Informations- och utbildningsmaterial

Den nya Dataskyddsförordningen

Dataskyddsförordningen/General Data Protection Regulation (GDPR)

- ska stärka enskilda personers rättigheter över hur myndigheter, organisationer och företag får samla in och använda deras personuppgifter.
- innebär att samma regler för hur personuppgifter får hanteras ska gälla i hela EU.
- ställer strängare krav på insamling och användning av personuppgifter.

1.0 Introduktion

Bakgrund

Från och med 2018-05-25 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, där företag som Google (grundat 1998) och Facebook (grundat 2004) 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 genom Personuppgiftslagen (PUL)) har visat sig otillräckligt och 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 vi genom 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 arbetet antingen vi ansvarar för en behandling eller hanterar personuppgifter som en del av vårt dagliga arbete.

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 är personuppgifter utan även användarnamn, e-postadresser, biometriska data, fysiologiska uppgifter och även kombinationer av uppgifter så länge det genom uppgifterna är möjligt att koppla dessa till en fysisk person. För all behandling av personuppgifter gäller att den måste följa dataskyddsförordningens samtliga principer för behandling och då gäller att:

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

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 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. Enligt förordningen måste vi redan när vi samlar in uppgifter veta vad vi ska ha dem till så att vi inte samlar in mer än nödvändigt, bara till berättigade ändamål och vi måste också veta hur länge vi ska använda uppgifterna (även om vi inte nödvändigtvis måste kunna ange ett exakt slutdatum).

Förutom att behandlingen måste uppfylla de sex principerna måste det också finnas laglig grund för behandlingen och då finns det sex tillåtna grunder för behandling angivna och det räcker med att en av dem är uppfylld för att behandlingen ska vara tillåten.

- Samtycke – den registrerade har lämnat sitt informerade samtycke till behandlingen. Samtycke måste registreras och kan när som helst återkallas.
- Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är delaktig i.
- Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse.
- Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade.
- Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.
- Behandlingen är nödvändig för tredje parts berättigade intressen (om inte den registrerades intressen, fri- eller rättigheter väger tyngre). Observera att möjligheten att använda denna grund är kraftigt begränsad för myndigheter.

För KMH faller mycket av vår verksamhet under myndighetsutövning (myndighetsutövning används i förordningen i en vidare tolkning än normalt för oss och omfattar det vi gör inom vårt uppdrag som myndighet) och här har vi normalt allt som exempelvis hör till utbildning och examination. Vidare anses vår forskning vara av ett allmänt intresse vilket även förtydligas genom lagen om forskningsdata. De arbeten som våra studenter producerar, företrädesvis inom ramen för sina examensarbeten, når sannolikt inte upp till allmänt intresse och behöver företrädesvis baseras på samtycke (mer om studenternas behandling av personuppgifter nedan). Övriga grunder kan bli aktuella beroende på omständigheterna och vid osäkerhet bör du kontakta KMH:s dataskyddsombud via epost på dataskyddsombud@kmh.se.

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

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

Informationsplikten gäller även om vi inte samlar in uppgifterna direkt från den registrerade (undantag kan göras om den registrerade sedan tidigare är informerad, om det är praktiskt omöjligt eller mycket svårt att informera eller om överföringen är föreskriven i lag). Detta betyder exempelvis att när en student begär ett användarkonto hos oss så hämtar vi normalt uppgifter från Ladok och vi är då skyldiga att informera studenten om att vi hämtar information från Ladok 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.

Lärosätet är också skyldigt att hålla reda på vilka personuppgiftsbehandlingar som pågår inom verksamheten och detta görs genom att man upprättar ett register. Den som är ansvarig för en behandling är också skyldig att anmäla den till registret där följande uppgifter noteras.

- Namn och kontaktuppgifter för den personuppgiftsansvarige,
- ev. företrädare och dataskyddsombudet.
- Ändamålen med behandlingen.

- En beskrivning av kategorierna av registrerade och vad som registreras.
- Vem/vilka som kommer att ta del av uppgifterna.
- Eventuell överföring till länder utanför EU och information om skyddsnivån hos mottagaren.
- Om möjligt, när uppgifterna kommer att raderas.
- Om möjligt, en beskrivning av säkerheten för behandlingen (både teknisk och administrativ säkerhet).

För den som ansvarar för en behandling av personuppgifter (exempelvis systemägaren till ett av lärosätets system eller digitala tjänster eller den som upprättat en behandling exempelvis inom ramen för sin forskning) är det nödvändigt att känna till de tillåtna grunderna, informationsplikten och följa principerna och registrera behandlingen medan det för den som arbetar i ett system som behandlar personuppgifter är det viktigt att ha kunskap om vad som gäller.

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 det KMH som är personuppgiftsansvarig. Det är KMH som har det yttersta ansvaret för all behandling av personuppgifter som sker inom ramen för verksamheten. 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. Vid fel och brister i hanteringen kan både personuppgiftsansvarig och personuppgiftsbiträdet drabbas av sanktionsavgifter (böter) som för svensk del bestäms av Integritetsskyddsmyndigheten (tidigare Datainspektionen) och utdöms av domstol. Sanktionsavgifterna ska vara effektiva, proportionella och avskräckande och kan bli mycket höga. Integritetsskyddsmyndigheten är tillsynsmyndighet 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 också fungera som hjälp och stöd för verksamheten. Dataskyddsombudet ska också vara tillgängligt för att kunna hantera frågor och klagomål från registrerade och kan kontaktas på dataskyddsombud@kmh.se. Som enskild medarbetare förväntas du hantera personuppgifter på ett korrekt sätt och ha kunskap om de regler som gäller för just dina arbetsuppgifter.

Den registrerades rättigheter
Genom Dataskyddsförordningen har den registrerade en rad rättigheter som är avsedda att stärka skyddet för den personliga integriteten och positionen gentemot den som behandlar personuppgifter. Alla, vars personuppgifter registreras, har rätt att få information på ett klart och tydligt sätt om behandlingen och också rätten att ta del av vilka uppgifter som behandlas (normalt får svar på en sådan begäran inte dröja mer än en månad men kan förlängas till tre om arbetet med att ta fram uppgifterna är komplicerat). Det ska också normalt vara kostnadsfritt att få ut den begärda informationen. Den registrerade har också rätt att få felaktig information rättad utan onödigt dröjsmål och rätten att få personlig information raderad eller behandlingen av den avslutad om den används längre än nödvändigt och något annat inte följer av lagkrav som exempelvis reglerna för hanteringen av allmänna handlingar eller behandling för forskningsändamål av allmänt intresse.
Den registrerade har också rätt att få ut sin information digitalt. Slutligen har den registrerade alltid rätten att lämna klagomål till Integritetsskyddsmyndigheten som sedan utreder och bestämmer om eventuella sanktionsavgifter.

Andra lagar som också styr behandlingen av personuppgifter
Dataskyddsförordningen styr inte ensamt hanteringen av personuppgifter utan kompletteras genom vissa lagar vi känner sedan tidigare och andra som träder ikraft samtidigt med ***förordningen (180525).*** Sedan tidigare är vi vana vid att arkivlagen (1990:782) reglerar bevarande och raderande av allmänna handlingar och tryckfrihetsförordningen (1949:105), där offentlighetsprincipen finns, tillsammans med offentlighets- och sekretesslagen (2009:400) styr allmänhetens tillgång till allmänna handlingar. Vad gäller personuppgifter är arkivlagen och tryckfrihetsförordningen av särskild vikt när det gäller rätten att bli glömd, eftersom det kan finnas bestämmelser i dem som innebär att uppgifter inte får raderas. Frågor om sekretess regleras i offentlighets- och sekretesslagen. Här anges även att allmänna handlingar ska registreras, vilket oftast innebär att personuppgifter behandlas. När en begäran om uppgifter inkommer måste den prövas inte bara utifrån dataskyddsförordningen utan även utifrån denna.

Den lagliga grunden för personuppgiftsbehandling i vår verksamhet är i många fall krav som ställs i högskolelagen (1992:1434) eller högskoleförordningen (1993:100), speciellt när det gäller uppgifter om studenter. Lagkrav som kan utgöra laglig grund för behandling av personuppgifter finns även i förvaltningslagen (1986:223 eller 2017:900 från och med 2018-07-01). Denna lag handlar främst om serviceskyldighet och handläggning av ärenden. Här finns också ytterligare bestämmelser om rätten att ta del av uppgifter om sig själv.

Utöver de lagar och förordningar som redan finns kommer ytterligare lagar att trädas ikraft samtidigt med förordningen och här finner vi dataskyddslagen som kompletterar förordningen med vissa nationella bestämmelser på ett mer övergripande plan (exempelvis att åldersgränsen för samtycke är 13 år) och en särskild forskningsdatalag som reglerar användningen av personuppgifter inom forskningen. Den senare samverkar med lagen om etikprövning (2003:460) när det gäller hanteringen av känsliga personuppgifter för forskningsändamål.

2.0 Administration

Inom lärosätets administrativa system pågår en rad olika behandlingar av personuppgifter som alla omfattas av Dataskyddsförordningens regler. All behandling måste ha ett tydligt och godkänt syfte, de, vars personuppgifter behandlas, har rätt till information om vad som sker, vilka uppgifter som behandlas och ett antal rättigheter som skydd för de personliga fri- och rättigheterna. Vi får inte heller samla in mer uppgifter än nödvändigt och inte behålla dessa längre än vad som krävs.

Tillåtna grunder
Varje behandling måste göras med en tillåten grund och för personaladministrativa handlingar gäller främst att behandlingen är nödvändig för att fullgöra en rättslig förpliktelse eller att behandlingen är en del vår myndighetsutövning. Dessa båda grunder täcker tillsammans huvuddelen av lärosätets administrativa funktioner och innebär därför inte några direkta förändringar i det praktiska arbetet inom administrationen. Behandlingen styrs också i många tillfällen av nationell lag och vi har sedan tidigare bokföringslagen, arkivlagen, arbetstidslagen, lagen om anställningsskydd, arbetsmiljölagen, arbetstidslagen, diskrimineringslagen, medbestämmandelagen, föräldraledighetslagen, semesterlagen, lagen om sjuklön med flera att rätta oss efter vid behandling av personuppgifter och kommer att göra så även framöver.

Typer av personuppgifter och deras behandling
De typer av personuppgifter som samlas in i administrativa sammanhang är huvudsakligen namn, adress, 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). I vissa system, exempelvis det personaladministrativa systemet, finns också möjligheter att införa egna, frivilliga personuppgifter.

Även sjukuppgifter behandlas, då med stöd av lagen om sjuklön, för att den anställde ska kunna få rätt ersättning. Dessa uppgifter gallras sedan med stöd av Riksarkivets föreskrifter: RA-FS 2012:9.

Andra typer av handlingar där personuppgifter behandlas kan vara: ansökningshandlingar, anställningsavtal, information om avslutande av tjänst, olika former av beslut, löneuppgifter, kontrolluppgifter, kvitton samt försäkran vid sjukdom.

Redovisningssystemen samlar in personuppgifter från enskilda individer, till exempel externa föreläsare som ska ha arvode, och från olika leverantörer av varor och tjänster. Hit hör även de skatte- och bankuppgifter samt annan information som kan behövas för en korrekt utbetalning.

3.0 Gemensam

Registrering av personuppgiftsbehandlingar
KMH är personuppgiftsansvarig för alla behandlingar inom dess verksamhet, allt ifrån den enskilde studentens examensarbete till de stora administrativa systemen. För att ha kontroll över vilka behandlingar som pågår och kunna redovisa dessa för tillsynsmyndigheten finns ett centralt register där den som upprättar en behandling av personuppgifter också går in och registrerar den. Vid KMH görs detta av respektive chef som ansvarar för registret i fråga. Detta krav gäller bara för den som upprättar en behandling men är bra att känna till även för dem som arbetar inom en befintlig behandling. Registreringen i detta övergripande register ska inte innehålla något av det material som behandlas utan bara uppgifter om att behandling görs och vem/vilka som utför den. I korthet följande information:

- ändamålet med behandlingen,
- kontaktperson för behandlingen,
- en beskrivning av vilka typer av uppgifter som samlas in,
- hur länge uppgifterna ska behandlas (om det är möjligt att ange)
- och om möjligt en beskrivning av de tekniska och organisatoriska skyddsåtgärderna.

Information till den registrerade
Vid insamlingstillfället har den registrerade rätt att få information om vilka uppgifter som samlas in. Detta är enkelt i de fall man samlar in uppgifterna direkt från den registrerade men kravet gäller också normalt i de fall man hämtar uppgifterna från en annan källa. Information ska lämnas om:

- ändamålet med behandlingen,
- vilken rättslig grund det finns för behandlingen,
- hur länge de ska användas,
- vem/vilka som ska använda uppgifterna,
- att KMH är personuppgiftsansvarig,
- att den registrerade har rätt att få tillgång till uppgifterna och få fel rättade och
- att det finns ett dataskyddsombud som kan nås via dataskyddsombud@kmh.se och att man kan vända sig till Integritetsskyddsmyndigheten med eventuella klagomål om inte KMH och den registrerade kan komma överens.

Den registrerades rättigheter och begränsningar av dessa
Den vars uppgifter behandlas har ett antal rättigheter som det är viktigt att tänka på. Detta gäller som tidigare har nämnts rätten att få information om vad uppgifterna ska användas till (ändamålet med behandlingen), vilka uppgifter som samlas in, hur länge uppgifterna kommer att sparas (eller vad som avgör hur länge de ska sparas) och rätten att få tillgång till de uppgifter som finns registrerade om den egna personen. Vidare har den registrerade också rättighet att invända mot behandlingen, få felaktiga uppgifter rättade, återkalla samtycke (utan att behöva ange någon anledning) och den registrerade har också rätt att klaga till Integritetsmyndigheten (tidigare Datainspektionen) om denne 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 starkare grund för att behålla uppgifterna (att vi exempelvis i enlighet med arkivlagen eller offentlighets- och sekretesslagen eller andra lagar 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 göra det eftersom vi har en rättslig förpliktelse att förmedla uppgifterna. Vid oklarheter kring vad som ska raderas och vad som ska bevaras bör dataskyddsombudet kontaktas. Generellt kan sägas att behandlingen av personuppgifter bör vara öppen och tydlig gentemot den registrerade och om det är möjligt bör vi tillmötesgå den registrerades önskemål.

Den registrerade har genom Dataskyddsförordningen bl.a. 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, rätt att få personlig information raderad (om det inte finns laglig grund för att behålla den). För den som forskar är det viktigt att känna till att forskningsdatalagen gör två begränsningar av dessa rättigheter:

- Rätten till rättelse ska inte gälla för sådana personuppgifter som behandlats för forskningsändamål om de enbart bevaras i arkiveringssyfte. Rätten till rättelse ska i övrigt gälla utan undantag.

- Rätt till begränsning av behandling ska inte gälla när den registrerade bestrider uppgifternas korrekthet under den utredningstid som krävs för att kontrollera om personuppgifterna är korrekta, om detta medför att forskningen inte kan utföras eller på ett avgörande sätt försenas eller försvåras. Detsamma ska gälla när den registrerade invänder mot behandlingen, i väntan på kontroll av huruvida den personuppgiftsansvariges berättigade skäl väger tyngre än den registrerades berättigade skäl.

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. I Dataskyddsförordningen ställs mycket stora krav på att den som behandlar personuppgifter väl dokumenterar hur det ska gå till. Detta innebär att innan ett projekt med personuppgifter som 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.
Exempel på 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. Enligt forskningsdatalagen ska personuppgifter pseudonymiseras eller vara skyddade på likvärdigt sätt om ändamålet med behandlingen kan uppfyllas på det viset.

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

- Anonymisering – Om uppgifterna inte längre, varken direkt eller indirekt, går att koppla till en person är dessa anonymiserade och formellt sett inte längre

personuppgifter (Dataskyddsförordningen gäller ej dessa). 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 regelverket för vem som får lov att göra vad med informationen (vem som får läsa, söka respektive ändra och i vilka delar av materialet.)

- Certifiering av den personal som ska jobba med personuppgifterna – Information och kunskap hos personalen är viktiga säkerhetsåtgärder som inte sällan försummas. 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 inte ett krav i Dataskyddsförordningen men kan vara nog så viktigt för exempelvis den enskilde forskaren. 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 arkivarierna vid behov.

- Filer med ekonomiska uppgifter till banken sänds krypterade enligt den internationella standarden ISO 20022/XML, så kallad SEPA-betalning.

Behandling av känsliga personuppgifter
Känsliga personuppgifter enligt Dataskyddsförordningen är 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, förutom i de fall den registrerade samtycker till behandlingen.

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

- 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 ***lag (2018:XX)*** med kompletterande bestämmelser till EU:s Dataskyddsförordning.

Dessa undantag är: Känsliga personuppgifter får med stöd av artikel 9.2 g i dataskyddsförordningen behandlas av en myndighet

- i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av ett ärende,

- om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag, eller

- i enstaka fall, om det är absolut nödvändigt för ändamålet med behandlingen och behandlingen inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

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
Det finns i princip bara en enda regel gällande lagring och gallring i dataskyddsförordning, sett till lärosätet i stort. Detta är att personuppgifterna endast får behandlas så länge det behövs för att uppfylla det ändamål för vilka de samlades in. Så snart de avsedda personuppgifterna inte längre behövs för sitt ändamål ska de gallras. Det kan dock vara så att personuppgifterna finns på en allmän handling, vilket gör att reglerna om handlingars offentlighet tar företräde. Detta betyder att gallringsföreskrift som anger omständigheterna för gallring och arkivering gäller framför förordningens grundprincip. Om lagstiftning annars anger att behandlingen ska fortgå gäller även dessa framför denna princip. Vid tveksamhet bör KMH:s arkivarie eller registrator rådfrågas.

Bevarande och gallring av personuppgifter följer de föreskrifter som Riksarkivet ålagt oss. Vad gäller själva lagringen av personuppgifter så ska dessa lagras på ett säkert sätt på KMH, i enlighet med KMH:s plan för informationssäkerhet. Om en molntjänst ska användas, får endast molntjänster godkända av KMH användas. Under alla omständigheter får endast en molntjänst användas, för att öka möjligheterna att kontrollera spridningen av personuppgifterna. Antalet personer som har tillgång till uppgifterna ska minimeras. Om personuppgifter inte behövs för att utföra en arbetsuppgift, bör den inte finnas tillgänglig för personen som ska utföra arbetsuppgiften.

Sociala medier och Internet
Vid sidan av vår utbildning och forskning har vi också en skyldighet att samverka med omvärlden och informera om vår verksamhet. Att via lärosätets webbplats eller vår närvaro på sociala medier berätta om vad vi gör, presentera aktuell forskning och i övrigt presentera vår verksamhet är även fortsatt tillåtet. Det är även tillåtet att publicera översiktsbilder från våra evenemang där enskilda personer inte kan identifieras eller där den som visas har godkänt publiceringen. Ur dessa aspekter skiljer sig inte vår webbplats och sociala medier sig åt. För den som däremot avser att upprätta någon form av behandling av personuppgifter är det endast tillåtet att använda de tjänster som rekommenderas av lärosätet. Ett av kraven för att få använda en tjänst för behandling av personuppgifter är att vi har tecknat ett särskilt avtal med leverantören om behandlingen och så har endast skett för de tjänster som rekommenderas av lärosätet. Även för dessa tjänster gäller som tidigare nämnts att man inte får samla in och behandla mer information än nödvändigt och att hantering sker på ett säkert och gentemot den registrerade öppet sätt.

E-post
Vi hanterar en stor mängd personuppgifter via e-post och vi kommer även i fortsättningen att göra så. Det finns dock vissa saker att tänka på i samband med användning av e-post. Korrespondens via e-post får inte användas för känsliga personuppgifter, såsom etniskt ursprung, politiska åsikter, religion, brottslighet, medlemskap samliv, hälsoinformation. Ej heller får korrespondens via e-post användas för extra skyddsvärda uppgifter såsom personnummer och information som innefattas av tystnadsplikt och sekretess.

Personuppgiftshantering vid särskilda tillfällen
Inte alla tillfällen av personuppgiftsbehandlingar kan dock sägas vara lagkrav eller myndighetsutövning. Ett lärosäte har ett brett spektrum 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 göras skriftligt (även digitalt) och bevaras så att det kan framvisas 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 önskemål istället för en hälsouppgift.

Sammanfattning
Sammantaget för den som arbetar inom KMH kan sägas, att vilken rättslig grundbehandlingen vilar på, formulering av ändamålet eller registreringen av behandlingen ofta inte är något som den enskilde medarbetaren behöver ta ställning till. En behandlings ändamål, registrering och rättsliga grund 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, en post i registret och rättslig förpliktelse som grund. Detta gäller för alla som för in resultat utan att den enskilde medarbetaren ska redovisa detta löpande. Det är viktigt att vara medveten om bakgrunden till arbetet men för den som arbetar med personuppgifter i en etablerad behandling är det viktigast att hålla sig informerad kring de regler och instruktioner som gäller och vid osäkerhet kontakta den som ansvarar för behandlingen. Vid KMH ligger ansvaret hos den chef där registret/behandlingen är placerad. För den som tänker etablera en behandling av personuppgifter, exempelvis inom ramen för sin forskning är det dock nödvändigt att uppfylla de formella kraven för att behandlingen ska bli godkänd. Lärosätets dataskyddsombud kan kontaktas för råd och stöd.

4.0 Arkivering

KMH är en myndighet och ansvarar för sin arkivbildning. Arkivbildningen består av den information som är allmänna handlingar och de innehåller givetvis också i många fall personuppgifter.

Personuppgifter ska inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Men denna bestämmelse hindrar inte att en myndighet arkiverar och bevarar allmänna handlingar eller att lärosätets arkivmaterial senare tas om hand av en arkivmyndighet. Detta räknas som laglig grund för att utföra uppgifter av allmänt intresse.
Känsliga personuppgifter har ett starkare skydd. Till känsliga personuppgifter räknas enligt Dataskyddsförordningen 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 samt personuppgifter som rör fällande domar i brottmål. Även genetiska uppgifter och biometriska uppgifter som entydigt identifierar en person kan enligt förordningen räknas som känsliga personuppgifter.

Enligt arkivlagen ska myndigheternas arkiv bevaras, hållas ordnade och vårdas så att de tillgodoser.

- Allmänhetens rätt till insyn - offentlighetsprincipen enligt tryckfrihetsförordningen (TF) är central i den svenska rättsordningen. Den innebär att allmänheten, ofta 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 bevisar vad myndigheten eller den enskilda tjänstemannen har gjort eller inte gjort, t.ex. vad myndigheten kommit överens om genom ett avtal med annan part, 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.

Förutom arkivlagens krav på bevarande finns det självklart även ett behov av att bevara information för att tillgodose verksamhetens behov av att kunna följa den egna verksamheten genom avslutade och arkiverade ärenden och projekt.

Begreppet handling och typer av handlingar
Begreppet handling är definierat i tryckfrihetsförordningen (TF) 2 kap. 3 §:
”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 oberoende av medium.

Det finns olika typer av handlingar:
Arbetshandling - är utkast eller koncept till en myndighets beslut eller skrivelse samt minnesanteckningar. Handlingen är inte allmän om den inte har expedierats eller tagits om hand för arkivering. Med minnesanteckning förstås promemoria och annan uppteckning eller upptagning som har kommit till endast för ärendes föredragning eller beredning. En arbetshandling som tillför ärendet sakuppgift ska alltid bevaras.

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

Handling med sekretess - Allmänna handlingar eller uppgifter i en allmän handling kan skyddas av sekretess i enlighet med offentlighets- och sekretesslagen (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.

Offentlig handling - Huvudregeln är att handlingar som är allmänna också är offentliga.

Bevarande av handlingar
Huvudprincipen är att allmänna handlingar ska bevaras.
Gallring innebär förstöring av allmän handling eller uppgift i allmän handling och är därmed en inskränkning i den del av offentlighetsprincipen (rätten att ta del av allmänna handlingar) som regleras i Tryckfrihetsförordningen. För att gallra en allmän handling oavsett om den innehåller personuppgifter eller inte krävs det ett stöd i regelverket.

Allmänna handlingar får enligt 10§ arkivlagen gallras om det arkivmaterial som återstår tillgodoser:

- allmänhetens rätt till insyn
- behovet av information för rättskipningen och förvaltningen
- forskningens behov

Arbetshandlingar kan rensas och för det krävs det inget stöd i regelverket.

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 att inte samla in mer information än vad som behövs, inte ha den kvar längre än man behöver och 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 led i integritetsskyddet.

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 i en Bevarande- och gallringsutredning bedömts ska bevaras, men också för att de handlingar som bedömts inte ska bevaras 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 handlingar med personuppgifter.
- Möjlighet att kunna logga händelser.
- Möjlighet att lämna ut allmän handling.

Arkivering – forskning särskilt
Forskningsverksamhet är grundforskning, tillämpad forskning och utvecklingsarbete som bedrivs vid universitet och högskolor enligt 1 kap. 2§ 2. högskolelagen (1992:1434) som vid särskilda forskningsinstitut och i verksamhetsorienterad forskning vid andra statliga myndigheter enligt instruktion eller särskilt uppdrag.

Handlingar ska enligt Riksarkivets föreskrifter och allmänna råd om gallring av handlingar i statliga myndigheters forskningsverksamhet (RA-FS 1999:1) bevaras 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 handlingar:

- Data-set 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 Doktorsavhandlingar.

Förutom ovannämnda 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.

Arkivering – regelverk
Myndigheternas allmänna handlingar omfattas av tryckfrihetsförordningen (1949:105), offentlighets- och sekretesslagen (2009:400), arkivlagen (1990:782), arkivförordningen (1991:446) samt av föreskrifter från Riksarkivet. I arkivförordningen (1991:446) regleras Riksarkivets rätt att föreskriva om arkivhanteringen hos statliga myndigheter. Föreskrifterna utfärdas bland annat för material och metoder för framställning av handlingar, arkivets organisation, arkivredovisning, arkivets skydd samt gallring och annat avhändande av handlingar. Riksarkivets föreskrifter ges ut i två olika serier, dels i Riksarkivets generella föreskrifter (RA-FS), dels i Riksarkivets myndighetsspecifika föreskrifter (RA-MS). För KMH gäller RA-FS 1997:6, RA-FS 2004:1, RA-FS 2006:5, RA-FS 2013:1 och RA-MS 2017:39.

Har du frågor om vilka handlingar som ska arkiveras och hur, kontaktar du KMH:s arkivarie eller registrator.