Instruktioner till Avtal för gemensamt personuppgiftsansvar

Mall ”Avtal för gemensamt personuppgiftsansvar” är framtagen för Parter i ett forsknings-projekt. Den svenska språkversionen tar uteslutande sikte på när samtliga Parter har sitt huvudsakliga verksamhetsställe i Sverige. Om en eller flera parter har sitt huvudsakliga verksamhetsställe utanför Sverige ska en engelskspråkig version tillämpas.

Det är endast parter som omfattas av GDPR som kan vara Part till detta avtal (för annars är denne inte personuppgiftsansvarig för den gemensamma behandlingen).

Parter: Det finns inget hinder mot att det är fler än två parter. På första sida anges endast parts firma; till exempel ”Region Skåne”. Utförlig information, som organisationsnummer med mera ska preciseras i Bilaga 1.

Bilaga 1:

En Parts huvudsakligt verksamhetsställe (enligt artikel 4.16 GDPR), är Organisationens verksamhetsställe och påverkar behörig tillsynsmyndighet.

En Parts representant enligt artikel 27 GDPR är en företrädare för personuppgiftsansvarig Part som inte är etablerade i unionen (artikel 20 GDPR). Ange ”ej tillämpligt” om detta inte är aktuellt.

Bilaga 2:

Det gemensamma ändamålet, eller ändamålen, med behandling av personuppgifter:
Här ska framgå det ändamål som föreligger för den gemensamma behandlingen av personuppgifterna. I de flesta fall torde detta vara klinisk forskning för att uppnå studieresultatet i det specifika forskningsprojektet.

Beskrivning av den behandling som sker för det gemensamma ändamålet:
Här ska framgå en beskrivning av den behandling som sker, alltså en i fritext beskriven process för vilka åtgärder det är som vidtas med personuppgifterna. Detta behöver inte vara på alltför detaljerad nivå men ändå tillräckligt för att det ska förstås vilka åtgärder som vidtas. Det kan handla om insamling av uppgifter, analys av uppgifter utifrån ett visst protokoll med mera

Respektive Parts rättslig grund för behandling av personuppgifter, samt för vilken eller vilka behandlingsåtgärder som den rättsliga grunden är tillämplig:
Här ska framgå den rättliga grund som behandlingar baseras på. För lärosäten och universitet, som är myndigheter, är det nästan utan undantag den rättsliga grunden allmänt intresse som är aktuell vid personuppgiftsbehandling i samband med forskning. Eftersom lärosäten och universitet har ett författningsreglerat uppdrag att bedriva forskning är personuppgifts-behandlingen nödvändig för att utföra en uppgift av allmänt intresse, vilket alltså utgör den rättsliga grund behandlingen stödjer sig på. I undantagsfall kan det även utgöras av andra

rättsliga grunder. De rättsliga grunderna som finns tillgängliga följer av artikel 6.1 GDPR. Om behandlingen består av flera olika åtgärder bör det även framgå vilka detta är.

Typer av personuppgifter:
Vika typer av personuppgifter som behandlingar består av, till exempel personnummer, adress och kontaktuppgifter, journalinformation, och liknande

Kategorier av känsliga personuppgifter:
En särskild kategori av personuppgifter, så kallade känsliga personuppgifter, är sådana personuppgifter som avslöjar:

- etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i fackförening
- uppgifter om hälsa, sexualliv eller sexuell läggning
- genetiska uppgifter
- biometriska uppgifter som entydigt identifierar en person.
- Känsliga personuppgifter omfattas av särskilda bestämmelser i GDPR.

Integritetskänsliga personuppgifter, som inte är känsliga personuppgifter:
Även personuppgifter som inte omfattas av de i GDPR definierade känsliga personuppgifterna kan anses vara särskilt integritetskänsliga, och därmed skyddsvärda. Det är till exempel personuppgifter som innehåller värderande bedömningar om en person (betyg och liknande), information om en persons ekonomiska situation,

Typer av registrerade:
Här ska framgå vilka grupper av registrerade som återfinns i behandlingarna. Detta torde i de flesta fall utgöras av ”forskningspersoner” men även andra grupper kan möjligen förekomma.

Bevarande- och gallring av personuppgifter:
Här ska framgå hur bevarande och gallring av personuppgifterna är tänkt att hanteras. Eftersom det är två eller flera personuppgiftsansvariga inblandade i behandlingen är det viktigt att det framgår vilken av parterna, eller om det är flera, som kommer att bevara personuppgifterna och i så fall under hur lång tid.

Bilaga 3:

Gemensam kontaktpunkt:
Här kan endast ett alternativ väljas. I vissa fall utses en gemensam kontaktpunkt för registrerade (alltså dit registrerade kan vända sig för att få information kring behandlingen av personuppgifter eller begära någon av sina rättigheter).

Information till registrerade:
Här definieras vilken information till de registrerade som ska tas fram och vad denna information (i enlighet med GDPR) ska innehålla som ett minimum). I flertalet fall torde det i praktiken vara en part som är mest aktiv i att ta fram informationen, men eftersom det handlar om ett gemensamt personuppgiftsansvar så är det viktigt att understryka att samtliga

som ingår i det ansvaret och ansvarar för att informationen är korrekt och uppfyller de krav som GDPR ställer. Därav punkten.

Bilaga 4:

I bilaga 4 redogörs för de tekniska och organisatoriska åtgärder som båda parter garanterar att de minst uppfyller vad gäller skyddet för behandlingen av personuppgifter.

I vissa fall kan det tänkas att ytterligare åtgärder bedöms krävas och/eller tillämpas av båda parter och det finns i sådant fall möjlighet att lägga till sådana åtgärder sist i bilagan.

Notera att samtliga organisationer som ingår i det gemensamma personuppgiftsansvaret genom ingåendet av avtalet garanterar att de uppfyller de åtgärder som beskrivs i bilaga 4. I det följande förklaras de olika åtgärderna:

Ledningssystem för informationssäkerhet
Respektive part ska ha ett ledningssystem för informationssäkerhet som tillämpas i verksamheten. Notera att myndigheter har skyldighet i lag att tillämpa detta genom myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter, MSBFS 2020:6 4 §. Aktörer inom hälso- och sjukvårdssektorn har även dessa har krav på sig genom HSLF-FS 2016:40 Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården 3 kap 2 och 4 §§.

Tillgänglighet – Säkerhetskopiering
Respektive part garanterar att de personuppgifter som omfattas av den aktuella personuppgiftsbehandlingen för vilket parterna är gemensamt ansvariga för omfattas av partens rutiner för säkerhetskopiering.

För det fall endast ena parten ska ansvara för att detta genomförs bör detta förtydligas i avtalet.

Tillgänglighet – Kontinuitetsplanering
Respektive part garanterar att de personuppgifter som omfattas av den aktuella personuppgiftsbehandlingen för vilket parterna är gemensamt ansvariga för omfattas av partens rutiner för kontinuitetsplanering. Detta innebär att det finns en etablerad plan för vilka åtgärder som ska vidtas vid tillfällig brist på åtkomst samt vilka tidsatta åtgärder som kommer att vidtas för att återupprätta åtkomst.

För det fall endast ena parten ska ansvara för att detta genomförs bör detta förtydligas i avtalet.

Riktighet
Respektive part garanterar att de personuppgifter som omfattas av den aktuella personuppgiftsbehandlingen för vilket parterna är gemensamt ansvariga för omfattas av partens rutiner för kontroll av riktighet. Detta innebär att det måste finnas en kontroll vid mottagande av extern information så att denna garanterat inte förvanskas under överföringen. Vidare ska det ingå behörighetsstyrning, loggning och liknande tillämpningar i informationssystemen så att det är möjligt att kontrollera på vilket sätt informationen påverkats över tid.

För det fall endast ena parten ska ansvara för att detta genomförs bör detta förtydligas i avtalet.

Konfidentialitet – Pseudonymisering
Punkt 4.1: Här garanteras att uppgifter som lämnas mellan de gemensamt ansvariga parterna, såväl som uppgifter som lämnas till annan extern part, endast utlämnas i pseudonymiserad form. Pseudonymiserad form innebär att inga identitetsuppgifter förekommer utan endast koder som genom en annan kodlista kan hänföras till den registrerade, det vill säga den individ vars personuppgifter behandlas.

Vidare framgår att kodlistan inte får lämnas ut, utan alltid ska kvarstå hos den part som är ansvarig för pseudonymiseringen av uppgifterna.

Punkt 4.2: Här understryks att även pseudonymiserade uppgifter fortfarande är att betrakta som personuppgifter och således ska hanteras i enlighet med GDPR. Det förekommer ibland missförstånd om att pseudonymiserade uppgifter förlorar sin egenskap av personuppgifter, så är inte fallet. Uppgifter som däremot är helt avidentifierade och inte längre, på något sätt, kan hänföras till den ursprunglige individen är inte längre personuppgifter och omfattas då inte heller av GDPR eller personuppgiftsansvaret.

Konfidentialitet - Utvärdering av skydd
Detta krav är något som normalt följer av informationssäkerhetsstandarder och som är direkt reglerat i de myndighetskrav som hänvisats till ovan.

Konfidentialitet – Behörighetstilldelning
Respektive part garanterar att de personuppgifter som omfattas av den aktuella personuppgiftsbehandlingen för vilket parterna är gemensamt ansvariga för endast är åtkomliga i enlighet med behörighetstilldelning. Det innebär att alla informationssystem är behörighetsstyrda, det vill säga att det maskinellt finns möjlighet att styra vilka personer som har möjlighet att ta del av information och på olika sätt manipulera information.

Vidare anges att parterna garanterar att de har rutiner för att tilldelade behörigheter följs upp så att de alltid är aktuella. I detta innefattas även att en bedömning sker att endast personal som har behov av informationen för att kunna utföra sitt arbete tilldelas en behörighet till detsamma och att denna behörighet endast tillämpas under den tid som personal faktiskt arbetar med denna arbetsuppgift.

Konfidentialitet – Autentisering
Autentisering innebär kontroll av uppgiven identitet, till exempel vid inloggning. Det vill säga kontrollera att en behörig användare faktiskt är den användare som den utger sig för att vara. I dessa fall krävs dessutom stark autentisering. Stark autentisering vilket avser en nivå av säkerhet som är starkare än endast användarnamn och lösenord. Stark autentisering innebär att minst två faktorer måste tillföras för att en individ ska anses säkert identifierad. I praktiken kan denna säkerhetsnivå exempelvis utgöras av att användaren, förutom sitt lösenord även får ett SMS till ett på förhand känt telefonnummer med en engångskod som skrivs in vid inloggningen.

För det fall uppgifterna anses vara mindre skyddsvärda kan parterna komma överens om att normal autentisering är tillräckligt (typiskt sätt individuellt användarnamn och unikt lösenord).

Konfidentialitet - Fysiskt skydd

Respektive part garanterar att de personuppgifter som omfattas av den aktuella personuppgiftsbehandlingen för vilket parterna är gemensamt ansvariga för skyddas rent fysiskt. Det innebär att alla informationssystem omfattas av fysiskt skalskydd där till exempel servrar och annan kritisk infrastruktur förvaras i låsta utrymmen.

Konfidentialitet - Flyttbart medium

Här ställs krav om att i de fall flyttbart fysiskt medium (till exempel USB-disk, extern hårddisk och liknande) används för lagring av personuppgifter som ingår i det gemensamma ansvaret endast får ske på medium med någon slags insynsskydd (normalt kryptering) samt att det även måste finns något sätt att återskapa informationen om det fysiska mediet går förlorat (till exempel rutiner om säkerhetskopiering vid export till fysiskt medium).

Vidare ställs krav att hårddiskar, USB-diskar och liknande när de inte längre är i bruk måste raderas på ett säkert sätt, normalt genom någon form av destruktion eller mycket säker permanent radering.

Spårbarhet

Respektive part garanterar att åtkomst och annan behandling av de personuppgifter som omfattas av den aktuella personuppgiftsbehandlingen för vilket parterna är gemensamt ansvariga för är spårbara. Det innebär att all åtkomst som sker genom tilldelade behörigheter ska loggas. Loggen ska kunna utvisa vem, när, hur och vad. Det vill säga vem som har haft åtkomst, när så skedde och vad denne vidtog för åtgärder med uppgifterna.

I spårbarhetskravet ingår också att de ska ske regelbundna uppföljningar av loggar genom stickprov eller annan form (det kan tänkas att det till exempel finns mjukvara som kontinuerligt gör kontroller och väljer ut ett antal loggar som följs upp av kontrollant) och att dessa kontroller dokumenteras.

Ett sista viktigt krav är att loggarna sparas under viss tid samt att de är tillförlitliga, det vill säga att de inte går att manipulera i efterhand.

Kontroll av efterlevnad

Parterna garanterar att de uppfyller krav på uppföljning av sina egna åtgärder. Sådan regelbunden uppföljning ingår i standarder inom informationssäkerhet