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 Personuppgiftsbehandling vid examensarbeten

Inledning

Den europeiska dataskyddsförordningen tillsammans med ett antal svenska lagar kopplade till denna ställer hårda krav på att allt arbete med personuppgifter utförs korrekt. Om du som student tänker använda personuppgifter för ditt examensarbete finns det därför mycket att tänka på. Denna text ger en kort genomgång av de steg som är nödvändiga för att hanteringen av personuppgifter ska bli korrekt. Utöver de regler som gäller för personuppgifter kan det, beroende på vad du avser att behandla, finnas ytterligare regler att ta hänsyn till och du bör därför ha en övergripande diskussion med din handledare om vilken information som ska hanteras och planera därefter.

Steg 1 - Måste personuppgifter behandlas?
Den första frågan är om det verkligen är nödvändigt att behandla personuppgifter? Den undersökning som ska göras kanske kan utföras utan att personuppgifter behandlas och då är detta att föredra. Om man inte behandlar personuppgifter gäller kraven i dataskyddsförordningen inte, vilket gör arbetet lättare. Det är dock viktigt att komma ihåg att som personuppgift räknas all information som direkt eller indirekt kan knytas till en levande människa vilket gör att det inte bara är sådant som namn, personnummer, DNA eller porträttfoto som är en personuppgift utan det kan även vara en kombination av mer anonyma uppgifter som sammantaget gör det möjligt att identifiera en enskild person.

Steg 2 - Definiera syftet med behandlingen och vilka uppgifter som måste samlas in
Innan det praktiska arbetet börjar är det viktigt att göra klart vilka uppgifter som ska samlas in och varför. För dig som ska göra ett examensarbete är detta inte någon svår uppgift utan syftet med behandlingen är helt enkelt att kunna utföra den undersökning som är nödvändig för att underbygga ditt arbete, men det är viktigt att du tänker igenom och formulerar syftet såväl som att du är klar över vilken information som är nödvändig för att nå det.

Steg 3 - Registrera behandlingen
Varje behandling av personuppgifter ska registreras i KMH register över personuppgifts-behandlingar. Till detta register ska du rapportera följande: syftet med behandlingen, vilka typer av uppgifter du tänker samla in och behandla, dina kontaktuppgifter, hur länge uppgifterna kommer att sparas (om det går), om någon annan part kommer att delta i arbetet med personuppgifterna och hur informationen kommer att skyddas. Registret ska inte innehålla några av de insamlade personuppgifterna utan bara en förteckning över vad som samlas in och behandlas så att KMH har kontroll över vilka behandlingar som pågår. KMH har formellt ansvar för de personuppgiftsbehandlingar som utförs inom hela verksamheten: Detta gäller även examensarbeten.

Steg 4 - Bestäm hur informationen ska förvaras och hanteras säkert under arbetet
Insamlad information måste behandlas på ett säkert sätt. Att förvara insamlade personuppgifter i din hemkatalog/lokala filserver är att rekommendera. Hemkatalogen har tillräcklig säkerhet även för känsliga personuppgifter (som känsliga personuppgifter räknas 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). Externa lagringstjänster (verktyg som inte tillhandahålls genom KMH) får inte användas för personuppgifter. Detta gäller exempelvis Dropbox, Google docs, iCloud med flera.

Steg 5 – Bestäm vilka delar av informationen som ska raderas respektive bevaras när arbetet är klart
Personuppgifter får inte bevaras längre tid än vad som är nödvändigt och ska raderas när de inte längre behövs. Samtidigt kan det finnas delar av informationen som måste bevaras för att kunna styrka slutsatserna i examensarbetet eller för att de är nödvändiga för framtida behandlingar. Innan det praktiska arbetet startar är det därför viktigt att bestämma vad som ska hända med de insamlade personuppgifterna efteråt. Vilka uppgifter ska bevaras respektive gallras? Under arbetets gång kan det finnas anledning att ompröva den ursprungliga planen men det är viktigt att det finns en grundläggande plan, inte minst för att kunna besvara frågor från de registrerade (personerna vars uppgifter samlas in).

Steg 6 - Inhämta samtycke, informera de registrerade och samla in de nödvändiga personuppgifterna
Personuppgifter får endast behandlas om det finns laglig grund för behandlingen. Dataskyddsförordningen anger ett antal grunder som betraktas som tillåtna men för ett examensarbete är det i praktiken endast samtycke som kan komma ifråga (om det inte är möjligt att använda samtycke bör du ta upp detta med din handledare och dataskyddsombudet för att se om det går att finna en annan lösning). Att använda samtycke som grund innebär att den registrerade ger sitt aktiva samtycke till behandlingen. Detta innebär i praktiken att du, på ett tydligt och klart sätt talar om vilka uppgifter du vill samla in, vad de ska användas till och av vem/vilka, hur länge uppgifterna ska användas, att det finns möjlighet att begära att få se den insamlade informationen och att det finns möjlighet att vända sig till dataskyddsombudet eller [tillsynsmyndigheten] med klagomål. Efter det att den registrerade har tagit del av informationen kan han/hon ge sitt samtycke till behandlingen och det är då tillåtet att behandla uppgifterna. Viktigt att veta om samtycke är att det ska registreras och sparas så att det kan plockas fram vid behov och att den registrerade har rätt att när som helst återkalla sitt samtycke. Samtycket ska därför göras skriftligt (även digital signering går bra) och [lärosätet] har tagit fram en samtyckesblankett som kan användas och som du hittar på [länk till samtyckesblankett]. Om den registrerade har samtyckt till behandlingen får även känsliga uppgifter behandlas (observera att känsliga uppgifter ställer stora krav på säkerheten i hanteringen).

Steg 7 – Behandla det insamlade materialet
Under förutsättning att de tidigare stegen har utförts är detta ett formellt enkelt steg som inte kräver några ytterligare åtgärder. Samtidigt är detta i praktiken det huvudsakliga arbetet.

Steg 8 - Efter behandling - radera eller arkivera personuppgiftsmaterialet efter behov
Tillsammans med behandlingen är även detta ett enkelt steg då nu det praktiska arbetet är avslutat. Materialet som har behandlats ska nu antingen föras över för bevarande/arkivering eller raderas enligt vad du beslutade i steg 5. Kontakta KMH:s registrator eller arkivarie för att utföra uppgiften.