



Dataskyddsanvisning

Vad bör man veta om dataskydd vid offentliga upphandlingar

Författare:

Eeva-Riitta Högnäs Rådgivningsenheten för offentlig upphandling
Susan Hindström finansministeriet

Organisationer som intervjuats:

Lappträsk kommun, Arbetshälsoinstitutet och Satakunta välfärdsområde

Publicerad 10/2024

1. Inledning.....	3
2. Dataskyddsregleringens roller vid offentlig upphandling.....	4
3. Vad är personuppgifter vid offentlig upphandling?	6
4. Den upphandlande enhetens personuppgifters geografiska läge	8
5. Dataskydd i upphandlingsförfarandet.....	10
5.1 Dataskydd vid beredningen av en upphandling	10
5.2 Dataskydd i upphandlingsförfarandet	12
5.2.1. Administrativa och funktionella krav	12
5.2.2 Utkast till dataskyddsavtal.....	13
5.2.3 Förhandlingar om kontraktet	15
5.2.4 Bedömning av dataskyddet vid flera upphandlingar från samma leverantör	15
6. Dataskydd under kontraktperioden för en upphandling	16
7. Dataskyddsbeskrivning för upphandlingar	17
Nyttiga länkar.....	18

1. Inledning

Denna anvisning är avsedd som stöd för att förstå dataskyddsfrågor för personer som genomför upphandlingar. Syftet med dataskyddet är att säkerställa att privatpersoners uppgifter behandlas i enlighet med kraven i lagstiftningen och på ett transparent sätt. Med hjälp av den rättsliga regleringen förverkligas gränserna och förutsättningarna för tillåten behandling av personuppgifter.

I Europeiska unionens allmänna dataskyddsförordning (GDPR, General Data Protection Regulation) beskrivs om dataskydd. Den nationella dataskyddslagen (1050/2018) kompletterar och preciserar EU:s allmänna dataskyddsförordning och tillämpas vid sidan av den allmänna dataskyddsförordningen. Den allmänna dataskyddsförordningen är direkt tillämplig rätt som gäller alla personuppgiftsansvariga och personuppgiftsbiträden som behandlar personuppgifter.

I anvisningen beaktas inte alla skyldigheter eller risker i dataskyddsförordningen och det berättas inte om de rättigheter för privatpersoner som dataskyddsförordningen möjliggör. Utöver denna anvisning och bedömningen av upphandlingen av den upphandlingsexpert som ansvarar för konkurrensutsättningen kan det i enskilda fall vara befogat att konsultera en expert som uttryckligen är insatt i dataskyddsregleringen.

Anvisningen utgår från den vanligaste situationen vid offentlig upphandling, där den upphandlande enheten är personuppgiftsansvarig och leverantören är personuppgiftsbiträde. Att vara personuppgiftsansvarig

innebär förenklat att personuppgifterna har samlats in eller erhållits och sparats av den upphandlande enheten och att uppgifterna lämnas ut till leverantören ur något slags register.

Leverantörens roll ska dock bedömas separat för varje upphandling. Om leverantören har en mer komplex roll i genomförandet av upphandlingen ska en dataskyddsexpert konsulteras.

Dataskyddslagstiftningen grundar sig på privatpersonens (den registrerades) rätt till sina egna uppgifter. Den som genomför en offentlig upphandling kommer mer sällan i kontakt med privatpersoners begäranden om information eller uppgifter, så i den här anvisningen behandlas inte privatpersoners ställning med tanke på dataskyddet.

Anvisningen har skrivits med tjänsteupphandlingar som standard. Anvisningen kan emellertid också tillämpas vid upphandling av entreprenader eller varor. Dessutom ska andra bestämmelser om till exempel kunduppgifter beaktas separat för varje upphandling. Till exempel vid upphandlingar inom social- och hälsovården bör man separat säkerställa att kunduppgifter behandlas på rätt sätt, det vill säga sekretess, registreringspraxis och användarrättigheter, samt att de system som används för behandlingen är datasäkra.

2. Dataskyddsregleringens roller vid offentlig upphandling

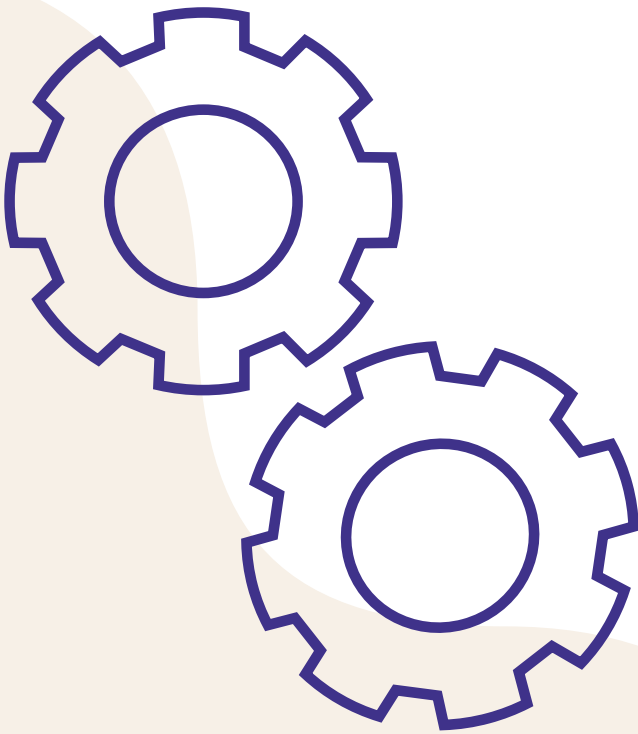
Avtalsparterna i en offentlig upphandling är den upphandlande enheten som är beställare och leverantören som är tjänsteleverantör. Parterna i dataskyddslagstiftningen är personuppgiftsansvariga och personuppgiftsbiträden. Dessa roller sammanfaller oftast tydligt när den upphandlande enheten är personuppgiftsansvarig och leverantören är personuppgiftsbiträde.

Den upphandlande enheten som personuppgiftsansvarig:

- Ger leverantören personuppgifter som den måste få för att kunna producera den beställda tjänsten
- Definierar medvetet föremålet för upphandlingen för att begränsa utlämnandet och behandlingen av uppgifter till det mest nödvändiga
- Bestämmer vad man får göra med uppgifterna, vad de får användas till och hur länge
- Definierar innehållet i behandlingen genom avtal eller annat dokument, t.ex. standardavtalsklausuler.

Leverantören som personuppgiftsbiträde:

- Tar emot nödvändiga personuppgifter från den personuppgiftsansvarige
- Följer den allmänna dataskyddsförordningen och den upphandlande enhetens anvisningar vid behandlingen av uppgifter
- Förstör personuppgifter när den inte längre behöver dem för att producera tjänsten.

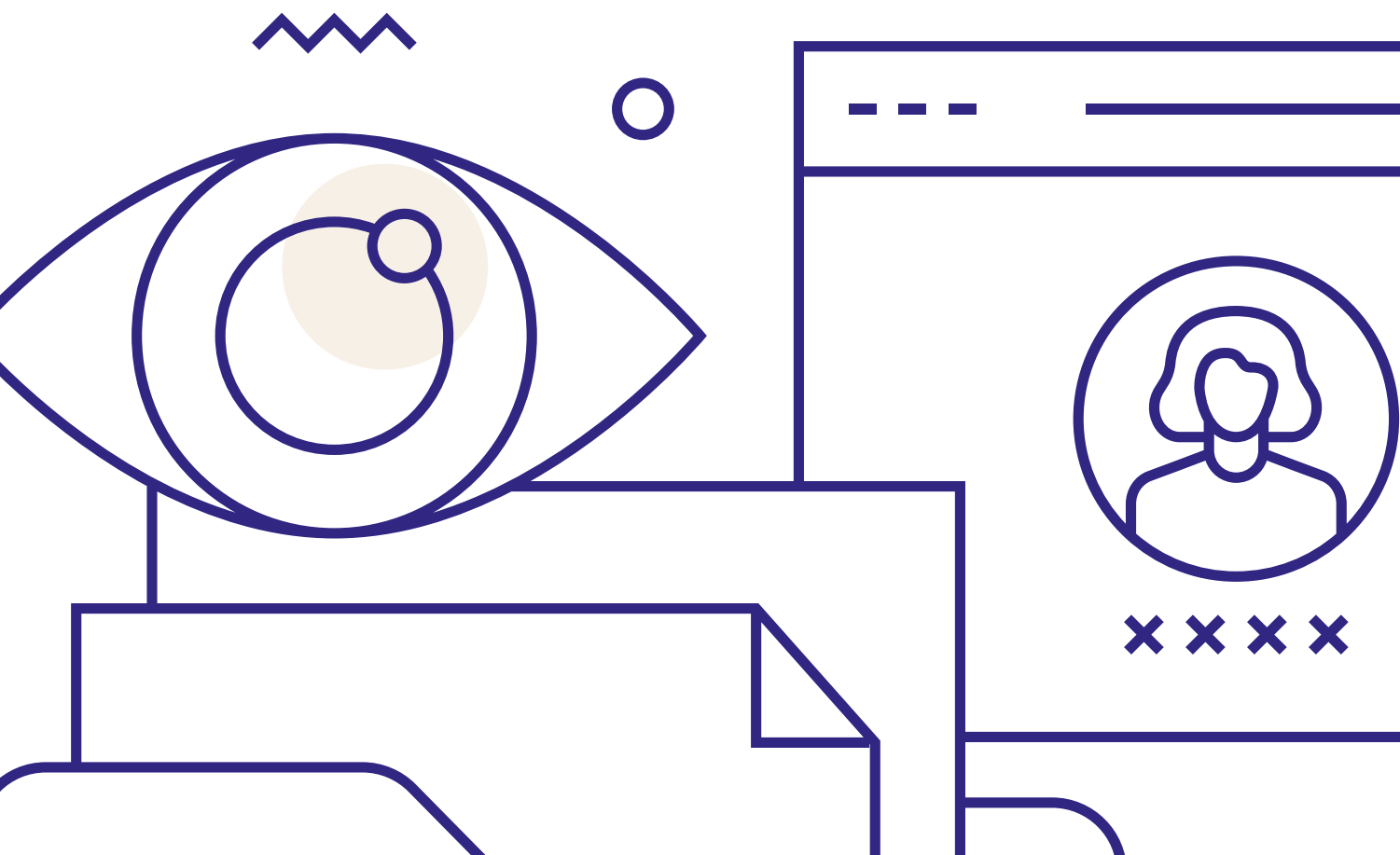


Den personuppgiftsansvarige, det vill säga den upphandlande enheten, har en viktig roll med tanke på personuppgifterna. I anbudsförfrågan vid en offentlig upphandling fastställer den upphandlande enheten i hur omfattande grad personuppgifter behandlas och under hur lång tid. Den personuppgiftsansvarige ansvarar för att personuppgifter som härstammar från dess register behandlas på behörigt sätt. Om något inträffar med personuppgifterna (t.ex. informationsläcka), är den upphandlande enheten i egenskap av personuppgiftsansvarig ansvarig för följderna.

Vid upphandlingar har tjänsteproducenten oftast rollen som personuppgiftsbiträde. Rollen är densamma oberoende av vem som äger eller administrerar det system som personuppgifterna behandlas i. Tjänsteproducenten fungerar oftast som personuppgiftsbiträde även om den sparar eller behandlar personuppgifter i sitt eget eller den upphandlande enhetens system.

Om leverantören använder en underleverantör i upphandlingen ska underleverantörens roll med tanke på personuppgifterna bedömas separat för varje upphandling. Vid varje upphandling ska man bedöma om leverantörens underleverantör behöver behandla personuppgifter utöver den huvudansvariga leverantören. Således kan det även om leverantören behöver personuppgifter från beställarens register för att genomföra tjänsten vara möjligt att planera upphandlingen så att leverantörens underleverantör inte behöver behandla uppgifterna. Detta ska beaktas när föremålet för upphandlingen definieras.

Om underleverantören behöver behandla beställarens personuppgifter vid produktionen av tjänsten, ska leverantören genom avtal försäkra sig om att underleverantören behandlar beställarens personuppgifter endast i den omfattning och enligt de anvisningar som den upphandlande enheten fastställt. Leverantören ansvarar för underleverantörens behandling av uppgifterna på samma sätt som för sin egen verksamhet.



3. Vad är personuppgifter vid offentlig upphandling?

Organisationer, bland annat upphandlande enheter, samlar in och behandlar många olika uppgifter om privatpersoner. De kan samla in information om besökare på sina webbplatser, upprätthålla information om sina anställda, ordna evenemang där det samlas in uppgifter om deltagarna eller producera lagstadgade tjänster eller andra tjänster där kunduppgifter samlas in. Alla ovan nämnda helheter av personuppgifter bildar ett personregister. Registret kan i praktiken vara till exempel innehållet i ett kunddatasystem, en Excel-fil som

sammanställts om deltagarna i ett evenemang eller en applikation för uppföljning av en webbplats. De personer vars uppgifter samlas in ska informeras om att det finns ett personuppgiftsregister, om vilka uppgifter som samlas in i registret och om vad uppgifterna används till i den upphandlande enhetens verksamhet. Informationen sker ofta i form av en beskrivning av behandlingsåtgärderna som finns till exempel på organisationens webbplats eller via en länk när man anmäler sig till evenemanget.

En personuppgift är vilken som helst uppgift som med rimligt besvär kan kopplas till en privatperson.

Personuppgifter är bland annat:

- Namn
- Personbeteckning, användarnamn
- Lokaliseringsinformation, adress, e-postadress
- Fotografi
- Fingeravtryck
- Onlineidentifikator (t.ex. IP-adress)
- En fysisk, fysiologisk, genetisk, psykisk, ekonomisk, kulturell eller social faktor



Dataskyddsförordningen ställer särskilda kategorier av personuppgifter, det vill säga uppgifter som till sin natur är särskilt känsliga och som i regel inte får behandlas, under särskilt skydd. Sådana uppgifter är till exempel uppgifter om hälsa, etniskt ursprung, religion eller sexualitet. Dessa uppgifter får behandlas endast i noggrant avgränsade situationer enligt dataskyddsförordningen (artikel 9). Inom vissa tjänster inom den offentliga sektorn finns det dock ett behov och en grund för att behandla sådana uppgifter. Om särskilda kategorier av personuppgifter behandlas vid en upphandling, bland annat kunduppgifter enligt lagen om kunduppgifter, ska den upphandlande enheten fästa särskild uppmärksamhet vid att säkerställa att det finns en med dataskyddsförordningen förenlig grund för att behandla uppgifterna. Dessutom ska uppmärksamhet fästas vid att behandlingen av uppgifterna begränsas samt vid personuppgiftsbitrådets anvisningar.

Vid offentlig upphandling är väsentliga personuppgifter de uppgifter som leverantören behöver för att producera tjänsten och den upphandlande enheten ger anvisningar om användningen av dem. I allmänhet är det fråga om uppgifter som lämnas direkt ur den upphandlande enhetens personregister, det vill säga uppgifter som den upphandlande enheten skickar till leverantören i något filformat eller i annat format efter att kontraktperioden har inletts. Det kan också vara fråga om personuppgifter som leverantören samlar in för den upphandlande enhetens räkning. Då ska den upphandlande enheten och leverantören ingå ett dataskyddsavtal om behandlingen av uppgifterna.

Om det vid upphandlingen inte överförs uppgifter från den upphandlande enhetens register till leverantören eller om leverantören i övrigt inte själv samlar in personuppgifter för den upphandlande enhetens räkning, behöver dataskyddet inte beaktas vid upphandlingen.



Om det vid en upphandling inte särskilt lämnas ut uppgifter ur ett personregister, men leverantören i samarbetet inom ramen för kontraktet ser kontaktpersonen för kontraktet och dennes två kollegers e-postadress i e-postmeddelanden som gäller upphandlingen, ska ett dataskyddsavtal ingås?

Nej, det behövs inte. Det är inte fråga om personuppgifter som den upphandlande enheten i egenskap av personuppgiftsansvarig har samlat in för ett visst ändamål.

4. Den upphandlande enhetens personuppgifters geografiska läge

EU:s dataskyddsförordning har förenhetligat dataskyddsregleringen inom Europeiska ekonomiska samarbetsområdet (EES-området). Därmed tillämpar alla EU- och EES-länder samma dataskyddsbestämmelser och avtal om behandlingen av uppgifter är enhetliga inom detta geografiska område. Det här innebär att det att en leverantör eller dennes underleverantör är placerad till exempel i ett annat EU-land inte utgör någon särskild risk som man separat borde reagera på.

Det som är besvärligt i fråga om behandling av elektroniska uppgifter är dock att även om den upphandlande enhetens kontraktsleverantör är placerad till exempel i Irland eller Estland, kan uppgifterna röra sig via datanäten utanför EES-området.

Den upphandlande enheten ska vid planeringen av upphandlingen vara medveten om var de leverantörer som levererar föremålet för upphandlingen geografiskt behandlar personuppgifter. Det här kan utredas till exempel med hjälp av en marknadsdialog. Ju mer kritisk upphandlingen är och ju känsligare uppgifter som behandlas i upphandlingen, desto mer kritiskt ska man i planeringen av föremålet för upphandlingen förhålla sig till att uppgifter behandlas utanför EES-området. Behandling utanför EES-området är ändå tillåten av grundad anledning och på basis av separat avtalsdokumentation.

Vid upphandling kan man som standard förutsätta att den upphandlande enhetens uppgifter behandlas inom EES-området, eller med andra ord att uppgifterna inte får behandlas utanför EES-området. Den upphandlande enheten ska dock säkerställa att det på marknaden finns anbudsgivare som uppfyller kravet.



Till exempel är det berättigat att den upphandlande enheten i en marknadsdialog utreder var personuppgifterna i den upphandlande enhetens register kommer att behandlas. Termen "behandling av uppgifter" kan ge en felaktig bild av att leverantören på något sätt aktivt behandlar uppgifter utanför EES-området. Enbart det att någon i leverantörens organisation potentiellt kan få tillgång till information i den upphandlande enhetens personregister utanför EES-området leder till att man separat ska avtala om behandlingen av uppgifter utanför EES-området med leverantören och säkerställa att behandlingen är ändamålsenlig.

Med "behandling" av uppgifter avses bland annat åtgärder beträffande personuppgifter, oberoende av om de utförs automatiserat eller ej, till exempel insamling, registrering, organisering, lagring, bearbetning, framtagning, läsning, användning, utlämning genom överföring, sammanförande eller förstöring.

Den upphandlande enheten och anbudsgivaren ska separat avtala om behandling av uppgifter utanför EES-området. Det här beror på att dataskyddsnivån i andra länder än EES-länderna inte nödvändigtvis motsvarar nivån enligt EU:s dataskyddsförordning. Till följd av överföringen kan nivån på skyddet av privatpersoners (registrerade) uppgifter äventyras. För överföring av personuppgifter ska dessutom finnas

en grund som fastställts i dataskyddsförordningen. Hur effektiv grunden för överföringen är och behovet av kompletterande skyddsåtgärder ska bedömas från fall till fall, så det rekommenderas att den expert som ansvarar för konkurrensutsättningen konsulterar en dataskyddsexpert gällande varje överföring av uppgifter utanför EES-området.

I dataskyddsförordningen fastställs grunder för överföring enligt vilka uppgifter får behandlas utanför EES-området. En grund för överföring kan till exempel vara Europeiska kommissionens beslut om en tillräcklig dataskyddsnivå i en viss stat. Sådana stater är till exempel Storbritannien, Schweiz, Japan och Nya Zeeland. Ett annat exempel på en grund för överföring är ett kontraktspaket som undertecknas mellan den upphandlande enheten och anbudsgivaren och som kallas kommissionens standardiserade dataskyddsbestämmelser. De standardiserade dataskyddsbestämmelserna kan användas för att ingå ett avtal i sig eller komplettera den upphandlande enhetens standardiserade dataskyddsvillkor. Kommissionens standardiserade dataskyddsbestämmelser är en tung och svårbegriplig helhet för användaren på grund av den dataskyddsterminologi som används i bestämmelserna, så det rekommenderas att upphandlande enheter tar hjälp av en expert.

Kommissionens standardiserade dataskyddsbestämmelser (kontraktsunderlag) och information om dem hittas [här](#).

5. Dataskydd i upphandlingsförfarandet

5.1 Dataskydd vid beredningen av en upphandling

När den expert som ansvarar för konkurrensutsättningen börjar bereda upphandlingen rekommenderas det att personen rutinmässigt kontrollerar med den substansexpert som ansvarar för upphandlingen om personuppgifter behandlas i upphandlingen. Även om den expert som ansvarar för konkurrensutsättningen ska hjälpa till att identifiera upphandlingar där personuppgifter behandlas, ligger ansvaret för dataskyddet dock i regel hos substansexperten.



Lämnar vi ut personuppgifter ur vårt register till tjänsteleverantören?

Samlar tjänsteleverantören in personuppgifter på vår begäran som en del av tjänsten?

Den expert som ansvarar för konkurrensutsättningen ska också säkerställa att överföringen av personuppgifter är nödvändig. Ibland kan en substansexpert svara jakande på den första frågan ovan av gammal vana, eftersom man kanske har gjort så tidigare. Dataskyddslagstiftningen förutsätter dock att personuppgifter behandlas endast då det är nödvändigt. Därmed är det skäl för konkurrensutsättningsexperten att försäkra sig om såväl behovet som hur länge behandlingen pågår.

Är utlämnandet av uppgifter till leverantören en nödvändig del av genomförandet av tjänsten?

Vilka personuppgifter är väsentliga och nödvändiga för att upphandlingen ska kunna genomföras (s.k. minimering av uppgifter)?

Kan behandlingen av personuppgifter tidsmässigt begränsas till exempel endast till början av kontraktsperioden eller måste uppgifter behandlas under hela kontraktsperioden?

Om personuppgifter behandlas i den tjänst som är föremål för upphandlingen ska detta beaktas när materialet i anbudsförfrågan utarbetas. Till materialet i anbudsförfrågan ska åtminstone bifogas ett utkast till ett avtal om behandling av personuppgifter eller till avtalsbilaga. Dessutom behöver den upphandlande enheten ofta också ställa obligatoriska krav på behandlingen av personuppgifter.

Det är viktigt att den expert som ansvarar för konkurrensutsättningen deltar i genomförandet av den upphandlande enhetens dataskyddsändanden enligt följande:

- Identifierar om personuppgifter behandlas i upphandlingen.
- Säkerställer att behandlingen av personuppgifter är nödvändig och att omfattningen av behandlingen begränsas.
- Om personuppgifter överförs i upphandlingen, bifogar organisationens mallvillkor för dataskydd till materialet i anbudsförfrågan.
- Säkerställer att substansexperten har kontrollerat att modellvillkoren är lämpliga.
- Säkerställer att man i datasäkerhetskraven beaktar att personuppgifterna skyddas tillräckligt, om detta inte redan har beaktats i den upphandlande enhetens mallvillkor för dataskydd.

Eftersom villkoren för behandling av personuppgifter blir en del av materialet i upphandlingen och kraven på upphandlingen, ska den som ansvarar för konkurrensutsättningen försäkra sig om att tolkningarna av personuppgifterna har gjorts på rätt sätt på samma sätt som för de övriga kraven i upphandlingen. Detta ska ske i samarbete med substansexperten och dataskyddsexperten. Den som ansvarar för konkurrensutsättningen behöver naturligtvis inte fatta beslut eller ta ställning till behandlingen av personuppgifter i oklara situationer, men personen ska uppmärksamma oklarheter. Om specifikationerna i anslutning till behandlingen av personuppgifter är oklara eller lämnar rum för tolkning ska den som ansvarar för konkurrensutsättningen antingen själv fråga en dataskyddsexpert om dataskyddsspecifikationerna eller delegera detta ansvar till substansexperten.

Fråga om personuppgifter – Säkerställ oklara – Bifoga villkoren – Delegera ansvaret

Beroende på föremålet för upphandlingen kan det vara motiverat att den upphandlande enheten utreder anbudsgivarnas processer för behandling av personuppgifter eller platsen för behandling av personuppgifter (läge inom EES-området). Den upphandlande enheten ska i sin definition av föremålet för upphandlingen överväga om placeringen av uppgifterna kan begränsas till EES-området och i vilka situationer det ska vara möjligt att överföra uppgifter utanför området för att åstadkomma tillräcklig konkurrens i upphandlingen. Utöver konkurrensen ska man i upphandlingen åtminstone beakta mängden personuppgifter och deras karaktär i den tjänst som är föremål för upphandlingen.

5.2 Dataskydd i upphandlingsförfarandet

5.2.1. Administrativa och funktionella krav

Om den tjänst som är föremål för upphandlingen inbegriper behandling av personuppgifter är det ofta motiverat att inkludera obligatoriska krav på genomförandet av datasäkerheten och dataskyddet i materialet i anbudsförfrågan. Det är ofta substansexperten som ansvarar för att utarbeta kraven, men det är bra om organisationen utarbetar mallar för kraven som är lätta att använda. Följande kravmallar är exempel på eventuella krav som ska redigeras utifrån organisationens behov och föremålet för upphandlingen:

Systemet ska följa och möjliggöra att alla registrerade rättigheter tillgodoses på det sätt som fastställts i EU:s och Finlands lagstiftning.

Leverantörens behandlingssystem och tjänster ska på ett effektivt sätt säkerställa att behandlingen av personuppgifter är säker och konfidentiell.

Leverantören ska omedelbart skicka alla begäranden om ändring och radering av eller mot av behandlingen av personuppgifter till de upphandlande enheterna. Leverantören ska på begäran av den upphandlande enheten stödja den upphandlande enheten i att uppfylla de begäranden som de registrerade lämnat in. Leverantören svarar inte själv på dessa begäranden.

Personuppgifter som ägs av den upphandlande enheten får inte användas för att utveckla eller testa leverantörens egna tjänster eller för leverantörens andra egna ändamål.

Leverantören har förmåga att tillhandahålla den upphandlande enhetens dataskyddsbeskrivning samt villkor för den upphandlande enhetens slutanvändare på överenskommet sätt.

Leverantören ska dokumentera alla överenskomna och genomförda skyddsåtgärder och säkerställa att alla dokument är uppdaterade. Leverantören och den upphandlande enheten bedömer regelbundet ovan nämnda tekniska skyddsåtgärder och skyddsåtgärder på organisationsnivå och deras tillräcklighet.

De funktionella kraven ska också fastställas enligt tjänsteleverantörernas mognadsnivå. Det är klart att behandlingen av särskilda kategorier av personuppgifter förutsätter mer avancerade dataskyddskrav. Det bör dock observeras att ju mindre anbudsgivarföretaget är, desto viktigare är det att ställa helt grundläggande krav på behandlingen av personuppgifter så att anbudsgivaren förstår sina skyldigheter. Till exempel en enskild näringsidkare har inte nödvändigtvis datasäkra system sedan tidigare. Då kan det vara nödvändigt att planera villkoren för behandlingen av uppgifter på en annan nivå än när man har att göra med större företag.

5.2.2 Utkast till dataskyddsavtal

Det rekommenderas att den upphandlande enheten utarbetar ett utkast till avtal om behandling av personuppgifter eller en avtalsbilaga om behandling

av personuppgifter. Organisationsspecifika avtalsmekanismer vid upphandlingar som omfattar behandling av personuppgifter varierar sällan särskilt mycket från ett föremål för upphandling till ett annat, även om en bedömning av villkorens lämplighet ska göras i varje enskilt fall.

Avtalsklausuler som gäller behandling av personuppgifter vid konkurrensutsatt upphandling bifogas anbudsförfrågan. De är en väsentlig del av villkoren för upphandlingen, eftersom villkor som hänför sig till dataskydd ibland påverkar anbudsgivarens beslut att delta i konkurrensutsättningen.

Avtalsvillkoren som berör dataskydd består i allmänhet av två delar:

1. Bestående, relativt oförändrade villkorsklausuler som organisationen fastställt vara nödvändiga, inklusive den upphandlande enhetens anvisningar om behandlingen av dess personuppgifter.
2. Punkter som ska fyllas i specifikt för varje upphandling och där det fastställs vilka uppgifter som överförs i just upphandlingen i fråga samt vad uppgifterna får användas till och när.

I de permanenta villkorspunkterna fastställs ofta:

- Parternas roller (vilken instans som är personuppgiftsansvarig och vilken instans som är personuppgiftsbiträde) och den personuppgiftsansvariges primära ansvar för att lagstiftningen följs.
- Leverantörens skyldigheter (leverantören följer kraven i den allmänna dataskyddsförordningen och den upphandlande enhetens anvisningar, har vidtagit ändamålsenliga tekniska och organisatoriska åtgärder för att behandla personuppgifterna på behörigt sätt, utser en person som ansvarar för dataskyddet, meddelar den upphandlande enheten om begäranden och kränkningar, skyldighet att bistå).
- Beställarens skyldigheter (upprätthåller och informerar om anvisningarna, utser en person som ansvarar för dataskyddet).
- Säkerställande av att personalen och underleverantören är medvetna om dataskydd och överföring av ansvar vidare till underleverantören, den upphandlande enhetens tillstånd att använda en underleverantör.
- Platsen för tjänsten.
- Avslutande av behandling av personuppgifter.

I de bestående punkterna kan den upphandlande enheten också specifikt för varje organisation fastställa praxis till exempel för felsituationer eller situationer av avtalsbrott som berör dataskyddet i fråga om särskilda hävnings- eller uppsägningsvillkor eller avtalsvite och skadestånd. När villkoren tillämpas ska anbudsgivarnas vilja att lämna ett anbud i upphandlingen beaktas, om villkoren är exceptionellt stränga. Om

man i upphandlingen till exempel fastställer ett villkor om hävning vid ett avtalsbrott, ska den upphandlande enheten på förhand fundera på hur tjänsten kan ordnas efter att kontraktet hävts, inklusive en ny tid för konkurrensutsättning. Den upphandlande enheten ska således alltid säkerställa att det finns en reservplan i en situation där den strikt kräver att ett beställarvänligt avtal följs.

I de bestående villkorspunkterna kan man också ta ställning till leverantörens eventuella företagsarrangemang under kontraktperioden. Enligt 136 § 2 mom. 4 punkten i lagen om offentlig upphandling och koncession (1397/2016) är det ofta möjligt att ändra upphandlingskontraktet vid företagsarrangemang och bedömningen ska göras från fall till fall. Även om ett byte av avtalspart skulle vara en tillåten ändring, kan man i villkoren för dataskyddet till exempel komma överens om att det förs nya förhandlingar om dataskyddsavtalet vid företagsarrangemang.

I praktiken kan de detaljer som fastställts för en enskild upphandling antingen vara olika alternativ som förtecknas i den upphandlande enhetens kontraktsmallar, varvid de som lämpar sig för upphandlingen väljs till exempel genom att de kryssas för, eller så kan det vara fråga om öppna punkter i kontraktet som ska fyllas i.

I upphandlingskontraktet ska man komma överens om förhållandet mellan det egentliga upphandlingskontraktet och dess bilagor, det vill säga i vilken ordning de tillämpas. Dataskyddsbilagan ska komma föra

Substansexperten på föremålet för upphandlingen ska delta i fastställandet av de villkor i dataskyddsvillkoren som är **specifika för upphandlingen**. Här fylls i till exempel:

Typer av personuppgifter och grupper av registrerade

- » Fyll i vilken kategori av personuppgifter som behandlas i upphandlingen (t.ex. den upphandlande enhetens anställda eller kunder) samt vilka uppgifter som överförs i upphandlingen (t.ex. arbetstagarens namn och användarnamn eller kundens namn, personbeteckning och bild).

Karaktären hos och syftet med behandlingen av personuppgifter

- » Fyll i varför och hur leverantören behandlar personuppgifter, till exempel: "Den upphandlande enheten beställer en installationstjänst för datorer av leverantören och därför ska leverantören behandla uppgifterna om de anställda vid den upphandlande enheten för att slutföra den användarspecifika installationen av datorerna".

Varaktigheten av behandling av personuppgifter.

- » Fyll i hur länge och i vilket skede av kontraktperioden leverantören behandlar personuppgifter, till exempel: "I samband med installationen av datorerna, därefter förstör leverantören personuppgifterna" eller "Under kontraktperioden".

Särskilda risker i anslutning till behandlingen av personuppgifter och nödvändiga skyddsåtgärder

- » Fyll i vilka risker situationen medför, hur säkerhetsnivån säkerställs och hur till exempel missbruk av personuppgifter eller lagstridig åtkomst till uppgifterna förhindras.

andra bilagor i tillämpningsordningen när det uppstår oklarheter i tolkningen av kontraktet ur ett dataskyddsperspektiv. I kontraktet kan till exempel följande mening anges: "Om ett dataskyddsavtal/en dataskyddsbilaga har fogats till kontraktet, tillämpas detta/denna i

första hand i förhållande till de övriga bilagorna."

Ledningsgruppen för digital säkerhet inom den offentliga förvaltningen (VAHTI) har på sin webbplats med anvisningar publicerat en mall för dataskyddsavtal och

dataskyddsbilaga som upphandlande enheter kan redigera och använda bland annat i sina upphandlingar. Alternativt kan mallarna användas som bakgrundsmaterial för att skapa en egen mall. Anvisningarna hittas på Myndigheten för digitalisering och befolkningsdatas webbplats under rubriken Verktyg och modeller ("Dataskyddsbilaga" (docx, 5/2023) och "Beskrivning av behandlingsåtgärder för personuppgifter" (docx, 5/2023): <https://dvv.fi/sv/publikationer-om-digital-sakerhet>

Även i rekommendationerna i kriterierna för bedömning av informationssäkerheten i den offentliga förvaltningen (Julkri) tas det ställning till behandlingen av personuppgifter: Kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen (Julkri): Rekommendation och kriterier – [Valto \(valtio-neuvosto.fi\)](https://valto.valtio-neuvosto.fi)

5.2.3 Förhandlingar om kontraktet

Ibland blir dataskyddsfrågor föremål för särskild diskussion i förhandlingarna om kontraktet. Det händer att utkastet till dataskyddsavtal i leverantörens organisation lämnas till dataskyddsexperten för kommentarer först efter att leverantören genom upphandlingsbeslutet har valts till leverantör i upphandlingen. I sådana fall kan leverantören försöka framföra även omfattande kommentarer till utkastet till dataskyddsavtal i efterhand.

Den upphandlande enheten ska komma ihåg att avtalsklausulerna om dataskydd har varit en del av materialet i anbudsförfrågan och därmed tillgängliga för alla anbudsgivare. Anbudsgivarna har lämnat anbud som grundar sig på anbudsförfrågan med beaktande av bland annat dataskyddsklausulerna. Därmed ska den upphandlande enheten förhålla sig försiktigt till att ens förhandla om dataskyddsklausulerna. När en anbudsgivare i sitt anbud har förbundit sig till en leverans enligt anbudsförfrågan, ska det inte finnas någon grund för att ändra sitt anbud ens i fråga om

dataskyddsklausulerna. Den upphandlande enheten är å sin sida förbjuden att ändra sitt material i anbudsförfrågan efter att konkurrensutsättningen avslutats i så väsentlig grad att det kan påverka slutresultatet av konkurrensutsättningen. Till exempel om behandling av personuppgifter inte tillåts i anbudsskedet, skulle ett avkall från detta krav och möjliggörande av en ändring efter att anbudstidens löpt ut sannolikt innebära en väsentlig och förbjuden ändring av kontraktet. När kontraktsvillkoren har varit med i anbudsförfarandet kan en anbudsgivare till exempel ha låtit bli att lämna ett anbud medan en annan tar någon risk i beaktande som en del av sin prissättning. Då skulle godkännandet av en ändring av villkoren ha kunnat ändra anbudsförfarandets slutresultat och därmed utgöra en förbjuden väsentlig ändring i upphandlingen.

5.2.4 Bedömning av dataskyddet vid flera upphandlingar från samma leverantör

Ibland upphandlar de upphandlande enheterna tjänster från samma leverantör med flera olika kontrakt. En sådan situation kan uppstå till exempel när samma leverantör vinner flera konkurrensutsättningar. Då ska dataskyddsfrågorna bedömas och avtalas separat för varje kontrakt.

Behovet av att avtala om dataskyddsfrågor specifikt för varje upphandling beror på att olika typer av personuppgifter kan överföras i olika upphandlingar (i en till exempel de anställdas användarnamn och e-postadresser och i en annan kundernas namn och IP-adresser) eller att personuppgifter kan behandlas av olika aktörer (till exempel har leverantören i en upphandling ingen underleverantör och i en annan finns det en underleverantör). Således gäller ett dataskyddsavtal som ingåtts med en viss leverantör inte någon annan upphandling än ett visst föremål för en upphandling. Ett dataskyddsavtal är inte ett allmänt avtal om alla dataöverföringar mellan den upphandlande enheten och en viss anbudsgivare, utan en upphandlingsspecifik specifikation av hur den personuppgiftsansvariges

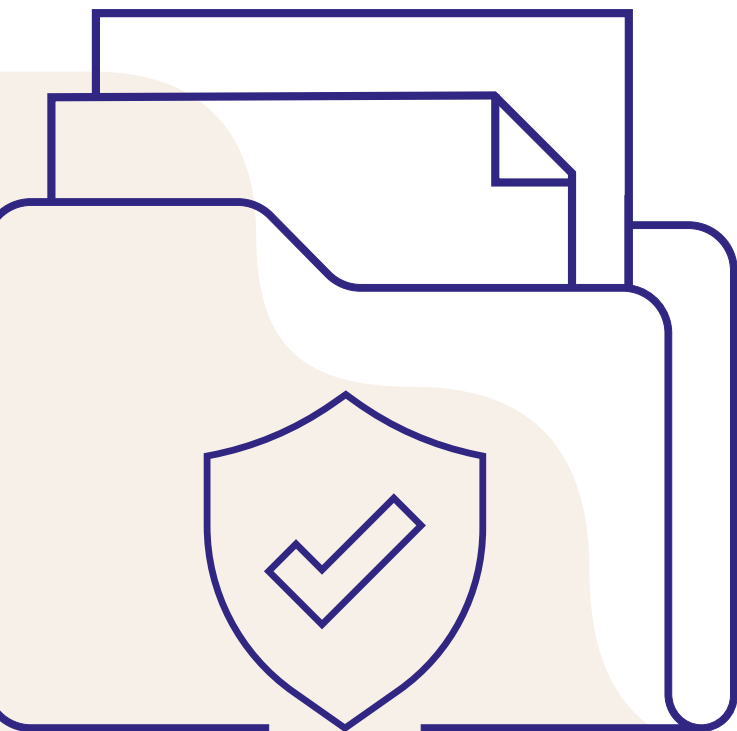
6. Dataskydd under kontraktperioden för en upphandling

Upphandlingsexpertens uppgifter i anslutning till dataskydd upphör ofta när kontraktperioden börjar. Liksom under planeringen av upphandlingen och konkurrensutsättningen fungerar substansexperter och eventuella dataskyddsexperter som ansvarspersoner i dataskyddsärenden när kontraktperioden inleds och medan den pågår. Det är dock bra att förstå att dataskyddsfrågor ofta är aktiva under hela kontraktperioden.

I det skede då kontraktet tas i bruk ska den upphandlande enheten och leverantören i samarbete skapa och starta de praktiska processerna i anslutning till dataskyddet (vem utför, i vilket system och vad), komma överens om det praktiska genomförandet av rapporteringsansvaret och de administrativa samarbetsorganens arbete.

Under kontraktperioden ska dataskyddssituationer aktivt följas upp och arrangemangen utvecklas. Under kontraktperioden kan praktiska tillvägagångssätt tas i bruk för att genomföra parternas ansvar. Den upphandlande enheten kan också behöva auditera, det vill säga granska, leverantörens dataskyddsprocesser.

När kontraktperioden löper ut ska leverantören sluta behandla den upphandlande enhetens personuppgifter och på ett kontrollerat sätt avsluta de åtgärder som hänför sig till uppgifterna. Leverantören ska återlämna den upphandlande enhetens personuppgifter. I praktiken sker detta genom att uppgifterna förstörs i leverantörens lagringsutrymmen. Beroende på tjänstens karaktär kan leverantören dock ha olika lagstadgade grunder eller andra grunder för att förvara uppgifterna i enlighet med kraven på förvaringstid även efter att tjänsten har upphört.



7. Dataskyddsbeskrivning för upphandlingar

Den upphandlande enheten ska utarbeta en dataskyddsbeskrivning för behandlingen av personuppgifter vid offentliga upphandlingar och lägga upp den så att den är allmänt tillgänglig på webbplatsen. Dataskyddsbeskrivningen är ett offentligt dokument med vilket den personuppgiftsansvarige informerar de registrerade om vilka uppgifter som samlas in om dem, varför och enligt vilka principer. Personuppgiftsansvarig är den aktör som fastställer ändamålen för behandlingen av personuppgifter.

I dataskyddsförordningen nämns inte ordet dataskyddsbeskrivning, men i GDPR-förordningen beskrivs om den personuppgiftsansvariges informationsskyldighet gentemot de registrerade (artiklarna 12–14) samt om skyldigheten att föra ett register över behandling som utförts under den personuppgiftsansvariges ansvar (artikel 30).

Enligt artikel 6.1 i EU:s dataskyddsförordning är behandlingen av personuppgifter laglig om åtminstone ett av villkoren i punkten är uppfyllt:

Artikel 6

1. Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:
 - a. Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.
 - b. Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

- c. Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.
- d. Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.
- e. Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.
- f. Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Vid upphandlande enheter är den allmänna rättsliga grunden för behandlingen av personuppgifter i dataskyddsbeskrivningen en rättslig förpliktelse (artikel 6 punkt 1 c). Den används till exempel när man behandlar personuppgifter för att genomföra upphandlingar genom konkurrensutsättning i enlighet med upphandlingslagen, granskar straffregisterutdrag eller utför inspektioner i anslutning till sanktioner.

En rättslig grund kan också vara till exempel ett allmänt intresse (artikel 6 punkt 1 e). Den kan användas till exempel när personuppgifter behandlas för att genomföra sådana upphandlingar som enligt upphandlingslagen inte ska konkurrensutsettas (till

exempel små upphandlingar eller undantag från upphandlingslagens tillämpningsområde) eller när personuppgifter behandlas för att genomföra marknadsundersökningar.

Den grund som presenteras i dataskyddsbeskrivningen för behandlingen av de personuppgifter som framställs i upphandlingen kan variera från organisation till organisation utifrån den upphandlande enhetens verksamhet eller skyldigheter.

Nyttiga länkar

- [Dataskyddsanvisningar för organisationer](#) | Dataombudsmannens byrå
- Modeller för dataskyddsavtal och behandlingsåtgärder för personuppgifter:
[Dataskyddsbilaga](#) (5/2023)
[Beskrivning av behandlingsåtgärder för personuppgifter](#) (5/2023)
- [Kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen](#) (Julkri): Rekommendation och kriterier
- [Kommissionens standardiserade dataskyddsbestämmelser](#)
Dataombudsmannens byrå

