

Personuppgiftsbiträdesavtal

Innehållsförteckning

1	PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER.....	2
2	DEFINITIONER	2
3	BAKGRUND OCH SYFTE	4
4	BEHANDLING AV PERSONUPPGIFTER OCH SPECIFIKATION	4
5	DEN PERSONUPPGIFTSANSVARIGES ANSVAR.....	4
6	PERSONUPPGIFTSBITRÄDETS ÅTAGANDEN	5
7	SÄKERHETSÅTGÄRDER	5
8	SEKRETESS/TYSTNADSPLIKT	6
9	GRANSKNING, TILLSYN OCH REVISION	6
10	HANTERING AV RÄTTELSE OCH RADERING M.M.....	7
11	PERSONUPPGIFTSINCIDENTER.....	7
12	UNDERBITRÄDE.....	8
13	LOKALISERING OCH ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND	9
14	ANSVAR FÖR SKADA I SAMBAND MED BEHANDLING.....	9
15	PUB-AVTALETS TECKNANDE, AVTALSTID OCH UPPSÄGNING	10
16	ÄNDRINGAR OCH UPPSÄGNING MED OMEDELBAR VERKAN M.M.	10
17	ÅTGÄRDER VID PUB-AVTALETS UPPHÖRANDE	10
18	MEDDELANDE INOM RAMEN FÖR DETTA PUB-AVTAL OCH INSTRUKTIONER	11
19	KONTAKTPERSONER	11
20	ANSVAR FÖR UPPGIFTER OM PARTERNA OCH KONTAKTPERSONER SAMT KONTAKTUPPGIFTER	11
21	LAGVAL OCH TVISTER	11
22	PARTERNAS UNDERTECKNANDE AV PUB-AVTALET	11

PERSONUPPGIFTSBITRÄDESAVTAL

Avtal enligt artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679¹

1 PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER

Personuppgiftsansvarig	Personuppgiftsbiträde
xxxx	Edith Care (Jobello Technology AB)
Organisationsnummer	Organisationsnummer
XXXXXX-XXXX	559311-6907 (Jobello Technology AB)
Postadress	Postadress
XXXXX	fredrik@edithcare.se
Kontaktperson för administration av detta personuppgiftsbiträdesavtal	Kontaktperson för administration av detta personuppgiftsbiträdesavtal
Namn: xxxx E-post: xxxx	Namn: Fredrik Gordh Riseby E-post: fredrik@edithcare.se
Kontaktperson för parternas samarbete om dataskydd	Kontaktpersoner för parternas samarbete om dataskydd
Namn: xxxx E-post: xxxx	Namn: Fredrik Gordh Riseby E-post: fredrik@edithcare.se

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 lokaliseringssuppgift 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 Personuppgiftsbiträdet ska genom behörighetskontrollsystem endast ge åtkomst till Personuppgifterna för sådana fysiska personer som arbetar under Personuppgiftsbitrådets 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 Personuppgiftsbitrådets 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 Personuppgiftsbiträdet ska bereda tillsynsmyndighet, eller annan myndighet som har laglig rätt till det, möjlighet att göra tillsyn enligt myndighetens begäran i enlighet med vad som stadgas i 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 RÄTTELSE OCH RADERING M.M.

- 10.1 För det fall den Personuppgiftsansvarige begärt rättelse eller radering på grund av Personuppgiftsbitrådets 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 Personuppgiftsbiträdet 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 obehörig Behandling och/eller åtkomst till Personuppgifterna.

- 11.3 Vid Personuppgiftsincident, vilken Personuppgiftsbiträdet 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:
- Personuppgiftsincidentens art och, om möjligt, de kategorier och antalet Registrerade som berörs samt kategorier och antalet personuppgiftsposter som berörs,
 - de sannolika konsekvenserna av Personuppgiftsincidenten, och
 - åtgärder som har vidtagits eller föreslagits samt åtgärder för att mildra Personuppgiftsincidentens 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
- Underbiträdets namn, organisationsnummer och säte (adress och land),
 - vilken typ av uppgifter och kategorier av Registrerade som behandlas, och
 - 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 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 Personuppgiftsbitrådets anlitande av ett nytt underbiträde, enligt detta PUB-avtal, punkten 12.6, 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 Personuppgiftsbitrådet 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 Personuppgiftsbitrådet erhållit genom informationsutbyte enligt PUB-avtalet.
- 17.2 I samband med återlämning ska Personuppgiftsbitrådet 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 Personuppgiftsbitrådet 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 ingås elektroniskt. Vårdgivaren accepterar avtalet genom att vid registrering i Tjänsten markera kryssrutan för godkännande av Personuppgiftsbiträdesavtalet. Vid acceptansen registreras avtalsversion, tidpunkt, accepterande användare samt en kryptografisk kontrollsumma (SHA-256) av dokumentet, vilket tillsammans utgör parternas ingående av avtalet. Ingen signatur därutöver krävs.

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: Tillhandahålla tjänsten Edith Care till den Personuppgiftsansvariges användare (utredare, psykologer och administratörer) inklusive kontohantering, inloggning, behörigheter, dokumentuppladdning, transkribering av kliniska samtal, AI-assisterad sammanställning av utredningsunderlag samt hantering av utredningsdokumentation. 1 b. Ändamålet med Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige är att: Möjliggöra AI-assisterad dokumentation och sammanställning vid neuropsykiatriska utredningar (autism, ADHD, kombinationsutredningar), samt administrativ hantering av användare och behörigheter inom den Personuppgiftsansvariges vårdverksamhet. 1 c. Personuppgiftsbiträdets Behandling av Personuppgifter på uppdrag av den Personuppgiftsansvarige avser huvudsakligen följande behandlingsåtgärder (Behandlingens art eller natur): Insamling (via användare/dokumentuppladdning), registrering, lagring, strukturering, transkribering, AI-assisterad analys och sammanställning, åtkomst, användning, rapportering, felsökning/support, säkerhetsloggning, radering/återlämning vid avtalets upphörande.
2. Behandlingen omfattar följande typer av Personuppgifter
Personuppgiftsbiträdet har rätt att behandla följande typer av Personuppgifter för den Personuppgiftsansvariges räkning: Kontouppgifter: - namn, e-post, användar-ID - roll (utredare/psykolog/admin), mottagningsnamn samt arbetsgrupp Tekniska uppgifter: - IP-adress - enhets-/webbläsarinfo (user agent) - loggar för inloggning och adminåtgärder Hälsö- och sjukvårdsdata (särskilda kategorier av personuppgifter, artikel 9 GDPR): uppladdade utredningsdokument, transkriberade kliniska samtal, AI-genererade sammanställningar, bedömningsunderlag och utredningsresultat

utredaradministration: patientärenden, utredningsmallar, utredningsstatus och dokumentflöden

Meddelanden/support:

supportärenden och kommunikation kopplad till ärendet

AI-assisterad analys:

- AI-genererade sammanställningar, utredningsförslag och dokumentutkast kopplade till patientärenden

Behandlingen avser till sin natur särskilda kategorier av personuppgifter (hälsodata). Laglig grund tillhandahålls av den Personuppgiftsansvarige i enlighet med artikel 9.2(h) GDPR och 3 kap. 5 § PDL.

3. Behandlingen omfattar vissa kategorier av Registrerade
Personuppgiftsbiträdet har rätt att Behandla Personuppgifter avseende följande kategorier av Registrerade: Patienter (personer som genomgår neuropsykiatrisk utredning) Vårdpersonal (utredare, psykologer, administratörer) Administratörer (verksamhetsledning/IT)
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: Gallring/retention: Kontodata + utredningsdata: sparas under avtalsperioden och raderas/återlämnas inom 30 dagar efter upphörande (om kunden inte begär export). Patientdata lagras i enlighet med Patientdatalagen (PDL) och HSLF-FS 2016:40. Supportärenden: 24 månader (för spårbarhet), därefter raderas/anonymiseras. Säkerhetskopior: roterande backups, max 35 dagar. Ljudbackuper av inspelade samtal omfattas inte av backuprotationen utan raderas automatiskt 7 dagar efter skapande. Loggar: 12 månader.
5. Ange de särskilda tekniska och organisatoriska säkerhetsåtgärder som gäller för Personuppgiftsbitrådets Behandling av Personuppgifter
Personuppgiftsbiträdet ska vidta följande säkerhetsåtgärder vid Behandlingen av Personuppgifterna: Tekniska • TLS/HTTPS i transit för frontend och backend samt tvingad HTTPS + HSTS och säkra cookies i backend. • Krypterade anslutningar till databasen där TLS krävs. • Kryptering i vila via Azure-plattformen (AES-256) för databas, objektlagring och backuper. • Åtkomstkontroll enligt least-privilege; separata adminkonton, MFA för administrativa konto. • Loggning/spårbarhet via plattformsloggar och applikationsloggar; loggar skyddas mot obehörig åtkomst. • Sårbarhetshantering och patchrutiner (Azure-plattform patchas av Microsoft; applikations-/beroenden patchas av Edith Care) samt backup- och återställningsrutiner via Azure Sweden Central. Organisatoriska

• Behörighetsstyrning inkl. onboarding/offboarding och regelbunden åtkomstöversyn. • Sekretessåtaganden för personal (och relevanta underkonsulter) samt grundläggande säkerhetsutbildning. • Incidentprocess inkl. rapportering till personuppgiftsansvarig utan onödigt dröjsmål. • Årlig egenkontroll/revision av relevanta säkerhetsrutiner.
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: Logga: inloggningar, behörighetsändringar, adminåtgärder, fel/incidenthändelser Åtkomst till loggar: endast utsedda admin/teknikroller Lagringstid: 12 månader (eller det ni kan stå för)
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: • Behandling sker inom EU/EES i Sverige (Azure Sweden Central, datacenter i Gävle/Sandviken och Staffanstorps). 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: • Personuppgifter får inte överföras till tredje land utan den Personuppgiftsansvariges skriftliga godkännande och dokumenterade instruktion
8. Behandlingens varaktighet
Så länge Huvudavtalet gäller och i övrigt enligt avsnitt 17 (åtgärder vid upphörande).
9. Övriga Instruktioner angående Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet
-

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 Underbitrådets Behandling	Behandlingstid	Ytterligare information om Underbitrådets Behandling av Personuppgifter
Microsoft Corporation (Azure Database for PostgreSQL)	Kontakt enligt Microsofts DPA (DPO/Privacy-contact)	Sverige (EU/EES) — Azure Sweden Central (Gävle/Sandviken, Staffanstorps)	Alla patientdata: kontouppgifter, utredningsdata, hälsodata (artikel 9), tekniska loggar	Primär databas för all persistent datalagring	Under avtalstiden + enligt instruktion (radering/återlämning efter upphörande)	Behandling sker uteslutande i Azure Sweden Central. Microsoft DPA: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA
Microsoft Corporation (Azure OpenAI Service)	Kontakt enligt Microsofts DPA (DPO/Privacy-contact)	Sverige (EU/EES) — Azure Sweden Central	Klinisk text (prompter/svar). Ingen lagring — data behandlas i realtid och raderas omedelbart	AI-textbehandling: generering av utkast till utredningsdokumentation	Ingen persistent lagring. Data behandlas i transit och raderas omedelbart efter svar	Zero data retention policy. Microsofts åtagande: inga kunddata används för modellträning. Microsoft DPA gäller.
Microsoft Corporation (Azure Speech Services)	Kontakt enligt Microsofts DPA (DPO/Privacy-contact)	Sverige (EU/EES) — Azure Sweden Central	Ljudinspelningar (samtal mellan kliniker och patient). Ingen persistent lagring	Transkribering av kliniska samtal (tal-till-text)	Ingen persistent lagring. Ljud behandlas i realtid och raderas efter transkribering	Zero data retention. Ljud processas i transit. Microsoft DPA gäller.
Microsoft Corporation (Azure Blob Storage)	Kontakt enligt Microsofts DPA (DPO/Privacy-contact)	Sverige (EU/EES) — Azure Sweden Central	Mallfiler, ljudbackup, genererade dokument	Fillagring och objektlagring för backup och dokumentmallar	Mallfiler och genererade dokument: under avtalstiden + enligt instruktion. Ljudbackup: endast när realtidstranskribering inte varit tillgänglig; raderas automatiskt genom lagringslivscykel 7 dagar efter skapande (effektiv lagring upp till ca 8 dagar)	Krypterat i vila (AES-256). Behandling i Azure Sweden Central. Microsoft DPA gäller.

PostHog Inc.	Kontakt enligt PostHogs DPA/Privacy Policy	EU (Frankfurt, Tyskland)	Anonymiserad metadata: sidvisningar, knapptryck, funktionsanvändning. Inga patientdata, inga personuppgifter	Produktanalys — cookieless, respekterar Do Not Track. Används för att förbättra användargränssnittet	Enligt PostHogs datalagringspolicy (typiskt 90 dagar för sessionsdata)	PostHog EU-hosting. Ingen åtkomst till patientdata. Anonymiserad metadata som inte utgör personuppgifter i GDPR-mening.
Langfuse GmbH	Kontakt enligt Langfuse DPA/Privacy Policy	EU (Frankfurt, Tyskland)	Anonymiserad metadata i produktion: latens, tokenantal, modellversion, felkoder. Inga prompter eller svar i produktionsmiljö	AI-övervakning och kvalitetssäkring — prestanda och felsökning av AI-komponenter	Enligt Langfuse datalagringspolicy	Langfuse EU-hosting. I produktionsmiljö loggas enbart metadata — inga prompter, svar eller patientdata. I utvecklingsmiljö kan syntetisk testdata användas.
Functional Software, Inc. (Sentry)	Kontakt enligt Sentries DPA/Privacy Policy (sentry.io/legal/dpa)	EU (Frankfurt, Tyskland) — Sentry EU-region (AWS eu-central-1)	Teknisk feldata: felmeddelanden, stacktrace, release/miljö, anrops-metadata. Inga IP/cookies/PII (sendDefaultPii: false). Inga patientdata.	Felövervakning och stabilitet (error tracking) — felsökning av applikationsfel	Enligt Sentries datalagringspolicy (standard 90 dagar för event)	Sentry EU-hosting. PII avstängt. Sentries DPA gäller. Server-side scrubbing (beforeSend) säkerställer att patientdata inte hamnar i felpayload.
Microsoft Corporation (Azure AI Document Intelligence)	Kontakt enligt Microsofts DPA (DPO/Privacy-contact)	Sverige (EU/EES) — Azure Sweden Central	Uppladdade utredningsdokument/PDF:er (kan innehålla hälsodata, särskilda kategorier art. 9 GDPR)	OCR — textextraktion ur uppladdade dokument (t.ex. labbsvar/1177) för vidare bearbetning	Ingen persistent lagring. Dokument behandlas i transit; extraerad text loggas aldrig.	Behandling sker uteslutande i Azure Sweden Central. Krypterat i transit. Microsoft DPA gäller. Extraerad text loggas ej (förhindrar att patientdata hamnar i loggar).
Resend, Inc.	Kontakt enligt Resends DPA/Privacy Policy (resend.com/legal)	EU/EES — Irland (AWS eu-west-1)	Kontouppgifter i transaktionsmejl: namn, e-postadress, organisation. Inga patientdata/hälsodata.	Transaktionsmejl: kontoaktivering, inbjudan, godkännande, lösenordsåterställning	Enligt Resends datalagringspolicy	Avsändardomän edithcare.se verifierad i EU-region (Irland). Resends DPA gäller. Inga kliniska data skickas via mejl.
Vercel Inc.	Kontakt enligt Vercels DPA (vercel.com/legal/dpa)	Sverige (EU/EES) — Vercel Function Region Stockholm (eu-north-1 / arn1)	All applikationstrafik i transit (kan inkludera hälsodata art. 9 vid API-anrop), samt anonym webbletemetri (Core Web Vitals, sidvisningar)	Applikationshosting/drift (serverless functions, Fluid Compute) samt anonym prestanda-/användningstelemetri	Ingen persistent lagring av patientdata (lagras i Azure PostgreSQL/Blob). Loggar enligt Vercels policy.	Serverfunktioner körs uteslutande i Stockholm (Sverige). Vercel DPA gäller. Patientdata passerar endast i transit/minne, lagras aldrig persistent hos Vercel.