

# **Mall Avtal för gemensamt personuppgiftsansvar**

Klinisk forskning

**Detta dokument är framtaget och kvalitetssäkrat av Kliniska Studier Sverige.**

Vi utvecklar och erbjuder stöd för kliniska studier i hälso- och sjukvården.

Stödet vi erbjuder ger goda förutsättningar för kliniska studier av hög kvalitet.

Om dokumentet

Mall Avtal för gemensamt personuppgiftsansvar publicerades första gången den 2022-03-21.

Avtal för gemensamt personuppgiftsansvar

ingått mellan

[Part A]

och

[Part B]

den 20ÅÅ-MM-DD

Innehåll

[1. Bakgrund och syfte 3](#_Toc112760901)

[2. Definitioner och tolkning 3](#_Toc112760902)

[3. Behandling av personuppgifter 4](#_Toc112760903)

[4. Etikprövning 5](#_Toc112760904)

[5. Registrerades rättigheter 5](#_Toc112760905)

[6. Tekniska och organisatoriska säkerhetsåtgärder 5](#_Toc112760906)

[7. Konsekvensbedömning avseende dataskydd 6](#_Toc112760907)

[8. Ansvarig tillsynsmyndighet vid gränsöverskridande behandling 6](#_Toc112760908)

[9. Personuppgiftsincidenter 6](#_Toc112760909)

[10. Personuppgiftsbiträden 7](#_Toc112760910)

[11. Överföring av personuppgifter till tredjeland eller en internationell organisation 7](#_Toc112760911)

[12. Förteckning över behandling 7](#_Toc112760912)

[13. Kostnader 7](#_Toc112760913)

[14. Ansvar 7](#_Toc112760914)

[15. Tystnadsplikt 8](#_Toc112760915)

[16. Tvistelösning, tillämplig lag, m.m. 8](#_Toc112760916)

[17. Parternas undertecknande 9](#_Toc112760917)

[Bilaga 1 – Parter till detta Avtal 10](#_Toc112760918)

[Bilaga 2 – Dokumentation av Behandlingen 11](#_Toc112760919)

[Bilaga 3 – Hantering av registrerades rättigheter 14](#_Toc112760920)

[Bilaga 4 – Tekniska och organisatoriska säkerhetsåtgärder 16](#_Toc112760921)

[Bilaga 5 – Personuppgiftsbiträden 19](#_Toc112760922)

Detta avtal för gemensamt personuppgiftsansvar (”**Avtal**”) har ingåtts mellan de juridiska personer som dokumenterats i Bilaga 1, var för sig **Part**, och gemensamt **Parterna**.

## Bakgrund och syfte

* 1. Parterna är sponsor respektive prövningsställe för en klinisk läkemedelsprövning, vilket preciseras i Bilaga 2. Mot den bakgrunden har Parterna gemensamt, genom prövningsprotokollet för en klinisk läkemedelsprövning, bestämt ändamål och medel för behandling av personuppgifter och är därför gemensamt personuppgiftsansvariga.
  2. Detta Avtal, med bilagor, utgör Parternas arrangemang enligt artikel 26 GDPR.
  3. Detta Avtal syftar till att, under öppna former, fastställa respektive Parts ansvar för att fullgöra skyldigheterna enligt Dataskyddslagstiftning, särskilt vad avser den registrerades rättigheter och att tillhandahålla den registrerade med information.
  4. Detta Avtal reglerar Parternas respektive ansvar för att fullgöra skyldigheterna enligt Dataskyddslagstiftning. Detta Avtal ska därför inte tolkas på så sätt att det medför förpliktelser eller rättigheter avseende den kliniska läkemedelsprövningen i övrigt.

## Definitioner och tolkning

* 1. Följande begrepp definieras enligt följande och återges i detta Avtal med inledande versal:

”Avtal” avser detta Avtal för gemensamt personuppgiftsansvar, med bilagor.

”Behandlingen” avser den behandling av personuppgifter för vilken Parterna är gemensamt personuppgiftsansvariga och dokumenterats i Bilaga 2.

”Dataskyddslagstiftning” avser GDPR, enligt definition nedan, och annan vid var tid tillämplig dataskyddslagstiftning för behandlingen enligt Bilaga 2.

”GDPR” avser 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), eller sådan författning som, vid var tid, ersätter denna förordning.

”Konsekvensbedömning” avser en konsekvensbedömning avseende dataskydd enligt artikel 35 GDPR.

”SCC” avser Stockholms Handelskammares Skiljedomsinstitut.

”Sponsor” avser den Part eller de parter som är sponsor för den kliniska prövningen.

* 1. Begrepp som definieras i GDPR ska ha identisk betydelse i detta Avtal. Dessa begrepp återges inte med inledande versal.
  2. Begrepp i avsnitt 4, nedan, ska ha identisk betydelse som i lag (2003:460) om etikprövning av forskning som avser människor.
  3. Om detta Avtal är en bilaga till ett annat kontrakt mellan Parterna ska detta avsnitt 2, i sin helhet, äga företräde framför andra bestämmelser avseende definitioner vid tolkning och tillämpning av detta Avtal.
  4. I Avtalet ska, om inte annat framgår:
     1. referenser till bilagor, avsnitt och punkter vara referenser till bilagor, avsnitt och punkter i detta Avtal,
     2. bilagorna anses vara en integrerad del av Avtalet,
     3. singular inkludera plural och vice versa, och;
     4. rubrikerna inte påverka tolkningen av Avtalet.
  5. Inget i detta Avtal ska tolkas till nackdel för en Part med anledning av att Part upprättade Avtalet eller delar av Avtalet.

## Behandling av personuppgifter

* 1. Parterna är gemensamt personuppgiftsansvariga för den behandling som dokumenterats i Bilaga 2.
  2. Parterna är införstådda med att de är gemensamt ansvariga för att efterleva skyldigheterna som ankommer på personuppgiftsansvariga enligt GDPR. Mot den bakgrunden ska var Part säkerställa lämpliga tekniska och organisatoriska åtgärder för visa att Behandlingen utförs i enlighet med GDPR.
  3. Parterna är eniga om att det gemensamma ändamålet för Behandlingen, så som det dokumenterats i Bilaga 2, är ett vetenskapligt forskningsändamål enligt GDPR, om inte annat är uttryckligen dokumenterat i denna Bilaga 2.
  4. Parterna är eniga om att behandling som sker för ett annat ändamål än det ändamål som dokumenterats i Bilaga 2 ska bedömas som en ny behandling av personuppgifter, och att den Part, eller de parter, som bestämmer ändamål och medel för denna nya behandling är personuppgiftsansvarig för densamma.
  5. Parterna är eniga att om en Part är en svensk myndighet så är denna Part personuppgiftsansvarig, enskilt och inte gemensamt, för den behandling av personuppgifter som är nödvändig för ändamålen att efterleva tryckfrihetsförordningen (1949:105) och offentlighets- och sekretesslagen (2009:400).

Parterna är införstådda med att en myndighet, enligt författning, självständigt ska genomföra en bedömning om en behandling enligt denna punkt 3.5 är förenligt med Dataskyddslagstiftning.

Parterna är eniga om att Parts behandling av personuppgifter enligt denna punkt 3.5 inte ska tolkas som en överträdelse av detta Avtal.

* 1. Parterna är eniga om att den behandling av personuppgifter som en vårdgivare utför i Sverige för att efterleva patientdatalagen (2008:355) faller utanför ramen för detta Avtal. Parterna är eniga om att sådan behandling inte ska tolkas som en överträdelse av detta Avtal.
  2. Eftersom Parterna är gemensamt personuppgiftsansvariga kräver en ändring av Behandlingen enligt detta Avtal samtliga Parters skriftliga godkännande.

## Etikprövning

* 1. Behandlingen förutsätter föregående godkännande av Etikprövningsmyndigheten och att forskningspersonen lämnat sitt informerade samtycke till forskningen.
  2. I syfte att undvika missförstånd: detta Avtal syftar inte till att reglera Parternas inbördes ansvar inom ramen för ansvaret som forskningshuvudman. Sådan reglering ska genomföras enligt separat överenskommelse.

## Registrerades rättigheter

* 1. Parterna är införstådda med att en registrerad har rätt att, enligt GDPR, utöva sina rättigheter i förhållande till varje Part. Oaktat detta återfinns i Bilaga 3 den uppdelning som parterna väljer att göra mellan om sig om vem som har det huvudsakliga praktiska ansvaret att hantera frågeställningar kring de registrerades rättigheter
  2. Parterna får utse en gemensam kontaktpunkt för syftet att underlätta registrerades utövande av sina rättigheter. Om en Part utsetts som gemensam kontaktpunkt ska detta dokumenteras i Bilaga 3.
  3. Part ska tillse att en registrerad informeras om Behandlingen i samband med att denne lämnar sitt informerade samtycke till forskning, eller senast innan behandling av den registrerades personuppgifter enligt detta Avtal påbörjas.
  4. Part ska säkerställa att det finns skriftlig dokumentation som visar att en registrerad har tagit del av information, och vilken information den registrerade har tagit del av.
  5. Registrerade har rätt att ta del av de väsentliga innehållet i detta Avtal. Parterna är eniga om att det ska ske med beaktande av Parternas ömsesidiga tystnadsplikt enligt   
     avsnitt 15, nedan.

## Tekniska och organisatoriska säkerhetsåtgärder

* 1. Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska vardera Part genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att Behandlingen utförs i enlighet med GDPR och Dataskyddslagstiftning. Dessa åtgärder ska ses över och uppdateras minst en (1) gång per kalenderår.
  2. Eftersom behandlingen sker för ett vetenskapligt forskningsändamål ställs särskilda krav på skydd för den registrerades rättigheter och friheter. Skyddsåtgärderna ska säkerställa att tekniska och organisatoriska åtgärder har införts för att se till att särskilt principen om uppgiftsminimering iakttas. Dessa åtgärder ska inbegripa pseudonymisering, under förutsättning att det gemensamma ändamålet enligt Bilaga 2 kan uppfyllas på det sättet.
  3. Parterna är införstådda med att särskilda kategorier av personuppgifter och nationella identifikationsnummer behandlas och att detta ställer särskilda krav på tekniska och organisatoriska åtgärder.
  4. Mot bakgrund av detta avsnitt 6 ska Part efterleva de tekniska och organisatoriska säkerhetsåtgärder som dokumenterats i Bilaga 4. Inget i detta Avtal ska tolkas som ett hinder för en Part att införa längre gående tekniska eller organisatoriska åtgärder, mot bakgrund av riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter.

## Konsekvensbedömning avseende dataskydd

* 1. Innan behandlingen påbörjas ska Parterna gemensamt göra en bedömning om en Konsekvensbedömning ska genomföras avseende Behandlingen. Parterna ska särskilt beakta nationella beslut om när en Konsekvensbedömning ska genomföras. En Konsekvensbedömning ska alltid genomföras om en Part begär det. Ett beslut om att inte genomföra en Konsekvensbedömning ska vara enigt mellan Parterna och ska dokumenteras skriftligen.
  2. Parternas dataskyddsombud ska särskilt, inom ramen för detta avsnitt 7, ges möjlighet att (i) lämna ett yttrande om en Konsekvensbedömning ska genomföras eller inte, (ii) övervaka genomförandet av en Konsekvensbedömning, (iii) lämna ett yttrande om dataskyddsombudet delar slutsatserna i Konsekvensbedömningen eller inte, och (iv) om Parterna ska genomföra ett förhandssamråd.
  3. En Konsekvensbedömning som avser Behandlingen ska genomföras av en Part. Övriga parter ska bistå denna Part med information och råd för genomförande av konsekvensbedömningen avseende dataskydd.
  4. En konsekvensbedömning avseende dataskydd ska skriftlig godkännas av Parterna. Parterna ska därigenom även ta ställning till om Parterna ska begära ett förhandssamråd hon tillsynsmyndighet enligt GDPR.
  5. En Konsekvensbedömning, förutsatt att Parterna beslutat att genomföra en sådan, ska utan undantag vara avslutad och godkänd av Parterna innan Behandlingen påbörjas.

## Ansvarig tillsynsmyndighet vid gränsöverskridande behandling

* 1. Samtliga Parter har sitt huvudsakliga verksamhetsställe i Sverige. Parternas gemensamma tolkning är därför att den svenska tillsynsmyndigheten Integritetsskyddsmyndigheten är den ansvariga tillsynsmyndigheten för Behandlingen.

## Personuppgiftsincidenter

* 1. Parterna är införstådda med att de, inom ramen för Behandlingen, är gemensamt ansvariga för att efterleva förpliktelser enligt GDPR avseende anmälan av en personuppgiftsincident till en behörig tillsynsmyndighet och avseende information till registrerade om en personuppgiftsincident.
  2. Part ska omedelbart informera övriga parter om Part fått vetskap om en personuppgiftsincident eller misstänker att en personuppgiftsincident har inträffat. Denna förpliktelse att omedelbart informera övriga parter gäller även utanför kontorsarbetstid och under helgdagar.
  3. En personuppgiftsincident ska anmälas till behörig tillsynsmyndighet, enligt detta avsnitt 9, utan onödigt dröjsmål och, inte senare än sjuttiotvå (72) timmar från dess att en Part fått vetskap om personuppgiftsincidenten, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter.
  4. I syfte att undvika missförstånd ska vardera Part i enlighet med Bilaga 4 införa lämpliga tekniska och organisatoriska säkerhetsåtgärder för att minska risken för personuppgiftsincidenter.
  5. Parterna ska föra en gemensam förteckning över konstaterade eller misstänka personuppgiftsincidenter.

## Personuppgiftsbiträden

* 1. Part får uppdra åt ett personuppgiftsbiträde att behandla personuppgifter inom ramen för detta Avtal endast med samtliga Parters skriftliga godkännande. Ett personuppgiftsbiträde som dokumenterats i Bilaga 5 ska bedömas som anlitat med samtliga parters skriftliga godkännande enligt första meningen denna punkt 10.1.
  2. Innan en Part anlitar ett personuppgiftsbiträde ska denna Part säkerställa att personuppgiftsbiträdet kan lämna tillräckliga garantier om att genomföra tillräckliga tekniska och organisatoriska åtgärder för att säkerställa att behandlingen uppfyller kraven i GDPR och detta Avtal, samt säkerställa att de registrerades rättigheter skyddas. Mot denna bakgrund ska denna Part genomföra en riskbedömning för att säkerställa att personuppgiftsbiträdets garantier är tillräckliga.
  3. Part är ansvarig mot övriga Parter för att innehållet i det avtal eller rättsakt (personuppgiftsbiträdesavtal) som tecknats med personuppgiftsbiträdet uppfyller krav ställda i Dataskyddslagstiftning och i detta Avtal.

## Överföring av personuppgifter till tredjeland eller en internationell organisation

* 1. Om det inte uttryckligen är dokumenterat i Bilaga 2 att Behandlingen innefattar överföring av personuppgifter till ett tredjeland eller en internationell organisation, i bemärkelsen kapitel V GDPR, är den Part som överför personuppgifter till ett tredjeland eller en internationell organisation personuppgiftsansvarig, enskilt och inte gemensamt, för sådan överföring.

## Förteckning över behandling

* 1. Vardera Part ska föra en förteckning enligt artikel 30 GDPR (registerförteckning) som inbegriper den gemensamma behandlingen.

## Kostnader

* 1. Inom ramen för detta Avtal ska vardera Part bära sin egen kostnad, om inte annat är uttryckligen överenskommet mellan Parterna.

## Ansvar

* 1. Parterna är införstådda med att de är solidariskt ansvariga för skadestånd i förhållande till registrerad. Inget i detta Avtal ska tolkas på så sätt att det inskränker registrerads rätt till skadestånd enligt Dataskyddslagstiftning.
  2. Parterna har på grundval av detta Avtal en förpliktelse att begränsa skada mot annan Part. Mot denna bakgrund ska Part utan dröjsmål omedelbart informera övriga parter om en sådan skada eller risken för en sådan skada.
  3. Mot bakgrund av Parts ansvar att visa efterlevnad av de grundläggande principerna för behandling av personuppgifter inom ramen för Behandlingen ska Part säkerställa att denne har dokumentation som visar att detta Avtal efterlevs. I syfte att undvika missförstånd: Parts oförmåga att visa efterlevnad enligt artikel 5.2 GDPR ska betraktas som en överträdelse av Parts förpliktelse enligt detta Avtal.

*Modellklausul för skadeståndsansvar mellan parterna (en ska väljas)*

* 1. Om en Part, på grundval av bristande efterlevnad av detta Avtal, orsakat en annan Part skada, ska den skadevållande parten hålla skadelidande Part skadelös.
  2. Om en Part, på grundval av oaktsamhet eller vållande, orsakat en annan Part skada, ska den skadevållande parten hålla skadelidande Part skadelös.

## Tystnadsplikt

* 1. Den registrerade har enligt GDPR rätt att ta del av det väsentliga innehållet i detta Avtal. Parterna är eniga om att information i avsnitt 6, 14, och 16, samt Bilaga 4 till detta Avtal omfattas av Parternas ömsesidiga tystnadsplikt och inte får röjas för registrerad eller en tredje part utan samtliga Parters samtycke.
  2. I syfte att undvika missförstånd gäller Parts tystnadsplikt enligt detta avsnitt 15 inte i förhållande till tillsynsmyndighet, i den mån denna tystnadsplikt skulle medföra ett hinder för Part att samarbeta med tillsynsmyndighet enligt förpliktelse i Dataskyddslagstiftning.
  3. Parterna är eniga att om en Part är en svensk myndighet så omfattas denna Part av offentlighetsprincipen vilket påverkar utrymmet för tystnadsplikt enligt denna punkt till att gälla den sekretess som följer av offentlighets- och sekretesslagen (2009:400).

## Tvistelösning, tillämplig lag, m.m.

* 1. Detta Avtal ersätter alla tidigare överenskommelser, oavsett muntlig eller skriftlig form, mellan Parterna avseende föremålet för detta Avtal.
  2. Parterna är eniga om att lag (1980:1102) om handelsbolag och enkla bolag inte ska vara tillämplig på detta Avtal.
  3. Detta Avtal ska tolkas och tillämpas enligt svensk rätt.

I syfte att undvika missförstånd: denna lagvalsklausul tar inte sikte på tillämplig Dataskyddslagstiftning för behandling av personuppgifter.

* 1. Tvister som uppstår i anledning av detta avtal ska slutligt avgöras genom skiljedomsförfarande administrerat av Stockholms Handelskammares Skiljedomsinstitut (SCC). Regler för Förenklat Skiljeförfarande ska tillämpas om inte SCC med beaktande av målets svårighetsgrad, tvisteföremålets värde och övriga omständigheter bestämmer att Skiljedomsregler ska tillämpas. I sistnämnda fall ska SCC också bestämma om skiljenämnden ska bestå av en (1) eller tre (3) skiljedomare.
  2. Skiljeförfarandets säte ska vara Malmö, Sverige.
  3. Språket för skiljeförfarandet ska vara svenska.
  4. Detta Avtal har signerats elektroniskt av vardera Part.

## Parternas undertecknande

### **[Part A]**

Signatur:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Namnförtydligande:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort, datum, och år:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### **[Part B]**

Signatur:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Namnförtydligande:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ort, datum, och år:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Bilaga 1 – Parter till detta Avtal

Detta Avtal har ingåtts mellan följande Parter, nedan:

### **[Part A]**

|  |  |
| --- | --- |
| Firma: |  |
| Organisationsnummer: |  |
| Säte: |  |
| Postadress: |  |
| Huvudsakligt verksamhetsställe enligt artikel 4.16 GDPR: |  |
| Representant enligt artikel 27 GDPR, om tillämpligt: |  |
| Parts roll inom ramen för (i) Behandlingen, och den (ii) kliniska läkemedelsprövningen. |  |

### **[Part B]**

|  |  |
| --- | --- |
| Firma: |  |
| Organisationsnummer: |  |
| Säte: |  |
| Postadress: |  |
| Huvudsakligt verksamhetsställe enligt artikel 4.16 GDPR: |  |
| Representant enligt artikel 27 GDPR, om tillämpligt: |  |
| Parts roll inom ramen för (i) Behandlingen, och den (ii) kliniska läkemedelsprövningen. |  |

## Bilaga 2 – Dokumentation av Behandlingen

|  |  |
| --- | --- |
| 1. Det gemensamma ändamålet, eller ändamålen, med behandling av personuppgifter:  * *Anledningen till att personuppgifterna behandlas.* | Ändamålet med behandlingen av personuppgifter är […… t.ex. att *genomföra forskning i enlighet med till projektet hörande etiskt prövningsbeslut.]* |
| 1. Beskrivning av den behandling som sker för det gemensamma ändamålet:  * *Vad är det som faktiskt ska ske med personuppgifterna?* | Behandling av personuppgifter består [……*i/av att dessa insamlas i samband med…….]*  *Här bör framgå vad behandlingen består av. Normalt avser detta insamling av forskningsunderlag, bearbetning av forskningsunderlag, analys av forskningsunderlag.* |
| 1. Respektive Parts rättsliga grund för behandling av personuppgifter, samt för vilken eller vilka behandlingsåtgärder som den rättsliga grunden är tillämplig:  * *Den rättsliga grund enligt GDPR som respektive personuppgiftsansvarig anropar som stöd för att behandlingen får ske.* | Den rättsliga grunden för behandling av personuppgifter[*… .inom ramen för forskningsprojektet är att behandlingen är nödvändig för att utföra en uppgift av allmänt intresse i enlighet med artikel 6 § e) GDPR.]*  *Här ska framgå den rättsliga grunden* ***för respektive part****. I de flesta fall torde den rättsliga grunden vara att de utför en uppgift av allmänt intresse. Det allmänna intresset utgår dels från organisationens uppgift att bedriva forskning (i form av lagstiftning vad gäller lärosäten och regioner) och detta uppdrag bekräfta också genom etikprövningsmyndighetens beslut att tillåta* |
| 1. Typer av personuppgifter:  * *Vilka slags kategorier av personuppgifter som förekommer.* | *Här ska beskrivas de typer av personuppgifter som förekommer, som exempel kan nämnas*   * *Grundläggande kontaktuppgifter som namn, adress, telefonnummer och e-postadress samt företag/organisation och roll.* * *Personnummer.* * *Bilder av individer* * *Personuppgifter om anhörig* * *Uppgifter från hälso- och sjukvårdsjournal* |
| 1. Kategorier av känsliga personuppgifter:  * *Vilka slags kategorier av känsliga personuppgifter som förekommer. Det finns ett visst antal kategorier angivna i GDPR som betraktas som känsliga.* | *Här ska beskrivas vilka eventuella kategorier av känsliga personuppgifter (enligt artikel 9.1 GDPR) som kommer att hanteras inom ramen för forskningsprojektet.*  *Dessa kategorier finns:*   * *etniskt ursprung.* * *politiska åsikter.* * *religiös eller filosofisk övertygelse.* * *medlemskap i en fackförening.* * *hälsa* * *en persons sexualliv eller sexuella läggning.* * *genetiska uppgifter.* * *biometriska uppgifter som används för att entydigt identifiera en person* |
| 1. Integritetskänsliga personuppgifter, som inte är känsliga personuppgifter:  * *Eventuellt förekommande kategorier som inte är känsliga enligt GDPR men ändå är särskilt integritetskänsliga och därmed kan behöva skyddas.* | *Här ska framgå om det ingår personuppgifter som inte omfattas av kategorin känsliga personuppgifter enligt artikel 9.1 GDPR, men ändå betraktas som särskilt skyddsvärda.*  *Detta kan exempelvis vara:*   * *värderande personuppgifter, såom t.ex. betyg eller annan graderad bedömning* * *uppgifter om en persons ekonomiska förhållanden* * *uppgifter om åsikter, (utöver politiska)* * *personnummer* |
| 1. Typer av registrerade:  * *Vilka kategorier av registrerade (personer vars uppgifter behandlas) som förkommer* | *Här ska framgå vilka typer av registrerade som förekommer inom ramen för forskningsprojektet, det kan vara t.ex.*   * *Forskningspersoner* * *Anhöriga* |
| 1. Bevarande- och gallring av personuppgifter:  * *Beskrivning av de rutiner och riktlinjer som finns avseende hur länge personuppgifterna kommer att bevaras efter att projektet är avslutat.* | När forskningsprojektet är avslutat kommer personuppgifterna att hanteras enligt följande*:*  *[…..på vilket sätt de kommer att bevaras och i så fall hur länge eller när de kommer att gallras. Sådan gallring kan ske antingen genom att personuppgifterna raderas eller helt avidentifieras.]* |

## Bilaga 3 – Hantering av registrerades rättigheter

### Gemensam kontaktpunkt för registrerade

* 1. Parterna har valt att inte utse en gemensam kontaktpunkt.
  2. Parterna har valt att utse [Part #] till gemensam kontaktpunkt med följande adress och kontaktuppgifter.

### Registrerades rättigheter

* 1. Parterna är överens om att de är solidariskt ansvariga för de registrerades rättigheter. Oavsett detta har parterna valt att göra en uppdelning mellan om sig enligt nedan om vem av dem som har det huvudsakliga praktiska ansvaret att hantera frågeställningar kring de registrerades rättigheter.

|  |  |
| --- | --- |
| **Rättighet** | **Uppdelning av praktiskt ansvar mellan parter** |
| Tillse att information till registrerade ges i enlighet med artikel 12-14 GDPR.  Denna information ska tas fram på svenska. Om denna information behöver översättas till ett annat språk ska Parterna uppdra åt en auktoriserad översättare att genomföra denna översättning. Parterna ska gemensamt bära kostnaden för framtagandet av information och eventuell översättning av information.  Informationen ska tydligt redovisa   * 1. att Parterna är gemensamt personuppgiftsansvariga för Behandlingen,   2. Parternas respektive roller i förhållande till den registrerade,   3. om en Part är gemensam kontaktpunkt avseende registrerades rättigheter, och   4. att en registrerad har rätt att utöva sina rättigheter avseende på, och emot var och en, av Parterna. | *Här anges den uppdelning parterna väljer att tillämpa avseende vem som ska se till att informationen delges de registrerade senast i samband med att behandlingen påbörjas.* |
| Tillse att inhämtade samtycken hanteras på ett korrekt sätt och att registrerade givits tillräcklig information för att samtycken ska anses korrekt givna.  (med samtycken avses de samtycken som forskningspersoner ska lämna i enlighet med Etikprövningsmyndighetens godkännande) | *Här anges den uppdelning parterna väljer att tillämpa avseende vem av dem som ska se till att samtycke inhämtas och bevara dokumentationen kring dessa.* |
| Tillse att de registrerade kan utöva sina rättigheter enligt 15-18 GDPR   * Tillgång * Rättelse * Radering * Invändningar * Begränsningar | *Här anges den uppdelning parterna väljer att tillämpa avseende vem av dem som ska se till att rättigheterna tillvaratas.* |
| Tillse att de registrerade kan utöva sina rättigheter enligt artikel 20 GDPR   * Dataportabilitet | *Här anges den uppdelning parterna väljer att tillämpa avseende vem av dem som ska se till att rättigheterna tillvaratas. Notera att dataportabilitet endast är en tillämplig rättighet om den rättsliga grunden för behandlingen är de registrerades samtycke, vilket det normalt inte är inom ramen för forskning (se ovan under rättslig grund)* |

## Bilaga 4 – Tekniska och organisa­toriska säkerhetsåtgärder

Parterna noterar att nedan ställda krav är ett minimum för behandling av aktuella personuppgifter och att dessa krav därför också finns tillämpade och uppfylls av samtliga ingående personuppgiftsansvariga organisationer.

Respektive ingående organisation i det gemensamma personuppgiftsansvaret bekräftar genom ingående av detta avtal att de i sin hantering av för avtalet aktuella personuppgifter tillämpar samtliga av nedanstående tekniska och organisatoriska säkerhetsåtgärder och därmed uppfyller artikel 32 i GDPR.

### Ledningssystem för informationssäkerhet

* 1. Part ska genom ett ledningssystem säkerställa att:
     1. dokumenterade personuppgifter hos Part är åtkomliga och användbara för den som är behörig (*tillgänglighet*),
     2. personuppgifterna är oförvanskade (*riktighet*),
     3. obehöriga inte ska kunna ta del av personuppgifterna (*konfidentialitet*), och;
     4. åtgärder kan härledas till en användare (*spårbarhet*) i informationssystem som är helt eller delvis automatiserade.
  2. Part ska ansvara för att det finns en informationssäkerhetspolicy. Den ska ange Parts övergripande mål för och inriktning på verksamhetens arbete med informationssäkerhet i syfte att säkerställa personuppgifters tillgänglighet, riktighet, konfidentialitet och spårbarhet.
  3. Part ska utse en (1) eller flera personer som ska leda och samordna informationssäkerhetsarbetet.
  4. Part ska regelbundet bedöma om det finns risker för händelser som kan medföra att förpliktelserna i denna Bilaga 4 inte kan efterlevas (riskanalys). För varje sådan händelse ska Part (i) uppskatta sannolikheten för att händelsen inträffar, och (ii), bedöma vilka negativa konsekvenser som skulle bli följden av händelsen. Riskanalysen ska dokumenteras skriftligen.
  5. I syfte att undvika missförstånd: Parterna ska säkerställa att eventuella personuppgiftsbiträden omfattas av förpliktelser avseende tekniska och organisatoriska åtgärder vilka materiellt motsvarar denna Bilaga 4.

### Tillgänglighet

#### Säkerhetskopiering

* 1. Part ska säkerställa att personuppgifter som behandlas i informationssystem säkerhetskopieras med en fastställd periodicitet. Säkerhetskopiorna ska förvaras på ett säkert sätt, väl åtskilda från originaluppgifterna. Part ska besluta om hur länge säkerhetskopiorna ska sparas och hur ofta återläsningstester av kopiorna ska göras.

#### Kontinuitetsplanering

* 1. Part ska planera för hur Behandlingen ska genomföras om informationssystem som används för behandling av personuppgifter inte fungerar. Part ska vidare planera för hur återstart eller återställande ska göras efter en sådan funktionsstörning.

### Riktighet

* 1. Part ska säkerställa att personuppgifter som behandlas i informationssystem är riktiga i den bemärkelsen att de inte utsätts för förvanskning och också överensstämmer med dess eventuella källa.

### Konfidentialitet

#### Pseudonymisering

* 1. Personuppgifter som utlämnas till en Part, eller annan mottagare, ska utlämnas i pseudonymiserad form. Part får inte utlämna kodnycklar eller annan information som möjliggör identifiering av registrerade. Kodnycklar eller annan information som möjliggör identifiering av registrerade får inte överföras till tredjeland.
  2. I syfte att undvika missförstånd: pseudonymiserade personuppgifter som utlämnats till en Part, till ett personuppgiftsbiträde eller en annan mottagare, eller till en tredje part, är fortsatt personuppgifter även om det inte är möjligt för mottagaren eller den tredje parten att identifiera den registrerade personen vilka personuppgifterna avser. Pseudonymisering är en säkerhetsåtgärd.

#### Utvärdering av skyddet mot olovlig åtkomst

* 1. Part ska årligen utvärdera skyddet mot såväl intern som extern olovlig åtkomst till datornätverk och informationssystem som används för behandling av personuppgifter.

#### Behörighetstilldelning

* 1. Part ska ansvara för att varje användare tilldelas en individuell behörighet för åtkomst till personuppgifter. Part ska ta fram rutiner för ändring, borttagning och regelbunden uppföljning av behörigheterna för att säkerställa att dessa är riktiga och aktuella.

#### Autentisering

* 1. Part ska ansvara för att varje användare kan nyttja sin behörighet först efter att denne autentiserats på ett säkert sätt. Detta kräver som minimum att åtkomst endast kan ske med hjälp av stark autentisering om inte parterna överenskommits om annat.

#### Fysiskt skydd

* 1. Part ska säkerställa att informationssystem som används för behandling av personuppgifter skyddas fysiskt mot skada, störning och obehörig åtkomst.

#### Flyttbart medium för informationslagring

* 1. Den Part som tillåter flyttbart medium för lagring av personuppgifter ska säkerställa att obehöriga inte kan ta del av lagrade personuppgifter, och att personuppgifter inte går förlorade.
  2. Medium för informationslagring som innehåller personuppgifter ska avvecklas på ett sådant sätt att uppgifterna inte kan läsas eller återskapas.

### Spårbarhet

* 1. Part ska ansvara för att:
     1. det av dokumentationen av åtkomsten (loggar) framgår vilka åtgärder som har vidtagits med personuppgifter,
     2. det av loggarna framgår vid vilken verksamhetsenhet åtgärderna vidtagits
     3. det av loggarna framgår vid vilken tidpunkt åtgärderna vidtagits,
     4. användarens identitet framgår av loggarna,
     5. systematiska och återkommande stickprovskontroller, eller annan form av kontroll, av loggarna görs,
     6. kontroller av loggarna dokumenteras, och;
     7. loggarna sparas minst fem (5) år för att möjliggöra kontroll av åtkomsten till personuppgifter.

### Kontroll av efterlevnad

* 1. För att kontrollera efterlevnad av denna Bilaga 4 ska Part säkerställa att en egenkontroll, eller kontroll av en oberoende tredje part, genomförs minst en gång per år. Sådan kontroll ska dokumenteras. Om Part väljer att genomföra en egenkontroll ska denne Part säkerställa att den eller de personer som genomför egenkontrollen har sakkunskap inom informationssäkerhet och är oberoende i hur egenkontrollen ska genomföras.

### Utbildning

#### Awareness training om personuppgiftsincidenter

* 1. Part ska årligen säkerställa att personer under dennes ledning får ändamålsenlig utbildning i hur en personuppgiftsincident identifieras och rapporteras.

## Bilaga 5 – Personuppgiftsbiträden

### [Personuppgiftsbiträde A]

|  |  |
| --- | --- |
| Den Part vilken avser anlita personuppgiftsbiträdet: |  |
| Personuppgiftsbiträdets firma och säte: |  |
| Typer av personuppgifter och kategorier av registrerade: |  |
| Om personuppgifter ska överföras till tredjeland för behandling av personuppgifter: |  |