

Bilaga 1 - Instruktioner för databehandlingen

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

1. Ändamål, föremålet och arten

Ändamålet är att uppfylla Personuppgiftsbiträdets åtaganden enligt Huvudavtalet. Föremålet för och arten av behandling är den behandling som Personuppgiftsbiträdet genomför för sina kunder i enlighet med respektive Huvudavtal vilket främst innebär i de fall då Personuppgiftsbiträdet

- tillhandahåller drift av systemet för Personuppgiftsansvarig
- tillhandahåller kommunikation av personuppgifter från och till andra system (exempelvis nationella tjänster)
- utför supporttjänster där personuppgifter förekommer (exempelvis support via fjärråtkomst, felsökning och rättningar enligt instruktion från Personuppgiftsansvarig)
- utför konsultuppdrag där personuppgifter förekommer (exempelvis migrering av data, konfigurerings och registrering av uppgifter på uppdrag av Personuppgiftsansvarig).

2. Behandlingen omfattar följande typer av Personuppgifter

Alla kategorier av personuppgifter som den Personuppgiftsansvarige kan komma att registrera/förmedla, vilket främst är;

För anställda/konsulter hos Personuppgiftsansvarig (notera att inte alla uppgifter är tillämpliga för alla anställda/konsulter);

- namn och kontaktuppgifter
- personnummer
- yrkesroll
- kompetens
- koder kopplade till personen (exempelvis HSA-ID, anställningsnummer, förskrivarkod etc)
- behörigheter
- logguppgifter (exempelvis tidsstämplar, åtkomst) och liknande uppgifter.

För vårdtagare (notera att inte alla uppgifter är tillämpliga för alla vårdtagare);

- namn och kontaktuppgifter
- personnummer
- andra typer av personrelaterade koder och person-ID
- kön
- medicinsk och hälsoinformation
- betalningsinformation
- tidsbokningar
- födelseland
- modersmål
- familjesituation
- släktband
- anhöriga
- samtyckesinformation
- skola/skolklass och företagstillhörighet.

Andra registrerade (se under rubriken Kategorier av registrerade ovan vilken typ av personer detta kan avse, notera att inte alla uppgifter är tillämpliga för alla andra registrerade);

- • namn och kontaktuppgifter
- • personnummer
- • yrkesroll
- • arbetsplats
- • koder kopplade till personen (exempelvis HSA-ID, förskrivarkod, laboratoriekod)
- • relation till/händelser relaterade till/kontakter/diskussioner om/protokoll/minnesanteckningar med/avseende Vårdtagare och liknande uppgifter.

Notera:

Möjligheter finns att skapa anteckningar som fritext i journalen och andra delar av systemet. I dessa fritextfält kan vilken typ av personuppgifter som helst antecknas, det är inte ovanligt att det här förekommer känsliga uppgifter även av annan art än medicinska och hälsouppgifter.

I systemet finns också omfattande möjligheter för Personuppgiftsansvarig att själv löpande konfigurera och lägga till nya typer av personuppgifter.

Dessa kommer då att ingå i de typer av personuppgifter som Personuppgiftsbiträdet kan komma att behandla.

3. Behandlingen omfattar kategorier av Registrerade

Alla kategorier av registrerade som den Personuppgiftsansvarige kan komma att registrera/förmedla, vilket främst är;

- • patienter/elever/anställda/brukare/andra personer som nyttjar eller har rätt att nyttja kundens tjänster ("Vårdtagare")
- • Vårdtagares närstående och andra kontakter
- • anställd personal (användare) hos kunden
- • konsulter/personal hos underleverantörer
- • vårdpersonal eller andra personer som inte är anställda hos kunden men som har koppling till vårdtagaren på annat sätt (ex. remissavsändare/mottagare på annan vårdenhet/laboratorium, annan skolpersonal, personal hos andra myndigheter eller liknande).

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

Personuppgiftsbiträdet innehar generellt rättigheterna till de system Personuppgiftsbiträdet tillhandahåller till Personuppgiftsansvarig, med de eventuella avvikelser som förekommer i Huvudavtalet. Personuppgiftsbitrådets utgångspunkt är att alla uppgifter som den Personuppgiftsansvarige, eller någon annan på uppdrag av den Personuppgiftsansvarige, för in i systemet, avseende exempelvis användare och patienter, ägs av den Personuppgiftsansvarige. Att den Personuppgiftsansvarige registrerar uppgifter i något av Personuppgiftsbitrådets system innebär därmed inte automatiskt att Personuppgiftsbiträdet blir biträde till sådan behandling, utan Personuppgiftsbiträdet utgör endast biträde i de fall där Personuppgiftsbiträdet på något sätt behandlar införda personuppgifter.

Personuppgiftsansvarig är alltid ansvarig för att insamling, registrering av uppgifter, information till registrerad person, raderingsrutiner och andra legala krav som ställs på insamling och hantering av personuppgifterna genomförs enligt tillämpliga lagar, förordningar och föreskrifter.

<p>Personuppgiftsbiträdet ansvarar endast för att den behandling som Personuppgiftsbiträdet genomför enligt Huvudavtalet sker i enlighet med detta personuppgiftsbiträdesavtal.</p>
<p>5. Ange särskilda tekniska och organisatoriska säkerhetsåtgärder vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet/biträdena</p>
<p>Att skydda kunders informationstillgångar innehållande personuppgifter är en prioriterad fråga för Personuppgiftsbiträdet. Grundprinciper för Personuppgiftsbitrådets informationssäkerhet är; tillgänglighet, riktighet, konfidentialitet samt spårbarhet.</p> <p>Bristande informations säkerhet kan leda till störningar i kunders samhällsviktiga verksamhet och medföra risker för den personliga integriteten. Personuppgiftsbiträdet följer därför nedanstående riktlinjer för att säkerställa att ovanstående principer följs för all personuppgiftsbehandling:</p> <ul style="list-style-type: none"> • Identifiera, riskhantera och tilldela ansvar för informationstillgångar som innehåller personuppgifter samt vidta relevanta och balanserade skyddsåtgärder för dessa. • Hantera informationstillgångar i enlighet med lagstiftning, policyer, riktlinjer samt kunders instruktioner. • Utbilda och informera medarbetare i informationssäkerhet så att en god utbildningsnivå erhålls och bibehålls samt att informationssäkerheten tillämpas. • Utforma och underhålla rutiner och verktyg för uppföljning som säkerställer informationssäkerheten. • Utforma och underhålla rutiner och verktyg för incidenthantering för incidenter som rör personuppgiftsbehandling. • Styra medarbetares tillgång till information, dvs. rätt information vid rätt tidpunkt och på rätt plats till en behörig användare. <p>Personuppgiftsansvarig kan, när kunden så önskar, begära ut kundanpassad dokumentation om Personuppgiftsbitrådets aktuella vidtagna tekniska och organisatoriska åtgärder.</p>
<p>6. Ange särskilda krav på Loggning vad gäller Behandling av Personuppgifter samt vilka som ska ha tillgång till dem</p>
<p>Inga särskilda krav utöver vad som framgår av Huvudavtalet och Personuppgiftsbiträdesavtalet. Notera: Systemet loggar alltid åtkomst till personuppgifter i enlighet med kraven i Patientdatalag (2008:355) - vårdtagarens identitet, användarens identitet, vilka åtgärder som vidtagits med uppgifterna (läsa, skapa, ändra etc), enhet och tidpunkt. Dessa loggar är alltid tillgängliga för Personuppgiftsansvarig.</p>
<p>7. Lokalisering och överföring av Personuppgifter till Tredje land</p>
<p>För samtliga kunder; Behandling kan komma att genomföras av personal hos Personuppgiftsbiträdet vid bolagets kontor i Sverige i Stockholm och Göteborg, på plats hos Personuppgiftsansvarig om Personuppgiftsbitrådets personal bedriver support/installation på plats eller hos underbiträden som anges i Bilaga 2. Fysisk lagring för kunder som har Personuppgiftsbitrådets hosting-tjänst i Sverige; Datahall i Göteborgsområdet, Sverige. Fysisk lagring för kunder som har Personuppgiftsbitrådets hosting-tjänst i Tyskland; Datahall i Tyskland, Frankfurt. Fysisk lagring (endast temporär) för kunder som har Personuppgiftsbitrådets tjänst e-enkät; Datahall i Uppsala, Sverige</p>
<p>8. Övriga Instruktioner angående Behandling av Personuppgifter som utförs av biträdet/biträdena</p>
<p>För undvikande av missförstånd noteras här att Personuppgiftsbiträdet även kan komma att genomföra automatiskt eller manuellt utlämnande av personuppgifter enligt Personuppgiftsansvarigs instruktioner till andra än underbiträden (se Bilaga 2 Underbiträden).</p>

Detta rör exempelvis utlämnande till

- laboratorium som Personuppgiftsansvarig har avtal med
- tredjepartsfunktionalitet som Personuppgiftsansvarig har avtal med
- kvalitetsregister
- nationell patientöversikt eller andra nationella system som Personuppgiftsansvarig har avtal med eller har bett Personuppgiftsbiträdet att av annan anledning att utlämna data till.

Personuppgiftsbiträdet förutsätter att Personuppgiftsansvarig har ett personuppgiftsbiträdesavtal eller annan laglig grund för sådant utlämnande till tredje part som Personuppgiftsansvarig ombesörjer eller som ombud att utföra när behandlingen inte anges i listan över underbiträdesbehandlingar.