuppgifter ska vara riktiga och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.

Lagringsminimering/Storage limitation – Personuppgifter får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

Konfidentialitet/Confidentiality – Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.[21]

---

[19] 9 kap. 4 § LOU.
[20] 9 kap. 13 § LOU.
[21] Art. 5 Dataskyddsförordningen.

Förutom de grundläggande rättsprinciperna finns två grundläggande förutsättningar för hantering av personuppgifter stadgade i Dataskyddsförordningen. Det måste finnas en rättslig grund[22] samt ett specifikt ändamål[23] i varje enskilt fall. Båda dessa ska vara fastställda innan personuppgiftsbehandlingen påbörjas. Möjligheterna att ändra eller lägga till ändamål efter det att en personuppgift har samlats in är ytterst begränsade.[24]

Av stor betydelse för kravställningen i IT-upphandlingar är den roll som IT-leverantören får i leveransen. I fall där leverantören blir personuppgiftsbiträde enligt Dataskyddsförordningens definition,[25] är det av särskild vikt att den upphandlande myndigheten i upphandlingens kravställning säkerställer att och på vilket sätt leverantören tillser att Dataskyddsförordningens regler uppfylls. I dessa fall ska ett särskilt personuppgiftsbiträdesavtal träffas mellan den upphandlande myndigheten och leverantören, vid sidan om det IT-avtal som upphandlas.[26]

Dataskyddsförordningen innehåller regler om att varje organ som behandlar personuppgifter är skyldig att med beaktande av den senaste utvecklingen, genomförandekostnaderna, de uppgifter som behandlas mm, tillse att vidta tillräckliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen sker i enlighet med Dataskyddsförordningen.[27] Förordningen ställer alltså krav dels på tekniken i IT-systemen (s.k. inbyggt dataskydd och dataskydd som standard)[28] och på den aktuella organisationens policys, processer och rutiner. Det är framför allt dessa regler i Dataskyddsförordningen som den upphandlande myndigheten har att förhålla sig till i sin kravställning i IT-upphandlingar.

2.4 Hur påverkar dataskyddsfrågor val av upphandlingsförfarande?

Det kan finnas skäl för den upphandlande myndigheten att fundera över hur och vilka dataskyddskrav som behöver hanteras i upphandlingen, redan vid valet av upphandlingsförfarande. Eftersom de krav som kan komma ifråga är beroende av omständigheterna i det enskilda fallet, bland annat om känsliga personuppgifter kommer att behandlas och i övrigt vilken riskklass aktuella

---

22 Art. 6 punkt 1 Dataskyddsförordningen.

23 Art. 5 punkt 1 b) Dataskyddsförordningen, se även skäl 39.

24 Art. 6 punkt 4 Dataskyddsförordningen.

25 Art. 4 punkt 8 Dataskyddsförordningen avses med personuppgiftsbiträde ”*en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning*”.

26 Art. 28 Dataskyddsförordningen. Se vidare om personuppgiftsbiträdesavtal i punkten 4 nedan.

27 Art. 24 och 32 Dataskyddsförordningen.

28 Art. 25 Dataskyddsförordningen, *eng*: privacy by design and privacy by defalult.

personuppgifter har, är det inte möjligt att generellt säga att vissa upphandlingsförfaranden är mer lämpliga än andra.

Genom införandet av den nya LOU ökade möjligheterna att använda förfaranden som medger förhandlingar och dialoger[29] vid upphandling av IT-lösningar. Bland annat kan förfarandena användas när behovet ”*inte kan tillgodoses utan anpassning av lättillgängliga lösningar*”.[30] Exempel på detta är att det fordras integrationer och anpassningar till befintlig IT-miljö. Ytterligare skäl att välja något av dessa båda förfaranden är att det finns särskilda omständigheter som ”*avser arten, komplexiteten eller den rättsliga eller ekonomiska utformningen…*”.[31] Ett exempel på detta där dataskyddsfrågorna kan vara av stor betydelse är om den upphandlande myndigheten inte i förväg bestämmer om upphandlingen ska avse tjänst eller leverans av ett system. Slutligen kan något av förfarandena väljas i fall där det inte går att formulera de tekniska specifikationerna med ”*tillräcklig precision*”.[32] Det är inte svårt att tänka sig situationer där dessa svårigheter att formulera kraven kan vara en följd av dataskyddsfrågor.

Man kan alltså konstatera att hantering av dataskyddsfrågor i kravställning i IT-upphandling kan påverka vilket upphandlingsförfarande som kan väljas i den enskilda upphandlingen. Hanteringen av dataskyddsfrågor kan motivera att den upphandlande myndigheten kan välja något av förfarandena förhandlad upphandling med föregående annonsering eller konkurrenspräglad dialog. På ett allmänt plan kan sägas att om det föreligger grund för att använda ett förfarande som tillåter diskussioner och muntlig kommunikation mellan den upphandlande myndigheten och anbudsgivare, är detta generellt att föredra.

3. DATASKYDD I KRAVSTÄLLNING

3.1 Allmänt om kravställning i IT-upphandlingar

En utgångspunkt för kravställande i offentlig upphandling är att kraven ska vara utformade på ett sätt så att offererade lösningar tillgodoser verksamhetens behov. Detta kan låta som en självklarhet, men att hålla kompassen på just verksamhetens behov och inte fastna i detaljerade IT och/eller tekniska formuleringar, kan ofta visa sig väl så svårt i praktiken. IT-avtal är ofta komplexa och för att leveranser av IT-system, IT-tjänster etc. ska bli ändamålsenliga och tillgodose det behov som verkligen finns i verksamheten, behöver upphandlingen spegla denna komplexitet.[33] För framgångsrik IT-upphandling fordras

[29] Förhandlat upphandlingsförfarande med föregående annonsering samt konkurrenspräglad dialog.
[30] 6 kap. 5 § punkt 1, samt 6 kap. 20 § LOU.
[31] 6 kap. 5 § punkt 3, samt 6 kap. 20 § LOU.
[32] 6 kap. 5 § punkt 4, samt 6 kap. 20 § LOU.
[33] Arrhed, L, Offentlig upphandling av komplexa IT-tjänster, Wolters Kluwer 2016, s. 29.

att kravställningen är inriktad på den funktionalitet som verksamheten har behov av, och inte en specifik teknisk lösning (som man tror man har behov av). För att beskriva detta har det utvecklats ett begrepp kallat ”*funktionsupphandling*”.[34] Funktionsupphandling är ett sätt att uttrycka kravställningen i termer av önskade funktioner, effekter och resultat, vilket medför att anbudsgivarna i sina anbud kan lämna olika förslag på lösningar. Funktionsupphandling kan användas vid upphandling av såväl tjänster som system och licenser.[35] Det är helt enkelt ett sätt att formulera och uttrycka kraven med fokus på vad man vill uppnå med lösningen. Detta ska skiljas från det mer sedvanliga sättet att utforma kravspecifikationer i form av specifikationskrav, vilket innebär att det uppställs detaljerade krav på hur lösningen ska vara utformad.

En utmaning vid upphandling av IT-lösningar är behovet av flexibilitet i det som levereras över tid.[36] Att tillgodose behov av flexibilitet i upphandling och avtal är en svårighet, som kan underlättas genom funktionsupphandling. Sättet att beskriva upphandlingsföremålet i termer av verksamhetens behov öppnar möjligheter att även ta med och beskriva hur behoven kan komma att förändras under avtalstiden.

Det fordras emellertid att behoven uttrycks och beskrivs på en tillräcklig detaljnivå. En alltför hög och abstrakt behovsbeskrivning är inte ändamålsenlig eftersom den riskerar att upphandlingen resulterar i att det som så småningom levereras faktiskt inte motsvarar behoven. Det riskerar också att strida mot LOU, främst de grundläggande principerna om transparens och förutsebarhet och proportionalitet samt förmodligen konkurrensprincipen. Att i IT-upphandlingar antingen uppställa ett krav eller föreskriva ett särskilt kontraktsvillkor att ”*leverantören är skyldig att tillse att man uppfyller GDPR*” eller det än mer långtgående att beställaren genom leveransen uppfyller GDPR, är inte godtagbart och måste anses strida mot LOU. Denna typ av skrivningar har dock under senare tid varit vanliga i IT-upphandlingar.

3.2 Kraven är beroende av upphandlingsföremålet

Vad Dataskyddsförordningen innebär och hur den ska tillämpas beror till stor del på vilka personuppgifter som hanteras.[37] Om känsliga personuppgifter[38] behandlas i det IT-system som upphandlas, är kraven på säkerheten i den tek-

[34] Se tex Upphandlingsmyndigheten www.upphandlingsmyndigheten.se/Dialog och innovation/Funktion.

[35] Det är en vanlig missuppfattning att funktionsupphandling är en form av tjänsteupphandling.

[36] Arrhed, s. 33.

[37] Se ovan avsnitt 2.3.

[38] S.k. ”särskilda kategorier av personuppgifter” tex uppgifter om etniskt ursprung, politiska åsikter, religion medlemskap i fackförening och biometriska uppgifter, regleras i Art. 9 Dataskyddsförordningen.

niska lösningen högre än om det är tämligen ”ofarliga” uppgifter. Dataskyddsförordningen relaterar också till den tekniska utvecklingen som ständigt sker och stadgar vad gäller säkerhet i samband med behandling att man ska vidta lämpliga tekniska och organisatoriska åtgärder bland annat men hänsyn till ”*den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar*”.[39] Av detta framgår att vad som behöver kravställas i IT-upphandlingar är beroende av olika omständigheter i det enskilda fallet. Detta innebär att generella, övergripande standardformuleringar i upphandlingsdokument inte fungerar. Den upphandlande myndigheten behöver istället göra ett arbete och formulera uttryckliga krav i förhållande till den information som avses att hanteras i den IT-lösning som den enskilda upphandlingen avser.

En annan faktor som är av stor betydelse för hur kraven i upphandlingen behöver utformas är vilken roll leverantören kommer att ha i leveransen. I fall där leverantören kommer att vara personuppgiftsbiträde[40] behövs mer långtgående krav ställas än i andra fall. Då behöver också personuppgiftsbiträdesavtal träffas vid sidan om huvudavtalet. Som utgångspunkt är det att rekommendera att leverantörens mall för personuppgiftsbiträdesavtal används,[41] men i fall då den upphandlande myndighetens mall används bör den lämpligen ingå i upphandlingsdokumenten.

3.3 Krav på teknisk lösning

Dataskyddsförordningen bygger på en grundläggande utgångspunkt att man inte får samla in och hantera fler personuppgifter, andra personuppgifter och under längre tid än vad som är *nödvändigt* för att tillgodose ändamålen med personuppgiftsbehandlingen.[42] Detta ställer stora krav på att uppgifter ska rensas ur IT-system. Möjligheter att gallra, manuellt och automatiskt (exempelvis genom tidsinställning) är grundläggande krav som måste ställas vid upphandling av IT-lösningar.

Som beskrivits ovan[43] ställer Dataskyddsförordningen krav på att IT-lösningar ska ha s.k. inbyggt dataskydd och dataskydd som standard.[44] Med det avses att det ska finnas inbyggda mekanismer i IT-system till skydd för den personliga integriteten (privacy på design) och att mekanismer ska vara inställda på ett sådant sätt att integriteten skyddas på ett automatiserat sätt (tex tidsinställningar för automatisk gallring).

---

39 Art. 32 Dataskyddsförordningen.
40 Se avsnitt 2.3 ovan.
41 Se avsnitt 4 nedan.
42 Art. 5 punkterna b) och e).
43 Se avsnitt 2.3 ovan.
44 Art. 25 Dataskyddsförordningen, *eng*: privacy by design och privacy by default.

Exempel på andra delar som beställaren behöver fundera över och kravställa i den enskilda upphandlingen är följande.

- Inloggning och lösenord på olika nivåer
- Kryptering på olika nivåer
- Säkerhet på olika nivåer i kommunikationen till och från aktuellt IT-system
- Behörighetsstyrning
- Begränsningar i funktionalitet avseende personuppgifter (tex användning av personnummer, följer vanligen av behörighetsstyrningen)
- Back up:er
- Loggning och logghantering

De krav som behöver ställas i upphandlingar av IT-lösningar till följd av Dataskyddsförordningen är alltså omfattande och berör den enskilda tekniska lösningen. Eftersom skyddsnivån är beroende av vilka personuppgifter som avses hanteras i IT-systemet, finns det inte några generella krav som kan användas i upphandlingsdokumenten. Det är exempelvis inte möjligt att säga att Dataskyddsförordningen innebär att det fordras två faktors autentisering vid inloggning eller liknande. Det kan mycket väl vara godtagbart med inloggning med lösenord. Vad som emellertid står klart är att de övervägningar som behöver göras i dessa delar inte kan överlåtas till leverantören genom en generell skrivning i upphandlingsdokumenten.

3.4 Krav på organisatoriska åtgärder

Vad gäller kraven på organisatoriska åtgärder kan dessa delas in i två delar. Den ena delen är det åtgärder som respektive organisation den upphandlande myndigheten och leverantören, behöver vidta internt. Den andra delen avser åtgärder som den upphandlande myndigheten behöver vidta för att genomföra och ”använda” de tekniska funktionerna. Detta kan exempelvis vara åtgärder för att använda och utnyttja det behörighetssystem som IT-lösningen tekniskt innehåller. Det kan också vara fråga om tex inställningar i systemet för att tillse att gamla behörigheter inte ligger kvar när en användare får nya behörigheter. Denna typ av åtgärder kan myndigheten inte kravställa om, utan Dataskyddsförordningens krav kan endast uppfyllas av myndigheten själv. Andra organisatoriska åtgärder som den upphandlande myndigheten behöver vidta är bland annat att anta en policy för behandling av personuppgifter, införa rutiner för att snabbt kunna hantera förfrågningar om information, rättning och radering från enskilda, ta fram en rutin för hantering och rapportering av personuppgiftsincidenter och lägga ut information om hantering av personuppgifter på hemsidan och andra forum. Inget av detta kan överföras på leverantören.

Däremot kan det vara av intresse för den upphandlande myndigheten att i en upphandling begära information och eventuellt kravställa kring vilka organisatoriska åtgärder leverantören har vidtagit i internt i sin organisation för att möta Dataskyddsförordningens krav.

I fall där leverantören kommer att vara personuppgiftsbiträde till den upphandlande myndigheten kan mer långtgående krav behöva ställas, eftersom leverantören i de fallen kommer att sköta och utföra en del av de åtgärder som åligger beställaren. Det kan tex vara leverantören som rent faktiskt ändrar en felaktig personuppgift i IT-systemet, när en registrerad begär rättning enligt Dataskyddsförordningens regler.

4. PERSONUPPGIFTSBITRÄDESAVTAL

4.1 Avtalet

Personuppgiftsbiträdesavtalen behöver vara mer omfattande enligt Dataskyddsförordningen än vad som fordrades enligt PuL.[45] Avtalet ska dels säkerställa att informationen hanteras på ett säkert sätt hos och av personuppgiftsbiträdet och dels reglera vilka åtgärder biträdet får respektive ska utföra.[46] Av Dataskyddsförordningen följer att en uttrycklig instruktion från personuppgiftsansvarige, sak biläggas avtalet.[47]

I fall där personuppgiftsbiträdet anlitar underbiträden ska biträdes skyldigheter enligt personuppgiftsbiträdesavtalet föras vidare genom avtal mellan biträdet och underbiträdet. Det uttrycks explicit att underbiträdet ska åläggas ”samma skyldigheter”. I fall underbiträdet inte fullgör sina skyldigheter, är personuppgiftsbiträdet ansvarigt gentemot den personuppgiftsansvarige.[48] Ett exempel på underbiträde kan vara att en IT-leverantör hyr datahallar där man har den utrustning som behövs för att realisera och tillhandahålla den aktuella IT-tjänsten. I det fallet kan leverantören av IT-hallar bli underbiträde till IT-leverantören som är personuppgiftsbiträde i förhållande till den upphandlande myndigheten som är personuppgiftsansvarig.

Skyldigheten för personuppgiftsbiträdet att ha ett motsvarande personuppgiftsavtal som ålägger underbiträdet ”samma skyldigheter” anses vara ett skäl för att som utgångspunkt använda leverantörens och inte den upphandlande myndighetens mall för personuppgiftsbiträdesavtal som utgångspunkt. Det bedöms vara förenat med stora svårigheter för ett personuppgiftsbiträde att hantera alltför många olika personuppgiftsbiträdesavtal i förhållande till underbiträdena.

---

45 PuL, Personuppgiftslagen (1998:20), tillämpades fram till den 25 maj 2018.
46 Art. 28 Dataskyddsförordningen.
47 Art. 28 punkt 3 a) Dataskyddsförordningen.
48 Art. 28 punkt 4 Dataskyddsförordningen.

4.2 Ansvar

Under senhösten 2017 och våren 2018 har stort fokus vid träffande av personuppgiftsbiträdesavtal lags på ansvarsfrågorna. Detta är förmodligen en effekt av den stora osäkerhet som råder om hur de sanktionsavgifter som stipuleras i Dataskyddsförordningen kommer att hanteras i praktiken och inte minst vilka belopp som kommer att utdömas i olika fall. På ett allmänt plan kan emellertid konstateras att eventuella skador till följd av brister i dataskyddshänseende inte är att betrakta på något annat sätt än andra skador som kan uppkomma i ett avtalsförhållande. Det som är kännetecknande för skador är just att de är en blandning av oväntade, plötsliga och ett risktagande. Vid bestämmande av ansvar och ansvarsbegränsningar i huvudavtalet har de olika faktorerna vägts samman och för det individuella avtalsförhållandet lämpliga nivåer har fastställts. Det finns inte någon anledning att betrakta dataskyddsskador på något annat sätt. Sådana skador bör därför hanteras enligt huvudavtalet, varvid personuppgiftsbiträdesavtalet bör innehålla en hänvisning till dessa delar av huvudavtalet.

5. DATASKYDD I AVROP FRÅN DE NATIONELLA RAMAVTALEN

En stor del av upphandlande myndigheters köp av IT-lösningar görs genom avrop från de nationellt upphandlade ramavtalen.[49] Många av dessa ramavtal har upphandlats innan frågor om hantering av dataskydd aktualiserades. Avtalen innehåller därför inte adekvat kravställning kring Dataskyddsfrågor.[50] Även personuppgiftsbiträdesavtalen kan avvika från vad som fordras enligt Dataskyddsförordningen.[51] I fall en upphandlande myndighet avser att avropa från ett Nationellt ramavtal, behöver det föregås av en analys om ifall det aktuella ramavtalet uppfyller de krav som uppställs i Dataskyddsförordningen, samt om det inte är så huruvida det är möjligt att inom ramen för LOU komplettera med sådana krav i avropet. Enligt LOU får villkoren i avropsavtalet inte avvika väsentligt från villkoren i det bakomliggande ramavtalet.[52] Det är svårt att tänka sig situationer där avropsupphandlingen innehåller omfattande krav på exempelvis teknisk lösning avseende säkerhet och kryptering av databaser, loggning och logghantering etc. som inte uppställdes i den bakomliggande ramavtalsupphandlingen. Behövs omfattande tilläggskrav ställas i det enskilda fallet, blir det snarast en fråga om att Dataskyddsförordningens krav motiverar att den upphandlande myndigheten gör en avstegsanmälan och går ut i en egen, separat upphandling.

---

[49] Statens inköpscentral vid Kammarkollegiet samt SKL Kommentus ramavtal.
[50] Exempelvis tekniska och organisatoriska krav, se avsnitt 3.3 och 3.4 ovan.
[51] Se avsnitt 4 ovan.
[52] 7 kap. 3 § LOU.

6. AVSLUTANDE KOMMENTARER

Avslutningsvis kan konstateras att Dataskyddsförordningen har stor betydelse i offentlig upphandling. Den här artikeln fokuserar på betydelsen för kravställning i IT-upphandlingar. Även andra aspekter aktualiseras, såsom exempelvis hantering av personuppgifter i de elektroniska upphandlingsverktygen och innebörden av LOU:s regler som begränsar möjligheten att ändra i ingångna avtal vilka har upphandlats offentligt.

Av den genomgång som görs i artikeln kan konstateras att upphandlande myndigheter behöver lägga ner tid, kraft och energi på att analysera och hantera Dataskyddsförordningens regler i arbetet med kravställning i IT-upphandlingar. Det är inte tillräckligt med generella skrivningar, vilka lägger över ansvaret för att uppfylla Dataskyddsförordningen på leverantören. Kraven måste vara balanserade och proportionerliga och baseras på de personuppgifter som avses att behandlas i det aktuella IT-systemet som upphandlingen avser. Sammanfattningsvis kan kraven delas i upp i tre delar. 1) krav på den tekniska lösningen, 2) krav på organisatoriska åtgärder, och 3) krav på personuppgiftsbiträdesavtalen där detta är aktuellt. Som så ofta i offentlig upphandling är framgångsfaktorn för kravställning av dataskydd i IT-upphandlingar att kraven tas fram i den enskilda upphandlingen baserat på den upphandlingens speciella omständigheter.