

Bilaga – Personuppgiftsbiträdesavtal

Detta avtal reglerar förhållandet mellan personuppgiftsansvarig, "Kunden", och "Personuppgiftsbiträdet", POISE AB.

Med "Personuppgiftsbiträdet" avses POISE AB för de av Kunden avtalade tjänsterna. Med "Personuppgiftsansvarig" avses Kunden.

För frågor kring POISE behandling av personuppgifter och aktuella gällande avtal samt villkor hänvisas till <https://www.poise.se/villkor/> och <https://www.poise.se/villkor/integritetspolicy>.

1 Inledning

1.1 Parterna bekräftar att de är behöriga att ingå detta personuppgiftsbiträdesavtal ("Avtal") som är en integrerad del av det/de tjänsteavtal som tecknats mellan Parterna ("Tjänsteavtalet").

Detta Avtal reglerar behandlingen av Personuppgifter med anledning av vid var tid gällande Tjänsteavtal.

1.2 POISE agerar i enlighet med POISE integritetspolicyn som finns tillgänglig på <https://www.poise.se/villkor/integritetspolicy/>.

2 Definitioner

2.1 Definitionen av Personuppgifter, Särskilda kategorier av Personuppgifter (Känsliga Personuppgifter), Behandling av Personuppgifter, Registrerad, Personuppgiftsansvarig och Personuppgiftsbiträdet är densamma som används i gällande dataskyddslagstiftning, inklusive den allmänna dataskyddsförordningen (GDPR – General Data Protection Regulation), gällande i detta Avtal samt i Europa från den 25 maj 2018 samt vid varje tidpunkt gällande nationell kompletterande lagstiftning, tillsammans nedan kallat "Gällande Personuppgiftslagstiftning".

2.2 I denna bilaga benämns Personuppgiftsansvarig som "Kunden" eller "Parten", Personuppgiftsbiträdet som "POISE" eller "Parten" och kollektivt som "Parterna".

3 Omfattning

3.1 Avtalet reglerar Behandling av Personuppgifter utförd av POISE på uppdrag av Kunden och beskriver hur POISE ska säkerställa dataskydd, genom tekniska och organisatoriska åtgärder enligt Gällande Dataskyddslagstiftning.

3.2 Syftet med POISE Behandling av Personuppgifter på uppdrag av Kunden är att uppfylla åtaganden enligt Tjänsteavtalet.

3.3 Detta Avtal har företräde framför eventuella motstridiga bestämmelser om Behandling av Personuppgifter i Tjänsteavtal eller i andra avtal som ingåtts mellan Parterna.

4 POISE skyldigheter

4.1 POISE får endast Behandla Personuppgifter på uppdrag av och i enlighet med Kundens dokumenterade instruktioner. Genom att ingå detta Avtal instruerar Kunden POISE att Behandla Personuppgifter på följande sätt:

- I) endast i enlighet med gällande svensk lag,
- II) för att uppfylla förpliktelserna enligt Tjänsteavtal,
- III) som vidare specificerat genom Kundens normala användning av POISE tjänster och
- IV) på så sätt som anges i detta Avtal.

4.2 Enligt POISE bedömning finns ingen gällande lagstiftning som förhindrar att POISE följer de ovan angivna instruktionerna. POISE ska, efter att ha blivit medveten om det, informera Kunden i de fall Kundens instruktioner eller behandling, enligt POISE förmenande, strider mot gällande dataskyddslagstiftning.

4.3 Vilka kategorier av Registrerade och Personuppgifter som omfattas av Behandling i detta Avtal framgår i detta dokument.

4.4 POISE ska säkerställa konfidentialitet, integritet och tillgänglighet av Personuppgifter enligt Gällande Personuppgiftslagstiftning.

POISE ska löpande genomföra systematiska, organisatoriska och tekniska åtgärder för att säkerställa en lämplig säkerhetsnivå, med hänsyn tagen till den senaste tekniken och implementationskostnader i förhållande till den risk som Behandlingen innebär, och typen av Personuppgifter som ska skyddas.

4.5 POISE ska bistå Kunden med lämpliga tekniska och organisatoriska åtgärder, så långt det är möjligt med hänsyn tagen till typ av Behandling och den informationen som är tillgänglig för POISE, för att uppfylla Kundens skyldigheter enligt gällande dataskyddslagstiftning avseende förfrågningar från Registrerade och allmänt dataskydd enligt dataskyddsförordningen artikel 32-36.

4.6 Om Kunden behöver information om säkerhetsåtgärder, dokumentation eller annan information om hur POISE Behandlar Personuppgifter, och sådana förfrågningar innebär mer information än den standardinformation som tillhandahålls av POISE för att följa gällande dataskyddslagstiftning som Personuppgiftsbiträde, och det innebär mer arbete för POISE, kan POISE debitera Kunden för sådana ytterligare tjänster.

4.7 POISE och personal anställd av POISE ska säkerställa konfidentialitet av Personuppgifter som Behandlas under detta Avtal. Detta villkor gäller även efter att Avtalet upphört att gälla.

4.8 POISE ska, genom att skyndsamt och utan onödigt dröjsmål meddela Kunden, göra det möjligt för Kunden att uppfylla de rättsliga krav som gäller för information till relevanta dataskyddsmyndigheter och Registrerade rörande personuppgiftsincidenter.

4.9 Vidare ska POISE, i den utsträckning det är praktiskt möjligt och lagligt, meddela Kunden om

- I) förfrågningar om utlämnande av Personuppgifter som erhållits från en Registrerad
- II) förfrågningar från myndigheter, till exempel rättsvärdande myndigheter, om utlämnande av Personuppgifter

4.10 POISE får inte svara direkt på förfrågningar från Registrerade utan medgivande från Kunden. POISE får inte delge innehåll rörande Avtalet till myndigheter som Polisen, inklusive Personuppgifter, med undantag för vad som är lagstadgat, exempelvis genom domstolsbeslut eller motsvarande beslut.

4.11 POISE har inte kontroll över huruvida och hur Kunden väljer att använda sig av eventuella tredjepartsintegrationer via av POISE tillhandahållet API, via direkt databaskoppling eller liknande. Ansvar för eventuell behandling av Personuppgifter via integrationer med tredje part åligger uteslutande Kunden.

5 Kundens skyldigheter

5.1 Genom att godkänna detta Avtal bekräftar Kunden att Kunden:

- vid användning av de tjänster som tillhandahålls av POISE enligt Tjänsteavtal, Behandla Personuppgifter i enlighet med kraven i gällande dataskyddslagstiftning.
- har rättslig grund att Behandla och utlämna de aktuella Personuppgifterna till POISE (inklusive eventuella underbiträden som POISE använder).
- är ensamt ansvarig för riktigheten, integriteten, innehållet, tillförlitligheten och lagenligheten av de Personuppgifter som lämnats till POISE.
- har uppfyllt alla eventuella obligatoriska krav och skyldigheter att anmäla hos eller få tillstånd från relevanta myndigheter för Behandlingen av Personuppgifter.
- har fullgjort sina skyldigheter att tillhandahålla relevant information till Registrerade avseende Behandling av Personuppgifter enligt Gällande Personuppgiftslagstiftning.
- instämmer i att POISE har lämnat garantier avseende implementeringen av tekniska och organisatoriska säkerhetsåtgärder som är tillräckliga för att skydda Registrerades integritet och Personuppgifter.
- vid användning av de tjänster som tillhandahålls av POISE under Tjänsteavtal inte överför några Känsliga Personuppgifter, eller uppgifter som rör fällande domar i brottmål och överträdelse till POISE. Sker sådan överföring kan inte POISE hållas ansvarig för felaktig behandling av dessa Känsliga Personuppgifter.
- ska upprätthålla ett uppdaterat register över de typer och kategorier av Personuppgifter som denne Behandlar.

6 Användande av underbiträden och överföring av data

6.1 Som en del av leveransen av tjänster till Kunden enligt Tjänsteavtal och detta Avtal, kan POISE använda sig av underleverantörer i rollen underbiträde. Sådana underbiträden kan vara systerbolag till POISE AB eller externa underleverantörer (tredje part) inom eller utanför EU. POISE ska säkerställa att underleverantörer genom avtal samtycker till att åta sig ansvar som motsvarar de skyldigheter som anges i detta Avtal.

6.2 Nuvarande underleverantörer med tillgång till Personuppgifter publiceras på POISE hemsida <https://www.poise.se/villkor/integritetspolicy/> vilka genom detta Avtal har accepterats som underbiträden av Kunden.

6.3 Kunden kan när som helst begära en fullständig översikt och mer detaljerad information om de underleverantörer som är involverade i leverans av tjänsten enligt Tjänsteavtalet.

6.4 Om underleverantörerna finns utanför EU ska POISE säkerställa att överföring sker enligt Gällande Personuppgiftslagstiftning.

Kunden ger härmed POISE behörighet och befogenhet för att säkerställa lämpliga rättsliga grunder för överföring av Personuppgifter utanför EU på Kundens uppdrag, t.ex. genom att för Kundens räkning godkänna EU-standardavtalsklausuler eller överföra Personuppgifter i enlighet med EU/US Privacy Shield.

6.5 Kunden ska underrättas innan ändringar sker rörande underleverantörer som Behandlar Personuppgifter. Om ny underleverantör bevisligen inte efterlever gällande dataskyddslagstiftning och underleverantören fortsatt inte efterlever gällande dataskyddslagstiftning, efter att POISE har fått rimlig tid på sig att säkerställa att underleverantören efterlever regelverket, kan Kunden säga upp Avtalet.

Sådan uppsägning kan innebära rätt att säga upp Tjänsteavtal, helt eller delvis, enligt de uppsägningsklausuler som finns i respektive Tjänsteavtal. En viktig del av sådana bedömningar ska vara i vilken mån underleverantörens Behandling av Personuppgifter är en nödvändig del av de tjänster som tillhandahålls enligt Tjänsteavtal.

En ändring av underleverantör ska inte i sig betraktas som ett brott mot Tjänsteavtal.

6.6 Genom att godkänna detta Avtal accepterar Kunden att POISE använder sig av underleverantörer på så sätt som beskrivs ovan.

7 Säkerhet

7.1 POISE har åtagit sig att tillhandahålla en hög säkerhetsnivå i sina produkter och tjänster. POISE tillhandahåller säkerhetsnivån genom organisatoriska, tekniska och fysiska säkerhetsåtgärder, i enlighet med kraven på informationssäkerhet som beskrivs i dataskyddsförordningen artikel 32.

Vidare syftar det interna dataskyddsramverk POISE AB använder till att skydda konfidentialitet, integritet, korrekthet och åtkomst av Personuppgifter. Följande åtgärder är av särskild betydelse för detta:

- Klassificering av Personuppgifter för att säkerställa genomförandet av säkerhetsåtgärder som motsvarar riskbedömning.
- Utvärdering av användning av kryptering och pseudonymisering som riskreducerande faktorer.
- Begränsning av tillgång till Personuppgifter till de som behöver tillgång för att fullgöra skyldigheterna i detta Avtal eller Tjänsteavtal.
- Användande av system som upptäcker, återställer, förhindrar och rapporterar personuppgiftsincidenter.
- Genomförande av säkerhetsanalyser för att bedöma kvaliteten i nuvarande tekniska och organisatoriska åtgärder för att skydda Personuppgifter, med beaktande av kraven i gällande dataskyddslagstiftning.

8 Revisionsrättigheter

8.1 Kunden har rätt att genomföra årlig revision av POISE uppfyllande av villkoren i Avtalet. Om lagstiftningen kräver det kan Kunden begära revisioner oftare. Då POISE AB:s tjänster är fleranvändarmiljöer ger Kunden POISE befogenhet, att av säkerhetsskäl, bestämma att revision ska utföras av en neutral tredjepartsrevisor som POISE väljer.

8.2 Om det begärda revisionsområdet är upptaget i en granskningsrapport som utförts av en kvalificerad tredjepartsrevisor inom de föregående tolv månaderna, och POISE bekräftar att det inte finns några kända väsentliga förändringar i de åtgärder som granskats, accepterar Kunden denna granskningsrapport istället för att begära en ny revision av åtgärder som redan granskats.

8.3 Om Kunden inte accepterar den av POISE AB valda neutrala tredjepartsrevisorn, kan Kunden tillsammans med POISE AB välja en annan neutral tredjepartsrevisor.

8.4 Kunden står för eventuella kostnader som uppstår i samband med begärda revisioner. Hjälptjänst från POISE som överstiger standardtjänsten som tillhandahålls av POISE och/eller POISE underleverantörer för att följa gällande dataskyddslagstiftning, kommer att debiteras.

9 Varaktighet och uppsägning

9.1 Detta Avtal är giltigt så länge som POISE Behandlar Personuppgifter på uppdrag av Kunden enligt gällande Tjänsteavtal.

9.2 Avtalet upphör automatiskt när Tjänsteavtalet upphör att gälla. När Avtalet upphör kommer POISE att radera eller återlämna Personuppgifter som Behandlas på uppdrag av Kunden, i enlighet med gällande klausuler i respektive Tjänsteavtal. Om inte annat avtalats skriftligen ska kostnaden för sådana åtgärder baseras på;

I) timtaxa för POISE tid och

II) komplexiteten i den begärda processen.

9.3 POISE kan behålla Personuppgifter efter att Avtalet har upphört, i den utsträckning det krävs enligt lag, med samma typ av tekniska och organisatoriska säkerhetsåtgärder som beskrivs i detta Avtal.

10 Ansvar

10.1 Ansvaret för överträdelse av villkoren i detta avtal, ska regleras av ansvars klausuler i respektive Tjänsteavtal mellan Parterna.

Detta gäller även för eventuella överträdelser som begåtts av POISE underleverantörer.

11 Tillämplig lag och jurisdiktion

11.1 Detta Avtal är underkastat tillämplig lag och den jurisdiktion som anges i respektive Tjänsteavtal mellan Parterna.

12 Kategorier av Personuppgifter och Registrerade

12.1 Då POISE tjänster medger att Kunden Behandlar godtyckligt data inom tjänsterna är det inte möjligt att generellt redovisa de kategorier av Registrerade och Personuppgifter som omfattas av Behandling.

Denna information åligger Kunden att registrera.

12.2 Kunden får inte överföra några Känsliga Personuppgifter till POISE. Sker sådan överföring kan inte POISE hållas ansvarig för felaktig behandling av dessa Känsliga Personuppgifter. Känsliga Personuppgifter definieras i Gällande Personuppgiftslagstiftning, d.v.s.:

- ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse,
- uppgifter om hälsa,
- uppgifter om en persons sexualliv eller sexuell läggning,
- medlemskap i fackförening,
- genetiska uppgifter eller biometriska uppgifter för att entydigt identifiera en fysisk person

12.3 Inte heller får Kunden överföra personuppgifter som rör fällande domar i brottmål och överträdelser.

13 Översikt över nuvarande underleverantörer

13.1 Aktuella underleverantörer till POISE som har tillgång till Kundens Personuppgifter redovisas på <https://www.poise.se/villkor/integritetspolicy/>

14 Tillämplig lag

14.1 Detta avtal regleras av svensk lag. Tvister skall avgöras i svensk domstol, företrädesvis vid Stockholms tingsrätt.