

# Bilaga 1 - Personuppgiftsansvariges Instruktion för Behandling av Personuppgifter

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

## 1. Ändamålet, föremålet och arten

1 a. Föremålet för Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige är att:

Syftet med registret är att kunna göra regionernas samlade biobanksprov och data om dessa sökbara samt för att skapa förutsättningar och underlätta *för biobankshuvudmännen att uppfylla sina legala skyldigheter gällande exempelvis samtyckeshantering, uppfyllande av offentlighetsprincipen eller att tillhandahålla registerutdrag till patienten själv* med stöd av dataskyddsförordningen. Registret är ett arbetsverktyg för att stödja förvaltningen av de biobanker som sjukvården upprättar i sin verksamhet. Systemet kommer att erbjuda funktioner som ger den spårbarhet som krävs för hanteringen av samlingar med humanbiologiska prov.

1 b. Ändamålet med Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige är att:

Systemet är utvecklat i avsikt att erbjuda funktionalitet till användare i deltagande verksamheter vilka hanterar sina egna uppgifter genom direktåtkomst villkorat av att legala förutsättningar föreligger. Biträdet ska på uppdrag av biobankshuvudmännen söka information om prov efter ett delegationsbeslut av biobankshuvudmännen.

1 c. Personuppgiftsbiträdets Behandling av Personuppgifter på uppdrag av den Personuppgiftsansvarige avser huvudsakligen följande behandlingsåtgärder (Behandlingens art eller natur):

Region Uppsala utgör hemvist för systemens utveckling och tekniska förvaltning. Därtill ska Region Uppsala företräda personuppgiftsansvariga huvudmän för att uppfylla tillämpliga lagar och föreskrifter vid systemets tekniska underhåll, utveckling och kvalitetssäkring såsom till exempel användarstöd, felsökning, uppgradering av mjuk eller hårdvara, säkerhetskopiering alt. återställning, uppgiftsminimering och de registrerades rättigheter.

## 2. Behandlingen omfattar följande typer av Personuppgifter

Personuppgiftsbiträdet har rätt att behandla följande typer av Personuppgifter för den Personuppgiftsansvariges räkning:

Registrerades personuppgifter i systemet utgörs av provgivare/patienter/deras legala företrädare, anställda/uppdragstagare/konsulter samt externa kontakter i forskningsstudier som kan identifieras direkt eller indirekt.

För provgivare/patienter kan direkt identifiering ske genom exempelvis

- Namn
- Personnummer

För provgivare/patienter kan indirekt identifiering ske genom exempelvis

- Var provet tagits (system där det lagras)
- Var prov lagras eller finns (biobank, provsamling, tillgängliggörande etc.)
- Prov-id (unikt, skapas av inrapporterande system)
- Samtyckesinformation och begränsning av samtycke
- Provtagningsstidpunkt
- Information om provet, typ och lokalisering det är taget ifrån
- Administrativa uppgifter om tidigare eller kommande studier

Detta utgör känsliga uppgifter då uppgifter om hälsa kan härledas ur praktiskt taget varje tänkbart prov i och med att orsaken till tagningen oftast är ett hälsoärende.

Identifiering av anställda/uppdragstagare/konsulter kan ske genom

- HSA-information
- Kontouppgifter (identifierare, tjänsteuppgifter, behörigheter)
- Användning av system (spårning av åtgärder i system)

Identifiering av externa kontakter i forskningsstudier kan ske genom

- Identifierande information (t.ex. personnummer via bank id)
- Information från ärenden vid ansökningar till biobank
- Upprättade avtal för provsamlingar och uttag

### **3. Behandlingen omfattar vissa kategorier av Registrerade**

Personuppgiftsbiträdet har rätt att Behandla Personuppgifter avseende följande kategorier av Registrerade:

Personuppgiftsbehandlingen kommer att innefatta uppgifter om följande kategorier av personer

- Anställda, uppdragstagare och konsulter
- Patienter, i förekommande fall, patientens legala ställföreträdare
- Studiedeltagare
- Externa kontakter såsom forskare och andra företrädare för forskningshuvudmän

### **4. Ange särskilda hanteringskrav vad gäller Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet**

Personuppgiftsbiträdet ska iaktta följande hanteringskrav vid Behandlingen av Personuppgifter åt den Personuppgiftsansvarige:

Reglering framgår av Avtalsbilaga – Informationssäkerhet för var tids gällande version som fastställs av Region Uppsala.

### **5. Ange de särskilda tekniska och organisatoriska säkerhetsåtgärder som gäller för Personuppgiftsbitrådets Behandling av Personuppgifter**

Personuppgiftsbiträdet ska vidta följande säkerhetsåtgärder vid Behandlingen av Personuppgifterna:

Tekniska och organisatoriska skyddsåtgärder framgår av Avtalsbilaga – Informationssäkerhet för var tids gällande version som fastställs av Region Uppsala.

Såväl primära uppgifter som säkerhetskopior skall förvaras enligt gällande regelverk.

Elektronisk åtkomst av eller direktåtkomst över öppna nät ska föregås av kryptering, stark autentisering och ska loggas i en åtkomstlogg.

Därvid ska biträdet vidta skäligen och rimligen integritetshöjande säkerhetsåtgärder såsom exempelvis att utveckling och testning av system bedrivs i test-miljö som saknar känsliga personuppgifter.

#### **6. Ange särskilda krav på Loggning vad gäller Behandling av Personuppgifter samt vilka som ska ha tillgång till dem**

Personuppgiftsbiträdet ska iaktta följande krav avseende loggning av användaraktivitet och logghantering:

Krav avseende loggning och åtkomst framgår av Avtalsbilaga – Informationssäkerhet för var tids gällande version som fastställs av Region Uppsala.

Åtkomster av personuppgifter genom direktåtkomst ska loggas och åtkomstlogg ska tillgängliggöras så att personuppgiftsansvarig kan genomföra åtkomstkontroller enligt dennes rutiner.

Åtkomster som biträdet gör för personuppgiftsansvarigs räkning i förvaltningsärenden skall loggas och loggen utgör underlag för åtkomstkontroll och regleras av delegationsbeslut och avtal med leverantörer.

Åtkomster av personuppgifter som genomförs i samband med teknisk förvaltning av systemet ska dokumenteras så att de i efterhand kan granskas. Uppgifter som ska framgå i denna dokumentation är:

- Referens till begäran om åtgärd
- Åtgärdens syfte
- Tidpunkt för åtkomst(er)
- Omfattning av åtkomst
- Utförande handläggare

Denna logg ska kunna lämnas ut till personuppgiftsansvarig på begäran.

#### **7. Lokalisering och överföring av Personuppgifter till Tredje land**

Personuppgiftsbiträdet ska iaktta följande krav avseende lokalisering av Personuppgifter:

Personuppgiftsbiträdet har endast rätt att behandla Personuppgifterna på följande plats/er:

Personuppgifterna får endast behandlas av ett biträde etablerat inom landet eller inom EU/EES.

Ingen överföring skall ske till tredje land utan samtliga berörda personuppgiftsansvarigas uttryckliga godkännande.

#### **8. Behandlingens varaktighet**

Under avtalsperioden enligt samverkansavtalet för Svenska biobanksregistret ("Samverkansavtal SBR okt 2020 Slutlig version" och personuppgiftsbiträdesavtal).

**9. Övriga Instruktioner angående Behandling av Personuppgifter som utförs av Personuppgiftsbiträdet**

Med iakttagande av punkt 5, får personuppgifter som skapas som ett resultat av att systemets användning loggas, kan användas för framställning av statistik, kvalitetssäkring och utveckling av Svenska biobanksregistret i enhetlighet med styrgruppens beslut.

Underbiträden får inte behandla personuppgifter för andra syften än för att fullgöra detta avtal.

## Versionshantering

<b>Version</b>	<b>Datum</b>	<b>Förändringar</b>	<b>Ansvarig</b>
0.2	2020-10-15	Initial version	Tomas Snäckerström
0.3	2024-10-22	Uppdaterad version	Lena M Jönsson