kahn
pedersen

GDPR

och offentlig upphandling – en introduktion

Inledning

Dataskyddsförordningen är ett omfattande och komplext regelverk som inte är lätt att läsa och förstå. Denna kortfattade broschyr är att avsedd att ge en snabb och enkel ingång till regelverket samt några punkter att tänka på i samband med offentlig upphandling.

För att göra texten mer lättillgänglig beskrivs bestämmelserna i dataskydds-förordningen översiktligt och i förenklad form, vilket inte ger den fullständiga innebörden av bestämmelserna. Vi rekommenderar att ni tar del av data-skyddsförordningen och annan mer detaljerad vägledning om den vid för-beredelserna inför en offentlig upphandling.

Vad är dataskyddsförordningen (GDPR)?

Dataskyddsförordningen[1] även kallad GDPR efter dess engelska förkortning ska tillämpas från och med den 25 maj 2018. Syftet med dataskyddsförord-ningen är att öka integritetsskyddet för individer samtidigt som d et ska underlätta för företag m.fl. att göra affärer inom EU/EES-området. Det förverkligas bl.a. genom att individer får mer kontroll över sina **personuppgifter**.

Dataskyddsförordningen innebär stora förändringar för många organisationer – t.ex. myndigheter och företag – vid hanteringen av personuppgifter. Även om större delen av bestämmelserna i dataskyddsförordningen i sak motsvarar be-stämmelserna i den tidigare regleringen (personuppgiftslagen), ställs i data-skyddsförordningen väsentligt högre krav på förebyggande åtgärder. Den som behandlar personuppgifter måste därför ha mer ordning och reda i den personuppgiftsbehandling som förekommer inom organisationen. Vidare tillkommer utökade och nya skyldigheter. För att understryka vikten av ett ökat integritetsskydd kommer Datainspektionen att få möjlighet att utdöma höga sanktionsavgifter mot de som inte följer bestämmelserna i den nya dataskyddsförordningen.

Dataskyddsförordningen kommer att gälla i alla medlemsstater i EU samt inom EES-området. Den enhetliga regleringen inom EU syftar till att öka den fria rörligheten och underlätta handeln på den inre marknaden. I vissa delar tillåts dock medlemsstaterna precisera tillämpningen av bestämmelserna i data-skyddsförordningen, särskilt för personuppgiftsbehandling som sker inom den offentliga sektorn.

---

[1]Europaparlamentets och rådets 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).

De viktigaste nyheterna

Dataskyddsförordningen innehåller ett antal större nyheter i integritetsskyddet. Några av de viktigaste är följande.

- Den svenska s.k. **missbruksregeln försvinner**. Missbruksregeln var avsedd att förenkla personuppgiftshanteringen i löpande texter, epost, webbpublicering m.m. Med dataskyddsförordningen måste samtliga bestämmelser tillämpas även när personuppgifter behandlas i sådana sammanhang.
- Det blir hårdare krav för att samla in giltigt **samtycke** för att få behandla någons personuppgifter och möjligheterna för myndigheter att stödja sin behandling på samtycke begränsas ytterligare.
- Skyldigheten att **informera den registrerade** blir mer omfattande och det ställs krav på att informationen ska vara lättillgänglig både till innehåll och form.
- Den registrerade får en rätt till s.k. **dataportabilitet** som i korthet innebär att den registrerade ska kunna flytta sina personuppgifter från ett företag till ett annat.
- Den som behandlar personuppgifter omfattas av principen om a**nsvarsskyldighet** och måste kunna visa på vilket sätt den följer bestämmelserna dataskyddsförordningen.
- Den som behandlar personuppgifter för någon annans räkning, ett **personuppgiftsbiträde**, får ett självständigt ansvar i förhållande till den registrerade och tillsynsmyndigheten.
- Den som ägnar sig åt personuppgiftsbehandling som innebär särskilda risker för de registrerade kan bli skyldig att upprätta en s.k. **konsekvensanalys** för att kunna bedöma riskerna och bl.a. vidta åtgärder för att minska dem.
- Om det inträffar en **säkerhetsincident**, till exempel ett dataintrång eller en oavsiktlig förlust av uppgifter, måste den personuppgiftsansvarige anmäla detta till Datainspektionen inom 72 timmar.
- Myndigheter, företag och organisationer som ägnar sig åt vissa former av integritetskänslig personuppgiftsbehandling är skyldiga att utse ett s.k. **dataskyddsombud**.
- Datainspektionen kan komma att utdöma s.k. **sanktionsavgift** på betydande belopp för den som bryter mot bestämmelserna i dataskyddsförordningen.

Grundläggande principer

I dataskyddsförordningen anges ett antal grundläggande principer som är vägledande för all behandling av personuppgifter. Förenklat och i korthet innebär de följande.

- All behandling av personuppgifter måste utföras enligt dataskyddsförordningen (**laglighet**).
- All behandling ska vara **skälig, rättvis och öppen** mot de individer som personuppgifterna avser (de registrerade), vilket bl.a. kan innebära att den personuppgiftsansvarige ska följa god sed på det aktuella området och behandla uppgifter på det sätt som man har angivit i t.ex. policies.
- Innan behandling av personuppgifter påbörjas måste **ändamålet** med behandlingen bestämmas. Utan ett angivet berättigat ändamål får personuppgifterna inte behandlas.
- Uppgifterna får inte behandlas för **andra ändamål** som inte är förenliga med det ändamål för vilket uppgifterna samlades in.
- Alla uppgifter som behandlas ska vara **relevanta** för det angivna ändamålet och inte vara fler än vad som behövs för ändamålet, dvs. inga ”bra-att-ha-uppgifter” får sparas.
- Alla uppgifter ska dessutom vara **korrekta** i förhållandet till ändamålet. Exempelvis är en läkares felaktiga diagnos korrekt om ändamålet är att dokumentera alla diagnoser, men den kan behöva kompletteras med uppgifter om att läkaren senare har ändrat diagnosen.
- Uppgifterna måste hållas **uppdaterade** om ändamålet med behandlingen kräver det. Däremot behöver t.ex. inte historiska uppgifter i arkiv uppdateras.
- När uppgifterna inte längre behövs för det ändamål för vilket de samlades in, ska de **raderas eller avidentifieras**. Om personuppgifterna behandlas för flera ändamål kan de dock få sparas för de kvarstående ändamålen.
- Personuppgifterna ska skyddas med en lämplig **skyddsnivå** med hjälp av tekniska och organisatoriska åtgärder så att inte obehöriga (inom eller utanför organisationen) får tillgång till dem, och så att de inte går förlorade eller blir förvanskade.

När gäller dataskyddsförordningen?

Dataskyddsförordningen har ett mycket brett tillämpningsområde. Den gäller för all, **helt eller delvis, automatiserad behandling** av personuppgifter oavsett om den sker i register, databaser eller s.k. ostrukturerad data. Den gäller alla former av behandling, t.ex. insamling, registrering, lagring, läsning på en skärm, överföring, spridning, radering m.m. I vissa fall gäller dataskyddsförordningen även för behandling av uppgifter som finns **på papper**, t.ex. utskrifter från ett ärendehanteringssystem eller i ett pärmsystem som är sökbart på minst två olika typer av personuppgifter.

Med **personuppgifter** avses alla upplysningar som avser en identifierad eller identifierbar fysisk person, oavsett om identifieringen sker direkt, t.ex. genom namn eller personnummer eller indirekt, t.ex. genom en epost-adress eller en lokaliseringsuppgift. Observera att både text, bild och ljud omfattas av begreppet.

Dataskyddsförordningen gäller inte för behandling av personuppgifter som sker **privat** inom en begränsad vänkrets. Den gäller inte heller sådan behandling av personuppgifter som sker av medier som omfattas av grundlagsskyddet för yttrandefrihet eller när någon annan utnyttjar sin **yttrandefrihet** för att t.ex. skapa opinion. För **brottsbekämpande** myndigheter gäller annan lagstiftning i stället för dataskyddsförordningen.

Vem ansvarar och vem gör vad?

Personuppgiftsansvarig är den som bestämmer varför personuppgifterna ska behandlas och på vilket sätt (ändamål och medel). Den personuppgiftsansvarige bär huvudansvaret enligt dataskyddsförordningen och är normalt ett företag, en myndighet eller en organisation. Om flera företag eller organisationer tillsammans bestämmer över behandlingen av personuppgifterna kan de ha ett gemensamt personuppgiftsansvar.

Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning, t.ex. tillhandahållaren av en serverhall, konsultbolaget som bemannar en funktion hos den personuppgiftsansvarige, en redovisningsbyrå eller ett IT-bolag som den personuppgiftsansvarige har anlitat. I många upphandlade avtal är den anlitade leverantören personuppgiftsbiträde. En nyhet i dataskyddsförordningen är att även biträden bär ett visst ansvar för behandlingen, bl.a. vad gäller skyldigheten att skydda personuppgifterna med tekniska och organisatoriska säkerhetsåtgärder. Förhållandet mellan den personuppgiftsansvarige och personuppgiftsbiträdet ska regleras i ett personuppgiftsbiträdesavtal.

Dataskyddsombudet är i vissa fall utsett av den personuppgiftsansvarige eller personuppgiftsbiträdet för att övervaka att organisationen uppfyller kraven enligt dataskyddsförordningen. Ombudet ger även råd för att förbättra efter-levnaden och informerar om behandlingen. Dataskyddsombudet har inget personligt ansvar för personuppgiftsbehandlingen. Dataskyddsombud ersätter personuppgiftsombud som rollen kallades enligt personuppgiftslagen.

Anställda och andra personer som behandlar personuppgifter i tjänsten hos den personuppgiftsansvarige eller personuppgiftsbiträdet får bara behandla personuppgifterna enligt instruktioner. De bär inget personligt ansvar.

Den registrerade är den vars personuppgifter behandlas. Den registrerade har rättigheter gentemot den personuppgiftsansvarige.

När är det tillåtet att behandla personuppgifter?

När personuppgifter ska behandlas måste det – förutom att ett berättigat ändamål – finnas en rättslig grund för behandlingen. Det finns sex sådana grunder.

1. **Samtycke** från den registrerade. Samtycke förutsätter bl.a. att den enskilde har en verklig valmöjlighet att avstå och att senare kunna återkalla samtycket. Av det skälet anses det vara svårt för myndigheter och arbetsgivare att samla in giltiga samtycken från enskilda och arbetstagare.
2. Om det är nödvändigt för att fullgöra ett **avtal** med den registrerade eller för att vidta åtgärder på begäran av den registrerade innan ett avtal ingås, t.ex. att ta en kreditupplysning.
3. Om det är nödvändigt för att fullgöra en **rättslig förpliktelse** som framgår av svensk lag, myndighetsbeslut eller EU-rätt. Inom arbetsrätten kan rättsliga förpliktelser också framgå av kollektivavtal.
4. Om det är nödvändigt för att skydda **intressen av grundläggande betydelse** för den registrerade eller någon annan fysisk person, t.ex. om den registrerade är medvetslös och inte kan lämna sitt samtycke.
5. Om det är nödvändigt för att utföra en **uppgift av allmänt intresse** eller som ett led i **myndighetsutövning**. Det är med dessa grunder som myndigheter och kommuner kan behandla personuppgifter i sina verksamheter när de agerar som myndigheter. En uppgift av allmänt intresse måste framgå av EU-rätten, svenska lag eller myndighetsbeslut eller kollektivavtal. Vid myndighetsutövning måste det finnas stöd i lag. Det förhållandet att upphandling inte innebär myndighetsutövning saknar i detta sammanhang betydelse.

6. Om det är nödvändigt för ett **berättigat intresse** som väger tyngre än den registrerades intressen och dennes fri- och rättigheter. Ett sådant berättigat intresse kan vara marknadsföring eller att förhindra bedrägeri.

Observera att det krävs att behandlingen är nödvändig (utom för samtycke) för att behandlingen ska få utföras. Det innebär bl.a. att man inte kan ta med personuppgifter som inte behöver behandlas. Det är t.ex. en rättslig förpliktelse att bokföra ekonomiska transaktioner i näringsverksamhet. Det kan innebära att man också måste registrera personuppgifter vid bokföringen, vilket är tillåtet så länge de krävs för att uppfylla skyldigheten enligt bokföringslagen.

Känsliga personuppgifter m.m.

Behandling av vissa kategorier av personuppgifter har ansetts vara förenad med särskilda integritetsrisker och för att få behandla sådana uppgifter krävs det enligt dataskyddsförordningen särskilt rättsligt stöd. Exempelvis kan det krävas ett särskilt uttryckligt samtycke från den registrerade för att få behandla personuppgifter om hälsa. Behandling av sådana uppgifter kräver också särskilda överväganden, t.ex. om behovet av högre säkerhet och i vissa fall krav på att göra en s.k. konsekvensanalys.

En kategori av personuppgifter som det krävs särskilt stöd för att få behandla är s.k. **känsliga personuppgifter**, dvs. uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, uppgifter om hälsa, sexualliv, sexuell läggning samt genetiska personuppgifter och vissa biometriska personuppgifter. Känsliga personuppgifter får bara behandlas om det finns stöd i t.ex. den registrerades uttryckliga samtycke, behandlingen är nödvändig för att fullgöra skyldigheter inom arbetsrätten, göra gällande rättsliga anspråk, för hälso- och sjukvård eller ett viktigt allmänt intresse.

Datainspektionen anser att det även behövs särskilt starka skäl för att få behandla s.k. **integritetskänsliga personuppgifte**r bl.a. uppgifter om enskild persons privatekonomi.

När andra än myndigheter behandlar **personuppgifter om lagöverträdelser** och brott måste det också finnas ett särskilt stöd för sådan behandling i svensk lag, i föreskrift eller särskilt beslut från Datainspektionen. Detta bör särskilt beak-tas vid hantering av personuppgifter i samband med prövning enligt uteslutningsgrunderna i LOU och LUF.

För att få använda **personnummer** utan samtycke krävs det att det är klart motiverat utifrån ändamålet med behandlingen, vikten av säker identifiering eller något annat beaktansvärt skäl.

Tänk på att behandling av känsliga personuppgifter, integritetskänsliga personuppgifter, personuppgifter om lagöverträdelse och personnummer ställer högre **krav på säkerhet** än annars. Datainspektionen har t.ex. ansett att överföring av känsliga personuppgifter och integritetskänsliga personuppgifter via ett öppet nät kräver kryptering och stark autentisering.

Överföring till länder utanför EU/EES

För att få föra över personuppgifter till länder utanför EU/EES (tredjeland) krävs särskilt grund i dataskyddsförordningen t.ex. att beslut av EU-kommissionen om att det mottagande landet har tillräckligt skydd för personuppgifter s.k. adekvat skyddsnivå. Även s.k. bindande företagsbestämmelser som gäller inom en koncern eller grupp av företag som deltar gemensam ekonomisk verksamhet kan utgöra en rättslig grund för överföring till länder utanför EU/EES. När överföringen sker till ett företag utanför en koncern e.d. kan stöd även ges i s.k. standardavtalsklausuler. EU-kommissionen har godkänt tre sådana standar-davtalsklausuler som kan användas i olika sammanhang, dels vid överföring från en personuppgiftsansvarig till en personuppgiftsansvarig utanför EU/EES, dels vid överföring från en personuppgiftsansvarig inom EU/EES till ett personupp-giftsbiträde utanför EU/EES.

Vid upphandling av molntjänster är det vanligt att överföring sker av personuppgifter till land utanför EU/EES. Det är i sådana fall viktigt att den upphandlande myndigheten har kontroll i vilka länder personuppgifter kommer att behandlas oavsett om den sker hos leverantören eller dennes underleverantörer.

De registrerade har rättigheter

Dataskyddsförordningen ger de registrerade vissa rättigheter som den personuppgiftsansvarige måste respektera. Den personuppgiftsansvarige måste också underlätta för de registrerade att utöva sina rättigheter bl.a. genom att i förväg vidta åtgärder för att ska vara möjligt att svara upp mot en begäran om t.ex. rättelse.

De registrerades rättigheter är följande.

1. Rätt till **information** om att hans eller hennes personuppgifter behandlas. Information ska ges både då personuppgifter samlas in och senare om den registrerade begär det (s.k. registerutdrag).

2. Rätt till **rättelse** av personuppgifter som är felaktiga eller till komplettering av ofullständiga uppgifter.

3. Rätt till **radering** av personuppgifter i vissa fall, bl.a. när uppgifter inte längre behövs för det ändamål som de samlades in eller då ett samtycke återkallas och det inte finns någon annan rättslig grund för behandlingen.

4. Rätt till **begränsning** av behandling t.ex. under tiden som den personuppgiftsansvarige kontrollerar om uppgifterna är korrekta efter att den registrerade har begärt rättelse.

5. Rätt till **dataportabilitet** vilket innebär att den registrerade under vissa förutsättningar kan begära att uppgifter som han eller hon har tillhandahållit den personuppgiftsansvarige ska lämnas ut till honom eller henne i ett elektroniskt format som gör det möjligt att föra över dem en annan personuppgiftsansvarigs tjänst, eller att uppgifter överförs direkt till annan personuppgiftsansvarig.

6. Rätt att göra **invändningar** mot personuppgiftsbehandling som sker för en uppgift av allmänt intresse, som ett led i myndighetsutövning eller efter en intresseavvägning. Vid invändningar mot behandling som sker för direkt marknadsföring måste behandlingen upphöra.

7. Rätt att inte bli föremål för **automatiserat beslutsfattande inklusive profilering**.

Rättigheterna som de registrerades ges i dataskyddsförordningen kan begränsas i nationell rätt. Sverige har utnyttjat den möjligheten och har bl.a. begränsat den information som måste tas med i s.k. registerutdrag.

Skyldigheter för de som behandlar personuppgifter

Med personuppgiftsansvaret kommer ett antal skyldigheter. I några fall gäller dessa skyldigheter även personuppgiftsbiträden. Förutom att de ovan angivna skyldigheterna – att respektera de grundläggande principerna, att ha rättsligt stöd för behandlingen och att respektera de registrerades rättigheter – anges bl.a. följande skyldigheter i dataskyddsförordningen.

- Skyldighet att upprätta och föra en **förteckning över alla personuppgiftsbehandlingar** som organisationen har ett personuppgiftsansvar för.

- Skyldighet att anlita endast sådana personuppgiftsbiträden som lämnar tillräckliga garantier för att de följer dataskyddsförordningen och att reglera förhållandet till biträdet i ett skriftligt personuppgiftsbiträdesavtal

- Om det finns ett **gemensamt personuppgiftsansvar** ska förhållandet mellan de gemensamt personuppgiftsansvariga fastställas i ett ”inbördes arrangemang”.

- Skyldighet att låta integritetsskyddet – särskilt de grundläggande principerna (se ovan) – påverka utformningen av IT-system men även deras användning och avveckling (**privacy by design**), t.ex. genom att minimera antalet personuppgifter som ska registreras eller begränsa åtkomsten till person-

uppgifterna till de handläggare som behöver upp-gifterna i tjänsten. Det finns även en skyldighet att se till att eventuella inställningar m.m. är förinställda så att de minskar integritetsriskerna genom att styra användaren mot ett integritetssäkert arbetssätt (**privacy by default**) t.ex. genom att minska bevarandetid eller spridningen av personuppgifterna.

- Myndigheter och offentliga organ måste utse ett **dataskyddsombud** som bl.a. ska övervaka organisationens efterlevnad av dataskydds-förordningen. Andra än myndigheter har vissa fall en skyldighet att utse dataskyddsombud.

- De personuppgiftsansvariga som ägnar sig åt mer integritetskänslig personuppgiftsbehandling har i vissa fall skyldighet att göra en s.k. **konsekvensbedömning** i syfte att kartlägga de särskilda riskerna, väga dem mot fördelarna och vidta åtgärder för att minska riskerna. En sådan konsekvensbedömning kan behövas vid t.ex. omfattande behandling av känsliga personuppgifter eller uppgifter om brott. Om riskerna inte går att undanröja ska den personuppgiftsansvarige begära ett **förhands-samråd** med Datainspektionen.

- Personuppgiftsansvariga har en skyldighet att **skydda personuppgifterna** från att förstörelse, förvanskning eller åtkomst av obehöriga. Den person-uppgiftsansvarige måste därför vidta åtgärder tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

- Personuppgiftsansvariga har en skyldighet att **anmäla säkerhetsincidenter** till Datainspektionen. Det kan t.ex. handla om att organisationen har blivit utsatt för ett dataintrång som innebär att obehöriga kan ha fått åtkomst till personuppgifter. Anmälan ska göras utan dröjsmål och inte senare än 72 timmar efter att den personuppgiftsansvarige fick kännedom om incidenten.

Dataskyddsförordningen och offentlighetsprincipen

Dataskyddsförordningen innebär inget hinder för myndigheter och andra som omfattas av offentlighetsprincipen att söka fram och sammanställa uppgifter ur allmänna handlingar, även om de innehåller personuppgifter, när det är nödvändigt för att kunna ge tillgång till allmänna handlingar enligt tryckfri-hetsförordningen.

Vid utlämnandet av sådana personuppgifter måste en sedvanlig sekretess-prövning göras. Observera att sekretess gäller för personuppgifter om det kan

antas att uppgifterna efter utlämnandet kommer att behandlas i strid med dataskyddsförordningen.

Det finns ingen generell skyldighet att lämna ut uppgifterna elektroniskt t.ex. via epost. Om uppgifterna inte omfattas av sekretess och myndigheten vill lämna ut uppgifterna via epost måste en bedömning göras enligt dataskyddsförordningen. Enligt Datainspektionens praxis innebär det att känsliga personuppgifter och integritetskänsliga personuppgifter normalt inte kan skickas via vanlig epost. Det är t.ex. inte möjligt att skicka lönespecifikationer eller patientuppgifter via epost.

Hur förbereder sig en organisation inför dataskyddsförordningen?

Förberedelsearbetet

Även om huvuddelen av bestämmelserna i dataskyddsförordningen har gällt enligt personuppgiftslagen sedan länge finns det anledning att ta ett krafttag kring alla frågor om behandling av personuppgifter inom organisationen. Det innebär bl.a. följande.

- Se till att organisationen blir medveten om reglerna
- Skapa en intern organisation för förberedelsearbete och för det löpande uppföljningsarbetet
- Kartlägga all behandling av personuppgifter inom organisationen (se nedan)
- Bedöm vilka integritetsrisker som finns
- Bedöm med vilket rättsligt stöd som personuppgifter kan behandlas, känsliga personuppgifter, uppgifter om brott, personnummer, överföring till tredje land
- Bedöm om ett dataskyddsombud behöver utses
- Dokumentera alla bedömningar
- Se över avtal med personuppgiftsbiträden och andra personuppgiftsansvariga
- Se över informationen till de registrerade
- Utbilda alla berörda inom organisationen

När förberedelserna är genomförda kan det vara lämpligt att kontrollera genomförandet och testa om organisationen är redo. Det kan ske genom en testinspektion (s.k. mock-audit).

Kartlägg hur personuppgifter behandlas

Varje **personuppgiftsansvarig** är skyldiga att upprätta en förteckning över samtliga behandlingar som utförs inom organisationen. Förteckningen ska upprättas skriftligen på papper eller i elektronisk form och ska kunna visas upp för tillsynsmyndigheten. Enligt dataskyddsförordningen ska förteckningen innehålla följande.

- Namn och kontaktuppgifter till den personuppgiftsansvarige
- Ändamålen med behandlingen
- Kategorier av registrerade, t.ex. anställda, kunder
- Kategorier av personuppgifter, t.ex. kontaktuppgifter, sjukfrånvaro
- Kategorier av mottagare till vilka personuppgifterna har lämnats ut
- Om personuppgifterna överförs till länder utanför EU/EES-området
- Om möjligt, gallringstider
- Om möjligt, beskrivning av tekniska och organisatoriska säkerhetsåtgärder

Även **personuppgiftsbiträden** är skyldiga att upprätta en förteckning över de kategorier av behandlingar av personuppgifter som de utför åt personuppgiftsansvariga. Den ska innehålla följande.

- Namn och kontaktuppgifter till personuppgiftsbiträdet
- Namn och kontaktuppgifter till personuppgiftsansvariga för vilka behandling av personuppgifter utförs
- Kategorier av behandlingar som utförts för varje personuppgiftsansvariges räkning
- Överföring av personuppgifter till länder utanför EU/EES-området
- Om möjligt, beskrivning av tekniska och organisatoriska säkerhetsåtgärder

Utöver de obligatoriska uppgifterna i förteckningarna **rekommenderar** vi att en personuppgiftsansvarig även tar med bl.a. följande.

- Med vilket rättsligt stöd de aktuella personuppgifterna behandlas, även för känsliga personuppgifter, uppgifter om lagöverträdelse, personnummer
- En beskrivning av flödet, dvs. hur personuppgifter samlas in och behandlas och slutligen raderas, bl.a. vilka IT-system som används
- Vilken information de registrerade har fått vid insamlingen av personuppgifterna
- Om det förekommer automatiserat beslutsfattande och profilering

- De särskilda dataskyddsrisker som den aktuella behandlingen kan innebära
- Vilka som har åtkomst till personuppgifterna
- Om personuppgiftsbehandlingen omfattas av särskilda regler om t.ex. särskilda svenska regler om personuppgiftsbehandling (s.k. registerförfattningar), arkivering eller sekretess
- Hur rutiner för att tillgodose de registrerades rättigheter ser ut, t.ex. hur s.k. registerutdrag ska kunna lämnas ut, eller hur en begäran om rättelse eller radering ska utföras för de aktuella personuppgifterna

Dataskyddsförordningens praktiska konsekvenser vid offentliga upphandlingar

Många upphandlingar innebär att leverantören ska behandla personuppgifter för den upphandlande myndighetens räkning. Det innebär att leverantören får ställning som personuppgiftsbiträde enligt dataskyddsförordningen.

De praktiska konsekvenserna som dataskyddsförordningen medför i upphandlingar måste kartläggas i varje enskilt fall. Konsekvenserna beror bl.a. på föremålet för upphandlingen och vilka personuppgifter som kommer att behandlas i det aktuella ärendet. En upphandling av exempelvis molntjänster som ska användas vid översättning av myndighetsdokument eller domar innehållande stora mängder känsliga personuppgifter eller uppgifter om brott, ställer av naturliga skäl större krav på noggrannhet och förberedelser, än en upphandling av ett system som i princip endast kommer att innehålla kontaktuppgifter till personer.

Att anlita personuppgiftsbiträden

Som personuppgiftsansvarig har en upphandlande myndighet skyldighet att endast anlita leverantörer (personuppgiftsbiträden) som kan lämna tillräckliga garantier för att de genomför tekniska och organisatoriska åtgärder så att den personuppgiftsbehandling som kommer utföras med anledning av upphandlingen, uppfyller kraven enligt dataskyddsförordningen och att de registrerades rättigheter skyddas. Det innebär att den upphandlande myndigheten i upphandlingen måste ställa krav på leverantörerna i detta avseende. Beroende på omfattningen och inriktningen av personuppgiftsbehandlingen krävs bl.a. att leverantörerna har tillräcklig sakkunskap och nödvändiga resurser framför allt vad gäller säkerhet i samband med behandlingen. Ett ätt för leverantörer att visa att de uppfyller sådana krav är att ansluta sig till en godkänd uppförandekod eller certifiering. Det finns ännu inga sådana uppförandekoder eller certifieringar men flera lär bli godkända under de

kommande åren, bl.a. arbetar Cloud Select Industry Group (C-SIG) med att ta fram en uppförandekod för molntjänster the Data Protection Code of Conduct for Cloud Service Providers. Om den upphandlande myndigheten väljer att ställa krav på viss certifiering, märkning eller liknande är det dock viktigt att det sker i enlighet med bestämmelserna i 9 kap. 12-15 §§ LOU.

Förhållandet mellan den personuppgiftsansvariga myndigheten och leverantören som agerar som personuppgiftsbiträde måste regleras i ett personuppgiftsbiträdesavtal eller annan bindande rättsakt.

Observera att ett personuppgiftsbiträde endast får behandla personuppgifter enligt instruktioner från den personuppgiftsansvarige, dvs. biträdet får inte behandla personuppgifterna för egna ändamål t.ex. för att förbättra tjänsterna. Det är den upphandlande myndigheten som måste förse leverantören med instruktioner eller godkänna de instruktioner som leverantören föreslår.

Rollfördelningen

Den upphandlande myndighetens och leverantörens förhållande bör vara klarlagt redan i förfrågningsunderlaget. Rollfördelningen ska tydligt framgå. Är myndigheten och leverantören gemensamt personuppgiftsansvariga? Eller är det bara myndigheten som ska ha sådana skyldigheter som följer med rollen som personuppgiftsansvarig?

Leverantörer som får rollen som personuppgiftsbiträden ska ha i åtanke att även denna roll medför självständiga skyldigheter som kan aktualisera sanktioner.

Vem som bär ett personuppgiftsansvar beror på vem eller vilka som bestämmer ändamål och medel för personuppgiftshanteringen, dvs. varför och hur behandlingen ska utföras. Är det flera som tillsammans tar dessa beslut kan de vara gemensamt personuppgiftsansvariga. När många parter är inblandade i ett samarbete där det ingår personuppgiftsbehandling kan det vara svårt att avgöra vem eller vilka som är personuppgiftsansvariga respektive personuppgiftsbiträden. Graden av självbestämmande och manöverutrymme i beslutsfat-tandet utgör i dessa fall utgångspunkter för bedömningen. Dataskyddsförordningen ställer krav på att förhållandet till personuppgiftsbiträdet regleras i ett avtal eller annan rättsakt och att förhållandet mellan gemensamt personuppgiftsansvariga ska fastställas i ett ”inbördes arrangemang”.

Aktörer som använder eller annars deltar i komplexa tjänster/samarbeten bör således först reda ut och dokumentera vilka personuppgiftsbehandlingar som aktualiseras och därefter – i den mån samordnade behandlingar identifieras – sinsemellan reda ut hur personuppgiftsansvaret ska delas och utövas i praktiken.

Läs mer i ”Att fördela personuppgiftsansvar under GDPR – en enkel sak?”, i Kahn Pedersens rapport, GDPR – några tillämpningsfrågor.

Bifoga villkoren för personuppgiftsbehandlingen

Den upphandlande myndigheten måste bifoga villkoren för personuppgiftsbehandlingen till förfrågningsunderlaget. Bilagan kan utgöra ett utkast till ett personuppgiftsbiträdesavtal mellan den personuppgiftsansvarige och personuppgiftsbiträdet. I avtalet bör det framgå att personuppgiftsbiträdet endast får behandla personuppgifterna efter instruktioner från den personuppgiftsansvarige.

Anpassning av befintliga personuppgiftsbiträdesavtal

Det kan finnas behov av att gå igenom tidigare personuppgiftsbiträdesavtal och eventuellt justera dem så att de uppfyller kraven i dataskyddsförordningen. Även om kraven i dataskyddsförordningen i stort sett överensstämmer med det som har ansetts gälla redan tidigare är det vanligt att biträdesavtal under personuppgiftslagen många gånger har ingåtts närmast slentrianmässigt och utan större diskussion eller förhandling mellan parterna. Dessutom är det, enligt vår erfarenhet, mycket sällan som biträdesavtal enligt personuppgiftslagen tydligt specificerar vilka uppgifter och vilken behandling som omfattas av avtalet.

Det ska också sägas att personuppgiftsbiträdets nya roll under dataskyddsförordningen, med utökat ansvar och skärpta sanktioner, kan medföra att befintliga personuppgiftsbiträdesavtal under alla omständigheter kan behöva ändras.

Läs mer i ”Behöver befintliga personuppgiftsbiträdesavtal ändras?”, i Kahn Pedersens rapport, GDPR – några tillämpningsfrågor.

Konflikt med LOU

Behovet av att anpassa befintliga personuppgiftsbiträdesavtal till kraven som anges i dataskyddsförordningen kan utlösa en konflikt med bestämmelserna i LOU. Ett förändringsbehov, i den mån ett sådant finns, föranleder en särskild problematik i upphandlingsrättsligt hänseende, eftersom upphandlande myndigheter har begränsade möjligheter att göra ändringar i befintliga kontrakt.

Huvudregeln är att bestämmelserna i ett kontrakt eller ett ramavtal inte får ändras utan att det genomförs en ny annonserad upphandling. Det finns emellertid ett antal undantag som innebär att ett befintligt kontrakt eller ramavtal får ändras utan en ny upphandling. Under vissa förutsättningar får

sådana ändringar ske när det handlar om ändringar av mindre värde, ändringar i enlighet med ändringsklausul, nödvändiga kompletterande beställningar, ändringar till följd av oförutsebara omständigheter samt ändringar som inte är väsentliga. Även om det är möjligt att göra ändringar i ett kontrakt eller ett ramavtal med stöd av de angivna undantagen har den upphandlande myndigheten ändå en skyldighet att, rent upplysningsvis, annonsera ändringar som föranletts av oförutsebara omständigheter respektive kompletterande beställningar.

Läs mer i ”GDPR vs LOU; särskilt om ”väsentlig ändring” i offentliga kontrakt”, i Kahn Pedersens rapport, GDPR – några tillämpningsfrågor.

Underbiträden

Om leverantören (personuppgiftsbiträdet) vill anlita en underleverantör (ett underbiträde) måste den upphandlande myndigheten (den personuppgiftsansvarige) godkänna detta. Om ett sådant godkännande ges ankommer det på den upphandlande myndigheten att säkerställa att även leverantören och underleverantören sinsemellan ingår ett personuppgiftsbiträdesavtal.

Avslutande kommentarer

Upphandling av IT-system som medför att personuppgifter kommer att behandlas av någon annan för den upphandlande myndighetens räkning t.ex. i molntjänster eller serverhall medför att förhållandet mellan myndigheten och leverantören måste regleras i enlighet med bestämmelserna i dataskyddsförordningen. Vid sidan av det ansvar för personuppgiftsbehandlingen som ligger på den upphandlande myndigheten kan upphandlingen medföra ett ansvar för leverantören, antingen som personuppgiftsbiträde eller som gemensamt personuppgiftsansvarig med den upphandlande myndigheten.

Som personuppgiftsbiträde har leverantören en skyldighet enligt dataskyddsförordningen att bistå den upphandlande myndigheten att uppfylla ansvaret och skyldigheter enligt dataskyddsförordningen. Personuppgiftsansvaret för den upphandlande myndigheten blir i princip inte mindre omfattande om ett personuppgiftsbiträde anlitas. Tvärtom innebär det ytterligare krav bl.a. på att kontrollera att personuppgiftsbiträdet kan uppfylla dataskyddsförordningens krav, att sluta personuppgiftbiträdesavtal och att ta fram dokumenterade instruktioner till biträdet.

Den som arbetar med upphandling behöver således ha en god inblick i myndighetens personuppgiftsbehandling och kunskap om hur dataskyddsförordningen kan påverka upphandlingsprocessen.

Om Advokatfirman Kahn Pedersen

Kahn Pedersen är en advokatbyrå helt inriktad på specialiserad affärsjuridik. Vi åtar oss uppdrag enbart inom våra två verksamhetsområden Digital och Public. Se www.kahnpedersen.se för mer information om vår verksamhet.

www.kahnpedersen.se

ISBN 978-91-983215-5-5