Personuppgiftsbiträdesavtal

a) Innehållsförteckning

PERSONUPPGIFTSBITRÄDESAVTAL

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

1 PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER

Personuppgiftsansvarig	Personuppgiftsbiträde
Region Västmanland/Hjälpmedelscentrum	Breas Medical AB
Organisationsnummer	**Organisationsnummer**
2321100-0172	556434-8968
Postadress	**Postadress**
Signalistgatan 2, 72131 Västerås	Företagsvägen 1, 435 33 Mölnlycke
Kontaktperson för administration av detta personuppgiftsbiträdesavtal	**Kontaktperson för administration av detta personuppgiftsbiträdesavtal**
Namn: Joakim Axelsson E-post: joakim.axelsson@regionvastmanland.se Tfn: 021-175649	Namn: Martina Liss E-post: martina.liss@breas.com Tfn: +46 790 66 19 81
Kontaktperson för parternas samarbete om dataskydd	**Kontaktpersoner för parternas samarbete om dataskydd**
Namn: Agata Cierzniak - DPO E-post: dataskyddsombudet@regionvastmanland.se	Namn: Ermira Gashi E-post: privacy@breas.com Tfn: +46 31 86 88 00
Affärsavtal/Huvudavtal som detta personuppgiftsbiträdesavtal gäller Avtal IN-IN25-0032 Andningshjälpmedel (molntjänst för telemedicin)	

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

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.

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. Personuppgifts-

biträdet 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 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 12.67, 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 Personuppgifts-ansvarige 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

Region Västmanland/Hjälpmedelscentrum

Ort och datum: Västerås 2026-03-09

_____

Magnus Loman, Verksamhetschef

_____

Signatur

Personuppgiftsbiträde

Breas Medical AB

Ort och datum: Mölnlycke 2026-03-09

_____

Sebastian Mommers, MD

_____

Signatur

Versionshantering

Versionshantering				
Dokument	Version	Datum	Ändringar	Ansvarig
Avtal, Bilaga 1, Bilaga 2, Bilaga 3	0.1	2026-02-23	Version 0.1 upprättas.	ML (Breas), JAX (RV)
Avtal, Bilaga 1, Bilaga 2	1.0	2026-03-04	Version 1.0 upprättas Bilaga 1, punkter 1, 4, 5, 7, 9 kompletteras/ justeras Bilaga 2, justeras	JR (Breas), JAX (RV)

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:

Molntjänst för telemedicin: EveryWare By Breas®

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

Distansmonitorering och -behandling i hemmet av patienter med hypoventilation (otillräcklig egen andning med koldioxidretention som följd) Behandling sker med medicinteknisk utrustning bilevelPAP eller ventilator. Telemedicintjänsten möjliggör uppföljning och i vissa fall inställning av behandlingsparametrar på distans.

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

- Insamling
- Lagring
- Analys
- Sammanställning

2. Behandlingen omfattar följande typer av Personuppgifter

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

Patienters personuppgifter

- Namn
- Personnummer
- Behandlingsapparatens enhetsnummer
- Andningsmönster
- Användningstid
- Behandlingsinställningar

Anställdas personuppgifter

- Namn
- E-postadress
- Ev. behörigheter

Känsliga personuppgifter som behandlas

- Patienters hälso- och sjukdomsdata.

3. Behandlingen omfattar vissa kategorier av Registrerade

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

Kategorier av registrerade utgörs av:

- Patienter
- Anställda

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:

- Samtliga Personuppgifter ska av Personuppgiftsbiträdet, vid anmodan från Personuppgiftsansvarig, i elektroniskt läsbart format återlämnas vid avslutande av Personuppgiftsbiträdesavtalet. Efter att Personuppgiftsansvarig skriftligen återkopplat till Personuppgiftsbiträdet att återlämnandet mottagits ska Personuppgiftsbiträdet radera samtliga Personuppgifter.
- Personuppgiftbiträdet ska radera samtliga Personuppgifter, om inte Personuppgiftsansvarig har anmodat Personuppgiftsbiträdet att återlämna Personuppgifterna, inom 6 månader från Personuppgiftsbiträdesavtalets upphörande.
- Skyldigheten för Personuppgiftsbiträdet att radera Personuppgifter gäller inte om lagring av Personuppgifter krävs enligt unionsrätten eller nationell rätt unionsrätten eller nationell rätt.

I övrgt se punkt 5 nedan.

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

Personuppgiftbiträdet ska vidta följande säkerhetsåtgärder vid Behandlingen av Personuppgifterna:

Samtliga obligatoriska informationssäkerhetskrav i detta avtal samt informationssäkerhetskraven som är ställda i upphandlingsunderlaget, och som är avtalade mellan parterna skall följas.

Upphandlingens IT-krav samt Informationssäkerhetskrav som är relevanta för detta PUB-avtal beskrivs i utdrag i Bilaga 3.

Krypteringsprotokoll ska vara standardiserad enligt lägst TLS 1.2-protokoll med 2048-bitars RSA/SHA256-krypteringsnycklar, som rekommenderas av CESG/NCSC, för att kryptera kommunikationen både mellan kunden och molnet, samt internt mellan Azure-system och datacenter

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:

Utöver samtliga krav rörande loggning i upphandlingsunderlaget, utgör nedanstående ett förtydligande av punkt 7.5 i detta huvudavtal.

En logg ska minst innehålla, men inte begränsas till följande:

- användarens unika identitet,
- datum,
- tid,
- vilken uppgift som är
  - skapad,
  - läst,
  - redigerat och
  - raderat.

7. Lokalisering och överföring av Personuppgifter till Tredje land

Personuppgiftsbiträdet ska iaktta följande krav avseende lokalisering av Personuppgifter:

Personuppgiftsbiträdets datalagring och personuppgiftsbehandling ska uppfylla en adekvat skyddsnivå enligt kravställan på Dataskydd i upphandlingsunderlaget.

Eventuella ändringar av förhållande bakom svar enligt sektionen för Dataskydd i kravställan ska anmälas till och godkännas av Personuppgiftsansvarig innan sådan ändring får utföras.

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 lokalisering av Personuppgifter: **Inga tredjelandsöverföringar får förekomma**

8. Behandlingens varaktighet

Personuppgiftsbiträdet får behandla Personuppgifter inom 5 år efter tidpunkten för sista leverans inom avtalet. Se upphandlingsunderlag, krav för Telemedicintjänst 5.1.4.

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

Rapportering av personuppgiftsincidenter

Personuppgiftsbiträdet ska ha en rutin för rapportering och hantering av personuppgiftsincidenter och säkerhetsincidenter samt återrapportera utan dröjsmål (inom 24 timmar) till den Personuppgiftsansvarige genom att kontakta **den Personuppgiftsansvariges kontaktperson för detta avtal** och dataskyddsombudet@regionvastmanland.se. Rapporten som förmedlas ska innehålla uppgifter om hur, vad, när, vilkas uppgifter och i vilken omfattning incidenten har skett samt vilka åtgärder som vidtagits.

Rapportering från Breas sker av:

- DPO Ermira Gashi
- Email: privacy@breas.com
- Telephone: +46 031 86 88 00
- Address: Breas Medical AB, Företagsvägen 1, 435 33 Mölnlycke, Sweden.

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**
Microsoft Corporation	Regeringsgatan 25, 111 43 Stockholm	Paris, Frankrike	Patienters personuppgifter •Namn •Personnummer • Behandlingsapparatens enhetsnummer •Andningsmönster •Användningstid •Behandlingsinställningar Anställdas personuppgifter •Namn •E-postadress •Ev. behörigheter	EveryWare-applikationen och databasservrarna är värd i Microsofts Azure-infrastruktur	Data från kliniker behandlas tills kontot för den specifika klinikern tas bort. Personuppgifter från patienter behandlas tills den specifika patientjournalen inom EveryWare tas bort. Breas kommer att behandla personuppgifter så länge du har ett EveryWare by Breas-konto; men kommer inte att lagras längre än 2 år, om inte annat avtalats.	Observera att Microsoft agerar som en tredje part där den enbart kommer att behandla användarens e-postadress i syfte att logga in/autentisera. Ingen PHI-data delas med någon annan tredje part enligt Bilaga 1 punkt 7.

Bilaga 3 – IT-samt Informationssäkerhetskrav

Utsnitt från IT-krav från upphandlingsunderlag bilaga 7B Kravspecifikation
Bilevel avancerad med telemedicin till affärsavtal IN-IN25-0032.

IT Krav/frågor område Andningshjälpmedel - selektion till PUB-avtal	
Pos.nr.	**Beskrivning, krav och frågor**
	IT-KRAV
18	**Användarstöd och support**
18.1	**Obligatoriska krav**
18.1.1	Vid behov får Leverantörens tekniker tillgång till systemets produktionsmiljö genom att Kunden tillhandahåller en klientprogramvara med krypterad förbindelse som nyttjas av Leverantören. Följande förutsättningar ska då gälla: • Leverantören ska underteckna förpliktelse om tystnadsplikt. • Icke avidentifierade patientdata ska inte lagras i Leverantörens utrustning, varken permanent eller ens temporärt. • Datasäkerheten ska inte på något sätt äventyras.
19	**Telemedicintjänst**
19.1	**Kommunikation**
19.1.1	**Obligatoriska krav**
19.1.1.1	All trafik mellan klient och webservrar ska ske via HTTPS
19.1.1.2	All nätverkskommunikation mellan parterna (system och stödtjänster) ska skyddas med TLS på transportnivå i enlighet med RFC 7525 och löpande uppdatera enligt nya versioner.
19.1.1.3	Systemet ska vid driftstart möjliggöra kommunikation enligt standarden TLS, som lägst 1.2, eller motsvarande. Se även informationssäkerhetskrav angående godkända cipher suites.
19.1.1.4	All kommunikation mellan klient och server ska skyddas av ett publikt utgivet certifikat från en betrodd CA för klienten.
19.1.1.5	Leverantören ska ange om lösningen kräver någon särskild nätverkskonfiguration i regionens nät, t ex öppna portar mm.
19.2	**Information och lagring**
19.2.2	**Obligatoriska krav**
19.2.2.1	Tjänsten ska spara data på ett sätt som säkerställer datakonsistens och korrekthet.
19.2.2.2	Tjänsten ska spara information tillräckligt länge och tillräckligt detaljerat för det kliniska behovet.
19.2.2.3	Tjänstens ska ha skyddsmekanismer (t ex säkerhetskopiering) så att möjlighet finns att återskapa information i händelse av att information försvinner eller blir korrupt.
19.2.2.4	Säkerhetskopior eller motsvarande ska förvaras åtskilda från produktionsdata.
19.2.2.5	Det ska vara möjligt att permanent radera data (t ex vid gallring enligt OSL eller rätt att bli bortglömd (GDPR))
19.2.2.6	Leverantören ska ange om data, insamlad i tjänsten, kan nås på något annat sätt än det kliniska webgränssnittet. Ange i så fall vilka förutsättningar som måste vara uppfyllda för åtkomst.
19.2.2.7	Leverantören ska ange om och hur export av data från lösningen kan ske.
19.6	**Användarhantering, identitet och åtkomst**
19.6.1	**Obligatoriska krav**
19.6.1.1	Leverantören ska beskriva hur behörighetstilldelning hanteras i tjänsten. Beskrivningen ska ge en bild av hur administration av användare, roller och behörigheter i systemet fungerar samt möjlighet till automation av detsamma
19.6.1.2	Autentiseringen av användaren ska ske så att adekvat skyddsnivå erhålls.

20.6	**Användarhantering, identitet och åtkomst**
20.6.1	**Obligatoriska krav**
20.6.1.1	Leverantören ska beskriva hur behörighetstilldelning hanteras i tjänsten. Beskrivningen ska ge en bild av hur administration av användare, roller och behörigheter i systemet fungerar samt möjlighet till automation av detsamma Särskilt ska framgå om behörighet är gemensam med eventuell telemedicintjänst.
20.6.1.2	Leverantören ska beskriva hur autentisering av användare kan ske. Ange om olika alternativ stöds.
20.7	**Säkerhet**
20.7.1	**Obligatoriska krav**
20.7.1.1	Information ska ha en adekvat skyddnivå under transport och i vila i hela tjänsten.
20.7.1.2	Lösningen, och sådana komponenter som ingår i lösningen, ska vid varje tidpunkt ha ett fullgott skydd mot kända sårbarheter. Skydd mot nya sårbarheter ska införas utan dröjsmål.
21.4	**Användarhantering, identitet och åtkomst**
21.4.1	**Obligatoriska krav**
21.4.1.1	Beskriv hur behörighetstilldelning hanteras i tjänsten. Beskrivningen ska ge en bild av hur administration av användare, roller och behörigheter i systemet fungerar samt möjlighet till automation av detsamma Särskilt ska framgå om behörighet är gemensam med eventuell telemedicintjänst.
21.4.1.2	Beskriv hur autentisering av användare kan ske. Ange om olika alternativ stöds.
21.5	**Säkerhet**
21.5.1	**Obligatoriska krav**
21.5.1.1	Information ska ha en adekvat skyddnivå under transport och i vila i hela tjänsten.
21.5.1.2	Lösningen, och sådana komponenter som ingår i lösningen, ska vid varje tidpunkt ha ett fullgott skydd mot kända sårbarheter. Skydd mot nya sårbarheter ska införas utan dröjsmål.

INFORMATIONSSÄKERHET	
22	**Organisation av informationssäkerhetsarbete**
22.1	**Obligatoriska krav**
22.1.1	Leverantören ska ha ett etablerat informations- och IT-säkerhetsarbete som är systematiskt och riskbaserat. (Leverantören ska för de delar av verksamheten som berörs i leveransen ha ett ledningssystem för informationssäkerhet (LIS) som baseras på SS-EN ISO/IEC27001:2017 eller motsvarande. Ledningssystemet ska omfatta bland annat att samtliga säkerhetskritiska administrativa och tekniska processer är dokumenterade och vilar på en formell grund där roller, ansvar och befogenheter finns tydligt definierade.
22.1.2	Uppgifter om informationssäkerhetshot ska samlas in och analyseras för att ta fram hotunderrättelser.
22.1.3	IKT-beredskap (informations- och kommunikationsteknik) ska planeras, införas, underhållas och testas utifrån målen för kontinuitetshantering och kraven på IKT-kontinuitet.
22.1.4	Leverantören ska ha dokumenterade rutiner för distansarbete. Informationsbehandlingen ska vara lika säker på distans som den är vid behandling på leverantörens arbetsplats.
22.1.5	Informationssäkerhetsincidenter som utgör personuppgiftsincidenter ska rapporteras till integritetsskyddsmyndigheten inom 72h från upptäckt
23	**Hantering av informationstillgångar**
23.1	**Obligatoriska krav**
23.1.1	Leverantören ska ha dokumenterade regler, rutiner och roller som beskriver tillåten användning av informationstillgångar och andra relaterade resurser (t.ex. arbetsdatorer, bärbara datorer eller mobila enheter) som ingår i leveransen. Leverantören ska årligen kontrollera att de efterlevs.
23.1.2	Leverantören ska ha rutiner och funktioner för att återlämna beställarens fysiska och elektroniska tillgångar då anställning, uppdrag eller avtal upphör. Leverantören ska på begäran kunna uppvisa underlag på att så skett.
23.1.3	Beställarens krav på informationshanteringen ska efterföljas i relation till beställarens informationsklassning. Om sådana krav inte ställts ska leverantören utan anmodan kunna uppvisa de rutiner som gäller hos leverantören för hantering av beställarens tillgångar.

23.1.4	Information som lagras i informationssystem, enheter eller andra lagringsmedier ska raderas när den inte längre behövs.
23.1.5	Datamaskning (anonymisering eller pseudonymisering) ska användas i enlighet med organisationens ämnesspecifika policy för åtkomstkontroll och andra relaterade ämnesspecifika policyer och tillämplig SS-EN ISO/IEC 27001:2023 (sv) lagstiftning. verksamhetskrav
24	**Driftssäkerhet**
24.1	**Obligatoriska krav**
24.1.1	Åtgärder för att förhindra dataläckage ska tillämpas på system, nätverk och andra enheter som behandlar, lagrar eller överför känslig information.
24.1.2	Principer för säker kodning ska tillämpas på programvaruutveckling.
24.1.3	Leverantören ska dokumentera ansvar för driftsrutiner och göra de tillgängliga för användare som behöver dem.
24.1.4	Leverantören ska ha rutiner för att planera, genomföra och dokumentera alla förändringar som påverkar leveransens säkerhet. Större förändringar ska följas upp, kontrolleras och redovisas minst årligen för beställaren.
24.1.5	Leverantören ska skydda mot skadlig kod. Det genom att ha säkerhetsåtgärder som inbegriper följande områden: förebygga, upptäcka, hantera och återställa Säkerhetsåtgärderna ska ses över minst årligen.
24.1.6	Leverantören ska ha rutiner och funktioner för säkerhetskopiering och återställande av information enligt överenskomna tillgänglighetskrav med beställaren. Säkerhetskopior ska skyddas på motsvarande sätt som originalinformationen. De ska förvaras på annan plats och på tillräckligt avstånd för att inte utsättas för eventuella skador vid katastrof på det ordinarie driftstället.
24.1.7	Leverantören ska tillse att information, tjänster och system har loggningsfunktioner för säkerhetsrelaterade händelser, minst för felaktiga inloggningar, förändring av behörigheter, otillåten anslutning samt överträdelser av behörigheter. Loggning ska ske i samråd med beställaren. Leverantören ska aktivt använda loggarna för att upptäcka och hantera incidenter. Beställaren ska kunna genomföra granskning av loggar vid behov.
24.1.8	Loggar över åtkomst till information ska sparas minst lika länge som informationen sparas.
24.1.9	Leverantören ska skydda loggningsfunktioner och loggningsverktyg mot manipulation och obehörig åtkomst som även omfattar leverantörens personal.
24.1.10	Leverantören ska ha funktioner, processer och rutiner för att övervaka och göra prognoser avseende framtida krav på systemprestanda.
24.1.11	Leverantören ska testa samtliga leveranser i separat testmiljö innan de införs i beställarens driftmiljö (produktion). Testdata ska skyddas, kontrolleras och får inte innehålla information som är känslig eller omfattas av sekretess.
24.1.12	Leverantören ska tillse att information, tjänster och system, samt relaterad infrastruktur använder tidssynkronisering mot en och samma tidskälla (förslagsvis GPS eller svenska UTC (SP)).
24.1.13	Leverantören ska verifiera och begränsa den mjukvara som får installeras på driftsystem.
24.1.14	Leverantören ska bedriva ett kontinuerligt arbete för att identifiera sårbarheter och utan dröjsmål informera en utpekad funktion hos beställaren om de kan innebära ett hot för beställarens information, tjänster och system. Upptäckta sårbarheter ska åtgärdas omgående.
25	**Kommunikationssäkerhet**
25.1	**Obligatoriska krav**
25.1.1	Leverantören ska säkerställa att all kommunikation till och från system samt lagring, tjänster eller information ska vara skyddad mot obehörig åtkomst eller förvanskning . Det avser kommunikation mellan klient och server och mellan olika systemkomponenter. Skyddet ska uppdateras löpande utifrån kända sårbarheter.
25.1.2	Leverantören ska tillhandahålla en logisk eller fysiskt separerad kundmiljö inklusive behörighetskontrollsystem, loggar och lagring för varje kund.
25.1.3	Informationsutbytet är kartlagt, dokumenterat, avtalat och spårbart. Informationen ska skyddas mot förändring och avlyssning vid överföringen.
25.1.4	Leverantören ska följa en överenskommelse med beställaren angående krav för informationsöverföring.
26	**Anskaffning, utveckling och underhåll av system**

26.1	**Obligatoriska krav**
26.1.1	Konfigurationer, inklusive säkerhetskonfigurationer, av hårdvara, programvara, tjänster och nätverk ska fastställas, dokumenteras, implementeras, övervakas och granskas.
26.1.2	Utvecklings- och testsystem skyddas antingen på likvärdigt sätt som produktionssystemet, alternativt innehåller inte konfidentiell eller känslig information.
26.1.3	Riktlinjer för säker systemutveckling för systemet ska finnas dokumenterade och efterlevs.
26.1.4	Leverantören ska ha fastlagda och dokumenterade principer och metoder för utveckling av säkra tjänster och system. Vid utveckling av webbapplikationer eller tillhandahållande av tjänster över publika nätverk ska OWASPs (www.owasp.org) rekommendationer följas.
26.1.5	Leverantören ska ha infört säkerhetsåtgärder som skyddar information i programtjänster på publika nätverk mot obehörig åtkomst och obehörig ändring. Vid utveckling av mobila appar ska OWASP Mobile App Security Checklist följas.
26.1.6	Leverantören ska ha riktlinjer för systemförändringar som avser informationssäkerhet inom sina utvecklingsprocesser. Vid större ändringar ska leverantören identifiera och hantera risker som säkerställer att säkerhetskraven i system eller tjänster är uppfyllda.
26.1.7	Leverantören ska ha rutiner för att granska och testa tillgänglighet och säkerhet efter ändringar i verksamhetskritiska driftsplattformar.
26.1.8	Leverantören ska övervaka och styra systemutveckling som är utlagd till en underleverantör.
27	**Leverantörsrelationer**
27.1	**Obligatoriska krav**
27.1.1	Leverantören ska följa beställarens rutiner och processer för åtkomst till organisationens tillgångar.
28	**Personalsäkerhet**
28.1	**Obligatoriska krav**
28.1.1	Ansvar och skyldigheter för informationssäkerhet som fortsätter att gälla efter att en anställning upphör eller ändras ska definieras, tillämpas och kommuniceras till relevant personal och andra intressenter.
28.1.2	Leverantören ska ha processer och rutiner på plats för relevant bakgrundskontroll av personal.
28.1.3	Leverantören ska ha avtal om tystnadsplikt med sina anställda. Tystnadsplikten ska omfatta information om leverantörens kunder. Via avtal ska leverantören även säkerställa tystnadsplikt för underleverantörer. Detta krävs dock inte om dessa redan omfattas av en straffsanktionerad tystnadsplikt som följer av lag.
28.1.4	Leverantören ska för sin personal varje halvår genomföra utbildningar för ökad medvetenhet kring informationssäkerhet samt hålla sig uppdaterad kring beställarens policys, regler och rutiner.
28.1.5	Leverantören ska ha en tydlig och disciplinär process med åtgärder för anställda som har brutit mot informationssäkerhetsregler.
29	**Styrning av åtkomst**
29.1	**Obligatoriska krav**
29.1.1	Leverantören ska tillse att information, tjänster och system har funktioner för att kunna kravställa autentiseringsinformation (pinkod, lösenord etc.) vad gäller komplexitet, längd och livslängd. Se DIGGs vägledning för **tillitsnivå 2** för detaljer.
29.1.2	Leverantören ska tillse att källkod framtagen i egen utveckling skyddas från obehöriga förändringar. Källkod ska deponeras på ett sådant sätt att beställaren garanteras tillgång om leverantören inte uppfyller sina avtalade förpliktelser.
29.1.3	Leverantören ska granska sina användares åtkomsträttigheter halvårsvis, Obehöriga eller användare som inte längre behöver åtkomst ska tas bort. Förändringar av åtkomsträttigheter ska dokumenteras av Leverantören och ska vid begäran tilldelas till beställaren.
29.1.4	Leverantören ska ha en rutin för att permanent ta bort användaridentiteter från information, tjänster, och system, vid avslutande av anställning, avtal eller uppdrag. Kontroll av efterlevnad ska ske årligen.
29.1.5	Leverantören ska ha en formell och dokumenterad process för hur användaridentiteter hanteras (registrering och avregistrering). Leverantören ska säkerställa att användaridentiteterna hos leverantör och beställare är personliga och unika över tid. Se tillitsramverket (ELN0700) **tillitsnivå 2** för detaljer.
29.1.6	Leverantören ska följa en överenskommelse för användaråtkomst till beställarens system, tjänster och information. Endast behöriga och enligt överenskommelsen godkända individer ska inneha åtkomst.

	Hanteringen ska vara spårbar och redovisas för beställaren enligt överenskommelse, minst årligen. Överenskommelsen är en del av regionens PUB-avtal.
29.1.7	Leverantören ska använda särskilda personliga användaridentiteter för systemadministration. Dessa konton ska vara spårbara och lätta att skilja från vanliga användare. Leverantören ska ha särskilda säkerhetsåtgärder kopplade till systemadministration (Exempelvis tidsbegränsade behörigheter eller striktare autentisering).
29.1.8	Leverantören ska ha systemfunktioner för att begränsa åtkomst till information. Behörigheterna ska tilldelas enligt principen där minsta möjliga behörighet tilldelas utifrån en användares roll och arbetsuppgifter. Detta gäller även konton som används vid kommunikation mellan systemkomponenter samt priviligierade konton. Endast information eller tjänster som ska vara publika ska kunna nås i system utan godkänd autentisering.
29.1.9	Leverantören ska tillse att autentiseringen till beställarens information, tjänster och system ska vara flerfaktorsbaserad i enlighet med kraven som följer av ELN0700. Endast utfärdare godkända av E legitimationsnämnden (minst nivå 3) eller anslutna inom eIDAS (minst nivå substantiell) rekommenderas. Se DIGGs vägledning för **tillitsnivå 2** för detaljer.
29.1.10	Leverantören ska på ett säkert sätt distribuera, lagra och återställa autentiseringsinformation (exempelvis lösenord) utan att det kan röjas till obehöriga. Autentiseringsinformation får ej lagras i klartext (gäller även systemkonton i källkod). Se DIGGs vägledning för **tillitsnivå 2** för detaljer.
29.1.11	Leverantören ska för sin personal ha fastställda regler för hur autentiseringsinformation ska skyddas och hanteras.
29.1.12	Leverantören ska skydda och tillse att det finns spårbarhet i de verktyg som avses för underhåll och säkerhetskonfiguration för information, tjänster och system.
30	**Kryptering**
30.1	**Obligatoriska krav**
30.1.1	Leverantören ska ha rutiner för kryptering där val av algoritmer, protokoll och nyckellängder samt hantering av krypteringsnycklar framgår och är följsam mot godkänd grön nivå i Ineras Riv-tekniska anvisningar om kryptering https://rivta.se/documents/ARK_0036/Anvisning_kryptering_v3.3.pdf
30.1.2	Vid överföring av den krypterade eller pseudonymiserade informationen till tredjeland ska krypteringsnyckeln/översättningstabellen stanna kvar hos huvudleverantören och får ej delges underleverantören.
31	**Fysisk och miljörelaterad säkerhet**
31.1	**Obligatoriska krav**
31.1.1	Leverantören ska ha rutiner som säkerställer att endast behörig personal har fysisk åtkomst till områden med konfidentiell information, exempelvis en datahall.
31.1.2	Leverantören ska tillse att fysiska avgränsningar är definierade och tillämpade för skydd av områden med känslig eller kritisk information. Om det avser en datahall eller motsvarande ska leverantören tillse att den uppfyller minst skyddsnivå 3 ("datahall" enligt MSB "Vägledning för fysisk informationssäkerhet i IT-utrymmen") eller likvärdigt.
32	**Hantering av informationssäkerhetsincidenter**
32.1	**Obligatoriska krav**
32.1.1	Leverantören ska bedöma och besluta ifall en informationssäkerhetshändelse ska klassas som en informationssäkerhetsincident. Om händelsen i någon mån påverkar beställaren så ska beställaren inkluderas i detta beslut.
32.1.2	Leverantören ska ha dokumenterade rutiner för övervakning, upptäckt, analys, rapportering, eskalering, hantering av säkerhetshändelser och säkerhetsincidenter. Om incidenten i någon mån påverkar beställaren så ska beställaren inkluderas i dessa rutiner.
33	**Efterlevnad**
33.1	**Obligatoriska krav**
33.1.1	Leverantören ska löpande och i samråd med beställaren arbeta för att leveransen i alla lägen följer de aktuella lagar, förordningar, regler och föreskrifter som ställs på beställarens verksamhet.
33.1.2	Leverantören ska utveckla och införa regler för skydd av personuppgifter med stöd i lagar och förordningar. Dessa regler ska kommuniceras till medarbetare hos leverantören som berörs av leveransen som hanterar personuppgifter.

33.1.3	Beställaren ska i samråd med leverantören ha rätt att genomföra säkerhetsrevisioner av ingående delar i leveransen.
33.1.4	Leverantören ska begära tillstånd innan information i system (texter, bilder, mätdata etc.) eller tjänster återanvänds i andra sammanhang.
34	**Dataskydd**
34.1	**Obligatoriska krav**
34.1.1	Personuppgiftshanteringen ska vara förenlig med gällande europeisk dataskyddslagstiftning; med kompletterande nationell lagstiftning inom Sverige, såsom exempelvis lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och, i förekommande fall, patientdatalag (2008:355), myndigheters föreskrifter (t ex HSLF-FS 2016:40) samt den domstolspraxis som utarbetats på området.
34.1.2	Leverantören ska säkerställa att personuppgifter endast behandlas inom EU/EES eller i länder som EU-kommissionen anser ha en adekvat skyddsnivå.
34.1.3	Om leverantören behandlar personuppgifter i USA ska berörda parter vara anslutna till EU-US Data Privacy Framework.
34.1.4	Om personuppgifter överförs till tredjeland ska hanteringen följa EDPBs och IMYs aktuella rekommendationer, inklusive standardklausuler och kompletterande skyddsåtgärder såsom kryptering eller pseudonymisering. Om leverantören tillämpar bindande företagsbestämmelser för tredjelandsöverföring godkända av IMY, ska detta anges och styrkas.
34.1.5	Leverantören ska tydligt ange i vilka länder regionens personuppgifter, inklusive psedunymiserade personuppgifter, kan hanteras eller lagras. Även vid tillfälliga driftstopp hos leverantören eller dess underleverantörer.
34.1.6	Leverantören ska redogöra för ägarförhållanden och juridisk hemvist för alla parter i leveransen, inklusive konsortiemedlemmar, underleverantörer och deras eventuella koncernmödrar.
34.1.7	Det ska vara möjligt att genom pseudonymisering eller på annat sätt undvika att föra in sekretessmarkerade eller skyddade personuppgifter i systemet, utan att behandlingen av patienten försämras.
34.1.8	Anbudsgivarens ägarförhållanden och affärsverksamhet ska vara förenliga med den svenska statliga värdegrunden.

Intyg

På denna sida visas namnen på den eller de personer som har skrivit under dokumentet digitalt samt tidpunkten då underskriften gjordes. Komplett information om vem som har skrivit under finns i underskriftscertifikaten, som kan ses med hjälp av t ex Acrobat Reader.
En digitalunderskrift är juridiskt lika giltig som en underskrift gjord med penna och papper. För mer information om digitala signaturer hos Inera, se www.inera.se

E-underskrifter

Detta dokument är underskrivet med en eller flera elektroniska underskrifter från Ineras Underskriftstjänst på uppdrag av nedanstående fysiska person eller personer

Undertecknat av:
Magnus Loman
2026-03-24 14:31:25

Undertecknat av:
Sebastianus Henricus Petrus Mommers
2026-03-25 09:13:29