VAHTI god praxis - stödmaterial

29.5.2023

**Dataskyddsbilaga**

Innehållsförteckning

[1. Allmänt 3](#_Toc148335487)

[2. Parternas roller vid behandlingen av personuppgifter 3](#_Toc148335488)

[3. Leverantörens allmänna skyldigheter 3](#_Toc148335489)

[4. Beställarens anvisningar 4](#_Toc148335490)

[5. Underleverantörer som behandlar personuppgifter 4](#_Toc148335491)

[6. Plats för behandlingen av personuppgifter 5](#_Toc148335492)

[7. Krav gällande personalen 5](#_Toc148335493)

[8. Personuppgiftsincidenter 5](#_Toc148335494)

[9. Upphöra med behandling av personuppgifter 6](#_Toc148335495)

[Bilagor 6](#_Toc148335496)

*[Anvisning]:*

*Denna dataskyddsbilaga är avsedd som modelldokument för upphandlingar där Leverantören behandlar Beställarens personuppgifter för Beställarens räkning.*

*Dataskyddsbilagan har utarbetats i samarbete med informationssäkerhetssektionen, Hansel och Valtori, och ingår i Rekommendation om upphandlingars informationssäkerhet och tillhörande bilagor som finns tillgängliga på informationshanteringsnämndens webbplats.*

***Observera följande:***

* ***Dokumentet innehåller punkter som ska redigeras så att de lämpar sig för upphandlingen i fråga – detta dokument kan alltså inte som sådant bifogas anbudsbegäran. Ta bort denna anvisningssida från den egentliga anbudsbegäran.***
* *Om du inte använder JIT:s allmänna villkor ska du använda följande villkor i avtalet: ”Om en avtalspart har betalat ersättning till en registrerad för skada som orsakats på grund av ett brott mot dataskyddslagstiftningen, har denna avtalspart, utan att begränsa de överenskomna ansvarsbegränsningarna, rätt att av en annan avtalspart som deltagit i samma databehandling ta ut en sådan andel av den ersättning som betalats till den registrerade som motsvarar dennes skadeståndsansvar. Avtalspartens ansvar för skada som orsakats för den registrerade bestäms enligt artikel 82.4 i EU:s allmänna dataskyddsförordning eller motsvarande bestämmelse i annan dataskyddslagstiftning.”*
* *Kontrollera att rätten till insyn i huvudavtalet eller de allmänna villkoren även omfattar dataskyddsgranskning, t.ex.: ”Leverantören tillåter att beställaren eller en auktoriserad utvärderare utför kontroller och deltar i dem.*
* *Punkterna 1.2, 3.5, 3.6 och 9.2: Fundera på hur du bygger upp prissättningen av informationssäkerhets- och dataskyddsarbetet.*
* *Punkt 3.1 Precisera vid behov lagstiftningen gällande din organisation.*
* *Punkt 5.2: Kontrollera att huvudavtalet eller de allmänna villkoren innehåller ett villkor för godkännande som uppfyller kraven på ändringar av underleverantör och rätt att motsätta sig en ny underleverantör.*
* *Punkt 6.2: Observera att beslutet om huruvida uppgifter får överföras utanför EES-området måste fattas innan anbudsbegäran skickas för att avtalsvillkoren ska vara korrekta redan i anbudsbegäran. Beakta detta särskilt när du skaffar molntjänster. Om uppgifterna inte överförs utanför EES-området kan du ta bort punkt 6.2. Om du för överföringen använder kommissionens modellavtalsklausuler eller andra grunder för överföring av personuppgifter ska du precisera dem i beskrivningen av behandlingsåtgärderna, inklusive grunden för överföringen. Kontrollera om Finland är behandlingsland i säkerhetsbilagan.*
* *Om behandlingen omfattar uppgifter som hör till särskilda kategorier av personuppgifter ska du säkerställa att du i förhandsvillkoren till verktyget för upphandlingsvillkor har valt alternativet ”Särskilda kategorier av personuppgifter” i punkten Personuppgifter för föremålet för upphandlingen.*

# Allmänt

* 1. Denna avtalsbilaga ”Dataskyddsbilaga” är en del av avtalet \_\_\_\_\_\_\_\_\_ (Dnr \_\_\_\_\_\_\_\_\_\_), nedan ”Avtalet”, som Beställaren har ingått med Leverantören.
	2. I denna avtalsbilaga fastställs på ett bindande sätt de avtalsvillkor för behandling av personuppgifter för Beställaren och Leverantören samt den personuppgiftsansvariges och personuppgiftsbiträdets skyldigheter och rättigheter enligt vilka Leverantören behandlar Beställarens personuppgifter för Beställarens räkning.
	3. Behandlaren ska kunna visa att han eller hon följer dessa avtalsvillkor.
	4. I denna bilaga används begrepp som definieras i dataskyddsförordningen.

# Parternas roller vid behandlingen av personuppgifter

* 1. Vid behandling av personuppgifter är Beställaren personuppgiftsansvarig och Leverantören personuppgiftsbiträde, om inte något annat följer av ändamålet med behandlingen av personuppgifter. Med Beställarens personuppgifter avses i dessa villkor personuppgifter som Beställaren ansvarar för i egenskap av personuppgiftsansvarig.
	2. Föremålet för, varaktigheten av, karaktären av och syftet med behandlingen av personuppgifter samt typer av personuppgifter och grupper av registrerade beskrivs i bilaga 1 ”Beskrivning av behandlingsåtgärder för personuppgifter” och/eller i Beställarens övriga skriftliga anvisningar. Leverantören förbinder sig till att följa villkoren och beskrivningarna i Avtalet, beskrivningen av behandlingsåtgärder för personuppgifter och anvisningarna. Beställaren ansvarar för underhållet av och tillgången till anvisningarna.
	3. Om en Beskrivning av behandlingsåtgärder för personuppgifter enligt punkt 2.2 inte har upprättats eller om den är bristfällig upprättar Beställaren och Leverantören bilagan i fråga tillsammans innan behandlingen av personuppgifter inleds.

# Leverantörens allmänna skyldigheter

* 1. Leverantören behandlar personuppgifter enligt lagstiftningen, Avtalet och Beställarens anvisningar.
	2. Leverantören vidtar tekniska och organisatoriska åtgärder för att säkerställa att Beställarens behandling av personuppgifter utförs i enlighet med kraven i avtalet och överenskommen praxis. Syftet med åtgärderna är att säkerställa att personuppgifterna behandlas lagenligt samt att behandlingssystemen och tjänsterna är konfidentiella, enhetliga, tillgängliga och tål fel.
	3. Leverantören får inte behandla eller på annat sätt utnyttja personuppgifterna som omfattas av avtalet i annat syfte och den omfattning som anges i Avtalet.
	4. Leverantören utser en dataskyddsansvarig eller dataskyddsansvarig kontaktperson för kontakter som gäller Beställarens personuppgifter. Leverantören meddelar dataskyddsombudets eller kontaktpersonens kontaktuppgifter skriftligt till Beställaren.
	5. Leverantören gör på Beställarens begäran alla uppgifter tillgängliga som Beställaren behöver för att påvisa att de skyldigheter som föreskrivits för den personuppgiftsansvarige och Leverantören uppfylls. Leverantören deltar på begäran på överenskommet sätt i beskrivningar och andra dokument som Beställaren ansvarar för, såsom konsekvensbedömning, upprättande och upprätthållande samt i genomförandet av förhandssamråd enligt dataskyddsförordningen.
	6. Leverantören ska utan dröjsmål meddela Beställaren om alla begäranden från registrerade som gäller utövande av den registrerades rättigheter. Leverantören svarar inte själv på dessa begäranden. Leverantören bistår Beställaren så att Beställaren kan uppfylla sin skyldighet att svara på dessa begäranden. Begäran kan förutsätta att Leverantören till exempel hjälper till med att informera och kommunicera med den registrerade, tillgodose den registrerades åtkomsträtt, redigera eller radera personuppgifter, begränsa behandlingen eller överföra den registrerades egna personuppgifter från ett system till ett annat.

# Beställarens anvisningar

* 1. Vid behandling av Beställarens personuppgifter iakttar Leverantören villkoren i avtalet och dessa specialvillkor samt Beställarens skriftliga anvisningar. Beställaren ansvarar för underhållet av och tillgången till anvisningarna. Leverantören meddelar Beställaren utan onödigt dröjsmål om Beställarens anvisningar är bristfälliga eller om Leverantören misstänker att de är lagstridiga.
	2. Beställaren har rätt att ändra, komplettera och uppdatera anvisningarna till Leverantören om behandlingen och skyddet av personuppgifterna. Om ändringarna i anvisningarna medför andra än mindre ändringar i anslutning till de avtalsenliga tjänsterna, kommer man överens om deras inverkan i det avtalsenliga ändringshanteringsförfarandet.

# Underleverantörer som behandlar personuppgifter

* 1. Till den del Leverantören i sin verksamhet anlitar underleverantörer som behandlar Beställarens personuppgifter ska utöver Avtalet även villkoren i denna avtalsbilaga tillämpas på underleveranserna. Användning av underleverantör förutsätter skriftligt tillstånd av beställaren på förhand. Underleverantörerna finns listade i bilaga X till avtalet.
	2. Leverantören ingår med underleverantören ett skriftligt avtal där Leverantören förbinder underleverantörerna att för egen del följa skyldigheterna som ålagts Leverantören i avtalet samt Beställarens vid var tid gällande anvisningar om behandling av personuppgifter. Leverantören säkerställer att Beställarens granskningsrätt enligt avtalet även omfattar underleverantören.
	3. Leverantören ansvarar för underleverantörens andel på samma sätt som för sin egen. Leverantören ansvarar för att underleverantören för sin del iakttar de skyldigheter som ålagts personuppgiftsbiträdet. Om Beställaren med fog anser att Leverantörens underleverantör inte uppfyller skyldigheterna i anslutning till dataskydd har Beställaren rätt att kräva att Leverantören byter underleverantör.
	4. Ändring av underleverantör som deltar i behandlingen av personuppgifter ska meddelas Beställaren på förhand. I meddelandet ska beskrivas hur underleverantören behandlar Beställarens personuppgifter i enlighet med dataskyddslagstiftningen. Beställaren har rätt att av grundad anledning motsätta sig den föreslagna underleverantören.

# Plats för behandlingen av personuppgifter

* 1. Leverantören har rätt att behandla Beställarens personuppgifter inom Europeiska ekonomiska samarbetsområdet (EES). Det som avtalats i avtalet och i dessa villkor om behandling av personuppgifter gäller också möjligheten att få tillgång till Beställarens personuppgifter till exempel via en administrations- och övervakningsförbindelse. [I avtalet har man kunnat definiera ett snävare område.]
	2. [Leverantören behandlar Beställarens personuppgifter utanför EES-området i följande länder: xx, xx. Leverantören gör en konsekvensbedömning för överföringen (transfer impact assessment, TIA) av behandlingen av personuppgifter, om EU-kommissionen inte har fattat ett beslut om huruvida dataskyddet för tredjelandet i fråga är tillräckligt. Konsekvensbedömningen av överföringarna ska uppdateras i samband med betydande förändringar. Leverantören godkänner överföringens konsekvensbedömning och överföringsgrund hos den personuppgiftsansvarige.]

# Krav gällande personalen

* 1. Leverantören ska säkerställa att alla personer som arbetar under dess överinseende och som får tillgång till Beställarens personuppgifter, känner till sina skyldigheter i samband med behandling av personuppgifter och endast behandlar personuppgifter i enlighet med avtalet, dessa specialvillkor och Beställarens anvisningar.
	2. Leverantören ger sin personal tillgång till Beställarens personuppgifter endast i den utsträckning som det är absolut nödvändigt för att verkställa, administrera och följa upp avtalet. Leverantören säkerställer att de personer som har rätt att behandla personuppgifterna har förbundit sig att iaktta den tystnadsplikt som avtalats i avtalet eller att de omfattas av en annan lagstadgad tystnadsplikt.

# Personuppgiftsincidenter

* 1. Leverantören ska utan obefogat dröjsmål skriftligen meddela Beställaren om en personuppgiftsincident som kommit till leverantörens kännedom. Dessutom förbinder sig Leverantören att utan obefogat dröjsmål underrätta Beställaren om andra störningar eller problem i tjänsten som kan påverka de registrerades ställning och rättigheter.
	2. Leverantören ska ge Beställaren minst följande uppgifter om en personuppgiftsincident:
1. en beskrivning av den inträffade kränkningen av dataskyddet, inklusive berörda grupper av och det uppskattade antalet registrerade samt grupper av personuppgiftstyper och uppskattat antal i den utsträckning man känner till dem,
2. dataskyddsombudets eller någon annan ansvarspersons namn och kontaktuppgifter som ger tilläggsuppgifter i ärendet,
3. en beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten, och
4. en beskrivning av de åtgärder som Leverantören föreslår eller redan har vidtagit för att åtgärda personuppgiftsincidenten, och när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.
	1. Det ursprungliga meddelandet ska kompletteras utan obefogat dröjsmål om Leverantören efter meddelandet får tilläggsuppgifter om personuppgiftsincidenten.
	2. Efter att ha upptäckt en personuppgiftsincident vidtar Leverantören utan dröjsmål tillräckliga och skäliga åtgärder för att avlägsna personuppgiftsincidenten och begränsa och korrigera dess konsekvenser.

# Upphöra med behandling av personuppgifter

* 1. Under avtalets giltighetstid får Leverantören inte avlägsna personuppgifter som behandlats för Beställarens räkning utan Beställarens uttryckliga samtycke.
	2. Efter att avtalet upphört returnerar Leverantören personuppgifterna i ett format som allmänt används eller förstör dem så att personuppgifterna inte längre kan återställas i läsbar form. Uppgifterna får inte avlägsnas om det i lagstiftningen eller genom en myndighetsföreskrift förutsätts att Leverantören förvarar personuppgifterna.

# Bilagor

Bilaga 1: Beskrivning av behandlingsåtgärder för personuppgifter