Personuppgiftsbiträdesavtal

Innehållsförteckning

PERSONUPPGIFTSBITRÄDESAVTAL

Avtal enligt artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679[1]

1 PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER

Personuppgiftsansvarig	**Personuppgiftsbiträde**
	Trelson AB
Organisationsnummer	**Organisationsnummer**
	559459-4649
Postadress	**Postadress**
	Mejerivägen 3 117 43 Stockholm
Kontaktperson för administration av detta personuppgiftsbiträdesavtal	**Kontaktperson för administration av detta personuppgiftsbiträdesavtal**
Namn: E-post: Tfn:	Namn: Jonatan Brown E-post: jonatan.brown@trelson.com Tfn: 0760225820
Kontaktperson för parternas samarbete om dataskydd	**Kontaktpersoner för parternas samarbete om dataskydd**
Namn: E-post: Tfn:	Namn: Jonatan Brown E-post: jonatan.brown@onlinepartner.se Tfn: 0760225820

2 DEFINITIONER

2.1 Utöver de begrepp som definieras i löptext, i detta personuppgiftsbiträdesavtal, ska dessa definitioner, oavsett om de används i plural eller singular, i bestämd eller obestämd form, ha nedanstående innebörd när de anges med versal som begynnelsebokstav.

[1] Allmänna dataskyddsförordningen EU 2016/679 föreskriver att det ska finnas ett skriftligt avtal om Personuppgiftsbiträdets Behandling av Personuppgifter för Den personuppgiftsansvariges räkning.

Behandling

En åtgärd eller kombination av åtgärder beträffande Personuppgifter eller uppsättningar av Personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring

Dataskyddslagstiftning

Avser all integritets- och personuppgiftslagstiftning, samt annan lagstiftning, förordningar och föreskrifter som är tillämplig på den Behandling som sker enligt detta PUB-avtal, inklusive nationell sådan lagstiftning och EU-lagstiftning.

Personuppgiftsansvarig

Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamål och medlen för Behandlingen av Personuppgifter.

Instruktion

De skriftliga instruktioner som närmare anger föremål, varaktighet, art och ändamål, typ av Personuppgifter samt kategorier av Registrerade och särskilda behov som omfattas av Behandlingen.

Logg

Logg är resultatet av Loggning.

Loggning

Loggning är ett kontinuerligt insamlande av uppgifter om den Behandling av Personuppgifter som utförs enligt detta PUB-avtal och som kan knytas till en enskild fysisk person.

Personuppgiftsbiträde

Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som Behandlar Personuppgifter för den Personuppgiftsansvariges räkning.

Personuppgift

Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Personuppgiftsincident

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.

Registrerad

Fysisk person vars Personuppgifter Behandlas.

Tredje land

En stat som inte ingår i Europeiska unionen (EU) eller inte är ansluten till Europeiska ekonomiska samarbetsområdet (EES).

Underbiträde

Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som i egenskap av underleverantör till Personuppgiftsbiträdet Behandlar Personuppgifter för Personuppgiftsansvariges räkning.

3 BAKGRUND OCH SYFTE

3.1 Med detta Personuppgiftsbiträdesavtal jämte Instruktioner och en eventuell förteckning över Underbiträden (nedan gemensamt ”PUB-avtalet”) reglerar den Personuppgiftsansvarige Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige. PUB-avtalets syfte är att säkerställa den Registrerades fri- och rättigheter vid Behandlingen, i enlighet med vad som stadgas i artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679 (”Dataskyddsförordningen”).

3.2 När PUB-avtalet utgör ett av flera avtalsdokument inom ramen för ett annat avtal benämns det andra avtalet ”Huvudavtalet” i PUB-avtalet.

3.3 För det fall något av det som stadgas i avsnitt 1, punkt 3.2, avsnitt 15 eller 16, punkt 17.6, avsnitt 18–20 eller 22 i PUB-avtalet regleras på annat sätt i Huvudavtalet, ska Huvudavtalets reglering ha företräde.

3.4 Hänvisningar i PUB-avtalet till nationell eller unionsrättslig lagstiftning, avser vid var tid tillämpliga bestämmelser.

4 BEHANDLING AV PERSONUPPGIFTER OCH SPECIFIKATION

4.1 Den Personuppgiftsansvarige utser härmed Personuppgiftsbiträdet att utföra Behandlingen för den Personuppgiftsansvariges räkning enligt vad som stadgas i detta PUB-avtal.

4.2 Den Personuppgiftsansvarige ska ge skriftliga Instruktioner till Personuppgiftsbiträdet om hur det ska utföra Behandlingen.

4.3 Personuppgiftsbiträdet får endast utföra Behandlingen i enlighet med PUB-avtalet och vid var tid gällande Instruktioner.

5 DEN PERSONUPPGIFTSANSVARIGES ANSVAR

5.1 Den Personuppgiftsansvarige ansvarar för att det vid var tid finns laglig grund för Behandlingen och för att utforma korrekta Instruktioner med hänsyn till Behandlingens art så att Personuppgiftsbiträdet och eventuellt Underbiträde kan fullgöra sitt eller sina uppdrag enligt detta PUB-avtal och Huvudavtal i förekommande fall.

5.2 Den Personuppgiftsansvarige ska utan onödigt dröjsmål informera Personuppgiftsbiträdet om förändringar i Behandlingen vilka påverkar Personuppgiftsbiträdets skyldigheter enligt Dataskyddslagstiftningen.

5.3 Den Personuppgiftsansvarige ansvarar för att informera Registrerade om Behandlingen och för att tillvarata Registrerades rättigheter enligt Dataskyddslagstiftningen samt vidta varje annan åtgärd som åligger den Personuppgiftsansvarige enligt Dataskyddslagstiftningen.

6 PERSONUPPGIFTSBITRÄDETS ÅTAGANDEN

6.1 Personuppgiftsbiträdet förbinder sig att endast utföra Behandlingen i enlighet med PUB-avtalet och för de specifika ändamål som anges i Instruktioner samt att följa Dataskyddslagstiftningen. Personuppgiftsbiträdet förbinder sig även att fortlöpande hålla sig informerad om gällande rätt på området.

6.2 Personuppgiftsbiträdet ska vidta åtgärder för att skydda Personuppgifterna mot alla slag av Behandlingar som inte är förenliga med PUB-avtalet, Instruktioner och Dataskyddslagstiftningen.

6.3 Personuppgiftsbiträdet åtar sig att säkerställa att samtliga fysiska personer som arbetar under dess ledning följer PUB-avtalet och Instruktioner samt att de fysiska personerna informeras om relevant lagstiftning.

6.4 Personuppgiftsbiträdet ska på begäran från den Personuppgiftsansvarige bistå denne med att säkerställa att skyldigheterna enligt artikel 32–36 i Dataskyddsförordningen fullgörs och svara på begäran om utövande av den Registrerades rättigheter i enlighet med Dataskyddsförordningen, kap. III, med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå.

6.5 För det fall att Personuppgiftsbiträdet finner att Instruktioner är otydliga, i strid med Dataskyddslagstiftningen eller saknas och Personuppgiftsbiträdet bedömer att nya eller kompletterande Instruktioner är nödvändiga för att genomföra sina åtaganden ska Personuppgiftsbiträdet utan dröjsmål informera den Personuppgiftsansvarige, tillfälligt upphöra med Behandlingen och invänta nya Instruktioner, om inte parterna kommer överens om annat.

6.6 För det fall att den Personuppgiftsansvarige förser Personuppgiftsbiträdet med nya eller ändrade Instruktioner ska Personuppgiftsbiträdet, utan onödigt dröjsmål från mottagandet, meddela den Personuppgiftsansvarige huruvida genomförandet av de nya Instruktionerna föranleder förändrade kostnader för Personuppgiftsbiträdet.

7 SÄKERHETSÅTGÄRDER

7.1 Personuppgiftsbiträdet ska vidta alla lämpliga tekniska och organisatoriska säkerhetsåtgärder som krävs enligt Dataskyddslagstiftningen för att förhindra Personuppgiftsincidenter, genom att säkerställa att Behandlingen uppfyller kraven i Dataskyddsförordningen och att den Registrerades rättigheter skyddas.

7.2 Personuppgiftsbiträdet ska fortlöpande säkerställa att den tekniska och organisatoriska säkerheten i samband med Behandlingen medför en lämplig nivå av konfidentialitet, integritet, tillgänglighet och motståndskraft.

7.3 Eventuella tillkommande eller ändrade krav på skyddsåtgärder från den Personuppgiftsansvarige, efter parternas tecknande av PUB-avtalet, ska betraktas som nya Instruktioner enligt PUB-avtalet.

7.4 Personuppgiftbiträdet ska genom behörighetskontrollsystem endast ge åtkomst till Personuppgifterna för sådana fysiska personer som arbetar under Personuppgiftsbiträdets ledning och som behöver åtkomsten för att kunna utföra sina arbetsuppgifter.

7.5 Personuppgiftsbiträdet åtar sig att kontinuerligt Logga åtkomst till Personuppgifterna enligt PUB-avtalet i den utsträckning det krävs enligt Instruktionen. Loggar får gallras först fem (5) år efter Loggningstillfället om inte annat anges i Instruktionen. Loggar ska omfattas av erforderliga skyddsåtgärder, i enlighet med Dataskyddslagstiftningen.

7.6 Personuppgiftsbiträdet ska systematiskt testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa Behandlingens säkerhet.

8 SEKRETESS/TYSTNADSPLIKT

8.1 Personuppgiftsbiträdet och samtliga fysiska personer som arbetar under dess ledning ska vid Behandlingen iaktta såväl sekretess som tystnadsplikt. Personuppgifterna får inte nyttjas eller spridas för andra ändamål, varken direkt eller indirekt, såvida inte annat avtalats.

8.2 Personuppgiftsbiträdet ska tillse att samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen, är bundna av sekretessförbindelse avseende Behandlingen. Detta krävs dock inte om dessa redan omfattas av en straffsanktionerad tystnadsplikt som följer av lag. Personuppgiftsbiträdet åtar sig även att tillse att det finns sekretessavtal med Underbiträdet samt sekretessförbindelser mellan Underbiträdet och samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen.

8.3 Personuppgiftsbiträdet ska skyndsamt underrätta den Personuppgiftsansvarige om eventuella kontakter med tillsynsmyndighet avseende Behandlingen. Personuppgiftsbiträdet har inte rätt att företräda den Personuppgiftsansvarige eller agera för den Personuppgiftsansvariges räkning gentemot tillsynsmyndigheter i frågor avseende Behandlingen.

8.4 Om den Registrerade, tillsynsmyndighet eller tredje man begär information från Personuppgiftsbiträdet vilken rör Behandlingen, ska Personuppgiftsbiträdet informera den Personuppgiftsansvarige om saken. Information om Behandlingen får inte lämnas till den Registrerade, tillsynsmyndighet eller tredje man utan skriftligt medgivande från den Personuppgiftsansvarige, såvida det inte framgår av tvingande lag att information ska lämnas. Personuppgiftsbiträdet ska bistå med förmedling av den informationen som omfattas av ett medgivande eller lagkrav.

9 GRANSKNING, TILLSYN OCH REVISION

9.1 Personuppgiftsbiträdet ska utan onödigt dröjsmål som en del av sina garantier, enligt artikel 28.1 i Dataskyddsförordningen, på den Personuppgiftsansvariges begäran kunna redovisa vilka tekniska och organisatoriska säkerhetsåtgärder som används för att Behandlingen ska uppfylla kraven enligt PUB-avtalet och artikel 28.3.h i Dataskyddsförordningen.

9.2 Personuppgiftsbiträdet ska minst en (1) gång om året granska säkerheten avseende Behandlingen genom en egenkontroll för att säkerställa att Behandlingen följer PUB-avtalet. Resultatet av sådan egenkontroll ska på begäran delges den Personuppgiftsansvarige.

9.3 Den Personuppgiftsansvarige äger rätt att, själv eller genom annan av denne utsedd tredje part (som inte får vara en konkurrent till Personuppgiftsbiträdet), följa upp att Personuppgiftsbiträdet uppfyller PUB-avtalets, Instruktionernas och Dataskyddslagstiftningens

krav. Personuppgiftsbiträdet ska vid sådan granskning bistå den Personuppgiftsansvarige, eller den som utför granskningen i den Personuppgiftsansvariges ställe, med dokumentation, tillgång till lokaler, IT-system och andra tillgångar som behövs för att kunna granska Personuppgiftsbiträdets efterlevnad av PUB-avtalet, Instruktioner och Dataskyddslagstiftningen. Den Personuppgiftsansvarige ska säkerställa att personal som genomför granskningen är underkastade sekretess eller tystnadsplikt enligt lag eller avtal.

9.4 Personuppgiftsbiträdet äger alternativt till vad som stadgas i punkterna 9.2–9.3, rätt att erbjuda andra tillvägagångssätt för granskning av Behandlingen, exempelvis granskning genomförd av oberoende tredje part. Den Personuppgiftsansvarige ska i sådant fall äga rätt, men inte skyldighet, att tillämpa detta alternativa tillvägagångssätt för granskning. Vid sådan granskning ska Personuppgiftsbiträdet ge den Personuppgiftsansvarige eller en tredje part den assistans som behövs för utförandet av granskningen.

9.5 Personuppgiftbiträdet ska bereda tillsynsmyndighet, eller annan myndighet som har laglig rätt till det, möjlighet att göra tillsyn enligt myndighetens begäran i enlighet med vid var tid gällande lagstiftning, även om sådan tillsyn annars skulle stå i strid med bestämmelserna i PUB-avtalet.

9.6 Personuppgiftsbiträdet ska tillförsäkra den Personuppgiftsansvarige rättigheter gentemot Underbiträdet vilka motsvarar den Personuppgiftsansvariges samtliga rättigheter gentemot Personuppgiftsbiträdet enligt avsnitt 9 i PUB-avtalet.

10 HANTERING AV RÄTTELSER OCH RADERING M.M.

10.1 För det fall den Personuppgiftsansvarige begärt rättelse eller radering på grund av Personuppgiftsbiträdets felaktiga Behandling ska Personuppgiftsbiträdet vidta lämplig åtgärd utan onödigt dröjsmål, senast inom trettio (30) dagar, från det att Personuppgiftsbiträdet mottagit erforderlig information från den Personuppgiftsansvarige. När den Personuppgiftsansvarige begärt radering får Personuppgiftsbiträdet endast utföra Behandling av den aktuella Personuppgiften som ett led i processen för rättelse eller radering.

10.2 Om tekniska och organisatoriska åtgärder (t.ex. uppgraderingar eller felsökningar) vidtas av Personuppgiftsbiträdet i Behandlingen, vilka kan påverka Behandlingen, ska Personuppgiftsbiträdet skriftligt informera den Personuppgiftsansvarige om detta i enlighet med vad som stadgas om meddelanden i avsnitt 18 i PUB-avtalet. Informationen ska lämnas i god tid innan åtgärderna vidtas.

11 PERSONUPPGIFTSINCIDENTER

11.1 Personuppgiftsbiträdet ska ha förmåga att återställa tillgängligheten och tillgången till Personuppgifterna i rimlig tid vid en fysisk eller teknisk incident enligt artikel 32.1.c i Dataskyddsförordningen.

11.2 Personuppgiftbiträdet åtar sig att med beaktande av Behandlingens art, och den information som Personuppgiftsbiträdet har att tillgå, bistå den Personuppgiftsansvarige med att fullgöra dennes skyldigheter vid en Personuppgiftsincident beträffande Behandlingen. Personuppgiftsbiträdet ska på den Personuppgiftsansvariges begäran även bistå med att utreda misstankar om eventuell obehörigs Behandling och/eller åtkomst till Personuppgifterna.

11.3 Vid Personuppgiftsincident, vilken Personuppgiftbiträdet fått vetskap om, ska Personuppgiftsbiträdet utan onödigt dröjsmål skriftligen underrätta den Personuppgiftsansvarige om händelsen. Personuppgiftsbiträdet ska, med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå, tillhandahålla den Personuppgiftsansvarige en skriftlig beskrivning av Personuppgiftsincidenten.

11.4 Beskrivningen ska redogöra för:

a. Personuppgiftsincidentens art och, om möjligt, de kategorier och antalet Registrerade som berörs samt kategorier och antalet personuppgiftsposter som berörs,
b. de sannolika konsekvenserna av Personuppgiftsincidenten, och
c. åtgärder som har vidtagits eller föreslagits samt åtgärder för att mildra Personuppgiftincidentens potentiella negativa effekter.

11.5 Om det inte är möjligt för Personuppgiftsbiträdet att tillhandahålla hela beskrivningen samtidigt, enligt punkten 11.3 i PUB-avtalet, får beskrivningen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

12 UNDERBITRÄDE

12.1 Personuppgiftsbiträdet äger rätt att anlita den eller de Underbiträden som framgår av bilagd förteckningen över Underbiträden, bilaga 2.

12.2 Personuppgiftsbiträdet åtar sig att teckna ett skriftligt avtal med Underbiträdet som reglerar den Behandling som Underbiträdet utför å den Personuppgiftsansvariges vägnar samt att endast anlita Underbiträden som ger tillräckliga garantier. Underbiträdet ska genomföra lämpliga tekniska och organisatoriska åtgärder så att Behandlingen uppfyller kraven i Dataskyddslagstiftningen. I fråga om dataskydd ska avtalet ålägga Underbiträdet samma skyldigheter som åläggs Personuppgiftsbiträdet i detta PUB-avtal.

12.3 Personuppgiftsbiträdet ska i avtalet med Underbiträdet säkerställa att den Personuppgiftsansvarige har rätt att säga upp Underbiträdet och instruera Underbiträdet att exempelvis radera eller återlämna Personuppgifterna om Personuppgiftsbiträdet har upphört att existera i faktisk eller rättslig mening eller hamnat på obestånd.

12.4 Personuppgiftsbiträdet ansvarar fullt ut för Underbiträdets Behandling gentemot den Personuppgiftsansvarige. Personuppgiftsbiträdet ska skyndsamt underrätta den Personuppgiftsansvarige om Underbiträdet underlåter att uppfylla sina skyldigheter i PUB-avtalet.

12.5 Personuppgiftsbiträdet äger rätt att anlita nya underbiträden och ersätta befintliga underbiträden om inte annat anges i Instruktionen.

12.6 När Personuppgiftsbiträdet avser att anlita ett nytt eller ersätta ett befintligt Underbiträde ska Personuppgiftsbiträdet säkerställa Underbiträdets kapacitet och förmåga att uppfylla sina skyldigheter enligt Dataskyddslagstiftningen. Personuppgiftsbiträdet ska skriftligen meddela den Personuppgiftsansvarige om

a. Underbiträdets namn, organisationsnummer och säte (adress och land),
b. vilken typ av uppgifter och kategorier av Registrerade som behandlas, och
c. var Personuppgifterna ska behandlas.

12.7 Den Personuppgiftsansvarige äger rätt att inom trettio (30) dagar från dag för meddelande enligt punkten 12.6 invända mot Personuppgiftsbiträdets anlitande av ett nytt Underbiträde

och att, med anledning av sådan invändning, säga upp detta PUB-avtal att upphöra i enlighet med vad stadgas i PUB-avtalet, punkten 16.4.

12.8 Personuppgiftsbiträdet ska vid var tid föra en korrekt och uppdaterad förteckning över de Underbiträden som anlitas för Behandling av Personuppgifter för den Personuppgiftsansvariges räkning samt göra denna förteckning tillgänglig för den Personuppgiftsansvarige. Av förteckningen ska särskilt framgå i vilket land Underbiträdet behandlar Personuppgifterna och vilka typer av Behandlingar som Underbiträdet utför.

12.9 När Personuppgiftsbiträdet slutar använda ett Underbiträde ska Personuppgiftsbiträdet skriftligen meddela den Personuppgiftsansvarige om detta. Personuppgiftsbiträdet ska när ett avtal upphör säkerställa att Underbiträdet raderar eller återlämnar Personuppgifterna.

12.10 Personuppgiftsbiträdet ska på den Personuppgiftsansvariges begäran översända en kopia av det avtal som reglerar Underbiträdets Behandling av Personuppgifter enligt punkten 12.2 och förteckningen över Underbiträden enligt punkten 12.1.

13 LOKALISERING OCH ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND

13.1 Personuppgiftsbiträdet ska säkerställa att Personuppgifterna hanteras och lagras inom EU/EES av en fysisk eller juridisk person som är etablerad inom EU/EES, om inte PUB-avtalets parter kommer överens om något annat.

13.2 Personuppgiftsbiträdet äger endast rätt att överföra Personuppgifter till Tredje land för Behandling (t.ex. service, support, underhåll, utveckling, drift eller liknande hantering) om den Personuppgiftsansvarige på förhand skriftligen godkänt sådan överföring och utfärdat Instruktioner för detta ändamål.

13.3 Överföring till Tredje land för Behandling enligt PUB-avtalet, punkten 13.2, får endast ske om den är förenlig med Dataskyddslagstiftningen och uppfyller de krav på Behandlingen vilka ställs i PUB-avtalet och Instruktioner.

14 ANSVAR FÖR SKADA I SAMBAND MED BEHANDLING

14.1 Vid ersättning för skada i samband med Behandling som, genom fastställd dom eller förlikning, ska utgå till den Registrerade på grund av överträdelse av bestämmelse i PUB-avtalet, Instruktioner och/eller tillämplig bestämmelse i Dataskyddslagstiftningen ska artikel i 82 i Dataskyddsförordningen tillämpas.

14.2 Sanktionsavgifter enligt artikel 83 i Dataskyddsförordningen, eller 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ska bäras av den av PUB-avtalets parter som påförts en sådan avgift.

14.3 Om endera part får kännedom om omständighet som kan leda till skada för motparten ska parten utan onödigt dröjsmål informera motparten om förhållandet och aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.

14.4 Oaktat vad som sägs i Huvudavtalet gäller detta PUB-avtal, punkterna 14.1 och 14.2, före andra regler om fördelning mellan parterna av krav sinsemellan såvitt avser Behandlingen.

15 PUB-AVTALETS TECKNANDE, AVTALSTID OCH UPPSÄGNING

15.1 PUB-avtalet gäller från och med den tidpunkt PUB-avtalet undertecknats av båda parter och tillsvidare. Parterna äger ömsesidig rätt att säga upp PUB-avtalet att upphöra med trettio (30) dagars varsel.

16 ÄNDRINGAR OCH UPPSÄGNING MED OMEDELBAR VERKAN M.M.

16.1 Endera part i PUB-avtalet äger rätt att påkalla omförhandling av PUB-avtalet om motpartens ägarförhållanden ändras väsentligt eller om tillämplig lagstiftning, eller tolkningen av den, ändras på ett för Behandlingen avgörande sätt. Påkallande av omförhandling enligt första meningen innebär inte att PUB-avtalet till någon del upphör att gälla utan endast att en omförhandling om PUB-avtalet ska påbörjas.

16.2 Tillägg till, och ändringar i, PUB-avtalet ska vara skriftliga och undertecknade av båda parter.

16.3 När någon av parterna får kännedom om att motparten agerar i strid med PUB-avtalet och/eller Instruktioner ska parten utan dröjsmål meddela motparten om agerandet. Därefter äger parten rätt att med omedelbar verkan upphöra att utföra sina förpliktelser enligt PUB-avtalet till den tidpunkt motparten förklarat att agerandet upphört och förklaringen accepterats av den part som påtalat agerandet.

16.4 Om den Personuppgiftsansvarige invänder mot Personuppgiftsbiträdets anlitande av ett nytt underbiträde, enligt detta PUB-avtal, punkten 12.7, har den Personuppgiftsansvarige rätt att säga upp PUB-avtalet att upphöra med omedelbar verkan.

17 ÅTGÄRDER VID PUB-AVTALETS UPPHÖRANDE

17.1 Efter uppsägning av PUB-avtalet ska Personuppgiftsbiträdet utan onödigt dröjsmål, beroende på vad den Personuppgiftsansvarige väljer, antingen radera och intyga för den Personuppgiftsansvarige att det är utfört, eller återlämna

a. alla Personuppgifter som Behandlats för den Personuppgiftsansvariges räkning och

b. all tillhörande information såsom Loggar, Instruktioner, systemlösningar, beskrivningar och andra handlingar som Personuppgiftsbiträdet erhållit genom informationsutbyte enligt PUB-avtalet.

17.2 I samband med återlämning ska Personuppgiftsbiträdet även radera befintliga kopior av Personuppgifter och tillhörande information.

17.3 Skyldigheten att radera eller återlämna Personuppgifter eller tillhörande information gäller inte om lagring av Personuppgifterna eller informationen krävs enligt unionsrätten eller relevant nationell rätt där Behandling får utföras enligt PUB-avtalet.

17.4 Om Personuppgifter eller tillhörande information återlämnas ska det ske i ett allmänt använt och standardiserat format, om parterna inte har kommit överens om något annat format.

17.5 Till dess att uppgifterna raderas eller återlämnas ska Personuppgiftsbiträdet säkerställa efterlevnaden av PUB-avtalet.

17.6 Återlämning eller radering enligt PUB-avtalet ska vara utförd senast trettio (30) kalenderdagar räknat från tidpunkten för uppsägningen av PUB-avtalet, om inte annat anges i Instruktionen.

Behandling av Personuppgifter som Personuppgiftsbiträdet utför därefter är att betrakta som otillåten Behandling.

17.7 Bestämmelser om sekretess/tystnadsplikt i avsnitt 8 ska fortsätta gälla även om PUB-avtalet i övrigt upphör att gälla.

18 MEDDELANDEN INOM RAMEN FÖR DETTA PUB-AVTAL OCH INSTRUKTIONER

18.1 Meddelanden om PUB-avtalet och dess administration inklusive uppsägning ska skickas via e-post eller på något annat av parterna överenskommet sätt till respektive parts kontaktperson för PUB-avtalet.

18.2 Meddelanden om parternas samarbete om dataskydd gällande Behandlingen ska skickas via e-post eller på något annat av parterna överenskommet sätt till respektive parts kontaktperson för parternas samarbete om dataskydd.

18.3 Ett meddelande ska anses ha kommit fram till mottagaren senast en (1) arbetsdag efter att meddelandet har skickats.

19 KONTAKTPERSONER

19.1 Parterna ska utse var sin kontaktperson för PUB-avtalet.

19.2 Parterna ska utse var sin kontaktperson för parternas samarbete om dataskydd.

20 ANSVAR FÖR UPPGIFTER OM PARTERNA OCH KONTAKTPERSONER SAMT KONTAKTUPPGIFTER

20.1 Varje part ansvarar för att de uppgifter som anges i avsnitt 1 i PUB-avtalet alltid är aktuella och korrekta.

20.2 Ändring av uppgifter i avsnitt 1 ska meddelas motparten enligt punkt 18.1 i PUB-avtalet.

21 LAGVAL OCH TVISTER

21.1 Vid tolkning och tillämpning av PUB-avtalet gäller svensk rätt med undantag för lagvals-reglerna. Tvister med anledning av PUB-avtalet ska avgöras av behörig svensk domstol.

22 PARTERNAS UNDERTECKNANDEN AV PUB-AVTALET

22.1 Detta PUB-avtal tillhandahålls antingen i digitalt format för elektroniskt undertecknande eller i pappersformat för egenhändigt undertecknande. I sistnämnda fall upprättas avtalet i två likalydande exemplar, varav parterna erhåller varsitt.

22.2 Om PUB-avtalet undertecknas elektroniskt lämnas signatursidan utan avseende.

_____

[Resten av sidan har avsiktligen lämnats tom. Signatursida följer.]

Personuppgiftsansvarig

Ort och datum:

_____

Namnförtydligande

_____

Signatur

Personuppgiftsbiträde

Trelson AB

Ort och datum:

_____

Namnförtydligande

_____

Signatur

Versionshantering

Version	Datum	Förändringar	Ansvarig
1.1	2018-12-19	10.1, 14.1, 18.2,	PR
1.2	2019-12-17	2, 3.1, 3.3, 5.1, 6.3, 6.4, 7.1, 8.2, 9.1, 9.2, 9.6, 10.1, 10.2, 11.4, 12, 13.3, 14.2, 14.3, 17.3, 17.4, 18.2, 18.3, 18.4, 21.1, 22.1	NE
1.2.1	2020-01-02	17.4	PR
2.0	2022-12-21	1, 2, 3.1, 3.3, 5.1, 6.1, 6.5, 10.2, 12.2, 12.3, 12.4, 12.5, 12.7, 12.8, 12.9, 12.10, 14.3, 15, 16, 17, 18, 19, 20, 21, 22	HA, EW, FS
2.1	2023-04-06	Ändrat hänvisning i 16.4 till 12.7	HA, PR

Bilaga 1 - Personuppgiftsansvariges Instruktion för Behandling av Personuppgifter

Utöver vad som redan framgår av Personuppgiftsbiträdesavtalet ska Personuppgiftsbiträdet även följa nedanstående Instruktion:

1. Ändamålet, föremålet och arten

1 a. Föremålet för Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige är att:

Personuppgifter behandlas i appen Trelson Assessment för att tillhandahålla tjänst för digitala prov, till exempel nationella prov.

1 b. Ändamålet med Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige är att:

Personuppgifterna används för att koppla vilken/vilka användare som ska få tillgång till provet samt vilket inlämnat prov de har lämnat in. De personuppgifter som vi sparar för elev och lärare är kopplat till ett specifikt prov i appen samt inlämningen i deras Google Drive. Vi sparar även alla administratörers och lärares e-post för att kunna tillhandahålla tjänsten. Personuppgifter sparas under 90 dagar i våra serverloggar för att kunna felsöka och tillhandahålla support åt kund.

1 c. Personuppgiftsbiträdets Behandling av Personuppgifter på uppdrag av den Personuppgiftsansvarige avser huvudsakligen följande behandlingsåtgärder (Behandlingens art eller natur):

Behandlingsåtgärder inkluderar läsning, lagring, överföring, strukturering, användning

2. Behandlingen omfattar följande typer av Personuppgifter

Personuppgiftsbiträdet har rätt att behandla följande typer av Personuppgifter för den Personuppgiftsansvariges räkning:

- Förnamn
- Efternamn
- E-postadress
- Grupptillhörighet
- IP-adress
- Inlämningar och feedback

3. Behandlingen omfattar vissa kategorier av Registrerade

Personuppgiftsbiträdet har rätt att Behandla Personuppgifter avseende följande kategorier av Registrerade:

- Personal
- Elev

4. Ange särskilda hanteringskrav vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet

Personuppgiftsbiträdet ska iaktta följande hanteringskrav vid Behandlingen av Personuppgifter åt den Personuppgiftsansvarige:

- På begäran av PuA ska PuB gallra/ta bort specificerad information som innehåller personuppgifter. Efter begäran har biträdet 30 dagar på sig att gallra/ta bort den information som PuA har angett.
- Vid villkor för avställning av personuppgifter (arkivering) inklusive borttagning av uppgifterna i databasen ska detta ske på begäran av PuA. Efter en sådan begäran har biträdet 60 dagar på dig att ta fram den information som PuA begärt skall avställas och ta bort informationen från databasen.

5. Ange de särskilda tekniska och organisatoriska säkerhetsåtgärder som gäller för Personuppgiftsbiträdets Behandling av Personuppgifter

Personuppgiftsbiträdet ska vidta följande säkerhetsåtgärder vid Behandlingen av Personuppgifterna:

- Vi krypterar all data at rest och data in transit
- Vi genomför löpande interna granskningar för att säkerställa och utveckla vår förmåga att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft i våra system.
- Vi åtar oss att så långt tekniskt möjligt återställa tillgänglighet och tillgång till personuppgifter i rimlig tid vid en fysisk eller teknisk incident. Vi testar, undersöker och utvärderar regelbundet effektiviteten hos de tekniska och organisatoriska åtgärderna som säkerställer behandlingens säkerhet.
- Vi begränsar åtkomst av data inom vår organisation till direkt behov för personal utifrån att kunna utföra sina åtaganden gentemot kund.
- Alla tjänster där vi lagrar persondata skyddas med krav på tvåfaktorsinloggning.
- Vi begränsar åtkomst för tredjepartsleverantör via Google Cloud access approval

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

Personuppgiftsbiträdet ska iaktta följande krav avseende loggning av användaraktivitet och logghantering:

Generellt kring bruket av loggar i appen

- Det av dokumentationen av åtkomsten (loggar) framgår vilka åtgärder som har vidtagits med uppgifter om en registrerad person,
- Det av loggarna framgår vid vilken enhet åtgärderna vidtagits,
- Det av loggarna framgår vid vilken tidpunkt åtgärderna vidtagits,

- Användarens och den registrerades identitet framgår av loggarna,
- Systematiska och återkommande stickprovskontroller av loggarna görs,
- Kontroller av loggarna dokumenteras automatiskt genom auditloggar.

Auditloggar sparas i 400 dagar. (Ex. konto X gjorde operation Y i produkt Z)

- Historik över vilka anställda på Trelson som har hämtat ut data serverloggar sparas i 90 dagar (Ex. användare X kallade på API Y)
- Historik över förändring av för enskild elev samt vem som genomfört förändringen.
- Historik över förändring av för enskilda medarbetare samt vem som genomfört förändringen.

Access transparency loggar

- Historik över vad, när, varför och vem från Google som har fått tillgång till delar Trelsons projekt i syfte för support.

7. Lokalisering och överföring av Personuppgifter till Tredje land

Personuppgiftsbiträdet ska iaktta följande krav avseende lokalisering av Personuppgifter:

Personuppgiftsbiträdet har endast rätt att behandla Personuppgifterna på följande plats/er:

- EU/EES, USA

Om den Personuppgiftsansvarige inte har gett anvisningar om överföring av Personuppgifter till ett Tredje land i Instruktionen, har Personuppgiftsbiträdet inte rätt att göra en sådan överföring.

Personuppgiftsbiträdet ska iaktta följande krav avseende överföring av Personuppgifter till Tredje land:

- Som en del av Personuppgiftsbiträdets fullgörande av tjänsterna som levereras enligt Tjänsteavtalet kan avidentifierade personuppgifter relaterade till supportärenden för personal samt personuppgifter i form av kontaktuppgifter såsom namn, telefonnummer och e-postadress hänförliga till den Personuppgiftsansvariges personal komma att föras över till tredje land via Personuppgiftsbiträdets underleverantör, se Bilaga 2.
- Google och Zendesk är certifierade enligt EU-US Data Privacy Framework.
- Överföring av persondata till USA omfattas av standardavtalsklausuler.
- Personuppgiftsbiträdet ska säkerställa att överföring till tredjeland uppfyller dataskyddsförordningens krav. se Bilaga 3.

8. Behandlingens varaktighet

Personuppgiftsbiträdet behandlar Personuppgifter i enlighet med PUB-avtalet tills det att avtalet upphör.

9. Övriga Instruktioner angående Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet

- PuB skall till PuA kunna lämna ut ett fullständigt registerutdrag som enbart omfattar en registrerades personuppgifter som behandlas i systemet på begäran av PuA.
- PuB ska ha rutiner för att bistå PuA i att uppfylla kravet att rapportera en personuppgiftsincident inom 72 timmar från det att PuA får kännedom om personuppgiftsincidenten.
- Bilaga 3 och de skyddsåtgärder som där presenteras i relation till mål nr C-311/18, “Schrems II” kommer att revideras och uppdateras löpande.

Bilaga 2 – Lista över godkända Underbiträden

Den Personuppgiftsansvarige godkänner att Personuppgiftsbiträdet anlitar nedanstående Underbiträden för Behandling av Personuppgifter.

Bolag/ organisation	Adress och kontaktuppgifter	Lokalisering av Personuppgifter (adress, land)	Typer av Personuppgifter som Behandlas av Underbiträdet	Ändamål med Underbiträdets Behandling	Behandlingstid	Ytterligare information om Underbiträdets Behandling av Personuppgifter
Google Cloud Platform	Privacy Help Center - Policies Help	Servrar inom EU/EES Frankfurt.	Namn, e-postadress, grupper, Publik IP-adress, Inlämningar och feedback	Drift av databas och applikationer. (Molntjänst)	Personuppgifter behandlas löpande under PUB-avtalets varaktighet	Our Cloud Data Privacy Commitments Google Cloud Platform: EU Standard Contract Clauses Google LLC är certifierade enligt EU-US Data Privacy Framework.
Zendesk	Zendesk's Global Privacy Counsel: Rachel Tobin, AGC, EMEA & Global Privacy Counsel, Zendesk International Ltd. 55 Charlemont Place, Saint Kevin's, Dublin, D02 F985 Ireland privacy@zendesk.com	EU, USA	Förnamn, Efternamn, E-postadress	Typ av tjänst: Supportsystem för att hantera och besvara förfrågningar från kunder.	Zendesk används vid supportärenden och inte vid användning av applikationen. Underleverantören behandlar Personuppgifter i enlighet med underbiträdesavtalet.	Trust center Update on Privacy Shield Invalidation by the European Court of Justice Zendesk är certifierade enligt EU-US Data Privacy Framework.

BILAGA 3. YTTERLIGARE SKYDDSÅTGÄRDER FÖR ATT SÄKERSTÄLLA ÖVERFÖRING, VID ANVÄNDNING AV STANDARDAVTALSKLAUSULER (STANDARD CONTRACT CLAUSES) OCH BCR (BINDING CORPORATE RULES), TILL TREDJE LAND AVSEENDE Trelson Assessment

Utifrån domslutet den 16 juli 2020 "Schrems II" (Case C-311/18) gäller inte längre Privacy Shield som laglig grund för behandling av personuppgifter som överförs till USA. Den 10 juli 2023 fattade EU-kommissionen beslut om adekvat skyddsnivå för USA. EU-kommissionens beslut innebär att överföringar som sker till organisationer som omfattas av "EU-US Data Privacy Framework" nu kan ske utan att lämpliga skyddsåtgärder, såsom standardavtalsklausuler, behöver vidtas enligt artikel 46 i

dataskyddsförordningen. Google och Zendesk är certifierade enligt EU-US Data Privacy Framework. Detta dokument beskriver vilka ytterligare skyddsåtgärder vi som företag (Trelson AB) vidtagit för att ytterligare skydda personuppgifter vid behandling i USA.

Detta dokument och skyddsåtgärder kommer att revideras och uppdateras löpande.

Trelson har noterat att följande tjänster och underbiträden innebär eller kan innebära överföring till USA. Trelson har övervägt och analyserat för det fall applikationen Trelson Assessment kan tillhandahållas utan nedanstående tjänster. Efter analys på marknaden och av tjänstens syfte och innehåll har det konstaterats att tjänsterna är nödvändiga för att kunna tillhandahålla Trelson Assessment till våra kunder och användare. Trelson har därför analyserat tjänsterna och vidtagit ytterligare skyddsåtgärder.

1 Generella organisatoriska säkerhetsåtgärder på Trelson

Kontohantering på Trelson

Personal på Trelson får vid tillträde av sin tjänst ett konto i Google workspace som används som en SSO-tjänst gentemot alla andra applikationer som används i företaget. För att kunna logga in på sitt Google Workspace konto på Trelson måste alla medarbetare använda den av företagets bestämda policy för tvåfaktorsinloggning. Utöver den specifika arbetstagaren är det endast en administratör som kan återställa ett konto för att komma åt personuppgifter. Denna administratör hanteras med ett no-reply konto som har en fysisk tvåfaktorsinloggning på ett USB förvarat på säker plats.

Tillgång till användares persondata på Trelson

På Trelson arbetar vi efter premissen att enbart de personer som på grund av sina arbetsuppgifter har i uppdrag att hantera användares persondata har tillgång till personuppgifterna. Detta innebär att det endast är personal för varje specifik tjänst som har tillgång till personuppgifterna. Personalen har sekretessåtaganden avseende de personuppgifter som behandlas.

Fysiska enheter på företaget

Alla enheter som används på Trelson använder senaste säkerhetsuppdateringar samt kryptering av hårddisk. Tjänsterna som används är molnbaserade och skyddas utav ett extra lager med tvåfaktorsinloggning. Se “Kontohantering på Trelson 1.1”

Skalskydd på företaget

Kontoret är beläget på femte våningsplan och nås endast från trapphuset och brandstege på baksidan. Ytterdörren till lokalen är tillverkat av Thoruns AB är av märket Forster Presto, uppfyller brandklass EIC-30 samt är försedd med ett nattlås som uppfyller branschkraven.

Inbrottslarm

Vi har ett inbrottslarm samt kameraövervakning.

2 Personuppgiftsbiträden för applikationen Trelson Assessment

Google Cloud Platform Ytterligare skyddsåtgärder

Googles Globala skyddsåtgärder:

Google har en global infrastruktur designad för att säkert hantera information i hela dess livscykel. Denna infrastruktur möjliggör säker driftsättning av tjänster, säker lagring av data, säker kommunikation mellan tjänster, säker kommunikation mellan tjänster och slutanvändarna, och säker administration av tjänster. Google använder denna infrastruktur för att bygga sina tjänster såsom Google Workspace och Google Cloud.

Säkerheten i infrastrukturen är byggd från grunden i progressiva lager som börjar med säkerheten för Googles datacenter till processerna för administrationen av tjänsterna.

Google investerar mycket i säkerheten av sin infrastruktur och har hundratals anställda ingenjörer dedikerade till att underhålla och förbättra både säkerheten och sekretessen inom hela Google.

Läs mer om Googles säkerhetsåtgärder här:
https://cloud.google.com/security/infrastructure/design

Säkerhetsåtgärder som Trelson vidtagit utöver Googles egna säkerhetsåtgärder

Begränsning av åtkomst till data för anställda på Google genom *Access approval*

Alla projekt i Google Cloud som innefattar personuppgifter och ägs av Trelson har den striktaste nivån av *access approval* vilket betyder att tillgång till projekt från anställda på Google kommer kräva ett explicit godkännande från en anställd på Trelson med tillräckligt hög behörighet i projektet.

Läs mer om Access approval hos Google här:

https://cloud.google.com/access-approval/docs?hl=e

Granskning av åtkomst till data för anställda på Google genom *Access transparency*

Om tillstånd ges för åtkomst till Trelsons projekt i Google Cloud till medarbetare på Google kommer alla handlingar som denne gör att sparas i speciella granskningsloggar för projekten.

Läs mer om Access transparency här:

https://cloud.google.com/logging/docs/audit/access-transparency-overview

Begränsning av åtkomst till data för anställda hos Trelson

Trelson har sedan tidigare begränsat all åtkomst till data och personuppgifter i Google Cloud Platform. Det är endast personal med direkt behov som har tillgång till personuppgifterna. Detta för att kunna utföra sina arbetsuppgifter så att våra användare får bästa servicenivå av tjänsten Trelson Assessment. Personalen har sekretessåtaganden avseende de personuppgifter som behandlas.

Audit loggar

Trelson sparar audit loggar av administrativa händelser och åtkomst av data i Google Cloud Platform. Detta för att kunna hantera eventuella incidenter av personuppgifter.

Krypterad nätverkskommunikation

Trelson använder sig av krypterade kommunikationsprotokoll mellan tjänst till tjänst och tjänst till slutanvändaren.

Inloggning av slutanvändare med Single Sign On

Trelson använder sig av den öppna industristandarden OpenID Connect 2.0 som tillåter användarna att återanvända deras befintliga konton för Single Sign On med tvåfaktors autentisering.

Dokumentation i relation till SCC (Standard contract clauses)
https://cloud.google.com/terms/sccs
https://cloud.google.com/security/privacy

3 Personuppgiftsbiträden för applikationen Trelson Assessment avseende specifika tjänster och avtal

Zendesk

3.1.1 Analys av eventuell överföring till tredje land

Vilket land utanför EU kan uppgifter skickas till?

I undantagsfall USA

När kan personuppgifter komma att överföras till USA?

Supportsystem för att hantera och besvara förfrågningar från användare. Det innebär att Zendesk endast används vid supportärenden inte vid användning av applikationen. Enligt FISA och Cloud Act kan amerikanska staten begära ut personuppgifter från europeiska medborgare i relation till grov brottslighet mot USA. Trelson har tecknat ett Data Processing Agreement med Zendesk.

Typ av personuppgifter relaterade till Zendesk

Förnamn, Efternamn, E-postadress

Vilka personuppgifter kan komma att överföras till USA

Förnamn, Efternamn, E-postadress

Dokumentation i relation till ECC/SCC (EU/Standard contract clauses) och BCR (Binding Corporate Rules)
https://www.zendesk.com/company/privacy-and-data-protection/

3.1.2 Ytterligare skyddsåtgärder

Zendesks skyddsåtgärder

Zendesk är certifierat enligt SOC 2 Typ 2, ISO 27001:2013, ISO 27001:2014

Alla data i vila och under transport är krypterad

Oberoende penetrationstestning genomförs på årlig basis

All data är begränsad genom rollbaserad åtkomstkontroll

How We Protect Your Service Data (Enterprise Services)

Säkerhetsåtgärder som Trelson vidtagit utöver Zendesk egna säkerhetsåtgärder

Datalagring

All persondata som behandlas av Zendesk lagras på server inom EU.

Begränsning av åtkomst till data

Det är endast personal med direkt behov som har tillgång till personuppgifterna. Detta för att kunna utföra sina arbetsuppgifter så att våra kunder får bästa servicenivå av tjänsten Trelson Assessment. Personalen har sekretessåtaganden avseende de personuppgifter som

behandlas. Trelson har regelbunden utbildning för supportpersonal i personuppgiftshantering.

Rutiner för gallring

Uppdaterat rutin för gallring av ärenden. När ett ärende är färdigbehandlat och stängt så sparar vi ärendet i 6 månader för möjlig uppföljning.

Utbildning

Vi utbildar regelbundet vår supportpersonal i relation till att hantera personuppgifter i Zendesk.

Maskning av personuppgifter

Trelson använder sig av en specifik tjänst från Zendesk - Ticket Redaction App. Denna tjänst medför att alla personuppgifter utöver e-postadress och namn som inkommer till Trelson i supportärenden maskas, dvs döljs permanent.

Inloggning

All inloggning i Zendesk sker genom SSO för Google Workspace där tvåfaktorsinloggning är ett krav. Se “Kontohantering på Trelson” 1.1

Zendesk support

Kontoövertagande av Zendesk support är avstängt och kan enbart aktiveras av administratörer. Rutinen för kontoövertagande sker enbart tidsbegränsat under tiden för det faktiska supportärendet.