Region Stockholm

Diarienummer
HSN 2020-1799

# 2 Informationshantering Transkulturellt centrum (TC) från och med 2025

## 2.1 Inledning

Beställaren har beslutat att digitalisering ska användas som ett strategiskt verktyg för att effektivisera och kvalitetssäkra hälso- och sjukvårdsverksamheten i Region Stockholm, erbjuda bättre samhällsservice samt öka patienters/medborgares delaktighet i hälso- och sjukvårdsverksamheten.

För vissa funktioner anvisar Beställaren ett digitalt informationsstöd. För annan funktionalitet får Leverantören själv välja informationsstöd.

Beställaren äger rätt att ändra, lägga till eller ta bort användande av digital tjänst, beskriven funktionalitet, informationsanvändning eller rapportering som beskrivs i denna bilaga.

## 2.2 Informationssäkerhet

Leverantören ska skydda sin information mot otillbörlig åtkomst och förstörelse i enlighet med gällande lagar, förordningar och föreskrifter. Leverantören ska följa Region Stockholms gällande policy och riktlinjer för informationssäkerhet, se Vårdgivarguiden – Policy för verksamhetsskydd och Riktlinjer för informationssäkerhet. Hur skyddet genomförs ska dokumenteras. Leverantören ska på begäran kunna uppvisa dokumentationen för Beställaren.

Informationssäkerhetsområdet utvecklas i snabb takt. Digitaliseringen inom hälso- och sjukvårdsområdet ökar. Nya tekniska möjligheter införs och den praxis och de standarder som finns på området utvecklas över tid. De interna och externa hoten mot de digitala informationssystemen förändras ständigt. Mot den bakgrunden är det viktigt att Leverantören kontinuerligt arbetar med utveckling av säkerhetslösningar och proaktiva åtgärder för att förhindra att sårbarheter och incidenter uppstår i syfte att skydda den information som hanteras i verksamheten.

Leverantören ska ha, och tillse att av Leverantören anlitade underleverantörer har, robusta och säkra informationssystem. Leverantören ska skydda, och tillse att av Leverantören anlitade underleverantörer skyddar, information hänförlig till Uppdraget och dess utförande mot otillbörlig åtkomst och förstörelse i enlighet med gällande lagar, förordningar och föreskrifter så som, men inte begränsat till, patientdatalagen (2008:355) och lag (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning och lagring av uppgifter.

Leverantören ska följa, och tillse att av Leverantören anlitade underleverantörer följer, Beställarens vid var tid gällande informationssäkerhetskrav för leverantörer, benämnda *HSF:s informationssäkerhetskrav för vårdgivare med hälso- och sjukvårdsuppdrag åt Region Stockholm,* som finns på Vårdgivarguiden.

Leverantören ska senast vid Driftstart ha

i) implementerat, och därefter under hela avtalstiden upprätthålla, ett ledningssystem för informationssäkerhet enligt HSLF-FS 2016:40 eller motsvarande;
ii) utsett en person hos Leverantören som ansvarar för informationssäkerheten i den verksamhet som berörs av Uppdraget; och
iii) etablerat en rutin för att identifiera informationssäkerhetsrelaterade risker hänförliga till Uppdraget och dess utförande.

Leverantören ska senast vid Driftstart inkomma med skriftlig redovisning som verifierar att kraven i punkterna i. – iii. ovan är uppfyllda.

Leverantören ska även i övrigt dokumentera hur Leverantören säkerställer att informationssäkerhetskraven i denna punkt 11 uppfylls.

Leverantören ska på Beställarens skriftliga begäran tillhandahålla dokumentation som redovisar hur Leverantören och i förekommande fall, Leverantörens underleverantörer, uppfyller informationssäkerhetskraven ovan, inkluderande utan begränsning kraven i *HSF:s informationssäkerhetskrav för vårdgivare med hälso- och sjukvårdsuppdrag åt Region Stockholm*. Sådan dokumentation ska tillhandahållas inom två (2) veckor från det att Leverantören mottagit Beställarens skriftliga begäran.

Leverantören ska vidare på Beställarens skriftliga begäran utan dröjsmål tillhandahålla/tillgängliggöra loggar/loggfiler från Leverantörens IT-miljö/IT-system och, i förekommande fall, från Leverantörens underleverantörers IT-miljö/IT-system, för att Beställaren, själv eller genom av Beställaren anlitad tredje man, ska kunna upptäcka och utreda

1. möjliga informationssäkerhetsincidenter i Leverantörens och/eller, i förekommande fall, Leverantörens underleverantörers IT-miljö;
2. hot mot Beställarens IT-miljö förorsakade av brister i Leverantörens och/eller, i förekommande fall, Leverantörens underleverantörers informationssäkerhetsskydd; och
3. misstänkta intrång i Leverantörens och/eller, i förekommande fall, Leverantörens underleverantörers IT-system.

## 2.3 Personuppgiftsbiträdesavtal - villkor för behandling av personuppgifter

I syfte att uppfylla kravet i artikel 28.2 i Europaparlamentets och rådets förordning (EU) 2016/679 (”Dataskyddsförordningen”) på skriftligt avtal mellan personuppgiftsansvarig och personuppgiftsbiträde ska följande villkor gälla för behandling av personuppgifter i sådana elektroniska tjänster och system i denna bilaga genom vilka någon nämnd, styrelse eller bolag inom Region Stockholm eller underleverantör till Region Stockholm behandlar personuppgifter för Leverantörens räkning.

**Parter**

Personuppgiftsansvarig: Leverantören

Personuppgiftsbiträde: Nämnd, styrelse eller bolag inom Stockholms läns landsting (Region Stockholm)

## Definitioner

I den mån Dataskyddsförordningen innehåller begrepp som motsvarar de som används i detta avtal ska sådana begrepp tolkas och tillämpas i enlighet med förordningen.

## Omfattning

Vilket/vilka elektroniska tjänster och system som berörs framgår av denna bilaga och Avtalet i övrigt. Information om föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, framgår på Vårdgivarguiden.

För viss personuppgiftsbehandling som Region Stockholm utför för Leverantörens räkning kan gälla ett annat personuppgiftsbiträdesavtal som avviker från bestämmelserna i detta avtal. Detta andra avtal har då företräde, i den mån det inte strider mot Dataskyddsförordningen eller annan tillämplig dataskyddslagstiftning.

## Ansvar och instruktion

- Leverantören är personuppgiftsansvarig och ansvarar därmed för att lagstöd finns för behandlingen av personuppgifter och att denna behandling även i övrigt sker i enlighet med Dataskyddsförordningen och annan tillämplig dataskyddslagstiftning.

- Region Stockholm åtar sig att i egenskap av personuppgiftsbiträde endast behandla personuppgifter för att tillhandahålla berörda elektroniska tjänster och system och då i enlighet med dokumenterade instruktioner, styrdokument samt träffade avtal och andra överenskommelser samt i enlighet med Dataskyddsförordningen och eventuell övrig tillämplig dataskyddslagstiftning. Grundläggande instruktioner avseende funktioner hos respektive tjänst framgår på Vårdgivarguiden.

- För det fall det skulle finnas behandlingar som Region Stockholm enligt tvingande lag måste utföra, utöver de dokumenterade instruktioner som lämnats av Leverantören, ska Region Stockholm underrätta Leverantören innan sådan behandling påbörjas, om det inte föreligger hinder mot att lämna sådan information enligt gällande rätt.

- Region Stockholm får endast överföra personuppgifter som behandlas enligt detta avtal till ett land utanför EU/EES (tredje land) eller internationell organisation om detta uttryckligen framgår av dokumenterade instruktioner.

- Region Stockholm ska ge Leverantören tillgång till all information som krävs för att visa att de skyldigheter som fastställs i detta biträdesavtal har fullgjorts, inklusive information om eventuell underleverantörs behandling

av personuppgifter. Information som omfattas av sekretess enligt lag får inte utlämnas. Region Stockholm ska möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av Leverantören eller av en annan revisor som bemyndigats av Leverantören.

- Inspektion enligt föregående punkt får endast göras om inte Region Stockholms tillhandahållande av information är tillräcklig. Om Leverantören önskar genomföra en inspektion ska Region Stockholm informeras om detta i skälig tid i förväg och samtidigt specificera inspektionens innehåll och omfattning. Region Stockholm har rätt till skälig ersättning från Leverantören i samband med genomförande av sådan granskning.

- Leverantören ger genom denna överenskommelse Region Stockholm ett allmänt skriftligt förhandstillstånd att anlita annat personuppgiftsbiträde för behandling av personuppgifter enligt detta avtal. Region Stockholm ska därvid informera Leverantören om anlitade personuppgiftsbiträden samt eventuella planer på att ersätta anlitade personuppgiftsbiträden eller anlita nya personuppgiftsbiträden, så att Leverantören har möjlighet att göra invändningar mot sådana förändringar. Vilka andra personuppgiftsbiträden som anlitas vid var tid framgår på Vårdgivarguiden.

- Om Region Stockholm anlitat eller anlitar annat personuppgiftsbiträde så ska det andra personuppgiftsbiträdet genom ett skriftligt avtal åläggas minst samma skyldigheter i fråga om behandling av personuppgifter som de som gäller för Region Stockholm.

- För att Leverantören ska kunna fullgöra sin skyldighet att svara på en begäran från registrerade vad avser registrerades rättigheter enligt Dataskyddsförordningen, och eventuell annan tillämplig dataskyddslagstiftning, åtar sig Region Stockholm att bistå Leverantören genom lämpliga tekniska och organisatoriska åtgärder.

- Region Stockholm ska bistå Leverantören med att se till att Leverantörens skyldigheter enligt Dataskyddsförordningens artikel 32–36 fullgörs, med beaktande av typen av behandling och den information som Region Stockholm har att tillgå.

- Föregående punkter innebär inte att Region Stockholm övertar något ansvar eller några skyldigheter som enligt Dataskyddsförordningen eller annan tillämplig dataskyddslagstiftning åvilar Leverantören.

- När behandlingen ska upphöra ska Region Stockholm, beroende på vad Leverantören väljer, radera eller återlämna alla personuppgifter till Leverantören och radera eventuella kopior, såvida inte lagring av personuppgifterna krävs enligt gällande rätt.

**Säkerhetsåtgärder och sekretess m.m.**

- Region Stockholm ska vidta alla lämpliga tekniska och organisatoriska åtgärder som avses i Dataskyddsförordningens artikel 32 för att uppnå en lämplig säkerhetsnivå för personuppgifterna.

- Region Stockholm ska säkerställa att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.

- Region Stockholm ansvarar för att endast personal som behöver åtkomst till personuppgifter för att kunna utföra sina arbetsuppgifter under detta avtal får åtkomst till dessa.

**Personuppgiftsbiträdesavtal avseende Inera AB:s tjänster**

Personuppgiftsbiträdesavtal avseende de tjänster som anges under punkt 8.5 i denna bilaga och som tillhandahålls via Inera AB.

- Inera AB (org. nr. 556559-4230) är ett bolag som ägs av Sveriges regioner, kommuner och SKR Företag. Uppdraget är att skapa förutsättningar för att digitalisera välfärden, genom att förse ägarna med gemensam digital infrastruktur och arkitektur.
- Därvid och i andra sammanhang kommer Inera AB att, beroende på tjänstens utformning i det enskilda fallet, för Leverantörens räkning själv behandla personuppgifter och/eller uppdra åt olika driftleverantörer att behandla personuppgifter. Inera AB och/eller sådana driftleverantörer, kommer då att inta ställning som personuppgiftsbiträde åt den personuppgiftsansvariga Leverantören.
- För att möjliggöra korrekt avtalsrelation mellan den personuppgiftsansvariga Leverantören och respektive personuppgiftsbiträde/underbiträde, ska som en integrerad del av detta avtal, Ineras Personuppgiftsbiträdesavtal 2 Avtal enligt artikel 28.3, Dataskyddsförordningen gälla mellan Leverantören (indirekt ansluten vårdgivare) och Region Stockholm (direktansluten vårdgivare) enligt dess vid var tid gällande fulla lydelse. Gällande version av Ineras Personuppgiftsbiträdesavtal 2 Avtal enligt artikel 28.3, Dataskyddsförordningen finns på Inera AB:s hemsida www.inera.se
- Om Leverantören ingått separat personuppgiftsbiträdesavtal med Inera AB skall det gälla i första hand.

## 2.4 Termer, begrepp, semantik

### 2.4.1 Termer

För information om termer och begrepp, se Vårdgivarguiden – Termer och begrepp.

### 2.4.2 Rapportering av informationsobjekt

Leverantören ska följa policy och regelverk för organisation i ”EK”.

## 2.5 Elektroniska tjänster, e-tjänster

### 2.5.1 Allmänt

Beställaren har i egenskap av hälso- och sjukvårdshuvudman ansvar för att det i tillräcklig omfattning finns strategiska elektroniska tjänster där verksamhetsnytta, patientnytta, säkerhet eller ekonomisk besparing utgör incitament.

I den här bilagan beskrivs de avtalsmässiga krav avseende funktionalitet som Leverantören är skyldig att använda eller uppfylla.

### 2.5.2 Generella krav

Funktionalitet som Leverantören ska använda eller uppfylla. För vissa funktioner anvisar Beställaren ett systemstöd. För annan funktionalitet får Leverantören själv välja systemstöd.

#### 2.5.2.1 Beställarens information

All information som Leverantören behöver för att utföra sitt uppdrag publiceras på Vårdgivarguiden.

| Skyldighet för Leverantören | Information/instruktion på Vårdgivarguiden |
|---|---|
| Leverantören ska hålla sig uppdaterad om aktuell information om uppdraget | www.vardgivarguiden.se |

#### 2.5.2.2 Rapportering, uppföljning, fakturering

Leverantören ska rapportera strukturerad information till Beställaren.

##### *2.5.2.2.1 Rapportering*

| Skyldighet för Leverantören | Information/instruktion på Vårdgivarguiden |
|---|---|
| Leverantören ska kontinuerligt upprätthålla aktuell kontaktinformation för verksamheten | Elektroniska Katalogen, EK |

#### 2.5.2.3 Gemensam infrastruktur för ökad säkerhet

Leverantören ska använda sig av verktyg och åtgärder som ska hindra att information läcker ut, förvanskas eller förstörs men som ska möjliggöra att informationen är tillgänglig när den behövs.

| Skyldighet för vårdgivare | Information/instruktion på Vårdgivarguiden |
|---|---|
| Leverantören ska kunna identifiera användare i verksamheten vid inloggning och åtkomst till elektroniska tjänster som hanterar känsliga personuppgifter på ett säkert sätt. | eTjänstekort |
| Leverantören ska säkerställa att de personposter som finns i EK är korrekta och uppdaterade | Elektroniska katalogen, EK |

## 2.6 SLLnet och kostnadsansvar

SLLnet är Region Stockholms gemensamma kommunikationsnät. Alla vårdgivare som har avtal med Region Stockholm har rätt att ha en anslutning till SLLnet, via fast anslutning eller distansanslutning (SAM). Beställaren bekostar denna

uppkoppling med en kapacitet och servicenivå som krävs för den rapportering Beställaren ställer krav på. Leverantören bekostar eventuell högre kapacitet som behövs för att klara annan funktionalitet i Leverantörens system/tjänster - t.ex. för samordnad journalhantering.  Om det inte längre är nödvändigt att vara ansluten till SLLnet för att rapportera information enligt detta avtal kommer anslutningen till SLLnet att upphöra att vara en kostnadsfri tjänst.