Riktlinjer **2018-05-22**
fastställd av rektor **Dnr 18/334**

Riktlinjer för behandling av personuppgifter vid KMH

Den 25 maj 2018 träder en ny allmän dataskyddsförordningen i kraft. Regleringen är en förordning ((EU) nr 2016/679) från Europaparlamentet och Europarådet vilken gäller som svensk lag. Förordningen förkortas GDPR efter engelskans *General Data Protection Regulation*. Syftet med förordningen är att stärka skyddet för den personliga integriteten och skapa ett enhetligt regelverk för hela EU. All hantering av personuppgifter inom EU ska, oavsett om det sker inom eller utom EU, respektera människors grundläggande fri- och rättigheter och särskilt deras rätt till skydd av personuppgifter.

Introduktion

Utgångspunkten i Dataskyddsförordningen är att den enskilde personen äger sina egna personuppgifter och att andra endast får behandla (samla in, lagra, bearbeta m.m.) uppgifterna om den enskilde lämnat sitt samtycke eller om det finns någon annan laglig grund för behandling (t.ex. uppgift av allmänt intresse, myndighetsutövning eller avtal). Därför måste rätten att hantera personuppgifter säkerställas innan behandling kan göras. Bakom införandet av dataskyddsförordningen märks den snabba tekniska utvecklingen kring insamling och behandling av personuppgifter som har lett till att det skydd som tidigare getts för den enskilde genom personuppgiftslagen är otillräckligt. Detta har bl.a. aktualiserats genom att några av världens största företag har försäljning av personuppgifter som huvudsaklig inkomstkälla.

Det finns **sex principer** som gäller för all behandling av personuppgifter: att behandlingen är laglig, korrekt och öppen mot den registrerade, att ändamålet med behandlingen är tydligt, att de uppgifter som hanteras är korrekta, att inte fler uppgifter än nödvändigt samlas in, att inte uppgifterna behandlas längre än nödvändigt och att lämpliga säkerhetsåtgärder finns på plats.

Det är den som önskar behandla personuppgifterna som ska säkerställa att det finns laglig grund samt att behandlingen sker i enlighet med gällande regler och instruktioner.

Definition av personuppgift

Varje uppgift som direkt eller indirekt kan kopplas till en levande person är en personuppgift. Hit hör namn och personnummer men också användarnamn, e-postadresser, biometriska data, fysiologiska uppgifter etc. Även kombinationer av uppgifter räknas som personuppgift om de kan kopplas till en fysisk person.

Förändring av skyddet

Tidigare reglering har gett den som samlat in uppgifterna större utrymme att samla in, behandla och spara uppgifter. Med den nya regleringen skärps kraven och det är endast tillåtet att samlas in och behandla uppgifter som behövs för ett särskilt ändamål. All behandling av personuppgifter måste följa dataskyddsförordningens samtliga sex principer. Det innebär 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 är självklara, medan de tre följande ställer nya krav. Det går inte längre att samla in brett med syfte att uppgifterna kanske kan vara användbara för annat ändamål i framtiden.

Lagliga grunder för behandling av personuppgifter

Förutom att behandlingen ska uppfylla alla sex principerna, ska det finnas en laglig grund för behandlingen. Det räcker att **en** laglig grund 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). Denna grund är kraftigt begränsad för myndigheter.

Vid KMH ryms allt som hör till utbildning och examination under ovan tillåtna grunder. Forskningen vid KMH anses vara av allmänt intresse. Däremot är det inte troligt att exempelvis studenternas egna arbeten, kan anses vara av allmänt intresse. Studenternas behandling av personuppgifter inom exempelvis examensarbeten bör därför baseras på samtycke. Övriga grunder kan bli aktuella beroende på omständigheterna.

Informationsplikt vid insamling

Vid insamling av personuppgifter är KMH skyldig att lämna följande information till den registrerade:

- identitet och kontaktuppgifter till den personuppgiftsansvarige,
- kontaktuppgifter till dataskyddsombudet,
- 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.

Informationsplikt gäller även om KMH inte samlar in uppgifterna direkt från den registrerade. Undantag kan göras om den registrerade sedan tidigare är informerad eller om det är praktiskt omöjligt eller mycket svårt att informera den det gäller. Ytterligare undantag kan göras om överföringen är föreskriven i lag.

Register över personuppgiftsbehandlingar upprättas

KMH är skyldig att hålla reda på vilka personuppgiftsbehandlingar som sker. Den som är ansvarig för en behandling är också skyldig att anmäla den till ett upprättat register där följande uppgifter noteras:

- Akademi/avdelning, namn och kontaktuppgifter till den som ansvarar för behandlingen.
- 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).

Roller och ansvar

Det är nödvändigt att **den som ansvarar för en behandling av personuppgifter** (t.ex. systemägaren till system eller en digital tjänst vid KMH, den som upprättat en behandling inom exempelvis sin forskning eller den student som samlar in uppgifter till sitt examensarbete) känner till de tillåtna grunderna, informationsplikten och följa principerna och registrera behandlingen.

Samtliga medarbetare förväntas hantera personuppgifter på ett korrekt sätt och ha kunskap om de regler som gäller för sina specifika arbetsuppgifter.

KMH som myndighet är **personuppgiftsansvarig** för all personuppgiftshantering inom verksamheten, från den enskilda studentens uppsatsarbete till forskningsprojekt och administrativa system.

Information om gällande regler finns, för såväl personal som studenter, på KMH:s hemsida.

När behandling av personuppgifter sker med stöd en tredje part (t.ex. Statens servicecenter) agerar denne som **personuppgiftsbiträde**. Förhållandet mellan biträde och ansvarig ska regleras genom ett **skriftligt avtal** och biträdet får endast behandla information enligt KMH:s instruktioner. De får således inte på egen hand behandla informationen utifrån egna önskemål. Vid fel och brister i hanteringen kan både personuppgiftsansvarig och personuppgiftsbiträdet drabbas av sanktionsavgifter (böter) som för svensk del bestäms av Integritetsskyddmyndigeten och utdöms av domstol.

KMH ska ha ett **dataskyddsombud** som internt ska granska hanteringen samt fungera som hjälp och stöd för verksamheten. Dataskyddsombudet ska också kunna ta emot frågor och klagomål från registrerade.

Den registrerades rättigheter

Alla, vars personuppgifter registreras, har

- rätt att få klar och tydlig information om behandlingen och om vilka uppgifter som behandlas (svar på en sådan begäran bör inte dröja mer än en månad men kan förlängas till tre om arbetet med att ta fram uppgifterna är komplicerat). Det ska normalt vara kostnadsfritt att få ut begärd information,
- rätt att få felaktig information rättad utan onödigt dröjsmål,
- rätt att få personlig information raderad eller behandlingen av den avslutad om den används längre än nödvändigt (om inte annat följer av lagkrav, som t.ex. hantering av allmänna handlingar eller behandling för forskningsändamål av allmänt intresse),
- rätt att få ut sin information digitalt så att denne exempelvis kan byta en tjänst mot en annan utan att förlora information,
- rätt att lämna klagomål till Integritetsskyddsmyndigheten som utreder och beslutar om eventuella sanktionsavgifter.

Övriga lagar styr också behandling av personuppgifter

Dataskyddsförordningen kompletteras dels av äldre lagar, dels av nya lagar som träder ikraft samtidigt med förordningen den 25 maj 2018.

Arkivlagen reglerar bevarande och raderande av allmänna handlingar medan tryckfrihetsförordningen, där offentlighetsprincipen finns, tillsammans med offentlighets- och sekretesslagen styr allmänhetens tillgång till allmänna handlingar. Arkivlagen och tryckfrihetsförordningen är av särskild vikt när det gäller rätten att bli glömd, då det finns bestämmelser som innebär att vissa uppgifter inte får raderas. I offentlighets- och sekretesslagen anges bland annat att allmänna handlingar ska registreras, vilket oftast innebär att personuppgifter behandlas. När en begäran inkommer måste den prövas inte bara utifrån dataskyddsförordningen utan även utifrån offentlighets- och sekretesslagen.

Vad KMH ska arkivera respektive får gallra (radera) styrs även av den lokala dokumenthanteringsplanen och Riksarkivets förskrifter.

Den lagliga grunden för behandlingen är i många fall de krav som ställs i högskolelagen eller högskoleförordningen, speciellt när det gäller uppgifter om studenter.

Lagkrav som kan utgöra laglig grund för behandling av personuppgifter finns även i förvaltningslagen. Detta rör främst serviceskyldighet och handläggning av ärenden. Här finns även bestämmelser om rätten att ta del av uppgifter om sig själv.

Dataskyddslagen (lag om kompletterande bestämmelser till EU:s dataskyddsförordning) kompletterar förordningen med vissa nationella bestämmelser (exempelvis att åldersgränsen för samtycke är 13 år). En särskild forskningsdatalag ska reglera användningen av personuppgifter inom forskningen. Den senare samverkar med lagen om etikprövning när det gäller hanteringen av känsliga personuppgifter för forskningsändamål.

Tillämpliga lagar, förordningar och föreskrifter

General Data Protection Regulation (EU) nr 2016/679)

Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning

Tryckfrihetsförordningen (1949:105)

Offentlighets- och sekretesslagen (2009:400)

Förvaltningslagen (2017:900)

Högskolelagen (1992:1434)

Högskoleförordningen (1993:100)

Lag (2003:460) om etikprövning av forskning som avser människor

Arkivlag (1990:782)

Riksarkivets föreskrifter och allmänna råd om arkiv hos statliga myndigheter (RA-FS 1997:4)

Riksarkivets föreskrifter och allmänna råd om gallring och återlämnande av handlingar vid universitet och högskolor (RA-FS2008:3)