Ineras personuppgiftsbiträdesavtal 2

Avtal enligt artikel 28.3, Dataskyddsförordningen

Detta avtal har träffats mellan följande parter:

1 Avtalets parter

1.1 Personuppgiftsansvarig (Namn på indirekt ansluten vårdgivare, ansvarig juridisk/fysisk person som är personuppgiftsansvarig, nedan kallad ”Personuppgiftsansvarige” alternativt ”Personuppgiftsansvarig”)

Fullständigt namn	Organisationsnummer

1.2 Personuppgiftsbiträde (Namn på direkt ansluten vårdgivare, ansvarig juridisk/fysisk person och nämnd som är personuppgiftsbiträde, nedan kallad ”Personuppgiftsbiträdet”)

Fullständigt namn	Organisationsnummer

2. Bakgrund och syfte

2.1 Inera AB (fortsättningsvis ”Inera”) ägs gemensamt av Sveriges Kommuner och Landsting (SKL) samt landets landsting och kommuner. Ineras uppdrag är att utveckla och förvalta en nationell tjänsteplattform (Nationella tjänsteplattformen) samt nationella och gemensamma digitala tjänster på ägarnas vägnar. Inera får även upplåta Nationella tjänsteplattformen och specifika digitala tjänster åt både enskilda personer, privata utförare som är anlitade av kommuner och landsting eller bedriver verksamhet självständigt samt statliga myndigheter. Säljverksamhet i offentlig regi begränsas av kommunallagen och konkurrenslagen.

2.2 Inera är en teknisk tillhandahållare av Nationella tjänsteplattformen och digitala tjänster, vilket kan innebära behandling av personuppgifter, där sådana förekommer, enligt uppdrag. Personuppgiftsbehandlingen sker således enbart för de kommuner, landsting och andra aktörer som väljer att ansluta sig till Nationella tjänsteplattformen och/eller aktuella digitala tjänster. Dessa aktörer är normalt personuppgiftsansvariga. Inera hanterar således personuppgifter i rollen som personuppgiftsbiträde.

2,3 När personuppgifter behandlas av ett personuppgiftsbiträde ska enligt Dataskyddsförordningen, artikel 28.3, hanteringen regleras genom ett skriftligt avtal eller annan rättsakt. Detta avtal utgör ett sådant skriftligt avtal som avses i artikel 28.3 i Dataskyddsförordningen, här benämnt ”Personuppgiftsbiträdesavtal 2”.

2.4 En personuppgiftsansvarig får anlita en eller flera personuppgiftsbiträden. En personuppgiftsansvarig får också ge ett anlitat personuppgiftsbiträde en rätt att anlita ett underbiträde. Nationella tjänsteplattformen innehåller tekniska lösningar som låter direkt anslutna landsting, kommuner eller statliga myndigheter till Ineras nationella digitala tjänster att ansluta aktörer indirekt till digitala tjänsterna, t.ex. företag som på uppdrag av ett landsting bedriver offentligt finansierad hälso- och sjukvård. I dessa situationer agerar direktansluten kommun, landsting eller statlig myndighet i rollen som personuppgiftsbiträde i förhållande till den indirekt anslutna aktören som i regel är personuppgiftsansvarig. Direkt och indirekt anslutna aktörer beskrivs närmare i avsnitt 2.

2.5 Landsting, kommuner eller statliga myndigheter som indirekt till andra aktörer upplåter digitala tjänster som tillhandahålls av Inera eller av Inera anlitat underbiträde, har i Ineras Personuppgiftsbiträdesavtal 1 förpliktat sig att teckna detta Personuppgiftsbiträdesavtal 2 mellan sig själv och varje indirekt ansluten juridisk eller fysisk person. Förpliktelsen att teckna Personuppgiftsbiträdesavtal 2 kan inte överföras på Inera. Detta Personuppgiftsbiträdesavtal 2 reglerar således parternas behandling av personuppgifter.

2.6 Enligt Dataskyddsförordningen, artikel 28.2, får ett personuppgiftsbiträde inte anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige. Personuppgiftsansvarige ger härmed Personuppgiftsbiträdet förhandstillstånd att anlita Inera som underbiträde. Förhandstillståndet innefattar också en rätt för Inera att i sin tur att anlita ett eller flera underbiträden. Personuppgiftsbiträdets skyldigheter i denna del regleras närmare under avsnitt 7.

2.7 Personuppgiftsbiträdet åtar sig att behandla personuppgifter, och i förekommande fall även avlidna personers uppgifter, endast i enlighet med detta Personuppgiftsbiträdesavtal 2, tillämplig svensk rätt och Personuppgiftsansvarigs övriga dokumenterade instruktioner samt att vidta de tekniska och organisatoriska åtgärder enligt Dataskyddsförordningen, artikel 32, som krävs för att skydda uppgifterna.

2.8 Detta Personuppgiftsbiträdesavtal 2 syftar också till att reglera parternas skyldigheter och rättigheter i övrigt avseende personuppgiftsbehandlingen. Personuppgiftsbiträdesavtal 2 omfattar all behandling av personuppgifter som Personuppgiftsbiträdet utför för den Personuppgiftsansvariges räkning med begräsning till de digitala tjänster som den Personuppgiftsansvarige indirekt anslutit sig till.

3. Direkt och indirekt anslutna aktörer

3.1 Myndigheter och enskilda som är direkt anslutna till Nationella tjänsteplattformen och/eller nationella digitala tjänster ska teckna Ineras Personuppgifts-biträdesavtal 1. I de fall en myndighet eller enskild är indirekt ansluten till Nationella tjänsteplattformen och/eller digitala tjänster genom ett landsting, en kommun eller en statlig myndighet, anses enligt Ineras Personuppgiftsbiträdesavtal 1 landstinget, kommunen eller den statliga myndigheten agera i rollen som personuppgiftsbiträde åt den indirekt anslutne.

3.2 Landsting, kommuner eller statliga myndigheter som tecknar Ineras Personuppgiftsbiträdesavtal 1 med Inera, och som indirekt till andra aktörer upplåter digitala tjänster som tillhandahålls av Inera eller av Inera anlitat underbiträde, förpliktar sig att teckna detta Personuppgiftsbiträdesavtal 2 mellan sig själv och varje indirekt ansluten juridisk eller fysisk person. Förpliktelsen att teckna Personuppgiftsbiträdesavtal 2 kan inte överföras på Inera.

3.3 Personuppgiftsbiträdesavtal 2 är ett standardiserat personuppgiftsbiträdesavtal som är framtaget av Inera och innehåller motsvarande villkor för personuppgiftsbehandling som framgår av Ineras Personuppgiftsbiträdesavtal 1.

3.4 Landsting, kommuner eller statliga myndigheter som tecknar föreliggande Personuppgiftsbiträdesavtal 2 med indirekt anslutna aktörer ska informera Inera om vilka myndigheter eller enskilda som är indirekt anslutna till en tjänst samt varje förändring avseende indirekt anslutna aktörer.

4. Begrepp och termer som används i Personuppgiftsbiträdesavtal 2

4.1 Med *behandling av personuppgifter* avses en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring (artikel 4.2 Dataskyddsförordningen).

4.2 Med *regionala och nationellt kvalitetsregister* avses en automatiserad och strukturerad samling av personuppgifter som inrättats särskilt för ändamålet att systematiskt och fortlöpande utveckla och säkra vårdens kvalitet. Kvalitetsregistren ska möjliggöra jämförelse inom hälso- och sjukvården på nationell eller regional nivå.

4.3 Med *Personuppgiftsansvarig* avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter (artikel 4.7 Dataskyddsförordningen).

4.4 Med *Personuppgiftsbiträde* avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning (artikel 4.8 Dataskyddsförordningen).

4.5 Med *personuppgifter* avses varje upplysning som avser en identifierad eller identifierbar fysisk person (registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet (artikel 4.1 Dataskyddsförordningen).

4.6 Med *personuppgiftsincident* avses 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 (se artikel 4.12 i Dataskyddsförordningen).

4.7 Med *Sammanhållen journalföring* avses ett elektroniskt system, som gör det möjligt för en vårdgivare att ge eller få direktåtkomst till personuppgifter hos en annan vårdgivare.

4.8 Med *registrerad* avses den som personuppgiften avser.

5. Ändamål och omfattning

5.1 Personuppgiftsbiträdet får endast enligt dokumenterade instruktioner utföra den behandling av personuppgifter som är nödvändig för att fullgöra sitt uppdrag åt den Personuppgiftsansvarige, till exempel, men inte begränsat till,

- hälso- och sjukvård,
- socialtjänst,
- förskola, grund- och gymnasieutbildning,
- samhällsbyggnad,
- personal- och ekonomiadministration
- person-, adress- och behörighetskontroll

5.2 Utöver detta Personuppgiftsbiträdesavtal 2 ska Personuppgiftsbiträdet följa de närmare instruktioner om och villkor för personuppgiftsbehandlingen som den Personuppgiftsansvarige bestämmer i avtal eller överenskommelse med Personuppgiftsbiträdet om upplåtelse av Ineras digitala tjänster.

5.3 Behandlingens art, omfattning, varaktighet, föremålet för behandlingen, ändamål, typen av personuppgifter och kategorier av registrerade som omfattas av personuppgiftsbehandlingen framgår av avtal om Ineras digitala tjänster mellan Personuppgiftsansvarige och Personuppgiftsbiträdet och kompletterande instruktioner till det avtalet.

5.4 För det fall att Personuppgiftsbiträdet bedömer att det saknas instruktioner som är nödvändiga för att genomföra uppdraget enligt detta Personuppgifts-biträdesavtal 2 eller bedömer att lämnade instruktioner strider mot gällande rätt ska Personuppgiftsbiträdet utan dröjsmål informera den Personuppgifts-ansvarige om sin inställning, ange om fullgörandet av uppdraget kan påverkas av behovet av instruktioner samt invänta vidare instruktioner från den Personuppgiftsansvarige.

5.5 Personuppgiftsbiträdet får enligt artikel 28.3 a) Dataskyddsförordningen endast överföra personuppgifter till ett tredjeland eller en internationell organisation med stöd av skriftliga instruktioner från den Personuppgiftsansvarige, såvida inte överföringen krävs enligt unionsrätten eller svensk rätt. I sådant fall ska Personuppgiftsbiträdet informera den Personuppgiftsansvarige om den rättsliga skyldigheten innan uppgifterna överförs, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt unionsrätten eller svensk rätt.

6. Allmänna Instruktioner för centrala tjänster

6.1 Vissa digitala tjänster är centrala för hälso- och sjukvårdens aktörer och följer patientdatalagens (2008:355) bestämmelser. De centrala tjänsterna innefattar bl.a. behandling av känsliga personuppgifter för hälso- och sjukvårdsändamål. Som exempel kan nämnas följande tjänster.

- System innebärande sammanhållen journalföring inklusive Nationell Patientöversikt
- Försäkringsmedicinska utredningar
- Kvalitetsregisterregistrering
- Vården i siffror och Öppna Data
- Journalen
- 1177 Vårdguidens e-tjänster

6.2 Personuppgiftsbiträdet ska på begäran av den Personuppgiftsansvarige tillhandahålla en lättillgänglig information om vilka vårdgivare som är direkt och indirekt anslutna till Sammanhållen journalföring. Personuppgiftsbiträdet får i denna del hänvisa den Personuppgiftsansvarige till Inera. I övrigt gäller för Personuppgiftsbiträdets personuppgiftsbehandling instruktionerna i detta Personuppgiftsbiträdesavtal 2 och i förekommande fall avtal om digitala tjänster mellan Personuppgiftsansvarig och Personuppgiftsbiträde och kompletterande instruktioner till det avtalet.

6.3 Personuppgiftsbiträdet får sammanställa och registrera patientuppgifter som en vårdgivare valt att lämna ut till ett regionalt eller nationellt kvalitetsregister. Sammanställning och registrering sker för de ändamål som framgår av 7 kap. 4 och 5 §§ patientdatalagen (2008:355). I övrigt gäller instruktionerna i detta Personuppgiftsbiträdesavtal 2.

7. Överlåtelse av personuppgiftsbehandling till ett underbiträde

7.1 Enligt punkt 3.6 äger Personuppgiftsbiträdet en rätt att anlita Inera som underbiträde avseende behandling av den Personuppgiftsansvariges personuppgifter samt tillåta Inera att anlita en eller flera underbiträden. Denna rätt utgör såväl ett särskilt som ett allmänt skriftligt förhandstillstånd" som framgår av artikel 28.2 Dataskyddsförordningen. Det särskilda förhandstillståndet innefattar endast en rätt för Personuppgiftsbiträdet att anlita Inera (och således inte Ineras underleverantörer) som underbiträde. Personuppgiftsbiträdet ska informera den Personuppgiftsansvarige om Ineras eventuella planer på att anlita underbiträden eller byta ut befintliga underbiträden så att den Personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar. En sådan invändning ska göras senast 10 dagar från det att Personuppgiftsbiträdet informerade den Personuppgiftsansvarige. Information om underbiträden som Inera har fått anlita med stöd av detta och andra förhandstillstånd lämnas på Ineras hemsida.

7.2 Enligt Dataskyddsförordningen, artikel 28.4, ska i de fall där ett personuppgiftsbiträde anlitar ett annat personuppgiftsbiträde för utförande av specifik behandling på den personuppgiftsansvariges vägnar, det andra personuppgiftsbiträdet, genom ett avtal eller en annan rättsakt enligt unionsrätten eller enligt medlemsstaternas nationella rätt, åläggas samma skyldigheter i fråga om dataskydd som de som fastställs i avtalet eller den andra rättsakten mellan den personuppgiftsansvarige och personuppgiftsbiträdet. Personuppgiftsbiträdet ska också särskilt tillse att artikel 28.2 och 28.4 i Dataskyddsförordningen beaktas vid anlitande av ett underbiträde samt tillse att underbiträdet ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i Dataskyddsförordningen. Personuppgiftsbiträdet intygar härmed att de skyldigheter om dataskydd som framgår av detta Personuppgiftsbiträdesavtal 2 har ålagts Inera genom tecknande av Ineras Personuppgiftsbiträdesavtal 1 med Inera.

7.3 Personuppgiftsbiträdet ska oaktat föregående punkt vara fullt ansvarig gentemot den Personuppgiftsansvarige för utförandet av skyldigheterna enligt detta Ineras Personuppgiftsbiträdesavtal 2.

7.4 I avtal som Personuppgiftsbiträdet träffar med Inera, enligt Ineras Personuppgiftsbiträdesavtal 1, ska Personuppgiftsbiträdet förplikta Inera att i avtal som Inera träffar med ett underbiträde ange att en begäran till Ineras underbiträden om utlämnade av en handling eller en uppgift som den Personuppgiftsansvarige ansvarar för omedelbart ska överlämnas till Inera, och att underbiträdet inte i något sammanhang själv får hantera en sådan begäran. Inera ska åläggas skyldighet i avtal att snarast överlämna begäran till Personuppgiftsbiträdet, och Personuppgiftsbiträdet sin tur ska överlämna begäran till Personuppgiftsansvarig och avvakta vidare instruktioner från Personuppgiftsansvarige.

7.5 Personuppgiftsbiträdets uppgifter ska vid överföring till Inera ha ett adekvat skydd i form av kryptering. Personuppgiftsbiträdet ska säkerställa i avtal att motsvarande skydd iakttas av Inera vid överföring av uppgifter till Ineras underbiträde. Inera personal omfattas av en lagreglerad tystnadsplikt. Personuppgiftsbiträdet ska därför säkerställa att Inera erinrar sin personal om aktuella sekretess- och tystnadspliktbestämmelser som Inera och dess personal ska iaktta. Sekretessförbindelse med personalen krävs inte eftersom de omfattas av lagreglerad tystnadsplikt. Omfattas Ineras underbiträde inte av en lagstadgad tystnadsplikt, ska Personuppgiftsbiträdet säkerställa i avtal att Inera tecknar sekretessavtal med underbiträdet och tillse att det finns sekretessförbindelser mellan underbiträdet och underbiträdets egen personal.

7.6 Om Inera eller av Inera anlitade underbiträden inte uppfyller sina skyldigheter i fråga om dataskydd enligt Ineras Personuppgiftsbiträdesavtal 1 ska Personuppgiftsbiträdet förbli fullt ansvarig gentemot den Personuppgiftsansvarige för Ineras uppfyllande av sina skyldigheter enligt föreliggande Personuppgiftsbiträdesavtal 2.

7.7 Upphör detta Ineras Personuppgiftsbiträdesavtal 2 att gälla får Personuppgiftsbiträdet eller ett underbiträde inte fortsätta behandla personuppgifter som omfattas av detta Personuppgiftsbiträdesavtal 2. Rätten för Personuppgiftsbiträdet att anlita Inera som underbiträde upphör, liksom Ineras rätt att anlita underbiträden. Förvarar Personuppgiftsbiträdet och dess underbiträden händelsevis personuppgifter ska personuppgifterna i ett sådant fall återlämnas till den Personuppgiftsansvarige eller raderas i enlighet med punkten 9.12 nedan.

8. Personuppgiftsbiträdets allmänna åtaganden

8.1 Personuppgiftsbiträdet förbinder sig att följa Dataskyddsförordningen samt andra vid var tid gällande tillämpliga registerförfattningar med avseende på behandling av personuppgifter.

8.2 Personuppgiftsbiträdet och dess underbiträden är tekniska tillhandahållare av Nationella tjänsteplattformen och nationella digitala tjänster. Personuppgiftsbiträdet och underbiträden får därför inte utan tillåtelse av den Personuppgiftsansvarige ta del av personuppgifter som behandlas för den Personuppgiftsansvariges räkning.

8.3 Personuppgiftsbiträdet och dess underbiträden har emellertid, oaktat punkten 8.2, tillåtelse av den Personuppgiftsansvarige att ta del av den Personuppgiftsansvariges data i Nationella tjänsteplattformen, digitala tjänster och i loggar, inklusive personuppgifter, för felsökning, driftskontroll, support och statistik, liksom för att utreda missbruk eller analysera intrång, om det är oundgängligen nödvändigt för att tillhandahålla tjänsten och om andra, mindre ingripande åtgärder av hänsyn till den personliga integriteten är uttömda.

8.4 Personuppgiftsbiträdet och dess underbiträden får vidare ta del av den Personuppgiftsansvariges uppgifter, inklusive personuppgifter, för att upprätthålla en förteckning över anslutna organisationer till Ineras tjänster samt upprätthålla kravet i artikel 30.2 Dataskyddsförordningen på ett register över alla kategorier av behandling som utförts för den Personuppgiftsansvariges räkning.

8.5 Personuppgiftsbiträdet och dess underbiträden får också behandla personuppgifter om den Personuppgiftsansvariges personal och uppdragstagare. Sådana personuppgifter är t.ex. uppgifter avseende namn, personnummer, mobiltelefonnummer, e-postadress, IP-adress och andra anteckningar. Sådana personuppgifter behandlas för att Personuppgiftsbiträdet och dess underbiträden ska kunna fullfölja avtal om tjänsten samt för administration, inklusive säkerhetsadministration.

8.6 Personuppgiftsbiträdet ska med hänsyn till arten av känsliga personuppgifter som finns hos vårdgivare och utförare av socialtjänst samt för att säkerställa att den Personuppgiftsansvarige kan leva upp till författningsenliga krav på en god kontroll över skyddet för personuppgifterna behandla dessa på utrustning som fysiskt befinner sig i Sverige. Även service – och supporttjänster ska tillhandahållas i Sverige. Personuppgiftsbiträdet ska ålägga Inera skyldighet att säkerställa att kravet i denna punkt beaktas vid upphandling av underbiträde för behandling av personuppgifter. På behandlingen ska svensk rätt vara tillämplig, bl.a. Dataskyddsförordningen.

8.7 Den Personuppgiftsansvarige har rätt att på egen bekostnad själv eller genom tredje man kontrollera att Personuppgiftsbiträdet följer detta Ineras Personuppgiftsbiträdesavtal 2. Personuppgiftsbiträdet och dess underbiträden, bl.a. Inera, ska därvid lämna den Personuppgiftsansvariges representanter den assistans som behövs. Den Personuppgiftsansvariges representanter ska ha rätt till inspektion av den hårdvara och mjukvara som används för behandling av personuppgifter som omfattas av detta Ineras Personuppgiftsbiträdesavtal 2 samt tillträde till de fysiska lokaler där utrustning och annan hård- och mjukvara finns. Personuppgiftsbiträdet och dess underbiträden ska säkerställa att kravet på kontroll enligt denna punkt beaktas vid upphandling av underleverantör för behandling av personuppgifter. Vid Personuppgiftsansvarigs utövande av kontroll enligt denna klausul ska Personuppgiftsbiträdet eller dess underbiträden informera andra Personuppgiftsansvariga som använder Ineras digitala tjänster om vem som genomfört kontrollen och tidpunkt.

8.8 Personuppgiftsbiträdet och dess underbiträden ska ge den Personuppgiftsansvarige tillgång till all information som krävs för att visa att skyldigheterna i artikel 28 Dataskyddsförordningen i rollen som personuppgiftsbiträde har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den Personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige. Personuppgiftsbiträdet ska omedelbart informera den Personuppgiftsansvarige om Personuppgiftsbiträdet anser att en instruktion strider mot Dataskyddsförordningen eller svensk rätt.

8.9 Personuppgiftsbiträdet och dess underbiträden ska utan dröjsmål informera den Personuppgiftsansvarige om eventuella kontakter från Integritetsskyddsmyndigheten eller andra tillsynsmyndigheter som rör eller kan vara av betydelse för behandling av personuppgifter. Personuppgiftsbiträdet och dess underbiträden har inte rätt att företräda den Personuppgiftsansvarige eller agera för dennes räkning gentemot Integritetsskyddsmyndigheten eller annan myndighet eller annan tredje man.

8.10 Personuppgiftsbiträdet och dess underbiträden ska hjälpa den Personuppgiftsansvarige, genom lämpliga tekniska och organisatoriska åtgärder att, i den mån detta är möjligt, och med beaktande av behandlingens art, fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter i enlighet med 3 kap. i Dataskyddsförordningen i den utsträckning dessa är tillämpliga.

8.11 Personuppgiftsbiträdet och dess underbiträden ska bistå den Personuppgiftsansvarige med att se till att skyldigheterna enligt artiklarna 32–36 i Dataskyddsförordningen fullgörs, med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå.

8.12 Personuppgiftsbiträdet och dess underbiträden ska när detta Ineras Personuppgiftsbiträdesavtal 2 upphör att gälla, beroende på vad den Personuppgiftsansvarige väljer, radera eller återlämna samtliga personuppgifter på av den Personuppgiftsansvarige angivet lagringsmedium och se till att det inte finns några personuppgifter kvar i sina egna system, såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller svensk rätt.

8.13 Den Personuppgiftsansvarige ska ersätta Personuppgiftsbiträdet eller det underbiträde som Personuppgiftsbiträdet anvisar till för sådant arbete och kostnader som följer av punkterna 8.10, 8.11 och 8.12. Den Personuppgiftsansvarige förbinder sig att följa Ineras vid var tid gällande prislista för sådant arbete och kostnader. Prislistan finns publicerad på Ineras hemsida.

9. Personuppgiftsansvarigs allmänna åtaganden

9.1 Den Personuppgiftsansvarige åtar sig att se till att Dataskyddsförordningens, samt övriga relevanta, vid var tid gällande, författningsbestämmelser efterlevs beträffande behandling av personuppgifter. Den Personuppgiftsansvarige ansvarar bland annat för att informera registrerade om behandlingen och för att i de fallen så krävs inhämta samtycke från den registrerade.

9.2 Den Personuppgiftsansvarige ska omedelbart informera Personuppgiftsbiträdet om förändringar i behandlingen vilka påverkar Personuppgiftsbiträdets skyldigheter enligt dataskyddsförordningen.

10. Förvaring av handling, offentlighet och utlämnande av handling

10.1 Landsting, kommuner och statliga myndigheter som agerar som personuppgiftsbiträde enligt detta Ineras Personuppgiftsbiträdesavtal 2 har att iaktta offentlighets- och sekretesslagens (2009:400) bestämmelser. Det innebär att Personuppgiftsbiträdets anställda och uppdragstagare omfattas av sekretess och tystnadsplikt med avseende på bl.a. uppgifter om hälsa och sexualliv (se 21 kap. 1 § offentlighets- och sekretesslagen) och personliga och ekonomiska förhållanden i den verksamhet som avser enbart teknisk bearbetning och teknisk lagring (40 kap. 5 § offentlighets- och sekretesslagen). Landsting och kommuner utövar vidare ett rättsligt bestämmande inflytande över Inera enligt 2 kap. 3 § offentlighets- och sekretesslagen. Det innebär att Ineras anställda och uppdragstagare också omfattas av en lagreglerad tystnadspliktmed avseende på bl.a. uppgifter om hälsa och sexualliv samt personliga och ekonomiska förhållanden i den verksamhet som avser enbart teknisk bearbetning och teknisk lagring.

10.2 Den Personuppgiftsansvarige ansvarar självständigt för att bedöma om det med beaktande av sekretess- och tystnadspliktsbestämmelser är lämpligt att låta Personuppgiftsbiträdet och dess underbiträden hantera uppgifter inom ramen för de tjänster som upplåtits.

10.3 Personuppgiftsbiträdet och dess underbiträden ansvarar för att egen personal och fysiska uppdragstagare har god kännedom om den sekretess och tystnadsplikt som kan gälla för de uppgifter som behandlas av Personuppgiftsbiträdet för den Personuppgiftsansvariges räkning. För det fall att registrerad, Integritetsskyddsmyndigheten, annan myndighet eller annan tredje man begär information från Personuppgiftsbiträdet som rör behandling av personuppgifter ska Personuppgiftsbiträdet eller dess underbiträden hänvisa till den Personuppgiftsansvarige. Det följer bl.a. av punkten 5.4 ovan att Personuppgiftsbiträdet inte får lämna ut personuppgifter om sådan behandling av personuppgifter som specifikt rör den Personuppgiftsansvarige utan skriftlig instruktion från den Personuppgiftsansvarige.

10.4 Personuppgiftsbiträdet och dess underbiträden ska bereda Riksarkivet, i egenskap av arkivmyndighet, och i förekommande fall arkivmyndighet hos den Personuppgiftsansvarige, möjlighet att kontrollera eventuella arkivbestämmelsers efterlevnad.

11. Säkerheten vid behandling av personuppgifter

11.1 Personuppgiftsbiträdet och dess underbiträden ska, med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter, vidta skäliga tekniska, administrativa och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt

a. pseudonymisering och kryptering av personuppgifter,
b. förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystem och digitala tjänster,
c. förmågan att återställa tillgänglighet och tillgång till personuppgifter i rimlig tid vid en fysisk eller teknisk incident, och
d. ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet; villkor för test och utvärdering av säkerheten framgår av avtal mellan den Personuppgiftsansvarige och Personuppgiftsbiträdet.

11.2 Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från 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.

11.3 Enligt artikel 28.5 Dataskyddsförordningen får ett personuppgiftsbiträde ansluta sig till en godkänd uppförandekod som avses i artikel 40 eller en godkänd certifieringsmekanism som avses i artikel 42 för att visa att tillräckliga garantier för dataskydd tillhandahålls, såsom avses i artikel 28.1 och 28.4 Dataskydds-förordningen. Personuppgiftsbiträdet och dess underbiträden är fria att ansluta sig till antingen en godkänd uppförandekod eller en godkänd certifierings-mekanism, med stöd av artikel 32 i Dataskyddsförordningen, för att visa att kraven i punkten 11.1 ovan följs.

Behörighetstilldelning

11.4 Personuppgiftsbiträdet och dess underbiträden ska ansvara för att det finns rutiner för tilldel-ning, förändring, borttagning och regelbunden uppföljning av den egna personalens och uppdragstagares behö-righeter för åtkomst till den Personuppgiftsansvariges personuppgifter, när det är tillåtet enligt detta Ineras Personuppgiftsbiträdesavtal 2.

Loggning

11.5 Se punkt 11.12.

Säkerhetskopiering

11.6 Personuppgiftsbiträdet och dess underbiträden ska ha rutiner för säkerhetskopiering av personuppgifter i ett allmänt erkänt och strukturerat format. Om detta Ineras Personuppgiftsbiträdesavtal 2 upphör gäller vad som framgår av punkt 8.12.

Elektronisk informationsöverföring

11.7 Personuppgiftsbiträdet och dess underbiträden ska vid elektronisk överföring av personuppgifter från eller till den Personuppgiftsansvarige skydda uppgifterna på ett adekvat sätt med hänsyn till personuppgifternas känslighet och art när de kommuniceras.

Drift och underhåll

11.8 Innan Personuppgiftsbiträdet och dess underbiträden driftsätter sina system för mottagande eller utlämnande av information enligt detta Ineras Personupp-giftsbiträdesavtal 2 ska systemen kvalitetssäkras genom tester och riskanalyser i testmiljö. I övrigt ska Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården beaktas.

11.9 Om Personuppgiftsbiträdet eller dess underbiträden avser att göra förändringar i sitt system (uppgradering, patchning etc.) på sätt som kan förväntas påverka informationshanteringen ska Personuppgiftsbiträdet eller dess underbiträden underrätta den Personuppgiftsansvarige om detta. Sådan information ska lämnas i god tid före förändringen.

Driftstörningar

11.10 Driftsäkerhet samt avhjälpande av fel eller brist regleras inte i detta Ineras Personuppgiftsbiträdesavtal 2.

11.11 Intrångsförsök eller annat bedrägligt förfarande för att få åtkomst till den Personuppgiftsansvariges personuppgifter ska utan dröjsmål, dock senast timmar från att incidenten upptäcktes, anmälas av Personuppgiftsbiträdet till den Personuppgiftsansvarige (personuppgiftsincident). Inga ändringar (omstart, uppgraderingar, felsökningar) får normalt vidtas utan samråd med den andra parten. Övriga personuppgiftsincidenter anmäls av Personuppgiftsbiträdet utan onödigt dröjsmål, dock senast timmar från att incidenten upptäcktes, till den Personuppgiftsansvarige enligt artikel 33 i Dataskyddsförordningen. Anmälningar om personuppgiftsincidenter av Personuppgiftsbiträdets underbiträden ska också rapporteras till den Personuppgiftsansvarige.

11.12 Personuppgiftsbiträdet och dess underbiträden åtar sig att kontinuerligt logga åtkomst till personuppgifter enligt detta Ineras Personuppgiftsbiträdesavtal 2. Personuppgiftsbiträdet och dess underbiträden ska ansvara för att

1. det av dokumentationen av åtkomsten (loggar) framgår vilka åtgärder som har vidtagits med uppgifter om en registrerad person,
2. det av loggarna framgår vid vilken enhet åtgärderna vidtagits,
3. det av loggarna framgår vid vilken tidpunkt åtgärderna vidtagits,
4. användarens och den registrerades identitet framgår av loggarna,
5. systematiska och återkommande stickprovskontroller av loggarna görs, och
6. kontroller av loggarna dokumenteras.

Loggarna ska ha ett adekvat säkerhetsskydd. Loggar får gallras först fem (5) år efter loggningstillfället. Loggen ska lämnas ut till den Personuppgiftsansvarige om detta Ineras Personuppgiftsbiträdesavtal 2 upphör att gälla.

12. Ersättning

12.1 Ersättning för tjänster enligt detta Ineras Personuppgiftsbiträdesavtal 2 regleras i punkten 8.13.

13. Ansvar mot registrering av skada

13.1 För parternas ansvar och ansvarsbegränsningar för skada med avseende på behandling av personuppgifter och dataskydd bestämmer parterna följande:

13.2

Parternas ansvar regleras i enlighet med artikel 82 och 83 i Dataskyddsförordningen 2016/679.

14. Avtalstid

14.1 Detta Ineras Personuppgiftsbiträdesavtal 2 gäller från dess undertecknande och så länge som Personuppgiftsbiträdet har ett uppdrag från den Personuppgiftsansvarige att behandla personuppgifter för dennes räkning.

15. Tvist

15.1 Tvist angående tolkning eller tillämpning av detta Ineras Personuppgiftsbiträdesavtal 2 ska avgöras av

Eventuell tvist i anledning av detta avtal som parterna inte kan lösa på egen hand ska avgöras av svensk allmän domstol.

Svensk rätt ska äga tillämpning på tvisten.

16. Undertecknanden

Ort och datum	
För Personuppgiftsbiträdet	Namnförtydligande samt befattning
Ort och datum	
För Personuppgiftsansvarig	Namnförtydligande och befattning