VÄSTRA GÖTALANDSREGIONEN
KONCERNKONTORET

Juridisk information
Datum 2022-08-17
Diarienummer RS 2022-03927

Västra Götalandsregionen
Koncernkontoret, juridiska enheten
Handläggare: Amanda Carlström
Telefon: 073 - 649 65 56
E-post: amanda.carlstrom@vgregion.se

Forskning på känsliga personuppgifter enligt GDPR

Innehåll

1. Inledning

I Västra Götalandsregionen (VGR) genomförs forskning på hälsodata med regionen som forskningshuvudman, samt i samverkan med andra forskningshuvudmän. Forskningen innebär nästan alltid någon form av personuppgiftsbehandling vilket gör att det är viktigt att ha koll på dataskyddsförordningen (GDPR) som reglerar detta.

Detta dokument är framtaget i syfte att ge en övergripande bild av vad du behöver tänka på utifrån ett GDPR-perspektiv när du ska forska på personuppgifter som rör hälsa. Dokumentet är därför forskningsspecifikt, men läs gärna också annan generell information om GDPR på insidan som även är tillämplig på personuppgiftsbehandling i forskning. Detta hittar du här.

2. Förklaring av centrala begrepp

2.1. Vad är forskning?

Enligt etikprövningslagen definieras forskning som vetenskapligt experimentellt eller teoretiskt arbete eller vetenskapliga studier genom observation, om arbetet eller studierna görs för att hämta in ny kunskap, och utvecklingsarbete på vetenskaplig grund, dock inte sådant arbete eller sådana studier som utförs endast inom ramen för högskoleutbildning på grundnivå eller på avancerad nivå.[1]

2.2. Vad är en personuppgift?

Personuppgifter är all slags information som direkt eller indirekt kan knytas till en person som är i livet.[2] Exempel på personuppgifter är namn, personnummer eller uppgifter om en persons hälsa.

2.3. Vad är en känslig personuppgift?

Vissa personuppgifter är till sin natur särskilt känsliga och har därför ett starkare skydd. De kallas för känsliga personuppgifter.

Känsliga personuppgifter är uppgifter om

- etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i fackförening
- genetiska uppgifter
- biometriska uppgifter som används för att entydigt identifiera en person
- hälsa
- en persons sexualliv eller sexuella läggning.[3]

Den kategori av känsliga personuppgifter som ofta är relevant för forskning inom VGR är uppgifter om hälsa. Exempel på uppgifter om hälsa är uppgifter som

[1] 2 §, Etikprövningslagen (2003:460).
[2] Art. 4, GDPR.
[3] Art. 9, GDPR.

kommer från tester eller undersökningar, uppgifter om sjukdom, sjukdomsrisk, eller sjukdomshistoria.

Enligt GDPR är behandling av känsliga personuppgifter som utgångspunkt förbjuden, men det finns undantag som gör det möjligt att behandla dessa personuppgifter om det sker för vetenskapliga forskningsändamål eller statistiska ändamål.[4] Förutsättningarna för undantaget utvecklas närmare senare i detta dokument.

2.4. Vad gäller för personnummer?

Personnummer räknas inte som en känslig personuppgift i GDPR:s mening, men anses ändå vara extra skyddsvärda. Samma gäller för de samordningsnummer som man kan få om man inte är folkbokförd i Sverige. Att personnummer anses vara extra skyddsvärda innebär bl.a. att behandlingen av dem bör vara restriktiv och att de ska exponeras så lite som möjligt.[5]

2.5. Vad är pseudonymiserade uppgifter?

Även så kallade pseudonymiserade uppgifter är personuppgifter och omfattas därför av GDPR. Pseudonymisering innebär att det inte längre är möjligt att tillskriva uppgifter till en specifik registrerad utan att kompletterande uppgifter används.[6] Ett exempel på en pseudonymiseringsteknik är att ta bort direkta identifierare som t.ex. namn och personnummer och ersätta med en indirekt identifierare som ett löpnummer. Denna teknik används frekvent inom forskning. Det måste alltså inte framgå direkt till vilken person den aktuella upplysningen hänför sig till så länge det finns andra uppgifter som tillsammans gör att det är möjligt att koppla ihop uppgifterna med en person.

När det gäller pseudonymisering ska de kompletterande uppgifterna (såsom exempelvis kodnyckel) förvaras separat. Denna förvaring ska kringgärdas av tekniska och organisatoriska åtgärder som gör det svårare att koppla samman uppgifterna.[7]

Nedan följer några exempel för att illustrera hur det är möjligt att tänka gällande pseudonymisering.

1. **Information: Kalle Karlsson med personnummer XXXXXX-XXXX har cancer**

   I exemplet nämns Kalle Karlsson vid namn vilket innebär att vi har att göra med en identifierbar fysisk person. Det är alltså inte fråga om pseudonymiserade uppgifter. Uppgiften att Kalle Karlsson har cancer är dessutom en känslig personuppgift (uppgift om hälsa).

2. **Information: Forskningsperson 123 har cancer.** I ett låst skåp på en klinik som bara behörig personal har tillgång till finns en lista som

[4] Art. 9, GDPR.
[5] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/personnummer/, hämtad 2022-08-17.
[6] Art. 4.5, GDPR.
[7] Art. 4.5, GDPR.

möjliggör att löpnumret 123 kan kopplas ihop med Kalle Karlsson. Listan förvaras separat från informationen.

I informationen nämns inte Kalle Karlsson vid namn. Informationen är dock ändå personuppgifter men i pseudonymiserad form. Att det finns kompletterande uppgifter med löpnummer gör att det finns en möjlighet att koppla ihop informationen med en identifierbar fysisk person (Kalle Karlsson). Uppgiften om cancer är dessutom en känslig personuppgift (uppgift om hälsa).

2.6. Vad är anonymiserade uppgifter?

GDPR tillämpas inte på så kallade anonymiserade uppgifter. Anonymiserade uppgifter är information som inte kan kopplas samman med en person.[8] Skillnaden mellan anonymiserade uppgifter och pseudonymiserade uppgifter är alltså att pseudonymiserade uppgifter med hjälpmedel (t.ex. en kodnyckel) kan kopplas samman med en person, vilket helt anonymiserade uppgifter inte kan. Det är svårt att helt anonymisera uppgifter och tröskeln för vad som är att betrakta som personuppgifter är låg. Vid forskning är det oftast fråga om pseudonymiserade uppgifter vilket gör att reglerna i GDPR måste följas. Om det råder osäkerhet om de uppgifter som ska användas i forskningen är anonymiserade rekommenderas att uppgifterna hanteras som personuppgifter.

3. Förutsättningar för att forska på känsliga personuppgifter

3.1. Vilar forskningen på rättslig grund?

Precis som för all annan personuppgiftsbehandling måste personuppgiftsbehandling som sker inom ramen för ett forskningsprojekt vila på en rättslig grund. Utan en rättslig grund är behandlingen av personuppgifter inte laglig.

I GDPR finns det olika rättsliga grunder för personuppgiftsbehandling. Vad gäller personuppgifter som används för forskning är det för myndigheter och offentlig verksamhet främst den rättsliga grunden *allmänt intresse* som är relevant.[9] Denna rättsliga grund kan användas om en personuppgiftsbehandling är nödvändig för att utföra en uppgift av allmänt intresse.

Det allmänna intresset måste också vara fastställt enligt unionsrätten eller medlemsstatens nationella rätt. Detta innebär att uppgifter av allmänt intresse ska ha stöd i lag eller författning. En relevant fråga att ställa sig är därför om det ingår i verksamhetens uppdrag att ägna sig åt forskning. Med andra ord: är forskningen kompetensenlig? För regioner finns stöd i t.ex. hälso- och sjukvårdslagen där det framgår att regioner ska medverka vid finansiering, planering och genomförande av dels kliniskt forskningsarbete på hälso- och sjukvårdens område, dels folkhälsovetenskapligt forskningsarbete. Det framgår också att regioner ska i dessa frågor, i den omfattning som behövs, samverka med varandra och med

[8] Skäl 26, GDPR.
[9] Art. 6.1. e, GDPR.

berörda universitet och högskolor.[10] I de flesta fall är det därför inte någon tvekan om att forskningen är kompetensenlig, men om en av regionens verksamheter som inte är en hälso- och sjukvårdsmyndighet vill bedriva forskning på personuppgifter kan frågan om kompetensenlighet behöva utredas noggrannare.

I GDPR finns också den rättsliga grunden samtycke. Det är lätt att blanda ihop den rättsliga grunden samtycke i GDPR med det samtycke som en forskningsperson i vissa fall ger till själva forskningen. Detta är dock två skilda saker och samtycke enligt GDPR används vanligtvis enbart då ingen annan rättslig grund går att tillämpa. I vissa fall kan det till och med vara olämpligt eller inte ens möjligt att använda samtycke som rättslig grund för personuppgiftsbehandlingen.

3.2. Ändamålsbegränsning

Vid forskning kan det antingen vara så att forskaren samlar in uppgifter ”från scratch” för det primära ändamålet forskning, eller så använder forskaren personuppgifter som redan samlats in för ett annat primärt ändamål, t.ex. ett vårdändamål.

I GDPR finns en grundläggande princip om ändamålsbegränsning. Denna princip innebär i korthet att den som samlar in personuppgifter måste ha klart för sig varför personuppgifterna samlas in redan vid insamlandet, och inte senare behandla personuppgifterna på ett nytt sätt som är oförenligt med varför personuppgifterna samlades in från första början. Det finns dock undantag från denna princip när det gäller just forskning.

Har någon med rättslig grund samlat in uppgifter för ett primärt ändamål som inte är forskning, kan dessa uppgifter utan hinder av principen om ändamålsbegränsning behandlas för ändamålet vetenskapligt forskningsändamål (s.k. behandling för ”ytterligare ändamål”).[11]

Tänk dock på att det kan finnas hinder i annan lagstiftning som gör att den ytterligare behandlingen förhindras, t.ex. att uppgifterna av sekretesskäl inte kan lämnas ut från vården till forskning.

Särskild reglering finns också exempelvis på följande områden:

- Nationella och regionala kvalitetsregister, (se Patientdatalag 7 kap. 6 §).
- Lagen om biobanker inom hälso- och sjukvården m.m., (se 5 kap. 5 §).
- Lagen om blodsäkerhet, (se 16 §).
- Lagen om kvalitets- och säkerhetsnormer vid hantering av mänskliga vävnader och celler, (se 21 §).

3.3. Forskningsundantag för känsliga personuppgifter

Behandling av känsliga personuppgifter är som tidigare nämnts som utgångspunkt förbjuden, men det finns ett viktigt undantag i GDPR som gör det möjligt att behandla känsliga personuppgifter för just vetenskapliga forskningsändamål.[12] Eftersom hälsa är en känslig personuppgift blir detta undantag mycket viktigt att ha koll på vad gäller forskning som sker inom ramen för regionens verksamhet.

[10] 18 kap 2 §, Hälso- och sjukvårdslag (2017:30).
[11] Art. 6.4 och 5.1.b, GDPR.
[12] Art. 9. 2.j, GDPR.

Nedan kommer en utveckling av förutsättningarna för att undantaget ska vara tillämpbart.

3.3.1. Vidta lämpliga och särskilda åtgärder

För att undantaget ska vara tillämpligt måste lämpliga och särskilda skyddsåtgärder vidtas i syfte att säkerställa den registrerades rättigheter och friheter. Detta inbegriper tekniska och organisatoriska åtgärder.[13] Vad för åtgärder som ska vidtas i varje specifik forskning är svårt att uttala sig generellt om, men nedan följer några åtgärder som är viktiga att ha koll på. Läs gärna också annan generell information om informationssäkerhet på insidan som även är relevant när det gäller forskning. Detta hittar du här.

Pseudonymisering
En åtgärd kan vara pseudonymisering av personuppgifter.[14] Om det fortfarande är möjligt att uppnå syftet med forskningen efter det att uppgifterna pseudonymiserats är rekommendationen att pseudonymiseringstekniker används. Som tidigare nämnts är ett exempel på en pseudonymiseringsteknik att byta ut namn och personnummer mot ett löpnummer.

Uppgiftsminimering
Vidare ska principen om uppgiftsminimering särskilt beaktas.[15] Principen innebär att de uppgifter som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Med andra ord ska ni inte behandla mer personuppgifter än de som ni behöver för er forskning.

Etikgodkännande
Enligt svensk rätt är också ett godkännande från etikprövningsmyndigheten en fastställd lämplig och särskild åtgärd som krävs vid personuppgiftsbehandling av känsliga personuppgifter för forskningsändamål och därför måste alltid ett sådant godkännande inhämtas innan forskningen påbörjas.[16]

3.3.2. Den registrerades rätt till information

I GDPR finns en rättighet för personer att få reda på hur regionen behandlar deras personuppgifter.[17] Som ovan nämnts måste den som genomför personuppgiftsbehandling för vetenskapliga forskningsändamål se till att den registrerades rättigheter tryggas genom lämpliga och särskilda åtgärder. Detta gäller även individers rätt till information. Informationen kan lämnas på lite olika sätt beroende på forskningstyp. Tänk på att det även kan finnas en informationsskyldighet för regionen i annan lagstiftning utöver GDPR, t.ex. i etikprövningslagen.

[13] Art. 5.1.c och 89.1, GDPR.
[14] Art. 89.1, GDPR.
[15] Art. 5.1.c och 89.1, GDPR.
[16] Etikprövningslagen (2003:460), SOU 2017:50 s. 332, lag (2018:1091) med kompletterande bestämmelser om etisk granskning till EU:s förordning om kliniska prövningar av humanläkemedel och lag (2021:603) med kompletterande bestämmelser om etisk granskning till EU:s förordning om medicintekniska produkter.
[17] Art. 12-14, GDPR.

Undantag från den registrerades rätt till information

Vad gäller forskning kan det i vissa fall vara möjligt att göra undantag från utgångspunkten att individer ska informeras om den personuppgiftsbehandling som sker. Nedan nämns några sådana exempel.

Ett undantagsfall som kan bli tillämpligt är när personuppgifterna samlats in från annan än individen själv och det bedömts vara omöjligt eller skulle innebära en oproportionerlig ansträngning att informera denne.[18] Undantaget ska tillämpas restriktivt. För att undantaget ska vara tillämpligt måste omöjligheten eller den oproportionella ansträngningen vara direkt kopplad till det faktum att uppgifterna inte samlats in direkt av den registrerade. En sammanvägd bedömning får göras i det enskilda fallet och denna avvägning bör alltid dokumenteras. Faktorer som spelar in i avvägningen är följande:

- Var det länge sedan personuppgifterna samlades in?
- Rör det sig om väldigt många registrerade?
- Har lämpliga skyddsåtgärder vidtagits och har en riskanalys gjorts?[19]

Även om man kommer fram till att undantaget blir tillämpligt ska information om att forskning och personuppgiftsbehandling äger rum ändå göras tillgängliga för allmänheten på något sätt.[20] Detta kan förslagsvis göras genom en skrivelse på någon av regionens externa webbplatser.

Ytterligare en undantagssituation gäller om personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt eller andra lagstadgade sekretessförpliktelser.[21] Enligt svensk rätt är det exempelvis förbjudet att vad gäller officiell statistik vidta åtgärder i syfte att söka utröna enskildas identitet.[22] Vidare gäller enligt GDPR att om de ändamål som personuppgifter behandlas för inte kräver eller inte längre kräver att den registrerade identifieras ska den personuppgiftsansvarige inte vara tvungen att bevara, förvärva eller behandla ytterligare information för att identifiera den registrerade endast i syfte att följa GDPR.[23] Detta innebär exempelvis att när ett forskningsprojekt tar emot personuppgifter i pseudonymiserad form som omfattas av statistiksekretess, ska forskningsprojektet inte i syfte att kunna informera de registrerade om den personuppgiftsbehandling som kommer att äga rum, efterforska vem uppgifterna är kopplade till.

3.3.3. Personuppgiftsbehandlingen måste vila på grundval av unionsrätt eller nationell rätt

För att forskningen ska få göras på känsliga personuppgifter måste den dessutom vila på grundval av unionsrätten eller medlemsstaternas nationella rätt. Detta innebär att forskningen måste vara förenlig med alla de aktuella och tillämpliga lagar och bestämmelser som gäller utöver GDPR och etikprövningslagen. Vilka lagar och bestämmelser som blir tillämpliga för ett specifikt forskningsprojekt kan variera och måste analyseras i varje specifikt fall.

3.3.4. Personuppgiftsbehandlingen måste vara proportionerlig

Personuppgiftsbehandlingen i forskningen måste dessutom vara proportionerlig i förhållande till det eftersträvade syftet. Detta innebär att den förväntade nyttan av forskning på känsliga personuppgifter ska vägas mot den enskildes rätt till integritet. Rätten till skydd av personuppgifter måste alltså förstås utifrån sin uppgift i samhället och också vägas mot andra grundläggande rättigheter.[24]

[18] Art. 14.5.b, GDPR.
[19] Skäl 62, GDPR.
[20] Art. 14.5.b, GDPR.
[21] Art. 14.5.d, GDPR.
[22] 6 §, Lag (2001:99) om den officiella statistiken.
[23] Art. 11, GDPR.
[24] Skäl 4, GDPR.

3.3.5. Personuppgiftsbehandlingen måste vara förenlig med dataskyddslag

För att få forska på känsliga personuppgifter måste forskningen vara förenlig aktuell dataskyddslag. Detta innebär bland annat att GDPR och dess grundläggande principer måste beaktas, samt även andra regler kring dataskydd i andra lagar. Läs därför gärna också annan generell information om GDPR på insidan. Detta hittar du här.

Att personuppgiftsbehandlingen måste vara förenlig med innehållet i dataskyddslag innebär också en påminnelse om att reglerna i patientdatalagen och andra nationella registerförfattningar gäller. Dessa regler begränsar i vissa fall ytterligare förutsättningarna för forskning på just känsliga personuppgifter samt förutsättningarna för hur forskare kan få tillgång till hälsodata.

Ett exempel på detta är regler kring elektronisk åtkomst och direktåtkomst. Om forskningsverksamheten bedrivs av en självständig verksamhetsgren inom myndigheten, av en annan myndighet eller av en enskild eller ett enskilt organ måste utlämnandet föregås av sekretessprövning.[25] Detta innebär att elektronisk åtkomst inte är tillåten i dessa fall. Klinisk forskning som sker inom en och samma vårdgivare och som ett led i vård av patient kan beroende på hur den är organiserad falla inom den inre sekretessen och för ett sådant ändamål är elektronisk åtkomst tillåten. Även om kliniskt forskningsarbete sker integrerat med patientvården kan forskningen i vissa fall ändå utgöra en självständig verksamhetsgren.[26] Vidare gäller att vårdgivare som deltar i sammanhållen journalföring inte får ges direktåtkomst till varandras patientuppgifter för forskningsändamål.[27] Tillgång till personuppgifter i dessa situationer kan endast ges genom principen om utlämnande av allmän handling. Utlämnande kan ske först efter det att en noggrann sekretessprövning gjorts.

4. Överväger ni att överföra personuppgifter utanför EU/EES?

Har ni tänkt att inom ramen för forskning överföra personuppgifter utanför EU/EES (ett så kallat tredje land)? Exempel på när detta kan ske är när ni samarbetar med en aktör utanför EU/EES såsom en amerikansk sponsor vid en klinisk läkemedelsprövning, eller om ni har tänkt att använda en molntjänst med amerikansk anknytning som ett verktyg i forskningen.

Tredjelandsöverföring av personuppgifter är som utgångspunkt förbjuden enligt GDPR, men det finns vissa undantag. Reglerna är dock strikta och komplicerade. Om ni avser att överföra personuppgifter utanför EU/EES rekommenderas därför att ni utreder möjligheterna för detta särskilt.

[25] Prop. 2007/08:126 s. 205.
[26] Prop. 2007/08:126 s. 51.
[27] Prop. 2007/08:126 s. 204.