



Hur ska dataskydds-
förordningen beaktas vid
konkurrensutsättning av
offentlig upphandling?

Innehåll

1. Inledning	3
1.1 Bakgrund	3
1.2 När behandlingen av personuppgifter läggs ut som en offentlig upphandling	3
2. Allmänt om dataskyddsförordningen och behandlingen av personuppgifter	5
2.1 Dataskyddsförordningens tillämpningsområde (artikel 1–3)	5
2.2 Definitioner (artikel 4)	5
2.3 Laglig behandling av personuppgifter	6
2.3.1 Principer för behandling av personuppgifter (artikel 5)	6
2.3.2 Behandlingens laglighet (artikel 6–11)	6
3. Den registrerades rättigheter	8
3.1 Öppen information och kommunikation samt klara och tydliga villkor för utövandet av den registrerades rättigheter (artikel 12)	8
3.2 Information som ska tillhandahållas (artikel 13–14)	8
3.3 Den registrerades rätt till tillgång (artikel 15)	9
3.4 Rätt till rättelse (artikel 16)	9
3.5 Anmälningsskyldighet avseende rättelse eller radering av personuppgifter och begränsning av behandling (artikel 19)	9
3.6 Rätt till dataportabilitet (artikel 20)	9
3.7 Rätt att göra invändningar (artikel 21)	10
4. Den personuppgiftsansvariges skyldigheter	11
4.1 Den personuppgiftsansvariges ansvar (artikel 24)	11
4.2 Inbyggt dataskydd och dataskydd som standard (artikel 25)	11
4.3 Dataskyddsombudet – utnämning, ställning och uppgifter (artikel 37–39)	12
5. Behandling av personuppgifter	13
5.1 Personuppgiftsbiträde (artikel 28)	13
5.2 Behandling under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende (artikel 29)	13
5.3 Säkerhet i samband med behandlingen (artikel 32)	13
5.4 Anmälan av en personuppgiftsincident (artikel 33–34)	14
5.5 Konsekvensbedömning avseende dataskydd samt föregående samråd (artikel 35–36)	14
6. Överföring av personuppgifter till tredjeländer	16
6.1 Allmän princip för överföring av uppgifter (artikel 44)	16
6.2 Överföring på grundval av ett beslut om adekvat skyddsnivå (artikel 45)	16
6.3 Överföring som omfattas av lämpliga skyddsåtgärder (artikel 46)	17
6.4 Bindande företagsbestämmelser (artikel 47)	17
6.5 Undantag i särskilda situationer (artikel 49)	17
7. Rättsskydd och påföljder	18
7.1 Rättsskydd	18
7.2 Ansvar och rätt till ersättning (artikel 82)	18
7.3 Administrativa sanktionsavgifter och övriga påföljder (artikel 83)	18
Bilaga: Villkor för behandling av personuppgifter	19

1. Inledning

1.1 Bakgrund

Lagstiftningen om behandling av personuppgifter (dataskydd) reviderades efter att EU:s allmänna dataskyddsförordning¹ trädde i kraft i maj 2016. Förordningen blir tillämplig efter en övergångsperiod på två år 25.5.2018.

Syftet med dessa anvisningar är att ge information om dataskyddsfrågor med fokus på organisationer med offentlig upphandling. Ett centralt tema är säkerställandet av att personuppgifter behandlas lagenligt i situationer där en extern partner kommer att behandla uppgifterna utgående från upphandlingskontraktet. Innan förordningen börjar tillämpas kommer dataombudsmannen att ge mer detaljerade anvisningar om tillämpningen av den. Dataombudsmannens anvisningar samt bestämmelserna i den nationella dataskyddslagen, som är under beredning, kommer att i tillämpliga delar beaktas i uppdateringen av detta dokument. Närmare information om dataombudsmannens anvisningar finns på adressen tietosuojafi/sv.

I de föreliggande anvisningarna beskrivs dataskyddsförordningens viktigaste skyldigheter till stöd för planeringen av upphandlingen. För ökad läsbarhet har en del detaljerad författningstext lämnats bort. I anvisningarna finns också mallklausuler för avtal. Som bilaga finns detaljerade villkor för avtal om behandling av personuppgifter. Om den upphandlande enheten inte är säker på om mallklausulen lämpar sig för en enskild upphandling, är det tillrådligt att reservera tillfälle för de företag som deltar i upphandlingsförfarandet att kommentera de villkor och krav som gäller dataskyddet till exempel i samband med dialogen om de tekniska egenskaperna.

Det är värt att föra in mallklausuler och krav som gäller dataskyddet i upphandlingsdokumenten redan i det inledande skedet så att anbudsgivarna kan bedöma deras effekter när de utarbetar anbudet. Det ovan nämnda gäller också förhandlade förfaranden: om anbudssökande utanför EES-området deltar i konkurrensutsättningen, har de stor nytta av att

den upphandlande enheten redan i anbudsansökan anger förutsättningarna för behandling av personuppgifter.

Anvisningarna har utarbetats genom samarbete mellan statens inköpscentral Hansel Ab, Kommunförbundet, rådgivningsenheten för offentlig upphandling och KL-Kuntahankinnat Oy.

1.2 När behandlingen av personuppgifter läggs ut som en offentlig upphandling

I dessa anvisningar är strävan att beskriva den rätt vanliga situation där en myndighet som är personuppgiftsansvarig (upphandlande enhet, beställare) lägger ut uppdrag med behandling av personuppgifter på entreprenad (till kontraktsleverantörer). I och med utläggningen är servicegivarna i princip aktörer som behandlar personuppgifter på den personuppgiftsansvariges vägnar. Med andra ord om servicegivaren inte har någon självständig beslutanderätt över förvaringen och användningen av personuppgifter, agerar servicegivaren på den personuppgiftsansvariges vägnar som personuppgiftsbiträde.

Från utläggningssituationen ska man särskilja de situationer där servicegivaren själv är personuppgiftsansvarig i och med produktionen av tjänster enligt upphandlingskontraktet. Till exempel resebyråer kan ha ett bokningssystem som de anställda i den upphandlande enheten använder för att boka tjänsteresor. Då ansvarar resebyrån i egenskap av personuppgiftsansvarig att personregistret är lagenligt. Bokningssystemet kan å andra sidan vara gemensamt med en annan servicegivare (t.ex. flygbolag), och då gäller den personuppgiftsansvariges ansvar båda servicegivarna.

Den personuppgiftsansvarige ansvarar för att personuppgifterna behandlas lagenligt. Därför har det inte ansetts vara nödvändigt att i dessa anvisningar behandla den personuppgiftsansvariges ansvar i samma omfattning som personuppgiftsbiträdets ansvar.

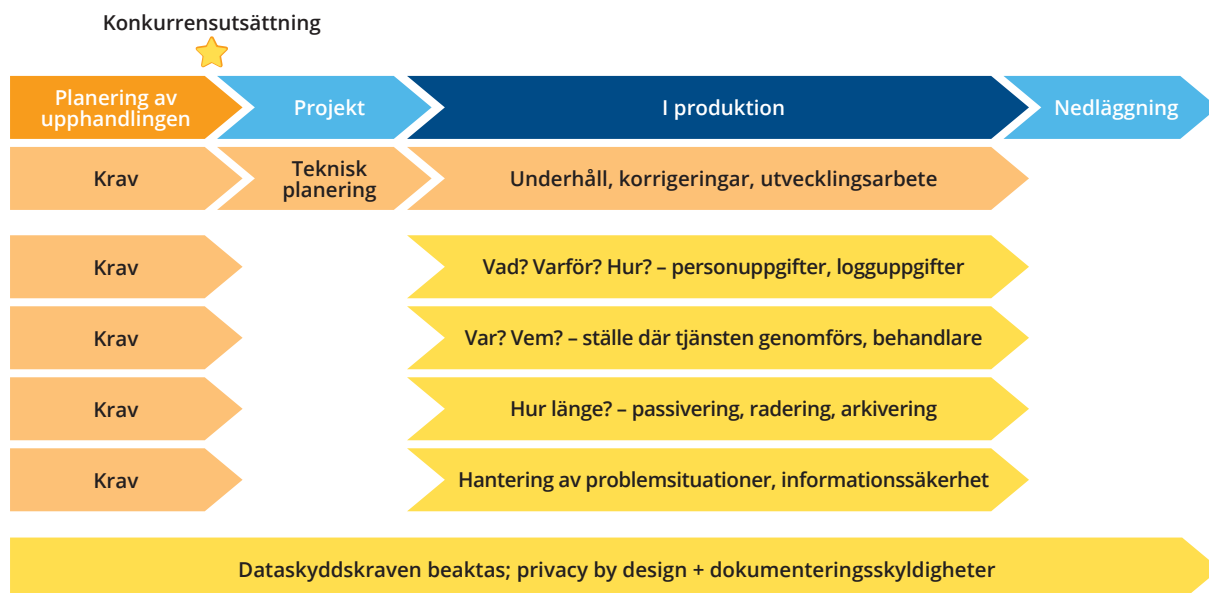
¹Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG.

När uppdrag som gäller behandling av personuppgifter ges genom avtal till en serviceproducent, är det nödvändigt att sörja för att personuppgiftsbiträdet genom avtalsförpliktelse har fått kännedom om villkoren för behandlingen av personuppgifter. Om personuppgiftsbiträdet till exempel började behandla personuppgifter för något annat ändamål än det avtalade, skulle det för biträdet kunna uppstå en personuppgiftsansvarigs ansvar eller behandlingen skulle kunna vara lagstridig.

Den personuppgiftsansvarige ska alltså innan upphandlingsförfarandet inleds från fall till fall bedöma vilken roll serviceproducenten kommer att ha i upphandlingen. Det är värt att notera att serviceproducenten kan vara både personuppgiftsansvarig och personuppgiftsbiträde. Den upphandlande enheten ska baserat på prövning fastställa de skyldigheter som hör till serviceproducenten, och som också be-

skrivs i dessa anvisningar, och införa dem i upphandlingsdokumenten. Det är också värt att observera att det på grund av utrymme för tolkning i lagstiftningen finns en rättslig osäkerhet redan enbart i gränsdragningen mellan den personuppgiftsansvarige och personuppgiftsbiträdet. Med villkoren i upphandlingskontraktet kan man försöka påverka tolkningen av de olika aktörernas ställning.

Den personuppgiftsansvarige är skyldig att planera behandlingen och utlämnandet av personuppgifterna samt detaljerna i sammanhanget, såsom policy för nyttjanderätt, tillgång till uppgifterna och förvaringstider. Behandlingen av uppgifterna bör planeras redan i god tid innan den eventuella konkurrensutsättningen inleds så att alla nödvändiga förpliktelser kan beaktas också i upphandlingskontrakten. Som hjälp för bedömningen kan man till exempel använda frågorna i figuren nedan.



Figur 1. Informationssystemets livscykel och kraven på dataskydd

2. Allmänt om dataskyddsförordningen och behandlingen av personuppgifter

2.1 Dataskyddsförordningens tillämpningsområde (artikel 1-3)

Dataskyddsförordningen ska tillämpas på automatisk behandling av personuppgifter. Förordningen tillämpas också på annan behandling av personuppgifter när de personuppgifter som ska behandlas utgör ett register eller en del av ett register.

Förordningen ska tillämpas på behandlingen av personuppgifter inom ramen för den verksamhet som bedrivs av en organisation som är etablerad i unionen, oavsett om behandlingen utförs i unionen eller inte. Vidare tillämpas förordningen också i vissa situationer på organisationer som är etablerade utanför unionen. Förordningen ska tillämpas på exempelvis behandlingen av uppgifter om personer som befinner sig i unionen, om behandlingen har anknytning till utbudande av varor eller tjänster till personerna eller anknytning till personernas beteende.

Eftersom förordningens tillämpningsområde är rätt omfattande, kommer förordningens krav att påverka en stor del av den offentliga upphandlingen, när personuppgifter behandlas i de tjänster som är föremål för upphandlingen.

Förordningen är inte tillämplig på

- sådan behandling av personuppgifter som är helt och hållet privat eller har samband med personens hushåll och saknar koppling till yrkes- eller affärsmässig verksamhet (t.ex. korrespondens eller innehav av adresser samt social nätverksbildning),
- frågor som berör skyddet av grundläggande rättigheter och friheter på områden som inte omfattas av unionsrätten, såsom verksamhet som gäller nationell säkerhet,
- medlemsstaternas behandling av personuppgifter när staterna agerar inom ramen för unionens

- gemensamma utrikes- och säkerhetspolitik,
- behandling av personuppgifter som myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder.

2.2 Definitioner (artikel 4)

Dataskyddsförordningen definierar personuppgift mer detaljerat än personuppgiftslagen. Förordningen tar också upp exempel på uppgifter som definieras som personuppgifter.

Med *personuppgift* avses i förordningen varje upplysning som avser en identifierad eller identifierbar fysisk person, dvs. en människa. En identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, geografisk information eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Enligt definitionen kan en personuppgift vara till exempel geografisk information som säger någonting om en viss person; ett fotografi som i kombination med exempelvis adressuppgifter säger någonting om en viss person eller om personens levnadsförhållanden; en IP-adress som kan kopplas till en viss person; eller användarnamn.

Med *behandling av personuppgifter* avses en åtgärd eller kombination av åtgärder som berör personuppgifter eller uppsättningar av personuppgifter, oberoende av om det utförs automatiserat eller inte. Exempel på detta är insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning eller användning av uppgifter, utlämning av uppgifter genom överföring, spridning

eller tillhandahållande av uppgifter på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring av uppgifter.

Ett *personregister* är en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden. Loggregister, användarregister och medlemsregister är exempel på personregister.

Den personuppgiftsansvarige är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.

Personuppgiftsbiträdet är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

2.3 Laglig behandling av personuppgifter

2.3.1 Principer för behandling av personuppgifter (artikel 5)

Vid behandling av personuppgifter ska man alltid iaktta de grundläggande principerna i dataskyddsförordningen:

- personuppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade ("**laglighet, korrekthet och öppenhet**").
- uppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och får inte senare behandlas på ett sätt som är oförenligt med dessa ändamål ("**ändamålsbegränsning**");
- uppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas ("**uppgiftsminimering**");
- uppgifterna ska vara korrekta 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 ("**korrekthet**");
- uppgifterna 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 ("**lagringsminimering**");
- uppgifterna 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 ("**integritet och konfidentialitet**").

Den personuppgiftsansvarige ansvarar för och ska också i praktiken kunna visa att den personuppgiftsansvarige och personuppgiftsbiträdet följer de grundläggande principerna för behandling av personuppgifter ("**ansvarsskyldighet**"). Detta ansvar kan den personuppgiftsansvarige inte lägga ut. Ansvarsskyldigheten innebär att den personuppgiftsansvarige följer de ovan nämnda principerna i praktiken till exempel genom att fastställa på vilket sätt principerna ska följas i praktiken i den tjänst som är föremål för upphandlingen. Till den personuppgiftsansvariges, dvs. beställarens skyldigheter hör således att vid upphandling kontrollera att serviceproducenten följer principerna i praktiken enligt den personuppgiftsansvariges anvisningar och krav.

2.3.2 Behandlingens laglighet (artikel 6–11)

Den personuppgiftsansvarige och personuppgiftsbiträdet får behandla personuppgifter endast på de grunder som framgår av dataskyddsförordningen (6 art.). I annat fall är behandlingen av personuppgifter olaglig. Enligt förordningen får personuppgifter behandlas om

- den registrerade har lämnat **sitt samtycke** till att dennes personuppgifter behandlas för ett eller flera specifika ändamål;
- 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;
- behandlingen är nödvändig för att **fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige**;
- behandlingen är nödvändig för att **skydda intressen som är av grundläggande betydelse** för den registrerade eller för en annan fysisk person;
- behandlingen är nödvändig för att utföra en uppgift av **allmänt intresse** eller som ett led i den personuppgiftsansvariges **myndighetsutövning**;
- behandlingen är nödvändig för ändamål som gäller 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.

Den personuppgiftsansvarige ansvarar för att personuppgifterna inte behandlas så att de avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt genetiska och biometriska uppgifter med vilka man entydigt kan identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

I artikel 9 i dataskyddsförordningen finns vissa undantag som gäller behandlingen av särskilda personuppgifter av ovan nämnda slag. Undantagen gäller främst situationer där den registrerades rättigheter tryggas eller där behandlingen av personuppgifterna

behövs på grund av ett viktigt allmänt intresse. Den personuppgiftsansvarige ansvarar för att uppgifterna behandlas i enlighet med undantagsbestämmelsen i förordningen.

I samband med kravspecifikationerna i anbudsförfrågan och villkoren i upphandlingskontraktet bör man bestämma huruvida serviceproducenten kan vara ett personuppgiftsbiträde som behandlar särskilda personuppgifter och vilka kontrollåtgärder som behövs samt utreda hurdana resurser och åtgärder detta skulle kräva av den upphandlande enheten och det system där uppgifterna behandlas.

3. Den registrerades rättigheter

3.1 Öppen information och kommunikation samt klara och tydliga villkor för utövandet av den registrerades rättigheter (artikel 12)

Den personuppgiftsansvarige ska planera sin verksamhet så att den registrerade på begäran får information som gäller behandlingen av personuppgifterna. Enligt dataskyddsförordningen ska informationen kunna presenteras i en koncis, klar och tydlig, begripelig och lättillgänglig form.

Informationen ska i regel tillhandahållas skriftligt. Om den registrerade lämnar begäran i elektronisk form, ska informationen i regel också tillhandahållas i elektronisk form. Om den registrerade begär det får informationen tillhandahållas muntligt, förutsatt att den registrerades identitet bevisats på ett tillförlitligt sätt.

Det finns tidsfrister för informationen till och åtgärderna angående den registrerade. Informationen ska ges utan onödigt dröjsmål och senast en månad efter att begäran togs emot. Det finns möjlighet till förlängning av tidsfristen på vissa villkor. I sammanhanget är det viktigt att också beakta bestämmelserna i lagen om offentlighet i myndigheternas verksamhet (621/1999, offentlighetslagen) om att lämna ut myndighetshandlingar. Om begäran om uppgifter förutom uppgifter om behandling av personuppgifter också gäller en myndighetshandling, tillämpas på myndighetshandlingen kortare tidsfrister enligt offentlighetslagen (14 dagar).

Samma tidsfrist på en månad följs i situationer där den personuppgiftsansvarige inte kommer att lämna ut uppgifter till den registrerade om behandlingen av dennes personuppgifter eller annars inte genomför åtgärder utgående från den registrerades begäran. Den som begär uppgifter ska samtidigt informeras om sin rättighet att använda rättsmedel, till exempel möjligheten att anföra besvär hos tillsynsmyndigheten.

Uppgifter som lämnas ut på den registrerades begäran och den personuppgiftsansvariges övriga åtgärder för utövandet av den registrerades rättigheter ska i regel tillhandahållas kostnadsfritt. Den person-

uppgiftsansvarige kan ändå ta ut en rimlig avgift för sina åtgärder eller vägra att tillmötesgå begäran, om den registrerades begäran är uppenbart ogrundad eller orimlig. Enligt förordningen kan en begäran anses orimlig till exempel då den registrerade upprepade gånger begär information uppenbart ogrundat.

Det ovan nämnda innebär att den upphandlande enheten genom krav på konkurrensutsättningen ska säkerställa att personuppgifterna kan lösgröras från informationssystemet och anslutas till det svar som skickas till den registrerade. Lösgrörandet borde i den mån det är möjligt ske på ett automatiserat sätt så att manuell insamling av uppgifter ur olika delar av systemet kan undvikas.

3.2 Information som ska tillhandahållas (artikel 13-14)

I dataskyddsförordningen finns en ingående beskrivning av den information som anknyter till behandling av personuppgifter och som den personuppgiftsansvarige, när personuppgifterna erhålls, ska lämna till den registrerade. I praktiken är det fråga om en registerbeskrivning eller ett motsvarande dokument.

Informationen ska lämnas till den registrerade, om inte någonting annat följer av förordningen. Informationen behöver inte ges exempelvis om den registrerade redan förfogar över informationen eller om informationen är sekretessbelagd. Informationen behöver inte heller ges om tillhandahållandet av sådan information visar sig vara omöjligt eller skulle medföra en oproportionell ansträngning.

Om personuppgifterna erhålls från den registrerade, ska informationen till den registrerade ges när personuppgifterna samlas in. Om personuppgifterna erhålls från någon annan källa, ska den personuppgiftsansvarige ge den i förordningen uppräknade informationen till den registrerade inom rimlig tid, men senast inom en månad.

Om personuppgifterna ska användas för kommunikation med den registrerade och de har fått från någon annan källa än den registrerade själv, ska

uppgifterna ges senast vid tidpunkten för den första kommunikationen med den registrerade. Om personuppgifterna avses lämnas ut till en annan mottagare, ska uppgifterna ges senast när personuppgifter lämnas ut för första gången.

Den upphandlande enheten bör i anbudsförfrågan vid behov ange kraven på hur informationsskyldigheten ska fullföljas på ett så automatiskt sätt som möjligt.

3.3 Den registrerades rätt till tillgång (artikel 15)

Den registrerade har rätt att med rimliga mellanrum få tillgång till de personuppgifter som har samlats in om honom eller henne. "Rimliga mellanrum" definieras inte i förordningen. Alla registrerade bör därför ha rätt att få kännedom och underrättelse om framför allt orsaken till att personuppgifterna behandlas och, om möjligt, under vilken tidsperiod behandlingen pågår, vilka som mottar personuppgifterna, logiken bakom automatisk behandling av personuppgifterna och de eventuella konsekvenserna av sådan behandling.

Den personuppgiftsansvarige ska på begäran meddela om denne behandlar personuppgifter om den som frågar. Den personuppgiftsansvarige ska förse den registrerade med en kopia av de personuppgifter som är under behandling, om det inte finns laga grund till att inte ge ut uppgifterna.

Den registrerades rätt att få tillgång till sina personuppgifter gäller också behandlingsåtgärderna. För att kunna informera den registrerade om dem ska den personuppgiftsansvarige loggföra behandlingsåtgärderna: vem som har behandlat uppgifterna, vilka uppgifter som har behandlats och när de har behandlats.

Uppgifterna ska i första hand ges i elektronisk form. Den personuppgiftsansvarige bör kontrollera identiteten på en registrerad som begär tillgång, särskilt inom ramen för nättjänster och i fråga om nätidentifierare. Till exempel stark elektronisk identifiering torde uppfylla det ovan nämnda behovet av identifiering av den registrerade på ett tillförlitligt sätt.

3.4 Rätt till rättelse (artikel 16)

Den registrerade ska ha rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få bristfälliga och felaktiga personuppgifter som berör honom el-

ler henne rättade. Den registrerade ska i princip ha rätt att komplettera ofullständiga personuppgifter, till exempel genom att lämna ett kompletterande utlåtande till den personuppgiftsansvarige.

Den upphandlande enheten ska se till att det går att korrigera uppgifter i det system där personuppgifterna behandlas. Det ska bli kvar en logganteckning för korrigeringen av uppgiften.

3.5 Anmälningsskyldighet avseende rättelse eller radering av personuppgifter och begränsning av behandling (artikel 19)

Enligt dataskyddsförordningen ska den personuppgiftsansvarige underrätta varje mottagare till vilken personuppgifterna har lämnats ut om eventuella rättelser eller radering av personuppgifterna eller begränsningar av behandlingen, om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Likaså ska den personuppgiftsansvarige på begäran underrätta den registrerade om till vem uppgifter har lämnats ut.

I praktiken kan den personuppgiftsansvarige till exempel förplikta serviceleverantören/personuppgiftsbiträdet att informera mottagaren av personuppgifterna direkt om de rättelser eller raderingar av uppgifterna eller begränsningar av behandlingen som den personuppgiftsansvarige gjort i enlighet med avtalet.

För att den personuppgiftsansvarige enligt kraven i förordningen ska kunna informera den registrerade om att uppgifter lämnats ut, ska det i det informationssystem som används för behandlingen av uppgifterna eller på något annat sätt kunna utredas vilka uppgifter som lämnats ut, till vem och när.

3.6 Rätt till dataportabilitet (artikel 20)

Den registrerade har rätt att få ut de personuppgifter som berör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige. Uppgifterna ska lämnas i ett strukturerat, allmänt använt och maskinläsbart format. Den registrerade har också rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som har personuppgifterna hindrar detta.

Utövandet av rätten till dataportabilitet förutsätter att behandlingen baserar sig på den registrerades samtycke eller på avtal och att den görs automatiskt.

När den registrerade utövar sin rätt till dataportabilitet ska han eller hon ha rätt till överföring av personuppgifterna direkt från en personuppgiftsansvarig till en annan, när detta är tekniskt möjligt.

På grund av detta kan den upphandlande enheten i samband med en upphandling kräva att serviceproducenten ska sörja för att personuppgifterna i systemet är i en sådan teknisk form att de smidigt kan överföras från ett system till ett annat och att överföringen inte orsakar den upphandlande enheten några tilläggskostnader.

3.7 Rätt att göra invändningar (artikel 21)

Den registrerade har rätt att motsätta sig behandling i direktmarknadssyfte och i en del andra situationer som nämns i dataskyddsförordningen, och då får hans eller hennes personuppgifter inte längre behandlas i syftena i fråga.

I praktiken ska den upphandlande enheten i anbudsförfrågan kräva att det i registret kan antecknas ett förbud mot direkt marknadsföring eller annat förbud mot behandling av uppgifter enligt artikeln.

4. Den personuppgifts-ansvariges skyldigheter

4.1 Den personuppgiftsansvariges ansvar (artikel 24)

Enligt dataskyddsförordningen ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och också i praktiken kunna visa att personuppgifterna behandlas i enlighet med förordningen.

Åtgärderna dimensioneras utifrån en riskbedömning, där man bland annat bör beakta behandlingens art, omfattning, sammanhang och ändamål samt de risker som gäller de registrerades rättigheter och friheter. Åtgärderna ska bedömas och ses över regelbundet och uppdateras vid behov.

Enligt lagstiftningen är det den personuppgiftsansvarige som ansvarar för genomförandet av de ovan nämnda åtgärderna. Om den personuppgiftsansvarige har lagt ut behandlingsuppdrag, ska han eller hon genom avtal säkerställa att serviceproducenten sörjer för de avtalade åtgärderna enligt den personuppgiftsansvariges anvisningar. För att kunna bevisa att tillräckliga åtgärder har vidtagits ska den personuppgiftsansvarige och serviceproducenten noggrant dokumentera de avtalade och vidtagna åtgärderna. Dokumentation ska hållas uppdaterad. Åtgärdernas tillräcklighet bör utvärderas gemensamt och regelbundet.

4.2 Inbyggt dataskydd och dataskydd som standard (artikel 25)

Enligt dataskyddsförordningen ska den personuppgiftsansvarige säkerställa att det system som används för behandlingen av personuppgifter uppfyller kravet på inbyggt dataskydd och dataskydd som standard (privacy by design). Enligt förordningen ska den personuppgiftsansvarige både vid planeringen av behandlingen och vid själva behandlingen effektivt genomföra lämpliga tekniska och organisatoriska åtgärder för genomförandet av förordningens dataskyddsprinciper som är utformade för att säkerställa

att kraven i denna förordning uppfylls och den registrerades rättigheter skyddas. Sådana åtgärder är till exempel

- pseudonymisering av uppgifter, minimering av uppgifter
- nödvändiga skyddsåtgärder
- utbildning, anvisningar, bestämmelser, förbindelser, kontokontroll, egenkontroll
- processer, uppförandekoder, certifikat
- krypteringsmekanismer, auditeringar, distansförbindelser, tekniska begränsningar, övervakningssystem.

När man bedömer vilka åtgärder som behövs bör man beakta den nyaste tekniken och genomförandekostnaderna samt de risker som behandlingen orsakar för den registrerades rättigheter och friheter, med hänsyn till behandlingens art och omfattning.

Den personuppgiftsansvarige kan bedöma och bestämma åtgärderna själv eller tillsammans med serviceproducenten. I konkurrensutsättningsskedet ska den personuppgiftsansvarige säkerställa att serviceproducenten genom avtal har förbundit sig till att det system eller den tjänst som upphandlas för behandling av uppgifter uppfyller kraven på inbyggt dataskydd och dataskydd som standard. Den personuppgiftsansvariges skyldigheter och den registrerades rättigheter ska beaktas och säkerställas redan när informationssystemet definieras och införs.

Avtalsvillkor:

Leverantören iakttar god databehandlingssed i enlighet med gällande personuppgiftslagstiftning och bestämmelserna om skydd för personuppgifter. Leverantören svarar för att tjänsten följer kraven i gällande personuppgiftslagstiftning och i detta avtal med särskild hänsyn till vad som bestäms om inbyggt dataskydd och dataskydd som standard.

4.3 Dataskyddsbudet – utnämning, ställning och uppgifter (artikel 37-39)

I vissa organisationer ska det alltid utnämnas ett dataskyddsbud. Ett dataskyddsbud ska alltid utnämnas när

- behandlingen genomförs av en myndighet eller ett offentligt organ, förutom när detta sker som en del av domstolarnas dömande verksamhet,
- den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling som kräver övervakning av de registrerade i stor omfattning,
- den personuppgiftsansvariges eller personuppgiftsbiträdets primära uppgifter består av omfattande behandling av känsliga uppgifter eller av uppgifter som gäller fällande domar i brottmål.

Dataskyddsbudet kan vara gemensamt på koncernnivå och myndigheterna kan utnämna gemensamma dataskyddsbud.

Dataskyddsbudet ska vara oberoende och rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbiträdets högsta förvaltningsnivå.

Avtalsvillkor:

Om en avtalspart är skyldig att utnämna ett dataskyddsbud, ska parten meddela ombudets kontaktuppgifter skriftligt till den andra avtalsparten.

5. Behandling av personuppgifter

5.1 Personuppgiftsbiträde (artikel 28)

Den personuppgiftsansvarige får endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen.

Personuppgiftsbitrådets ansvar ska fastställas genom ett avtal som binder biträdet i förhållande till den personuppgiftsansvarige. I avtalet fastställs åtminstone föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade samt den personuppgiftsansvariges skyldigheter och rättigheter.

Avtalsvillkor:

Leverantören följer i egenskap av personuppgiftsbiträde de villkor för behandling av personuppgifter som finns som bilaga till detta avtal. Leverantören får inte använda underleverantörens tjänster för behandling av personuppgifter utan skriftligt förhandstillstånd av Beställaren.

5.2 Behandling under den personuppgiftsansvariges eller personuppgiftsbitrådets överinseende (artikel 29)

Personuppgifter får behandlas endast enligt den personuppgiftsansvariges anvisningar, om inte annat följer av lag.

Avtalsvillkor:

Leverantören får inte använda eller på annat sätt utnyttja de personuppgifter som Leverantören behandlar på basis av avtalet till något annat än det syfte som är förenligt med avtalet och även då endast i den omfattning som syftet kräver och enligt Beställarens anvisningar.

5.3 Säkerhet i samband med behandlingen (artikel 32)

Dataskyddsförordningen förpliktar till bedömning av en riskbaserad säkerhetsnivå och fastställande av datasäkerhetskrav. Under hela behandlingen och personuppgifternas livscykel ska processernas, behandlingens och systemens säkerhetsnivå bedömas. Vid bedömningen fästs vikt bland annat vid behandlingens art och omfattning. Enligt förordningen ska både den personuppgiftsansvarige och personuppgiftsbiträdet bedöma säkerhetsnivåns tillräcklighet.

Den personuppgiftsansvarige ska redan innan anbudsförfrågan utarbetas fastställa en lämplig säkerhetsnivå för behandling av personuppgifter och ställa tekniska och organisatoriska krav på hur säkerhetsnivån ska nås. Förordningen fastställer de åtgärder som ska vidtas för att bedöma säkerhetsnivån och ger anvisningar för kravställandet. Den personuppgiftsansvarige kan inte överföra detta ansvar till någon annan aktör.

Vid bedömningen av en riskbaserad säkerhetsnivå ska hänsyn tas till de risker som behandlingen medför, i synnerhet när det gäller oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Vid bedömningen av säkerhetsnivån kan i praktiken bland annat följande beaktas:

- klassificeringen av skyddsnivån på de uppgifter som behandlas i den tjänst eller det system som utgör föremål för upphandlingen
- den egna klassificeringen av den tjänst eller det system som utgör föremål för upphandlingen; här bedöms bland annat
 - > hurdana uppgifter som behandlas
 - > huruvida det primära kravet är konfidentialitet, användbarhet eller integritet
 - > betydelsen av behandlingen, tjänsten eller systemet för organisationens kärnverksamhet
 - > betydelsen av behandlingen, tjänsten eller

systemet för kunderna eller det övriga verksamhetsnätverket

- › betydelsen av behandlingen, tjänsten eller systemet för samhället och de indirekta kunderna.

Bestämmandet av säkerhetsnivån leder till fastställande av kraven på datasäkerhet och dataskydd. Enligt förordningen ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Dessa åtgärder kan enligt förordningen till exempel vara

- pseudonymisering och kryptering av personuppgifter,
- förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
- förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,
- ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Som stöd vid fastställandet av kraven kan man också använda VAHTI:s datasäkerhetskrav.

Kraven, som kallas åtgärder i förordningen, tas med i anbudsförfrågan och det eventuella datasäkerhetsavtalet som bilaga och införs till behövliga delar direkt i avtalet.

Avtalsvillkor:

Leverantören sörjer för att skydda de personuppgifter som Leverantören behandlar på basis av detta avtal enligt sin praxis, avtalets krav och Beställarens skriftliga anvisningar för att säkerställa personuppgifternas konfidentialitet, integritet och tillgänglighet.

Avtalsvillkor:

Leverantören dokumenterar de avtalade och genomförda åtgärderna och ser till att dokumentationen är uppdaterad. Avtalsparterna bedömer regelbundet de ovan avsedda tekniska och organisatoriska åtgärderna och deras tillräcklighet.

5.4 Anmälan av en personuppgiftsincident (artikel 33–34)

Enligt dataskyddsförordningen ska den personuppgiftsansvarige anmäla en personuppgiftsincident till tillsynsmyndigheten inom 72 timmar efter att ha fått vetskap om den. Av artikel 33 i förordningen framgår kraven på innehållet i anmälan till tillsynsmyndigheten.

Anmälan behöver dock inte göras i situationer där incidenten sannolikt inte kommer att medföra en risk för de registrerades rättigheter och friheter. Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige om personuppgiftsincidenten utan onödigt dröjsmål efter att ha fått vetskap om den.

Den personuppgiftsansvarige ska också informera den registrerade om en personuppgiftsincident, om incidenten sannolikt kommer att innebära en hög risk för den registrerades rättigheter och friheter. Anmälan motsvarar till sitt väsentliga innehåll den anmälan som lämnas till tillsynsmyndigheten.

Anmälan behöver inte göras, om den personuppgiftsansvarige har vidtagit åtgärder som säkerställer att någon hög risk för den registrerades rättigheter och friheter sannolikt inte längre kommer att uppstå eller om anmälan skulle medföra en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas.

Den personuppgiftsansvarige ska genom bestämmelser i avtalet säkerställa att han eller hon får tillräckliga uppgifter om personuppgiftsincidenten och dess konsekvenser av serviceproducenten utan dröjsmål så att den personuppgiftsansvarige kan uppfylla sin skyldighet om anmälan till tillsynsmyndigheten inom 72 timmar. Det finns ett villkor om denna anmälningsskyldighet för leverantören i bilaga 1.

5.5 Konsekvensbedömning avseende dataskydd samt föregående samråd (artikel 35–36)

Innan behandlingen av personuppgifter inleds ska den personuppgiftsansvarige enligt förordningen bedöma den planerade behandlingens konsekvenser för skyddet av personuppgifter. En sådan konsekvensbedömning ska göras, om behandlingen, i synnerhet vid användning av ny teknik, sannolikt kommer att innebära en hög risk för fysiska personers rättigheter och friheter.

Om konsekvensbedömningen visar att behandlingen skulle leda till en hög risk om den personuppgiftsansvarige inte vidtog åtgärder för att minska risken, ska den personuppgiftsansvarige samråda med tillsynsmyndigheten innan behandlingen påbörjas. Tillsynsmyndigheten kan till exempel ge den personuppgiftsansvarige skriftliga anvisningar om behandlingen.

Den personuppgiftsansvarige ska i avtalet inkludera åtgärderna i de ovan nämnda anvisningarna till den del som åtgärderna hör till serviceproducentens ansvarsområde.

6. Överföring av personuppgifter till tredjeländer

6.1 Allmän princip för överföring av uppgifter (artikel 44)

Personuppgifter får överföras till länder utanför EES-området endast om den personuppgiftsansvarige och personuppgiftsbiträdet uppfyller villkoren i dataskyddsförordningen.

Överföring av personuppgifter till tredjeländer sker till exempel när molntjänster används. Molntjänsterna kan använda servrar som finns utanför EES-området. Den databehandlingsutrustning som anknyter till molntjänsterna kan innehas av en serviceproducent som finns utanför EES-området. I båda fallen ska överföringen av personuppgifter via molntjänster ske enligt reglerna om tredjeländer i förordningen.

Den upphandlande enheten ska i anbudsförfrågan ta ställning till huruvida personuppgifter kan behandlas utanför EES-området. Det är värt att komma ihåg att behandlingen av personuppgifter kan tolkas brett och att till exempel tillgång via distansförbindelse eller lagring av uppgifter i en molntjänst utanför EES uppfyller kännetecknen på behandling. Om uppgifter behandlas i dessa s.k. tredjeländer, ska den upphandlande enheten i avtalet ange vad som är en laglig grund för överföring av uppgifter och förplikta serviceproducenten och dess underleverantörer att förbinda sig att följa EU:s dataskyddsförordning med kommissionens standardklausuler, standardavtalsvillkor eller andra skyddsåtgärder som bestäms i förordningen.

Avtalsvillkor:

Leverantören behandlar personuppgifter endast inom det avtalade serviceproduktionsområdet. Det som avtalas om behandling av personuppgifter i detta avtal gäller även situationer där tillgång till personuppgifter ges till exempel via en hanterings- eller övervakningsförbindelse.

Leverantören har rätt att behandla personuppgifter endast inom Europeiska ekonomiska samarbetsområdet (EU-medlemsstaterna, Island, Norge och Liechtenstein), om inte avtalsparterna har avtalat om att behandlingen av personuppgifter endast sker i Finland och om det inte följer annat av kraven i detta avtal. Andra än ovan nämnda stater är vad som senare avses med "tredjeländer".

Leverantören kan behandla personuppgifter i tredjeländer endast om Leverantören skriftligt har avtalat om behandlingen med Beställaren och om behandlingen uppfyller kraven på behandling i kapitel V i dataskyddsförordningen.

I det syfte som anges i denna punkt samarbetar parterna för att säkerställa de lämpliga åtgärder som behövs för att behandlingen av personuppgifterna i tredjeländer ska uppfylla dataskyddsförordningens krav. Leverantören har inte rätt att kräva ersättning för kostnader som leverantören kan ha för att ge behandlingen av uppgifterna en sådan form att den uppfyller dataskyddsförordningens krav eller för att uppfylla samarbetsskyldigheten enligt denna punkt.

Observera att de villkor som finns som bilaga till detta dokument också innehåller villkor om överföring av personuppgifter. Det är en god idé att jämföra texterna med varandra och överväga huruvida bestämmelserna i frågan ska vara i de egentliga avtalsvillkoren eller i villkoren enligt bilaga 1.

6.2 Överföring på grundval av ett beslut om adekvat skyddsnivå (artikel 45)

Personuppgifter får överföras till ett tredjeland utan särskilt tillstånd, om kommissionen har beslutat att det tredje landet i fråga säkerställer en adekvat skyddsnivå.

I artikel 45 bestäms om kommissionens befogenheter att fatta ovan nämnda beslut. Med tredje land

jämställs också ett visst område eller en viss sektor i ett tredjeland samt internationella organisationer.

Kommissionen ska i Europeiska unionens officiella tidning och på sin webbplats offentliggöra en förteckning över de tredjeländer för vilka den har fastställt att skyddsnivån är eller inte längre är adekvat. För tillfället finns förteckningen på adressen http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

6.3 Överföring som omfattas av lämpliga skyddsåtgärder (artikel 46)

Om kommissionen inte har fattat beslut i enlighet med artikel 45 om adekvat skyddsnivå i tredjeland, får en personuppgiftsansvarig eller ett personuppgiftsbiträde endast överföra personuppgifter till ett tredjeland efter att ha vidtagit lämpliga skyddsåtgärder, och på villkor att lagstadgade rättigheter för registrerade och effektiva rättsmedel finns tillgängliga.

I förordningen anges de lämpliga skyddsåtgärder som inte kräver tillsynsmyndighetens tillstånd:

- ett rättsligt bindande och verkställbart avtal mellan offentliga myndigheter,
- bindande företagsbestämmelser som godkänns av tillsynsmyndigheten,
- kommissionens standardiserade dataskyddsbestämmelser,
- standardiserade dataskyddsbestämmelser som antagits av dataskyddsmyndigheten och godkänts av kommissionen,
- godkända uppförandekoder och ett avtal med den personuppgiftsansvarige eller personuppgiftsbiträdet i tredjelandet – i dessa ska lämpliga skyddsåtgärder och de registrerades rättigheter säkerställas,
- en godkänd certifieringsmekanism och ett avtal med den personuppgiftsansvarige eller personuppgiftsbiträdet i tredjelandet – i dessa ska lämpliga skyddsåtgärder och de registrerades rättigheter säkerställas.

Därutöver finns skyddsåtgärder som kan genomföras med den behöriga tillsynsmyndighetens tillstånd. Dessa kan till exempel vara

- avtalsklausuler mellan den personuppgiftsansvarige eller personuppgiftsbiträdet och den personuppgiftsansvarige, personuppgiftsbiträdet eller mottagaren av personuppgifterna i tredjelandet eller den internationella organisationen,
- bestämmelser som ska införas i administrativa överenskommelser mellan offentliga myndigheter vilka inbegriper verkställbara och faktiska rättigheter för registrerade.

6.4 Bindande företagsbestämmelser (artikel 47)

Om ett företag regelbundet överför personuppgifter mellan koncerndelar i olika länder lönar det sig att utarbeta bindande företagsbestämmelser som dataskyddsmyndigheten godkänner. I vissa situationer kan man av anbudsgivarföretaget kräva att sådana bestämmelser utarbetas och följs, om personuppgifter behandlas i tredjeländer enligt avtalet.

6.5 Undantag i särskilda situationer (artikel 49)

Det är möjligt att överföra uppgifter till tredjeländer, om EU-kommissionen har fattat ett beslut om att dataskyddsnivån i tredjelandet i fråga är adekvat. Om det inte har fattats något sådant beslut och om det inte har fastställts bindande bestämmelser för företaget i fråga, kan dataöverföring till tredjeländer dock genomföras sporadiskt om dataskyddsförordningens villkor uppfylls, om inte utlämnandet av uppgifter uttryckligen begränsas i annan lagstiftning på grund av ett viktigt allmänt intresse. Den personuppgiftsansvarige ska se till att bedömningen av överföringens laglighet och de vidtagna skyddsåtgärderna dokumenteras på ett tillbörligt sätt.

7. Rättsskydd och påföljder

7.1 Rättsskydd

I den kommande nationella dataskyddslagen föreslås en dataskyddsbyrå som ska vara den tillsynsmyndighet som avses i dataskyddsförordningen. Om den personuppgiftsansvarige vägrar att genomföra åtgärder på den registrerades begäran, kan denne föra saken till dataskyddsbyrån för behandling.

Med stöd av dataskyddsförordningen kan dataskyddsbyrån också genomföra egna kontroller och utifrån resultaten av dessa ge exempelvis varningar, meddela bestämmelser om den personuppgiftsansvariges verksamhet eller utfärda administrativa sanktionsavgifter.

Dataskyddsbyråns beslut får överklagas genom besvär hos förvaltningsdomstolen. Parterna har besvärsmätt.

7.2 Ansvar och rätt till ersättning (artikel 82)

Enligt dataskyddsförordningen ska varje person som har lidit skada till följd av en överträdelse av dataskyddsförordningen ha rätt till full ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan. Den personuppgiftsansvarige och alla personuppgiftsbiträden har alltså ett solidariskt ansvar för att behandlingen sker lagenligt i förhållande till den registrerade. Den part som betalat ersättning kan kräva den del som parten betalat utan grund av de övriga parterna med solidariskt ansvar enligt respektive parts andel av skadan.

I första hand har den personuppgiftsansvarige det primära ansvaret. Den personuppgiftsansvarige ansvarar alltså alltid för den skada som föranletts av sådan behandling av personuppgifter som inte har varit förenlig med dataskyddsförordningen. Den personuppgiftsansvarige blir befriad från ansvaret endast om han eller hon kan påvisa att incidenten orsakats av ett hinder som ligger utanför hans eller hennes kontroll.

Personuppgiftsbiträdet har ett sekundärt ansvar. Personuppgiftsbiträdet ska ansvara för skada endast om denne inte har fullgjort de skyldigheter i dataskyddsförordningen som specifikt riktar sig till personuppgiftsbiträden eller agerat utanför eller i strid med den personuppgiftsansvariges lagenliga anvisningar. Biträdet ska således kunna påvisa att han eller hon har beaktat ovan avsedda förpliktelser och anvisningar.

I upphandlingskontraktet kan införas en bestämmelse om att personuppgiftsbiträdet ska meddela den personuppgiftsansvarige om dennes anvisningar är bristfälliga eller om personuppgiftsbiträdet misstänker att de strider mot lagen. Ett sådant villkor finns i bilaga 1.

7.3 Administrativa sanktionsavgifter och övriga påföljder (artikel 83)

Utöver skadestånd till den registrerade kan den personuppgiftsansvarige och personuppgiftsbiträdet bli tvungna att betala administrativa sanktionsavgifter på grundval av överträdelse av dataskyddsförordningen. En administrativ sanktionsavgift kan uppgå till högst 20 000 000 euro eller, om det gäller ett företag, utgöra 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst.

Parallellt med eller i stället för administrativa sanktioner kan tillsynsmyndigheterna använda flera andra metoder att styra personuppgiftsansvariga samt få en lagstridig behandling att upphöra. Det kan till exempel vara fråga om att utfärda reprimander eller varningar till den personuppgiftsansvarige, förelägga att behandlingen ska motsvara lagen inom en viss tid, förelägga att den lagstridiga situationen rättas eller att felaktiga uppgifter rättas, uppställa behandlingsbegränsningar samt förelägga att dataöverföringar avbryts till en mottagare i ett tredjeland.

BILAGA _____ TILL KONTRAKT NR _____

Villkor för behandling av personuppgifter

ANVISNINGAR TILL UPPHANDLANDE ENHETER: Kontrollera villkoren i dessa anvisningar samt de bestämmelser och bilagor i huvudavtalet som det hänvisas till här. Ändra vid behov innan villkoren ansluts till anbudsförfrågan. Avlägsna denna anvisning.

1. Allmänt

- 1.1. Denna avtalsbilaga, "Villkor för behandling av personuppgifter", är en del av avtal X (Dnr X), nedan "Avtalet", som Beställaren har ingått med Leverantören.
- 1.2. I denna avtalsbilaga fastställs de avtalsvillkor för behandling av personuppgifter och dataskydd som, liksom villkoren i Avtalet, binder Beställaren och Leverantören och enligt vilka Leverantören på Beställarens uppdrag behandlar personuppgifter på Beställarens vägnar och för dennes räkning.
- 1.3. Parterna förbinder sig att i sin verksamhet följa tillämplig gällande lagstiftning om behandling av personuppgifter och dataskydd. Parterna förbinder sig också att anpassa behandlingen av personuppgifter och dataskyddet till den nivå som krävs i EU:s allmänna dataskyddsförordning (EU)2016/679 senast 25.5.2018, då dataskyddsförordningen ska börja tillämpas.

2. Parternas roller vid behandling av personuppgifter

- 2.1. Beställaren är en sådan personuppgiftsansvarig (i personuppgiftslagen: registeransvarig) som avses i lagstiftningen om behandling av personuppgifter och dataskydd när Beställaren fastställer ändamålet och metoderna för behandlingen av personuppgifter. Parterna är införstådda med att Beställaren i egenskap av personuppgiftsansvarig endast ska anlita personuppgiftsbiträden (i personuppgiftslagen: registerförare) som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i den gällande lagstiftningen om behandling av personuppgifter och dataskydd och från 25.5.2018 i EU:s dataskyddsförordning och säkerställer att den registrerades rättigheter skyddas.
- 2.2. Leverantören är ett sådant personuppgiftsbiträde som avses i lagstiftningen om behandling av personuppgifter och dataskydd och som behandlar Beställarens personuppgifter på Beställarens vägnar och för dennes räkning. De underleverantörer som Leverantören anlitar i enlighet med Avtalet och denna avtalsbilaga och som deltar i behandlingen av Beställarens personuppgifter är också personuppgiftsbiträden på Beställarens vägnar och för dennes räkning. Om Leverantören är en grupp, gäller skyldigheterna i denna avtalsbilaga samtliga medlemmar i gruppen och de underleverantörer som gruppen anlitar och som deltar i behandlingen av personuppgifter.
- 2.3. Beställaren förbinder sig att sörja för den personuppgiftsansvariges skyldigheter enligt lagstiftningen om behandling av personuppgifter och dataskydd.
- 2.4. Föremålet och ändamålet för behandlingen av personuppgifter och behandlingens natur, typer av personuppgifter och grupper för registrerade samt den personuppgiftsansvariges och personuppgiftsbiträdets skyldigheter och rättigheter beskrivs i Avtalet, den dokumentation som utarbetas under den avtalsenliga tjänsten och som binder Leverantören eller i Beställarens övriga anvisningar. Leve-

BILAGA _____ TILL KONTRAKT NR _____

rantören förbinder sig att iaktta de villkor för och beskrivningar av behandling av personuppgifter som anges i Avtalet, dokumentationen och anvisningarna. Beställaren ansvarar för att anvisningarna uppdateras och hålls tillgängliga.

- 2.5. Om det inte har gjorts någon beskrivning enligt punkt 2.4 eller om beskrivningen är bristfällig, utarbetar Beställaren en beskrivning eller kompletterar vid behov den befintliga i samarbete med Leverantören. Leverantören ska meddela Beställaren, om dennes anvisningar är bristfälliga eller om Leverantören misstänker att de strider mot lagen.
- 2.6. Leverantören deltar på Beställarens begäran i att utarbeta ett register över informationssystemet. Leverantören genomför de krävda uppgifterna till de priser för personarbete som fastställs i Avtalet, om inget annat har avtalats.

3. Underleverantörer som behandlar personuppgifter

- 3.1. Leverantören får inte anlita en underleverantörs tjänster för behandling av personuppgifter utan skriftligt förhandstillstånd av Beställaren. Leverantören ska skriftligt informera Beställaren om alla eventuella planer på att ersätta underleverantörer som är personuppgiftsbiträden eller anlita nya, så att Beställaren har möjlighet att göra invändningar mot sådana förändringar.
- 3.2. I den mån som Leverantören i sin verksamhet anlitar underleverantörer som behandlar personuppgifter tillämpas utöver Avtalet villkoren i denna avtalsbilaga på underentreprenaden.
- 3.3. Leverantören och alla underleverantörer som i egenskap av personuppgiftsbiträde behandlar Beställarens personuppgifter på Beställarens vägnar och för dennes räkning förbinder sig att fullfölja personuppgiftsbitrådets skyldigheter i denna avtalsbilaga. Leverantören är skyldig att genom avtal förbinda de underleverantörer som Leverantören anlitar att följa villkoren i denna avtalsbilaga.
- 3.4. Leverantören ansvarar för sina underleverantörers eventuella överträdelser eller försummelser av Avtalet, denna avtalsbilaga, tillämplig lagstiftning eller EU:s allmänna dataskyddsförordning i samband med behandling av Beställarens personuppgifter som för sina egna. Om en underleverantör som behandlar personuppgifter inte fullföljer sina dataskyddsskyldigheter, har Leverantören fortfarande fullt ansvar i förhållande till Beställaren. Om Beställaren motiverat anser att Leverantörens underleverantör inte fullgör sina dataskyddsskyldigheter, har Beställaren rätt att kräva att Leverantören byter underleverantör.

4. Personuppgiftsbitrådets allmänna skyldigheter

- 4.1. Personuppgiftsbitrådet behandlar personuppgifter enligt Avtalet och Beställarens anvisningar.
- 4.2. Personuppgiftsbitrådet förbinder sig att säkerställa att alla personer under dess överinseende med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.
- 4.3. Utöver vad som avtalas i Avtalet om krav på skydd för personuppgifter, informationssäkerhet och konfidentialitet, i syfte att vid behandling av personuppgifter säkerställa en säkerhetsnivå som motsvarar risken, förbinder sig personuppgiftsbitrådet att vidta lämpliga tekniska och organisatoriska åt-

BILAGA _____ TILL KONTRAKT NR _____

gärder. I samband med detta ska personuppgiftsbiträdet beakta den senaste tekniken, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter. Personuppgiftsbiträdet ska också följa Beställarens anvisningar och eventuella uppdateringar av dem.

- 4.4. Personuppgiftsbiträdet ska också vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under personuppgiftsbitrådets överinseende och som har tillgång till personuppgifter endast behandlar dessa enligt Avtalet och Beställarens anvisningar.
- 4.5. Personuppgiftsbiträdet förbinder sig att utan onödigt dröjsmål informera Beställaren om varje begäran från de registrerade som gäller utövandet av de registrerades rättigheter enligt gällande lagstiftning och EU:s allmänna dataskyddsförordning.
- 4.6. Personuppgiftsbiträdet förbinder sig att hjälpa Beställaren genom lämpliga tekniska och organisatoriska åtgärder, så att Beställaren kan fullgöra sin skyldighet att svara på begäran som gäller utövandet av den registrerades rättigheter. Personuppgiftsbiträdet är införstått med att begäran som gäller utövandet av dessa rättigheter kan förutsätta att Personuppgiftsbiträdet hjälper till med att informera den registrerade, tillgodose den registrerades rätt att få tillgång till uppgifter, rätta eller radera personuppgifter, begränsa behandlingen av personuppgifter och/eller överföra personuppgifter från ett system till ett annat. Om det inte har avtalats om att dessa uppgifter ingår i de tjänster som omfattas av Avtalet och i de avgifter som tas ut för dessa, har Leverantören rätt att ta ut en rimlig ersättning för arbetskostnaderna till de priser för personarbete som fastställs i Avtalet.
- 4.7. Leverantören ska sörja för att de personuppgifter som Leverantören behandlar är i ett sådant allmänt använt och maskinläsbart format att de automatiskt kan lösas från systemet för att överföras till ett annat system.
- 4.8. Personuppgiftsbiträdet förbinder sig att vid behov hjälpa Beställaren med genomförandet av en konsekvensbedömning som gäller dataskydd enligt EU:s allmänna dataskyddsförordning, ett eventuellt förhandssamråd och en eventuell certifiering för dataskydd. Leverantören har rätt att ta ut en rimlig ersättning för arbetskostnaderna till de priser för personarbete som fastställs i Avtalet.
- 4.9. Personuppgiftsbiträdet förbinder sig att, beroende på vad Beställaren väljer, radera eller återlämna alla Beställarens personuppgifter till Beställaren efter det att tillhandahållandet av behandlingstjänster har avslutats. Personuppgiftsbiträdet raderar befintliga kopior såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstatens nationella rätt. Beställaren kan i detta hänseende ge personuppgiftsbiträdet närmare anvisningar.
- 4.10. Personuppgiftsbiträdet får inte överföra personuppgifter utanför EU eller EES. Personuppgifter kan överföras till tredjeländer genom ett tillbörligt överföringsavtal enligt EU-kommissionens gällande mallklausuler och/eller övriga gällande krav på överföring av personuppgifter.
- 4.11. Personuppgiftsbiträdet ska ge Beställaren tillgång till all information som krävs för att visa att de skyldigheter som beskrivs i denna avtalsbilaga har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den revisor som bemyndigats av Beställaren. Närmare bestämmelser om granskningarna finns i Avtalet.

BILAGA _____ TILL KONTRAKT NR _____**5. Personuppgiftsbiträdets särskilda skyldigheter**

- 5.1. Leverantören ska ha färdigheter att ställa och administrera begränsningar som gäller utlämning av uppgifter till exempel på grund av spärrmarkering för den registrerade enligt befolkningsdatalagen. Leverantören ska kunna begränsa behandlingen av den registrerades personuppgifter delvis eller helt på det sätt som Beställaren kräver. Begränsningen av den registrerades personuppgifter får inte leda till begränsning av personuppgifter om andra fysiska personer i registret, om inte annat avtalas skriftligt mellan Beställaren och Leverantören.
- 5.2. Om inte annat avtalas, är Leverantören skyldig att upprätthålla en förteckning över rättelser och raderingar av de registrerades personuppgifter samt begränsningar av behandlingen. Förteckningen ska på begäran överlämnas till Beställaren. Leverantören ska på Beställarens begäran lämna ut uppgifter i förteckningen i begärd omfattning till de tredje parter som Beställaren specificerar.

6. Personuppgiftsincidenter

- 6.1. Personuppgiftsbiträdet ska informera Beställaren om en personuppgiftsincident skriftligt och utan onödigt dröjsmål efter att ha fått vetskap om incidenten och senast inom 36 timmar. Leverantören förbinder sig också att informera Beställaren om övriga väsentliga störningar eller problem i den tjänst som Leverantören producerar, om störningen eller problemet kan påverka de registrerades ställning och rättigheter. Beställaren ska informeras inom ovan nämnd tidsfrist, om det inte avtalas om en kortare tidsfrist i Avtalet eller dess bilagor.
- 6.2. Personuppgiftsbiträdet ska åtminstone ge Beställaren följande uppgifter om personuppgiftsincidenten:
- 1) personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,
 - 2) namnet på och kontaktuppgifterna för dataskyddsombudet eller annan ansvarig person hos vilken mer information kan erhållas,
 - 3) de sannolika konsekvenserna av personuppgiftsincidenten, och
 - 4) de åtgärder som personuppgiftsbiträdet har föreslagit eller vidtagit för att åtgärda personuppgiftsincidenten, samt, när så är lämpligt, också åtgärder för att mildra dess potentiella negativa effekter.

7. Övriga krav

- 7.1. Beställaren har rätt att ändra, komplettera och uppdatera de anvisningar om behandling av personuppgifter och dataskydd som Beställaren gett Leverantören. Anvisningarna kan bestå av ändringar, kompletteringar och uppdateringar av tekniska eller organisatoriska åtgärder som gäller behandling av personuppgifter eller dataskydd. Leverantören gör behövliga ändringar enligt Beställarens anvisningar. Om Beställarens anvisningar orsakar väsentliga ändringsarbeten för Leverantören (mer än ett (1) dagsverke), avtalar parterna om tilläggskostnaderna separat enligt prisbilagan. Leverantören och övriga personuppgiftsbiträden förbinder sig att följa dessa ändrade, kompletterade eller uppdaterade anvisningar.
- 7.2. Parterna är införstådda med att också dataskyddsfrågor behandlas i Avtalet och dess bilagor.

BILAGA _____ TILL KONTRAKT NR _____

- 7.3. Leverantören förbinder sig att reagera senast inom 72 timmar från att Beställaren tagit kontakt och svara senast inom en (1) vecka på Beställarens meddelanden om dataskydd, reklamationer eller andra meddelanden, exklusive personuppgiftsincidenter enligt EU:s allmänna dataskyddsförordning. På nämnda personuppgiftsincidenter tillämpas de tidsfrister som fastställs i Avtalet och ovan i denna bilaga.
- 7.4. Om Leverantören försummar eller överträder denna avtalsbilaga, den tillämpliga lagstiftningen eller EU:s allmänna dataskyddsförordning, fastställs Leverantörens ersättningsansvar förutom i Avtalet också i den tillämpliga lagstiftningen. En sådan försummelse eller överträdelse utgör dessutom en väsentlig avtalsöverträdelse enligt Avtalet, varvid Beställaren har rätt till de rättsmedel som fastställs i Avtalet.
- 7.5. Parterna är införstådda med att lagstiftningen om dataskydd håller på att ändras när Avtalet och denna avtalsbilaga utarbetas. Om det i lagstiftningen i fråga eller i rekommendationer, anvisningar eller bestämmelser som gäller lagstiftningen eller tolkningen av den görs ändringar som påverkar Beställarens ställning eller skyldigheter eller de skyldigheter eller det ansvar som fastställs i denna avtalsbilaga, kan avtalsbilagan vid behov revideras i detta hänseende. Om det i denna avtalsbilaga görs sådana ändringar som orsakar väsentliga tilläggskostnader för Leverantören (mer än ett (1) dagsverke), kan parterna avtala om ersättning av dem separat enligt prisbilagan till Avtalet. Leverantören och de övriga personuppgiftsbiträdena förbinder sig att följa den reviderade avtalsbilagan.



Version 1.0 maj 2017

Arbetsgrupp

Katariina Huikko, Rådgivningsenheten för offentlig upphandling

Jukka Hämäläinen, Hansel Ab

Pauliina Juntunen, KL-Kuntahankinnat Oy

Karolina Lehto, Hansel Ab

Ida Sulin, Finlands Kommunförbund rf