**Lathund för att fylla i PuB-avtalsinstruktion**

Innehållsförteckning

Inledning

I vilka situationer ska vi ha ett PuB-avtal?

När ni köper en tjänst av en leverantör ska ni som regel ha någon form av skriftligt avtal med leverantören. I avtalet bör det framgå vad det är för tjänst, vad priset är för tjänsten etc.

I vissa särskilda situationer måste ni ha ytterligare ett avtal med tjänsteleverantören, alltså två stycken olika avtal totalt:

* Det första avtalet är ett vanligt avtal, t.ex. köp av tjänst.
* Det andra avtalet är ett personuppgiftsbiträdesavtal (PuB-avtal), vilket är ett särskilt avtal som innehåller regler för behandling av personuppgifter.

Ni måste ha ett PuB-avtal med alla leverantörer som behandlar personuppgifter för er räkning.

**Exempel**

Exempelvis kanske ni använder er av ett IT-system för att administrera de anställdas löneuppgifter, så som:

* Förnamn
* Efternamn
* Personnummer
* bankkontonummer mm.

Låt säga att ni har köpt detta IT-system av det påhittade företaget *LöneSystem AB*. Eftersom LöneSystem AB har tillgång till personuppgifterna i IT-systemet, som ni är ansvariga för, måste ni ha ett PuB-avtal med LöneSystem AB.

Varför ska vi ha ett PuB-avtal?

Enligt dataskyddsförordningen (GDPR) måste alla som är ansvariga för personuppgiftsbehandlingar (personuppgiftsansvariga) ha ett PuB-avtal med de leverantörer som hjälper till att behandla personuppgifter på något vis.

Följande framgår dock inte inte av dataskyddsförordningen:

* den exakta gränsen för hur många personuppgifter som måste behandlas för att ett PuB-avtal måste upprättas
* hur ofta personuppgifterna kommer behandlas för att ett PuB-avtal måste upprättas
* eller vilka slags personuppgifter som kommer behandlas för att ett PuB-avtal måste upprättas.

Eftersom det inte finns någon exakt gräns för något av ovanstående exempel kan ni utgå från att ni behöver ha ett PuB-avtal med en leverantör om leverantören kommer behandla personuppgifter om t.ex. församlingarnas eller pastoratens:

* medlemmar
* anställda eller,
* andra personer med koppling till församlingarna och pastoraten.

Vad består avtalet av?

Ett PuB-avtal kan delas upp i tre delar.

1. **Avtalstexten**

Den första delen är själva avtalstexten. Av den avtalsmall ni har fått tillgång till avser denna del allt från avsnitt 1 ”Parterna, parternas ställning, kontaktuppgifter och kontaktpersoner” till avsnitt 24 ”Parternas undertecknande av PuB-avtalet”.

Själva avtalstexten kommer vara densamma oavsett vilken leverantör ni använder er av. Den behöver ni alltså inte uppdatera, annat än kontaktuppgifter till er och leverantören.

1. **Instruktionen**

Instruktionen är den första av två bilagor som tillhör varje PuB-avtal. Instruktionen kommer ni behöva fylla i varje gång ni upprättar ett nytt PuB-avtal med en leverantör. Instruktionen är bindande precis på samma vis som själva avtalstexten är bindande.

Det är i instruktionen som ni anger exakt vad det är som er leverantör får göra och inte får göra med de personuppgifter som ni är ansvariga för.

I instruktionen anger ni t.ex:

* Vad syftet är med personuppgiftsbehandlingen

(att bistå med ett IT-system för löneadministration)

* Vilka personuppgifter som leverantören får behandla

(så som t.ex. förnamn, efternamn, personnummer, bankkontonummer mm)

**Instruktionen har åtta stycken rutor och varje ruta har en egen rubrik. I varje ruta finns det möjlighet att ge en särskild instruktion kopplad till rubriken.**

* Den första rutan har rubriken ”Ändamål, föremålet och arten”. I denna ruta fyller ni t.ex. i vad ändamålet är med personuppgiftsbehandlingen.
* Den andra rutan har rubriken ”Behandlingen omfattar följande typer av personuppgifter”. I denna ruta fyller ni typerna av personuppgifter som kommer behandlas, t.ex. förnamn, efternamn, e-postadress etc.
1. **Lista på godkända underbiträden**

Listan på godkända underbiträden är den andra bilagan som tillhör varje PuB-avtal. Den bilagan är till för att ni ska veta vilka andra företag än ert personuppgiftsbiträde som kan komma att behandla de personuppgifter ni är ansvariga för.

*Varför måste då andra företag anges i avtalet, vi har ju bara en leverantör?*

Jo det är för att er leverantör kan komma att behöva hjälp av något annat/några andra företag för att kunna utföra den personuppgiftsbehandling som leverantören utför på uppdrag av er. Det är vanligt att företag behöver hjälp av andra företag för att utföra den tjänst som de säljer.

*Vem fyller i listan på godkända underbiträden?*

Det är ert personuppgiftsbiträde som fyller i listan och anger vilka underbiträden de tänker använda sig av. Genom att skriva på PuB-avtalet godkänner ni de underbiträden som ert personuppgiftsbiträde har angett på listan.

**Exempel**

I exemplet med LöneSystem AB kan det vara så att LöneSystem AB har ett avtal med *IT-Support AB* där IT-Support AB har i uppdrag att:

* hjälpa till med att åtgärda problem som kan uppstå med det IT-system för löneadministration som ni har köpt av LöneSystem AB.

Eftersom IT-Support AB måste få tillgång till ert IT-system för löneadministration för att kunna hjälpa er att lösa de problem som kan uppstå, är det mycket möjligt att även IT-Support AB får tillgång till de personuppgifter som finns i IT-systemet för löneadministration.

I en sådan situation måste LöneSystem AB meddela er att de kommer att använda IT-Support AB för att hjälpa till med att lösa eventuella problem med IT-systemet för löneadministration. Om ni godkänner att LöneSystem AB får använda sig av IT-Support AB för att lösa eventuella problem i systemet så ska IT-Support AB *anges i listan över godkända underbiträden*. Det är denna lista som är den andra bilagan till PuB-avtalet.

Lathundsbeskrivning för instruktion (bilaga 1)

Instruktionen är uppdelad i åtta stycken rutor med tillhörande rubrik. Här följer en beskrivning av vad ni ska fylla i för information i varje ruta.

Ändamål, föremålet och arten

I denna ruta ska ni fylla i vad syftet, föremålet och arten är för personuppgiftsbehandlingen.

**Exempel**

I vårt exempel med LöneSystem AB kan ändamålet, föremålet och arten beskrivas som:

* *Ändamålet* – är att administrera löneutbetalningar till anställda.
* *Föremålet* – är själva IT-systemet
* *Arten* – kan t.ex. vara IT-drift, tekniskt underhåll och säkerhetskopiering. Arten kan variera beroende på vad det är för tjänst ni köper.

I vårt exempel med LöneSystem AB kan ni fylla i rutan med följande:

* Personuppgiftsbiträdet kommer behandla samtliga personuppgifter i IT-system för löneadministration i syfte att administrera löneutbetalningar, bistå med IT-drift, tekniskt underhåll och säkerhetskopiering.

Behandlingen omfattar följande typer av Personuppgifter

I denna ruta ska ni fylla i vilka typer av personuppgifter som er leverantör kommer behandla för er räkning, alltså vilka personuppgifter som er leverantör kommer få tillgång till på något sätt.

I vårt exempel med LöneSystem AB kommer företaget t.ex. få tillgång till:

* Förnamn
* Efternamn
* Tjänst
* Sjukfrånvaro
* Ledighet
* Semester
* Bank
* Bankkontonummer
* Clearing nummer

Det ni ska göra är helt enkelt att fylla i exakt vilka typer av personuppgifter som kommer behandlas. Undvik ord så som etc, mfl, mm, eftersom det inte går att veta exakt vilka typer av personuppgifter ni avser.

**Exempel**

I vårt exempel med LöneSystem AB så kommer företaget behandla många olika typer av personuppgifter. Så är inte fallet med alla leverantörer, utan det beror helt och hållet på vad det är för tjänst ni har köpt. Det kan uppstå situationer då leverantören endast kommer behandla några anställdas förnamn, efternamn och e-postadresser i en kontaktlista. I ett sådant fall fyller ni i rutan med följande typer av personuppgifter:

* Förnamn
* Efternamn
* E-postadress

Behandlingen omfattar följande kategorier av Registrerade

I denna ruta ska ni fylla i vilka kategorier av registrerade vars personuppgifter er leverantör kommer behandla.

**Exempel**

I vårt exempel med LöneSystem AB kommer de behandla de anställdas personuppgifter. Då fyller ni i följande i rutan:

* Anställda

Ange särskilda hanteringskrav vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet/biträdena

I denna ruta ska ni fylla de särskilda hanteringskrav som ni kan ha.

*Vad är särskilda hanteringskrav?*

Det kan t.ex. var att ni har särskilda krav på hur länge er leverantör får spara personuppgifterna, hur länge leverantören får spara säkerhetskopior etc.

Om ni t.ex. vill att personuppgifter ska gallras (raderas) efter ett år kan ni fylla i rutan med följande:

* Personuppgifterna ska gallras efter ett år.

Ni måste inte fylla i denna ruta. Är det så att ni inte har några särskilda hanteringskrav så kan ni lämna denna ruta tom.

Ange särskilda tekniska och organisatoriska säkerhetsåtgärder vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet/biträdena

I denna ruta ska ni fylla i de särskilda tekniska och organisatoriska säkerhetsåtgärder ni kan ha.

*Vad är tekniska och organisatoriska säkerhetsåtgärder för något?*

Jo det är sådana åtgärder som en organisation kan vidta för att säkerställa att information, i det här fallet personuppgifter, hanteras och behandlas på ett säkert sätt.

En teknisk säkerhetsåtgärd kan t.ex. vara kryptering, alltså att personuppgifterna inte är läsbara för alla. En organisatorisk säkerhetsåtgärd kan t.ex. vara behörighetsbegränsning, alltså att endast ett fåtal personer har tillgång till personuppgifterna.

Om ni har tekniska eller organisatoriska säkerhetsåtgärder som ni vill att er leverantör använder, så som de ovanstående exemplen kryptering och behörighetsbegräsning, kan ni fylla i följande i rutan:

* Biträdet ska använda sig av kryptering för att säkerställa personuppgifternas säkerhet.
* Biträdet ska säkerställa att endast de personer som behöver tillgång till personuppgifterna har tillgång. Behörigheten till personuppgifterna ska tilldelas utifrån principen om ”minsta möjliga behörighet”.

Ni måste inte fylla i denna ruta. Är det så att ni inte har några särskilda tekniska eller organisatoriska säkerhetsåtgärder som ni vill att er leverantör ska använda kan ni lämna denna ruta tom.

Ange särskilda krav på Loggning vad gäller Behandling av Personuppgifter samt vilka som ska ha tillgång till dem

I denna ruta ska ni fylla i särskilda krav på loggning och vilka av er leverantörs anställda som ska ha tillgång till loggarna.

*Vad är loggning för något?*

Loggning är en funktion som finns i vissa system vilket gör det möjligt att se vilka aktiviteter som har skett i systemet, alltså en slags aktivitetshistorik. Beroende på hur avancerad loggningsfunktionen är kan det vara möjligt att se:

* vilken användare som har gjort vad, så som att öppna, lägga till eller ta bort en fil
* vilken tidpunkt som en viss aktivitet skedde

Loggning kan vara särskilt viktigt om leverantören kommer behandla känsliga personuppgifter. En känslig personuppgift kan t.ex. vara en uppgift som avslöjar religiös övertygelse eller uppgift om hälsa. Skulle det vara så att ett system kommer behandla personuppgifter som avslöjar religiös övertygelse eller uppgift om hälsa kan det vara en bra idé att ställa krav på loggning. Ni skulle då kunna fylla i rutan enligt följande:

* Av loggar ska framgå;
* Historik över förändring av de kategorier av känsliga personuppgifter som instruktionen avser.

Ni måste inte fylla i denna ruta. Är det så att ni inte har några särskilda krav på loggning så kan ni lämna denna ruta tom.

Lokalisering och överföring av Personuppgifter till Tredje land

I denna ruta ska ni fylla i de krav ni ställer på vart någonstans leverantören och leverantörens underbiträden får utföra personuppgiftbehandlingen och om personuppgifterna får överföras till tredje land.

**I denna ruta kan ni ställa fyra olika slags krav:**

1. Vart personuppgiftsbiträdet och underbiträdena får vara lokaliserade.
2. Vilken laglig grund för överföring av personuppgifter till tredje land som ni godkänner.
3. Vilka typer av personuppgifter som underbiträdena får behandla.
4. Vilka personuppgifter som får överföras till tredje land, alltså länder utanför EU/EES.

***Krav nr 1***

Det är viktigt att ni fyller i information i denna ruta med de krav ni ställer.

Ni bör ställa krav på att personuppgifterna endast får behandlas av biträden som är etablerade inom EU/EES. Ni kan fylla i rutan enligt följande:

* Personuppgifterna får endast behandlas av ett biträde etablerat inom EU/EES.

***Krav nr 2***

Det är viktigt att ni fyller i information i denna ruta om de krav ni ställer.

*Vad är laglig grund för överföring av personuppgifter till tredje land?*

När en organisation tänker överföra personuppgifter ett annat land är ett EU-lan eller EES-land (Norge, Island och Liechtenstein) måste organisationen ha ett särskilt stöd att luta sig på för att detta ska vara tillåtet.

Detta särskilda stöd kallas laglig grund och det finns bara ett fåtal lagliga grunder en organisation kan använda sig av.

Ni bör ställa krav på att personuppgifter endast får överföras till tredje land om det föreligger ett beslut från Kommissionen om adekvat skyddsnivå, vilket är den lagliga grunden. Ni kan fylla i rutan enligt följande:

* Personuppgifter får endast överföras till de länder för vilka Kommissionen har fattat ett beslut om att en adekvat skyddsnivå föreligger.

***Krav nr 3***

I denna ruta har ni möjlighet att ställa krav på vilka typer av personuppgifter som ni godkänner att ett eventuellt underbiträde kan få tillgång till.

Om ert personuppgiftsbiträde kommer behandla känsliga personuppgifter kan ni ställa krav på att underbiträden inte får behandla känsliga personuppgifter så till vida att det inte omöjliggör ert personuppgiftsbiträdes möjlighet att uppfylla sina avtalsförpliktelser enligt huvudavtalet och PuB-avtalet. Ni kan fylla i rutan enligt följande:

* Känsliga personuppgifter får inte överföras till personuppgiftsbiträdes underbiträden.

***Krav nr 4***

I denna ruta har ni möjlighet att ställa krav på vilka typer av personuppgifter som får föras över till tredje land.

Ni bör ställa krav på att inga känsliga personuppgifter får överföras till tredje land. Ni kan fylla i rutan enligt följande:

* Inga känsliga personuppgifter får överföras till tredje land, oavsett vilken laglig grund för överföring som kan tillämpas.

Övriga instruktioner angående behandling av personuppgifter som utföras av biträdet/biträdena

I denna ruta ska ni fylla övriga instruktioner som ni vill lämna till ert personuppgiftsbiträde. Det skulle exempelvis kunna vara att ni anger att en viss del av avtalstexten inte gäller eller att en viss del av avtalstexten ska kompletteras.

Ni måste inte fylla i denna ruta. Är det så att ni inte har några övriga instruktioner så kan ni lämna denna ruta tom.