Allmänna instruktioner för behandling av personuppgifter i Ineras Tjänster

Innehåll

Allmänna instruktioner för behandling av personuppgifter i Ineras Tjänster 2

1. Inledning 2

2. Tekniska och organisatoriska säkerhetsåtgärder 2

2.1 Allmänt 2

2.2 Incidenthantering och uppföljning 3

2.3 Skalskydd 3

2.4 Åtkomst och loggning 3

2.5 Tillgänglighet 4

3. Övriga instruktioner 4

Allmänna instruktioner för behandling av personuppgifter i Ineras Tjänster

1. Inledning

1.1 Detta dokument, Allmänna instruktioner för behandling av personuppgifter i Ineras Tjänster (”Allmänna instruktioner”) innehåller allmänna instruktioner för Ineras behandling av personuppgifter och utgör en integrerad del av Avtalet. Det består av kompletterande regleringar gällande för Inera och Kunden. I [Tjänsten] - Beskrivning och tjänstespecifika villkor finns specifika instruktioner för Ineras behandling av personuppgifter i Tjänsten.

1.2 Dessa Allmänna instruktioner ska tillämpas på Ineras tillhandahållande av Tjänster som behandlar personuppgifter.

2. Tekniska och organisatoriska säkerhetsåtgärder

Inera ska vidta följande tekniska och organisatoriska åtgärder:

2.1 Allmänt

a. Inera tillämpar en av Ineras styrelse beslutad informationssäkerhetspolicy.

b. I syfte att säkerställa ett systematiskt informationssäkerhetsarbete använder Inera ett ledningssystem för informationssäkerhet. Ledningssystemet är utformat i linje med SS-EN ISO/IEC 27001 Ledningssystem för informationssäkerhet.

c. Inera informationsklassificerar känslig information enligt fastställd informationsklassningsmodell som grundas på Myndigheten för samhällsskydd och beredskaps metodstöd.

d. Inera har en avdelad tjänsteförvaltare för Tjänsten.

e. Inera genomför riskanalyser regelbundet och vid förändringar.

f. Ineras personal omfattas av lagstadgad tystnadsplikt enligt offentlighets- och sekretesslagen.

g. Drift av Tjänster sker inom EU/EES.

h. Inera har ett utsett dataskyddsombud vilket är ansvarigt för att kontrollera att personuppgifter behandlas i enlighet med dataskyddsförordningen och verka som rådgivande till verksamheten.

2.2 Incidenthantering och uppföljning

Inera:

a. har rutiner vilka stödjer en korrekt hantering av informationssäkerhetsincidenter.

b. följer lagstadgad rapportering av incidenter till tillsynsmyndigheter samt informerar Kunden om inträffade incidenter på sådant sätt att Kunden kan uppfylla sin lagstadgade rapportering av incidenter till tillsynsmyndigheter.

c. har rutiner för uppföljning av SLA-nivåer för de Tjänster Inera tillhandahåller.

d. genomför systematiskt och regelbundet säkerhetstester i syfte att säkerställa att det tekniska skyddet är uppdaterat och verkningsfullt.

e. genomför systematiska informationssäkerhetsgranskningar i enlighet med Ineras revisionsprogram.

2.3 Skalskydd

Inera har:

a. ett implementerat och kontinuerligt aktiverat skydd för att upptäcka och förhindra dataintrång.

b. ett implementerat och kontinuerligt aktiverat skydd för att upptäcka och förhindra skadlig kod.

c. lokaler skyddade mot obehörigt tillträde genom magnet- eller chipkort.

d. kryptografiska metoder för skydd av känslig information.

2.4 Åtkomst och loggning

Inera:

a. sparar tekniska loggar innehållande driftsinformation.

b. sparar åtkomstloggar gällande patientuppgifter i minst fem år.

c. tillämpar användaridentitet och lösenord vilka är personliga och inte får lämnas ut eller överlåtas på någon annan.

d. tillämpar vid åtkomst till patientinformation i Tjänster stark autentisering.

e. beslutar och godkänner autentiseringsmetoder.

f. tillser att loggning av åtkomst till information sker i enlighet med Socialstyrelsens föreskrifter och allmänna råd HSLF-FS 2016:40.

g. har ett behörighetssystem för att styra och kontrollera att användare har behörighet för åtkomst och ändring av data.

h. begränsar medarbetares behörighet varigenom dessa har åtkomst till information vilken krävs för att utföra dessas arbetsuppgifter.

2.5 Tillgänglighet

Inera:

a. har en driftsmiljö vilken är redundant uppbyggd i syfte att upprätthålla avtalade tillgänglighetsnivåer.

b. utför regelbunden säkerhetskopiering.

c. utför drift av Tjänster i lokaler vilka skyddas med larm för bränder, vattenskador och inbrott.

d. utför drift av Tjänster i separata datahallar med ett individuellt avstånd av minst 15 km.

e. utför regelbunden mätning och uppföljning av kapacitet i syfte att förebygga kapacitets- eller prestandaproblem.

f. upprättar för varje Tjänst system-, drift- och användardokumentation.

g. övervakar kontinuerligt Ineras driftsmiljöer.

h. har separata IT-miljöer för utveckling, test och drift.

3. Övriga instruktioner

Vid behandling av Kundens personuppgifter ska Inera:

a. iaktta de skyldigheter som åligger Inera enligt Avtalet och gällande lagstiftning.

b. säkerställa, om Kunden är vårdgivare, att endast vårdgivare med fast driftställe i Sverige och registrering hos Inspektionen för vård och omsorg (”IVO”) får ta del av Kundens patientuppgifter inom ramen för Tjänsten, om Tjänsten hanterar patientuppgifter.

c. radera personuppgifter vilka mellanlagras hos Inera när dessa inte längre behövs för att tillhandahålla Tjänsten.

d. inte utan tillåtelse av den personuppgiftsansvarige ta del av personuppgifter som behandlas för den personuppgiftsansvariges räkning. Oaktat detta har emellertid Inera tillåtelse av den personuppgiftsansvarige att:

   i. 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;

ii. säkerställa Kundens behov av statistik över användningen av Tjänsten samt tillåtelse för Inera att fritt sammanställa sådan statistik i avidentifierad form med andra Kunders användning av Tjänsten;

iii. bearbeta personuppgifter för att visa avidentifierad statistik gällande Ineras tjänster och som på begäran kan lämnas ut till allmänheten;

iv. 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; och

v. 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.

e. behandla avlidna personers uppgifter i enlighet med samma villkor som följer av Avtalet.

f. behandla känsliga personuppgifter som i vissa digitala tjänster är centrala för hälso- och sjukvårdens aktörer som följer patientdatalagens (2008:355) bestämmelser, såsom i tjänsten Kvalitetsregistrering och Öppna Data.