Personuppgiftsbiträdesavtal Sunet Molnportal

Avtal enligt artikel 28.3 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), nedan kallad dataskyddsförordningen.

1. Parter

Personuppgiftsansvarig:	Uppsala universitet, NBIS, Institutionen för cell- och molekylärbiologi Org. nr. 202100-2932 BOX 596 751 24 Uppsala
Personuppgiftsbiträde	Vetenskapsrådet, Avdelningen för Sunet och anknutna tjänster org.nr 202100–5208 Tulegatan 11 pl 3, 113 53. Stockholm.

2. Giltighet

Personuppgiftsansvarig har tecknat avtal om köp av *Sunet Molnportal* (nedan kallat Tjänsten) av Personuppgiftsbiträdet. Personuppgiftsbiträdesavtalet gäller tillsvidare och upphör att gälla först när personuppgiftsbiträdet har slutat behandla personuppgifterna för den personuppgifts- ansvariges räkning. Detta Biträdesavtal ersätter i förekommande fall tidigare personuppgiftsbiträdesavtal när det gäller tjänsten *Sunet Molnportal*.

I händelse av konflikt mellan bestämmelserna i personuppgiftsbiträdesavtalet och tjänsteavtalet ska biträdesavtalets bestämmelser ha företräde när de avser Personuppgiftsbiträdets behandling av personuppgifter.

Detta personuppgiftsbiträdesavtal består av detta dokument inklusive Bilaga 1–3.

3. Bakgrund och syfte

Personuppgiftsansvarig köper Tjänsten, som tillhandahålls av avdelningen för Sunet vid Vetenskapsrådet. Användningen av Tjänsten innebär att detta biträdesavtal behöver tecknas för person-uppgiftsbehandlingen som följer av nyttjandet av tjänsten. Personuppgiftsbiträdet behandlar personuppgifter för de anslutnas räkning. Personuppgiftsbiträdesavtalet reglerar ansvar och åtaganden för personuppgiftsbiträdets behandling av personuppgiftsansvarigs personuppgifter.

Personuppgiftsbiträdesavtalet, som sådant, syftar till att säkerställa de registrerades fri- och rättigheter när personuppgiftsansvarig anlitar ett personuppgiftsbiträde vid behandling av personuppgifter och för att uppfylla artikel 28.3 i dataskyddsförordningen.

4. Definitioner

Personuppgiftsbiträdesavtalet använder definitionerna i artikel 4 dataskyddsförordningen avseende följande begrepp: personuppgiftsansvarig, personuppgiftsbiträde, personuppgifter, behandling (av personuppgifter) och personuppgiftsincident.

Övriga begrepp definieras enligt följande:

Registrerad	Den som uppgifterna avser.
Tredjeland	En stat som inte igår i Europeiska unionen eller är ansluten till europeiska ekonomiska samarbetsområdet.
Dataskyddslagstiftning	Sådan lagstiftning som är tillämplig på behandlingen av personuppgifter enligt detta avtal.

5. Behandling av personuppgifter, ändamål, typen av personuppgifter m.m.

Vid användning av Tjänsten kommer personuppgifter att behandlas hos Personuppgiftsbiträdet eller anlitade underbiträden. De kategorier av persondata som behandlas i Tjänsten är:

De personuppgifter som behandlas är samtliga förekommande personuppgifter i det material som Personuppgiftsansvarig lagrar i Tjänsten (inklusive känsliga personuppgifter, om den Personuppgiftsansvarige tillåter det), samt de uppgifter som behövs för att kunna tillhandahålla Tjänsten.

Några av de kategorier av uppgifter som behandlas kan vara:

- namn
- inloggnings-ID eller annan personlig unik identifierare
- kontaktinformation, t.ex. E-post, eller telefonnummer
- organisations-, grupp- och rolltillhörighet (t.ex. anställd/student/forskare/övrigt)
- behörighet till specifika tjänster
- publika nycklar eller andra åtkomstmekanismer
- IP-adress, samt viss annan metadata associerad med Internetprotokoll

Beskrivning av personuppgiftsbehandlingen inom ramen för tjänsten framgår av bilaga 1. Personuppgiftsbiträdet får endast behandla personuppgifterna i enlighet med dataskyddslagstiftningen och detta personuppgiftsbiträdesavtal med tillhörande skriftliga instruktioner i bilaga 1.

6. Personuppgiftsansvariges åtaganden

Den personuppgiftsansvarige ansvarar för och ska säkerställa att behandlingen av personuppgifter sker i enlighet med dataskyddslagstiftningen, bland annat att det finns en rättslig grund för aktuella behandlingar. Vidare ska den personuppgiftsansvarige utforma skriftliga instruktioner för att personuppgiftsbiträdet och eventuella underbiträden ska kunna fullgöra sitt eller sina uppdrag enligt personuppgiftsbiträdesavtalet.

Den personuppgiftsansvarige ska, utan dröjsmål, skriftligen informera personuppgiftsbiträdet om förändringar i behandlingen som påverkar personuppgiftsbiträdets skyldigheter.

Om personuppgiftsbiträdet saknar instruktioner som biträdet bedömer nödvändiga för att genomföra sitt uppdrag som personuppgiftsbiträde ska den personuppgiftsansvarige utan dröjsmål lämna sådana instruktioner.

Den personuppgiftsansvarige ansvarar för att informera registrerade om behandlingarna av personuppgifterna enligt dataskyddsförordningens krav samt i de fall som krävs inhämta samtycke från den registrerade.

7. Personuppgiftsbiträdets åtaganden

7.1. Generella åtaganden

Personuppgiftsbiträdet och den eller de personer som arbetar under biträdets ledning får bara behandla personuppgifter i enlighet med gällande dataskyddslagstiftning, detta biträdesavtal samt skriftliga instruktioner från den personuppgiftsansvarige.

Personuppgiftsbiträdet ska omedelbart informera den personuppgiftsansvarige om biträdet saknar instruktioner som bedöms nödvändiga för att genomföra uppdraget eller om personuppgiftsbiträdet anser att en instruktion strider mot dataskyddsförordningen eller mot andra av unionens eller medlemsstaternas dataskyddsbestämmelser.

Personuppgiftsbiträdet ska, i så stor utsträckning som möjligt, bistå den personuppgiftsansvarige för att säkerställa regelefterlevnad.

Personuppgiftsbiträdet ska utan dröjsmål informera den personuppgiftsansvarige om eventuella kontakter från tillsynsmyndigheten som rör eller kan vara av betydelse för behandlingen av personuppgifter.

Personuppgiftsbiträdet får inte företräda den personuppgiftsansvarige gentemot tillsynsmyndigheten om inte parterna har avtalat om en sådan ordning.

Vid förfrågningar som rör ansvaret för behandlingen av personuppgifter som omfattas av avtalet ska personuppgiftsbiträdet hänvisa till den personuppgiftsansvarige.

Personuppgiftsbiträdet ska inte lämna ut personuppgifter eller annan information om behandlingen av personuppgifter utan uttrycklig instruktion från den personuppgiftsansvarige. Detta gäller inte om personuppgiftsbiträdet omfattas av en författningsreglerad skyldighet för ett sådant utlämnande.

Personuppgiftsbiträdet får inte nyttja information om behandlingen av personuppgifter för andra ändamål än vad som följer av detta avtal.

7.2. Säkerhetsåtgärder

Personuppgiftsbiträdet ska i enlighet med gällande dataskyddslagstiftning, tillämpliga rekommendationer från tillsynsmyndighet och den personuppgiftsansvariges instruktioner vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna mot förstöring, ändring, otillåten spridning och obehörig tillgång samt mot varje annat slag av otillåten behandling.

Personuppgiftsbiträdet ska vidta alla åtgärder som krävs enligt artikel 32 dataskyddsförordningen. Bedömningen av säkerhetsnivå ska göras utifrån kriterierna för en sådan avvägning som anges i samma artikel.

7.3. Sekretess

Personuppgiftsbiträdet får inte lämna ut eller på annat sätt till tredje man röja information om behandlingen av personuppgifter som omfattas av detta avtal. Biträdet får heller inte nyttja information om behandlingen av personuppgifter för andra ändamål än vad som följer av detta personuppgifts-biträdesavtal.

Part får inte för tredje man röja information om den andra parten som part erhållit med anledning av detta avtal om inte

- parten kan visa att informationen var allmänt känd vid tidpunkten för mottagandet,
- om annat följer av lag eller förordning, eller
- parten föreläggs av behörig myndighet att utge informationen till myndigheten eller till tredje man.

Personuppgiftsbiträdet får i övrigt endast lämna ut personuppgifter på instruktion och efter godkännande från den personuppgiftsansvarige.

Personuppgiftsbiträdet ska se till att berörd personal informeras om och iakttar vid var tid gällande sekretess. Tystnadsplikt gäller även efter detta avtals upphörande.

7.4. Kapacitet och förmåga

Personuppgiftsbiträdet ska för behandlingen av personuppgifter besitta nödvändig teknisk och organisatorisk kapacitet och förmåga såsom tekniska lösningar, sakkunskap och annan relevant kompetens, ekonomiska och personella resurser, rutiner och metoder för att fullgöra sina skyldigheter i enligt dataskyddslagstiftningen, personuppgiftsbiträdesavtalet samt det avtal till vilket biträdesavtalet hör.

8. Granskning och kontroll

Personuppgiftsansvarig har rätt att, själv eller genom ombud, kontrollera att personuppgiftsbiträdet följer personuppgiftsbiträdesavtalet. Samma rätt ska gälla i förhållande till underbiträden. Personuppgiftsbiträdet eller underbiträdet ska lämna personuppgiftsansvarig den assistans som behövs vid en sådan kontroll.

Om tillsynsmyndigheten eller annan myndighet med tillsynsuppdrag inleder granskning av sådan behandling av personuppgifter som utförs av personuppgiftsbiträdet ska biträdet bistå den

personuppgiftsansvarige för att möjliggöra sådan granskning. Detsamma gäller om en enskild väcker talan mot den personuppgiftsansvarige.

9. Registrerades rättigheter

Personuppgiftsbiträdet ska på begäran och i möjlig utsträckning bistå den personuppgiftsansvarige att tillgodose de rättigheter som tillkommer den registrerade enligt dataskyddslagstiftningen.

Personuppgiftsbiträdet ska utan dröjsmål vidta rättelse av felaktiga eller ofullständiga personuppgifter efter instruktion från den personuppgiftsansvarige.

10. Drift och underhåll

Personuppgiftsbiträdet ska kontinuerligt logga åtkomst till personuppgifter enligt detta avtal i den utsträckning som krävs enligt instruktion från den personuppgiftsansvarige.

Om personuppgiftsbiträdet avser att göra förändringar i sina system på sätt som kan förväntas påverka informationshanteringen ska personuppgiftsbiträdet informera den personuppgiftsansvarige om detta.

11. Personuppgiftsincidenter

Vid obehörig behandling, obehörig åtkomst, förstörelse eller ändring av personuppgifter ska personuppgiftsbiträdet utan dröjsmål, dock senast inom 48 timmar från att biträdet fått kännedom om incidenten, underrätta den personuppgiftsansvarige om att en personuppgiftsincident har inträffat. Underrättelsen ska ställas till adress enligt punkt 18 nedan.

Personuppgiftsbiträdet ska tillhandahålla den personuppgiftsansvarige en beskrivning av personuppgiftsincidenten samt bistå den personuppgiftsansvarige att fullgöra dennes skyldigheter enligt artiklarna 33 och 34 i dataskyddsförordningen.

12. Underbiträden

Personuppgiftsbiträdet har inte rätt att anlita andra underbiträden för behandling av personuppgifter utan godkännande från den personuppgiftsansvarige. Information om underleverantörer finns i bilaga 2.

Först efter ett godkännande får och ska personuppgiftsbiträdet teckna avtal med underbiträden. Ett sådant avtal ska motsvara villkoren för behandlingen av personuppgifterna som gäller enligt detta avtal. Detta för att säkerställa att underbiträdet omfattas av samma åtaganden och skyldigheter som personuppgiftsbiträdet. Personuppgiftsbiträdet ska efter undertecknandet på begäran skicka en kopia av underbiträdesavtalet till den personuppgiftsansvarige. Den personuppgiftsansvarige ska ha rätt att på begäran få ta del av underbiträdesavtalet före undertecknandet.

Anlitande av underbiträde påverkar inte personuppgiftsbiträdets skyldigheter gentemot den personuppgiftsansvarige. Personuppgiftsbiträdet ansvarar på samma sätt för ett anlitat underbiträdes behandling av personuppgifterna.

Personuppgiftsbiträdet ska i god tid informera den personuppgiftsansvarige om eventuella planer på att upphöra att använda sig av ett godkänt underbiträde.

13. Överföring av personuppgifter till tredje land

Om personuppgifter ska överföras till tredje land ska den personuppgiftsansvarige, efter samråd med personuppgiftsbiträdet och i enlighet med dataskyddsförordningens bestämmelser (artikel 44–46), besluta om ett förfarande som innebär att behandlingen är tillåten. Hur sådan behandling ska genomföras ska framgå av instruktioner från den personuppgiftsansvarige. Personuppgiftsbiträdet får endast överföra personuppgifter till tredjeland på instruktioner från den personuppgiftsansvarige.

14. Ansvar för skada

Personuppgiftsbiträdet ska hålla den personuppgiftsansvarige skadelös för skada som uppkommit till följd av behandling av personuppgifter som innebär att biträdet inte har fullgjort sina skyldigheter enligt bestämmelser i dataskyddslagstiftningen som specifikt riktar sig till personuppgiftsbiträdet eller att biträdet har agerat utanför eller i strid med detta personuppgiftsbiträdesavtal med tillhörande instruktioner (artikel 82.1–3 dataskyddsförordningen).

15. Upphörande av behandling

När personuppgiftsbiträdesavtalet upphör, oavsett orsak, ska personuppgiftsbiträdet överlämna eller radera personuppgifter på det sätt som anges av den personuppgiftsansvarige samt vidta relevanta åtgärder för att se till att inga personuppgifter finns kvar hos personuppgiftsbiträdet.

16. Ändringar och tillägg m.m.

Ändringar av och tillägg till personuppgiftsbiträdesavtalet ska vara skriftliga och undertecknas av båda parter.
Parterna får inte utan skriftligt medgivande från den andra parten överlåta eller på annat sätt överföra sina rättigheter och skyldigheter eller sätta annan i sitt ställe.

17. Lagval och tvistlösning

Tvister om tolkning eller tillämpning av personuppgiftsbiträdesavtalet ska lösas genom förhandling mellan parterna på ledningsnivå eller, om parterna är statliga förvaltningsmyndigheter, slutligen avgöras av regeringen.

Om personuppgiftsbiträdet eller personuppgiftsansvarig inte är en statlig myndighet ska tvister slutligen avgöras i allmän domstol enligt svensk rätt.

18. Övrigt

Parterna ska utse var sin kontaktperson med ansvar för parternas samarbete. Ändring av kontaktperson eller kontaktuppgifter ska skriftligen meddelas den andra parten. Meddelanden om incidenter ska skickas till den personuppgiftsansvarige på denna mailadress: dataskyddsombud@uu.se

Det ska inte utgå någon ersättning för personuppgiftsbiträdets behandling av personuppgifter enligt personuppgiftsbiträdesavtalet.

Personuppgiftsbiträdesavtalet har upprättats i två (2) exemplar varav parterna har tagit var sitt.

Ort: Uppsala
Datum: 2023-10-12
För personuppgiftsansvarig:

Bengt Persson

Föreståndare, NBIS

Uppsala universitet

Stockholm
2023-10-17
För personuppgiftsbiträdet:

Maria Häll

Avdelningschef

Avdelningen för SUNET, Vetenskapsrådet

Bilaga 1
Instruktioner för personuppgiftsbiträdes behandling av Personuppgiftsansvarigs personuppgifter
Bilaga 2
Underbiträden
Bilaga 3
Tillägg avseende personuppgiftsbiträdesavtal med Uppsala universitet

Bilaga 1

- **Instruktioner för personuppgiftsbiträdets behandling av Personuppgiftsansvarigs personuppgifter**

Utöver vad som framgår av personuppgiftsbiträdesavtalet ska personuppgiftsbiträdet behandla de aktuella personuppgifterna enligt följande instruktioner.

Ändamål

Personuppgiftsbiträdet får endast behandla personuppgifterna för ändamålen som framgår i avsnitt 5 i personuppgiftsbiträdesavtalet. Personuppgiftsbiträdet får även behandla personuppgifterna för att uppfylla de åtaganden som personuppgiftsbiträdet har enligt personuppgiftsbiträdesavtalet och för andra författningsrättsliga skyldigheter, exempelvis att lämna uppgifter till en tillsynsmyndighet eller att lämna ut uppgifter enligt offentlighetsprincipen.

Personuppgifter som får behandlas

De kategorier av personuppgifter som får behandlas framgår i avsnitt 5 i personuppgiftsbiträdesavtalet. Personuppgiftsbiträdet får även behandla andra personuppgifter om det är nödvändigt för att uppfylla de åtaganden som personuppgiftsbiträdet har enligt detta avtal och tjänsteavtalet.

Kategorier av registrerade

De registrerade utgör anställda, studenter, uppdragstagare eller annan person som utför arbete för eller samverkar med den personuppgiftsansvarige.

Tillåten behandling

Personuppgiftsbiträdet får behandla personuppgifterna endast för att fullgöra sitt uppdrag och i enlighet med de instruktioner som lämnats av den personuppgiftsansvarige.

Personuppgifterna får behandlas endast för ovanstående ändamål och för den personuppgiftsansvariges räkning. Personuppgiftsbiträdet får inte använda personuppgifterna för några andra ändamål.

Personuppgiftsbiträdet ska behandla personuppgifterna på följande sätt:

- För att tillhandahålla och administrera Tjänsten.
- För drift, underhåll och support.
- Besvara förfrågningar från och tillhandahålla support till de registrerade.

Personuppgifter som behandlas av personuppgiftsbiträdet får endast lämnas ut till

- behörig personal hos den personuppgiftsansvarige, och
- den som personuppgifterna avser (den registrerade).

Särskilda säkerhetskrav

För att åstadkomma i avtalet föreskriven säkerhetsnivå ska personuppgiftsbiträdet se till att:

- arbetsrutiner och arbetsuppgifter är utformade på ett sådant sätt att det blir möjligt för personalen att arbeta och tänka säkerhetsmedvetet,
- där det är möjligt använda pseudonymisering och kryptering av personuppgifter,
- ha förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos de system och tjänster som behandlar personuppgifter,
- har förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,
- ha ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska, administrativa och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet,
- personalen informeras om vikten av att följa gällande säkerhetsrutiner,
- IT-utrustning som används för behandling av personuppgifter har ett tillfredsställande skydd mot stöld och händelser som kan förstöra utrustningen,
- nödvändiga åtgärder vidtas för att förhindra att personuppgifter förstörs, ändras eller förvanskas vid överföring via nät och för att skydda anslutna tjänster mot obehörig åtkomst,

- ha ett system för behörighetskontroll finns för att förhindra obehörig åtkomst, och
- att utrustning som är ansluten till internet eller annat öppet nät skyddas från obehörig trafik.

Loggar

Personuppgiftsbiträdet ansvarar för att genom dokumentation (inklusive loggar) av åtkomst kunna visa hur uppgifterna om den registrerade har hanterats (hur och när) och av vem/vilka.

Tredjelandsöverföring

Inom ramen för personuppgiftsbiträdets behandling av Personuppgiftsansvarigs personuppgifter kommer uppgifterna inte att överföras till tredje land.

Gallring

När den personuppgiftsansvarige har markerat en registrerad för radering ska personuppgiftsbiträdet radera samtliga uppgifter om den registrerade, alternativt avidentifiera samtliga uppgifter på ett sådant sätt som medför att den registrerade inte längre kan identifieras. Dessa åtgärder ska vidtas utan oskäligt dröjsmål, dock senast inom 90 dagar.

När avtalet rörande tjänsterna och/eller personuppgiftsbiträdesavtalet upphör ska samtliga personuppgifter raderas från personuppgiftsbiträdets system. Detta ska ske så snart det är praktiskt möjligt.

Bilaga 2. Underbiträden

Blue Safespring AB	org.nr 559075–0245 Smidesvägen 12, 6 tr. 171 41, Solna

Bilaga 3. Tillägg avseende personuppgiftbiträdesavtal med Uppsala universitet

Mot bakgrund av dialog mellan personuppgiftsansvarig och personuppgiftsbiträde gällande detaljer i detta Avtal har följande bilaga slutits till detta Avtal för att förtydliga rubricerade områden.

Bakgrund

Uppsala universitet behandlar personuppgifter för andra svenska lärosätens räkning rörande behandling av personuppgifter som deponerats hos FEGA Sweden, dvs. den Svenska noden av Federerade EGA. Inom ramen för ovan nämnda personuppgiftsbehandling vill Uppsala universitet såsom primärt personuppgiftsbiträde använda sig av Sunets tjänst *Molnportal* och därmed anlita Sunet såsom personuppgiftsunderbiträde för behandling av de personuppgifter som Uppsala universitet behandlar för personuppgiftsansvarigs (övriga lärosäten) räkning. Uppsala universitet och Sunet är överens om att Sunet ska behandla sådana personuppgifter för Uppsala universitets räkning på villkor som följer av detta avtal.

Detta avtal ska säkerställa att de personuppgifter som omfattas av Sunets Behandling hanteras i enlighet med de krav som följer av Dataskyddsförordningen, annan gällande lagstiftning och etablerad standard samt att personuppgifterna inte blir tillgängliga för obehöriga. Mot bakgrund av att Uppsala universitet på sätt som redogörs för här har åtaganden gentemot övriga personuppgiftsansvariga har i denna bilaga särskilt rubricerande områden förtydligats för att säkerställa att de åtaganden som Uppsala universitet tagit på sig också omhändertas av Sunet. Det noteras att begreppen Personuppgiftsansvarig (Uppsala Universitet) och Personuppgiftsbiträde (Sunet – Vetenskapsrådet) i huvudavtalet ska tillämpas utifrån de förutsättningar som givits i denna bakgrund, det vill säga att Uppsala universitet är ett personuppgiftsbiträde gentemot deltagande lärosäten och Sunet agerar som underbiträde till Uppsala universitet.

Förtydligande av punkten 5 ”Behandling av personuppgifter, ändamål, typen av personuppgifter m.m.”

Specificering av behandlade personuppgifter – känsliga personuppgifter

Mot bakgrund av att tjänsten som tillhandahålls är en ren innehållstjänst så saknar personuppgiftsbiträde kontroll över vilken information som lagras i tjänsten av den personuppgiftsansvarige. Med det sagt kommer Uppsala Universitet inom ramen för användningen av denna tjänst inom FEGA Sweden använda tjänsten för lagring av känsliga personuppgifter i enlighet med artikel 9 Dataskyddsförordningen, bland annat genetiska uppgifter och uppgifter om hälsa.

Personuppgiftsbiträdets direktåtkomst till lagrad information

Personuppgiftsbiträde har teknisk möjlighet att ha direktåtkomst till information som lagras i tjänsten men utnyttjar denna möjlighet enbart på direkt uppdrag av personuppgiftsansvarige.
Personuppgiftsansvarig kan genom att tillämpa kryptering eller liknande mekanismer motverka personuppgiftsbiträdets möjligheter till direktåtkomst till lagrad information.

Kategorier av registrerade

Personuppgiftsbiträdet saknar kontroll över vilka personuppgifter som lagras i lagringsutrymmet och således också vilka de väljer att lagra där. Med det sagt kommer Uppsala Universitet inom ramen för användningen av denna tjänst inom FEGA Sweden använda tjänsten för lagring av uppgifter inom ramen för forskningsprojekt varför känsliga personuppgifter tillhörande individer som deltagit i forskningsstudier som genererar genetisk och/eller fenotypisk information.

Kategorier av uppgifter som behandlas är:

- namn
- inloggnings-ID eller annan personlig unik identifierare
- kontaktinformation, t.ex. E-post, eller telefonnummer
- organisations-, grupp- och rolltillhörighet (t.ex. anställd/student/forskare/övrigt)
- behörighet till specifika tjänster
- publika nycklar eller andra åtkomstmekanismer

- IP-adress, samt viss annan metadata associerad med Internetprotokoll
- Pseudonymiserade molekylära data, genomikdata, bilddata eller andra datatyper genererade från analys av prover inlämnade till infrastrukturenheten inom serviceprojekt, samt metadata med relevans för projektet, beskrivande utförd analys och eventuell provbehandling. Det kan t.ex. vara genetisk sekvensinformation från individer eller andra datatyper och information, enligt ovan, som rör hälsa. Dessa personuppgifter är normalt känsliga personuppgifter då de berör den registrerades hälsa.

Periodvisa genomgångar

Personuppgiftsansvarige ska initiera genomgångar.

Förtydligande av avsnitt 7.1 "Personuppgiftbiträdets skyldigheter"

De skyldigheter som redogörs för i avsnitt 7.1 kompletteras med följande förtydliganden.
Personuppgiftsbiträdet ska vidta alla rimliga åtgärder för att bistå Personuppgiftsansvarig för det fall det sker en incident eller någon registrerad begär att få nyttja någon av sina rättigheter enligt Dataskyddsförordningen.

Förtydligande av avsnitt 8 "Granskning och kontroll"

Uppföljningsmöte mellan personuppgiftsansvarig och personuppgiftsbiträdet ska genomföras en gång om året.

Förtydligande av avsnitt 12 "Underbiträde"

De skyldigheter som redogörs för i avsnitt 12 kompletteras med följande förtydliganden.
Med formuleringen "Personuppgiftsbiträdet ansvarar på samma sätt för ett anlitat underbiträdes behandling av personuppgifterna." avses att om anlitade underbitärden inte uppfyller sina skyldigheter i fråga om behandling enligt ett underbiträdesavtal är personuppgiftsbiträdet som anlitat underbiträdet fullt ansvarig gentemot personuppgiftsansvarig.

Förtydligande av avsnitt 14, "Ansvar för skada"

De skyldigheter som redogörs för i avsnitt 14 kompletteras med följande förtydliganden.
Dataskyddsförordningens reglering i artikel 82 ska i sin helhet tillämpas vad gäller ansvar för skada. För annan skada än sådan angiven i punkt 14 svarar Parterna med eventuella begränsningar när så framgår av tjänsteavtalet. Parterna är överens om att sanktionsavgifter enligt artikel 83 Dataskyddsförordningen eller 6 kap. 2 § lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning inte utgör skada enligt denna punkt utan ska bäras av den Part som påförts sådan avgift.

Förtydligande av Bilaga 1 – "Kategorier av registrerade"

De registrerade utgör anställda, studenter, uppdragstagare eller annan person som utför arbete för eller samverkar med den personuppgiftsansvarige. Individer som deltagit i forskningsstudier som genererar data för forskningsändamål.

Förtydligande av Bilaga 1 – "Särskilda säkerhetskrav"

Personuppgiftsbiträdet ska arbeta i enlighet med föreskrifter och allmänna råd från myndigheten för samhällsskydd och beredskap, MSBFS 2020:6, MSBFS 2020:7 och MSBFS 2020:8.

Detta innebär att personuppgiftsbiträdet har genomfört informationsklassificering och en analys baserad på informationssäkerhetsmässiga krav enligt svensk och internationell standard SS-ISO/IEC 27001.

Underbiträdet garanterar att

- Informationssäkerhetsarbete bedrivs i enlighet med ISO/IEC 27001 eller motsvarande inom detta område.

- Utveckling av personuppgiftsbiträdets informationssystem/IT-tjänster genomförs med hänsyn till informationssäkerhet, det vill säga krav på konfidentialitet, riktighet och tillgänglighet.
- Grundläggande för personuppgiftsbiträdets hantering av informationssäkerhet är: åtkomstbegränsning, riktighet, spårbarhet och tillgänglighet.
- Skalskydd till personuppgiftsbiträdets lokaler finns i form av lås och larm. Procedurer finns för tilldelning respektive hantering av utrustning och behörighet och ses över regelbundet.
- Skyddsmekanismer finns i form av brandvägg.
- Endast behörig personal har tillgång till personuppgiftsbiträdets IT-miljö.
- Personuppgiftsbiträdet har administrativa rutiner och tekniska åtgärder för att information från olika kunder särskiljs.
- Personuppgiftsbiträdet arbetar efter implementerade ledningssystem för informationssäkerhet, som reglerar uppföljning av IT-säkerhetsincidenter.
- Personuppgiftsbiträdet kommer att anmäla eventuella Personuppgiftsincidenter som berör Biträdets data i uppdraget enligt erhållen kontaktinformation.