

Pass 6 Forskningsjuridik

Skydd för personlig integritet

I den här presentationen kommer du att få en introduktion till personlig integritet. Inledningsvis ska jag prata om vad personlig integritet egentligen handlar om, vad en kränkning av den personliga integriteten innebär, för att sedan gå över till att prata om personuppgifter och hur de får behandlas i enlighet med regelverk.

Det finns ingen tydlig, juridisk, definition av vad personlig integritet innebär, så när man talar om personlig integritet kan det handla om olika saker för olika personer; det kan handla om rätten att få vara ifred, rätten till ett privatliv utan annan insyn än vad man bjuder in människor till, rätten att inte bli kränkt och uthängd i olika sammanhang. Vad som utgör en kränkning av den personliga integriteten blir därför också beroende av sammanhanget: av vilka uppgifter som samlats in, vem som har samlat in dem, varför de används, vilken spridning de fått och vilka konsekvenser det har eller kan få. Det som en person upplever som en kränkning av sin personliga integritet behöver därför inte en annan person uppleva på samma sätt.

Vi lämnar ifrån oss personuppgifter i alla möjliga slags situationer i livet: i vårt offentliga liv lämnar vi personnummer och kontaktuppgifter i föreningar vi är med i, kontonummer och personuppgifter i autogiromedgivanden, flera olika personuppgifter i körkortsregistret, till arbetsgivaren och i vården.

I privatlivet delar vi med oss av mängder med information, till exempel i sociala medier, evenemangslistor och e-post.

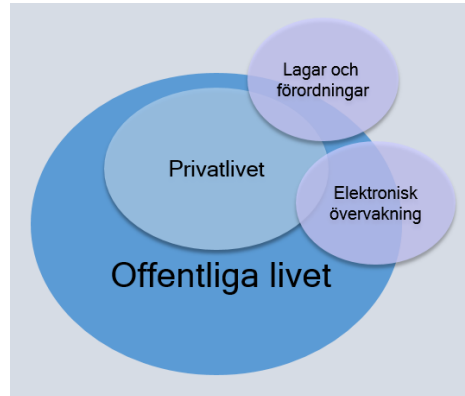
Vi har dessutom lagar och förordningar som *säger* att vi ska dela med oss av våra personuppgifter i olika sammanhang. Våra data finns t.ex. i register hos Försäkringskassan, Skatteverket och Statistiska centralbyrån. Det finns också grundlagar som innebär att uppgifter om enskilda personer får spridas, som till exempel offentlighetsprincipen.

Vidare lämnar vi också spår i affärer när vi betalar med kort, biometriska uppgifter samlas in via övervakningskameror, telefoner, i samband med inlogningar och inpasseringar – så uppgifter om oss finns överallt.

När det gäller uppgifter vi lämnar privat, så ska vi kunna vänta oss att de förblir privata om vi inte godkänt något annat (till exempel i olika sociala

mediers dokument för godkännande av tjänstens villkor), medan uppgifter vi lämnar i det offentliga livet är föremål för mycket mer omfattande data-behandling.

Vad vill jag ha sagt med det här?
Vi lever i en komplex värld och personuppgifter sparas utan att vi alltid har så mycket att säga till om. Som jag redan belyst är personlig integritet inte ett definierat begrepp och vi har nog alla en uppfattning om vad det är, men om vi skulle sätta oss ner och diskutera innebörden skulle vi nog kunna få lika många åsikter som deltagare i diskussionen.



Det regelverk som skyddar människorna mot att den personliga integriteten kränks genom behandling av personuppgifter regleras från och med den 25 maj 2018 i Dataskyddsförordningen, som på engelska benämns General Data Protection Regulation och förkortas GDPR.

Dataskyddsförordningen innebär i det stora hela inga större förändringar jämfört med tidigare regelverk, men man förstärker rättigheterna för den som personuppgifterna avser, och skärper skyldigheterna för den som behandlar personuppgifterna. Den som bryter mot förordningens regler kan komma att få höga sanktionsavgifter.

EU:s dataskyddsförordning kompletteras med ett antal nationella lagstiftningar, däribland Forskningsdatalagen som ska vara tillämplig för personuppgiftsbehandling för forskningsändamål.

Men vad är det som lagstiftningen vill hjälpa mig med och skydda mig mot? Det vill säga: vad är en integritetskränkning? Jo, då säger man att det kan beskrivas som att *förlora kontrollen över sin egen person eller en viss typ av uppgifter om sig själv*.

Som jag sa tidigare finns det faktorer som har betydelse. Det spelar t.ex. roll vilken typ av personuppgifter som samlas in och registreras, varför det görs, på vilket sätt och av vem, hur uppgifterna används, mängden av uppgifter, och huruvida uppgifterna är tillgängliga för bearbetningar och sammanställningar.

Man kan ha olika anledningar till att samla in och registrera personuppgifter. Det är till exempel stor skillnad på om du samlar in personuppgifter för att bjuda hem några vänner på middag eller om tvivelaktig politisk organisation samlar in samma uppgifter. *Var uppgifterna landar* kan innebära en integritetskränkning, inte bara att uppgifterna är insamlade. Det spelar också roll *varför* uppgifterna samlas in. Att bli bjuden på middag är ju trevligt, men att hamna i ett tvivelaktigt register är kanske inte lika angenämt – det är ju inte för att de vill bjuda en på middag. *Hur uppgifterna används* har också betydelse. Används de för skicka hotbrev till journalister, eller används de för att vi ska träffas och ha trevligt?

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.

Du är kanske redan bekant med definitionen av en personuppgift. Lagstiftaren säger att det är *”All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet”*.

Direkta personuppgifter är sådana uppgifter som tydligt identifierar en person, t.ex. namn, foto eller personnummer. I forsknings-sammanhang brukar man dock 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 på ett sådant sätt att de ska vara anonyma 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.

Till sist ska jag också nämna känsliga personuppgifter, vilka har ett starkare skydd i regelverket och generellt sett inte får behandlas alls. För att behandla

dessa krävs uttryckligt samtycke från den registrerade och godkänd etikprövning.

Till känsliga personuppgifter räknas uppgifter om:

- 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.

Det finns också särskilda bestämmelser som avser behandling av personnummer och uppgifter som avser lagöverträdelse. Dessa uppgifter är inte känsliga personuppgifter men betraktas som särskilt skyddsvärda.

För att data 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. Om alla dessa möjligheter är undanröjda och det inte går att identifiera en person i datamängden så upphör uppgifterna att vara personuppgifter. Det innebär därmed att uppgifterna kan behandlas utan att tillämpa regelverket som avser personuppgifter.

Behandling av personuppgifter

Nu ska jag prata lite mer om just behandling av personuppgifter. Alla former av hantering av personuppgifter räknas som en slags behandling. Det kan innefatta allt från insamling, registrering, sammanställning, bearbetning och användning, till spridning, återvinning, lagring och utlämnande.

För att man överhuvudtaget ska få behandla personuppgifter finns det vissa principer som måste vara uppfyllda:

- Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt.
- 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 – det som även kallas för finalitetsprincipen.

- Uppgifterna måste vara adekvata, relevanta och inte för omfattande i förhållande till ändamålet.
- Uppgifterna 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.
- Uppgifterna får inte förvaras under längre tid än nödvändigt för ändamålet. Undantag görs för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål och statistiska ändamål.
- 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.
- Det ska också finnas en personuppgiftsansvarig som ansvarar för och kan visa att dessa principer efterlevs. För högskolor och universitet är det lärosätet som är personuppgiftsansvarig.

Nu är det inte så enkelt som att man kan behandla personuppgifter bara man uppfyller de grundläggande principerna för hur uppgifter behandlas, utan det måste även finnas rättsliga grunder för att få göra det.

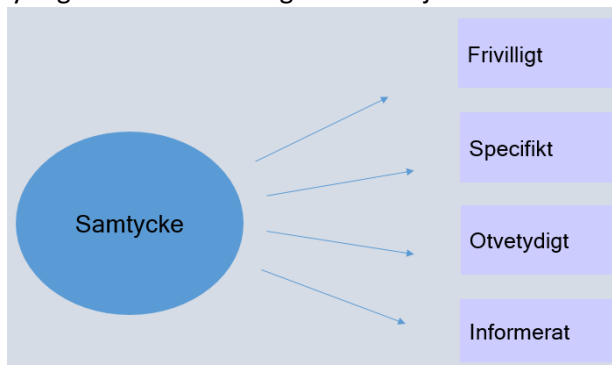
Samtycke

Det allra vanligaste kravet är att personuppgifter bara får behandlas med den registrerades *samtycke*. I vissa situationer kan det vara tillåtet att behandla personuppgifter utan att ha fått samtycke, för att man bedömer att behandlingen är nödvändig och inte av skada för den registrerade. Det kan t.ex. handla om *skydd för den registrerades vitala intresse* som ger möjlighet att utan samtycke behandla personuppgifter vid akut sjukvård. För forskning är det också möjligt att hantera personuppgifter utan samtycke om *behandlingen är nödvändig för att utföra en uppgift av allmänt intresse*. Det här blir framför allt aktuellt när det handlar om exempelvis registerforskning, där man med hjälp av undantagsregeln kan samla in och behandla personuppgifter som i annat fall skulle innebära en omöjlig eller proportionerligt stor arbetsinsats.

Samtycket ska vara frivilligt och individuellt, det vill säga att varje forskningsperson måste själv, eller genom sin vårdnadshavare, ge sitt samtycke till att personuppgifter får behandlas.

Samtycket ska vara specifikt för en viss behandling och ett visst ändamål. Som vi redan talat om så gäller finalitetsprincipen: personuppgifter får inte senare användas för andra ändamål än vad man har fått samtycke för, så det är viktigt för en forskare att vara noggrann och tydlig i forskningspersons-informationen.

Samtycket ska vara otvetydigt – uttalat eller genom en entydigt bekräftande handling. Om det handlar om känsliga personuppgifter måste samtycket vara uttryckligt. Jag kommer att prata om detta längre fram. En bekräftande handling är till exempel när man skickar in en besvarad enkät, eftersom det kan ses som att man genom en medveten handling samtycker till att enkätsvaren får behandlas. Ett samtycke får däremot inte vara hypotetiskt, där man utgår från att den registrerade hade samtyckt om frågan hade ställts, och inte heller tyst genom att den registrerade själv förväntas ta initiativ till att säga nej till behandlingen av dennes uppgifter. Det ska vara otvetydigt att personen samtycker, så i ett dokument där personen också tar ställning till andra frågor ska samtycket tydligt framgå.



Samtycket ska vara informerat, vilket innebär att den registrerade – eller forskningspersonen – tydligt och på ett sätt som hen förstår ska ha fått information som anger vilka uppgifter som kommer att samlas in, hur de kommer att behandlas och lagras, samt för vilket ändamål.

Samtycket måste inte vara skriftligt, men eftersom den personuppgiftsansvarige ska kunna bevisa att den registrerade personen har lämnat samtycke måste samtycket på något sätt ha dokumenterats.

En registrerad har när som helst rätt att återkalla sitt samtycke, och att få sina uppgifter raderade. Detta gäller inte i de fall där det finns ett tyngre vägande rättsligt skäl eller viktigt allmänt intresse att inte radera dem.

Personuppgifter i forskning

I grunden gäller samma regler för behandling av personuppgifter för forskning som i andra fall. Personuppgifter får även inom forskning behandlas med forskningspersonens informerade samtycke, eller för att behandlingen är nödvändig för något av de villkor som anges i lagen. Det villkor som är närmast till hands för forskning är det som tillåter att *personuppgifter får behandlas om det är nödvändigt för att en arbetsuppgift av allmänt intresse ska kunna utföras.*

Om det rör sig om behandling av känsliga personuppgifter är regelverket striktare och som jag tidigare nämnde är det generellt sett förbjudet att behandla sådana uppgifter. Det finns dock undantag. Ett sådant är om forskningspersonen har lämnat sitt *uttryckliga* samtycke till behandling av uppgifterna. Ett annat undantag är om behandlingen avser forskningsändamål och har prövats och godkänts av en etikprövningsnämnd.

En viktig del av skyddet för forskningspersoners integritet är att de får information om hur deras uppgifter kommer att användas och t.ex. om vad forskningen gäller, vilka metoder som används, att deltagandet är frivilligt och att forskningspersonen har rätt att när som helst avbryta sin medverkan och dra tillbaka sitt samtycke. Om det görs en etikprövning så kan etikprövningsnämnden ställa krav på vilken information som ska lämnas till forskningspersoner, och det finns bra faktablad kring forskningspersonsinformation via Datainspektionen och etikprövningsnämndernas webbplatser.

Stöd till forskare

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. Här är det givetvis bra om det finns tillgänglig juristkompetens, som kan vara behjälplig vid frågor och funderingar.

Vi ska nu avsluta med den här presentationen med att kika på hur du kan gå tillväga för att hjälpa forskare att resonera avseende hantering av personuppgifter. Forskargruppen behöver hjälp med att reda ut om deras forskningsprojekt innefattar personuppgifter, och hur de i sådana fall ska hantera dessa på bästa sätt.

Det första är att identifiera vilket regelverk som ska användas. Då vet du att det från och med 25 maj 2018 är Dataskyddsförordningen som reglerar hantering av personuppgifter. För att svara på om forskningsprojektet hanterar personuppgifter behöver du ta reda på vilka uppgifter som finns i datamaterialet och ta ställning till om de utgör personuppgifter. Här kan du behöva läsa lagtext, även om du säkert minns att definitionen på personuppgifter är "All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet". Om vi fastställer att det handlar om personuppgifter behöver vi sedan bestämma oss för om det handlar om *behandling* av personuppgifter i ett forskningsprojekt. Du kommer kanske ihåg att alla typer av hantering av personuppgifter räknas som behandling. Därefter behöver vi ta ställning till om de grundläggande principerna för behandling av personuppgifter är uppfyllda, dvs. får forskargruppen överhuvudtaget behandla personuppgifterna? De grundläggande principerna innebär t.ex. att uppgifterna bara får samlas in för särskilda, uttryckligt angivna och berättigade ändamål, att de är riktiga och aktuella, och att de förvaras på ett säkert sätt. Nästa steg är att svara på om den tilltänkta behandlingen är tillåten. Har forskningspersonen lämnat samtycke till behandlingen, eller är behandlingen att betrakta som nödvändig utifrån det som framgår i regelverket?

Nästa fråga blir att fundera på om det i den här personuppgiftsbehandlingen finns några särskilda uppgifter som kräver ytterligare restriktioner. Innehåller forskningsprojektet känsliga personuppgifter, personnummer, eller finns där uppgifter om lagöverträdelse, dvs. forskar man på lagöverträdelse? Regelverket reglerar hur var och en av dessa får behandlas. Det finns också andra aspekter som är relevanta att ta reda på, t.ex. huruvida behandlingen innebär några tredje landsöverföringar och hur personuppgifterna behandlas utifrån informationssäkerhet. Jag kommer inte att gå in djupare på dessa delar nu. Informationsklassning och säkerhet finns att ta del av i pass 2, presentationen Säkerhet och personuppgifter.

Sammanfattning

Du har nu fått en introduktion till personlig integritet och fått ta del av hur regelverket är tänkt att skydda människorna mot att den personliga integriteten kränks genom behandling av personuppgifter. Integritetskränkning handlar om att förlora kontrollen över sin egen person eller en viss typ av uppgifter om sig själv. Från och med den 25 maj 2018 är det Data-skyddsförordningen som reglerar hur personuppgifter får behandlas. Det informerade samtycket är centralt för behandling av personuppgifter och i forskningssammanhang är information till forskningsdeltagaren en väldigt viktig del.

Det här var den sista presentationen i BAS Online. Jag hoppas att du tycker att det har varit givande och att du har fått med dig lite nya kunskaper. Nu tackar vi för oss. Har du några frågor som gäller sådant som inte togs upp i kursen, eller stötte du på något som du funderar över är du välkommen att höra av dig till oss på SND.

Hej då!