Region Uppsala

Dnr: RK2020-00365

Personuppgiftsbiträdesavtal

Version 2.1 (230406)

Innehållsförteckning

Bilagor:

- Bilaga 1 - Instruktioner till personuppgiftsbiträdet_2024-10-22
- Bilaga 2 - Avtalsbilaga-informationssäkerhet_2024-10-22
- Bilaga 3 - Underbiträden 2024-10-22

PERSONUPPGIFTSBITRÄDESAVTAL

Avtal enligt artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679[1]

1. PARTER, PARTERNAS STÄLLNING, KONTAKTUPPGIFTER OCH KONTAKTPERSONER

Personuppgiftsansvarig	**Personuppgiftsbiträde**
Region Västmanland	Region Uppsala
Organisationsnummer	**Organisationsnummer**
232100-0172	232100-0024
Postadress	**Postadress**
Region Västmanland Regionhuset, 721 89 Västerås	Box 602, 751 25 Uppsala
Kontaktperson för administration av detta personuppgiftsbiträdesavtal	**Kontaktperson för administration av detta personuppgiftsbiträdesavtal**
Namn: Henrik Drott E-post: henrik.drott@regionvastmanland.se Tfn: 021-175136	Namn: Sonja Eaker Fält E-post: sonja.eaker.falt@regionuppsala.se Tfn: 018-617 71 05
Kontaktperson för parternas samarbete om dataskydd	**Kontaktpersoner för parternas samarbete om dataskydd**
Namn: Agata Cierzniak E-post: agata.cierzniak@regionvastmanland.se Tfn: 021-173000	Namn: Andreas Kappen E-post: dataskyddsombud@regionuppsala.se Tfn: 018-611 00 00

2. DEFINITIONER

Utöver de begrepp som definieras i löptext, i detta personuppgiftsbiträdesavtal, ska dessa definitioner oavsett om de används i plural eller singular, i bestämd eller obestämd form, ha nedanstående innebörd när de anges med versal som begynnelsebokstav.

Behandling	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.
Dataskyddslagstiftning	Avser all integritets- och personuppgiftslagstiftning, samt all annan eventuell lagstiftning (inklusive förordningar och föreskrifter), som är tillämplig på den Behandling som sker enligt detta PUB-avtal, inklusive nationell sådan lagstiftning och EU-lagstiftning.

[1] Allmänna dataskyddsförordningen EU 2016/679 föreskriver att det ska finnas ett skriftligt avtal om Personuppgiftsbiträdets Behandling av Personuppgifter för Den personuppgiftsansvariges räkning.

Personuppgiftsansvarig	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamål och medlen för Behandlingen av Personuppgifter.
Instruktion	De skriftliga instruktioner som närmare anger föremål, varaktighet, art och ändamål, typ av Personuppgifter samt kategorier av Registrerade och särskilda behov som omfattas av Behandlingen.
Logg	Logg är resultatet av Loggning.
Loggning	Loggning är ett kontinuerligt insamlande av uppgifter om den Behandling av Personuppgifter som utförs enligt detta PUB-avtal och som kan knytas till en enskild fysisk person.
Personuppgiftsbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som Behandlar Personuppgifter för den Personuppgiftsansvariges räkning.
Personuppgift	Varje upplysning som avser en identifierad eller identifierbar fysisk person, 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.
Personuppgiftsincident	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.
Registrerad	Fysisk person vars Personuppgifter Behandlas.
Tredje land	En stat som inte ingår i Europeiska unionen (EU) eller inte är ansluten till Europeiska ekonomiska samarbetsområdet (EES).
Underbiträde	Fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som i egenskap av underleverantör till Personuppgiftsbiträdet Behandlar Personuppgifter för Personuppgiftsansvariges räkning.

3. BAKGRUND OCH SYFTE

3.1 Detta PUB-avtal (definition enligt nedan) utgör en bilaga till och en integrerad del av Samverkansavtalet gällande förvaltningssamverkan avseende Svenska biobanksregistret (SBR) vilket är Regionernas gemensamma IT-system för SBR. Samverkansavtalet har ingåtts år 2020 och med Region Upsalas dnr RK2020-00365. PUB-avtalet ska läsas och förstås mot bakgrund av Samverkansavtalet.

3.2 Med detta Personuppgiftsbiträdesavtal jämte Instruktioner och en eventuell förteckning över Underbiträden (nedan gemensamt "PUB-avtalet") reglerar den Personuppgiftsansvarige Personuppgiftsbiträdets Behandling av Personuppgifter åt den Personuppgiftsansvarige. PUB-avtalets syfte är att säkerställa den Registrerades fri- och rättigheter vid Behandlingen, i enlighet med vad som stadgas i artikel 28.3 i Allmänna dataskyddsförordningen EU 2016/679 ("Dataskyddsförordningen").

3.3 För det fall något av det som stadgas i punkterna 1, 3.1, avsnitt 15 eller 16, punkt 17.6, avsnitt 18-20 och 22 i PUB-avtalet regleras på annat sätt i Samverkansavtalet ska Samverkansavtalets reglering ha företräde.

3.4 Hänvisningar i PUB-avtalet till nationell eller unionsrättslig lagstiftning, avser vid var tid tillämpliga bestämmelser.

4. BEHANDLING AV PERSONUPPGIFTER OCH SPECIFIKATION

4.1 Den Personuppgiftsansvarige utser härmed Personuppgiftsbiträdet att utföra Behandlingen för den Personuppgiftsansvariges räkning enligt vad som stadgas i detta PUB-avtal.

4.2 Den Personuppgiftsansvarige ska ge skriftliga Instruktioner till Personuppgiftsbiträdet om hur det ska utföra Behandlingen.

Instruktioner till personuppgiftsbiträdet	**Bilaga 1**
Avtalsbilaga – informationssäkerhet	**Bilaga 2**

4.3. Personuppgiftsbiträdet får endast utföra Behandlingen i enlighet med PUB-avtalet och vid var tid gällande Instruktioner.

5. DEN PERSONUPPGIFTSANSVARIGES ANSVAR

5.1 Den Personuppgiftsansvarige ansvarar för att det vid var tid finns laglig grund för Behandlingen och för att utforma korrekta Instruktioner så att Personuppgiftsbiträdet och eventuellt Underbiträde kan fullgöra sitt eller sina uppdrag enligt detta PUB-avtal och Samverkansavtal i förekommande fall.

5.2 Den Personuppgiftsansvarige ska utan onödigt dröjsmål informera Personuppgiftsbiträdet om förändringar i Behandlingen vilka påverkar Personuppgiftsbiträdets skyldigheter enligt Dataskyddslagstiftningen.

5.3 Den Personuppgiftsansvarige ansvarar för att informera Registrerade om Behandlingen och för att tillvarata Registrerades rättigheter enligt Dataskyddslagstiftningen samt vidta varje annan åtgärd som åligger den Personuppgiftsansvarige enligt Dataskyddslagstiftningen.

6. PERSONUPPGIFTSBITRÄDETS ÅTAGANDEN

6.1 Personuppgiftsbiträdet förbinder sig att endast utföra Behandlingen i enlighet med PUB-avtalet och Instruktioner samt att följa Dataskyddslagstiftningen. Personuppgiftsbiträdet förbinder sig även att fortlöpande hålla sig informerad om gällande rätt på området.

6.2 Personuppgiftsbiträdet ska vidta åtgärder för att skydda Personuppgifterna mot alla slag av Behandlingar som inte är förenliga med PUB-avtalet, Instruktioner och Dataskyddslagstiftningen.

6.3 Personuppgiftsbiträdet åtar sig att säkerställa att samtliga fysiska personer som arbetar under dess ledning följer PUB-avtalet och Instruktioner samt att de fysiska personerna informeras om relevant lagstiftning.

6.4 Personuppgiftsbiträdet ska på begäran från den Personuppgiftsansvarige bistå denne med att säkerställa att skyldigheterna enligt artikel 32–36 i Dataskyddsförordningen fullgörs och svara på begäran om utövande av den Registrerades rättigheter i enlighet med Dataskyddsförordningen, kap.

III, med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå.

6.5 För det fall att Personuppgiftsbiträdet finner att Instruktioner är otydliga, i strid med Dataskyddslagstiftningen eller saknas och Personuppgiftsbiträdet bedömer att nya eller kompletterande Instruktioner är nödvändiga för att genomföra sina åtaganden ska Personuppgiftsbiträdet utan dröjsmål informera den Personuppgiftsansvarige, tillfälligt upphöra med Behandlingen och invänta nya Instruktioner, om inte parterna kommer överens om annat.

6.6 För det fall att den Personuppgiftsansvarige förser Personuppgiftsbiträdet med nya eller ändrade Instruktioner ska Personuppgiftsbiträdet, utan onödigt dröjsmål från mottagandet, meddela den Personuppgiftsansvarige huruvida genomförandet av de nya Instruktionerna föranleder förändrade kostnader för Personuppgiftsbiträdet.

7. SÄKERHETSÅTGÄRDER

7.1 Personuppgiftsbiträdet ska vidta alla lämpliga tekniska och organisatoriska säkerhetsåtgärder som krävs enligt Dataskyddslagstiftningen för att förhindra Personuppgiftsincidenter, genom att säkerställa att Behandlingen uppfyller kraven i Dataskyddsförordningen och att den Registrerades rättigheter skyddas.

7.2 Personuppgiftsbiträdet ska fortlöpande säkerställa att den tekniska och organisatoriska säkerheten i samband med Behandlingen medför en lämplig nivå av konfidentialitet, integritet, tillgänglighet och motståndskraft.

7.3 Eventuella tillkommande eller ändrade krav på skyddsåtgärder från den Personuppgiftsansvarige, efter parternas tecknande av PUB-avtalet, ska betraktas som nya Instruktioner enligt PUB-avtalet.

7.4 Personuppgiftbiträdet ska genom behörighetskontrollsystem endast ge åtkomst till Personuppgifterna för sådana fysiska personer som arbetar under Personuppgiftsbiträdets ledning och som behöver åtkomsten för att kunna utföra sina arbetsuppgifter.

7.5 Personuppgiftsbiträdet åtar sig att kontinuerligt Logga åtkomst till Personuppgifterna enligt PUB-avtalet i den utsträckning det krävs enligt Instruktionen. Loggar får gallras först fem (5) år efter Loggningstillfället om inte annat anges i Instruktionen. Loggar ska omfattas av erforderliga skyddsåtgärder, i enlighet med Dataskyddslagstiftningen.

7.6 Personuppgiftsbiträdet ska systematiskt testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa Behandlingens säkerhet.

8. SEKRETESS/TYSTNADSPLIKT

8.1 Personuppgiftsbiträdet och samtliga fysiska personer som arbetar under dess ledning ska vid Behandlingen iaktta såväl sekretess som tystnadsplikt. Personuppgifterna får inte nyttjas eller spridas för andra ändamål, vare sig direkt eller indirekt, såvida inte annat avtalats.

8.2. Personuppgiftsbiträdet ska tillse att samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen, är bundna av sekretessförbindelse avseende Behandlingen. Detta krävs dock inte om dessa redan omfattas av en straffsanktionerad tystnadsplikt som följer av lag. Personuppgiftsbiträdet åtar sig även att tillse att det finns sekretessavtal med Underbiträdet samt sekretessförbindelser mellan Underbiträdet och samtliga fysiska personer som arbetar under dess ledning, vilka deltar i Behandlingen.

8.3 Personuppgiftsbiträdet ska skyndsamt underrätta den Personuppgiftsansvarige om eventuella kontakter med tillsynsmyndighet avseende Behandlingen. Personuppgiftsbiträdet har inte rätt att företräda den Personuppgiftsansvarige eller agera för den Personuppgiftsansvariges räkning gentemot tillsynsmyndigheter i frågor avseende Behandlingen.

8.4 Om den Registrerade, tillsynsmyndighet eller tredje man begär information från Personuppgiftsbiträdet vilken rör Behandlingen, ska Personuppgiftsbiträdet informera den Personuppgiftsansvarige om saken. Information om Behandlingen får inte lämnas till den Registrerade, tillsynsmyndighet eller tredje man utan skriftligt medgivande från den Personuppgiftsansvarige, såvida det inte framgår av tvingande lag att information ska lämnas. Personuppgiftsbiträdet ska bistå med förmedling av den informationen som omfattas av ett medgivande eller lagkrav.

9. GRANSKNING, TILLSYN OCH REVISION

9.1 Personuppgiftsbiträdet ska utan onödigt dröjsmål som en del av sina garantier, enligt artikel 28.1 i Dataskyddsförordningen, på den Personuppgiftsansvariges begäran kunna redovisa vilka tekniska och organisatoriska säkerhetsåtgärder som används för att Behandlingen ska uppfylla kraven enligt PUB-avtalet och artikel 28.3.h i Dataskyddsförordningen.

9.2 Personuppgiftsbiträdet ska minst en (1) gång om året granska säkerheten avseende Behandlingen genom en egenkontroll för att säkerställa att Behandlingen följer PUB-avtalet. Resultatet av sådan egenkontroll ska på begäran delges den Personuppgiftsansvarige.

9.3 Den Personuppgiftsansvarige äger rätt att, själv eller genom annan av denne utsedd tredje part (som inte får vara en konkurrent till Personuppgiftsbiträdet), följa upp att Personuppgiftsbiträdet uppfyller PUB-avtalets, Instruktionernas och Dataskyddslagstiftningens krav. Personuppgiftsbiträdet ska vid sådan granskning bistå den Personuppgiftsansvarige, eller den som utför granskningen i den Personuppgiftsansvariges ställe, med dokumentation, tillgång till lokaler, IT-system och andra tillgångar som behövs för att kunna granska Personuppgiftsbiträdets efterlevnad av PUB-avtalet, Instruktioner och Dataskyddslagstiftningen. Den Personuppgiftsansvarige ska säkerställa att personal som genomför granskningen är underkastade sekretess eller tystnadsplikt enligt lag eller avtal.

9.4 Personuppgiftsbiträdet äger alternativt till vad som stadgas i punkten 9.2-9.3, rätt att erbjuda andra tillvägagångssätt för granskning av Behandlingen, exempelvis granskning genomförd av oberoende tredje part. Den Personuppgiftsansvarige ska i sådant fall äga rätt, men inte skyldighet, att tillämpa detta alternativa tillvägagångssätt för granskning. Vid sådan granskning ska

Personuppgiftsbiträdet ge den Personuppgiftsansvarige eller en tredje part den assistans som behövs för utförandet av granskningen.

9.5 Personuppgiftbiträdet ska bereda tillsynsmyndighet, eller annan myndighet som har laglig rätt till det, möjlighet att göra tillsyn enligt myndighetens begäran i enlighet med vid var tid gällande lagstiftning, även om sådan tillsyn annars skulle stå i strid med bestämmelserna i PUB-avtalet.

9.6 Personuppgiftsbiträdet ska tillförsäkra den Personuppgiftsansvarige rättigheter gentemot Underbiträdet vilka motsvarar den Personuppgiftsansvariges samtliga rättigheter gentemot Personuppgiftsbiträdet enligt punkten 9 i PUB-avtalet.

10. HANTERING AV RÄTTELSER OCH RADERING M.M.

10.1 För det fall den Personuppgiftsansvarige begärt rättelse eller radering på grund av Personuppgiftsbiträdets felaktiga Behandling ska Personuppgiftsbiträdet vidta lämplig åtgärd utan onödigt dröjsmål, senast inom trettio (30) dagar, från det att Personuppgiftsbiträdet mottagit erforderlig information från den Personuppgiftsansvarige. När den Personuppgiftsansvarige begärt radering får Personuppgiftsbiträdet endast utföra Behandling av den aktuella Personuppgiften som ett led i processen för rättelse eller radering.

10.2 Om tekniska och organisatoriska åtgärder (t.ex. uppgraderingar eller felsökningar) vidtas av Personuppgiftsbiträdet i Behandlingen, vilka kan väntas påverka Behandlingen, ska Personuppgiftsbiträdet skriftligt informera den Personuppgiftsansvarige om detta i enlighet med vad stadgas om meddelanden i punkten 18 i PUB-avtalet. Informationen ska lämnas i god tid innan åtgärderna vidtas.

11. PERSONUPPGIFTSINCIDENTER

11.1 Personuppgiftsbiträdet ska ha förmåga att återställa tillgängligheten och tillgången till Personuppgifterna i rimlig tid vid en fysisk eller teknisk incident enligt artikel 32.1.c i Dataskyddsförordningen.

11.2 Personuppgiftbiträdet åtar sig att med beaktande av Behandlingens art, och den information som Personuppgiftsbiträdet har att tillgå, bistå den Personuppgiftsansvarige med att fullgöra dennes skyldigheter vid en Personuppgiftsincident beträffande Behandlingen. Personuppgiftbiträdet ska på den Personuppgiftsansvariges begäran även bistå med att utreda misstankar om eventuell obehörigs Behandling och/eller åtkomst till Personuppgifterna.

11.3 Vid Personuppgiftsincident, vilken Personuppgiftbiträdet fått vetskap om, ska Personuppgiftsbiträdet utan onödigt dröjsmål skriftligen underrätta den Personuppgiftsansvarige om händelsen. Personuppgiftsbiträdet ska, med beaktande av typen av Behandling och den information som Personuppgiftsbiträdet har att tillgå, tillhandahålla den Personuppgiftsansvarige en skriftlig beskrivning av Personuppgiftsincidenten.

11.4 Beskrivningen ska redogöra för:

a) Personuppgiftsincidentens art och, om möjligt, de kategorier och antalet Registrerade som berörs samt kategorier och antalet personuppgiftsposter som berörs,
b) de sannolika konsekvenserna av Personuppgiftsincidenten, och
c) åtgärder som har vidtagits eller föreslagits samt åtgärder för att mildra Personuppgiftincidentens potentiella negativa effekter.

11.5 Om det inte är möjligt för Personuppgiftsbiträdet att tillhandahålla hela beskrivningen samtidigt, enligt punkten 11.3 i PUB-avtalet, får beskrivningen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

12. UNDERBITRÄDE

12.1 Personuppgiftsbiträdet äger rätt att anlita den eller de Underbiträden som framgår av bilagd förteckning över Underbiträden, **Bilaga 3.**

12.2 Personuppgiftsbiträdet åtar sig att teckna ett skriftligt avtal med Underbiträdet som reglerar Behandlingen som Underbiträdet utför å den Personuppgiftsansvariges vägnar samt att endast anlita Underbiträden som ger tillräckliga garantier för att genomföra lämpliga tekniska och organisatoriska åtgärder så att Behandlingen uppfyller kraven i Dataskyddsförordningen. I fråga om dataskydd ska avtalet ålägga Underbiträdet samma skyldigheter som åläggs Personuppgiftsbiträdet i detta PUB-avtal.

12.3 Personuppgiftsansvarige har rätt att säga upp Underbiträdet och instruera Underbiträdet att exempelvis radera eller återlämna Personuppgifterna om Personuppgiftsbiträdet har upphört att existera i faktisk eller rättslig mening eller hamnat på obestånd.

12.4 Personuppgiftsbiträdet ansvarar fullt ut för Underbiträdets Behandling gentemot den Personuppgiftsansvarige. Personuppgiftsbiträdet ska skyndsamt underrätta den Personuppgiftsansvarige om Underbiträdet underlåter att uppfylla sina skyldigheter i PUB- avtalet.

12.5 Personuppgiftsbiträdet äger rätt att anlita nya underbiträden och ersätta befintliga underbiträden om inte annat anges i Instruktionen.

12.6 När Personuppgiftsbiträdet avser att anlita ett nytt eller ersätta ett befintligt Underbiträde ska Personuppgiftsbiträdet säkerställa Underbiträdets kapacitet och förmåga att uppfylla sina skyldigheter enligt Dataskyddslagstiftningen. Personuppgiftsbiträdet ska skriftligen meddela den Personuppgiftsansvarige om:

a) Underbiträdets namn, organisationsnummer och säte (adress och land),
b) vilken typ av uppgifter och kategorier av Registrerade som behandlas, och
c) var Personuppgifterna ska behandlas.

12.7 Den Personuppgiftsansvarige äger rätt att inom trettio (30) dagar från dag för meddelande enligt punkten 12.7 invända mot Personuppgiftsbiträdets anlitande av ett nytt underbiträde och att, med anledning av sådan invändning, säga upp detta PUB-avtal att upphöra i enlighet med vad stadgas i PUB-avtalet, punkten 16.4.

12.8 Personuppgiftsbiträdet ska vid var tid föra en korrekt och uppdaterad förteckning över de Underbiträden som anlitas för Behandling av Personuppgifter för den Personuppgiftsansvariges räkning samt göra denna förteckning tillgänglig för den Personuppgiftsansvarige. Av förteckningen ska särskilt framgå i vilket land Underbiträdet behandlar Personuppgifterna och vilka typer av Behandlingar som Underbiträdet utför.

12.9 När Personuppgiftsbiträdet upphör med att anlita Underbiträdet ska Personuppgiftsbiträdet skriftligen meddela den Personuppgiftsansvarige om detta. Personuppgiftsbiträdet ska när ett avtal upphör säkerställa att Underbiträdet raderar eller återlämnar Personuppgifterna.

12.10 Personuppgiftsbiträdet ska på den Personuppgiftsansvariges begäran översända en kopia av det avtal som reglerar Behandling av Underbiträdets Behandling av Personuppgifter enligt punkten.

13. LOKALISERING OCH ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND

13.1 Personuppgiftsbiträdet ska säkerställa att Personuppgifterna hanteras och lagras inom EU/EES av en fysisk eller juridisk person som är etablerad inom EU/EES, om inte PUB-avtalets parter kommer överens om något annat.

13.2 Personuppgiftsbiträdet äger endast rätt att överföra Personuppgifter till Tredje land för Behandling (t.ex. service, support, underhåll, utveckling, drift eller liknande hantering) om den Personuppgiftsansvarige på förhand skriftligen godkänt sådan överföring och utfärdat Instruktioner för detta ändamål.

13.3 Överföring till Tredje land för Behandling enligt PUB-avtalet, punkten 13.2, får endast ske om den är förenlig med Dataskyddslagstiftningen och uppfyller de krav på Behandlingen vilka ställs i PUB-avtalet och Instruktioner.

14. ANSVAR FÖR SKADA I SAMBAND MED BEHANDLING

14.1 Vid ersättning för skada i samband med Behandling som, genom fastställd dom eller förlikning, ska utgå till den Registrerade på grund av överträdelse av bestämmelse i PUB-avtalet, Instruktioner och/eller tillämplig bestämmelse i Dataskyddslagstiftningen ska artikel i 82 i Dataskyddsförordningen tillämpas.

14.2 Sanktionsavgifter enligt artikel 83 i Dataskyddsförordningen, eller 6 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning ska bäras av den av PUB-avtalets parter som påförts en sådan avgift.

14.3 Om endera part får kännedom om omständighet som kan leda till skada för motparten ska parten omedelbart informera motparten om förhållandet och aktivt arbeta tillsammans med motparten för att förhindra och minimera sådan skada.

14.4 Oaktat vad sägs i Samverkansavtalet gäller detta PUB-avtal, punkterna 14.1 och 14.2, före andra regler om fördelning mellan Parterna av krav sinsemellan såvitt avser Behandlingen.

15. PUB-AVTALETS TECKNANDE, AVTALSTID OCH UPPSÄGNING

PUB-avtalet gäller från och med den tidpunkt PUB-avtalet undertecknats av båda parter och tillsvidare. Parterna äger ömsesidig rätt att säga upp PUB-avtalet att upphöra med trettio (30) dagars varsel.

16. ÄNDRINGAR OCH UPPSÄGNING MED OMEDELBAR VERKAN M.M.

16.1 Endera part i PUB-avtalet äger rätt att påkalla omförhandling av PUB-avtalet om motpartens ägarförhållanden ändras väsentligt eller om tillämplig lagstiftning, eller tolkningen av den, ändras på ett för Behandlingen avgörande sätt. Påkallande av omförhandling enligt första meningen innebär inte att PUB-avtalet till någon del upphör att gälla utan endast att en omförhandling om PUB-avtalet ska påbörjas.

16.2 Tillägg till, och ändringar i, PUB-avtalet ska vara skriftliga och undertecknade av båda parter.

16.3 När någon av parterna får kännedom om att motparten agerar i strid med PUB-avtalet och/eller Instruktioner ska parten utan dröjsmål meddela motparten om agerandet. Därefter äger parten rätt att med omedelbar verkan upphöra att utföra sina förpliktelser enligt PUB-avtalet till den tidpunkt motparten förklarat att agerandet upphört och förklaringen accepterats av den part som påtalat agerandet.

16.4 Om den Personuppgiftsansvarige invänder mot Personuppgiftsbiträdets anlitande av ett nytt underbiträde, enligt detta PUB-avtal, punkten 12.7, har den Personuppgiftsansvarige rätt att säga upp PUB-avtalet att upphöra med omedelbar verkan.

17. ÅTGÄRDER VID PUB-AVTALETS UPPHÖRANDE

17.1 Efter uppsägning av PUB-avtalet ska Personuppgiftsbiträdet utan onödigt dröjsmål, beroende på vad den Personuppgiftsansvarige väljer, antingen radera och intyga för den Personuppgiftsansvarige att det är utfört, eller återlämna

a) alla Personuppgifter som Behandlats för den Personuppgiftsansvariges räkning och

b) all tillhörande information såsom Loggar, Instruktioner, systemlösningar, beskrivningar och andra handlingar som Personuppgiftsbiträdet erhållit genom informationsutbyte enligt PUB-avtalet.

17.2 I samband med återlämning ska Personuppgiftsbiträdet även radera befintliga kopior av Personuppgifter och tillhörande information.

17.3 Skyldigheten att radera eller återlämna Personuppgifter eller tillhörande information gäller inte om lagring av Personuppgifterna eller informationen krävs enligt unionsrätten eller relevant nationell rätt där Behandling får utföras enligt PUB-avtalet.

17.4 Om Personuppgifter eller tillhörande information återlämnas ska det ske i ett allmänt använt, öppet och standardiserat format, om parterna inte har kommit överens om något annat format.

17.5 Till dess att uppgifterna raderas eller återlämnas ska Personuppgiftsbiträdet säkerställa efterlevnaden av PUB-avtalet.

17.6 Återlämning och radering enligt PUB-avtalet ska vara utförda senast trettio (30) dagar räknat från tidpunkten för uppsägningen av PUB-avtalet, om inte annat anges i Instruktionen.

Behandling som utförs av Personuppgiftsbiträdet därefter är att betrakta som en otillåten behandling.

17.7 Bestämmelser om sekretess/tystnadsplikt i punkten 8 enligt detta PUB-avtal ska fortsätta gälla även om PUB-avtalet i övrigt upphör av gälla.

18. MEDDELANDEN INOM RAMEN FÖR DETTA PUB-AVTAL OCH INSTRUKTIONER

18.1 Meddelanden om PUB-avtalet och dess administration inklusive uppsägning ska skickas via e-post eller på något annat av parterna överenskommet sätt till respektive parts kontaktperson för PUB-avtalet.

18.2 Meddelanden om parternas samarbete om dataskydd gällande Behandlingen ska skickas via e-post eller på något annat av parterna överenskommet sätt till respektive parts kontaktperson för parternas samarbete om dataskydd.

18.3 Ett meddelande ska anses ha kommit fram till mottagaren senast en (1) arbetsdag efter att meddelandet har skickats.

19. KONTAKTPERSONER

19.1 Parterna ska utse var sin kontaktperson för PUB-avtalet.

19.2 Parterna ska utse varsin kontaktperson för parternas samarbete om dataskydd.

20. ANSVAR FÖR UPPGIFTER OM PARTERNA OCH KONTAKTPERSONER SAMT KONTAKTUPPGIFTER

20.1 Varje part ansvarar för att de uppgifter som anges i punkten 1 i PUB-avtalet alltid är aktuella och korrekta.

20.2 Ändring av uppgifter i punkten 1 ska meddelas skriftligen enligt punkten 18.1 i PUB-avtalet.

21. LAGVAL OCH TVISTLÖSNING

Vid tolkning och tillämpning av PUB-avtalet gäller svensk rätt med undantag för lagvals-reglerna. Tvister med anledning av PUB-avtalet ska avgöras av behörig svensk domstol.

22. PARTERNAS UNDERTECKNANDEN AV PUB-AVTALET

22.1 Detta PUB-avtal tillhandahålls antingen i digitalt format för elektroniskt tecknande eller i pappersformat för egenhändigt undertecknande. I sistnämnda fall upprättas avtalet i två likalydande exemplar, varav parterna erhåller varsitt.

22.2 Om PUB-avtalet undertecknas elektroniskt lämnas signatursidan utan avseende.

(Resten av sidan har avsiktligt lämnats tom. Signatursida följer.)

Personuppgiftsansvarig

Region Västmanland

Ort och datum: Dec 6, 2024

Lars Almroth, Hälso-och sjukvårdsdirektör

Namnförtydligande

Lars Almroth (Dec 6, 2024 10:42 GMT+1)

Signatur

Personuppgiftsbiträde

Region Uppsala

Ort och datum: Dec 9, 2024

Mikael Köhler, Hälso-och sjukvårdsdirektör

Namnförtydligande

Mikael Köhler (Dec 9, 2024 18:00 GMT+1)

Signatur

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
- Provtagningstidpunkt
- Information om provet, typ och lokalisation 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 Personuppgiftsbiträdets Behandling av Personuppgifter

Personuppgiftbiträdet 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 skäliga och rimliga 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

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

Bilaga 2 - Avtalsbilaga - Informationssäkerhet

Version	Datum	Ansvarig	Kommentar
1.0-SNAPSHOT	2024-10-22		

1 Inledning

1.1 I denna Bilaga beskrivs de närmare åtaganden som Region Uppsala ska efterleva i fråga om informationssäkerhet för den personuppgiftsansvariga huvudmannens information. Inkluderande all data som den personuppgiftsansvariga huvudmannen tillhandahåller Region Uppsala, inklusive eventuella underleverantörer, under avtalstiden, inklusive men inte begränsat till ändringar och bearbetningar därav inom ramen för Tjänsteleveransen, med avseende på konfidentialitet, riktighet och tillgänglighet.

1.2 Parternas överenskommelse avseende informationssäkerhet ska förebygga att PUA:s Information obehörigen röjs, ändras, görs otillgängliga för behöriga eller förstörs. Detta åstadkoms genom fysisk tillträdesbegränsning, it-säkerhetsåtgärder och administrativa säkerhetsåtgärder i enlighet med vad som närmare framgår av punkterna 4-14 nedan.

1.3 Definierade begrepp som används i denna Bilaga har den betydelse som anges i punkt 3, Definitioner, såvida inte omständigheterna uppenbarligen föranleder annat.

1.4 Bilagan omfattar informationssäkerhet för PUA:s Information. För personuppgifter kan särskilda krav tillkomma i Personuppgiftsbiträdesavtalet. Oavsett typ av Information ska kraven i denna bilaga efterföljas.

1.5 I och med att SBR är ett system som utvecklas och förvaltas över tid kommer det att finnas förhållanden och omständigheter som kan påverka hur bilagans avsikter och direktiv implementeras praktiskt. Till stöd för tolkning av bilagans implementation finns löpande dokumentation publicerad på för ändamålet avsett dokumentationssystem[1]. Detta system har versionshantering av alla dokument och Region Uppsala har ansvar att hålla dokumentationen uppdaterad vid förändringar som påverkar det berörda innehållet. Region Uppsala ansvarar även för att meddela PUA om dokumentationen flyttas till annan plats.

[1] https://biobanksverige.atlassian.net/wiki/spaces/PUBLICWIKI/overview
Systemet dokumenterar alla versioner som publiceras. Vilken version som varit aktuell vid vilken tidpunkt kan utläsas under historik.

2 Omfattning

2.1 Denna Bilaga ska tillämpas för leverans i enlighet med Samverkansavtalet för Svenska Biobanksregistret (SBR). Enligt samverkansavtalet ska Region Uppsala ansvara för utveckling och drift av SBR, samt gemensamma upphandlingar för samverkans ändamål. I och med att systemet lagrar personuppgifter företräder Region Uppsala personuppgiftsansvarig huvudmän i sin tekniska förvaltning av systemet. Utöver lagring inkluderas alla åtgärder som genomförs i syfte att säkerställa systemets korrekta funktion samt åtgärder som utgör skyldigheter till följd av personuppgiftsbehandlingen.

2.2 Styrgrupp för SBR företräder beställarna gemensamt i enlighet med villkoren i samverkansavtalet.

2.3 Vid tolkningstvist äger Samverkansavtalet och PUB-avtalet företräde.

3 Definitioner

Följande definitioner används i denna bilaga:

Begrepp	Förklaring
Avtalet	Samverkansavtalet
Avvikelse	Icke-uppfyllande av ett krav.
Incidenthantering	Tillämpning av ett konsekvent och effektivt arbetssätt för att hantera och svara på säkerhetshändelser som kan påverka konfidentialitet, integritet eller tillgänglighet av information.
Information	Data som har organiserats och bearbetats på ett sätt som gör det meningsfullt och användbart. Information kan representera kunskap som kan lagras, återhämtas, överföras och bearbetas av datorer.
Informationssäkerhet	Bevarande av konfidentialitet, riktighet och tillgänglighet hos information.
Informationssäkerhets-incident	En händelse med en faktisk negativ inverkan på säkerheten i nätverk och informationssystem
Ledningssystem för informationssäkerhet	Del av leverantörens övergripande ledningssystem, baserad på en metodik för verksamhetsrisk, som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och utveckla organisationens informationssäkerhet.
Tjänsteleveransen	Tjänsteleveransen utgör den slutprodukt som definieras av den nationella styrgruppen för SBR, med stöd av för var tid gällande Avtalssamverkan avseende Svenska Biobanksregistret
Dokumentationssystem	Förvaltningen använder ett webbaserat dokumentationssystem (en wiki) för att kunna uppdatera dokumentation av system och förvaltningsåtgärder löpande vart efter de utförs. Denna spelar en viktig roll för löpande kommunikation av gällande rutiner och åtgärder. Via denna publiceras även all dokumentation som PUA efterfrågar i denna bilaga undantaget sådant som kan innehålla PUA:s personuppgifter.
Säkerhetsloggar	Register som används för att spåra och dokumentera säkerhetsrelaterade händelser, såsom inloggningsförsök, åtkomst till systemresurser, systemförändringar, nätverksaktiviteter och eventuella säkerhetsincidenter.
Åtkomstloggar	Enligt HSLF-FS 2016:40 4 kap 9 §.

4 Ledningssystem för informationssäkerhet

4.1. Region Uppsala, inklusive eventuella underleverantörer, ska ha ett ledningssystem för informationssäkerhet i enlighet med ISO 27001 eller motsvarande som omfattar Tjänsteleveransen.

5 Organisation

5.1 Det ska hos Region Uppsala finnas en tillsatt roll med ansvar och mandat som informationssäkerhetsansvarig för Tjänsten gentemot PuA. Rollen ansvarar för den totala informationssäkerheten, inklusive underleverantörer. Den Informationssäkerhetsansvarige har därför mandat att fatta relevanta beslut i frågor som rör informationssäkerhet i Tjänsten och som syftar till att upprätthålla skyddet för PuAs uppgifter.

Rollen ska närvara i styrgruppsmöten för samarbetspartners samt därutöver på begäran av PuA vara tillgänglig för möten och deltagande i ärenden med PuA.

5.2 Region Uppsala inklusive eventuella underleverantörer ansvarar för att tillhandahålla en utpekad funktion för hantering av informationssäkerhetsfrågor och skydd av PUA:s Information som hanteras under Avtalet.

5.3 Region Uppsala ska ha systemägare eller motsvarande för de it-system som används för Tjänsteleveransen under Avtalet. Systemägaren har vid var tid ett överordnat ansvar för säkerhet i varje sådant it-system.

6 Säkerhetsåtgärder

6.1 Region Uppsala ska löpande dokumentera hur åtgärder som anges i punkt 7-13 nedan uppfylls.

7 Behörighet

7.1 Behörighet till PUA:s Information får endast ges till personer hos Region Uppsala, eller eventuella underleverantörer som:

- tilldelats roll och ansvar och enligt rutinbeskrivning för behörighetstilldelning,
- bedöms lämpliga att arbeta med uppgifterna,
- har tillräckliga kunskaper om informationssäkerhet däribland legala befogenheter vid åtkomst till känsliga personuppgifter, samt och
- behöver åtkomst till PUA:s Information för att utföra sitt uppdrag.

8 Hantering av PUA:s Information

8.1 Region Uppsala ska vidta de säkerhetsåtgärder som är nödvändiga vid hanteringen av PUA:s Information under Avtalet. Region Uppsala ska redogöra för PUA vilka säkerhetsåtgärder som har vidtagits.

8.2 Region Uppsala ska informera berörd personal om innebörden av tystnadsplikten och informationssäkerhetskraven. Region Uppsala ska säkerställa att personal som hanterar sekretessbelagda uppgifter är bundna av lagreglerad tystnadsplikt.

8.3 Region Uppsala får inte röja PUA:s Information till obehörig tredje part.

8.4 Region Uppsala kommer under Leveransen att behandla data för PUA som är föremål för lagreglerad tystnadsplikt. PUA har rätt begära ändring av Avtalet om det blir otillåtet att anlita en leverantör vars personal inte omfattas av en lagreglerad och straffsanktionerad tystnadsplikt och en sådan ändring enligt PUA är nödvändig för att avtalad leverans ska vara förenlig med gällande rätt.

9 Tillträdesbegränsning

9.1 PUA:s företrädare enligt tecknat samverkansavtal ska i samråd med Region Uppsala fastställa nivån för tillträdesbegränsning och det tillträdesskydd som ska gälla för de lokaler, områden eller motsvarande utrymmen som Region Uppsala, eller eventuella underleverantörer, avser att använda vid tillhandahållandet av Tjänsteleveransen.

9.2 Beslut om tillträdesbegränsning och tillträdesskydd ska fattas av Region Uppsala i enlighet med tecknat samverkansavtal.

9.3 Tillträde till lokaler och utrustning som medför åtkomst till PUA:s Information får endast ges till personer som behöver sådan åtkomst för att utföra sina arbetsuppgifter under Avtalet. All sådan åtkomst ska vara individuellt anpassad, spårbar och dokumenterad.

10 Lämplighetsprövning

10.1 Innan en person, anställd eller uppdragstagare i Region Uppsala eller eventuella underleverantörer, får eller kan få tillgång till PUA:s Information ska vederbörandes lämplighet prövas ur säkerhetssynpunkt. Detta sker i samband med anställningsprocessen och behörighetstilldelningen, som föregås av risk- och behovsanalys.

10.2 Vid anlitande av underleverantörer och konsulter ska lämplighetsprövning under alla omständigheter innebära att Region Uppsala identifierar eventuella brister i fråga om pålitlighet och lojalitet i förhållande till det arbete som respektive individ ska utföra ~~för~~ under Avtalet, samt klargöra eventuella intressekonflikter för den berörda individens utförande av sådant arbete.

10.3 Lämplighetsprövningen vid anlitande av underleverantör och konsulter bör omfatta en bedömning baserad på intervjuer och inhämtade betyg, intyg och referenser. Omfattningen av prövningen får anpassas baserat på Informationens skyddsvärde. De personer som har tillgång till sekretessbelagda uppgifter, eller som har möjlighet att i hög grad påverka Tjänsteleveransens tillgänglighet eller funktion, ska alltid genomgå intervju innan de ges sådan tillgång.

10.4 Varje lämplighetsprövning ska dokumenteras av Region Uppsala och redovisning utlämnas till PUA på begäran.

10.5 Region Uppsala ska till PUA anmäla omständigheter som kan vara av betydelse för bedömningen av en lämplighetsprövad individs fortsatta lämplighet och pålitlighet. Detta gäller endast om Region Uppsala avser att låta personen i fråga fortsatt ha tillgång till PUA:s Information.

10.6 Om en individ som har lämplighetsprövats och påbörjat sitt uppdrag inom ramen för Avtalet anses olämplig ur säkerhetssynpunkt av PUA eller Region Uppsala, ska Region Uppsala vidta lämpliga åtgärder för att vederbörande inte ska få tillträde till lokaler, områden eller andra utrymmen där ifrågavarande individ kan få tillgång till PUA:s Information.

11 Kompetenskrav avseende informationssäkerhet

11.1 Region Uppsala ansvarar för att de personer, inklusive eventuella underleverantörer och konsulter, som Region Uppsala ansvarar för fortlöpande utbildas om informationssäkerheten. Sådan utbildning ska bland annat avse:

- hot och risker som från säkerhetssynpunkt föreligger mot eller är förknippade med Region Uppsalas åtaganden under Avtalet och
- säkerhetsåtgärder som ska vidtas mot föreliggande hot och risker.

12 Avvikelserapportering och incidenthantering

12.1 Region Uppsala ska ha dokumenterade rutiner för hantering, rapportering och uppföljning av Informationssäkerhetsincidenter. Detta ska anknytas till den övergripande avvikelserapporteringen enligt Avtalet och i enlighet med gällande lagar och föreskrifter.

12.2 Region Uppsala ska säkerställa övervakning av säkerhetsloggar i it-system där PUA:s Information hanteras för att upptäcka hot mot informationen.

12.3 Region Uppsalas rapportering ska, för att vara fullständig, omfatta all den Information som behövs för att PUA ska kunna vidta de åtgärder som rimligen kan krävas för att skydda PUA:s verksamhet, enskilda personer, ekonomi eller andra väsentliga intressen.

12.4 Om PUA är skyldig att vidarerapportera inträffade händelser till annat organ, t.ex. tillsynsmyndighet för integritetsskydd eller informationssäkerhet, ska Region Uppsala bistå i skälig och proportionerlig omfattning i enlighet med PUAs instruktioner. Till förtydligande anges att Region Uppsala inte utan särskild överenskommelse med PUA är behörig att självständigt företräda PUA i förhållande till tillsynsmyndighet.

12.5 Vid misstänkt dataintrång så ska Region Uppsala bistå PUA med relevanta digitala evidens, som PUA behöver för att tillvarata sina och de registrerades legitima intressen.

13 Revision och uppföljning

13.1 Region Uppsala ska minst en gång per kalenderår genomföra egenrevision i enlighet med myndigheters tillämpliga föreskrifter, för att kontrollera att denna Bilaga efterlevs och att skyddsnivån är adekvat anpassad med avseende på Region Uppsalas åtaganden under Avtalet. Region Uppsala skall även med motsvarande regelbundenhet granska aktuella underleverantörer i syfte att säkerställa att informationssäkerhetskrav efterlevs.

13.2 Region Uppsala ansvarar för formerna för sådan egenrevision. Region Uppsalas egenrevision kan ske genom interna revisorer eller genom externt anlitad rådgivare för granskning, dock förutsatt att adekvata lämplighetskontroller och sekretessåtaganden iakttas.

13.3 Region Uppsala ska skriftligen rapportera sin egenrevision till PUA inom 2 månader efter genomförd revision. Av rapporten ska framgå vad revisionen omfattar, de slutsatser som revisionen resulterat i samt vilka åtgärder som har vidtagits eller ska vidtas till följd av egenrevisionen. Även förändringar i fråga om uppföljning av tidigare genomförda egenrevisioner ska framgå av rapporten. Rapporten ska struktureras så att åtminstone alla Region Uppsalas åtaganden enligt denna Bilaga omfattas.

13.4 PUA har också rätt att genomföra revision av Region Uppsala.

Allmänt

13.5 Denna punkt innehåller bestämmelser avseende hantering av PUA:s Information i it-miljö som nyttjas för Tjänsteleveransen. Detta inkluderar även de it-system och it-verktyg som Region Uppsala använder för Tjänsteleveransen, inklusive men inte begränsat till supportsystem och test- och utvecklingsmiljöer.

13.6 Region Uppsala ska lämna uppgift till PUA om samtliga it-system och it-verktyg som används för Tjänsteleveransen, inklusive information om på vilket sätt it-system och it-verktyg kan komma att användas för att behandla PUA:s Information i samband med utredning av rapporterade avvikelser och incidenter. För ändamålet används överenskommet dokumentationssystem där informationen löpande hålls uppdaterad.

13.7 Region Uppsala ska dokumentera nivå och bestämmelser för säkerheten i it-system som används för Tjänsteleveransen. Region Uppsala ska även säkerställa att instruktioner för förvaltning och drift av it-system som är avsedda för behandling av PUA:s Information under Avtalet är dokumenterade.

Behörighetskontroll och säkerhetsloggning

13.8 Samtliga it-system där PUA:s Information hanteras under Avtalet ska omfatta adekvata system för behörighetskontroll där varje användare är spårbar till en och endast en fysisk person.

13.9 Behörighetskontrollen ska säkerställa att individer och system bara har tillgång till den Information som behövs för att lösa tilldelade arbetsuppgifter.

13.10 Region Uppsalas behörighetskontroll ska minst innefatta uppgift om vilka användare som har eller har haft behörighet till PUA:s Information genom de tjänster Region Uppsala tillhandahåller.

13.11 En förteckning över sådana behörigheter ska sparas i syfte att säkerställa spårbarhet bakåt i tiden. Förteckning ska även inkludera ej längre aktiva användare. Förteckningen ska på begäran överlämnas till PUA utan dröjsmål.

13.12 Region Uppsalas it-tjänster ska logga händelser som är av betydelse för säkerheten i Tjänsteleveransen (så som men inte begränsat till användaridentitet, datum och tidpunkt för inloggning och utloggning samt användaraktiviteter). Dessa adekvata säkerhetsloggar ska bevaras så att de är skyddade mot obehörig förändring och destruktion. Region Uppsala ska dokumentera hur säkerhetsloggar ska analyseras och redovisa det som säkerhetsåtgärder i enlighet med punkt 8 ovan.

13.13 Region Uppsala ska tillhandahålla en funktion som synkroniserar tiden i it-system med en tillförlitlig källa för att generera pålitliga tidsstämplar i loggposter.

13.14 Region Uppsala ska garantera tillgång till åtkomst- och säkerhetsloggar åt PUA vid begäran om dessa.

13.15 Åtkomst- och säkerhetsloggarna och relaterad information ska bevaras under en period om minst fem (5) år, om inte styrgruppen beslutar annat.

Skydd mot skadlig kod

13.16 Region Uppsala ska, på sätt som framgår av punkten 4.1, ha skydd mot skadlig kod i it-tjänsterna som levereras om tillämpligt.

13.17 Region Uppsala ska dokumentera skyddet mot skadlig kod.

13.18 It-systemen ska använda programvara som vid var tid supporteras av programvarans tillverkare (dvs. programvaran ska inte vara i skedet end-of-life). Region Uppsala installerar den senaste stabila versionen av säkerhetsrelaterade uppdateringar enligt process för förändringshantering.

Säkerhetskopiering

13.19 Säkerhetskopiering av PUA:s uppgifter skall utföras i enlighet med det skyddsvärde som uppgifterna bedöms ha enligt bedömd klassning. Aktuell rutin skall dokumenteras i förvaltningens dokumentationssystem och vara tillgänglig för PUA.

Intrångsdetektering och skydd mot intrång

13.20 Samtliga it-system där PUA:s Information hanteras under Avtalet ska vara försedda med adekvat, dvs i enlighet med punken 4.1, digitalt intrångsskydd och funktioner för intrångsdetektering. Region Uppsala ska dokumentera intrångsskyddet och intrångsdetekteringen.

13.21 I Tjänsteleveransen ingående it-system ska i enlighet med punkten 4.1 kontrolleras och säkerhetstestas i enlighet med rekommendationer från respektive it-systems leverantör. Dokumentation från genomförda säkerhetstester ska publiceras i förvaltningens dokumentationssystem så att den även är tillgänglig för PUA.

Skydd mot obehörig avlyssning och insyn

13.22 Samtliga it-system där PUA:s Information hanteras under Avtalet ska vara försedda med adekvat skydd mot obehörig avlyssning och insyn (t.ex. Krav på autentisering, kryptering m.m.).

13.23 Vid kryptering av information ska etablerade och pålitliga algoritmer samt nyckellängder användas. Etablerade och pålitliga algoritmer samt nyckellängder innebär i detta sammanhang att algoritmer och nyckellängder som angetts som 'Acceptable' i senaste version av NIST Special Publication 800-131A ska användas. Styrgruppen har möjlighet att besluta om tillämpning av annan standard både som enskilda undantag eller som ett generellt byte av standard.

13.24 Kryptering enligt ovan skall tillämpas då PUA:s uppgifter transporteras över öppna nät samt vid lagring på digitala medier oavsett om de är fristående eller monterade i en dator.

Hantering av digitala lagringsmedier

13.25 Ett lagringsmedium som innehåller eller har innehållit PUA:s Information får endast återanvändas av behörig personal.

13.26 Vid ett eventuellt utlämnande av PUA:s uppgifter, som endast kan ske efter beslut av PUA, skall RU hantera utlämningen enligt instruktioner som ges av PUA i det enskilda fallet.

13.27 När ett lagringsmedium som innehåller eller har innehållit PUA:s Information utrangeras ska det destrueras enligt metod som godkänts av styrgruppen. Region Uppsala ska föreslå metod för destruering om annat inte överenskommits skriftligen mellan Parterna.

14 Ersättning för kostnader till följd av säkerhetskrav

14.1 Samverkansavtalet reglerar hur kostnader för systemleveransen hanteras mellan deltagande regioner. Till dessa hör alla kostnader som uppstår som en direkt konsekvens av tjänsteleveransen och dess systemförvaltning inklusive de kostnader som uppstår till följd här ställda säkerhetskrav. Region Uppsala äger dock inte rätt att bilägga kostnader för allmänt IT-stöd eller IT-säkerhetsarbete som utförs generellt i regionen, ens om det kan anses vara till nytta för den tjänsteleverans som täcks av samverkansöverenskommelsen.

Bilaga 3 - Lista över godkända Underbiträden

Den Personuppgiftsansvarige godkänner att Personuppgiftsbiträdet anlitar nedanstående Underbiträden för Behandling av Personuppgifter.

Bolag/ organisation	Adress och kontaktuppgifter	Lokalisering av Personuppgifter (adress, land)	Typer av Personuppgifter som Behandlas av Underbiträdet	Ändamål med Underbiträdets Behandling	Behandlingstid	Ytterligare information om Underbiträdets Behandling av Personuppgifter
Proact Sweden AB	Frösundaviks Allé, 169 70 Solna, Mårten Wikforss +46 702 4326 04 marten.wikforss@conoa.se	Sverige	Alla uppgifter som behandlas i SBR, uppgifter om användare och deras åtgärder i systemet samt motsvarande för IT-personalens arbete med teknisk förvaltning.	Att tillhandahålla IT-miljöer för SBR	240124-250124	Ombudets behandling avser lagring av uppgifter som behandlas i berörda system.
Signicat AB	Kungsgatan 64 111 22 Stockholm Thomas Kjøglum +47 99 77 83 77 privacy@signicat.com	Sverige, Norge	Personuppgifter från information i BankID. Uppgifter om ärendet vilket kan innefatta uppgift om tagna prover, vårdenhet samt personens ställningstaganden för provernas användning.	Behandling sker i syfte att ställa ut en digital kryptografisk signatur för ärende om samtyckesreglering samt för inloggning.	221026-251026	-
Post-Nord Strålfors AB	Terminalvägen 24 171 73 Solna Ingela Hertz +46 10 436 5695 Ingela.hertz@postnord.com	Sverige	Namn, Adress Personnummer/samordningsnummer Uppgifter om ärendet vilket kan innefatta uppgift om tagna prover, vårdenhet samt personens ställningstaganden för provernas användning.	Utskrift och försändelse av handlingar för ett samtyckesärende.	230502-270219	Behandlingen omfattas även av Postlagen (2010:1045)

SBR PuB-avtal Region Västmanland 2024-10-22

Final Audit Report 2024-12-09

Created:	2024-12-06
By:	Maria Gray (maria.gray@regionuppsala.se)
Status:	Signed
Transaction ID:	CBJCHBCAABAAfDQf4NiJzg4WIAV_7gIU-F6oU1Yj7XKe

"SBR PuB-avtal Region Västmanland 2024-10-22" History

Document created by Maria Gray (maria.gray@regionuppsala.se)
2024-12-06 - 8:01:11 AM GMT- IP address: 83.254.149.123

Document emailed to Mikael Köhler (mikael.kohler@regionuppsala.se) for signature
2024-12-06 - 8:03:35 AM GMT

Document emailed to lars.almroth@regionvastmanland.se for signature
2024-12-06 - 8:03:35 AM GMT

Email viewed by lars.almroth@regionvastmanland.se
2024-12-06 - 9:28:46 AM GMT- IP address: 52.102.16.149

Signer lars.almroth@regionvastmanland.se entered name at signing as Lars Almroth
2024-12-06 - 9:42:42 AM GMT- IP address: 172.225.69.153

Document e-signed by Lars Almroth (lars.almroth@regionvastmanland.se)
Signature Date: 2024-12-06 - 9:42:44 AM GMT - Time Source: server- IP address: 172.225.69.153

Email viewed by Mikael Köhler (mikael.kohler@regionuppsala.se)
2024-12-09 - 9:13:41 AM GMT- IP address: 192.36.34.244

Document e-signed by Mikael Köhler (mikael.kohler@regionuppsala.se)
Signature Date: 2024-12-09 - 5:00:13 PM GMT - Time Source: server- IP address: 192.36.34.245

Agreement completed.
2024-12-09 - 5:00:13 PM GMT