BESLUT	Datum:	Diarienummer:
	2014-02-03	V-2014-0113

Beslutat av Anders Lundgren, förvaltningschef	Expeditionsdatum 2014-02-04
Föredragande Robin Roy, UF/AD	För åtgärd Regelverksgruppen
Övriga närvarande	För kännedom Dokumentsamordnare

Revidering av riktlinje nr 2/13

Beslut

Förvaltningschefen beslutar att reviderad riktlinje "Behandling av personuppgifter på KTH" (nr 2/13) ska gälla fr.o.m. 10 februari 2014.

Bakgrund

I riktlinje nr 2/13 förekom otydligheter , vilka är korrigerade i och med den reviderade riktlinjen.

I samband med revideringen har även stav- och grammatiska fel korrigeras.

Vid protokollet

Robin Roy

KTH
Universitetsförvaltning
Brinellvägen 8 | 100 44 Stockholm
08 790 60 00 | registrator@kth.se | www.kth.se

Behandling av personuppgifter på KTH

Riktlinje nr 2/ 13
Gäller fr.o.m. 2013-04-22
Reviderad 2014-02-03

Syfte

Syftet med riktlinjen är att ange de grundläggande kraven för behandling av personuppgifter som gäller för KTH enligt personuppgiftlagen (1998:204), PUL.

Kraven i riktlinjen är teknikneutrala och avser samtliga verksamhetsprocesser. Om det i PUL, annan lag eller förordning finns avvikande anvisningar äger dessa företräde.

Stöddokument till riktlinjen utfärdas separat.

Denna riktlinje grundar sig på:

- Personuppgiftslagen (1998:204)
- Personuppgiftsförordning (1998:1191)

Allmänt

KTH hanterar personuppgifter i olika grad i såväl stöd- (administration) som kärnprocesser (utbildning och forskning). De övergripande bestämmelserna som reglerar vad KTH får och inte får göra med personuppgifter finns i PUL.

PUL syftar till att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. [1] Lagen bygger på ett EU-direktiv.[2] Direktivet syftar till att underlätta det fria flödet av personuppgifter mellan EU:s medlemsländer samt uppnå en likvärdig hög nivå på skyddet av den personliga integriteten.

[1] jfr. KTH:s *Etisk policy* (Policy nr 5/2008) och 2 kap. 6 § andra stycket regeringsformen.

[2] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter

PUL ska tillämpas av personuppgiftsansvarig som är etablerad eller använder sig av utrustning som finns i Sverige. Bestämmelserna i PUL tillämpas inte om de skulle strida mot tryckfrihetsförordningen, yttrandefrihetsgrundlagen, offentlighetsprincipen eller andra lagar och förordningar. Undantag finns även när behandlingen omfattas av privata och journalistiska ändamål samt i konstnärligt eller litterärt skapande.

Begrepp

Nedan beskrivna begrepp förekommer i riktlinjen och har samma definition som i 3 och 13 §§ PUL.

Personuppgifter

Personuppgifter är all information som direkt eller indirekt kan hänföras till en fysisk och levande person. Exempel på personuppgifter är avbildningar/fotografier, KTH:s personliga e-postadresser, IP-adresser och krypterade eller kodade uppgifter (om dessa kan göras läsbara genom kodnyckel).

Känsliga personuppgifter

Känsliga personuppgifter är sådana som avslöjar hälsa (t.ex. uppgift om graviditet eller sjukhusbesök) eller sexualliv, ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse samt medlemskap i fackförening.

Behandling

Med behandling avses varje enskild åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter. Behandling kan vara t.ex. insamling, registrering, lagring, samkörning mellan olika system, överföring, bearbetning och analys.

Personuppgiftsansvarig

Den som ensam eller tillsammans med andra bestämmer varför och hur personuppgifter ska behandlas samt de tekniska och organisatoriska medlen för detta. Personuppgiftsansvarig ska se till att bestämmelserna i PUL efterföljs och har ett skadeståndssanktionerat ansvar. I regel är KTH, i egenskap av myndighet, personuppgiftsansvarig.

Personuppgiftsbiträde

Den som utanför den personuppgiftansvariges organisation behandlar personuppgifter för dennes räkning. Personuppgiftsbiträdet kan exempelvis vara ett företag som utför tester i laboratorium för KTH eller tillhandhåller molntjänster. Personuppgiftsbiträdet kan i sin tur anlita en eller flera underentreprenör/-er (sk. underbiträden).

Den registrerade

Den fysiska person som personuppgifterna avser (t.ex. anställd eller student).

Grundläggande krav

KTH ska som personuppgiftsansvarig alltid se till att följande grundläggande krav är uppfyllda (jfr. 9 § PUL):

- KTH ska endast behandla personuppgifter om det är lagligt.
- Behandlingen ska ske på ett korrekt sätt och enlighet med god sed (bl.a. enligt branschöverenskommelser och interna styrdokument).
- KTH ska endast samla in personuppgifter för särskilda, uttryckligt angivna och berättigade ändamål. Inga andra personuppgifter får därmed insamlas än vad som krävs för handläggning och övrig myndighetsutövning.
- De behandlade uppgifterna ska vara relevanta, riktiga och aktuella.
- Fler personuppgifter ska inte behandlas än vad som är nödvändigt med hänsyn till syftet.
- Felaktiga och ofullständiga personuppgifter ska med rimliga åtgärder rättas, blockeras eller utplånas.
- Personuppgifterna ska inte bevaras längre tid än vad som är nödvändigt med hänsyn till ändamålen om inte lag eller förordning föreskriver annat.

Tillåten behandling

För att en behandling av personuppgift ska vara tillåten ska KTH se till att de grundläggande kraven är uppfyllda samt att den registrerade har lämnat sitt samtycke. Samtycket ska lämnas innan behandlingen har påbörjats. En behandling utan ett samtycke, men som uppfyller de grundläggande kraven, är tillåten i situationer (10 § punkt a- f PUL):

- För att fullfölja ett avtal eller åtgärder som den registrerade begärt skall kunna vidtas innan ett avtal träffas.

- För att fullfölja rättsliga skyldigheter (t.ex. KTH:s åtagande vid avslut av anställning).

- För att skydda vitala intressen för den registrerade.

- För att utföra en arbetsuppgift av allmänt intresse (t.ex. arkivering och framställning av statistik).

- För att utföra en arbetsuppgift i samband med myndighetsutövning.

- Om behandlingen är nödvändig för ett ändamål som rör ett berättigat intresse hos den personuppgiftsansvarige eller hos en sådan tredje man till vilken personuppgifterna lämnas ut skall kunna tillgodoses. Detta under förutsättning att KTH:s intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten. Samråd bör i dessa fall göras med personuppgiftsombudet.

KTH ska försäkra sig om att samtycket uppfyller följande krav:

- Den registrerade ska ha ett fritt val att lämna samtycke.

- Samtycket ska vara en klar och uttrycklig viljeyttring från den registrerade, dvs. inte påtvingad, och med möjligheten att senare ta tillbaka denna.

- Samtycket måste avse behandling för ett eller flera angivna ändamål och får därför inte vara allmänt hållet.

- Det ska innehålla all nödvändig information, bl.a. hur uppgifterna kommer att behandlas och hur länge dessa sparas.
- Om samtycket återkallas får inte några ytterligare personuppgifter behandlas. De redan insamlade personuppgifterna får emellertid behandlas.

Information till den registrerade

Tydlig, begriplig och korrekt information till den registrerade ska självmant lämnas ut av KTH. Den utlämnade informationen kan begränsas om det i andra lagar eller förordningar finns bestämmelser om sekretess eller tystnadsplikt.

KTH ska lämna informationen i anslutning till att personuppgifter inhämtas från den registrerade, när uppgiften hämtas från en annan källa

(t.ex. externt system) eller när behandlingen i väsentliga delar förändras. Om personuppgifterna är avsedda att lämnas ut till någon annan än KTH eller till ett personuppgiftsbiträde (dvs. till sk. tredje man) ska informationen lämnas till den registrerade när uppgifterna lämnas ut för första gången.

Den information som KTH ska självmant delge är:

- Vem som är personuppgiftsansvarig och kontaktuppgifter.
- Ändamålet med behandlingen.
- Information om mottagare av uppgifterna.
- Rätt att få information efter ansökan.
- Hur länge uppgifterna kommer att sparas.
- Rätten att få felaktiga uppgifter blockerade och korrigerade.
- Information om möjligheten att ansöka om ett registerutdrag.
- Övrig information som är viktig för den registrerade att känna till.

Den registrerade har rätt att på egen begäran, en gång per kalenderår få information om pågående behandling av sina personuppgifter. Ansökan ska vara egenhändigt signerad och skickas till personuppgiftsombudet.

KTH behöver inte lämna ut information om insamlingen eller utlämnandet sker enligt annan lag eller förordning, om det som redan är känt av den registrerade eller om det skulle vara omöjligt eller innebära en oproportionellt stor arbetsbörda för KTH.

Känsliga personuppgifter och personnummer/samordningsnummer

KTH ska inte behandla känsliga personuppgifter eller uppgifter om lagöverträdelser om inte stöd finns i 15-19§§ PUL eller i annan lag eller förordning. De undantagna behandlingarna i PUL måste alltid uppfylla de grundläggande kraven (se kap. *Grundläggande krav* och *Tillåten behandling*). Känsliga uppgifter får inte behandlas endast med stöd av en intresseavvägning (se kap. *Tillåten behandling*). Enstaka känsliga uppgifter får behandlas av KTH i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggning (jfr. 8 § Personuppgiftsförordningen).

KTH ska se till att personnummer eller samordningsnummer endast används om den registrerade har lämnat sitt samtycke eller när det är klart motiverat med hänsyn till ändmålet med behandlingen, vikten av säker identifiering eller något annat beaktningsvärt skäl (jfr. 22 § PUL).

Personuppgiftsbiträde

KTH frånsäger sig inte sitt personuppgiftsansvar när ett personuppgiftsbiträde anlitas. Anlitas personuppgiftsbiträde ska KTH upprätta ett skriftligt personuppgiftsbiträdesavtal. I avtalet ska det tydligt framgå bl.a. att personuppgifterna endast får behandlas enligt KTH:s angivna instruktioner, lämpliga åtgärder som ska vidtas för att skydda personuppgifterna och skyldigheter för underentreprenörer. Bestämmelserna i avtalet ska anpassas till den specifika situationen och uppgifternas känslighet.

Personuppgiftsombudet bör i dessa fall kontaktas för samråd.

Säkerhet och överföring till annat land

KTH:s övergripande informations- och IT-säkerhet, se även Informations- och IT-säkerhet vid KTH.

KTH ska vid all behandling vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Säkerhetsåtgärderna på KTH ska vara anpassade till de tekniska möjligheter som finns (t.ex. inloggning, behörighetskontroll), kostnader för åtgärderna, de särskilda risker som finns samt uppgifternas känslighet.

En särskild bedömning ska av KTH göras i vissa situationer. Samråd bör göras med personuppgiftsombudet.

Särskild bedömning är aktuell när följande situationer föreligger:

- Ett större antal personer ingår i behandlingen.
- En större mängd uppgifter om varje person behandlas.
- Behandling som rör personer som inte är anställda vid KTH eller har annan närmare anknytning till KTH.
- Behandling av känsliga personuppgifter eller sekretessbelagda uppgifter enligt offentlighets- och sekretess lagen (2009:400).
- Innan en molntjänst ska tas i bruk.

KTH ska försäkra sig om att överföring till och digital behandling i en stat som inte är ansluten till EU eller EES (s.k. Tredje land) inte sker utan att den registrerade har lämnat sitt samtycke, överföringen är nödvändig eller om landet har en tillfredställande skyddsnivå.

Vid tveksamheter om digital överföring till, automatisk behandling och skyddsnivå i tredje land bör samråd göras med personuppgiftsombudet.

Personuppgiftsombudets roll och anmälan av behandling av personuppgifter

KTH:s personuppgiftsombud har till uppgift att:

- Utfärda stöddokument till föreliggande föreskrift.
- Självständigt se till att KTH behandlar personuppgifter på ett lagligt, korrekt sätt i enligt med god sed och påpeka brister.
- Anmäla till tillsynsmyndigheten (Datainspektionen) om bristerna inte åtgärdas.
- Hjälpa den registrerade med rättelse och information.
- Utbilda och informera anställda om PUL.
- Samråda med Datainspektionen vid tveksamheter om tillämpningar av PUL.
- Upprätta en förteckning över pågående behandlingar av personuppgifter.

En påbörjad och avslutad behandling av personuppgifter ska anmälas till personuppgiftsombudet på blanketten "Anmälan av behandling av personuppgifter" (blankettkod: JU-PUL). Anmälan ska inte göras för bl.a. personuppgifter i löpande text, om samtycke har lämnats från den registrerade eller om behandlingen har stöd i annan lag eller förordning.

Begäran om massuttag av personuppgifter

Enligt 21 kap. 7 § offentlighets- och sekretesslagen (2009:400) gäller sekretess för personuppgifter om det kan antas att uppgiften behandlas i strid med PUL. Bestämmelsen avser främst när en begäran inkommer om dels att få ta del av uppgifter från ett stort antal personer (s.k. massuttag), dels ett urval av personer med t.ex. vissa språkliga- och politiska tillhörigheter (s.k. selekterade uppgifter).

Samråd med personuppgiftsombudet bör i dessa fall göras innan ett utlämnade.

Övrig information

www.datainspektionen.se

Kontaktuppgifter till personuppgiftsombudet

Robin Roy

Universitetsförvaltningen/avdelningen för Dokumenthantering

Brinellvägen 8, 100 44 Stockholm

rroy@kth.se, 08-790 87 52, 070-778 87 52

Funktionsadress: personuppgiftsombud@kth.se