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.