

Personuppgiftsbiträdesavtal

Dnr ICM 2019/186

Detta avtal reglerar förutsättningarna för behandling av personuppgifter vid EGA-SE, Inst. f. cell- och molekyllärobiologi, Uppsala universitet för Karolinska Institutets räkning.

1. Parter

Personuppgiftsansvarig: Karolinska Institutet, (nedan kallad **PuA**), organisationsnummer 202100-2973, 171 77 Stockholm,

Personuppgiftsbiträde: Uppsala universitet, NBIS, Institutionen för cell- och molekyllärobiologi, (nedan kallad **Biträdet**), organisationsnummer 202100-2932, Box 337, 751 05 Uppsala,

har denna dag ingått följande personuppgiftsbiträdesavtal ("**Biträdesavtal**").

2. Avtalets bakgrund och syfte

Detta Biträdesavtal ska säkerställa att de Personuppgifter som omfattas av Bitrådets 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.

Parterna har ingått en överenskommelse rörande långtidslagring av humangenetisk forskningsdata ("**Överenskommelsen**"). Detta Biträdesavtal har ingått för att reglera långtidslagring av humangenetisk forskningsdata.

Detta Biträdesavtal syftar till att uppfylla Dataskyddsförordningens krav, som föreskriver att det ska finnas ett skriftligt Biträdesavtal om Bitrådets behandling av Personuppgifter för den PuA:s räkning.

3. Definitioner

Detta Biträdesavtal har motsvarande definitioner som återfinns i artikel 4 i Dataskyddsförordningen, vilket bland annat innebär följande.

Med **Behandling** (eller **Behandla**) avses en åtgärd eller kombination av åtgärder beträffande Personuppgifter eller uppsättning av Personuppgifter, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Med **Dataskyddsförordningen** avses 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) (EUT 119, 4.5.2016, s 1).

Med **Personuppgifter** avses 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 lokaliseringssuppgift eller online identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Med **Personuppgiftsansvarig** avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensam eller tillsammans med andra bestämmer ändamålen och

medlen för Behandling av Personuppgifter; om ändamålen och medlen för Behandling bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den Personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

Med **Personuppgiftsbiträde** avses en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som Behandlar Personuppgifter för den Personuppgiftsansvariges räkning.

Med **Personuppgiftsincident** avses 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.

Med **Registrerad** avses den person som Personuppgiften avser.

4. Biträdesavtalets avtalshandlingar

Biträdesavtalet består av detta dokument, inklusive bilaga 1 och 2.

5. Behandlingen som omfattas av Biträdesavtalet

5.1 Preciserade instruktioner till Biträdet avseende dess Behandling av Personuppgifter inom ramen för detta Biträdesavtal framgår av **bilaga 1**. Parterna är överens om att PuA kan ändra eller utfärda ytterligare skriftliga instruktioner i den utsträckning det är nödvändigt för att Behandlingen ska vara laglig eller för att Biträdet ska kunna genomföra Behandlingen som följer av punkt 2 i detta Biträdesavtal, vilka det åligger Biträdet att följa. PuA ska säkerställa att vid var tid gällande instruktioner framgår av **bilaga 1**.

5.2 Bitrådets *informationssäkerhet i samband med behandlingen* omfattande dess Behandling av Personuppgifter enligt detta Biträdesavtal framgår av **bilaga 2**. Biträdet äger inte avstå från någon av *informationssäkerhetsåtgärderna* i **bilaga 2** utan att detta skriftligen godkänts av PuA. Parterna ska säkerställa att vid var tid tillämpade *informationssäkerhetsåtgärder* framgår av **bilaga 2**.

6. Behandling av Personuppgifter

6.1 Biträdet åtar sig att Behandla Personuppgifter i enlighet med Dataskyddsförordningen, detta Biträdesavtal samt i enlighet med vid var tid gällande skriftliga instruktioner från PuA hänförliga till detta Biträdesavtal.

6.2 PuA bestämmer ensam ändamålet med och medlen för den Behandling av Personuppgifter som Biträdet utför för PuAs räkning.

6.3. Biträdet får inte Behandla Personuppgifter för något annat ändamål eller på något annat sätt än vad som vid varje Behandlingstillfälle är absolut nödvändigt för att uppfylla sina åtaganden enligt detta Biträdesavtal eller annan åtgärd som PuA särskilt skriftligen medger.

7. Personuppgiftsbitrådets grundläggande skyldigheter

7.1 Biträdet garanterar att denne besitter nödvändig kapacitet och förmåga att fullgöra sina skyldigheter enligt detta Biträdesavtal och gällande dataskyddslagstiftning, samt att denne löpande vidtar sådana lämpliga tekniska och organisatoriska åtgärder som krävs för att säkerställa att den Registrerades rättigheter skyddas.

7.2 För det fall att Biträdet saknar instruktioner som Biträdet bedömer är nödvändiga för att genomföra uppdraget ska Biträdet utan dröjsmål, informera PuA om sin inställning och invänta instruktioner från PuA.

7.3 Biträdet ska utan dröjsmål informera PuA om eventuella kontakter från tillsynsmyndighet som rör eller kan vara av betydelse för Behandling av Personuppgifterna. Biträdet har inte rätt att företräda PuA eller agera för PuA:s räkning gentemot tillsynsmyndighet eller annan tredje man.

7.4 För det fall att Registrerad, tillsynsmyndighet eller annan tredje man begär information från Biträdet som rör Behandlade Personuppgifter ska Biträdet hänvisa till PuA. PuA och Biträdet ska därefter komma överens om lämpligt tillvägagångsätt för utgivande av efterfrågad information.

7.5 Biträdet ska vid behov bistå den PuA att tillmötesgå en begäran om rättelse, blockering eller utplåning av Personuppgifter som framställts av den Registrerade.

7.6 Biträdet ska underrätta PuA utan onödigt dröjsmål efter att ha fått vetskap om en Personuppgiftsincident.

7.7 PuA har rätt att själv eller genom tredje man kontrollera att Biträdet följer vad som anges i detta Biträdesavtal och av de instruktioner som utfärdats av PuA. Biträdet ska därvid kostnadsfritt och inom ramen för vad som är lagligen möjligt för Biträdet ge tillgång till all information som krävs för att visa att Biträdet uppfyller sina skyldigheter samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den PuA eller den PuA bemyndigat för detta ändamål.

7.8 Uppgifter i tjänstens logg får endast användas av Biträdet för vad som krävs för upprätthållande eller förbättring av tjänstens funktionalitet och kvalitet.

8. Konfidentialitet och tystnadsplikt

8.1 Personuppgifterna omfattas av konfidentialitet och om annat inte följer av tvingande lag får Biträdet, dennes anställda eller underbiträden inte lämna ut några Personuppgifter till tredje man utan att först ha inhämtat PuA:s samtycke.

8.2 Biträdet ansvarar för att berörd personal informeras om och iakttar gällande konfidentialitet. Om PuA så önskar ska särskild sekretessförbindelse undertecknas av berörd personal.

9. Underbiträde

9.1 Biträdet får inte anlita ett annat underbiträde utan att ett särskilt skriftligt medgivande i förväg har erhållits av PuA. Detta får dock endast ske genom ingående av ett skriftligt avtal med underbiträdet. Enligt detta underbiträdesavtal ska underbiträdet åläggas motsvarande skyldigheter som enligt detta biträdesavtal åligger Biträdet och framförallt ska underbiträdet ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder så att Behandlingen uppfyller kraven i Dataskyddsförordningen.

9.2 Om underbiträdet inte uppfyller sina skyldigheter i fråga om Behandling av Personuppgifter är Biträdet fullt ansvarig gentemot PuA.

9.3 För att PuA ska kunna uppfylla sina lagstadgade skyldigheter som Personuppgiftsansvarig, ska samtliga underbiträden vara kända av och redovisade för PuA. PuA måste även ha kännedom om i vilket land Behandlingen äger rum.

10. Säkerhetsåtgärder

10.1 Biträdet ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att Behandlingen utförs i enlighet med Dataskyddsförordningen samt säkerställa att den Registrerades rättigheter skyddas mot bland annat obehörig åtkomst, förstörelse och ändring. Biträdet ska även iaktta av tillsynsmyndighet utfärdade tillämpliga föreskrifter och allmänna råd.

10.2 I enlighet med Dataskyddsförordningen artikel 32 ansvarar Parterna var för sig och i samråd med beaktande av senaste utvecklingen, genomförandekostnader och Behandlingens art, omfattning, sammanhang och ändamål samt risker, för att vidta lämpliga tekniska och organisatoriska åtgärder utformade för ett inbyggt dataskydd och dataskydd som standard i enlighet med gällande dataskyddslagstiftning.

11. Underrättelse i händelse av Personuppgiftsincident

Biträdet ska efter att ha fått vetskap om en personuppgiftsincident lämna underrättelse till PuA i enlighet med punkt 7.6.

En sådan underrättelse ska åtminstone innehålla följande information.

- a. En beskrivning av Personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs, samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,
- b. Förmedla namnet och kontaktuppgifterna för Bitrådets dataskyddsombud eller andra kontaktpersoner där mer information kan erhållas,
- c. En beskrivning av de sannolika konsekvenserna av Personuppgiftsincidenten och
- d. En beskrivning av de åtgärder som Biträdet har vidtagit eller föreslagit för att åtgärda Personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

Om och i den utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

På begäran av PuA ska Biträdet, med beaktande av typen av behandling och den information som Biträdet har tillgång till, bistå PuA med att informera de Registrerade om Personuppgiftsincidenten.

12. Konsekvensbedömning och förhandssamråd

12.1 Om en typ av Behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål sannolikt leder till en högre risk för fysiska personers rättigheter och friheter ska Biträdet före det att Behandlingen utförs, på egen bekostnad, vid behov och på begäran av PuA, bistå PuA vid en bedömning av den planerade Behandlingens konsekvenser för skyddet av Personuppgifter. En enda bedömning kan omfatta en serie liknande Behandlingar som medför liknande höga risker.

12.2 För det fall bedömningen av den planerade Behandlingen visar att Behandlingen skulle leda till hög risk om PuA inte vidtar åtgärder för att minska risken ska Biträdet före Behandlingen utförs vara PuA behjälplig vid samråd med tillsynsmyndigheten.

13. Överföring av personuppgifter till tredje land

13.1 Biträdet äger inte rätt att överföra Personuppgifter till tredjeland eller en internationell organisation utan att PuA först har lämnat sitt skriftliga samtycke i förväg till en sådan överföring.

13.2 En överföring till tredjeland förutsätter under alla förhållanden, dvs. även för det fall PuA lämnat sitt skriftliga samtycke, att Biträdet uppfyller de krav och åtgärder som följer av Dataskyddsförordningen vad avser tredjelandsöverföring.

14. Skada och ansvar

14.1 I fall där Registrerade riktar anspråk avseende ersättning mot någon av Parterna med anledning av materiell eller immateriell skada som den Registrerade lidit ska artikel 82 i Dataskyddsförordningen äga tillämpning, varvid vad som anges i femte punkten, artikel 82, tillämpas i fråga om återkrävande av ersättning motsvarande den andra Partens del av ansvaret för skadan. Biträdet är därvid gentemot PuA ansvarig för skada orsakad av underbiträde.

14.2 För annan skada än sådan angiven i punkt 14.1 svarar Parterna med eventuella begränsningar när så framgår av tjänsteavtal (se punkt 2 ovan). 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 14.2 utan ska bäras av den Part som påförts sådan avgift.

14.3 Parterna ska informera varandra om de får kännedom om omständighet som kan leda till skadestånd eller betalningsansvar för den andre Parten och arbeta tillsammans för att förhindra och minimera sådant skadestånd eller betalningsansvar.

14.4 Innan Part inleder förhandling, ingår förlikning eller träffar avtal eller förbinder sig till någon annan förpliktelse gentemot de Registrerade eller annan tredje man eller med domstol eller annan myndighet med anledning av ersättningskrav, anspråk eller påföljd enligt punkterna 14.1 – 14.2, ska Parten bereda den andra Parten möjlighet att lämna biträde i saken eller på annat lämpligt sätt tillvarata sina rättigheter.

15. Kontaktpersoner

15.1 Vid underrättelse om personuppgiftsincident, information om kontakt med tillsynsmyndighet eller Registrerad eller annan kommunikation av avgörande betydelse för Behandlingen ska Biträdet i första hand vända sig till dataskyddsombudet vid PuA:

dataskyddsombud@ki.se

15.2 Kontaktperson vid Biträdet för Behandlingen är:

Föreståndaren vid NBIS.

16. Ändring och tillägg

16.1 Ändringar och tillägg till detta Biträdesavtal ska göras skriftligen och undertecknas av behöriga företrädare för båda Parter för att vara giltiga. PuA äger dock ändra i den vid var tid gällande instruktionen som framgår av **bilaga 1** i enlighet med vad som anges i punkt 5.1 i detta Biträdesavtal.

16.2 Om tjänstens innehåll ändras, till exempel genom att nya funktioner tillkommer eller genom att nya sätt att behandla Personuppgifter uppstår, ska PuA omgående skriftligen underrättas om förändringarna.

17. Avslut

17.1 Vid Biträdesavtalets upphörande ska Personuppgifterna antingen återföras till PuA eller raderas. Om annat inte meddelas av PuA ska Personuppgifterna återföras till PuA och därefter raderas hos Biträdet inom 30 dagar om inte annat framgår av instruktionen i bilaga 1. På begäran ska Biträdet lämna ett skriftligt besked om vilka åtgärder som vidtagits med Personuppgifterna i samband med att Behandlingen slutförts.

17.2 För det fall att Biträdet på grund av lag, förordning, myndighetsföreskrifter eller beslut är skyldigt att behålla Personuppgifter även efter det att detta Biträdesavtal har upphört att gälla får dessa Personuppgifter endast användas för det ändamål som framgår av den lag, förordning, myndighets föreskrifter eller beslut som föranleder att Personuppgifterna behålls. PuA ska informeras om detta och grunderna härför.

18. Överlåtelse av avtal

Biträdet äger inte rätt att helt eller delvis överlåta sina åtaganden enligt detta Biträdesavtal till annan utan skriftligt medgivande från PuA.

19. Avtalstid

Detta Biträdesavtal gäller från det att båda Parter signerat avtalet och så länge som Biträdet Behandlar Personuppgifter för PuA:s räkning.

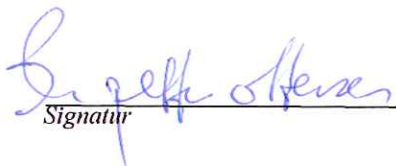
20. Tillämplig lag och tvist

20.1 Parternas rättigheter och skyldigheter enligt detta Biträdesavtal omfattas i sin helhet av svensk rätt.

20.2 Tvist angående tolkning eller tillämpning av detta Biträdesavtal ska avgöras enligt svensk lag och föras vid allmän svensk domstol. För det fall PuA är en svensk myndighet ska tvist istället slutligt avgöras av närmast överordnad myndighet eller eljest av den tillämpliga tvistelösningsmekanism inom svenska staten som står till buds.

Detta Biträdesavtal har upprättats i två (2) likalydande exemplar av vilka Parterna tagit var sitt.

Karolinska Institutet


Signatur

OLE P. OTTERSEF
Namnförtydligande, befattning

Stockholm 17/12-19
Ort och datum

Uppsala universitet


Signatur

Bengt Persson, Föreståndare NBIS
Namnförtydligande, befattning

Uppsala 19/12-19
Ort och datum

Bilaga 1 – PuA:s instruktioner

Parterna har nedan konkretiserat vad som ingår i Behandlingen enligt Biträdesavtalet.

- I. Ändamålet med Behandlingen**

Ändamålet med Behandlingen av Personuppgifter är att långtidslagra genetisk och fenotypisk data från forskningsstudier. Tillika att på den PuA:s anvisningar, via en formaliserad process, tillgängliggöra sådan data för andra forskare som är berättigade att ta del av densamma.
- II. Kategorier av Registrerade**

Individer som deltagit i forskningsstudier som genererar genetisk information.
- III. Vilken typ av Personuppgifter Behandlas**

De Personuppgifter som överförs är av följande slag: pseudonymiserade genetiska, och fenotypiska uppgifter eller annan metadata som är av relevans för forskningsfrågeställningen vid insamlandet.
- IV. Känsliga/ integritetskänsliga Personuppgifter (i förekommande fall)**

De känsliga personuppgifter som överföringen rör är genetiska, och eventuellt fenotypiska uppgifter eller annan metadata som kan vara uppgifter om hälsa.
- V. Behandling**

De känsliga personuppgifterna kommer att behandlas på följande sätt:

Efter att den PuA tillhandahållit personuppgifterna i krypterad form, omkrypteras de maskinellt med en system-specifik kryptonyckel och flyttas till en skyddad disk-area för lagring. I det fall personuppgifterna ska lämnas ut till andra behöriga, på PuA instruktion, krypteras personuppgifterna om maskinellt med en nyckel som är specifik för mottagaren, och tillgängliggörs för denne.
- VI. Särskilda instruktioner rörande Behandlingen:**

Intet.
- VII. Behandling av underbiträden i tredje land (i förekommande fall)**

PuB ska inte använda sig av underbiträden i land utanför EU/EES, eventuellt med undantag för EMBL (internationell organisation).
- VIII. Avslutsrutiner**

Se punkt 17 i Biträdesavtalet.

IX. Godkända underbiträden

Namn	Typ av Behandling	Plats för Behandling
SUNET (Notera att SUNET kan använda sig av underbiträden för att tillhandahålla tjänsten)	Tillhandahålla infrastruktur för datalagring	Sverige
Central EGA vid 1. EMBL-EBI https://www.ebi.ac.uk/about 2. The Centre for Genomic Regulation (CRG) https://www.crg.eu/content/about-us/general-information	Långtidslagring av krypterade personuppgifter och relaterad metadata. För att möjliggöra replikering av dataset deponerade i EGA-SE och tillhörande relevant metadata, enligt samma principer som beskrivs för EGA-SE i Bilaga 2	1. EMBL, internationell organisation 2. Spanien
EGA-FI IT Center for Science https://www.csc.fi/about-us	Långtidslagring av krypterade personuppgifter. För att möjliggöra replikering av dataset deponerade i EGA-SE, enligt samma principer som beskrivs för EGA-SE i Bilaga 2	Finland
EGA-NO Oslo universitet https://www.usit.uio.no/english/about/organisation/	Långtidslagring av krypterade personuppgifter. För att möjliggöra replikering av dataset deponerade i EGA-SE, enligt samma principer som beskrivs för EGA-SE i Bilaga 2	Norge

Bilaga 2 – Informationssäkerhet i samband med behandlingen

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

Biträdet garanterar att

- Informationssäkerhetsarbete sker inom ramen för Bitrådets ledningssystem, uppbyggt i enlighet med ISO/IEC 27001, inom detta område.
- Utveckling av Bitrådets informationssystem/IT-tjänster genomförs med hänsyn till informationssäkerhet, det vill säga krav på konfidentialitet, riktighet och tillgänglighet.
- Grundläggande för Bitrådets hantering av informationssäkerhet är: åtkomstbegränsning, riktighet, spårbarhet och tillgänglighet.
- Skalskydd till Bitrådet 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 Bitrådets IT-miljö.
- Bitrådet har administrativa rutiner och tekniska åtgärder för att information från olika kunder särskiljs.
- Bitrådet arbetar efter implementerade ledningssystem för informationssäkerhet, som reglerar uppföljning av IT-säkerhetsincidenter.
- Bitrådet kommer att anmäla eventuella personuppgiftsincidenter som berör PuA:s data i uppdraget enligt erhållen kontaktinformation.

EGA-SE är del av ett federerat repositorium för human genomik-data, där icke-känslig metadata finns vid centrala instanser. Användarkonton och behörigheter administreras vid de centrala instanserna. EGA-SE syftar till att långtidslagra känslig genetisk och fenotypisk forskningsdata, och möjliggöra delning av sådan data till andra behöriga forskare, på ett sätt som minimerar risken för oönskad åtkomst till känsliga personuppgifter och med bibehållen dataintegritet.

PuA kommer att tillhandahålla pseudonymiserade personuppgifter i krypterad form (inklusive checksummor för det ingående filerna), varpå dessa kommer att krypteras om maskinellt (utan manuell intervention) med en system-specifik kryptonyckel i RAM-minnet, och flyttas till en skyddad diskarea ("valvet"), efter validering av dataintegriteten.

Den enda del i systemet som är tillgängligt från internet är uppladdningsservern (sftp) som enbart har funktionalitet för att ladda upp filer. Autentisering och behörighetsinformation för att kunna ladda upp data hålls i de centrala instansernas system, mot vilka behörighetskontroll sker med ett krypterat och certifikat-identifierat protokoll.

I det fall personuppgifterna ska lämnas ut till andra behöriga tillämpas en formaliserad process där den sökande ansöker om tillgång till dataset hos en av PuA definierad "datatillgänglighetskommitté" (*Data Access Committee - DAC*), som avgör om den sökandes forskningsändamål överensstämmer med de förbehåll för datadelning som finns för datasetet. Den sökande förbinder sig också att ingå ett på förhand definierat "datatillgänglighetsavtal" (*Data Access Agreement - DAA*) med PuA. Behörighet till dataset administreras i den centrala instansen som ovan. En behörig användare får efter autentisering tillgång till de dataset som

denne har rätt att ta del av, och som är omkrypterade med en krypteringsnyckel specifik för den användaren, via nedladdningslänkar eller monterat i ett säkert filsystem.

Endast ett fåtal systemadministratörer med särskild behörighet har tillgång till systemet. All operationell hantering av personuppgifterna sker automatiserat och programmatiskt. Behöriga systemadministratörer har teknisk möjlighet att ta del av de känsliga personuppgifterna, men enligt de definierade rutinerna så är detta endast tillåtet om så erfordras för att felsöka systemet.