Personuppgiftsbiträdesavtal – Plask

Version: 1.14

Detta personuppgiftsbiträdesavtal (”Biträdesavtalet”) är en del av avtalet om kundens användning av Plask (”Huvudavtalet”).

1. Parter

Personuppgiftsansvarig (”Kunden”)
Den juridiska person som har ingått Huvudavtalet eller accepterat detta Biträdesavtal. Kundens juridiska namn, organisationsnummer, kontaktuppgifter och behöriga företrädare dokumenteras tillsammans med accepten.

Personuppgiftsbiträde (”Plask”)
AddSoftware i Norden AB
Org.nr: 559464-8742
Gunnarskogs gränd 4, 671 31 Arvika
`support@plask.nu`

2. Omfattning och roller

Kunden bestämmer ändamålen och de väsentliga medlen för behandlingen av de personuppgifter som Kunden lägger in eller skapar i Plask och är personuppgiftsansvarig för dem. Plask behandlar uppgifterna som personuppgiftsbiträde endast för att tillhandahålla, säkra, underhålla och ge support för tjänsten.

Behandlingens föremål, varaktighet, art, ändamål, personuppgiftstyper och kategorier av registrerade beskrivs i bilagan Behandling, säkerhet och leverantörer, som är en del av Biträdesavtalet och finns publicerad på https://app.plask.nu/dpa#bilaga.

För Plasks egna användarkonton, inloggning, säkerhetsadministration, support- och avtalskontakter kan AddSoftware i Norden AB vara självständigt personuppgiftsansvarig. Den behandlingen omfattas inte av instruktionerna i detta Biträdesavtal.

3. Kundens ansvar och instruktioner

Kunden ansvarar för att

- behandlingen har rättslig grund och är öppen gentemot de registrerade,
- uppgifterna är relevanta och begränsade till vad verksamheten behöver,
- användare har rätt behörighet och skyddar sina konton,
- inte lägga in hälsouppgifter eller andra särskilda kategorier av personuppgifter i Plask, och
- dokumenterade instruktioner är förenliga med dataskyddslagstiftningen.

Huvudavtalet, Biträdesavtalet, Kundens inställningar och normala användning av Plask utgör Kundens dokumenterade instruktioner. Ytterligare instruktioner ska vara skriftliga och överenskommas mellan parterna. Om Plask bedömer att en instruktion strider mot GDPR eller annan dataskyddslag ska Kunden informeras utan onödigt dröjsmål och behandlingen pausas i berörd del i den mån det är möjligt.

Plask får behandla uppgifter på annat sätt om det krävs enligt EU-rätt eller svensk rätt. Plask ska då informera Kunden före behandlingen, om inte lagen förbjuder sådan information.

4. Konfidentialitet och säkerhet

Plask ska säkerställa att personer som får behandla Kundens personuppgifter endast gör det enligt instruktion och omfattas av lämplig sekretessförbindelse eller lagstadgad tystnadsplikt.

Plask ska vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder enligt artikel 32 GDPR med hänsyn till behandlingens art, kostnad, teknikens ståndpunkt och riskerna för de registrerade. Nuvarande huvudåtgärder anges i bilagan. Åtgärder får utvecklas under avtalstiden om den samlade skyddsnivån inte väsentligen försämras.

5. Underbiträden

Kunden ger Plask ett generellt skriftligt tillstånd att anlita de underbiträden som anges i bilagan. Plask ska

- ingå skriftligt avtal som ålägger underbiträdet dataskyddsskyldigheter som i sak motsvarar skyldigheterna i detta Biträdesavtal,
- ansvara gentemot Kunden för underbiträdets fullgörande av dessa skyldigheter, och
- informera Kunden minst 30 dagar före ett planerat tillägg eller byte så att Kunden kan invända på sakliga dataskyddsgrunder.

Om parterna inte kan lösa en berättigad invändning får Kunden upphöra att använda den berörda behandlingen eller säga upp Huvudavtalet enligt dess villkor.

6. Behandling utanför EU/EES

Plask får endast överföra personuppgifter utanför EU/EES enligt Kundens instruktioner och om kraven i GDPR kapitel V är uppfyllda. När adekvansbeslut inte kan användas ska lämpligt överföringsstöd användas, normalt EU-kommissionens standardavtalsklausuler tillsammans med kompletterande skyddsåtgärder när det krävs.

7. Registrerades rättigheter

Plask ska, med hänsyn till behandlingens art, genom lämpliga tekniska och organisatoriska åtgärder hjälpa Kunden att besvara begäran enligt artiklarna 12–22 GDPR. Om en begäran om Kundens uppgifter kommer direkt till Plask ska Plask utan onödigt dröjsmål hänvisa eller vidarebefordra den till Kunden och inte besvara den i sak utan Kundens instruktion, om inte lag kräver annat.

8. Personuppgiftsincidenter

När Plask får vetskap om en personuppgiftsincident som berör Kundens uppgifter ska Plask underrätta Kundens dataskyddskontakt utan onödigt dröjsmål. Plask ska lämna tillgänglig information successivt och, så långt den är känd, beskriva

- incidentens art och tid,
- berörda kategorier och ungefärlig omfattning,
- sannolika konsekvenser,
- vidtagna eller planerade begränsningsåtgärder, och
- kontaktpunkt för fortsatt hantering.

Plask ska skäligen bistå Kundens dokumentation, riskbedömning och skyldigheter enligt artiklarna 33 och 34 GDPR. Kunden ansvarar för beslut om anmälan till tillsynsmyndighet och information till registrerade, om parterna inte uttryckligen kommer överens om annat.

9. Konsekvensbedömning och samråd

Plask ska med hänsyn till behandlingens art och tillgänglig information skäligen bistå Kunden med säkerhet, konsekvensbedömning och eventuellt förhandssamråd enligt artiklarna 32 och 35–36 GDPR.

10. Radering och återlämning

Under avtalstiden kan Kunden radera uppgifter genom tjänstens funktioner eller ge Plask en skriftlig instruktion. När Huvudavtalet upphör ska Plask efter Kundens val radera eller återlämna Kundens personuppgifter och radera återstående kopior, om inte EU-rätt eller svensk rätt kräver fortsatt lagring. Om Kunden inte begär återlämning behandlas avslutet som en instruktion att radera uppgifterna enligt Plasks ordinarie avslutsprocess.

Uppgifter kan finnas kvar i isolerade säkerhetskopior tills dessa skrivs över eller gallras automatiskt enligt Plasks dokumenterade backup-rutin. Sådana uppgifter får inte återföras till normal drift annat än vid nödvändig återställning och ska då omfattas av den ursprungliga raderingsinstruktionen. Redan levererade mejl hos mottagarens e-postleverantör ligger utanför Plasks kontroll.

Närmare lagringstider och gallringsåtgärder framgår av gallringsrutinen i bilagan, som utgör en del av Kundens dokumenterade instruktion.

11. Information och granskning

Plask ska tillhandahålla den information som skäligen behövs för att visa att skyldigheterna i artikel 28 GDPR följs. Kunden får högst en gång per år, samt efter en väsentlig incident eller på krav från tillsynsmyndighet, begära en rimligt avgränsad granskning.

Parterna ska i första hand använda dokumentation, intyg och skriftliga svar. En inspektion ska aviseras i rimlig tid, ske under sekretess och får inte äventyra andra kunders uppgifter eller Plasks säkerhet. Kunden står för sina och Plasks skäliga merkostnader, om granskningen inte visar ett väsentligt avtalsbrott från Plask.

12. Giltighet, ansvar och övrigt

Biträdesavtalet gäller så länge Plask behandlar personuppgifter för Kundens räkning. Vid konflikt om dataskyddsfrågor har Biträdesavtalet företräde framför Huvudavtalet. Ansvar, ansvarsbegränsningar, tillämplig lag och tvist följer Huvudavtalet i den utsträckning tvingande dataskyddslag inte kräver annat.

Biträdesavtalet kan accepteras elektroniskt, exempelvis av en behörig administratör i tjänsten eller genom ett skriftligt meddelande som hänvisar till avtalets version. Accepten ska dokumentera Kundens juridiska namn och organisationsnummer, vem som accepterade, personens behörighet, datum och den accepterade versionen. Parterna kan i stället underteckna avtalet separat om de önskar.