JHS 166 Allmänna avtalsvillkor för IT-upphandlingar inom den offentliga förvaltningen

Bilaga 9. Specialvillkor för behandlingen av personuppgifter (JIT 2015 – Personuppgifter)

Version: 1.0
Publicerad: 30.7.2018
Giltighetstid: tills vidare

BRUKSANVISNING

Dessa specialvillkor ska tillämpas i situationer där en leverantör behandlar personuppgifter för beställarens räkning som en del av en köpt tjänst. Villkoren ska inte tillämpas som sådana, utan specialvillkoren för respektive tjänst och de allmänna avtalsvillkoren för IT-upphandlingar inom den offentliga förvaltningen (*JIT 2015 – Allmänna villkor*) ska alltid bifogas avtalet. Dessa villkor ska prioriteras före andra specialvillkor.

Avtalet ska vid behov fastställa den personuppgiftsansvarige och personuppgiftsbiträdet samt beakta kraven för behandling av personuppgifter i *EU:s allmänna dataskyddsförordning (EU) 2016/679*. När beställaren fastställer ändamål och medel för behandlingen av personuppgifter är beställaren den personuppgiftsansvarige som avses i lagstiftningen om behandling av personuppgifter och dataskydd. Även om beställaren vanligtvis är den personuppgiftsansvarige för personuppgifterna som används i en tjänst, bör man tänka på att även leverantören har personuppgifter som rör leverantörens verksamhet och som leverantören kan utnyttja i tjänsten. Sådana uppgifter är till exempel kontaktuppgifterna i leverantörens kundregister. Dessa uppgifter omfattas inte av beställarens anvisningar.

Det är bra att till avtalet bifoga ett dokument där det konkret framgår vilka personuppgifter som behandlas, hur och till vilket ändamål. Enligt artikel 28 i EU:s allmänna dataskyddsförordning ska behandlingen av personuppgifter regleras genom en bindande akt i vilken föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade anges.

Avtalsparterna bestämmer tillsammans vilken säkerhetsnivå som krävs för tjänsten som är föremål för avtalet. Säkerhetsnivåkraven kan till exempel baseras på en riskbedömning som utförts av beställaren och som behandlats gemensamt, den tillgängliga tekniken och de tekniska möjligheterna samt vilken typ av uppgifter som ska behandlas.

Enligt dataskyddsförordningen ska den personuppgiftsansvarige på förhand godkänna personuppgiftsbiträdets underleverantörer. Ett skriftligt förhandstillstånd kan vara särskilt eller allmänt. Leverantören ska dessutom informera beställaren om alla planerade förändringar beträffande underleverantörer. Beställaren kan ge ett skriftligt samtycke till dem som hanterar underleverantörer, till exempel genom att underteckna ett avtal där underleverantörerna namnges.

Bestämmelser om skadestånd och eventuell regressrätt mellan den personuppgiftsansvarige och personuppgiftsbiträdet finns i *JIT 2015 – Allmänna villkor*.

Denna bruksanvisning utgör inte en del av avtalet.

Innehåll

1Tillämpning....1
2Definitioner....1
3Avtalsparternas roller i behandlingen av personuppgifter....2
4Leverantörens allmänna skyldigheter....2
5Beställarens anvisningar....3
6Personal....3
7Underleverantörer som behandlar personuppgifter....3
8Platsen för tjänsten....4
9Personuppgiftsincidenter....4
10Upphörande av behandling av personuppgifter....4

1 Tillämpning

(1) Dessa specialvillkor iakttas när upphandlande enheter inom den offentliga förvaltningen köper tjänster där leverantören är personuppgiftsbiträde, om dessa specialvillkor åberopas i avtalen och om inte något annat har avtalats skriftligen om någon del av dem.

(2) Dessa specialvillkor används tillsammans med de allmänna avtalsvillkoren för IT-upphandlingar inom den offentliga förvaltningen. I händelse av motstridighet har specialvillkoren prioritet över motsvarande punkter i de ovan nämnda allmänna avtalsvillkoren för IT-upphandlingar inom den offentliga förvaltningen.

2 Definitioner

Utöver definitionerna för specialvillkoren nedan följs definitionerna i *JIT 2015 Allmänna villkor*.

personuppgiftsbiträde
fi käsittelijä

den part i dataskyddslagstiftningen, som behandlar personuppgifter för den personuppgiftsansvariges räkning

personuppgiftsansvarig
fi rekisterinpitäjä

den part i dataskyddslagstiftningen, som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter

dataskyddslagstiftning
fi tietosuojalainsäädäntö

Europeiska unionens allmänna dataskyddsförordning (EU) 679/2016 och övriga rättsakter om dataskydd samt dataskyddsmyndigheternas bestämmelser

personuppgiftsincident
fi henkilötietojen tietoturvaloukkaus

en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats

beställarens personuppgifter
fi tilaajan henkilötieto

personuppgifter, som beställaren ansvarar för i egenskap av personuppgiftsansvarig

3 Avtalsparternas roller i behandlingen av personuppgifter

(1) Beställaren är personuppgiftsansvarig och leverantören personuppgiftsbiträde, om inget annat följer av avtalet eller ändamålet med behandlingen av personuppgifter. I avtalet preciseras avtalsparternas uppgifter och ansvar i fråga om behandlingen av personuppgifter.

(2) Föremålet för behandlingen av personuppgifter, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, tillämpliga dataskyddsåtgärder samt leverantörens och beställarens skyldigheter och rättigheter beskrivs närmare i avtalet, dess bilagor och beställarens anvisningar. Leverantören iakttar villkoren i avtalet, dess bilagor och anvisningar.

4 Leverantörens allmänna skyldigheter

(1) Leverantören ska iaktta bestämmelserna om förfaranden samt behandling och skyddande av personuppgifter i den gällande dataskyddslagstiftningen. Leverantören ska ansvara för att tjänsten är förenlig med gällande dataskyddslagstiftning och avtalskrav, och tar särskilt i beaktande bestämmelserna om inbyggt dataskydd och dataskydd som standard.

(2) Leverantören ska vidta ändamålsenliga tekniska och organisatoriska åtgärder för att säkerställa att behandlingen av beställarens personuppgifter sker enligt avtalskraven och avtalad praxis. Syftet med åtgärderna är att säkerställa att behandlingen av personuppgifter sker lagenligt och att säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos systemen och tjänsterna.

(3) Leverantören får inte behandla eller på annat sätt utnyttja personuppgifterna som omfattas av avtalet i annat syfte eller i annan omfattning än vad som krävs för att fullfölja avtalet.

(4) Leverantören ska namnge dataskyddsombudet eller den dataskyddsansvariges kontaktperson för kontakter som rör beställarens personuppgifter. Leverantören ska informera beställaren skriftligen om dataskyddsombudets eller kontaktpersonens kontaktuppgifter.

(5) Leverantören ska på beställarens begäran ge beställaren tillgång till all information som krävs för att visa att den personuppgiftsansvariges och personuppgiftsbiträdets fastställda uppgifter har fullgjorts samt på överenskommet sätt bistå i arbetet med att upprätta och uppdatera beskrivningar och andra dokument som beställaren ansvarar för, till exempel konsekvensbedömningen, och i genomförandet av det förhandssamråd som avses i dataskyddsförordningen. Leverantören ska utföra dessa uppgifter enligt priserna i avtalet, om inget annat avtalas.

(6) Leverantören ska informera beställaren utan dröjsmål om varje begäran om en registrerad, som rör utövandet av den registrerades rättigheter. Leverantören ska inte själv ansvara för en sådan begäran. Leverantören ska bistå beställaren, så att beställaren kan uppfylla sina skyldigheter att svara på en sådan

begäran. En begäran kan förutsätta att leverantören ska hjälpa till att informera och kommunicera med den registrerade, ge den registrerade åtkomsträttigheter, korrigera eller radera personuppgifter, begränsa behandlingen eller överföra den registrerades personuppgifter från ett system till ett annat. Om inget annat avtalats, har leverantören rätt att fakturera beställaren enligt priserna i avtalet om leverantören orsakas extra kostnader på grund av hjälpen. Leverantören är skyldig att på förhand informera beställaren om eventuella extra kostnader.

(7) Leverantören ska möjliggöra och bidra till granskningar som genomförs av beställaren eller av en annan revisor som bemyndigats av beställaren. De detaljerade villkoren för granskningsförfarandet finns i de allmänna avtalsvillkoren för IT-upphandlingar inom den offentliga förvaltningen (JIT 2015 – Allmänna villkor) och i avtalet.

5 Beställarens anvisningar

(1) Vid behandlingen av beställarens personuppgifter ska leverantören iaktta villkoren i avtalet och i dessa specialvillkor samt beställarens skriftliga anvisningar. Beställaren ansvarar för att anvisningarna är uppdaterade och tillgängliga. Leverantören ska utan obefogat dröjsmål informera beställaren om beställarens anvisningar är bristfälliga eller om leverantören misstänker att de strider mot lagen.

(2) Beställaren har rätt att ändra, komplettera och uppdatera sina anvisningar om behandling av personuppgifter och dataskydd. Om de ändrade anvisningarna ger upphov till större än ringa förändringar i anslutning till de avtalade tjänsterna, ska effekterna av förändringarna avtalas i ett förfarande för ändringshantering.

6 Personal

(1) Leverantören ska säkerställa att alla personer som arbetar under dess överinseende och som har rätt att behandla beställarens personuppgifter, har förbundit sig att följa de avtalade sekretessvillkoren eller att de omfattas av den lagstadgade tystnadsplikten.

(2) Leverantören ska säkerställa att alla personer som arbetar under dess överinseende och som får tillgång till personuppgifter, känner till sina skyldigheter i samband med behandling av personuppgifter och endast behandlar personuppgifter i enlighet med avtalet, dessa specialvillkor och beställarens anvisningar.

7 Underleverantörer som behandlar personuppgifter

(1) Om en underleverantör till leverantören ska behandla beställarens personuppgifter, förutsätter användningen av underleverantören ett skriftligt förhandstillstånd från beställaren.

(2) Leverantören ska ingå ett skriftligt avtal med underleverantören, som förbinder underleverantören att för sin del iaktta leverantörens avtalsenliga skyldigheter och beställarens gällande anvisningar om behandling av personuppgifter. Leverantören ska säkerställa att beställarens avtalsenliga rätt till insyn kan omfatta underleverantören.

(3) Leverantören ansvarar för underleverantörens andel på samma sätt som för sin egen. Leverantören ansvarar för att underleverantören för sin del fullgör de skyldigheter som ålagts personuppgiftsbiträdet.

(4) Beställaren ska informeras på förhand om utbyte av en underleverantör som deltar i behandling av personuppgifter. Anmälan ska beskriva hur underleverantören behandlar beställarens personuppgifter i

enlighet med dataskyddslagstiftningen. Beställaren har rätt att av grundad anledning motsätta sig den föreslagna underleverantören.

8 Platsen för tjänsten

(1) Om inget annat har avtalats om platsen där tjänsten produceras, har leverantören rätt att behandla beställarens personuppgifter endast inom Europeiska ekonomiska samarbetsområdet. Det som bestäms om behandling av personuppgifter i avtalet och dessa specialvillkor, gäller även möjligheten att få tillgång till beställarens personuppgifter till exempel via förvaltnings- och tillsynsförbindelsen.

(2) Om avtalsparterna kommer överens om att leverantören får överföra beställarens personuppgifter till en plats utanför Europeiska ekonomiska samarbetsområdet, ska avtalsparterna se till att överföringen av personuppgifter genomförs i enlighet med lagstiftningen.

9 Personuppgiftsincidenter

(1) Leverantören ska oavsett den avtalade betjäningstiden utan onödigt dröjsmål göra en skriftlig anmälan till beställaren om personuppgiftsincidenter som kommer till leverantörens kännedom och som rör beställarens personuppgifter. Därtill ska leverantören utan onödigt dröjsmål informera beställaren om andra väsentliga störningar i eller problem med tjänsten, som kan påverka de registrerades ställning och rättigheter.

(2) Leverantörens skriftliga anmälan till beställaren om en personuppgiftsincident ska innehålla åtminstone följande information:

i. en beskrivning av den inträffade personuppgiftsincident, inbegripet de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs, med så detaljerade uppgifter som leverantören har kännedom om;

ii. namnet på och kontaktuppgifterna till dataskyddsombudet eller en annan kontaktperson, som kan ge mer information om ärenden;

iii. en beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten;

iv. 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.

(3) När en personuppgiftsincident har upptäckts ska leverantören utan dröjsmål vidta de avtalade åtgärderna för att undanröja personuppgiftsincidenten och begränsa och åtgärda dess effekter.

10 Upphörande av behandling av personuppgifter

(1) Under avtalets giltighetstid får leverantören inte radera personuppgifter som leverantören behandlar för beställarens räkning utan att beställaren uttryckligen begär det.

(2) När avtalet upphör eller hävs återlämnar leverantören till beställaren alla personuppgifter som leverantören har behandlat för beställarens räkning samt raderar på egen bekostnad eventuella kopior av personuppgifterna från sina egna medier, om inget annat har avtalats. Uppgifterna får inte raderas om

lagstiftning eller en myndighetsbestämmelse kräver att leverantören sparar personuppgifterna. Leverantören har inte rätt att göra en separat debitering för återlämnandet av personuppgifter, om inget annat har avtalats.