UMEÅ UNIVERSITET

Informations- och utbildningsmaterial angående dataskyddsförordningen

FÖRFATTARE TILL ORIGINALMANUSET:

Åsa Dryselius, Högskolan i Borås Benita Falenius, Stockholms universitet Inger Helldal, Högskolan i Gävle

Sten Leander, Södertörns högskola

Erik Stavegren, Sveriges lantbruksuniversitet Erika Tegström, Mittuniversitetet

Jesper Wokander, Malmö universitet

REDIGERING OCH STRUKTUR:

Jesper Wokander, Malmö universitet

FÖRFATTARE TILL OMARBETAT MANUS SOM LIGGER TILL GRUND FÖR DENNA VERSION:

Erika Tegström, Mittuniversitetet

Förord

Med utgångspunkt i det gemensamma behovet av ett underlag för utbildning av lärosätenas personal, studenter och forskare för den kommande dataskyddsförordningen har följande grundmaterial arbetats fram genom ett samarbete mellan några högskolor. Materialet består av moduler som kan kombineras beroende på behovet hos den enskilde och är avsett att beskriva de generella grunderna i lagstiftningen. Det är tänkt att ge läsaren en grundkunskap kring förordningen och förhoppningsvis göra att vad som gäller för det dagliga arbetet blir tydligt. Tanken är också att man ska veta när det är dags att söka ytterligare kunskap och var denna finns att hämta.

Tanken är att läsaren börjar med att läsa en gemensam introduktion till den nya lagstiftningen som ger en allmän översikt och därefter följer olika moduler beroende på behov. Alla har nytta av att enkelt kunna ta del av varje block och därför är det paketerat tillsammans och inte i helt egna moduler. Materialet är inte avsett att täcka behovet för de grupper som behöver en djupare kunskap inom ämnet, exempelvis dataskyddsombud, arkivarier, jurister med flera. Dessa grupper hänvisas till de aktuella lagtexterna.

1.0 Introduktion

Bakgrund

Från och med den 25 maj 2018 ersätter dataskyddsförordningen det drygt 20 år gamla dataskyddsdirektivet. Den tekniska utvecklingen har under dessa år gått mycket snabbt, särskilt inom insamling och behandling av personuppgifter. Företag som Google och Facebook har vuxit sig till några av världens största och mest lönsamma företag med försäljning av personuppgifter som huvudsaklig inkomstkälla. Det skydd som den enskilde fick genom det tidigare dataskyddsdirektivet, i Sverige genomfört i personuppgiftslagen (PUL), har visat sig otillräckligt. EU har därför antagit den nya dataskyddsförordningen vars syfte är dels att stärka skyddet för den personliga integriteten och dels att skapa ett enhetligt regelverk för hela EU. Den som behandlar personuppgifter för personer inom unionen ska, oavsett om behandlingen sker inom eller utanför Europa, respektera människors grundläggande fri- och rättigheter och särskilt deras rätt till skydd av personuppgifter. Vad detta innebär i praktiken för vårt lärosäte och oss som anställda är vad denna text ska försöka förmedla. Förordningen gäller all hantering av personuppgifter och det är därför viktigt att vi har förståelse för de regler som styr. Detta oavsett om vi ansvarar för en behandling eller om det enbart är som en del av det dagliga arbetet som hantering av personuppgifter sker.

Termen *den registrerade* används genomgående och betyder en identifierad eller identifierbar fysisk person vars information på något sätt används i vårt arbete. Skillnaden mellan dessa är att den förstnämnda syns i klartext, t.ex. i Ladok eller Primula, medan den andra sortens personuppgifter behöver exempelvis en krypteringsnyckel för att personen ska kunna bli identifierad.

Insamling och bearbetning av personuppgifter

Varje uppgift som direkt eller indirekt kan kopplas till en levande person är en personuppgift. Detta innebär att det inte bara är sådant som namn och personnummer som kan vara personuppgifter utan även användarnamn, adresser, telefonnummer, e-post- eller IP-adresser, biometriska data, fysiologiska uppgifter och även exempelvis en röstinspelning. Även kombinationer av uppgifter omfattas så länge det genom uppgifterna är möjligt att koppla dessa till en fysisk person. För all *behandling* av personuppgifter (samla in, lagra, bearbeta mm.) gäller att behandlingen måste följa dataskyddsförordningens samtliga principer för behandling. Det innebär bl.a. att:

- behandlingen ska ske på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade,
- uppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål,
- uppgifterna får inte vara för omfattande i förhållande till syftet de samlas in för och
- uppgifterna ska vara korrekta och uppdaterade,
- uppgifterna inte får förvaras i form av identifierbara personuppgifter längre än vad som krävs för behandlingen och

- uppgifterna ska behandlas på ett säkert sätt.

De första tre punkterna, att behandlingen ska vara laglig och att uppgifterna ska vara korrekta och behandlas säkert kan närmast sägas vara självklara men de tre följande medför begränsningar i förhållande till hur vi ofta tidigare har behandlat personuppgifter. Tidigare har vi gärna samlat in vad vi har kunnat med tanke på att vi kanske skulle komma att behöva uppgifterna någon gång i framtiden, även om redan det var tveksamt utifrån dataskyddsdirektivet. Enligt förordningen måste vi redan när vi samlar in uppgifter veta vad vi ska ha dem till. Detta för att vi inte ska samla in mer än nödvändigt, bara samla till berättigade ändamål och för att vi också måste veta hur länge vi ska använda uppgifterna (även om vi inte nödvändigtvis måste kunna ange ett exakt slutdatum).

Laglig grund

Förutom att behandlingen måste uppfylla principerna måste det också finnas *laglig grund* för behandlingen. Det finns sex stycken lagliga grunder och det räcker med att en av dem är uppfylld för att behandlingen ska vara tillåten. Det är givetvis även möjligt med en kombination av grunder.

- Samtycke – den registrerade har lämnat sitt informerade samtycke till behandlingen. Samtycket ska av bevisskäl dokumenteras och kan när som helst återkallas.
- Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är delaktig i (t.ex. anställningsavtal).
- Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse (t.ex. lagar och myndighetsföreskrifter men även kollektivavtal omfattas).
- Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade (t.ex. hälsa och sjukvård).
- Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse (t.ex. forskning) eller som ett led i den personuppgiftsansvariges myndighetsutövning.
- Behandlingen är nödvändig för tredje parts berättigade intressen (denna grund kan inte användas av myndigheter).

Vid Umeå universitet är en stor del av vår verksamhet myndighetsutövning. Här ryms exempelvis allt som normalt hör till utbildning och examination. Myndighetsutövning används i förordningen i en vidare tolkning än vad vi normalt brukar använda begreppet till i Sverige och omfattar det vi gör inom vårt uppdrag som myndighet.

Vidare anses forskning vara av allmänt intresse och grunden för detta finns i högskolelagen. De arbeten som våra studenter producerar når sannolikt inte upp till allmänt intresse och behöver företrädesvis baseras på samtycke om personuppgifter används. Se mer om studenternas behandling av personuppgifter under **2.3 Utbildning**. Övriga grunder kan bli aktuella beroende på omständigheterna och vid osäkerhet bör du kontakta dataskyddsombudet.

Behandling av särskilda kategorier av personuppgifter (känsliga personuppgifter)

Särskilda kategorier av personuppgifter är enligt dataskyddsförordningen uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Grundregeln är att behandling av sådana uppgifter är förbjuden.

Det finns ett antal undantag från denna regel, där de som främst är användbara för verksamheten är:

- den registrerade samtycker till behandlingen
- om det krävs för att uppfylla ett viktigt allmänt intresse,
- om behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk,
- eller i de fall som anges i 3 kap. 3 § i förslaget till dataskyddslagen. Förslaget är att särskilda kategorier av personuppgifter (känsliga personuppgifter) får med stöd av artikel 9.2 g i dataskyddsförordningen behandlas av en myndighet

    1. om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag,
    2. om behandlingen är nödvändig för handläggningen av ett ärende, eller
    3. i enstaka fall, om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

Informationsplikt

När vi samlar in personuppgifter har vi en skyldighet att lämna information till den registrerade som bl.a. ska innehålla:

- identitet och kontaktuppgifter för den personuppgiftsansvarige (mer om personuppgiftsansvarig nedan),
- kontaktuppgifter för dataskyddsombudet (mer om dataskyddsombud nedan),
- ändamålet med/anledningen till behandlingen samt stödet för denna,
- vem/vilka som kommer att ta del av uppgifterna samt
- eventuell överföring till länder utanför EU och information om skyddsnivån hos mottagaren.

Det finns checklistor för vad denna information ska innehålla som bilaga till detta dokument.

Informationsplikten gäller även när vi samlar in uppgifterna från andra källor än direkt från den registrerade. Det finns dock vissa utrymmen för undantag. Om den registrerade sedan tidigare är informerad, om det är praktiskt omöjligt/mycket svårt att informera eller om behandlingen är en skyldighet på grund av lagstiftning behöver ingen information ges. Ett exempel är när en student begär ett datorkonto hämtar vi normalt uppgifter från Ladok. Vi är då skyldiga att informera studenten om att detta sker och vilka uppgifter det rör sig om i samband med att kontot begärs. Däremot behöver vi inte särskilt informera om att en students studieresultat skrivs in i Ladok eftersom det står i förordningen (1993:1153) om studieregistrering att detta ska göras.

Uppgifterna ska behandlas på ett korrekt och öppet sätt i förhållande till den registrerade. Om den registrerade har frågor eller vill använda sig av sina rättigheter i förhållande till behandlingen som vi utför är det vår skyldighet att hjälpa till. Detta gäller så länge som det inte finns hinder mot detta på grund av exempelvis sekretess- eller arkiveringsregler.

Den registrerades rättigheter och begränsningar av dessa

Genom dataskyddsförordningen har den registrerade en rad rättigheter som är till för att stärka skyddet för den personliga integriteten, vilket är viktigt att tänka på. Grundtanken är att den registrerade ska kunna förutse vad som kommer hända med den aktuella informationen.

Detta gäller som tidigare nämnts rätt att få utförlig information om vad uppgifterna ska användas till och rätt att få tillgång till de uppgifter som finns registrerade om den egna personen. Den registrerade har också rätt att få felaktig information korrigerad utan onödigt dröjsmål samt rätt att få personlig information raderad, där så är juridiskt och praktiskt möjligt. Vidare har den registrerade också rätt att invända mot behandlingen, att återkalla eventuella samtycken och rätt att klaga till tillsynsmyndigheten om den registrerade anser att behandlingen är felaktig.

Rätten att radera uppgifter eller begränsa en behandling är inte en absolut rättighet och det kan finnas anledning att inte tillmötesgå en sådan begäran. Det kan finnas en annan grund som säger att vi ska behålla uppgifterna, exempelvis att vi i enlighet med arkivbestämmelserna, olika regler kring ekonomi eller arbetsrätt är skyldiga att bevara materialet. Exempelvis kan en anställd visserligen begära att få sina uppgifter raderade från lönespecifikationen vi lämnar till Skatteverket men vi kommer inte att genomföra det eftersom vi har en rättslig förpliktelse att lämna dessa uppgifter. Vid oklarheter kring vad som ska raderas och vad som ska bevaras bör i första hand arkivarie kontaktas. Generellt kan sägas att behandlingen av personuppgifter ska vara öppen och tydlig gentemot den registrerade och om det är möjligt bör vi tillmötesgå den registrerades önskemål.

Roller och ansvar

För all personuppgiftshantering, från den enskilda studentens uppsatsarbete till forskningsprojekt och administrativa system, finns det en *personuppgiftsansvarig* och för den verksamhet som bedrivs inom lärosätet är detta Umeå universitet. Det är Umeå universitet som har det yttersta ansvaret för all behandling av personuppgifter som sker inom ramen för verksamheten. Som enskild medarbetare ska du hantera personuppgifter på ett korrekt sätt och ha kunskap om de regler som gäller för just dina arbetsuppgifter.

Vid framförallt vissa forskningssamarbeten kan personuppgiftsansvaret vara delat. Då är det viktigt att detta är tydligt reglerat mellan parterna och att det ändå finns en part som har huvudansvaret för exempelvis lagringen. Vid vissa tillfällen sker behandlingen av personuppgifterna av en tredje part och denne agerar då som *personuppgiftsbiträde*. Förhållandet mellan biträde och ansvarig ska regleras genom ett skriftligt avtal och biträdet får inte på egen hand behandla den information som kommer från lärosätet.

Datainspektionen är *tillsynsmyndighet* för dataskyddsförordningen och har därmed ansvar för att granska vår hantering av personuppgifter och hantera klagomål från registrerade. Vid lärosätet finns också ett dataskyddsombud som internt ska granska hanteringen men även fungera som hjälp och stöd för verksamheten. Dataskyddsombudet ska också vara tillgängligt för att kunna hantera frågor och klagomål från registrerade och kan nås via kontaktuppgifter på hemsidan.

Vid fel och brister i hanteringen kan både personuppgiftsansvarig och personuppgiftsbiträdet drabbas av sanktionsavgifter (böter). Det är tillsynsmyndigheten som ansöker om detta och det döms ut av domstol. Sanktionsavgifterna ska vara effektiva, proportionella samt avskräckande och kan bli mycket höga.

Register

Lärosätet har även en skyldighet att genom ett register hålla ordning på vilka personuppgiftsbehandlingar som pågår inom verksamheten. Detta register ska bl.a. innehålla ändamålet med personuppgiftsbehandlingen, en beskrivning av registrerade och vad som registreras och vem eller vilka som kommer att ta del av uppgifterna som behandlingen omfattar. Mer detaljer om registret finns under avsnittet om **Registrering av personuppgiftsbehandlingar** under **3.0 Gemensam**.

Säkerhet

De insamlade uppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna med användning av lämpliga tekniska eller organisatoriska åtgärder. Detta omfattar skydd mot obehörig eller otillåten behandling och skydd mot förlust, förstöring eller skada genom olyckshändelse. Detta innebär att vi måste se till att endast behöriga personer har tillgång till uppgifterna och att eventuella databaser eller system omfattas av olika säkerhetsåtgärder. Att besluta om, införa och övervaka lämpliga säkerhetsåtgärder såväl tekniska som administrativa är ett krav i dataskyddsförordningen och detta ska även dokumenteras. Mer under avsnittet **Säkerhet i arbetet** i **3.0 Gemensam.**

Andra lagar som också styr behandlingen av personuppgifter

Dataskyddsförordningen styr inte ensamt hanteringen av personuppgifter utan kompletteras dels genom vissa lagar som redan gäller och dels genom ny lagstiftning som träder ikraft samtidigt som förordningen.

Sedan tidigare är vi vana vid att tryckfrihetsförordningen tillsammans med exempelvis offentlighets- och sekretesslagen styr allmänhetens tillgång till allmänna handlingar. Regelverket för arkiv med bl.a. arkivlagen reglerar i sin tur vilka av dessa handlingar som ska bevaras och vilka som kan raderas (gallras). Det är särskilt viktigt att uppmärksamma arkivlagen och tryckfrihetsförordningen när det gäller rätten att få sina uppgifter rättade eller raderade. Detta eftersom det kan finnas bestämmelser i dessa som innebär att uppgifter inte får vare sig ändras eller raderas.

I vår undervisande och forskande verksamhet är den lagliga grunden för vår personuppgiftsbehandling i många fall krav som ställs på oss i högskolelagen, i högskoleförordningen eller i andra lagar som rör verksamheten på universitet och högskolor. I egenskap av exempelvis arbetsgivare har vi en långtgående skyldighet via lagar och kollektivavtal att behandla personuppgifter som rör våra anställda. Det finns även regler kring personuppgifter i andra delar av vår lagstiftning. Det viktiga är dock att ta reda på att våra behandlingar är korrekta och varför.

Utöver de lagar och förordningar som redan finns kommer ytterligare lagar att träda ikraft samtidigt med förordningen. Dataskyddslagen kompletterar förordningen med vissa nationella bestämmelser på ett mer övergripande plan men möjliggör även exempelvis forskning genom att tillåta behandling för allmänt intresse. Även lagen om etikprövning när det gäller hanteringen av känsliga personuppgifter för forskningsändamål håller på att ses över. Dataskyddsförordningen kräver även en mängd följdändringar i annan lagstiftning vilket gör att det under våren 2018 pågår ett intensivt lagstiftningsarbete.

Sammanfattning

Det är viktigt att vara medveten om bakgrunden till de arbetsuppgifter man har men för den som arbetar med personuppgifter i en etablerad behandling är det viktigast att hålla sig informera kring de regler och instruktioner som gäller och vid osäkerhet kontakta den som är ansvarig för behandlingen, systemägaren, forsknings- eller utbildningsansvarige etc. Dataskyddsförordningen innebär en del förändringar och en del nya regler, men generellt kan sägas att de krav vi haft på oss sedan tidigare att bevara information, men även att gallra information, gäller även framöver. För den som tänker skapa en behandling av personuppgifter, exempelvis inom ramen för sin forskning är det dock nödvändigt att uppfylla de formella kraven för att behandlingen ska vara ok. Universitetets dataskyddsombud kan kontaktas för råd och stöd.

2.1 Forskning

”Vetenskapliga forskningsändamål”

Behandling av personuppgifter för vetenskapliga forskningsändamål ska enligt dataskyddsförordningen ges en vid tolkning och omfattar exempelvis teknisk utveckling och demonstration, grundforskning, tillämpad forskning och privatfinansierad forskning. Även studier som utförs av ett allmänt intresse inom folkhälsoområdet är exempel på vad som omfattas av förordningen.

Utgångsläge

Utgångspunkten i dataskyddsförordningen är att den enskilde personen äger sina egna personuppgifter och att andra endast får behandla uppgifterna om man har fått lov från den enskilde (samtycke) eller har annan laglig grund för behandling såsom uppgift av allmänt intresse, myndighetsutövning eller avtal. Innan behandling måste det därför säkerställas att det finns en rätt att hantera personuppgifterna. Sedan måste behandlingen ske i enlighet med gällande regler och instruktioner. Dessa två är helt beroende av varandra. Det är den som vill behandla personuppgifterna som ska försäkra sig om att det finns laglig grund samt att behandlingen sker i enlighet med gällande regler och instruktioner. Stort fokus ska läggas på att säkerställa att den registrerade är fullt informerad kring vilken behandling som sker och att hanteringen sker säkert.

Finns det en möjlighet att med rimliga medel nå sitt forskningsmål utan att använda personuppgifter ska personuppgifter inte användas. Detta innebär också att det regelverk som finns kring behandling av personuppgifter inte är tillämpligt och den praktiska hanteringen blir lättare (notera att beroende på forskningens art kan det finnas annan lagstiftning som måste följas).

Regelverk

Dataskyddsförordningen omfattar all hantering av personuppgifter men vissa delar ska kompletteras genom nationell lag. För den som forskar är det därför nödvändigt att ha kunskap om minst två ytterligare lagar; den dataskyddslagen och lagen om etikprövning. Syftet med dessa båda lagar är att möjliggöra personuppgifts- behandling för forskningsändamål samtidigt som den enskildes fri- och rättigheter skyddas.

Dataskyddslagen introduceras tillsammans med dataskyddsförordningen och kompletterar förordningen i olika avseenden, exempelvis genom att tillåta personuppgiftsbehandling för allmänt intresse (vilket forskning anses vara). Om den nationella rätten skulle anses krocka med dataskyddsförordningen går förordningen i princip alltid först.

Det är viktigt att komma ihåg att både dataskyddsförordningen och dataskyddslagen reglerar behandlingen av personuppgifter och att forskning som bedrivs utan användning av personuppgifter inte omfattas av dessa. Etikprövningslagen avser

huvudsakligen personuppgifter men omfattar även ingrepp på avlidna människor, vilket de båda förstnämnda inte gör.

Tillåtna grunder för forskning

Förutom att de grundläggande principerna om exempelvis laglighet, enbart samla in personuppgifter för berättigade ändamål och en säker hantering måste vara uppfyllda är det nödvändigt även för forskning att det finns en tillåten grund för behandlingen. För forskning är det särskilt två grunder som främst kan vara tillämpliga; behandling med samtycke och behandling nödvändig för att utföra uppgift av allmänt intresse.

Samtycke

För att samtycke ska vara tillämpligt måste det röra sig om en frivillig, specifik och otvetydig viljeyttring. Den registrerade ska genom denna, antingen genom ett uttalande eller genom en entydig bekräftande handling, godta behandling av personuppgifter som rör honom eller henne. Handlingen ska vara tydligt inriktad på personuppgiftsbehandlingen och inte blandas ihop med andra förklaringar och ställningstaganden för den enskilde. För ett giltigt samtycke krävs att det finns en tydlig beskrivning av vilka uppgifter som ska samlas in och för vilket ändamål dessa ska användas. Detta ska den enskilde sedan ta ställning till. Det är den som tänker behandla personuppgifterna som ansvarar för att formulera ändamålsbeskrivningen.

Samtycke ska dokumenteras och sparas för att kunna redovisas vid behov. För information om vad av och hur länge forskningsmaterial ska sparas, se Umeå universitets dokumenthanteringsplan. Det är viktigt att veta att ett samtycke när som helst kan återkallas av den registrerade utan något krav på motivering.

Återkallelse innebär att det då inte längre är tillåtet att göra nya behandlingar av den registrerades uppgifter med samtycke som grund. Redan genomförda behandlingar, ex. framtagna forskningsresultat får dock fortsätta att användas. Observera att en behandling som ursprungligen har skett med samtycke som rättslig grund med tiden kan ha bytt grund vilket gör att viss behandling ändå kan fortsätta, ex. ekonomisk redovisning av ett projekt. Vid oklarhet bör dataskyddsombudet konsulteras.

Eftersom samtycke måste vara frivilligt är det problematiskt om det finns någon form av beroendesituation mellan parterna som gör förhållandet ojämlikt. Ett exempel på ett sådant förhållande är om lärosätet vill forska med hjälp av personuppgifter som gäller studenter eller anställda på lärosätet. Om det kan misstänkas att samtycket inte är helt frivilligt måste en prövning göras från fall till fall. Vid de tillfällen man finner att det kan vara tveksamt om samtycket kan anses vara helt frivilligt är det inte möjligt att använda detta som laglig grund för behandling.

Dataskyddsförordningen öppnar dock upp för en bredare syn på samtycke i samband med forskning än vad som hittills tillämpats. I skälen till dataskyddsförordningen anges att det ofta inte är möjligt att fullt ut identifiera syftet med en behandling av personuppgifter för vetenskapliga forskningsändamål i samband med insamlingen av uppgifter. En registrerad bör därför kunna ge sitt samtycke till vissa områden för vetenskaplig

forskning, när vedertagna etiska standarder för vetenskaplig forskning iakttas. En förutsättning är att detta kan ske utan att det görs avkall på kraven att specificera ändamålen och att ett förnyat samtycke är nödvändigt om det rör sig om andra ändamål. I praktiken kan sannolikt forskning bedrivas på tidigare insamlat material förutsatt att den nya forskningen ligger i linje med det syfte för vilket materialet tidigare har samlats in. Detta är som sagt nytt och hur långt detta sträcker sig kommer att bli tydligare över tid.

För *samtycke* gäller att:

- det måste vara en klar och tydlig viljeyttring från den registrerade,
- det får inte vara ett ojämlikt förhållande mellan den som ger sitt samtycke och den som samlar in det för behandling av personuppgifter,
- det kan tas tillbaka när som helst och då får inte ny behandling ske,
- uttryckligt samtycke är giltig grund för att behandla känsliga personuppgifter, och
- det är inte självklart att ytterligare behandling för forskningsändamål utan en ny laglig grund är tillåtet.

Relationen mellan den registrerade och den personuppgiftsansvarige får alltså inte vara ojämn. Det är t.ex. tveksamt om ett samtycke kan vara helt frivilligt om den registrerade är beroende av den personuppgiftsansvarige för nödvändig vård och kan tro att samtycke till en forskningsstudie är nödvändig för att få denna. Det är alltså väldigt viktigt hur information om ex. en studie ges och att det är tydligt att det inte finns några negativa aspekter i att avstå från att delta, vare sig konkreta eller implicita.

Allmänt intresse

Personuppgifter får med stöd av allmänt intresse behandlas för forskningsändamål om behandlingen är nödvändig och proportionerlig för att utföra forskning av allmänt intresse. Om det är möjligt att uppfylla forskningens syfte utan att personuppgifter används samtidigt som detta inte leder till att arbetet därigenom blir onödigt komplext eller dyrt ska sådana inte användas. Om det däremot visar sig svårt att nå resultat utan personuppgifter är användningen normalt sett tillåten.

Vid behandling av personuppgifter för forskningsändamål bör en nödvändighets- bedömning göras; behandlingen måste bedömas vara nödvändig för att forskningen ska få utföras. Det behöver också göras en rimlighetsbedömning av vilka alternativa sätt att utföra forskningsuppgiften som är möjliga. I bedömningen ingår också möjligheten att användandet av personuppgifter kan ge högre kvalitet och tillförlitlighet i forskningsmaterialet. Ett bättre resultat kan därför vara en tillåten grund för att använda personuppgifter även om det hade varit möjligt att nå ett resultat utan.

Den registrerades rättigheter och begränsningar av dessa inom forskning

Den registrerade har genom dataskyddsförordningen bland annat rätt att få information om behandlingen, rätt att ta del av vilka uppgifter som behandlas och få

utdrag av uppgifterna kring den egna personen, rätt att få felaktig information rättad och rätt att få personlig information raderad om det inte finns laglig grund för att behålla den.

Vid frågor kring den registrerades rättigheter, kontakta dataskyddsombudet.

Etikprövning

Utgångspunkten för känsliga personuppgifter är att de är förbjudna att använda. Detta gäller uppgifter om ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska och biometriska uppgifter samt uppgifter om en persons hälsa, sexualliv eller sexuella läggning. Under vissa förutsättningar är det ändå tillåtet att använda dessa uppgifter vilket för forskningens del primärt förutsätter en godkänd etikprövningsansökan. Om du hanterar data inom dessa kategorier men har samlat in data helt anonymt är inte etikprövning nödvändigt.

I Sverige har vi haft denna form av etisk prövning under lång tid. Den egentligen viktigaste skillnaden som dataskyddsförordningen medför gentemot tidigare är att det är något fler kategorier av personuppgifter som kräver en etikprövning. Hittills har studentarbeten varit undantagna etisk prövning men nu finns det ett förslag på att ändra detta. Detta förslag innebär dock inte en förändring i synen på vad som är forskning utan enbart förutsättningarna för etisk prövning.

Förutom vid forskning på känsliga personuppgifter krävs det en godkänd etikansökan för att få forska på material som innehåller personuppgifter om lagöverträdelser. Andra situationer som kräver godkänd etikprövning är forskning på t.ex. material från en avliden människa, om det man vill göra har en klar risk att en person kommer till skada fysiskt och/eller psykiskt mm. Se 4 § etikprövningslagen för mer detaljer kring dessa situationer.

Om forskningen sker med stöd av samtycke måste detta enligt såväl dataskyddsförordningen som enligt etikprövningslagen vara uttryckligt. Detta innebär att det är ett högre krav än för samtycke rent generellt för behandling av personuppgifter.

För frågor angående etikprövning, kontakta den regionala etikprövningsnämnden i Umeå, www.cepn.se.

2.2 Administration

Inom lärosätets administrativa system pågår en rad olika behandlingar av personuppgifter som alla omfattas av dataskyddsförordningens regler. All behandling måste ha ett tydligt syfte, den registrerade har rätt till information om vad som sker, vilka uppgifter som behandlas och har ett antal rättigheter som skydd för de personliga fri- och rättigheterna. Det är heller inte tillåtet att samla in mer uppgifter eller behålla uppgifter längre än vad som är nödvändigt för att sköta vårt jobb. Hur länge detta kan vara varierar stort beroende på vilken typ av uppgift som är aktuell och anledningen till att den används.

Tillåtna grunder

Varje behandling måste ha en rättslig grund. För behandling inom förvaltningen gäller främst att behandlingen är nödvändig för att fullgöra en rättslig förpliktelse via lagstiftningen eller att behandlingen är en del av vår myndighetsutövning. Dessa båda grunder täcker tillsammans huvuddelen av lärosätets administrativa funktioner och innebär därför inte några större direkta förändringar i det praktiska arbetet inom administrationen.

- Ekonomiska händelser styrs av exempelvis årsredovisnings- och bokföringslagen.
- Personaladministrationen på universitetet måste följa bl.a. lagen om anställningsskydd, arbetsmiljö- och diskrimineringslagen samt kollektivavtal.
- Universitetets hantering av studenters personuppgifter regleras till stor del av högskolelagen och högskoleförordningen samt förordningen om studieregistrering
- I vår myndighetsutövning är vi styrda av bl.a. tryckfrihetsförordningen, förvaltningslagen, offentlighets- och sekretesslagen samt arkivlagstiftningen.

Typer av personuppgifter och deras behandling

De typer av personuppgifter som samlas in i administrativa sammanhang är huvudsakligen namn, kontaktuppgifter, personnummer samt skatte- och bankuppgifter. De första tre uppgifterna är till för att kunna säkerställa en riktig identifiering av den anställde samt de två sistnämnda naturligtvis för att kunna betala ut lön och ersättning med korrekt skattesats. Viktigt att komma ihåg om personnummer är att det är en uppgift som ska hanteras med försiktighet och bara om det är nödvändigt för att unikt identifiera en person, vilket normalt är fallet i våra administrativa system. Är det tveksamt om personnummer egentligen behövs, kontakta dataskyddsombudet för en diskussion.

I vissa system, exempelvis det personaladministrativa systemet, finns det möjlighet att lägga in egna, frivilliga personuppgifter. Detta kan exempelvis gälla uppgifter om närmaste anhöriga vilket givetvis underlättar för arbetsgivaren om något skulle hända men är högst frivilligt att fylla i. Detsamma gäller foton på medarbetare, vilket också frivilligt att lägga upp.

Även sjukuppgifter angående de anställda behandlas av universitetet med stöd av bl.a. lagen om sjuklön. Detta för att den anställde dels ska kunna få rätt ersättning och dels för att arbetsgivaren ska kunna fullfölja sitt rehabiliteringsansvar. Dessa uppgifter gallras sedan med stöd av Riksarkivets föreskrifter: RA-FS 2012:9.

Andra typer av handlingar där personuppgifter behandlas inom administrationen kan vara ansökningshandlingar, anställningsavtal, information om avslutande av tjänst, olika former av beslut, löneuppgifter, kontrolluppgifter, kvitton samt försäkran vid sjukdom. För en fullständig uppräkning av olika handlingstyper, se Umeå universitets dokumenthanteringsplan.

Sammanfattning

Sammantaget för den som arbetar vid Umeå univeristet kan sägas att detaljer kring vilken rättslig grund en behandling stödjer sig på, formulering av ändamålet eller registreringen av behandlingen m.m. ofta inte är något som den enskilde medarbetaren behöver ta ställning till. Ändamålet, registreringen och den rättsliga grunden gäller för hela behandlingen och då för varje enskilt fall inom tillämpningen. Arbetet med exempelvis Ladok är därför en behandling som har som syfte att registrera studieresultat, det finns i registret och har sin grund i en rättslig förpliktelse. Detta gäller för alla som för in resultat utan att den enskilde medarbetaren behöver redovisa detta löpande. Som enskild medarbetare ska du däremot hantera personuppgifter på ett korrekt sätt och sätta dig in i de regler som gäller för just dina arbetsuppgifter. Är du osäker på vad som krävs av dig i detta avseende, prata med din närmaste chef.

2.3 Utbildning

Personuppgifter i utbildningen

För att kunna bedriva utbildning måste vi också hantera personuppgifter. Det är nödvändigt för oss att veta vilka vi undervisar och att kunna registrera och redovisa de framsteg som våra studenter gör inom sina respektive utbildningar. Samtidigt omfattas även dessa behandlingar av kraven i dataskyddsförordningen och det är nödvändigt för oss att uppfylla förordningens regler och principer samt att ha en tillåten grund för behandlingen.

Tillåtna grunder inom utbildning

Vad gäller de rättsliga grunderna är utgångspunkten att det flesta fall av behandling inom utbildningsområdet utförs med grunden ”uppgift av allmänt intresse”, ”del i myndighetsutövning” eller ”rättslig förpliktelse”. För mer detaljer kring grunder, se avsnittet om **Lagliga grunder** under **1.0 Introduktion**.

Grunden ”samtycke” kan normalt sett inte användas i de fall där den registrerade står i en beroendeställning till den personuppgiftsansvarige. I egenskap av utbildningsanordnare har vi ett klart övertag mot våra studenter och därför kan behandling av studenters personuppgifter endast i undantagsfall baseras på samtycke. Att utbildningen utgår från ett frivilligt deltagande påverkar inte detta. Samtycke kan endast användas som grund om inga negativa konsekvenser inträffar som ett resultat av att samtycket inte lämnas. Dessa konsekvenser behöver inte vara formella, utan kan vara av

karaktären ”Det är frivilligt… men alla gör det…” och alltså syfta på sociala förhållanden. Det finns dock andra grunder som är tillåtna för arbetet inom lärosätets utbildningar.

- *Allmänna intressen*

Ett allmänt intresse fungerar som en rättslig grund för personuppgifts- behandling. Enligt svensk myndighetstradition anses oftast att allt ett lärosäte gör är av allmänt intresse. Enligt dataskyddslagstiftningen bör dock detta allmänna intresse vara utskrivet i svensk rätt för att få användas som grund för användning av personuppgifter. Detta kan ske antingen genom lag, förordning, myndighetsföreskrifter eller kollektivavtal etc. Det måste dessutom vara nödvändigt att behandla personuppgifter för att uppnå detta allmänna intresse för att det ska få användas som grund för behandlingen.

- *Led i myndighetsutövning*

Inledningsvis ska sägas att detta myndighetsutövningsbegrepp inte är detsamma som det som har använts i förvaltningslagen, utan det är det EU- rättsliga begreppet myndighetsutövning som används. Det innebär en vidgning av vad som ryms i begreppet mot tidigare. Om en åtgärd inom ramen för myndighetsutövningen hos ett lärosäte kräver personuppgiftsbehandling kan detta läggas som grund för behandlingen.

Exempel på detta är så gott som all verksamhet som en högskola ska utföra enligt högskoleförordningen. Viktigt att tänka på är dock att personuppgiftsbehandlingen måste ha ett tydligt samband med den uppgift som är en del av myndighetsutövningen. Går uppgiften att utföra utan att personuppgifter används ska vi göra på det sättet.

- *Rättslig förpliktelse*

För att en rättslig förpliktelse ska kunna läggas till grund för en person-uppgiftsbehandling krävs att denna är fastställd i svensk rätt, inklusive genom regerings- eller myndighetsbeslut eller genom kollektivavtal.

Skillnaden gentemot de två grunderna som behandlas ovan är att den rättsliga förpliktelsen måste vara så pass tydlig att den enskilde kan förstå vilken typ av behandling som kommer utföras med stöd av den rättsliga förpliktelsen. Typexempel på denna typ av förpliktelse är förordningen (1993:1153) om redovisning av studier m.m. vid universitet och högskolor, även känd som ”Ladokförordningen”.

Studenters personuppgiftsbehandling

Umeå universitetet är inte bara ansvarigt för de behandlingar av personuppgifter som utförs inom administration och forskning utan också för studenternas egna behandlingar så länge som dessa är en del av utbildningen. Detta innebär att om en student använder personuppgifter för sina studier gäller samma regler som för lärosätets övriga behandlingar. Det måste alltså finnas en grund för behandlingen, principerna måste följas (hanteringen ska vara laglig, öppen, korrekt, ändamålsenlig och uppgiftsminimerad), de registrerade måste informeras och behandlingen ska registreras via handledaren/ansvarig lärare. Mer information om detta i avsnittet **Registrering av personuppgiftsbehandlingar** i **3.0 Gemensam**.

Att studenter upprättar en personuppgiftsbehandling inom ramen för sin utbildning är något som kan ske exempelvis då de skriver examensarbeten. Det är dock inte begränsat till just examensarbeten utan alla uppsatser, redovisningar etc. som sker inom ramen för utbildningen omfattas, om studenten använder personuppgifter. Det är därför viktigt att kursansvariga lärare och de som fungerar som handledare är väl medvetna om att reglerna för behandling av personuppgifter också gäller för våra studenter och kan stödja dem i detta.

Grund för behandling vid studentarbeten

Om studenters arbeten ska innehålla personuppgifter kan det vara svårt att finna en grund för behandlingen utöver samtycke. Detta gör det extra viktigt att man förstår vikten av att lämna korrekt information till de registrerade samt att dokumentera och spara samtyckena på något sätt. Det kan vara lämpligt att fundera på om det är nödvändigt att arbetet verkligen innehåller personuppgifter eller om det skulle kunna lösas med anonyma uppgifter som inte omfattas av lagstiftningens krav på ex. laglig grund, information och säkerhet. Viktigt här är att komma ihåg att detta inte bara gäller det färdiga studentarbetet utan även vägen dit. Om det färdiga arbetet inte innehåller personuppgifter men sådana har använts under exempelvis skriv- eller utvecklingsprocessen så gäller de vanliga principerna som togs upp under

1.0 Introduktion.

Det är också viktigt att komma ihåg att pseudonymiserade uppgifter räknas som personuppgifter. Det krävs alltså att det inte finns någon möjlighet att återskapa en koppling mellan uppgifterna och den fysiska personen för att de ska räknas som anonyma och därmed undantagna från dataskyddslagstiftningen.

Vad en student får samla in med samtycke som grund för behandlingen är inte i sig begränsat men uppgifterna får inte vara mer omfattande än nödvändigt och de ska samlas in för ett specifikt och uttryckligt angivet ändamål. Insamling, hantering och lagring måste ske på ett säkert sätt som motsvarar känsligheten hos uppgifterna och precis på samma sätt som för övriga behandlingar ska det göras en konsekvens- bedömning om det är sannolikt att behandlingen kan leda till hög risk för de registrerades fri- och rättigheter. Vid frågor kring när det behövs en sådan, och för hjälp med själva bedömningen, kontakta dataskyddsombudet.

3.0 Gemensam

Registrering av personuppgiftsbehandlingar

Umeå universitet är personuppgiftsansvarig för alla behandlingar inom vår verksamhet, allt ifrån den enskilde studentens projektredovisning till de stora administrativa systemen och forskningsprojekt som kräver etikprövning. För att ha kontroll över vilka behandlingar som pågår och kunna redovisa dessa för tillsynsmyndigheten finns ett register där våra behandlingar av personuppgifter ska föras in. Umeå universitetet använder sig av det digitala verktyget DraftIT för att upprätta detta register.

Den som är ansvarig för en behandling är den som är skyldig att lägga in information om behandlingen i DraftIT men det är bra att känna till även för dem som arbetar inom en befintlig behandling. Det ska läggas in detaljer om bland annat följande:

- kontaktperson för behandlingen,
- ändamålet/syftet med behandlingen,
- en beskrivning av vilka typer av uppgifter som samlas in,
- vem eller vilka som kommer åt uppgifterna
- hur länge uppgifterna kommer att användas (om det är möjligt att ange)
- om möjligt en beskrivning av de tekniska och organisatoriska skyddsåtgärderna.

Alla behandlingar av personuppgifter som sker inom ramen för verksamhet ska registreras, från olika jättesystem ner till individuella forskningsprojekt (om personuppgifter behandlas inom projektet). Om du behöver registrera en behandling ska du maila till pulo@umu.se. Registreringen ska inte innehålla något av det material som behandlas utan bara uppgifter om behandlingen och vem/vilka som utför den.

För den som ansvarar för en behandling av personuppgifter är det nödvändigt att känna till de tillåtna grunderna, informationsplikten, principerna och kravet på att registrera behandlingen. Detta kan exempelvis vara systemägaren till ett av lärosätets system, huvudanvändaren av digitala tjänster eller den som upprättat en behandling inom ramen för sin forskning. För den som enbart arbetar i ett system som använder personuppgifter är det viktigt att ha kunskap om vad som gäller men det behöver inte vara på samma detaljnivå som för systemansvarig eller för systemägaren.

Säkerhet i arbetet

När det bedömts att det finns en laglig grund för behandling av de specifika personuppgifterna ska all behandling – i alla led – vara i enlighet med gällande regler och instruktioner. Det är den som initierar behandlingen som har att säkerställa att detta sker.

Dataskyddsförordningen ställer mycket stora krav på att den som behandlar personuppgifter dokumenterar hur det ska ske på ett bra sätt. Detta innebär att innan ett projekt med personuppgifter behandlas måste man säkerställa att det finns tillräckliga skyddsåtgärder, att säkerheten är tillräcklig

samt att alla som behandlar personuppgifterna gör detta på ett korrekt och lagligt vis. Detta måste kunna visas och det är därför viktigt med en tydlig dokumentation.

Vilka skydds- och säkerhetsåtgärder som ska vidtas beror på vilka sorters personuppgifter som behandlas, hur känsliga de är, om det är en stor mängd etc.

Här kommer en rad exempel på möjliga skydds- och säkerhetsåtgärder.

- *Pseudonymisering*. Om uppgifterna som behandlas inte är direkt kopplade till en person utan det finns en separat nyckel som kopplar person till information är dessa pseudonymiserade. Uppgifterna räknas fortfarande formellt sett som personuppgifter men hanteringen sker med en större säkerhet.

- *Kryptering och kodning.* Att kryptera eller koda information är ett sätt att minimera skadorna vid dataläckage och är bra som tekniskt skydd.

- *Anonymisering.* Om uppgifterna inte, varken direkt eller indirekt, går att koppla till en person är dessa anonymiserade och formellt sett inte längre personuppgifter. Det innebär att dataskyddsförordningen inte behöver användas. Om arbetet kan bedrivas på anonymiserade uppgifter ska detta ske.

- *Accesskontroll.* Att sätta upp och dokumentera regler för vilka som ska ha åtkomst till den insamlade informationen är en administrativ skyddsåtgärd som bör användas. Här ingår också att ta fram ett regelverk för vem som får lov att göra vad med informationen. (Vem får läsa, söka och/eller ändra och i vilka delar av materialet?)

- *Certifiering* av den personal som ska jobba med personuppgifterna kan vara en relevant åtgärd. Information och kunskap hos personalen är viktiga säkerhetsåtgärder som tyvärr ofta glöms bort. Att försäkra sig om att de som arbetar med personuppgifter också är medvetna om och följer de regler som finns för arbetet är viktigt.

- *Fysiskt avskilda servar, backup etc*. Att tekniskt skydda information från förlust vid olika typer av haverier är visserligen inte ett krav i dataskyddsförordningen men är nödvändigt för ett fungerande informationssäkerhetsarbete, vilket vi är skyldiga att ha enligt andra regelverk. Ett absolut minimum är att se till att informationen lagras på ett sätt som omfattas av backup.

- *Gallring och radering.* Personuppgifter som inte längre behövs för behandling ska raderas. Följ gallringsbeslut och konsultera arkivarien vid behov.

Konsekvensbedömning

Dataskyddsförordningen ställer krav på att en konsekvensbedömning ska göras om behandlingen bedöms sannolikt leda till en hög risk för personers rättigheter och friheter. Den som är ansvarig för den planerade behandlingen ska då göra en bedömning av behandlingens konsekvenser för skyddet av personuppgifter. Denna bedömning ska dokumenteras skriftligt och görs i samarbete med dataskyddsombudet. Om det är oklart om den planerade behandlingen ”sannolikt leder till en hög risk” bör dataskyddsombudet konsulteras.

Lagring och gallring

Bevarande och gallring av personuppgifter sker efter lärosätets dokumenthanteringsplan. Vad gäller själva lagringen av personuppgifter så ska dessa lagras på ett säkert sätt vid Umeå universitetet, i enlighet med framtagna lagringsregler. Om en ny molntjänst ska användas måste det vara kontrollerat att molntjänsten är upphandlad på ett korrekt sätt och att det finns personuppgiftsbiträdesavtal. Mer om arkiv under **4.1 Arkivering**.

Internet och sociala medier

Det svenska undantaget för personuppgifter i ostrukturerat material som finns i den nuvarande personuppgiftslagen försvinner genom dataskyddsförordningen. Detta innebär att användning av personuppgifter på t.ex. internet, i e-posten, sociala medier etc. måste följa förordningens regler. Vi måste alltså hitta ett juridiskt stöd för varje användning av namn, bild eller annan personuppgift vi har. Detta kan vara särskilt problematiskt kring användning av personuppgifter på webben och sociala medier.

I högskolelagen anges att lärosäten ska samverka med omvärlden och informera om sin verksamhet. Detta är alltså en grund för användning av personuppgifter för t.ex. marknadsföring av aktuella forskningsprojekt, vad som händer rent generellt på lärosätet, samverkan med näringsliv/kommuner/andra lärosäten etc.

Umeå universitet kommer under hösten 2018 att utarbeta rutiner för hur material som innehåller personuppgifter får behandlas när det gäller bland annat att lägga upp bilder, kommunicera på vår webb m.m.

Uppladdning på vår egen webb

Att ladda upp personuppgifter på en egen hemsida som utgår från egna servrar (alt. på servrar inom EU/EES under vår kontroll) innebär inte att uppgifterna förs över till tredje land, även om de kan ses var man än är i världen. De personuppgifter vi har samlat in för att informera om vår verksamhet eller samverka med vår omvärld är alltså ok att ladda upp/publicera på vår egen webb så länge som den ligger på vår egen server eller åtminstone inte flyttas utanför EES. Det behövs alltså inte något ytterligare stöd för detta än vad vi har för att samla in uppgiften från första början.

Är webbpubliceringen en del i exempelvis ett forskningsprojekt, en upphandling eller ett anställningsförfarande finns stödet för att använda personuppgifter i grundbehandlingen. Däremot måste vi informera om att webben kommer att användas, om inte det redan tydligt framgår av t.ex. en annons placering.

Sociala medier

Vi ansvarar för att användningen av personuppgifter på universitetets sociala medier följer dataskyddsförordningens regler. Exempel på sociala medier är LinkedIn, Twitter, Instagram, Facebook, Youtube, Snapchat etc.

De flesta sociala medier har nationellt hemvist i USA såsom Facebook, Instagram, Twitter och Youtube. Att ladda upp information där innebär alltså många gånger en överföring av personuppgifter till tredje land, vilket bara är tillåtet om det finns ett juridiskt stöd för överföringen. Än så länge är vi hänvisade till ett uttryckligt samtycke till överföring av personuppgifter till tredje land för att kunna ladda upp bilder på identifierbara personer, namnge personer etc. på sociala medier. Detta oavsett om det gäller en student, en anställd eller någon extern eller under vilka förutsättningar.

Samtycke för överföring av person måste vara skriftligt, inspelat eller tydligt dokumenterat på annat sätt och måste finnas kvar så att det kan granskas. Det ska även enkelt kunna återkallas så att framtida användning av personuppgiften stoppas. Innan samtycke kan ges ska den registrerade först få den allmänna informationen om vad vi kommer att göra med personuppgifterna men denna information ska även innehålla att vi inte kan garantera att användningen av dennes personuppgifter stannar vid vad vi har samlat in dem för.

E-post

Vi hanterar stora mängder personuppgifter via e-post och kommer att göra så även fortsättningsvis. Huvudprinciperna är samma som för övriga personuppgifter i förordningen, dvs. att personuppgifter får bara användas när det behövs, ska behandlas på ett lagligt och korrekt sätt mm. och ska bara sparas så länge som det är nödvändigt. Det är alltså väldigt viktigt att sätta sig in i vad som är en allmän handling, när allmänna handlingar får gallras (raderas) m.m. för att kunna göra en bedömning av när du får slänga ett e-postmeddelande. Det finns alltså inget enkelt svar på när en e-post kan slängas utan det beror helt på innehållet.

E-post som är en del av en redan anmäld behandling, t.ex. ett forskningsprojekt, behöver inte anmälas särskilt. Sådan behandling ingår i den redan anmälda behandlingen. Detsamma lär oftast gälla vid behandling av studenters personuppgifter. Det som är viktigt att tänka på är säkerheten. Det är inte rekommenderat att skicka känsliga personuppgifter via e-post.

Personuppgiftshantering vid särskilda tillfällen

Inte alla tillfällen av personuppgiftsbehandlingar kan dock sägas vara lagkrav eller myndighetsutövning. Ett lärosäte har ett brett spektra av aktiviteter och det kan vara nödvändigt att behandla personuppgifter baserat på samtycke, exempelvis vid våra olika evenemang med deltagare utifrån. Observera att ett samtycke ska dokumenteras och sparas så att vi kan visa det vid behov. Det kan endast lämnas av den registrerade själv och det är därför viktigt att vi försäkrat oss om att den registrerade själv har lämnat samtycke, särskilt i samband med känsliga personuppgifter. Notera exempelvis att om vi, vid en middag samlar in uppgifter om kost beroende på eventuella allergier, är detta en känslig personuppgift. I samband med frågor om kost kan det vara lämpligt att vi formulerar frågan så att det handlar om behov istället för en hälsouppgift.

4.1 Arkivering

Umeå universitetet är en myndighet och har därför ansvar för något som kallas ”arkivbildning”. Arkivbildningen består av den information på myndigheten som är allmänna handlingar, vilka givetvis i många fall innehåller personuppgifter.

Personuppgifter ska inte sparas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Denna bestämmelse hindrar inte att en myndighet arkiverar och bevarar allmänna handlingar eller att Umeå universitetets arkivmaterial senare tas om hand av en arkivmyndighet. Det förfarandet är istället en laglig grund och räknas till att utföra uppgifter av allmänt intresse.

Enligt arkivreglerna ska myndigheternas arkiv bevaras, hållas ordnade och vårdas så att följande tillgodoses:

- *Allmänhetens rätt till insyn*

Offentlighetsprincipen som finns i TF är central i den svenska rättsordningen. Den innebär att allmänheten, ofta i egenskap av enskilda individer och företrädare för media, har rätt till insyn i myndighetens arbete och tillgång till dess allmänna handlingar. De allmänna handlingar som beskriver verksamheten över tid ska därför bevaras.

- *Rättskipningen och förvaltningen*

Handlingar som visar vad myndigheten eller den enskilda tjänstemannen har gjort eller inte gjort, t.ex. vad myndigheten kommit överens om genom ett avtal med någon, är viktiga att bevara.

- *Forskningens behov*

De handlingar som bedöms vara värdefulla för framtida forskning ska bevaras. Den bedömningen görs ofta i samråd med verksamheten och då framför allt med universitetets arkivarie.

Förutom kraven på bevarande finns det självklart även ett internt behov av att spara information för att kunna följa den egna verksamheten genom avslutade och arkiverade ärenden och projekt.

Begreppet handling och typer av handlingar
Begreppet handling är definierat i 2 kap. 3 § TF:

”Med handling förstås framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel”. En handling är inte begränsad till att enbart omfatta papper, digitala filer eller liknande.

Det finns olika typer av handlingar:

Arbetshandling – Detta är utkast eller koncept till myndighets beslut eller skrivelse samt minnesanteckningar. Handlingen är inte allmän om den inte har expedierats eller tagits om hand för arkivering. Minnesanteckning är ex. en promemoria eller liknande eller en upptagning som enbart har skapats för att kunna presentera ärendet inför ett beslut eller en inom beredningsprocessen. En arbetshandling som tillför ärendet en eller flera sakuppgifter ska alltid finnas kvar.

Allmän handling - En handling är allmän, om den förvaras, inkommer eller upprättas hos en myndighet.

Offentlig handling - Huvudregeln är att handlingar som är allmänna också är offentliga. Detta innebär att vem som än begär ut handlingen får läsa den, titta på den eller ta del av den på annat sätt. Undantag från detta kan göras om det finns bestämmelser om sekretess som ska användas.

Handling med sekretess - Allmänna handlingar eller uppgifter i en allmän handling kan skyddas av sekretess i enlighet med OSL med hänsyn till:

- rikets säkerhet eller dess förhållande till annan stat eller mellanfolklig organisation,
- rikets centrala finanspolitik, penningpolitik eller valutapolitik,
- myndigheters verksamhet för inspektion, kontroll eller annan tillsyn,
- intresset att förebygga eller beivra brott,
- det allmännas ekonomiska intresse,
- skyddet för enskilds personliga eller ekonomiska förhållanden eller
- intresset att bevara djur- eller växtarter.

Bevarande av handlingar
Huvudprincipen är att allmänna handlingar ska finnas kvar!

Gallring innebär förstöring av allmän handling eller uppgift i allmän handling och är därmed en inskränkning i den del av offentlighetsprincipen som regleras i tryckfrihetsförordningen. För att gallra en allmän handling, oavsett om den innehåller personuppgifter eller inte, krävs det ett stöd i regelverket. Gallringsbeslut som talar om vilka allmänna handlingar som får gallras och efter hur lång tid finns på webbsidan för arkiv samt i diariet.

Allmänna handlingar får gallras om det arkivmaterial som återstår tillgodoser allmänhetens rätt till insyn, behovet av information för rättskipningen och förvaltningen och/eller forskningens behov. Arbetshandlingar får rensas utan att det behöver något stöd i regelverket då detta inte är någon allmän handling.

Arkivering – privacy by design

Begreppet *privacy by design*, eller *inbyggd integritet* som det kallas på svenska, går ut på att låta integritetsfrågor påverka systemets hela livscykel – från förstudie och

kravställning via design och utveckling till användning och avveckling. Några grundläggande principer inom integritetsskydd är som bekant att inte samla in mer information än vad som behövs, att inte ha den kvar längre än man behöver och att inte använda den till något annat än vad man samlade in den för. Att informera om hur uppgifterna ska behandlas, att begära samtycke och att tillåta insyn i den vidare hanteringen är också en del i detta.

Privacy by design går hand i hand med de krav som arkiven ställer vid utvecklingen av en ny IT-tjänst. Kraven är ställda för att möjliggöra en arkivering av de allmänna handlingar som bedömts ska bevaras, men också för att de handlingar som inte ska vara kvar ska kunna gallras.

Arkivkrav – några exempel

- Möjlighet att göra ett arkivuttag med information för att bevara eller migrera.
- Möjlighet att bl.a. kunna skilja på information som ska bevaras från information som ska gallras.
- Möjlighet att konvertera filformat till bevarande-/standardformat.
- Möjlighet att ge filer unika beteckningar.
- Möjlighet att hålla en god informationskvalité, t.ex. förvalda begrepp eller värden.
- Möjlighet att använda metadata för att t.ex. kunna skilja ut handlingar med personuppgifter.
- Möjlighet att kunna logga händelser.
- Möjlighet att lämna ut allmän handling.

Arkivering – särskilt om forskning

Forskningsverksamhet är grundforskning, tillämpad forskning och utvecklingsarbete som bedrivs vid universitet och högskolor enligt högskolelagen eller vid särskilda forskningsinstitut samt i verksamhetsorienterad forskning vid andra statliga myndigheter enligt instruktion eller särskilt uppdrag.

Handlingar som ska bevaras enligt Riksarkivets föreskrifter och allmänna råd om gallring av handlingar i statliga myndigheters forskningsverksamhet (RA-FS 1999:1) tillsammans med Umeå universitetets lokala gallringsbeslut avseende forskning är handlingar som:

- innehåller grundläggande uppgifter om projektets syfte, metod och resultat
- speglar projektets kontext avseende t.ex. ekonomiska förutsättningar och externa kontakter, samt visar eventuella förändringar i inriktning under arbetets gång.
- bedöms ha ett fortsatt inomvetenskapligt värde eller värde för annat forskningsområde, som bedöms vara av stort vetenskapshistoriskt, kulturhistoriskt eller personhistoriskt värde, eller som bedöms vara av stort allmänt intresse.

Exempel på sådana handlingar som ska bevaras är:

- Dataset inklusive kodnycklar.
- Metadata (t.ex. den slags information som ingår i en datahanteringsplan/Data Management Plan).
- Projektansökningar.
- Beslut om medel.
- Etikprövningshandlingar.
- Enkät- och intervjuformulär.
- Rapporter, publikationer och avhandlingar.

Förutom ovan nämnda exempel ska även de handlingar bevaras som hjälper till att ge en god förståelse för vad som hänt under projektet och hur materialet ska tolkas. Har du frågor om vilka handlingar som ska arkiveras och hur kontaktar du universitetets arkivarie.