



PERSONUPPGIFTSBITRÄDESAVTAL

Avtal enligt artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679¹

1. PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER

Personuppgiftsansvarig	Personuppgiftsbiträde
Region Västmanland	Abbott Diabetes Care, Inc.
Organisationsnummer	Organisationsnummer
232100-0172	2322426
Postadress	Postadress
Regionhuset, 721 89 Västerås	1420 Harbor Bay Parkway, Alameda, CA 94502, U.S.A.
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: Örjan Lehnberg E-post: orjan.lehnberg@abbott.com Tfn: +46 76 142 38 91
Kontaktperson för parternas samarbete om dataskydd	Kontaktpersoner för parternas samarbete om dataskydd
Namn: Agata Cierzniak E-post: dataskyddsombudet@regionvastmanland.se	EU-DPO@abbott.com
Personuppgiftsbiträdesavtal gäller för följande affärsavtal	
Libre View – VF2023-00039-06	

2. DEFINITIONER

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, framtagnings, 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 all annan eventuell lagstiftning (inklusive 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 Personuppgiftsbitrådets Behandling av Personuppgifter åt den Personuppgiftsansvarige. PUB-avtalets syfte är att säkerställa den Registrerades fri- och rättigheter vid Behandlingen, i enlighet med vad 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 punkterna 1, 16, 17, 18.2, 19–22 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 Personuppgiftsbitrådet att utföra Behandlingen för den Personuppgiftsansvariges räkning enligt vad som stadgas i detta PUB-avtal.

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

4.3. Personuppgiftsbitrådet 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 så att Personuppgiftsbitrådet 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 Personuppgiftsbitrådet om förändringar i Behandlingen vilka påverkar Personuppgiftsbitrådets 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 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.

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 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 punkten 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 väntas påverka Behandlingen, ska Personuppgiftsbiträdet skriftligt informera den Personuppgiftsansvarige om detta i enlighet med vad stadgas om meddelanden i punkten 19 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.

Beskrivningen ska redogöra för:

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

11.4 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 förteckning över Underbiträden.

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

12.3 Personuppgiftsbiträdet ansvarar fullt ut för Underbitrådets Behandling gentemot den Personuppgiftsansvarige.

12.4 Personuppgiftsbiträdet äger rätt att anlita nya underbiträden och ersätta befintliga underbiträden.

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

1. Underbitrådets namn, organisationsnummer och säte (adress och land),
2. vilken typ av uppgifter och kategorier av Registrerade som behandlas, och
3. var Personuppgifterna ska behandlas.

12.6 Den Personuppgiftsansvarige äger rätt att inom trettio (30) dagar från dag för meddelande enligt punkten 12.5 invända mot Personuppgiftsbitrådets anlitan 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 17.4.

12.7 När Personuppgiftsbiträdet upphör med att anlita Underbiträdet ska Personuppgiftsbiträdet skriftligen meddela den Personuppgiftsansvarige om att det upphör med att anlita Underbiträdet.

12.8 Personuppgiftsbiträdet ska på den Personuppgiftsansvariges begäran översända en kopia av det avtal som reglerar Behandling av Underbitrådets Behandling av Personuppgifter enligt punkten 12.2.

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 omedelbart informera motparten om förhållandet och aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.

14.4 Oaktat vad 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. LAGVAL OCH TVISTLÖSNING

15.1 För detta avtal gäller svensk rätt. Eventuell tolkning eller tvist i anledning av PUB-avtalet, som parterna inte kan lösa på egen hand, ska avgöras av svensk allmän domstol.

16. PUB-AVTALETS TECKNANDE, AVTALSTID OCH UPPSÄGNING

16.1 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.

17. ÄNDRINGAR OCH UPPSÄGNING MED OMEDELBAR VERKAN M.M.

17.1 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.

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

17.3 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.

17.4 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.

18. ÅTGÄRDER VID PUB-AVTALETS UPPHÖRANDE

18.1 Vid uppsägning av PUB-avtalet ska den Personuppgiftsansvarige utan onödigt dröjsmål begära att Personuppgiftsbitrådet överlämnar samtliga Personuppgifter till den Personuppgiftsansvarige eller raderar dem, enligt dennes önskemål. Om Personuppgifterna överlämnas ska det ske i ett öppet och standardiserat format. Med samtliga Personuppgifter avses alla Personuppgifter vilka har omfattats av Behandlingen samt annan tillhörande information såsom Loggar, Instruktioner, systemlösningar, beskrivningar och andra handlingar som Personuppgiftsbitrådet erhållit genom informationsutbyte enligt PUB-avtalet.

18.2 Överlämning och radering enligt PUB-avtalet, punkten 18.1, ska vara utförda senast trettio (30) dagar räknat från den tidpunkt uppsägning gjorts enligt detta PUB-avtal, punkten 16.1.

18.3 Behandling som utförs av Personuppgiftsbitrådet efter den tidpunkt som stadgas i punkten 18.2 är att betrakta som en otillåten Behandling.

18.4 Bestämmelser om sekretess/tystnadsplikt i punkten 8 enligt detta PUB-avtal ska fortsätta gälla även om PUB-avtalet i övrigt upphör av gälla.

19. MEDDELANDEN INOM RAMEN FÖR DETTA PUB-AVTAL OCH INSTRUKTIONER

19.1 Meddelanden om PUB-avtalet och dess administration inklusive uppsägning ska skickas till respektive parts kontaktperson för PUB-avtalet.

19.2 Meddelanden om parternas samarbete om dataskydd, gällande Behandlingen, ska skickas till respektive parts kontaktperson för parternas samarbete om dataskydd.

19.3 Meddelanden inom ramen för PUB-avtalet och Instruktioner ska skickas skriftligt. Ett meddelande ska anses ha kommit fram till mottagaren senast en (1) arbetsdag efter att meddelandet har skickats.

20. KONTAKTPERSONER

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

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

21. ANSVAR FÖR UPPGIFTER OM PARTERNA OCH KONTAKTPERSONER SAMT KONTAKTUPPGIFTER

21.1 Varje part ansvarar för att de uppgifter som anges i punkten 1 i PUB-avtalet alltid är aktuella. Ändring av uppgifter i punkten 1 ska meddelas skriftligen enligt punkten 19.1 i PUB-avtalet.

22. PARTERNAS UNDERTECKNANDEN AV PUB-AVTALET

22.1 Detta PUB-avtal tillhandahålls antingen i digitalt format för elektroniskt tecknande eller i pappersformat för tecknande med penna. Om PUB-avtalet tillhandahålls i digitalt format utgår punkter 22.2–22.3.

22.2 Den Personuppgiftsansvariges undertecknande av PUB-avtalet

Ort	Datum
Västerås	2024-11-26

.....

Undertecknande



.....

Namnförtydligande

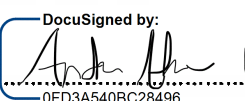
Magnus Loman
Verksamhetschef Hjälpmedelscentrum

22.3 Personuppgiftsbiträdets undertecknande av PUB-avtalet

Ort	Datum
Stockholm	2024-11-26

.....

Undertecknande

DocuSigned by:

0FD3A540BC28496...

.....

Namnförtydligande

Andreas Almroth
General Manager Nordic, Abbott Diabetes Care



AVTALSBILAGA 1

PERSONUPPGIFTSANSVARIGES INSTRUKTION FÖR BEHANDLING AV PERSONUPPGIFTER

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

1. Ändamål, föremålet och arten

Ändamålet är att tillhandahålla god, patientsäker och effektiv diabetesvård till användare enligt Socialstyrelsens nationella riktlinje för Diabetesvård.

- Möjliggöra för patienter att bedriva god egenvård.
- Möjliggöra för vårdpersonalen att vägleda och utbilda patienterna för egenvård.
- Leverantör ska ge teknisk support för de diabetestekniska produkter som leverantören tillhandahåller för den personuppgiftsansvarige.

Personuppgiftsbiträdet ska behandla personuppgifter för följande ändamål

- För att göra det möjligt att tillhandahålla Tjänsterna enligt beskrivningen i Huvudavtalet, inklusive:
 - För patienter: Behandling av relevanta personuppgifter om den registrerade och att göra dessa uppgifter fjärråtkomliga för personer som har fått behörighet av Personuppgiftsansvarige.
 - För vårdpersonal: Behandling av relevanta personuppgifter om den registrerade inom ramen för användningen av produkterna och Tjänsterna.
- Säkerställa att Tjänsterna samt produkter, teknik och infrastruktur som krävs för att tillhandahålla dessa fungerar korrekt, bland annat genom regelbundet underhåll, incidentrespons, felsökning och teknisk support för Personuppgiftsansvarige och de registrerade, inklusive patienter.
- Utvärdering av prestanda och användning av Tjänsterna samt utrustning, teknik och infrastruktur som krävs för deras tillhandahållande samt av produkterna, bland annat identifiera områden för förbättring som kan bidra till Tjänsternas, produkternas och patientbehandlingarnas säkerhet och kvalitet, inklusive, men inte begränsat till:
 - Skapa och utvärdera aggregerade data avseende produktinställningar, produktprestanda och kliniska data för produkterna, möjlighet till proaktiv optimering av utbildning och information till vårdpersonal med fokus på optimal patientbehandling.
 - Skapa och utvärdera aggregerade data erhållna från incidentrespons, felsökning och teknisk support för Personuppgiftsansvarige och patienterna för att förbättra Tjänsterna och relaterad utbildning för Personuppgiftsansvarige och patienterna.
 - Skapa och utvärdera data avseende överföringar för att proaktivt kunna optimera utbildning och information för Personuppgiftsansvarige och patienterna.
- Utvärdera, analysera och rapportera om insamlade personuppgifter på begäran av Personuppgiftsansvarig.
- Vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå för Behandlade Personuppgifter, vilket kan inkludera pseudonymisering, anonymisering och kryptering.

- Efterkomma rimliga begäranden från behörig brottsbekämpande personal eller representanter, rättsliga myndigheter, offentliga myndigheter eller organ, inklusive behöriga dataskyddsmyndigheter, varvid behandlingen begränsas till miniminivån för att uppfylla begäran. Personuppgiftsbiträde kommer i vilket fall att underrätta Personuppgiftsansvarig om en sådan begäran, förutom om förhandsanmälan inte är tillåten på grund av skyldighet till sekretess som åläggs Personuppgiftsbiträdet enligt tillämplig lag eller av begärande person, representant, myndighet eller organ.

Behandlingens föremål är Personuppgifter som Personuppgiftsbiträdet behandlar för den Personuppgiftsansvariges räkning i samband med fullgörandet av Huvudavtalet (Terms of Use för LibreView om leverans av LibreView-systemet).

Behandlingen av Personuppgifter sker i syfte att:

Tillhandahålla och leverera tjänsten till den Personuppgiftsansvarige och fullgöra åtaganden enligt Huvudavtalet

- Ge support till användare, superanvändare och administratörer
- Administrera och förvalta molntjänsten
- Genomföra tekniskt underhåll och säkerhetskrav

Arten och syftet med Abbotts behandling av personuppgifter härstammar från LibreView-avtalets syfte, vilket är att tillhandahålla LibreView-systemet som beskrivs i Terms of Use. Behandlingen av Personuppgifter sker i samband med att Personuppgiftsbiträdet tillhandahåller en webbaserad tjänst för Glukosövervakning på den Personuppgiftsansvariges uppdrag. Behandlingen av Personuppgifter sker även i samband med att Personuppgiftsbiträdet ger support avseende tjänsten till den Personuppgiftsansvariges medarbetare. Behandlingen av Personuppgifter sker delvis automatiserat och helt automatiserat.

2. Behandlingen omfattar följande typer av Personuppgifter

Patientens personuppgifter:

Förnamn, efternamn, postadress, e-postadress, telefonnummer, födelsedata, patientdata, apparatdata och hälsodata.

Patientens Indirekta personuppgifter: typ av behandling/diagnos.

Personuppgiftsansvariges anställdas personuppgifter:

Förnamn, efternamn, e-postadress, telefonnummer, inloggningsuppgifter och arbetsplatsadress.

Anställdas indirekta personuppgifter: befattning.

3. Behandlingen omfattar kategorier av Registrerade

Personuppgifter i systemet utgörs av:

- Patienter
- Personuppgiftsansvariges anställda
- Vårdnadshavare, god man, anhörig eller annat ombud

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

I samband med supportärenden/uppföljningsärenden ska leverantören ge support till uppringaren som kan bekräfta utrustningens serienummer utan att efterfråga namn eller födelsedata.

Personuppgiftsbiträdet bör på Personuppgiftsansvariges begäran exportera patientdata i standardiserat filformat till en mottagare som Personuppgiftsansvarige utser.

5. Ange särskilda tekniska och organisatoriska säkerhetsåtgärder vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet/biträdena

Personuppgiftsbiträdet ska säkerställa att personuppgifter behandlas enbart i enlighet med Personuppgiftsansvariges instruktioner (anvisningskontroll).

Ledningssystem:

Personuppgiftsbiträdet ska ha ett ledningssystem för informationssäkerhet.

Fysisk åtkomstkontroll:

Personuppgiftsbiträdet ska vidta tekniska och organisatoriska åtgärder som förhindrar obehörigt tillträde och skadlig inverkan på personuppgifter och system där personuppgifter behandlas. Personuppgiftsbärande system ska skyddas mot elavbrott och andra störningar orsakade i tekniska försörjningssystem. Utrymmen där personuppgifter förvaras, så som serverhallar, ska skyddas genom lämpliga tillträdeskontroller för att säkerställa att endast behörig personal får tillträde. Det ska också finnas ett tillfredställande skydd mot stöld och händelser som kan förstöra IT-system och lagringsmedia. När datorutrustning och löstagbara datamedier hos PUB inte står under uppsikt ska utrustningen och medierna låsas in för att skyddas mot obehörig användning, påverkan och stöld. I annat fall ska personuppgifterna krypteras.

Logisk åtkomst:

Personuppgiftsbiträdet ska ha en effektiv behörighetsstyrning. Personal med behörighet till personuppgiftsansvariges personuppgifter ska vara dokumenterade.

Personuppgiftsbiträdet ska säkerställa att personer som har rätt att använda system för behandling av personuppgifter får åtkomst till sådana personuppgifter endast i den utsträckning de har rätt till, i enlighet med sina åtkomsträttigheter, och att det under behandlingen eller användningen och efter lagringen inte går att läsa, kopiera, ändra eller radera personuppgifter utan behörighet (kontroll av dataåtkomst).

Autentisering/Identifiering:

Personuppgiftsbiträdet ska se till att endast behörig personal kan komma åt personuppgifterna genom att skydda personuppgifterna med rätt identifiering. Personalen ska instrueras att hantera och förvara användaridentitet och lösenord med försiktighet och att använda lösenord som inte har anknytning till person eller på annat sätt som med lätthet kan forceras. Personuppgiftsbiträdet ska ha en överenskommen lösenordspolicy med den personuppgiftsansvarige som gäller för patienter. Inloggning all personal sker också med stark autentisering. Personalen ska logga ut från sina respektive klientdatorer när de inte används.

Behörighetsstyrning: Ett tekniskt system för behörighetskontroll ska styra åtkomsten till personuppgifterna för PUB. Behörigheten ska begränsas till dem som behöver uppgifterna för sitt arbete. Användaridentitet och lösenord ska vara personliga och får inte överlåtas på någon annan. Det ska finnas rutiner för tilldelning och borttagande av behörigheter.

Risk- och incidenthantering:

Personuppgiftsbiträdet ska ha ett arbetssätt som upptäcker och identifierar incidenter samt förankrade rutiner för incidentrapportering inom organisationen och till personuppgiftsansvarig. Personuppgiftsbiträdet ska ha ett etablerat arbetssätt för riskhanteringar.

Tidsfrister för radering:

Personuppgiftsbiträdet ska på begäran av personuppgiftsansvarige och/eller 6 månader efter avslutat konto radera samtliga personuppgifter och tillhörande kontouppgifter. Utrustningens diagnostikdata kan sparas av Personuppgiftsbiträdet efter att samtliga personuppgifter är avidentifierade.

Kryptering i samband med dataöverföring:

I samband med att beställning sker via en webbsida, kunddatabas och/eller övrigt informationssystem som lagrar Personuppgiftsansvariges patientuppgifter ska personuppgifterna vara krypterade.

I samband med att det sker en dataöverföring mellan applikationer och analysverktyg ska personuppgifterna vara krypterade.

Krypteringsprotokoll ska vara standardiserad enligt TLS 1.3/AES256 eller motsvarande.

Kryptering av fil:

För det fall eventuella bärbara datorer används vid behandlingen ska personuppgifterna på fasta och löstagbara lagringsmedier alltid vara krypterade.

Separering och segmentering av data:

Personuppgiftsbiträdet ska separera och segmentera Personuppgiftsansvariges personuppgifter från övriga kunders personuppgifter.

Driftsäkerhet och tekniskt underhåll:

Personuppgiftsbiträdet ska upprätthålla driftsäkerhet och tekniskt underhåll för att tillhandahålla den tjänst och utrustning som den personuppgiftsansvarige använder. Personuppgiftsbiträdet ska säkerställa att personuppgifter skyddas mot oavsiktlig förstöring eller förlust samt säkerställa säkerhetskopiering och kontinuitet (tillgänglighetskontroll). Leverantören ska ha en inbyggd funktion för automatisk utloggning efter 15 minuters inaktivitet.

Skadlig kod:

Personuppgiftsbärande system ska vara skyddade mot virus, trojaner och andra former av digitala intrång.

Datakommunikation:

PUB ska se till att PUB:s informationssystem är skyddade från extern åtkomst genom exempelvis perimeterskydd och kontroll av fjärråtkomst vid extern access.

Insynsskydd ska tillföras transport och lagring när behovet finns.

Personuppgiftsbiträdets åtkomst till personuppgifter via fjärrstyrd datakommunikation: Service och support via fjärrstyrd datakommunikation får endast ske efter säker elektronisk identifiering av den som utför servicen. Servicepersonal ska ges åtkomst i systemet endast vid servicetillfället. Finns separat kommunikationsingång för service ska den vara stängd när service inte pågår.

Säkerhetskopiering: Personuppgiftsbiträdet ska regelbundet säkerhetskopiera den personuppgiftsansvariges personuppgifter med tillhörande data minst 1 gång per dygn. Säkerhetskopieringen ska lagras fysiskt åtskilt från produktionsdata, inte vara beroende av samma it-komponenter och vara väl skyddade så att personuppgifterna kan återläsas efter en störning samt vara geografisk separerad. Personuppgiftsbiträdet ska ha en rutin för test av återläsning.

Stark autentisering: Åtkomst till känsliga personuppgifter ska föregås av stark autentisering.

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

Personuppgiftsbiträdet ska ansvara för att:

1. det av dokumentationen av åtkomsten (loggar) framgår vilka åtgärder som har vidtagits med uppgifter om en patient,
2. det av loggarna framgår vid vilken organisatoriska enhet åtgärderna vidtagits,
3. det av loggarna framgår vid vilken tidpunkt åtgärderna vidtagits,
4. användarens och patientens identitet framgår av loggarna,
5. systematiska och återkommande stickprovskontroller av loggarna görs,
6. kontroller av loggarna dokumenteras, och
7. loggarna sparas minst fem år för att möjliggöra kontroll av åtkomsten till uppgifter om en patient

Loggarna ska delges den Personuppgiftsansvarige på begäran.

7. Lokalisering och överföring av Personuppgifter till Tredje land

Inga tredjelandsöverföringar ska förekomma, vid de fall där det är absolut nödvändigt för att kunna utföra support ska det särskilt överenskommas med personuppgiftsansvarig och ett av nedanstående kriterier måste uppfyllas, dokumenteras och godkännas.

- Leverantören ska ha ett av Integritetsskyddsmyndigheten eller annan tillsynsmyndighet inom EU godkänt BCR (Binding corporate rules)
- Om leverantören är registrerad och lokaliserad i ett land som EU-kommissionen godkänt som ett land med adekvata skyddsnivå ska SCC (Standard contractual clauses som är framtagna av EU-kommissionen) tecknas med samtliga biträden i tredjeland där det är relevant. EU SCC läggs till som bilaga till avtalet och börjar gälla om Data Privacy Framework skulle ogiltigförklaras.

- Tredjelsöverföring som uppkommer i samband med nyttjande av underbiträde ska biträdet tillse att lämpliga skyddsåtgärder vidtas enligt artikel 46 allmänna dataskyddsförordningen och enligt EDPBs riktlinjer om säkerhetsåtgärder.
- Tredjelsöverföring till USA som av EU-kommissionen har bedömts ha adekvat skyddsnivå enligt artikel 45 ska vara anslutna och certifierade mot Data Privacy Framework, personuppgiftsbiträde och personuppgiftsunderbiträden ska uppvisa certifieringsdokumenten.

8. Övriga Instruktioner angående Behandling av Personuppgifter som utförs av biträdet/biträdena

- *I samband med personuppgiftsincidenter ska Personuppgiftsbiträdet rapportera incident utan onödigt dröjsmål från att incidenten upptäckts till kontaktperson för detta personuppgiftsbiträdesavtal och Region Västmanlands dataskyddsombud, dataskyddsombud@regionvastmanland.se*
- Vid utökning eller införande med behandling av ny eller innovativ teknik så som AI funktionalitet eller annan liknande automatiserad teknik/funktion skall detta regleras genom separat instruktion som särskilt beaktar den nya AI förordningen (AI- Act) samt godkännas av personuppgiftsansvarig innan personuppgiftsbehandlingen får påbörjas.
- När nya/uppdaterade funktioner lanseras i molntjänsten ska följande göras:
 - Följa upp säkerhetskrav
 - Funktionstester så att inga fel hittas i programmet vid driftsättning
 - Produktionsdata är inte tillåtet att använda under testning
 - Uppdatering av operativa dokument och användardokument. Detta görs innan ett säkerhetsgodkännande kan ges och driften kan påbörjas.

Interna säkerhetsgranskningar måste göras periodvis dock minst en gång om året. Interna aktiviteter som förbättrar säkerheten och omständigheterna kring informationen måste göras kontinuerligt och omfattande.

Anlitande av personuppgiftsunderbiträde enligt Personuppgiftsbiträdesavtal 12.6 ska informera kontaktperson för detta personuppgiftsbiträdesavtal och Region Västmanlands dataskyddsombud.

**AVTALSBILAGA A - STANDARDAVTALSCLAUSULER****AVSNITT I*****Klausul 1*****Syfte och tillämpningsområde**

- a) Syftet med dessa standardavtalsklausuler är att säkerställa överensstämmelse med kraven i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän dataskyddsförordning)² vid överföring av personuppgifter till ett tredjeland.
- b) Parterna:
- i) den eller de fysiska eller juridiska personer, den eller de offentliga myndigheter, den eller de byråer eller andra organ (enheterna) som överför personuppgifter enligt förteckningen i bilaga I.A. (uppgiftsutföraren), och
 - ii) den eller de enheter i ett tredjeland som tar emot personuppgifter från uppgiftsutföraren, direkt eller indirekt via en annan enhet som också är part i dessa klausuler, enligt förteckningen i bilaga I.A. (uppgiftsinföraren)

har kommit överens om dessa standardavtalsklausuler (klausulerna).

- c) Dessa klausuler är tillämpliga med avseende på överföring av personuppgifter enligt vad som anges i bilaga I.B.
- d) Det tillägg till dessa klausuler som innehåller de bilagor som det hänvisas till utgör en integrerad del av dessa klausuler.

Klausul 2**Klausulernas verkan och beständighet**

- a) Genom dessa klausuler fastställs lämpliga skyddsåtgärder, däribland verkställbara rättigheter och effektiva rättsmedel för de registrerade enligt artikel 46.1 och artikel 46.2 c i förordning (EU) 2016/679 och, när det gäller överföring av personuppgifter från personuppgiftsansvariga till personuppgiftsbiträden och/eller från personuppgiftsbiträden till personuppgiftsbiträden, standardavtalsklausuler enligt artikel 28.7 i förordning (EU) 2016/679, under förutsättning att de inte ändras, förutom för att välja en eller flera lämpliga moduler eller lägga till eller uppdatera informationen i tillägget. Detta hindrar inte parterna från att inbegripa de standardavtalsklausuler som fastställs i dessa klausuler i ett mer övergripande avtal och/eller att lägga till andra klausuler eller ytterligare skyddsåtgärder, under förutsättning att de inte direkt eller indirekt står i strid med dessa klausuler eller påverkar de registrerades grundläggande rättigheter eller friheter.

² Om uppgiftsutföraren är ett personuppgiftsbiträde som omfattas av förordning (EU) 2016/679 och som agerar på uppdrag av en unionsinstitution eller ett unionsorgan som personuppgiftsansvarig, säkerställer användningen av dessa klausuler vid anlåtande av ett annat personuppgiftsbiträde (som underentreprenör) som inte omfattas av förordning (EU) 2016/679 även överensstämmelse med artikel 29.4 i Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39), i den utsträckning som dessa klausuler och de skyldigheter i fråga om uppgiftsskydd som fastställs i avtalet eller en annan rättsakt mellan den personuppgiftsansvarige och personuppgiftsbiträdet i enlighet med artikel 29.3 i förordning (EU) 2018/1725 har samordnats. Detta kommer särskilt att vara fallet om den personuppgiftsansvarige och personuppgiftsbiträdet använder de standardavtalsklausuler som ingår i beslut 2021/915.

- b) Dessa klausuler påverkar inte de skyldigheter som uppgiftsutföraren omfattas av med stöd av förordning (EU) 2016/679.

Klausul 3

Berättigade tredje parter

- a) Registrerade personer får åberopa och verkställa dessa klausuler, i egenskap av berättigade tredje parter, gentemot uppgiftsutföraren och/eller uppgiftsinföraren, med följande undantag:
- i) Klausul 1, klausul 2, klausul 3, klausul 6, klausul 7;
 - ii) Klausul 8 – modul två: Klausul 8.1(b), 8.9(a), (c), (d) och (e);
modul tre: Klausul 8.1(a), (c) och (d) och klausul 8.9(a), (c), (d),
(e), (f) och (g);
 - iii) Klausul 9 – modul två: Klausul 9(a), (c), (d) och (e);
modul tre: klausul 9(a), (c), (d) och (e);
 - iv) Klausul 12 – klausul 12 a, d och f;
 - v) Klausul 13,
 - vi) Klausul 15.1 c, d och e;
 - vii) Klausul 16 e;
 - viii) Klausul 18 – modulerna ett, två och tre:
Klausul 18(a) och (b).
- b) Led a påverkar inte de registrerades rättigheter enligt förordning (EU) 2016/679.

Klausul 4

Tolkning

- a) Om begrepp som definieras i förordning (EU) 2016/679 används i dessa klausuler ska begreppen ha samma betydelse som i den förordningen.
- b) Dessa klausuler ska läsas och tolkas mot bakgrund av bestämmelserna i förordning (EU) 2016/679.
- c) Dessa klausuler ska inte tolkas på ett sätt som står i strid med de rättigheter och skyldigheter som föreskrivs i förordning (EU) 2016/679.

Klausul 5

Hierarki

Om en konflikt uppstår mellan dessa klausuler och bestämmelserna i de överenskommelser mellan parterna som gäller vid den tidpunkt då dessa klausuler överenskoms eller därefter träder i kraft, ska dessa klausuler ha företräde.

Klausul 6

Beskrivning av överföringen eller överföringarna

Närmare uppgifter om överföringen eller överföringarna, och i synnerhet de kategorier av personuppgifter som överförs och det eller de ändamål för vilka de överförs, anges i bilaga I.B.

Klausul 7

Ej tillämplig

AVSNITT II – PARTERNAS SKYLDIGHETER

Klausul 8

Skyddsåtgärder för uppgifter

Uppgiftsutföraren garanterar att han eller hon har gjort rimliga ansträngningar för att se till att uppgiftsinföraren, genom genomförandet av lämpliga tekniska och organisatoriska åtgärder, kan fullgöra sina skyldigheter enligt dessa klausuler.

MODUL TVÅ: Överföring från personuppgiftsansvarig till personuppgiftsbiträde

8.1 Instruktioner

- a) Uppgiftsinföraren ska endast behandla personuppgifterna enligt dokumenterade instruktioner från uppgiftsutföraren. Uppgiftsutföraren får ge sådana instruktioner under hela avtalets giltighetstid.
- b) Uppgiftsinföraren ska omedelbart informera uppgiftsutföraren om han eller hon inte kan följa dessa instruktioner.

8.2 Ändamålsbegränsning

Uppgiftsinföraren ska endast behandla personuppgifterna för det eller de specifika ändamålen med överföringen, enligt vad som fastställs i bilaga I.B, såvida inte uppgiftsutföraren har gett andra instruktioner.

8.3 Öppenhet

På begäran ska uppgiftsutföraren tillhandahålla en kopia av dessa klausuler, inklusive tillägget när det har fyllts i av parterna, till den registrerade utan kostnad. I den mån det är nödvändigt för att skydda affärshemligheter eller andra konfidentiella uppgifter, inklusive de åtgärder som beskrivs i bilaga II och personuppgifter, får uppgiftsutföraren redigera delar av texten i tillägget till dessa klausuler innan en kopia tillhandahålls, men han eller hon måste bifoga en meningsfull sammanfattning om den registrerade annars inte skulle kunna förstå dess innehåll eller utöva sina rättigheter. På begäran ska parterna tillhandahålla skälen till redigeringen till den registrerade, i möjligaste mån utan att avslöja de redigerade uppgifterna. Denna klausul påverkar inte uppgiftsutförarens skyldigheter enligt artiklarna 13 och 14 i förordning (EU) 2016/679.

8.4 Korrekthet

Om uppgiftsföraren får kännedom om att de personuppgifter som han eller hon har tagit emot är felaktiga, eller har blivit inaktuella, ska han eller hon informera uppgiftsutföraren utan onödigt dröjsmål. I sådana fall ska uppgiftsföraren samarbeta med uppgiftsutföraren för att radera eller rätta uppgifterna.

8.5 Behandlingens varaktighet och radering eller återlämnande av uppgifter

Uppgiftsförarens behandling ska endast äga rum under den period som anges i bilaga I.B. När tillhandahållandet av behandlingstjänsterna har avslutats ska uppgiftsföraren, enligt uppgiftsutförarens val, radera alla personuppgifter som behandlats på uppdrag av uppgiftsutföraren och intyga för uppgiftsutföraren att detta har skett, eller till uppgiftsutföraren återlämna alla personuppgifter som har behandlats på uppdrag av uppgiftsutföraren och radera befintliga kopior. Till dess att uppgifterna raderats eller återlämnats ska uppgiftsföraren fortsätta att se till att dessa klausuler följs. Om återlämnande eller radering av personuppgifterna är förbjudet enligt lokal lagstiftning som är tillämplig för uppgiftsföraren ska uppgiftsföraren garantera att han eller hon kommer att fortsätta att uppfylla kraven i dessa klausuler och endast kommer att behandla personuppgifterna i den utsträckning och under den tid som krävs enligt den lokala lagstiftningen. Detta påverkar inte klausul 14, i synnerhet kravet enligt klausul 14 e att uppgiftsföraren under hela avtalets giltighetstid ska meddela uppgiftsutföraren om han eller hon har anledning att misstänka att han eller hon är eller har blivit föremål för lagar eller förfaranden som inte stämmer överens med kraven i klausul 14 a.

8.6 Säkerhet vid behandling

- a) Uppgiftsföraren, och under överföring även uppgiftsutföraren, ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa uppgifternas säkerhet, däribland genom skydd mot säkerhetsbrott som skulle leda till oavsiktlig eller olaglig förstöring, förlust, ändring, obehörigt utlämnande eller obehörig åtkomst till uppgifterna (personuppgiftsincident). Vid bedömning av lämplig säkerhetsnivå ska parterna ta vederbörlig hänsyn till de senaste rönen, kostnaderna för genomförandet, behandlingens karaktär, omfattning, sammanhang och ändamål samt riskerna för de registrerade i samband med behandlingen. Parterna ska i synnerhet överväga att använda kryptering eller pseudonymisering, även under överföringen, om ändamålet med behandlingen kan uppfyllas på detta sätt. Vid användning av pseudonymisering ska uppgiftsutföraren om möjligt behålla sin fullständiga kontroll över den ytterligare information som krävs för att knyta personuppgifterna till en viss registrerad. För att fullgöra sina skyldigheter enligt denna punkt ska uppgiftsföraren åtminstone genomföra de tekniska och organisatoriska åtgärder som anges i bilaga II. Uppgiftsföraren ska göra regelbundna kontroller för att säkerställa att dessa åtgärder även fortsättningsvis ger en lämplig säkerhetsnivå.
- b) Uppgiftsföraren ska endast ge sin personal tillgång till personuppgifterna i den utsträckning det är absolut nödvändigt för att genomföra, förvalta och övervaka avtalet. Uppgiftsföraren ska säkerställa att personer som har tillstånd att behandla personuppgifterna har förbundit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.
- c) I händelse av en personuppgiftsincident som gäller uppgifter som har behandlats av uppgiftsföraren enligt dessa klausuler ska uppgiftsföraren vidta lämpliga åtgärder för att hantera incidenten, däribland åtgärder för att mildra dess negativa konsekvenser. Uppgiftsföraren ska även meddela uppgiftsutföraren utan onödigt dröjsmål efter att ha fått kännedom om incidenten. Meddelandet ska innehålla uppgifter om en kontaktpunkt som kan lämna mer information, en beskrivning av incidentens karaktär (inbegripet, om möjligt, vilka kategorier och det ungefärliga antalet registrerade och personuppgiftsregister som berörs), dess sannolika konsekvenser samt vilka åtgärder som har vidtagits eller föreslagits för att hantera incidenten, däribland, i tillämpliga fall, åtgärder för att mildra dess möjliga negativa konsekvenser. Om, och i den mån, det inte är möjligt att tillhandahålla all information vid samma tillfälle ska det inledande meddelandet innehålla den information som då

finns tillgänglig, varefter ytterligare information ska tillhandahållas utan onödigt dröjsmål efterhand som den blir tillgänglig.

- d) Uppgiftsinföraren ska samarbeta med och bistå uppgiftsutföraren så att uppgiftsutföraren kan fullgöra sina skyldigheter enligt förordning (EU) 2016/679, framför allt att meddela den behöriga tillsynsmyndigheten och de berörda registrerade, med beaktande av behandlingens karaktär och den information som finns tillgänglig för uppgiftsinföraren.

8.7 Känsliga uppgifter

Om överföringen inbegriper personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska eller biometriska uppgifter för unik identifiering av en fysisk person, uppgifter om hälsa eller en persons sexualliv eller sexuella läggning, eller uppgifter om brottmålsdomar och lagöverträdelser (känsliga uppgifter) ska uppgiftsinföraren tillämpa de särskilda begränsningar och/eller de ytterligare skyddsåtgärder som beskrivs i bilaga C.

8.8 Vidare överföringar

Uppgiftsinföraren ska endast lämna ut personuppgifter till en tredje part enligt dokumenterade instruktioner från uppgiftsutföraren. Dessutom får uppgifterna endast lämnas ut till en tredje part utanför Europeiska unionen³ (i samma land som uppgiftsinföraren eller i ett annat tredjeland, nedan kallat vidare överföring), om den tredje parten är eller samtycker till att vara bunden av dessa klausuler i motsvarande modul, eller

- i) om den vidare överföringen sker till ett land som omfattas av ett beslut om adekvat skyddsnivå enligt artikel 45 i förordning (EU) 2016/679 som täcker den vidare överföringen,
- ii) om den tredje parten på annat sätt säkerställer lämpliga skyddsåtgärder enligt artikel 46 eller 47 i förordning (EU) 2016/679 med avseende på behandlingen i fråga,
- iii) om den vidare överföringen är nödvändig för att fastställa, göra gällande eller försvara ett rättsligt anspråk i samband med särskilda administrativa, tillsynsrelaterade eller rättsliga förfaranden, eller
- iv) om den vidare överföringen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.

Vid varje vidare överföring måste uppgiftsinföraren uppfylla kraven för alla andra skyddsåtgärder i dessa klausuler, i synnerhet ändamålsbegränsning.

8.9 Dokumentation och efterlevnad

- a) Uppgiftsinföraren ska skyndsamt och på ett lämpligt sätt hantera förfrågningar från uppgiftsutföraren angående behandlingen enligt dessa klausuler.
- b) Parterna ska kunna visa att de uppfyller kraven i dessa klausuler. Framför allt ska uppgiftsinföraren föra lämplig dokumentation över den behandling som utförts på uppdrag av uppgiftsutföraren.
- c) Uppgiftsinföraren ska se till att uppgiftsutföraren har tillgång till all information som behövs för att visa att de skyldigheter som fastställs i dessa klausuler har fullgjorts och, på uppgiftsutförarens begäran, möjliggöra och bidra till revisioner av den behandling som omfattas av dessa klausuler med rimliga mellanrum eller om det finns indikationer på bristande efterlevnad. När beslut fattas

³ Enligt avtalet om Europeiska ekonomiska samarbetsområdet (EES-avtalet) ska EU:s inre marknad utvidgas till att omfatta de tre EES-staterna Island, Liechtenstein och Norge. Unionens dataskyddslagstiftning, inbegripet förordning (EU) 2016/679, omfattas av EES-avtalet och har införlivats i bilaga XI till avtalet. Om uppgiftsinföraren lämnar ut uppgifter till en tredje part inom EES ska detta därmed inte betraktas som en vidare överföring vid tillämpning av dessa klausuler.

om en granskning eller revision får uppgiftsutföraren ta hänsyn till relevanta intyg som innehas av uppgiftsinföraren.

- d) Uppgiftsutföraren får välja att utföra revisionen själv eller anlita en oberoende revisor. Revisionerna får omfatta inspektioner i uppgiftsinförarens lokaler eller fysiska anläggningar och ska, om så är lämpligt, utföras med rimligt varsel.
- e) Parterna ska se till att den information som avses i leden b och c, inklusive resultaten av eventuella revisioner, finns tillgänglig för den behöriga tillsynsmyndigheten på begäran.

MODUL TRE: Överföring från personuppgiftsbiträde till personuppgiftsbiträde

8.1 Instruktioner

- (a) Uppgiftsutföraren har informerat uppgiftsinföraren om att han eller hon agerar i egenskap av personuppgiftsbiträde enligt den eller de personuppgiftsansvarigas instruktioner, vilka uppgiftsutföraren ska göra tillgängliga för uppgiftsinföraren före behandlingen.
- (b) Uppgiftsinföraren ska endast behandla personuppgifter enligt dokumenterade instruktioner från den personuppgiftsansvarige, vilka uppgiftsutföraren ska tillhandahålla uppgiftsinföraren, och eventuella ytterligare dokumenterade instruktioner från uppgiftsutföraren. Sådana ytterligare instruktioner får inte stå i strid med den personuppgiftsansvariges instruktioner. Den personuppgiftsansvarige eller uppgiftsutföraren får ge ytterligare dokumenterade instruktioner avseende behandlingen av personuppgifter under hela avtalets giltighetstid.
- (c) Uppgiftsinföraren ska omedelbart informera uppgiftsutföraren vid eventuell oförmåga att följa dessa instruktioner. Om uppgiftsinföraren inte kan följa den personuppgiftsansvariges instruktioner ska uppgiftsutföraren omedelbart informera den personuppgiftsansvarige.
- (d) Uppgiftsutföraren garanterar att han eller hon har ålagt uppgiftsinföraren samma skyldigheter i fråga om uppgiftsskydd som fastställs i avtalet eller annan rättsakt enligt unionens eller medlemsstaternas lagstiftning mellan den personuppgiftsansvarige och uppgiftsutföraren⁴.

8.2 Ändamålsbegränsning

Uppgiftsinföraren ska endast behandla personuppgifter för det eller de specifika ändamålen med överföringen, enligt vad som fastställs i bilaga I.B, såvida inte andra instruktioner har lämnats av den personuppgiftsansvarige, enligt information från uppgiftsutföraren till uppgiftsinföraren, eller av uppgiftsutföraren.

⁴ Se artikel 28.4 i förordning (EU) 2016/679 och, om den personuppgiftsansvarige är en EU-institution eller ett EU-organ, artikel 29.4 i förordning (EU) 2018/1725.

8.3 Öppenhet

På begäran ska uppgiftsutföraren tillhandahålla en kopia av dessa klausuler, inklusive tillägget när det har fyllts i av parterna, till den registrerade utan kostnad. I den mån det är nödvändigt för att skydda affärshemligheter eller andra konfidentiella uppgifter, inklusive personuppgifter, får uppgiftsutföraren redigera delar av texten i tillägget innan en kopia tillhandahålls, men han eller hon måste bifoga en meningsfull sammanfattning om den registrerade annars inte skulle kunna förstå dess innehåll eller utöva sina rättigheter. På begäran ska parterna tillhandahålla skälen till redigeringen till den registrerade, i möjligaste mån utan att avslöja de redigerade uppgifterna.

8.4 Korrekthet

Om uppgiftsinföraren får kännedom om att de personuppgifter som han eller hon har tagit emot är felaktiga, eller har blivit inaktuella, ska han eller hon informera uppgiftsutföraren utan onödigt dröjsmål. I sådana fall ska uppgiftsinföraren samarbeta med uppgiftsutföraren för att rätta eller radera uppgifterna.

8.5 Behandlingens varaktighet och radering eller återlämnande av uppgifter

Uppgiftsinförarens behandling ska endast äga rum under den period som anges i bilaga I.B. När tillhandahållandet av behandlingstjänsterna har avslutats ska uppgiftsinföraren, enligt uppgiftsutförarens val, radera alla personuppgifter som behandlats på uppdrag av den personuppgiftsansvarige och intyga för uppgiftsutföraren att detta har skett, eller till uppgiftsutföraren återlämna alla personuppgifter som har behandlats på uppdrag av uppgiftsutföraren och radera befintliga kopior. Till dess att uppgifterna raderats eller återlämnats ska uppgiftsinföraren fortsätta att se till att dessa klausuler följs. Om återlämnande eller radering av personuppgifterna är förbjudet enligt lokal lagstiftning som är tillämplig för uppgiftsinföraren ska uppgiftsinföraren garantera att han eller hon kommer att fortsätta att uppfylla kraven i dessa klausuler och endast kommer att behandla personuppgifterna i den utsträckning och under den tid som krävs enligt den lokala lagstiftningen. Detta påverkar inte klausul 14, i synnerhet kravet enligt klausul 14 e att uppgiftsinföraren under hela avtalets giltighetstid ska meddela uppgiftsutföraren om han eller hon har anledning att misstänka att han eller hon är eller har blivit föremål för lagar eller förfaranden som inte stämmer överens med kraven i klausul 14 a.

8.6 Säkerhet vid behandling

- (a) Uppgiftsinföraren, och under överföring även uppgiftsutföraren, ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa uppgifternas säkerhet, däribland genom skydd mot säkerhetsbrott som skulle leda till oavsiktlig eller olaglig förstöring, förlust, ändring, obehörigt utlämnande eller obehörig åtkomst till uppgifterna (*personuppgiftsincident*). Vid bedömning av lämplig säkerhetsnivå ska de ta vederbörlig hänsyn till de senaste rönen, kostnaderna för genomförandet, behandlingens karaktär, omfattning, sammanhang och ändamål samt riskerna för den registrerade i samband med behandlingen. Parterna ska i synnerhet överväga att använda kryptering eller pseudonymisering, även under

- överföringen, om ändamålet med behandlingen kan uppfyllas på detta sätt. Vid användning av pseudonymisering ska uppgiftsutföraren eller den personuppgiftsansvarige om möjligt behålla sin fullständiga kontroll över den ytterligare information som krävs för att knyta personuppgifterna till en viss registrerad. För att fullgöra sina skyldigheter enligt denna punkt ska uppgiftsinföraren åtminstone genomföra de tekniska och organisatoriska åtgärder som anges i bilaga II. Uppgiftsinföraren ska göra regelbundna kontroller för att säkerställa att dessa åtgärder även fortsättningsvis ger en lämplig säkerhetsnivå.
- (b) Uppgiftsinföraren ska endast ge sin personal tillgång till uppgifterna i den utsträckning det är absolut nödvändigt för att genomföra, förvalta och övervaka avtalet. Uppgiftsinföraren ska säkerställa att personer som har tillstånd att behandla personuppgifterna har förbundit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.
 - (c) I händelse av en personuppgiftsincident som gäller uppgifter som har behandlats av uppgiftsinföraren enligt dessa klausuler ska uppgiftsinföraren vidta lämpliga åtgärder för att hantera incidenten, däribland åtgärder för att mildra dess negativa konsekvenser. Uppgiftsinföraren ska även, utan onödigt dröjsmål, meddela uppgiftsutföraren och, om det är lämpligt och genomförbart, den personuppgiftsansvarige efter att ha fått kännedom om incidenten. Meddelandet ska innehålla uppgifter om en kontaktpunkt som kan lämna mer information, en beskrivning av incidentens karaktär (inbegripet, om möjligt, vilka kategorier och det ungefärliga antalet registrerade och personuppgiftsregister som berörs), dess sannolika konsekvenser samt vilka åtgärder som har vidtagits eller föreslagits för att hantera incidenten, däribland åtgärder för att mildra dess möjliga negativa konsekvenser. Om, och i den mån, det inte är möjligt att tillhandahålla all information vid samma tillfälle ska det inledande meddelandet innehålla den information som då finns tillgänglig, varefter ytterligare information ska tillhandahållas utan onödigt dröjsmål efterhand som den blir tillgänglig.
 - (d) Uppgiftsinföraren ska samarbeta med och bistå uppgiftsutföraren så att uppgiftsutföraren kan fullgöra sina skyldigheter enligt förordning (EU) 2016/679, framför allt att meddela den personuppgiftsansvarige så att denne i sin tur kan meddela den behöriga tillsynsmyndigheten och de berörda registrerade, med beaktande av behandlingens karaktär och den information som finns tillgänglig för uppgiftsinföraren.

8.7 Känsliga uppgifter

Om överföringen inbegriper personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska eller biometriska uppgifter för unik identifiering av en fysisk person, uppgifter om hälsa eller en persons sexualliv eller sexuella läggning, eller uppgifter om brottmålsdomar och lagöverträdelse (känsliga uppgifter) ska uppgiftsinföraren tillämpa de särskilda begränsningar och/eller de ytterligare skyddsåtgärder som beskrivs i bilaga I.B.

8.8 Vidare överföringar

Uppgiftsinföraren ska endast lämna ut personuppgifterna till en tredje part efter dokumenterade instruktioner från den personuppgiftsansvarige, enligt den information som

uppgiftsinföraren har fått av uppgiftsutföraren. Dessutom får uppgifterna endast lämnas ut till en tredje part utanför Europeiska unionen⁵ (i samma land som uppgiftsinföraren eller i ett annat tredjeland, nedan kallat *vidare överföring*), om den tredje parten är eller samtycker till att vara bunden av dessa klausuler i motsvarande modul, eller

- (i) om den vidare överföringen sker till ett land som omfattas av ett beslut om adekvat skyddsnivå enligt artikel 45 i förordning (EU) 2016/679 som täcker den vidare överföringen,
- (ii) om den tredje parten på annat sätt säkerställer lämpliga skyddsåtgärder enligt artikel 46 eller 47 i förordning (EU) 2016/679,
- (iii) om den vidare överföringen är nödvändig för att fastställa, göra gällande eller försvara ett rättsligt anspråk i samband med särskilda administrativa, tillsynsrelaterade eller rättsliga förfaranden, eller
- (iv) om den vidare överföringen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.

Vid varje vidare överföring måste uppgiftsinföraren uppfylla kraven för alla andra skyddsåtgärder i dessa klausuler, i synnerhet ändamålsbegränsning.

8.9 Dokumentation och efterlevnad

- (a) Uppgiftsinföraren ska skyndsamt och på lämpligt sätt hantera förfrågningar från uppgiftsutföraren eller den personuppgiftsansvarige angående behandlingen enligt dessa klausuler.
- (b) Parterna ska kunna visa att de uppfyller kraven i dessa klausuler. Framför allt ska uppgiftsinföraren föra lämplig dokumentation över den behandling som utförts på uppdrag av den personuppgiftsansvarige.
- (c) Uppgiftsinföraren ska se till att uppgiftsutföraren får tillgång till all information som behövs för att visa att de skyldigheter som fastställs i dessa klausuler har fullgjorts; uppgiftsutföraren ska sedan vidarebefordra denna information till den personuppgiftsansvarige.
- (d) Uppgiftsinföraren ska möjliggöra och bidra till uppgiftsutförarens revisioner av den behandling som omfattas av dessa klausuler, med rimliga mellanrum eller om det finns indikationer på bristande efterlevnad. Detsamma ska gälla om uppgiftsutföraren begär en revision enligt instruktioner från den personuppgiftsansvarige. När beslut fattas om en revision får uppgiftsutföraren ta hänsyn till relevanta intyg som innehålls av uppgiftsinföraren.
- (e) Om revisionen utförs efter den personuppgiftsansvariges instruktioner ska uppgiftsutföraren göra resultaten tillgängliga för den personuppgiftsansvarige.

⁵ Enligt avtalet om Europeiska ekonomiska samarbetsområdet (EES-avtalet) ska EU:s inre marknad utvidgas till att omfatta de tre EES-staterna Island, Liechtenstein och Norge. Unionens dataskyddslagstiftning, inbegripet förordning (EU) 2016/679, omfattas av EES-avtalet och har införlivats i bilaga XI till avtalet. Om uppgiftsinföraren lämnar ut uppgifter till en tredje part inom EES ska detta därmed inte betraktas som en vidare överföring vid tillämpning av dessa klausuler.

- (f) Uppgiftsutföraren får välja att utföra revisionen själv eller anlita en oberoende revisor. Revisionerna får omfatta inspektioner i uppgiftsinförarens lokaler eller fysiska anläggningar och ska, om så är lämpligt, utföras med rimligt varsel.
- (g) Parterna ska se till att den information som avses i leden b och c, inklusive resultaten av eventuella revisioner, finns tillgänglig för den behöriga tillsynsmyndigheten på begäran.

Klausul 9

Användning av underentreprenörer

MODUL TVÅ: Överföring från personuppgiftsansvarig till personuppgiftsbiträde

- a) Uppgiftsinföraren har uppgiftsutförarens allmänna tillstånd att anlita en eller flera underentreprenörer i en överenskommen förteckning. Uppgiftsinföraren ska informera uppgiftsutföraren skriftligen om alla planerade ändringar av förteckningen genom tillägg eller ersättning av underentreprenörer minst 90 dagar i förväg, så att uppgiftsutföraren har tillräckligt med tid för att invända mot sådana ändringar före anlitandet av underentreprenören(-erna). Uppgiftsinföraren ska ge uppgiftsutföraren all information som behövs för att uppgiftsutföraren ska kunna utöva sin rätt att göra invändningar.
- b) Om uppgiftsinföraren anlitar en underentreprenör för att utföra särskilda behandlingar (på uppdrag av uppgiftsutföraren) ska han eller hon göra detta genom ett skriftligt avtal som, i sak, innehåller samma skyldigheter i fråga om dataskydd som de avtal som är bindande för uppgiftsinföraren enligt dessa klausuler, däribland vad gäller de registrerades rättigheter som berättigade tredje parter⁶. Parterna är överens om att uppgiftsinföraren, genom att uppfylla kraven i denna klausul, fullgör sina skyldigheter enligt klausul 8.8. Uppgiftsinföraren ska säkerställa att underentreprenören fullgör de skyldigheter som uppgiftsinföraren omfattas av enligt dessa klausuler.
- c) Uppgiftsinföraren ska, på uppgiftsutförarens begäran, tillhandahålla en kopia av avtalet med underentreprenören och eventuella senare ändringar till uppgiftsutföraren. I den mån det är nödvändigt för att skydda affärshemligheter eller andra konfidentiella uppgifter, inklusive personuppgifter, får uppgiftsinföraren redigera texten i avtalet innan en kopia tillhandahålls.
- d) Uppgiftsinföraren ska fortsatt vara fullt ansvarig inför uppgiftsutföraren för fullgörandet av underentreprenörens skyldigheter inom ramen för dennes avtal med uppgiftsinföraren. Uppgiftsinföraren ska meddela uppgiftsutföraren om underentreprenören underlåter att fullgöra sina skyldigheter inom ramen för avtalet.
- e) Uppgiftsinföraren ska komma överens om en klausul om tredjepartsberättigande med underentreprenören, varigenom uppgiftsutföraren – om uppgiftsinföraren har upphört att existera i faktisk eller rättslig mening eller har hamnat på obestånd – ska ha rätt att säga upp avtalet med underentreprenören och beordra underentreprenören att radera eller återlämna personuppgifterna.

⁶ Detta krav får uppfyllas av den underentreprenör som anslutit sig till dessa klausuler inom ramen för den tillämpliga modulen i enlighet med klausul 7.

MODUL TRE: Överföring från personuppgiftsbiträde till personuppgiftsbiträde

- (a) Uppgiftsinföraren har den personuppgiftsansvariges allmänna tillstånd att anlita en eller flera underentreprenörer i en överenskommen förteckning. Uppgiftsinföraren ska informera den personuppgiftsansvarige skriftligen om alla planerade ändringar av förteckningen genom tillägg eller ersättning av underentreprenörer minst 90 dagar i förväg, så att den personuppgiftsansvarige har tillräckligt med tid för att invända mot sådana ändringar före anlitandet av underentreprenören(-erna). Uppgiftsinföraren ska ge den personuppgiftsansvarige all information som behövs för att den personuppgiftsansvarige ska kunna utöva sin rätt att göra invändningar. Uppgiftsinföraren ska informera uppgiftsutföraren om anlitandet av underentreprenören(-erna).
- (b) Om uppgiftsinföraren anlitar en underentreprenör för att utföra särskilda behandlingar (på uppdrag av den personuppgiftsansvarige) ska han eller hon göra detta genom ett skriftligt avtal som, i sak, innehåller samma skyldigheter i fråga om dataskydd som de avtal som är bindande för uppgiftsinföraren enligt dessa klausuler, däribland vad gäller de registrerades rättigheter som berättigade tredje parter⁷. Parterna är överens om att uppgiftsinföraren, genom att uppfylla kraven i denna klausul, fullgör sina skyldigheter enligt klausul 8.8. Uppgiftsinföraren ska säkerställa att underentreprenören fullgör de skyldigheter som uppgiftsinföraren omfattas av enligt dessa klausuler.
- (c) Uppgiftsinföraren ska, på uppgiftsutförarens eller den personuppgiftsansvariges begäran, tillhandahålla en kopia av avtalet med underentreprenören och eventuella senare ändringar. I den mån det är nödvändigt för att skydda affärshemligheter eller andra konfidentiella uppgifter, inklusive personuppgifter, får uppgiftsinföraren redigera texten i avtalet innan en kopia tillhandahålls.
- (d) Uppgiftsinföraren ska fortsatt vara fullt ansvarig inför uppgiftsutföraren för fullgörandet av underentreprenörens skyldigheter inom ramen för dennes avtal med uppgiftsinföraren. Uppgiftsinföraren ska meddela uppgiftsutföraren om underentreprenören underlåter att fullgöra sina skyldigheter inom ramen för avtalet.
- (e) Uppgiftsinföraren ska komma överens om en klausul om tredjepartsberättigande med underentreprenören, varigenom uppgiftsutföraren – om uppgiftsinföraren har upphört att existera i faktisk eller rättslig mening eller har hamnat på obestånd – ska ha rätt att säga upp avtalet med underentreprenören och beordra underentreprenören att radera eller återlämna personuppgifterna.

Klausul 10**De registrerades rättigheter****MODUL TVÅ: Överföring från personuppgiftsansvarig till personuppgiftsbiträde**

⁷ Detta krav får uppfyllas av den underentreprenör som anslutit sig till dessa klausuler inom ramen för den tillämpliga modulen i enlighet med klausul 7.

- a) Uppgiftsinföraren ska skyndsamt meddela uppgiftsutföraren om varje begäran från en registrerad. Uppgiftsinföraren ska inte själv besvara begäran, såvida inte han eller hon har fått tillstånd att göra detta av uppgiftsutföraren.
- b) Uppgiftsinföraren ska bistå uppgiftsutföraren med att fullgöra dennes skyldigheter att tillgodose de registrerades begäranden om att utöva sina rättigheter enligt förordning (EU) 2016/679. I detta avseende ska parterna fastställa lämpliga tekniska och organisatoriska åtgärder i bilaga II, med beaktande av behandlingens karaktär, genom vilka biståndet ska tillhandahållas, såväl som tillämpningsområdet för och omfattningen av det bistånd som begärs.
- c) När uppgiftsinföraren fullgör sina skyldigheter enligt leden a och b ska han eller hon följa uppgiftsutförarens instruktioner.

MODUL TRE: Överföring från personuppgiftsbiträde till personuppgiftsbiträde

- (a) Uppgiftsinföraren ska skyndsamt meddela uppgiftsutföraren och, om så är lämpligt, den personuppgiftsansvarige om varje begäran som tas emot från en registrerad, utan att besvara begäran såvida inte han eller hon har den personuppgiftsansvariges tillstånd att göra detta.
- (b) Uppgiftsinföraren ska bistå den personuppgiftsansvarige, i tillämpliga fall i samarbete med uppgiftsutföraren, med att fullgöra dennes skyldigheter att tillgodose de registrerades begäranden om att utöva sina rättigheter enligt förordning (EU) 2016/679 eller förordning (EU) 2018/1725, enligt vad som är tillämpligt. I detta avseende ska parterna fastställa lämpliga tekniska och organisatoriska åtgärder i bilaga II, med beaktande av behandlingens karaktär, genom vilka biståndet ska tillhandahållas, såväl som tillämpningsområdet för och omfattningen av det bistånd som begärs.
- (c) När uppgiftsinföraren fullgör sina skyldigheter enligt leden a och b ska han eller hon följa den personuppgiftsansvariges instruktioner, vilka meddelas av uppgiftsutföraren.

Klausul 11

Tillgång till prövning

- a) Uppgiftsinföraren ska informera de registrerade i ett öppet och lättillgängligt format, genom enskilda meddelanden eller på sin webbplats, om en kontaktpunkt som har tillstånd att hantera klagomål. Uppgiftsinföraren ska skyndsamt hantera varje klagomål som tas emot från en registrerad.

MODUL TVÅ: Överföring från personuppgiftsansvarig till personuppgiftsbiträde

MODUL TRE: Överföring från personuppgiftsbiträde till personuppgiftsbiträde

- b) Om en tvist uppstår mellan en registrerad och en av parterna när det gäller efterlevnaden av dessa klausuler ska den parten göra sitt yttersta för att lösa tvisten i godo på ett skyndsamt sätt. Parterna ska informera varandra om sådana tvister och, i tillämpliga fall, samarbeta för att lösa dem.
- c) Om den registrerade åberopar en rättighet som berättigad tredje part enligt klausul 3 ska uppgiftsinföraren godta den registrerades beslut att

- i) inge ett klagomål till tillsynsmyndigheten i den medlemsstat där han/hon är stadigvarande bosatt eller har sin arbetsplats, eller till den behöriga tillsynsmyndigheten enligt klausul 13,
- ii) hänskjuta tvisten till de behöriga domstolarna i den mening som avses i klausul 18.
- d) Parterna godtar att den registrerade får företräddas av ett organ, en organisation eller sammanslutning utan vinstsyfte enligt de villkor som fastställs i artikel 80.1 i förordning (EU) 2016/679.
- e) Uppgiftsinföraren ska följa ett beslut som är bindande enligt tillämplig lagstiftning i EU eller medlemsstaterna.
- f) Uppgiftsinföraren är införstådd med att det val som gjorts av den registrerade inte kommer att påverka hans/hennes materiella och processuella rättigheter att begära prövning i enlighet med tillämplig lagstiftning.

Klausul 12

Ansvarsskyldighet

MODUL TVÅ: Överföring från personuppgiftsansvarig till personuppgiftsbiträde

MODUL TRE: Överföring från personuppgiftsbiträde till personuppgiftsbiträde

- a) Varje part ska vara ansvarig inför den andra parten eller de andra parterna för eventuella skador den orsakar den andra parten eller de andra parterna genom överträdelse av dessa klausuler.
- b) Uppgiftsinföraren ska vara ansvarig inför den registrerade, och den registrerade ska ha rätt till ersättning, för varje materiell eller immateriell skada som uppgiftsinföraren eller dess underentreprenör orsakar den registrerade genom att kränka rättigheterna för en berättigad tredje part enligt dessa klausuler.
- c) Utan att det påverkar led b ska uppgiftsutföraren vara ansvarig inför den registrerade, och den registrerade ska ha rätt till ersättning, för varje materiell eller immateriell skada som uppgiftsutföraren eller uppgiftsinföraren (eller dess underentreprenör) orsakar den registrerade genom att kränka rättigheterna för en berättigad tredje part enligt dessa klausuler. Detta påverkar inte uppgiftsutförarens ansvarsskyldighet eller, om uppgiftsutföraren är ett personuppgiftsbiträde som agerar på uppdrag av en personuppgiftsansvarig, den personuppgiftsansvariges ansvarsskyldighet enligt förordning (EU) 2016/679 eller förordning (EU) 2018/1725, enligt vad som är tillämpligt.
- d) Parterna är överens om att en uppgiftsutförare som enligt led c hålls ansvarig för skada som orsakats av uppgiftsinföraren (eller dess underentreprenör) ska ha rätt att återkräva den del av ersättningen från uppgiftsinföraren som motsvarar dennes ansvarsskyldighet för skadan.
- e) Om fler än en part är ansvariga för eventuell skada som orsakats den registrerade till följd av en överträdelse av dessa klausuler ska alla ansvarsskyldiga parter vara solidariskt ansvariga, och den registrerade ska ha rätt att väcka talan i domstol mot var och en av dessa parter.
- f) Parterna är överens om att en part som hålls ansvarig enligt led e ska ha rätt att återkräva från den andra parten eller de andra parterna den del av ersättningen som motsvarar dess/deras ansvarsskyldighet för skadan.
- g) Uppgiftsinföraren får inte åberopa en underentreprenörs uppförande för att undvika sitt eget ansvar.

Klausul 13**Tillsyn****MODUL TVÅ: Överföring från personuppgiftsansvarig till personuppgiftsbiträde****MODUL TRE: Överföring från personuppgiftsbiträde till personuppgiftsbiträde**

- a) [Om uppgiftsutföraren är etablerad i en av EU:s medlemsstater:] Den tillsynsmyndighet som har ansvar för att säkerställa uppgiftsutförarens efterlevnad av förordning (EU) 2016/679 när det gäller överföring av uppgifter, enligt vad som anges i bilaga I.C, ska fungera som behörig tillsynsmyndighet.
- b) Uppgiftsinföraren samtycker till att godta den behöriga tillsynsmyndighetens behörighet och samarbeta med den i varje förfarande som syftar till att säkerställa efterlevnaden av dessa klausuler. Uppgiftsinföraren samtycker i synnerhet till att svara på förfrågningar, gå med på revisioner och iakttä de åtgärder som antagits av tillsynsmyndigheten, inbegripet korrigerande och kompenserade åtgärder. Uppgiftsinföraren ska ge tillsynsmyndigheten en skriftlig bekräftelse på att nödvändiga åtgärder har vidtagits.

**AVSNITT III – LOKALA LAGAR OCH SKYLDIGHETER VID ÅTKOMST AV
OFFENTLIGA MYNDIGHETER**

Klausul 14**Lokala lagar och förfaranden som påverkar efterlevnaden av klausulerna****MODUL TVÅ: Överföring från personuppgiftsansvarig till personuppgiftsbiträde****MODUL TRE: Överföring från personuppgiftsbiträde till personuppgiftsbiträde**

- a) Parterna garanterar att de inte har någon anledning att misstänka att de lagar och förfaranden i det mottagande tredjelandet som är tillämpliga på uppgiftsinförarens behandling av personuppgifter, däribland eventuella krav på att lämna ut personuppgifter eller åtgärder för att bevilja åtkomst för offentliga myndigheter, hindrar uppgiftsinföraren från att fullgöra sina skyldigheter enligt dessa klausuler. Detta bygger på förutsättningen att lagar och förfaranden som är förenliga med andemeningen i de grundläggande rättigheterna och friheterna, och som inte går utöver vad som är nödvändigt och proportionerligt i ett demokratiskt samhälle för att skydda de ändamål som anges i artikel 23.1 i förordning (EU) 2016/679, inte strider mot dessa klausuler.
- b) Genom att tillhandahålla den garanti som avses i led a intygar parterna att de har tagit vederbörlig hänsyn till särskilt följande aspekter:
 - i) De särskilda omständigheterna kring överföringen, däribland behandlingskedjans längd, antalet inblandade aktörer och vilka överföringskanaler som använts; planerade vidare överföringar; typen av mottagare; ändamålet med behandlingen; de överförda personuppgifternas kategorier och format; den ekonomiska sektor inom vilken överföringen äger rum; platsen för lagring av de överförda uppgifterna.
 - ii) De lagar och förfaranden i det mottagande tredjelandet – inbegripet krav på att lämna ut uppgifterna till offentliga myndigheter eller att ge sådana myndigheter åtkomst till uppgifterna –

som är relevanta mot bakgrund av överföringens särskilda omständigheter samt tillämpliga begränsningar och skyddsåtgärder⁸.

- iii) Alla relevanta avtalsenliga, tekniska eller organisatoriska skyddsåtgärder som införts för att komplettera skyddsåtgärderna enligt dessa klausuler, inbegripet åtgärder som tillämpats under överföringen och vid behandlingen av personuppgifterna i det mottagande tredjelandet.
- c) Uppgiftsinföraren garanterar att han eller hon, i samband med den bedömning som avses i led b, har gjort sitt yttersta för att ge uppgiftsutföraren relevant information, och samtycker till att fortsätta att samarbeta med uppgiftsutföraren för att säkerställa efterlevnaden av dessa klausuler.
- d) Parterna är överens om att dokumentera den bedömning som avses i led b och att på begäran göra den tillgänglig för den behöriga tillsynsmyndigheten.
- e) Uppgiftsinföraren samtycker till att skyndsamt meddela uppgiftsutföraren om han eller hon, efter att ha godkänt dessa klausuler och under hela avtalets giltighetstid, har anledning att misstänka att han eller hon är eller har blivit föremål för lagar eller förfaranden som inte stämmer överens med kraven i led a, däribland efter en ändring i lagarna i tredjelandet eller en åtgärd (såsom en begäran om utlämnande av uppgifter) som antyder att en tillämpning av sådana lagar i praktiken inte stämmer överens med kraven i led a. [För modul tre: Uppgiftsutföraren ska vidarebefordra meddelandet till den personuppgiftsansvarige.]
- f) Efter att ha tagit emot ett meddelande i enlighet med led e, eller om uppgiftsutföraren har andra anledningar att misstänka att uppgiftsinföraren inte längre kan fullgöra sina skyldigheter enligt dessa klausuler, ska uppgiftsutföraren skyndsamt fastställa lämpliga åtgärder (t.ex. tekniska eller organisatoriska åtgärder för att säkerställa säkerhet och konfidentialitet) som ska antas av uppgiftsutföraren och/eller uppgiftsinföraren för att hantera situationen [för modul tre: , i tillämpliga fall efter samråd med den personuppgiftsansvarige]. Uppgiftsutföraren ska avbryta överföringen av uppgifter om han eller hon anser att inga lämpliga skyddsåtgärder kan säkerställas för överföringen, eller efter att ha fått instruktioner från [för modul tre: den personuppgiftsansvarige eller] den behöriga tillsynsmyndigheten att göra det. I sådana fall ska uppgiftsutföraren ha rätt att säga upp avtalet i den mån det gäller behandling av personuppgifter enligt dessa klausuler. Om avtalet omfattar fler än två parter får uppgiftsutföraren utöva denna rätt att säga upp avtalet med endast den berörda parten, såvida inte parterna har kommit överens om annat. Om avtalet sägs upp enligt denna klausul ska klausul 16 d och e tillämpas.

Klausul 15

Uppgiftsinförarens skyldigheter vid åtkomst av offentliga myndigheter

MODUL TVÅ: Överföring från personuppgiftsansvarig till personuppgiftsbiträde

MODUL TRE: Överföring från personuppgiftsbiträde till personuppgiftsbiträde

15.1 Meddelanden

⁸ När det gäller konsekvenserna av sådana lagar och förfaranden för efterlevnaden av dessa klausuler kan olika aspekter anses utgöra en del av den övergripande bedömningen. Sådana aspekter kan omfatta relevant och dokumenterad praktisk erfarenhet av tidigare begäranden om utlämnande av uppgifter från offentliga myndigheter, eller avsaknad av sådana begäranden, som täcker en tillräckligt representativ tidsram. Detta gäller särskilt interna register eller annan dokumentation som upprättats kontinuerligt i enlighet med tillbörlig aktsamhet och som godkänts på ledningsnivå, under förutsättning att denna information kan delas med tredje parter på ett lagligt sätt. Om denna praktiska erfarenhet används som grund för slutsatsen att uppgiftsinföraren inte kommer att hindras från att uppfylla kraven i dessa klausuler måste den stödjas av andra relevanta, objektiva aspekter, och parterna måste noggrant överväga huruvida dessa aspekter tillsammans har tillräckligt stor vikt, vad gäller deras tillförlitlighet och representativitet, för att underbygga denna slutsats. Parterna måste i synnerhet ta hänsyn till huruvida deras praktiska erfarenhet bekräftas och inte motsägs av offentligt tillgänglig eller på annat sätt åtkomlig och tillförlitlig information om förekomst eller avsaknad av begäranden inom samma sektor och/eller av tillämpningen av lagstiftningen i praktiken, t.ex. rättspraxis och rapporter från oberoende tillsynsorgan.

- a) Uppgiftsinföraren samtycker till att skyndsamt meddela uppgiftsutföraren och, om så är möjligt, den registrerade (vid behov med hjälp av uppgiftsutföraren) om han eller hon
- i) får en rättsligt bindande begäran från en offentlig myndighet, inbegripet en rättslig myndighet, i enlighet med det mottagande landets lagstiftning om att personuppgifter som överförts enligt dessa klausuler ska lämnas ut; meddelandet ska innehålla information om de begärda personuppgifterna, den begärande myndigheten, den rättsliga grunden för begäran och det svar som lämnats, eller
 - ii) får kännedom om att offentliga myndigheter har haft direkt tillgång till enligt dessa klausuler överförda personuppgifter i enlighet med det mottagande landets lagstiftning; meddelandet ska innehålla all information som uppgiftsinföraren har tillgång till.
- [För modul tre: Uppgiftsutföraren ska vidarebefordra meddelandet till den personuppgiftsansvarige.]
- b) Om uppgiftsinföraren är förbjuden att meddela uppgiftsutföraren och/eller den registrerade enligt det mottagande landets lagstiftning samtycker uppgiftsinföraren till att göra sitt yttersta för att få till stånd ett undantag från förbudet, för att kunna tillhandahålla så mycket information som möjligt inom kortast möjliga tid. Uppgiftsinföraren samtycker till att dokumentera sina ansträngningar för att kunna bekräfta dem på begäran av uppgiftsutföraren.
- c) Om det är tillåtet enligt det mottagande landets lagstiftning samtycker uppgiftsinföraren till att, med jämna mellanrum under hela avtalets giltighetstid, ge uppgiftsutföraren så mycket relevant information som möjligt om de begäranden som tagits emot (i synnerhet antalet begäranden, vilken typ av uppgifter som begärts, den eller de begärande myndigheterna, om begärandena har bestridits och resultaten av bestridandena etc.). [För modul tre: Uppgiftsutföraren ska vidarebefordra informationen till den personuppgiftsansvarige.]
- d) Uppgiftsinföraren samtycker till att lagra den information som avses i leden a–c under hela avtalets giltighetstid och göra den tillgänglig för den behöriga tillsynsmyndigheten på begäran.
- e) Leden a–c påverkar inte uppgiftsinförarens skyldighet enligt klausul 14 e och klausul 16 att skyndsamt informera uppgiftsutföraren om han eller hon inte kan uppfylla kraven i dessa klausuler.

15.2 Granskning av laglighet och uppgiftsminimering

- a) Uppgiftsinföraren samtycker till att granska lagligheten i begäran om utlämnande av uppgifter, särskilt om begäran omfattas av de befogenheter som har beviljats den begärande offentliga myndigheten, och att bestrida begäran om han eller hon, efter noggrann bedömning, drar slutsatsen att det finns rimliga skäl att betrakta begäran som olaglig enligt det mottagande landets lagstiftning, tillämpliga skyldigheter enligt internationell rätt och principen om internationell hövlighet. Uppgiftsinföraren ska, enligt samma villkor, fullfölja möjligheterna att överklaga. Om uppgiftsinföraren bestrider en begäran ska han eller hon vidta provisoriska åtgärder för att upphäva konsekvenserna av begäran tills den behöriga rättsliga myndigheten har fattat beslut i frågan. Uppgiftsinföraren får inte lämna ut de begärda personuppgifterna förrän han eller hon är skyldig att göra detta enligt tillämpliga förfaranderegler. Dessa krav påverkar inte uppgiftsinförarens skyldigheter enligt klausul 14 e.
- b) Uppgiftsinföraren samtycker till att dokumentera sin rättsliga bedömning och varje bestridande av begäran om utlämnande av uppgifter och, i den mån det är tillåtet enligt det mottagande landets lagstiftning, göra dokumentationen tillgänglig för uppgiftsutföraren. Uppgiftsinföraren ska även göra dokumentationen tillgänglig för den behöriga tillsynsmyndigheten på begäran. [För modul tre: Uppgiftsutföraren ska se till att den personuppgiftsansvarige får tillgång till bedömningen.]
- c) Uppgiftsinföraren samtycker till att tillhandahålla den minsta tillåtna mängden information när han eller hon besvarar en begäran om utlämnande av uppgifter, baserat på en rimlig tolkning av begäran.

AVSNITT IV – SLUTBESTÄMMELSER

Klausul 16

Bristande efterlevnad av klausulerna och avtalets uppsägning

- a) Uppgiftsinföraren ska skyndsamt informera uppgiftsutföraren om han eller hon inte kan uppfylla kraven i dessa klausuler, oavsett orsak.
- b) Om uppgiftsinföraren bryter mot dessa klausuler eller inte kan uppfylla kraven i dessa klausuler ska uppgiftsutföraren avbryta överföringen av personuppgifter till uppgiftsinföraren tills efterlevnaden åter har säkerställts eller avtalet har sagts upp. Detta påverkar inte tillämpningen av klausul 14 f.
- c) Uppgiftsutföraren ska ha rätt att säga upp avtalet i den mån det gäller behandlingen av personuppgifter enligt dessa klausuler om
 - i) uppgiftsutföraren har avbrutit överföringen av personuppgifter till uppgiftsinföraren enligt led b och om efterlevnaden av dessa klausuler inte har återupprättats inom en rimlig tidsperiod, under alla omständigheter inom en månad efter avbrytandet,
 - ii) uppgiftsinföraren gör sig skyldig till allvarliga eller upprepade överträdelser av dessa klausuler, eller
 - iii) uppgiftsinföraren inte följer ett bindande beslut av en behörig domstol eller tillsynsmyndighet angående hans eller hennes skyldigheter enligt dessa klausuler.

I sådana fall ska uppgiftsutföraren informera den behöriga tillsynsmyndigheten [för modul tre: och den personuppgiftsansvarige] om denna bristande efterlevnad. Om avtalet omfattar fler än två parter får uppgiftsutföraren utöva denna rätt att säga upp avtalet med endast den berörda parten, såvida inte parterna har kommit överens om annat.

- d) [För modulerna ett, två och tre: Personuppgifter som överförts före uppsägningen av avtalet i enlighet med led c ska efter uppgiftsutförarens eget val omedelbart återlämnas till uppgiftsinföraren eller raderas i sin helhet. Detsamma ska gälla för eventuella kopior av uppgifterna.] Uppgiftsinföraren ska intyga för uppgiftsutföraren att uppgifterna har raderats. Till dess att uppgifterna raderats eller återlämnats ska uppgiftsinföraren fortsätta att se till att dessa klausuler följs. Om återlämnande eller radering av de överförda personuppgifterna är förbjudet enligt lokal lagstiftning som är tillämplig för uppgiftsinföraren ska uppgiftsinföraren garantera att han eller hon kommer att fortsätta att uppfylla kraven i dessa klausuler och endast kommer att behandla personuppgifterna i den utsträckning och under den tid som krävs enligt den lokala lagstiftningen.
- e) Endera parten får återkalla sin överenskommelse om att vara bunden av dessa klausuler om i) Europeiska kommissionen antar ett beslut i enlighet med artikel 45.3 i förordning (EU) 2016/679 som omfattar den överföring av personuppgifter som dessa klausuler gäller för, eller ii) förordning (EU) 2016/679 blir en del av den rättsliga ramen i det land till vilket personuppgifterna överförs. Detta påverkar inte övriga skyldigheter som är tillämpliga på behandlingen i fråga enligt förordning (EU) 2016/679.

Klausul 17**Tillämplig lag****MODUL TVÅ: Överföring från personuppgiftsansvarig till personuppgiftsbiträde****MODUL TRE: Överföring från personuppgiftsbiträde till personuppgiftsbiträde**

Dessa klausuler ska regleras genom lagstiftningen i den medlemsstat i EU i vilken uppgiftsutföraren är etablerad. Om lagstiftningen inte omfattar rättigheter för berättigade tredje parter ska klausulerna regleras genom lagstiftningen i en annan medlemsstat i EU som omfattar rättigheter för berättigade tredje parter. Parterna är överens om att detta ska vara lagstiftningen i Irland.

Klausul 18**Val av forum och jurisdiktion****MODUL TVÅ: Överföring från personuppgiftsansvarig till personuppgiftsbiträde****MODUL TRE: Överföring från personuppgiftsbiträde till personuppgiftsbiträde**

- a) Varje tvist som uppstår på grund av dessa klausuler ska lösas av domstolarna i en medlemsstat i EU.
- b) Parterna är överens om att dessa ska vara domstolarna i den medlemsstat vars lag tillämpas enligt Klausul 17.
- c) En registrerad får även inleda rättsliga förfaranden mot uppgiftsutföraren och/eller uppgiftsinföraren vid domstolarna i den medlemsstat där han/hon har sin stadigvarande vistelseort.
- d) Parterna är överens om att underkasta sig sådana domstolars jurisdiktion.

BILAGA I

A. FÖRTECKNING ÖVER PARTER

MODUL TVÅ: Överföring från personuppgiftsansvarig till personuppgiftsbiträde

Uppgiftsutförare:

Professionell användare, leverantör av sjukvårdstjänster till patienter.

Roll: Personuppgiftsansvarig

Uppgiftsinförare:

Abbott, leverantör av LibreView Data Management System.

Roll: Personuppgiftsbiträde

MODUL TRE: Överföring från personuppgiftsbiträde till personuppgiftsbiträde

Uppgiftsutförare:

Abbott, leverantör av LibreView Data Management System.

Roll: Personuppgiftsbiträde

Uppgiftsinförare:

Abbott Laboratories

Roll: Underentreprenör

B. BESKRIVNING AV ÖVERFÖRINGEN

MODUL TVÅ: Överföring från personuppgiftsansvarig till personuppgiftsbiträde

Kategorier av registrerade vars personuppgifter överförs:

De överförda personuppgifterna gäller följande kategorier av datasubjekt:

- Professionella användares anställda som har sitt namn och e-postadress i ett professionellt användarkonto; och
- Patienter som den professionella användaren har registrerat i LibreView datahanteringssystem förutom där patienter har registrerat sig separat för ett LibreView- konto via LibreViews webbplats.

Kategorier av personuppgifter som överförs

De överförda personuppgifterna gäller följande datakategorier:

Registreringsdata

- Patientens personuppgifter:
 - Förnamn, efternamn, postadress, e-postadress, telefonnummer, födelsedata, patientdata, apparatdata och hälsodata.
- Patientens Indirekta personuppgifter: typ av behandling/diagnos.
- Personuppgiftsansvariges anställdas personuppgifter:
 - Förnamn, efternamn, e-postadress, telefonnummer, inloggningsuppgifter och arbetsplatsadress.
- Anställdas indirekta personuppgifter:
 - Befattning.
- andra personuppgifter som tillhandahålls av datasubjekt när de registrerar sig för LibreView Data Management System (till exempel namn på förälder eller vårdnadshavare om patienten är minderårig utan möjlighet att samtycka).

IT-användningsdata

- Information om användningen av mobilappen för LibreView Data Management System i förhållande till datasubjektet (till exempel antal uppladdningar från mätanordningen, inloggningstider); och
- Andra IT-användningsdata som skapats och behandlats i samband med LibreView Data Management System med avseende på datasubjektet, inklusive, men inte begränsat till, information om operativsystemet eller programvaruversionen som används.

Känsliga uppgifter som överförs (i tillämpliga fall) och tillämpade begränsningar eller skyddsåtgärder där full hänsyn tas till uppgifternas karaktär och de medföljande riskerna, till exempel strikt ändamålsbegränsning, åtkomstbegränsningar (däribland åtkomst endast för personal som har specialutbildning), registrering av åtkomst till uppgifterna, begränsningar av vidare överföringar eller ytterligare säkerhetsåtgärder.

- Typ av diabetesmätinstrument;
- Serienummer för diabetesmätinstrument;

- Diabetestyp;
- Genomsnittligt antal blodsockermätningar under en given tidsperiod;
- Information om insulinbehandling;
- Data från patienternas mätinstrument;
- Relaterad hälsoinformation laddad upp av de registrerade, till exempel måltidsplaner; och
- Historiska glukosdata, glukostestresultat och ketontestresultat.

Frekvens för överföringen (t.ex. om uppgifterna överförs vid ett engångstillfälle eller kontinuerligt).

Kontinuerligt så länge dataexportören använder dataimportörens tjänst.

Behandlingens karaktär

De personuppgifter som överförs ska vara föremål för följande behandlingsförfaranden:

- Tillhandahålla åtkomst till personuppgifter från LibreView Data Management System för auktoriserade anställda hos professionella användare via funktionen "Practice" i LibreView, inklusive, men inte begränsat till, kollegor, läkare, sjuksköterskor och/eller vårdgivare som arbetar inom samma medicinska praktik; och
- Underhåll, support och uppdatering av LibreView Data Management System för vilket åtkomst till personuppgifter (via fjärråtkomst) inte kan uteslutas.

Ändamålet/ändamålen med överföringen av uppgifter och den efterföljande behandlingen

För att tillhandahålla, driva och underhålla LibreView Data Management System.

Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period:

Dataimportören kommer att fortsätta att lagra dataexportörens patients personuppgifter under den period som dataexportören har ett aktivt Professional User LibreView Data Management System-konto, såvida inte dataexportören väljer att radera sin patientinformation tidigare. Dataexportörens professionella användares LibreView Data Management System-konto kommer att anses vara inaktivt när det inte har varit någon aktivitet på det på sex (6) månader. Vidare kan dataimportören behålla personuppgifter i enlighet med gällande lagkrav.

MODUL TRE: Överföring från personuppgiftsbiträde till personuppgiftsbiträde

Kategorier av registrerade vars personuppgifter överförs:

De överförda personuppgifterna gäller följande kategorier av datasubjekt:

- Professionella användares anställda som har sitt namn och e-postadress i ett professionellt användarkonto; och
- Patienter som den professionella användaren har registrerat i LibreView datahanteringssystem förutom där patienter har registrerat sig separat för ett LibreView- konto via LibreViews webbplats.

Kategorier av personuppgifter som överförs:

De överförda personuppgifterna gäller följande datakategorier:

Registreringsdata

- Patientens personuppgifter:
 - Förnamn, efternamn, postadress, e-postadress, telefonnummer, födelsedata, patientdata, apparatdata och hälsodata.
- Patientens Indirekta personuppgifter: typ av behandling/diagnos.
- Personuppgiftsansvariges anställdas personuppgifter:
 - Förnamn, efternamn, e-postadress, telefonnummer, inloggningsuppgifter och arbetsplatsadress.
- Anställdas indirekta personuppgifter:
 - Befattning.
- andra personuppgifter som tillhandahålls av datasubjekt när de registrerar sig för LibreView Data Management System (till exempel namn på förälder eller vårdnadshavare om patienten är minderårig utan möjlighet att samtycka).

IT-användningsdata

- Information om användningen av mobilappen för LibreView Data Management System i förhållande till datasubjektet (till exempel antal uppladdningar från mätanordningen, inloggningstider); och
- Andra IT-användningsdata som skapats och behandlats i samband med LibreView Data Management System med avseende på datasubjektet, inklusive, men inte begränsat till, information om operativsystemet eller programvaruversionen som används.

Känsliga uppgifter som överförs (i tillämpliga fall) och tillämpade begränsningar eller skyddsåtgärder där full hänsyn tas till uppgifternas karaktär och de medföljande riskerna, till exempel strikt ändamålsbegränsning, åtkomstbegränsningar (däribland åtkomst endast för personal som har specialutbildning), registrering av åtkomst till uppgifterna, begränsningar av vidare överföringar eller ytterligare säkerhetsåtgärder.

- Typ av diabetesmätinstrument;
- Serienummer för diabetesmätinstrument;
- Diabetestyp;
- Genomsnittligt antal blodsockermätningar under en given tidsperiod;
- Information om insulinbehandling;
- Data från patienternas mätinstrument;
- Relaterad hälsoinformation laddad upp av de registrerade, till exempel måltidsplaner; och
- Historiska glukosdata, glukostestresultat och ketontestresultat.

Frekvens för överföringen (t.ex. om uppgifterna överförs vid ett engångstillfälle eller kontinuerligt):

När underhåll tillhandahålls.

Behandlingens karaktär:

De personuppgifter som överförs ska vara föremål för följande behandlingsförfaranden:

- Underhåll, support och uppdatering av LibreView Data Management System för vilket åtkomst till personuppgifter (via fjärråtkomst) inte kan uteslutas.

Ändamålet/ändamålen med överföringen av uppgifter och den efterföljande behandlingen:

För att tillhandahålla, driva och underhålla LibreView Data Management System.

Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period:

När problemet för vilket underhållet tillhandahålls har lösts, raderas personuppgifterna av uppgiftsinföraren.

C. BEHÖRIG TILLSYNSMYNDIGHET

MODUL TVÅ: Överföring från personuppgiftsansvarig till personuppgiftsbiträde

MODUL TRE: Överföring från personuppgiftsbiträde till personuppgiftsbiträde

Den tillsynsmyndighet som är behörig avseende uppgiftsutföraren.

BILAGA II

TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER, INKLUSIVE TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER FÖR ATT SÄKERSTÄLLA UPPGIFTERNAS SÄKERHET

En beskrivning av de tekniska och organisatoriska åtgärder som Abbott implementerar i enlighet med Klausul 8.6 i standardavtalsklausulerna ges i bilaga C (Säkerhetsåtgärder).

BILAGA III

FÖRTECKNING ÖVER UNDERENTREPRENÖRER

Den personuppgiftsansvarige har gett tillstånd att använda följande underentreprenörer: Så som anges i bilaga B till detta PUB-avtal.



AVTALSBILAGA B

Personuppgiftsbitrådets biträdeshållande vid avtalstecknandet.

Personuppgiftsbitrådet ingår inte i en koncern.

Bitrådet ska vid de fall det är aktuellt ange vilka underbiträden bolaget anlitar som kommer behandla eller ta del av personuppgiftsansvariges personuppgifter.

Inom parentes anges de länder där respektive bolag är etablerat och från vilka personal kan komma att behandla personuppgifter.

Behandla supportärenden, samtal och andra supportförfrågningar från den personuppgiftsansvarige.

Underentreprenörer (underbiträden)

MODUL TVÅ: Överföring från personuppgiftsansvarig till personuppgiftsbiträde

Underentreprenörens namn	Underentreprenörens adress	Beskrivning av tjänsterna	Plats varifrån tjänsterna tillhandahålls
Amazon Web Services	410 Terry Avenue North, Seattle, WA 98109, U.S.A.	Hosting och förvaltning av konton i LibreView datahanteringssystem, som tillhör användare inom EES, Schweiz och Storbritannien.	Frankrike för användare i Frankrike, Tyskland för användare i Tyskland, Irland för alla andra EES-, schweiziska och brittiska användare, Japan för japanska användare.

MODUL TRE: Överföring från personuppgiftsbiträde till personuppgiftsbiträde

Underentreprenörens namn	Underentreprenörens adress	Beskrivning av tjänsterna	Plats varifrån tjänsterna tillhandahålls
Abbott Laboratories	100 Abbott Park Road, Abbott Park, IL11, 60064 USA	Tillhandahållande av underhållstjänster, särskilt felsökning och annan applikations – och programvarusupport.	USA

BILAGA C

Säkerhetsåtgärder

TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER, INKLUSIVE TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER FÖR ATT SÄKERSTÄLLA UPPGIFTERNAS SÄKERHET

MODUL TVÅ: Överföring från personuppgiftsansvarig till personuppgiftsbiträde

MODUL TRE: Överföring från personuppgiftsbiträde till personuppgiftsbiträde

Abbott har infört de tekniska och organisatoriska säkerhetsåtgärder som anges i denna Bilaga II. Syftet är att se till att konfidentialiteten, integriteten, tillgängligheten och motståndskraften i dess system och tjänster för behandling kontinuerligt är säkerställda. Abbott behandlar personuppgifter på servrar i EES som drivs av en branschledande leverantör av molntjänster som erbjuder avancerade tekniska åtgärder till skydd mot obehörig åtkomst.

1. **Kontroll av åtkomst på platser där behandling sker (konfidentialitet):** Följande lämpliga åtgärder vidtas av Abbotts branschledande leverantör av molntjänster för att förhindra obehörig åtkomst till utrustning för databehandling (till exempel telefoner, databas- och applikationsservrar samt tillhörande hårdvara) med vilken personuppgifter behandlas:
 - En mångskiktad säkerhetsmodell vars säkerhetsdetaljer består i bland annat specialanpassade elektroniska tillträdeskort, larm, inträdeshinder för fordon, grindar, metalldetektorer och biometriska kännetecken.
 - Datacentra som övervakas dygnet runt av inomhus- och utomhuskameror med hög upplösning, vilka kan upptäcka och spåra obehöriga personer.
 - Loggåtkomst, aktivitetsregister och kamerainspelningar som finns att tillgå vid inbrott.
 - Fysisk tillträdeskontroll för att förhindra obehörig åtkomst till databehandlingssystem, såsom behörighetsområden och säkerhet i tekniska anordningar. Kontroll av rätten till fysiskt tillträde och av autentisering (till exempel nycklar, ID-kort och chipkort) för säkerhetsutrymmen genomförs som dokumenteras och kontrolleras regelbundet.
2. **Kontroll av åtkomst till databehandlingssystem (konfidentialitet):** Abbott vidtar lämpliga åtgärder för att förhindra att dess databehandlingssystem används av obehöriga personer. Detta sker genom följande:
 - Multifaktorautentisering, inbegripet identitets- och åtkomsthantering som integreras med hårdvara.
 - Begränsad tillgång till tjänster genom kryptering, signaturalgoritmer och säkra certifikat.
 - Data som kommuniceras mellan en användares webbläsare, mobilapplikation, partnerapplikation eller annan tjänsteinteraktion med plattformen krypteras med HTTPS-protokollet och FIPS-certifierade TLS 1.3-chiffer med säkra SSL-certifikat.
 - Data krypteras under överföring, från början till slut och i vila.
 - Lagring av uppgifter i en säker databas som använder kryptering på filnivå. Centrala lagringsmekanismer hindrar leverantören av härbärgeringstjänster från att se uppgifterna.
 - Uppbackning av databaser med olika nycklar från de primära databaserna.

- Loggning av misslyckade försök till autentisering och regelbunden granskning av sådana loggar.
- Använder kryptering och lösenordskrav enligt branschstandard (till exempel, minimilängd, användning av specialtecken osv.).
- Blockering av tillgång efter misslyckade försök eller inaktiva perioder samt en metod för att återställa blockerad tillgång.

3. **Kontroll av åtkomst för användning av vissa områden av databehandlingssystem**

(konfidentialitet): De ur Abbotts personal som får använda databehandlingssystem har endast tillgång till personuppgifter om de har tillräckligt omfattande tillstånd för detta. Krypterade personuppgifter kan inte läsas, kopieras, ändras eller raderas utan tillstånd. Detta sker genom följande:

- Åtkomst begränsas utifrån roller och ansvar och bibehålls genom tillstånd på organisationsnivå.
- Privilegier tilldelas efter behov och från händelse till händelse.
- Tillträdesförfrågningar och ändringar av åtkomst övervakas och behålls.
- Tillträdeskontroller är alltid inställda på "ingen åtkomst" om det inte specifikt krävs.
- Lösenord skyddat; unikt användarnamn och lösenordskrav; multifaktorautentisering aktiverad; Trafiken kontrolleras genom AWS säkerhetsgrupper.
- Rätten till åtkomst ses över med jämna mellanrum i syfte att se till att korrekta rättigheter har beviljats. Rätten till åtkomst upphör när roller och ansvar ändras, däribland när anställningen upphör.
- Effektiva disciplinära åtgärder vidtas mot personer som utan behörighet kommer åt personuppgifter.

4. **Kontroll av överföring (integritet).** Abbott genomför åtgärder för att förhindra att personuppgifter läses, kopieras, ändras eller tas bort av obehöriga personer under överföring eller transport av uppgifterna. Detta sker genom följande:

- Överföringen av uppgifter är krypterad, krypteringen sker på serversidan.
- Servrarna är lokaliserade i ett virtuellt privat moln och använder ett säkert nät som endast kan nås via certifikatbaserad autentisering som begränsar trafik till endast https.
- Data som kommuniceras mellan en användares webbläsare, mobilapplikation, partnerapplikation eller annan tjänsteinteraktion med plattformen krypteras med HTTPS-protokollet och FIPS-certifierade TLS 1.3-chiffer med säkra SSL-certifikat.
- Data i vila krypteras med AES-256.
- Lagring av personuppgifter på bärbara lagringsmedia för transport och på bolagets bärbara datorer och andra mobila enheter undviks såvida inte personuppgifterna är krypterade.
- Minimering av risker genom nätavstängning.
- Viktiga programfixar för säkerhet implementeras inom 30 dagar efter att de gjorts tillgängliga.

5. **Kontroll av registrering (integritet).** Abbott tillträder inte den professionella användarens innehåll såvida det inte är nödvändigt för att förse användaren med de produkter och tjänster som denne har valt. Abbott tillträder inte den professionella användarens innehåll i syften andra än dem som anges i

användarvillkoren och detta biträdesavtal. Därför vet inte Abbott vilket innehåll den professionella användaren lagrar på systemen och kan inte skilja mellan personuppgifter och annat innehåll. Följaktligen behandlar Abbott den professionella användarens hela innehåll på samma sätt. På detta sätt har den professionella användarens hela innehåll samma säkerhetsnivå, oberoende av huruvida detta innehåll består av personuppgifter eller inte.

Abbott genomför lämpliga åtgärder för att se till att det går att verifiera och fastställa att inga personuppgifter har förts in i eller tagits bort från databehandlingssystemen. Detta sker genom följande:

- Skyddsåtgärder för läsning, ändring och radering av lagrade uppgifter.
 - Dokumentation för att kontrollera vilka personer som är auktoriserade och ansvariga för att föra in uppgifter i databehandlingssystem på grundval av deras arbetsuppgifter.
 - Protokoll som kräver loggning av eventuell inmatning och/eller radering av personuppgifter.
6. **Kontroll av order.** När personuppgifter behandlas, vidtar Abbott åtgärder för att se till att dessa hanteras helt i linje med den professionella användarens anvisningar. Detta sker genom följande:
- Tydliga anvisningar till Abbott om omfattningen på den begärda behandlingen av personuppgifterna i enlighet med användarvillkoren och detta biträdesavtal. Detta begränsas till särskilda krav för utveckling av den professionella användarens system och databashantering (till exempel framtagning av nya rapportmallar för vilka uppgifter måste behandlas så att dessa mallar kan testas).
7. **Kontroll av tillgänglighet (tillgänglighet).** Abbott genomför åtgärder för att se till att personuppgifter skyddas från att oavsiktligt förstöras eller förloras. Detta sker genom följande:
- Regelbunden säkerhetskopiering av uppgifter.
 - Riktlinjer som förbjuder permanent lokal lagring (på arbetsplatsen) av personuppgifter.
 - Införande av en beredskapsplan som innehåller de viktiga åtgärder som ska vidtas och uppgift om vilka personer som ska underrättas om en incident.
8. **Separering av behandling för olika syften.** Abbott genomför åtgärder för att se till att personuppgifter som samlas in för olika syften kan behandlas separat. Detta sker genom följande:
- Databasdriven säkerhet säkerställs genom att patientinformation separeras från glukosinformation med separata krypteringsnycklar på filnivå.
 - Utformning av gränssnitt, processer för satsvis behandling och rapporter endast för specifika syften och funktioner gör att uppgifter som samlats in för särskilda syften kan behandlas separat.
9. **Motståndskraft.** Abbott har genomfört följande tekniska och organisatoriska säkerhetsåtgärder, främst för att se till att dess system och tjänster för behandling är tillförlitliga:
- Policyer och förfaranden för hantering av dataskydd.
 - Dataskyddsfrämjande förinställningar (enligt krav i artikel 25(1) i GDPR).
 - Kontroll av order.

Abbott har också genomfört organisatoriska och tekniska åtgärder med hänsyn till Europeiska dataskyddsstyrelsens rekommendationer 01/2020 samt EU-domstolens "Schrems II" beslut.

Versionshantering				
Dokument	Version	Datum	Ändringar	Ansvarig
Avtal	0.1	2024-10-15		JAX (RV)
Bilaga 1	0.1	2024-10-15	Instruktioner	JAX (RV)
Bilaga 2	0.1	2024-10-15	Utgår, ersätts av Bilaga B	JAX (RV)
Avtal	0.2	2024-10-24	Kommentarer/tillägg Abbott	JAX (RV) ÖL (A)
Bilaga 1	0.2	2024-10-24	Instruktioner Kommentarer/tillägg Abbott	JAX (RV) ÖL (A)
Bilaga A - SCC	0.1	2024-10-24	Standardavtalsklausuler	ÖL (A)
Bilaga B	0.2	2024-10-24	Underentreprenörer SCC	ÖL (A)
Bilaga C	0.1	2024-10-24	Säkerhetsåtgärder Abbott	ÖL (A)
Bilaga 1	0.3	2024-11-12	Instruktioner	JAX/AC (RV)
Bilaga A – SCC	0.3	2024-11-12	Standardavtalsklausuler	JAX/AC (RV)
Bilaga 1	1.0	2024-11-18	Instruktioner	JAX/AC (RV) ÖL (A)
Bilaga A - SCC	1.0	2024-11-18	Standardavtalsklausuler	JAX/AC (RV) ÖL (A)