SND
Svensk nationell datatjänst

Personuppgifter i forskning – allmänt om dataskyddsförordningen

Pass 6: Forskningsjuridik

BAS Online 2021-01-20

Skyddet för enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter regleras från och med den 25 maj 2018 i EU:s dataskyddsförordning, (GDPR). Området reglerades tidigare i personuppgiftslagen som nu är upphävd. Hädanefter kommer jag att använda begreppet dataskydds-förordningen.

Dataskyddsförordningen innebär vissa förändringar jämfört med personuppgiftslagen, bland annat förstärks rättigheterna för den som personuppgifterna avser och skyldigheterna skärps för den som behandlar personuppgifterna. Den som bryter mot för-ordningens regler kan komma att få höga sanktionsavgifter. Detta gäller även myndigheter. Det finns också bestämmelser om ansvarsskyldighet, vilket innebär att den som behandlar person-uppgifter ska kunna visa att reglerna efterlevs. Detta innebär i praktiken att det är viktigt att dokumentera alla ställningstaganden som görs.

EU:s dataskyddsförordning kompletteras med ett antal nationella lagstiftningar, däribland dataskyddlagen. EU:s dataskydds-förordning är dock direkt tillämplig och regelverket träffar alla verksamheter som behandlar personuppgifter inom EES/EU.

Det kan ibland vara svårt att hålla isär dataskyddsförordningen och offentlighets- och sekretesslagen (OSL). Lite förenklat kan man säga att båda lagstiftningarna gäller samtidigt men reglerar helt olika

situationer. Dataskyddsförordningen gäller all personuppgifts-behandling i all verksamhet, oavsett vad som görs med uppgifterna, medan OSL aktiveras när uppgifter som berörs av sekretess ska lämnas ut eller delas med andra utanför en offentlig verksamhet (en sekretessgräns ska passeras). Dataskyddsförordningen träffar enbart personuppgifter medan OSL reglerar vad som omfattas av sekretess, vilket även andra uppgifter än personuppgifter kan omfattas av.

Personuppgiftsbehandling

I princip alla former av åtgärder med personuppgifter räknas som en behandling av personuppgifter. En behandling kan bestå av insamling, registrering, sammanställning, bearbetning och användning, spridning, återvinning, lagring och utlämnande av personuppgifter. Även begränsning, radering eller förstöring av personuppgifter räknas som en personuppgiftsbehandling.

Personuppgifter

Innan jag pratar vidare kring behandling av personuppgifter ska jag först gå igenom vad en personuppgift är och nämna några olika typer av personuppgifter. Dessa kommer du säkert att känna igen från pass 2, i presentationen om säkerhet och personuppgifter.

Definitionen av vad som utgör personuppgifter är mycket vid-sträckt. Det som avgör om en uppgift ska anses vara en person-uppgift eller inte är om uppgiften enskilt eller i kombination med andra uppgifter kan knytas till en levande person.

Ett registreringsnummer på en bil kan till exempel utgöra en personuppgift om numret går att härleda till en person, men behöver inte vara det om det är en företagsbil som används av flera olika personer på företaget. Ett bolagsnummer är inte en personuppgift om det är ett stort företag, men kan vara en person-uppgift om det är ett enmansföretag. Personuppgiftsbegreppet kan

alltså variera och avgörande är om uppgiften går att koppla till en levande person eller inte.

Direkta personuppgifter är sådana uppgifter som tydligt identifierar en person, t.ex. namn, foto eller personnummer. I forsknings-sammanhang försöker man undvika att använda sådana typer av uppgifter när data t.ex. sammanställs i en datafil. Istället för personnummer kan man använda ID-nummer eller andra koder som sedan kan kopplas till personnummer med hjälp av en kodnyckel. Då kan man istället prata om krypterade eller kodade uppgifter, det vill säga insamlade personuppgifter som är kodade för den som behandlar uppgifterna, men möjligheten att koppla uppgifter till enskilda individer kvarstår. Så länge kodnyckeln finns kvar kommer dessa data därför att betraktas som personuppgifter och behöver behandlas och skyddas på ett adekvat sätt.

Indirekta personuppgifter är flera uppgifter som i kombination med varandra kan användas för att identifiera en person. Det kan exempelvis vara medlemskap i en viss förening, bostadsort, information om inkomst eller hälsorelaterade uppgifter. Relaterat till forskning kan uppgifter om bostadsort och yrke vara tillräcklig information för att identifiera en person, om orten är liten och det bara finns en person med ett visst yrke.

Känsliga personuppgifter

Känsliga personuppgifter är personuppgifter som anses särskilt känsliga till sin natur och därför har ett starkare skydd. Behandling av känsliga personuppgifter är som utgångspunkt förbjuden och det krävs att något av undantagen i dataskyddsförordningens artikel 9 är tillämpligt för att behandlingen ska få göras. Ett av undantagen är forskningsändamål. En förutsättning för att tillämpa detta undantag är att det finns ett giltigt etiktillstånd för forskningen samt att lämpliga och särskilda åtgärder för att säkerställa forskningspersonens grundläggande rättigheter och intressen tas

tillvara. Behandling av känsliga personuppgifter kräver särskilda skyddsåtgärder som till exempel pseudonymisering och andra tekniska och organisatoriska åtgärder som till exempel kryptering, behörighetsbegränsningar och avtal.

Till känsliga personuppgifter räknas uppgifter som:

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i en fackförening
- uppgifter om hälsa
- en persons sexualliv eller sexuella läggning
- genetiska uppgifter
- biometriska uppgifter som identifierar en person.

När upphör personuppgifter att vara personuppgifter?

För att personuppgifter ska vara avidentifierade behöver alla möjligheter till identifiering vara borta. Det innebär att det inte får finnas några direkta identifierare, inte heller indirekta uppgifter som möjliggör bakvägsidentifiering, och det får inte heller finnas en kodnyckel som till exempel gör det möjligt att koppla ett ID-nummer till ett personnummer. Det spelar heller ingen roll om en kodlista för pseudonymiserade uppgifter bevaras hos en annan myndighet eller på ett annat lärosäte – uppgifterna bedöms fortfarande vara personuppgifter så länge kodlistan finns kvar. Det krävs att kodnyckeln förstörs för att pseudonymiserade uppgifter ska upphöra att vara personuppgifter.

Om alla möjligheter att identifiera personer är undanröjda och det inte längre går att identifiera en person i datamängden så upphör uppgifterna att vara personuppgifter. Det innebär i sin tur att dataskyddsförordningen inte längre är tillämplig.

Innan vi går vidare och pratar om vilka krav som dataskydds-förordningen ställer på den som behandlar personuppgifter vill jag beröra begreppen personuppgiftsansvarig och personuppgifts-biträde.

Personuppgiftsansvarig

En personuppgiftsansvarig är den som bestämmer *ändamål* och *medel* för en personuppgiftsbehandling. Det är alltid organisationen som är personuppgiftsansvarig och inte enskilda personer. Normalt sett är det alltså lärosätet som är personuppgiftsansvarig och inte en enskild forskare eller prefekt. Om ett personuppgiftsansvarigt lärosäte samarbetar med ett annat lärosäte inom forskning eller med ett sjukhus är det oftast fråga om två självständiga person-uppgiftsansvariga som var och en för sig ansvarar för respektive verksamhets personuppgiftsbehandling. Det finns även en möjlighet att vara gemensamt personuppgiftsansvariga.

Personuppgiftsbiträde

Vad är då ett personuppgiftsbiträde? Jo, den som behandlar person-uppgifter för den personuppgiftsansvariges räkning är person-uppgiftsbiträde. Personuppgiftsbiträdet har ingen egen bestämmanderätt över behandlingen. Om en personuppgifts-ansvarig anlitar ett personuppgiftsbiträde så kräver dataskydds-förordningen att ett personuppgiftsbiträdesavtal upprättas. Ett sådant avtal kallas ofta PUB-avtal eller PUBA. Det kan vara bra att känna till att ett PUBA måste kopplas till ett annat befintligt avtal, som till exempel ett uppdragsavtal eller samverkansavtal. Ett typexempel på en biträdessituation är om ett lärosäte anlitar ett externt företag för att tillhandahålla e-post. Det externa företaget har ingen egen bestämmanderätt över de personuppgifter som går genom företagets servrar – all behandling av personuppgifter sker på uppdrag av lärosätet.

Grundläggande principer

I dataskyddsförordningen finns ett antal grundläggande principer som kan sägas vara kärnan i förordningen. Principerna gäller för all personuppgiftsbehandling. Man ska alltid ha principerna i bakhuvudet när man arbetar med personuppgiftsbehandling. Principerna innebär att den som är personuppgiftsansvarig ska följa nedanstående.

Principen om laglighet, korrekthet och öppenhet:

- Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt. Detta uppfylls bland annat genom att fastställa en rättslig grund för behandlingen. Kravet på korrekthet innebär att behandlingen ska vara rimlig och proportionerlig i förhållande till de registrerade. Öppenhetskravet uppfylls genom att de registrerade får information om behandlingen.

Principen om ändamålsbegränsning:

- Uppgifterna får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål och får inte senare behandlas på ett sätt som är oförenligt med ändamålen.

Principen om uppgiftsminimering:

- Uppgifterna som ska behandlas är adekvata, relevanta och inte för omfattande i förhållande till ändamålet.

Principen om riktighet:

- Uppgifterna som behandlas ska vara riktiga och aktuella. Uppgifter som är felaktiga för ändamålet måste kunna raderas eller korrigeras, vilket ställer krav på den teknik som används för bearbetning och lagring.

Principen om lagringsminimering:

- Uppgifterna ska inte förvaras under längre tid än nödvändigt för ändamålet. Undantag görs för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål och statistiska ändamål.

Principen om integritet och konfidentialitet:

- Uppgifterna ska behandlas på ett säkert sätt, som skyddar mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada – det här minns du säkert från pass 2 om datahantering.

Principen om ansvarsskyldighet:

- Det ska finnas en personuppgiftsansvarig som ansvarar för och kan visa att dessa principer efterlevs. Detta kan uppfyllas genom att till exempel upprätta en dataskydds-policy, informera de registrerade, utse ett dataskydds-ombud och genom att utföra konsekvensbedömningar vid särskilt riskfyllda behandlingar.

Rättslig grund

För att man överhuvudtaget ska få behandla personuppgifter måste man ha en rättslig grund för personuppgiftsbehandlingen. Det finns sex olika rättsliga grunder, där det i huvudsak är det den rättsliga grunden *allmänt intresse* som gäller vid forskning vid en myndighet. I enstaka fall är det den rättsliga grunden *samtycke* som är tillämplig.

För att en myndighet ska ha stöd i den rättsliga grunden allmänt intresse för sin personuppgiftsbehandling måste myndigheten ha en lagreglerad uppgift att utföra. Lärosäten faller i de flesta fall under högskolelagen av vilken det framgår att undervisning, forskning och samverkan är en lagreglerad uppgift. Detta innebär

att lärosäten alltså har den rättsliga grunden allmänt intresse som stöd för att utföra undervisning, forskning och samverkan.

Den rättsliga grunden samtycke är problematisk för myndigheter att använda. Det är mycket svårt att få ett giltigt samtycke för personuppgiftsbehandling inom forskning eftersom det anses råda en obalans i maktförhållandet mellan de enskilda forskningspersonerna och forskningsutföraren. I en sådan situation är det i princip omöjligt att få ett samtycke som bedöms vara giltigt. Det rekommenderas därför att den rättsliga grunden allmänt intresse används.

Personuppgiftsbehandlingen som sker med anledning av forskningsprojekt sker alltså vanligen med stöd av den rättsliga grunden allmänt intresse och forskaren behöver därför inte hämta in samtycke för själva personuppgiftsbehandlingen. Däremot måste man i de allra flesta fall hämta in samtycke för deltagande i själva forskningsprojektet. Det är en mycket vanlig missuppfattning att de här två olika samtyckena blandas ihop. Jag kommer att prata lite mer om detta i passet för etikprövningslagen.

Information till de registrerade

En viktig del av dataskyddsregleringen och skyddet för forskningspersonerna är att forskningspersonerna, eller de registrerade som man säger i dataskyddssammanhang, ska få information om hur deras uppgifter kommer att behandlas.

Detta krav på information om personuppgiftsbehandlingen tillkommer alltså utöver kraven på information om själva forskningsprojektet. Det sistnämnda är reglerat i etikprövningslagen och gäller vad man brukar kalla informerat samtycke.

Informationskravet enligt dataskyddsförordningen ser lite annorlunda ut och gäller annan typ av information.

Dataskyddsförordningen ställer krav på att forskningspersonerna ska informeras om vem som är personuppgiftsansvarig och vilket dataskyddsombud som kan kontaktas. Forskningspersonerna ska också få information om vad som är ändamålet med behandlingen och vilken rättslig grund behandlingen stödjer sig på. Om uppgifterna samlas in från någon annan, till exempel från ett register, ska detta uppges. Det ska framgå om uppgifterna kommer att lämnas vidare eller lämnas ut samt hur länge uppgifterna ska lagras. Det ska också framgå var forskningspersonerna kan vända sig för att klaga på behandlingen, vilket oftast är Datainspektionen, om personuppgiftsbehandlingen sker inom Sverige. Det ska vidare lämnas information om hur de registrerades rättigheter hanteras och en hänvisning ska finnas till dataskyddsombud.

Som DAU-medarbetare fyller du en viktig roll i att hjälpa forskaren att identifiera regelverk som kommer att bli aktuella under forskningen, vilket behöver göras tidigt i forskningsprocessen. Det är inte minst viktigt för att veta vad man har att förhålla sig till och vilka säkerhetskrav som kommer att vara nödvändiga för att hålla lämplig skyddsnivå till materialet. Redan vid planeringen av ett forskningsprojekt ska forskaren göra en konsekvensbedömning, dvs. en risk- och sårbarhetsanalys. I en sådan analys tar man med vilka regelverk som kommer att bli aktuella med hänsyn till den forskning som ska bedrivas.

Sammanfattning

Du har nu fått en introduktion till personuppgifter i forskning och dataskyddsförordningen. Dataskyddsförordningen är det regelverk som är tillämpligt på all personuppgiftsbehandling. All person-uppgiftsbehandling kräver en rättslig grund och att de allmänna principerna beaktas. Känsliga personuppgifter kräver etiktillstånd och skyddsåtgärder. Det är viktigt att forskningspersonerna får korrekt information angående personuppgiftsbehandlingen.