SPA & POOL CONTROL

Smartare. Enklare. Effektivare.

PERSONUPPGIFTS-BITRÄDESAVTAL (DPA)

Spa & Pool Control

Vi skyddar dina uppgifter – på ditt uppdrag

Säkerhet • Ansvar • Regelefterlevnad

DOKUMENT	VERSION	UPPDATERAD
Personuppgiftsbiträdesavtal (DPA)	1.0	Augusti 2026

Innehåll

1. Parter, avtalets ställning och företräde

Detta personuppgiftsbiträdesavtal ("DPA") ingås mellan Kunden som personuppgiftsansvarig och Philip Ahlqvist, som tillhandahåller tjänsten under namnet Spa & Pool Control ("Personuppgiftsbiträdet" eller "Leverantören").

DPA utgör en integrerad del av avtalet om Tjänsten och accepteras elektroniskt samtidigt med Användarvillkoren när en behörig företrädare för Kunden klickar på "Godkänn" i Tjänsten. Leverantören får dokumentera tidpunkt, Kund, användaridentitet och accepterad dokumentversion för att kunna visa vilket DPA som gäller mellan parterna.

DPA och övriga avtalsdokument ska göras tillgängliga före godkännandet på ett sätt som gör det möjligt för Kunden att spara och återge dem.

DPA är en integrerad del av avtalet om Spa & Pool Control och gäller när Leverantören behandlar personuppgifter för Kundens räkning. Vid motstridighet har DPA företräde i frågor om personuppgiftsbehandling.

DPA ska uppfylla artikel 28 GDPR och ska tolkas så att Kundens dokumenterade instruktioner, GDPR och annan tvingande dataskyddsrätt får fullt genomslag. DPA reglerar inte Leverantörens separata behandling som självständig personuppgiftsansvarig, vilken beskrivs i Integritetspolicyn.

2. Definitioner

Begrepp	Betydelse
GDPR	Europaparlamentets och rådets förordning (EU) 2016/679.
Personuppgifter	Varje upplysning som avser en identifierad eller identifierbar fysisk person enligt GDPR.
Behandling	Varje åtgärd eller kombination av åtgärder som vidtas beträffande Personuppgifter, såsom insamling, registrering, strukturering, lagring, läsning, användning, överföring, radering eller annan behandling.
Personuppgiftsansvarig	Kunden, i den utsträckning Kunden bestämmer ändamål och medel för behandlingen.
Personuppgiftsbiträde	Leverantören, i den utsträckning Leverantören behandlar Personuppgifter för Kundens räkning.
Underbiträde	Tredje part som Leverantören anlitar för att behandla Personuppgifter för Kundens räkning.
Personuppgiftsincident	Säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust, ändring, obehörigt röjande av eller obehörig åtkomst till Personuppgifter.
Tjänsten	Spa & Pool Control och de funktioner som omfattas av Kundens avtal.

3. Roller och dokumenterade instruktioner

Kunden är Personuppgiftsansvarig och ansvarar för att det finns rättslig grund, korrekt information till registrerade och i övrigt lagliga ändamål och instruktioner för behandlingen.

Leverantören får endast behandla Personuppgifter enligt dokumenterade instruktioner från Kunden, inklusive instruktioner om överföringar till tredjeland eller internationell organisation, om inte Leverantören enligt unionsrätt eller svensk rätt är skyldig att behandla uppgifterna på annat sätt. I sådant fall ska Kunden informeras före behandlingen, om inte lag förbjuder informationen.

Kundens dokumenterade instruktioner består av detta DPA och Bilaga 1, Kundens användning och konfiguration av Tjänsten, aktiverade integrationer och ytterligare skriftliga instruktioner från behörig företrädare.

Om Leverantören bedömer att en instruktion strider mot GDPR eller annan tillämplig dataskyddsrätt ska Kunden informeras utan onödigt dröjsmål. Leverantören får pausa den berörda instruktionen till dess att frågan har klargjorts, när detta är nödvändigt för att undvika en olaglig behandling.

Leverantören får inte använda Kundens Personuppgifter för egen direktmarknadsföring, egen produktprofilering eller andra självständiga ändamål som är oförenliga med rollen som Personuppgiftsbiträde.

4. Behandlingens omfattning

Föremål, varaktighet, art och ändamål för behandlingen, typer av Personuppgifter, kategorier av registrerade samt Kundens rättigheter och skyldigheter framgår av Bilaga 1. Bilagan utgör en bindande behandlingsinstruktion enligt artikel 28.3 GDPR.

Leverantören får utföra de behandlingsmoment som är nödvändiga för att tillhandahålla, driva, underhålla, säkerhetskopiera, säkra, supportera och på Kundens instruktion integrera Tjänsten, men får inte utvidga ändamålet på egen hand.

Leverantören ska föra sådant register över behandling som krävs av artikel 30.2 GDPR.

5. Konfidentialitet och åtkomst

Leverantören ska säkerställa att anställda, konsulter och andra personer som får behandla Personuppgifter har åtagit sig konfidentialitet eller omfattas av lämplig lagstadgad tystnadsplikt.

Åtkomst ska begränsas till personer med ett dokumenterat verksamhetsbehov och i möjligaste mån följa principerna om minsta privilegium och behovsstyrd åtkomst. Behörigheter ska kunna återkallas när behovet upphör.

Sekretesskyldigheten gäller även efter att personens uppdrag eller detta DPA har upphört.

6. Tekniska och organisatoriska säkerhetsåtgärder

Leverantören ska vidta alla säkerhetsåtgärder som krävs enligt artikel 32 GDPR med beaktande av den tekniska utvecklingen, genomförandekostnader, behandlingens art, omfattning, sammanhang och ändamål samt riskerna för registrerades rättigheter och friheter.

Säkerhetsåtgärderna ska, där de är relevanta för risken, omfatta förmåga att säkerställa fortlöpande konfidentialitet, integritet, tillgänglighet och motståndskraft, förmåga att återställa tillgång till Personuppgifter inom rimlig tid efter en incident samt ett förfarande för regelbunden testning, bedömning och utvärdering av åtgärdernas effektivitet.

Minimikategorier av säkerhetsåtgärder framgår av Bilaga 2. Leverantören får förbättra eller ersätta åtgärderna under avtalstiden under förutsättning att den övergripande skyddsnivån inte väsentligen försämras.

7. Underbiträden

Kunden ger Leverantören ett allmänt skriftligt förhandstillstånd att anlita Underbiträden enligt detta avsnitt och Bilaga 3.

Aktuell förteckning över Underbiträden ska hållas tillgänglig på https://spaopoolcontrol.se/juridik/underbitraden. Leverantören ska säkerställa att Underbiträdet genom skriftligt avtal åläggs dataskyddsskyldigheter som i sak motsvarar de skyldigheter som är relevanta enligt detta DPA och artikel 28 GDPR.

Leverantören ska informera Kunden minst 14 kalenderdagar innan ett nytt Underbiträde börjar behandla Personuppgifter eller en väsentlig förändring görs, om inte en akut säkerhets- eller kontinuitetssituation kräver snabbare byte. Vid akut byte ska Kunden informeras så snart det är rimligt möjligt.

Kunden får inom 10 kalenderdagar från meddelandet invända på sakliga dataskyddsgrunder. Parterna ska därefter i god tro försöka hitta en rimlig lösning, exempelvis en alternativ teknisk lösning. Om ingen lösning är möjlig får Kunden säga upp den del av Tjänsten som berörs innan Underbiträdet börjar användas, utan ytterligare avgift för den återstående förskottsbetalda perioden för just den delen.

Leverantören är fullt ansvarig gentemot Kunden för ett Underbiträdes fullgörande av de dataskyddsskyldigheter som Leverantören lagt ut på Underbiträdet, i den utsträckning GDPR kräver.

8. Internationella överföringar

Leverantören får endast överföra Personuppgifter till ett land utanför EES enligt Kundens dokumenterade instruktion och när överföringen uppfyller kapitel V GDPR.

Överföringsmekanism kan exempelvis vara EU-kommissionens beslut om adekvat skyddsnivå eller standardavtalsklausuler (SCC) tillsammans med en bedömning av överföringen och kompletterande skyddsåtgärder när det krävs.

På begäran ska Leverantören lämna rimlig information om tillämplig överföringsmekanism och relevanta kompletterande skyddsåtgärder, med nödvändiga begränsningar för säkerhet, affärshemligheter och andra kunders uppgifter.

9. Bistånd till Kunden och registrerades rättigheter

Med beaktande av behandlingens art ska Leverantören genom lämpliga tekniska och organisatoriska åtgärder bistå Kunden så långt det är möjligt med att fullgöra registrerades rättigheter enligt kapitel III GDPR, inklusive tillgång, rättelse, radering, begränsning, dataportabilitet och invändning när rättigheten är tillämplig.

Leverantören ska, med beaktande av behandlingens art och den information som finns tillgänglig, bistå Kunden med skyldigheterna enligt artiklarna 32-36 GDPR, inklusive säkerhet, incidenthantering, konsekvensbedömning (DPIA) och förhandssamråd med tillsynsmyndighet.

En begäran från en registrerad som Leverantören tar emot direkt och som avser Kundens behandling ska utan onödigt dröjsmål vidarebefordras till Kunden. Leverantören ska inte själv avgöra begäran utan Kundens instruktion, om inte lag kräver annat.

Bistånd som kan lämnas genom Tjänstens standardfunktioner ingår i ordinarie avgift. Om Kunden begär omfattande manuellt arbete som går utöver standardfunktionerna får Leverantören ta skälig ersättning efter förhandsinformation, utom i den mån arbetet är nödvändigt på grund av Leverantörens eget avtalsbrott eller en brist som Leverantören ansvarar för.

10. Personuppgiftsincidenter

Leverantören ska informera Kunden utan onödigt dröjsmål efter att Leverantören fått vetskap om en Personuppgiftsincident som rör Kundens Personuppgifter. Leverantören behöver inte först bedöma om incidenten medför risk för registrerade innan Kunden informeras.

Meddelandet ska, i den mån informationen finns tillgänglig, beskriva incidentens art, kategorier och ungefärligt antal berörda registrerade, kategorier och ungefärligt antal berörda personuppgiftsposter, sannolika konsekvenser, vidtagna eller planerade åtgärder samt kontaktpunkt för uppföljning. Informationen får lämnas stegvis utan ytterligare onödigt dröjsmål.

Leverantören ska dokumentera relevanta incidenter och bistå Kunden med den information som behövs för Kundens bedömning och eventuella anmälan eller information till registrerade. Det juridiska ansvaret för anmälan till tillsynsmyndighet och information till registrerade ligger hos Kunden, om inte tillämplig lag uttryckligen föreskriver annat eller parterna skriftligen kommit överens om en särskild rapporteringsåtgärd.

Incidentmeddelande ska skickas till den administratörs- eller säkerhetskontakt som Kunden registrerat i Tjänsten och, om en separat incidentadress har lämnats skriftligen, även till den adressen.

11. Revision, inspektion och informationsrätt

Leverantören ska på begäran ge Kunden den information som krävs för att visa att skyldigheterna enligt artikel 28 GDPR och detta DPA har fullgjorts.

Leverantören ska möjliggöra och bidra till revisioner och inspektioner som genomförs av Kunden eller en oberoende revisor som Kunden utsett. Kunden ska i första hand använda tillgängliga säkerhetsrapporter, beskrivningar och skriftliga svar om dessa ger tillräckligt underlag.

Om ytterligare revision behövs får Kunden normalt genomföra högst en revision per tolvmånadersperiod med minst 30 dagars skriftligt varsel, under normal kontorstid och utan oskälig störning. Begränsningen gäller inte efter en allvarlig Personuppgiftsincident, vid välgrundad misstanke om väsentlig brist eller när tillsynsmyndighet eller lag kräver annan granskning.

Revision ska begränsas till Kundens behandling och får inte ge åtkomst till andra kunders uppgifter, källkod, säkerhetsnycklar eller annan information vars röjande skulle skapa en säkerhetsrisk. Leverantören får använda rimliga skyddsåtgärder, såsom sekretessavtal, kontrollerad åtkomst och maskning, men får inte åberopa sådana skydd som skäl för att vägra en revision som krävs enligt artikel 28.3 h GDPR.

Kunden står för sina och sin revisors kostnader. Leverantören får ta skälig ersättning för betydande extra arbete efter förhandsinformation, utom när revisionen visar en väsentlig brist som Leverantören ansvarar för eller revisionen krävs på grund av en sådan brist.

12. Myndighetsförfrågningar

Om Leverantören får en rättsligt bindande begäran från en myndighet om Kundens Personuppgifter ska Leverantören, i den utsträckning lag medger, informera Kunden innan uppgifter lämnas ut.

Leverantören ska granska begärans rättsliga grund och begränsa utlämnandet till vad som krävs. Leverantören ska inte frivilligt ge en myndighet bredare åtkomst till Kundens Personuppgifter än vad som följer av lag eller Kundens dokumenterade instruktion.

13. Återlämnande och radering

När behandlingen upphör ska Leverantören, enligt Kundens val, radera Personuppgifterna eller göra dem tillgängliga för återlämnande/export och därefter radera befintliga kopior, om inte unionsrätt eller svensk rätt kräver fortsatt lagring.

Kunden ska före eller i samband med upphörandet använda tillgänglig exportfunktion eller begära den standardiserade export som ska tillhandahållas enligt avtalet och tillämplig rätt. Leverantören ska inte villkora den rätt till återlämnande eller radering som följer av artikel 28.3 g med att åtgärden är "tekniskt möjlig".

Personuppgifter i säkerhetskopior som inte kan raderas separat utan oproportionerlig påverkan på backupens integritet får finnas kvar endast under ordinarie backupcykel, ska vara skyddade från ordinarie användning och ska raderas eller skrivas över när backupcykeln medger det. Under denna period fortsätter DPA:s säkerhets- och sekretesskrav att gälla.

Leverantören ska på skriftlig begäran bekräfta att radering har genomförts i enlighet med detta avsnitt, med förbehåll för lagstadgad lagring och tekniskt nödvändiga backupcykler.

14. Ansvar

Vardera parten ansvarar för sina egna skyldigheter enligt GDPR och detta DPA. Kunden ansvarar särskilt för laglig grund, transparens, uppgiftsminimering och lagliga instruktioner. Leverantören ansvarar för behandling som sker i strid med Leverantörens egna skyldigheter som Personuppgiftsbiträde eller utanför lagliga instruktioner.

Mellan parterna gäller huvudavtalets ansvarsbegränsningar även för detta DPA i den utsträckning de är förenliga med tvingande dataskyddsrätt. Ingen begränsning ska tolkas som att den inskränker en registrerads rätt till ersättning eller en tillsynsmyndighets befogenheter enligt GDPR.

Om en part betalar ersättning eller kostnad som enligt tillämplig rätt slutligen hänför sig till den andra partens ansvar får parterna göra regress gällande i den utsträckning som följer av GDPR och tillämplig nationell rätt.

15. Avtalstid och ändringar

DPA gäller från den tidpunkt då Leverantören börjar behandla Personuppgifter för Kundens räkning och så länge sådan behandling pågår. Bestämmelser om sekretess, revision av historisk efterlevnad, radering och ansvar gäller även efter upphörandet i den utsträckning deras natur kräver det.

Leverantören får uppdatera DPA när det krävs av lag, tillsynsbeslut, säkerhet eller en saklig förändring av Tjänsten. En ändring får inte väsentligen sänka den dataskyddsnivå Kunden har enligt GDPR.

Väsentliga ändringar ska meddelas minst 30 dagar i förväg när det är möjligt. Om en ändring är materiellt negativ och inte krävs av tvingande lag får Kunden säga upp den berörda Tjänsten före ikraftträdandet. En ändring som krävs omedelbart av lag eller tillsynsbeslut får träda i kraft från den tidpunkt som krävs.

16. Tillämplig lag och tvister

DPA ska tolkas enligt svensk rätt, med företräde för direkt tillämplig EU-rätt såsom GDPR. Tvist ska hanteras enligt tvistbestämmelsen i huvudavtalet, utan att detta begränsar registrerades rättigheter eller en behörig tillsynsmyndighets befogenheter.

17. Kontaktuppgifter

Personuppgiftsbiträde: Philip Ahlqvist, som tillhandahåller Spa & Pool Control

Dataskydds-/DPA-kontakt: info@spaopoolcontrol.se

Webbplats: https://spaopoolcontrol.se

Kundens incidentkontakt: den administrator som Kunden registrerat i Tjänsten eller annan skriftligen angiven kontakt.

Bilaga 1. Behandlingsinstruktion

Punkt	Instruktion
Föremål	Tillhandahållande och drift av Spa & Pool Control för Kundens räkning, inklusive lagring, ärendehantering, planering, dokumentation, kommunikation, kundportal/delning, protokoll, integrationer, support, säkerhetskopiering och säkerhet i den omfattning Kunden använder funktionerna.
Varaktighet	Under huvudavtalets löptid samt den begränsade tid efter upphörandet som behövs för återlämnande/radering och ordinarie backupcykel, om inte lag kräver längre lagring.
Art av behandling	Insamling på Kundens instruktion, registrering, strukturering, organisering, lagring, läsning, användning, överföring till av Kunden valda mottagare/integrationer, säkerhetskopiering, återställning, felsökning, begränsning och radering.
Ändamål	Att tillhandahålla de funktioner Kunden beställer och konfigurerar i Tjänsten samt att tekniskt säkra, underhålla och supportera dessa funktioner. Leverantören bestämmer inte nya självständiga ändamål för Kunddata.
Kategorier av registrerade	Kundens Användare och personal; Kundens slutkunder, kontaktpersoner, fastighets-/anläggningsägare och servicebeställare; tekniker och underleverantörer; leverantörs-/partnerkontakter; andra personer som Kunden väljer att registrera inom ramen för sin lagliga användning.
Typer av personuppgifter	Namn, e-post, telefon, service-/besöksadress, företagsanknytning, ärende- och arbetsorderdata, serviceanteckningar, protokoll, produkt-/anläggningsinformation, bilder och dokument, kommunikationsinnehåll, användar-/behörighetsuppgifter, tekniska identifierare och loggar, platsuppgifter när funktionen används samt andra uppgifter Kunden frivilligt registrerar.
Särskilda kategorier	Tjänsten är inte avsedd för rutinmässig behandling av särskilda kategorier enligt artikel 9 GDPR eller uppgifter om lagöverträdelser. Om Kunden instruerar sådan behandling ansvarar Kunden för rättslig grund, nödvändighet och instruktioner; Leverantören får kräva särskild riskbedömning eller vägra en olaglig eller säkerhetsmässigt olämplig instruktion.
Kundens rättigheter och skyldigheter	Kunden får bestämma lagliga ändamål, konfigurera funktioner, lägga till/rätta/radera data, begära bistånd, export, revision och avslut enligt DPA. Kunden ska säkerställa laglig grund, transparens, korrekta instruktioner, dataminimering, behörigheter och säker hantering av sina användarkonton.

Bilaga 2. Tekniska och organisatoriska åtgärder

Åtgärderna nedan beskriver miniminivåer och kontrollområden. De ska tillämpas proportionerligt till risk och kan ersättas av likvärdiga eller starkare åtgärder när tekniken utvecklas.

Kontrollområde	Minimikrav
Identitet och åtkomst	Personliga konton där det är lämpligt, roll-/behörighetsstyrning, minsta privilegium, möjlighet till flerfaktorsautentisering och skyndsam avregistrering av obehöriga konton.
Logisk separering	Tekniska och organisatoriska kontroller som syftar till att hindra att en kund får åtkomst till en annan kunds data.
Kommunikationssäkerhet	Krypterad överföring via moderna protokoll för trafik mellan användare och Tjänsten samt för relevanta systemintegrationer när tekniskt möjligt.
Lagring och backup	Kontrollerad datalagring, säkerhetskopiering i proportion till Tjänstens behov och dokumenterade rutiner för återställning och skydd av backupdata.
Loggning och övervakning	Relevanta autentiserings-, revisions-, fel- och säkerhetshändelser loggas och används för felsökning,

Kontrollområde	Minimikrav
	incidentdetektion och spårbarhet i proportion till risk.
Sårbarheter och uppdateringar	Rutiner för säkerhetsuppdateringar, beroendehantering och prioriterad hantering av kända sårbarheter utifrån risk.
Incidenthantering	Dokumenterade processer för mottagning, klassificering, begränsning, utredning, kommunikation och efteranalys av säkerhetsincidenter.
Tillgänglighet och återställning	Åtgärder för rimlig motståndskraft och för att återställa tillgänglighet och åtkomst efter fysisk eller teknisk incident, med hänsyn till Tjänstens risk och arkitektur.
Test och utvärdering	Regelbunden bedömning av säkerhetskontrollers effektivitet genom exempelvis logggranskning, tekniska tester, sårbarhetskontroller eller andra proportionerliga metoder.
Personal och sekretess	Behovsstyrd åtkomst, sekretessåtaganden och säkerhetsmedvetenhet för personer som kan få åtkomst till Kunddata.
Leverantörskontroll	Bedömning och avtalsreglering av Underbiträden i enlighet med artikel 28 GDPR samt kontroll av relevant överföringsmekanism vid tredjelandsbehandling.
Säker utveckling	Rimliga processer för kodändringar, behörighet till produktionsmiljöer, felhantering och säkerhetsgranskning i utvecklings- och driftsflödet.

Bilaga 3. Underbiträden och ändringsprocess

Den bindande och aktuella underbiträdesförteckningen ska publiceras på https://spaopoolcontrol.se/juridik/underbitraden. Kunden godkänner de Underbiträden som står i förteckningen när DPA accepteras och ger det allmänna förhandstillstånd som anges i avsnitt 7.

Förteckningen ska minst ange	Exempel på innehåll
Leverantör	Juridiskt namn på Underbiträdet.
Tjänst/funktion	Exempelvis hosting, autentisering, e-post/SMS, felövervakning eller support.
Behandling	Vilka huvudkategorier av Kunddata som kan beröras och behandlingens ändamål.
Behandlingsregion	Relevant land/region där behandling eller åtkomst kan ske.
Tredjelandsmekanism	Adekvansbeslut, SCC eller annan laglig mekanism när sådan behövs.

Process för nya Underbiträden: Leverantören meddelar enligt avsnitt 7, Kunden har den angivna invändningsfristen och en invändning måste grundas på sakliga dataskyddsskäl. Ett akut byte får ske snabbare endast när det krävs för säkerhet eller kontinuitet och ska då kommuniceras så snart det är rimligt möjligt.