Ineras Personuppgiftsbiträdesavtal 1

Avtal enligt artikel 28.3, Dataskyddsförordningen

Innehåll

1. Bakgrund och syfte

1.1 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.

1.2. 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.

1.3. När personuppgifter behandlas av ett personuppgiftsbiträde ska enligt Dataskyddsförordningen, artikel 28.3, hanteringen regleras genom ett skriftligt avtal eller någon annan rättsakt. Parternas reglering i detta avtal utgör ett sådant skriftligt avtal som avses i artikel 28.3 Dataskyddsförordningen, här benämnt ”Ineras Personuppgiftsbiträdesavtal 1”.

1.4. Ineras Personuppgiftsbiträdesavtal 1 reglerar i huvudsak följande:

- Ineras hantering och skydd av personuppgifter inom ramen för bolagets drift och förvaltning av Nationella tjänsteplattformen och/eller nationella digitala tjänster.
- Rättigheter och skyldigheter för Inera om Inera själv anlitar ett underbiträde.
- Ineras behandling av personuppgifter i vissa centrala tjänster (se avsnitt 5).

1.5. Inera åtar sig att behandla personuppgifter, och i förekommande fall även avlidna personers uppgifter, i enlighet med detta Ineras Personuppgiftsbiträdesavtal 1, tillämplig svensk rätt och Personuppgiftsansvarigs övriga instruktioner samt att vidta de tekniska och organisatoriska åtgärder enligt artikel 32 Dataskyddsförordningen, som krävs för att skydda uppgifterna.

1.6. Detta Ineras Personuppgiftsbiträdesavtal 1 syftar också till att reglera parternas skyldigheter och rättigheter i övrigt för personuppgiftsbehandlingen. Ineras Personuppgiftsbiträdesavtal 1 omfattar all behandling av personuppgifter som Inera utför för den Personuppgiftsansvariges räkning med begräsning till de digitala tjänster som den Personuppgiftsansvarige valt att använda.

2. Direkt och indirekt anslutna aktörer

2.1. Myndigheter och enskilda som är direkt anslutna till Nationella tjänsteplattformen och/eller nationella digitala tjänster ska teckna föreliggande Ineras Personuppgiftsbiträdesavtal 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 detta Ineras Personuppgiftsbiträdesavtal 1 landstinget, kommunen eller den statliga myndigheten agera i rollen som personuppgiftsbiträde åt den indirekt anslutne (se Ineras Allmänna villkor).

2.2. Landsting, kommuner eller statliga myndigheter som tecknar föreliggande Personuppgiftsbiträdesavtal med Inera, och som indirekt till andra aktörer upplåter digitala tjänster som tillhandahålls av Inera eller av Inera anlitat underbiträde, förpliktar sig att teckna Ineras Personuppgiftsbiträdesavtal 2 mellan sig själv och varje indirekt ansluten juridisk eller fysisk person (se vidare punkt 2.3). Förpliktelsen att teckna Ineras Personuppgiftsbiträdesavtal 2 kan inte överföras på Inera.

2.3. Ineras Personuppgiftsbiträdesavtal 2 är ett standardiserat personuppgiftsbiträdesavtal som är framtaget av Inera och innehåller motsvarande rättigheter och skyldigheter för personuppgiftsbehandling som framgår av föreliggande Ineras Personuppgiftsbiträdesavtal. I syfte att säkerställa en kontinuerlig och rättssäker kedja av behandling av personuppgifter innehåller Ineras Personuppgiftsbiträdesavtal 2 ett godkännande från den indirekt anslutna aktören till den direkt anslutna aktören att anlita Inera som personuppgiftsbiträde samt en rätt för Inera att i sin tur anlita underbiträden.

2.4. Landsting, kommuner eller statliga myndigheter som tecknar detta Ineras Personuppgiftsbiträdesavtal 1 med Inera, och som indirekt till andra aktörer upplåter digitala tjänster som tillhandahålls av Inera eller av Inera anlitad leverantör, ska informera Inera om vilka myndigheter eller enskilda som är indirekt anslutna till en tjänst samt varje förändring avseende indirekt anslutna aktörer.

3. Begrepp och termer som används i Ineras Personuppgiftsbiträdesavtal

3.1. 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).

3.2. 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.

3.3. 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).

3.4. 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). I föreliggande fall är Inera personuppgiftsbiträde.

3.5. 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).

3.6. 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).

3.7. 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.

3.8. Med *registrerad* avses den som personuppgiften avser.

4. Ändamål och omfattning

4.1. Inera får endast enligt dokumenterade instruktioner från den Personuppgiftsansvarige 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

4.2. Utöver detta Ineras Personuppgiftsbiträdesavtal 1 ska Inera följa de närmare instruktioner om och villkor för personuppgiftsbehandlingen som den Personuppgiftsansvarige bestämmer i kundavtal med Inera om en specifik e-tjänst. Inera ska även iaktta kompletterande instruktioner som den Personuppgiftsansvarige bilägger ett kundavtal och instruktioner i särskilda fall.

4.3. Behandlingens art, omfattning, varaktighet, föremålet för behandlingen, ändamål, typen av personuppgifter och kategorier av registrerade som omfattas av personuppgiftsbehandlingen framgår av kundavtal som Personuppgiftsansvarig tecknar med Inera och kompletterande instruktioner till kundavtal.

4.4. För det fall att Inera bedömer att det saknas instruktioner som är nödvändiga för att genomföra uppdraget enligt detta Ineras Personuppgiftsbiträdesavtal 1 eller bedömer att lämnade instruktioner strider mot gällande rätt ska Inera utan dröjsmål informera den personuppgiftsansvarige om sin inställning, ange om fullgörandet av uppdraget kan påverkas av behovet av instruktioner samt invänta vidare instruktioner från den personuppgiftsansvarige.

4.5. Inera får enligt art 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 Inera 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.

5. Allmänna instruktioner för centrala tjänster

5.1. 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 på centrala tjänster 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
- Elektroniskt utlämnande till individen själv

5.2. Inera får för den Personuppgiftsansvariges räkning behandla bl.a. känsliga personuppgifter för ändamål som anges i kundavtal.

5.3. Inera förbinder sig att löpande tillhandahålla en lättillgänglig information om vilka vårdgivare som är direkt och indirekt anslutna till Sammanhållen journalföring genom Inera samt i förekommande fall underbiträdetill vårdgivare som erbjuder tjänster för sammanhållen journalföring. I övrigt gäller för Ineras personuppgiftsbehandling instruktionerna i detta Ineras Personuppgiftsbiträdesavtal 1 och i förekommande fall kundavtal.

5.4. Inera 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 för Ineras personuppgiftsbehandling instruktionerna i detta Ineras Personuppgiftsbiträdesavtal 1.

6. Överlåtelse av personuppgiftsbehandling till ett underbiträde

6.1. Inera äger rätt att anlita ett eller flera underbiträden avseende behandling av den Personuppgiftsansvariges personuppgifter. Denna rätt utgör ett sådant ”allmänt skriftligt förhandstillstånd” som framgår av artikel 28.2 Dataskyddsförordningen. Inera ska alltid informera den personuppgiftsansvarige om eventuella planer på att anlita nya underbiträden eller byta ut 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 har anlitats efter ett ”allmänt skriftligt förhandstillstånd”, vilka den Personuppgiftsansvarige inte gjort invändningar mot enligt förfarandet i denna punkt, lämnas på Ineras hemsida.

6.2. Om Inera anlitar ett underbiträde, ska underbiträdet i ett skriftligt personuppgiftsbiträdesavtal med Inera (Ineras Personuppgiftsbiträdesavtal 3) åläggas samma skyldigheter i fråga om dataskydd som enligt detta Ineras Personuppgiftsbiträdesavtal 1. Inera ska 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.

6.3. I Ineras Personuppgiftsbiträdesavtal 3 som Inera träffar med underbiträde ska Inera tydliggöra att en begäran till underbiträdet om utlämnade av en handling eller en uppgift omedelbart ska överlämnas till Inera, och att underbiträdet inte i något sammanhang själv får hantera en sådan begäran. Inera ska snarast överlämna mottagen begäran till den Personuppgiftsansvarige och avvakta vidare instruktioner från den Personuppgiftsansvarige.

6.4. Ineras uppgifter ska vid överföring till underbiträde ha ett adekvat skydd i form av kryptering, sekretessavtal med underbiträdet och Inera ska tillse att det finns sekretessförbindelser mellan underbiträdet och underbiträdets egen personal. Om underbiträdets personal omfattas av en lagreglerad tystnadsplikt ska i stället Inera tillse att underbiträdet erinras om aktuella sekretess- och tystnadspliktbestämmelser som underbiträdet och underbiträdets personal ska iaktta. Inera behöver inte tillse att det finns sekretessförbindelse mellan underbiträdet och underbiträdets egen personal om underbiträdet och underbiträdets egen personal omfattas av lagreglerad tystnadsplikt.

6.5. Om underbiträdet inte uppfyller sina skyldigheter i fråga om dataskydd ska Inera förbli fullt ansvarig gentemot den Personuppgiftsansvarige för underbiträdets uppfyllande av sina skyldigheter enligt föreliggande Ineras Personuppgiftsbiträdesavtal 1.

6.6. Upphör detta Ineras Personuppgiftsbiträdesavtal 1 att gälla får Inera eller ett underbiträde inte fortsätta behandla personuppgifter som omfattas av detta Ineras Personuppgiftsbiträdesavtal 1. Förvarar underbiträdet händelsevis personuppgifter åt Inera ska Inera tillse att personuppgifterna i ett sådant fall återlämnas till Inera eller till den Personuppgiftsansvarige eller raderas i enlighet med punkten 7.12 nedan.

7. Ineras allmänna åtaganden

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

7.2. Inera är en teknisk tillhandahållare av Nationella tjänsteplattformen och nationella digitala tjänster. Inera får därför inte utan tillåtelse av den Personuppgiftsansvarige ta del av personuppgifter som behandlas för den Personuppgiftsansvariges räkning.

7.3. Inera har emellertid, oaktat punkten 7.2, tillåtelse av den Personuppgiftsansvarige att ta del av den Personuppgiftsansvariges data i Nationella tjänsteplattformen, centrala tjänster och andra 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.

7.4. Inera 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.

7.5. Inera 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 Inera ska kunna fullfölja avtal om tjänsten samt för administration, inklusive säkerhetsadministration.

7.6. Inera 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. Inera ska säkerställa att kravet i denna punkt beaktas vid upphandling av underbiträde för behandling av personuppgifter. På behandlingen är svensk rätt tillämplig, bl.a. Dataskyddsförordningen.

7.7. Den Personuppgiftsansvarige har rätt att på egen bekostnad själv eller genom tredje man kontrollera att Inera följer detta Ineras Personuppgiftsbiträdesavtal 1. 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 1 samt tillträde till de fysiska lokaler där utrustning och annan hård- och mjukvara finns. Inera ska säkerställa att kravet på kontroll enligt denna punkt beaktas vid upphandling av underbiträdeför behandling av personuppgifter. Vid Personuppgiftsansvarigs utövande av kontroll enligt denna klausul ska Inera informera andra Personuppgiftsansvariga som använder Ineras digitala tjänster om vem som genomfört kontrollen och tidpunkt.

7.8. Inera 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. Inera ska omedelbart informera den Personuppgiftsansvarige om Inera anser att en instruktion strider mot Dataskyddsförordningen eller svensk rätt.

7.9. Inera 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. Inera har inte rätt att företräda den Personuppgiftsansvarige eller agera för dennes räkning gentemot Integritetsskyddsmyndigheten eller annan myndighet eller annan tredje man.

7.10. Inera ska hjälpa den Personuppgiftsansvarige, genom lämpliga tekniska och organisatoriska åtgärder att, i den mån detta är möjligt, och med tanke på 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.

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

7.12. Inera ska när detta Ineras Personuppgiftsbiträdesavtal 1 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 det egna systemet, såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller svensk rätt.

7.13. Den Personuppgiftsansvarige ska ersätta Inera för sådant arbete och kostnader som följer av punkterna 7.10, 7.11 och 7.12. Ersättning för nämnda arbete och kostnader publiceras på Ineras hemsida.

8. Personuppgiftsansvarigs allmänna åtaganden

8.1. 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 det fall så krävs inhämta samtycke från den registrerade.

8.2. Den Personuppgiftsansvarige ska omedelbart informera Inera om förändringar i behandlingen vilka påverkar Ineras skyldigheter enligt Dataskyddsförordningen.

9. Förvaring av handling, offentlighet och utlämnande av handling

9.1. Landsting och kommuner utövar ett rättsligt bestämmande inflytande över Inera enligt 2 kap. 3 § offentlighets- och sekretesslagen (2009:400). Det innebär att Ineras anställda och uppdragstagare omfattas av en lagreglerad 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).

9.2. Den Personuppgiftsansvarige ansvarar självständigt för att bedöma om det med beaktande av sekretess- och tystnadspliktsbestämmelser är lämpligt att låta Inera hantera information inom ramen för de tjänster parterna träffar avtal om.

9.3. Inera ansvarar för att egen personal och fysiska uppdragstagare hos bolaget har god kännedom om den sekretess och tystnadsplikt som kan gälla för de uppgifter som behandlas av Inera för den Personuppgiftsansvariges räkning. För det fall att registrerad, Integritetsskyddsmyndigheten, annan myndighet eller annan tredje man begär information från Inera som rör behandling av personuppgifter ska Inera hänvisa till den Personuppgiftsansvarige. Det följer bl.a. av punkten 4.4 ovan att Personuppgiftsbiträdet inte får lämna ut personuppgifter om sådan behandling av personuppgifter som specifikt rör den Personuppgiftsansvarige utan skriftlig instruktion från den Personuppgiftsansvarige.

9.4. Inera ska bereda Riksarkivet, i egenskap av arkivmyndighet, och i förekommande fall arkivmyndighet hos den Personuppgiftsansvarige, möjlighet att kontrollera eventuella arkivbestämmelsers efterlevnad hos Inera.

10. Säkerhet vid behandling av personuppgifter

10.1. Inera 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 kundavtal.

10.2. 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.

10.3. 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 Dataskyddsförordningen. Inera, och Ineras underbiträden, är fria att ansluta sig till antingen en godkänd uppförandekod eller en godkänd certifieringsmekanism, med stöd av artikel 32 i Dataskyddsförordningen, för att visa att kraven i punkten 10.1 ovan följs.

Behörighetstilldelning

10.4. Inera ska ansvara för att det finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av den egna personalens och uppdragstagares behörigheter för åtkomst till den Personuppgiftsansvariges personuppgifter, när det är tillåtet enligt detta Ineras Personuppgiftsbiträdesavtal 1.

Loggning

10.5. Se punkt 10.12.

Säkerhetskopiering

10.6. Inera ska ha rutiner för säkerhetskopiering av personuppgifter i ett allmänt erkänt och strukturerat format. Om detta Ineras Personuppgiftsbiträdesavtal 1 upphör gäller vad som framgår av punkt 7.12.

Elektronisk informationsöverföring

10.7. Inera 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

10.8. Innan Inera driftsätter sina system för mottagande eller utlämnande av information enligt detta Ineras Personuppgiftsbiträdesavtal 1 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.

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

Driftstörningar

10.10 Driftsäkerhet samt avhjälpande av fel eller brist regleras inte i detta Ineras Personuppgiftsbiträdesavtal 1.

10.11. Intrångsförsök eller annat bedrägligt förfarande för att få åtkomst till den Personuppgiftsansvariges personuppgifter ska utan onödigt dröjsmål, dock senast 48 timmar från att incidenten upptäcktes, anmälas av Inera till den Personuppgiftsansvarige (Personuppgiftsincident). Inga ändringar (omstart, uppgraderingar, felsökningar) får normalt vidtas utan samråd med den andra parten. Övriga personuppgiftsincidenter ska anmälas av Inera utan onödigt dröjsmål, dock senast 48 timmar från att incidenten upptäcktes, till den Personuppgiftsansvarige enligt artikel 33 i Dataskyddsförordningen. Anmälningar om personuppgiftsincidenter av Ineras underbiträden ska också rapporteras till den Personuppgiftsansvarige.

10.12 Inera åtar sig att kontinuerligt logga åtkomst till personuppgifter enligt detta Ineras Personuppgiftsbiträdesavtal 1. Inera 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 1 upphör att gälla.

11. Ersättning

11.1 Ersättning för tjänster enligt detta Ineras Personuppgiftsbiträdesavtal 1 regleras i punkten 7.13. Ersättning för Ineras tillhandahållande av digitala tjänster som inte omfattas av detta Ineras Personuppgiftsbiträdesavtal 1 regleras i kundavtal.

12. Ansvar mot registrerad för skada

12.1 Parternas ansvar och ansvarsbegränsningar för skada med avseende på behandling av personuppgifter och dataskydd regleras i kundavtal.

13. Avtalstid

13.1 Ineras Personuppgiftsbiträdesavtal 1 gäller från dess undertecknande och så länge som Inera har ett uppdrag från den Personuppgiftsansvarige att behandla personuppgifter för dennes räkning.

14. Tvist

14.1 Tvist angående tolkning eller tillämpning av detta Ineras Personuppgiftsbiträdesavtal 1 ska avgöras av Stockholms tingsrätt. Svensk rätt ska äga tillämpning på tvisten.