Ansvarig enhet
Universitetskansliet

Datum
2018-05-14

Dnr
LTU-1380-2018

Beslutsfattare: Rektor	Beslutsdatum: 2018-05-14
Dokumenttyp: Riktlinje	Träder i kraft: 2018-05-14
Giltighetstid: tillsvidare	Bör revideras före:2019-05-14
Dokument som upphävs:LTU-286-2012	

Riktlinjer för behandling av personuppgifter

1. Inledning

Inom ramen för verksamheten vid Luleå tekniska universitet behandlas personuppgifter i betydande omfattning och i många olika sammanhang.

Dataskyddsförordningen ”EU förordning 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter” ersätter Personuppgiftslagen (PuL) den 25 maj 2018.

Syftet med Dataskyddsförordningen är fortfarande att förhindra att människors personliga integritet kränks vid behandling av personuppgifter. De registrerade har dessutom ett antal rättigheter som personuppgiftsansvarig ska tillmötesgå.

Dataskyddsförordningen är subsidiär i förhållande till andra mer specifika lagbestämmelser i den mån det är tillåtet enligt dataskyddsförordningen. Detta innebär att regler i annan lagstiftning tar över bestämmelserna i Dataskyddsförordningen. Exempel på detta är regler om hur personuppgifter ska behandlas inom skatteförvaltningen, hälso- och sjukvården, socialtjänsten och polisen. Dataskyddsförordningen gäller inte för rent privat behandling av personuppgifter. Det finns dessutom undantag med hänsyn till offentlighetsprincipen samt tryck- och yttrandefriheten.

2. Syfte

Universitetets hantering och behandling av personuppgifter handlar om att tillgodose individers rättssäkerhet och anspråk på integritetsskydd tillvaratas på lagenligt och lämpligt sätt i samband med behandling av personuppgifter.

Dokumentet syftar till att ge stöd till samtliga universitetsanställda så att de på ett korrekt och lagenligt sätt ska kunna hantera personuppgifter i verksamheten.

3. Förhållningssätt

Vid behandling av personuppgifter gäller följande principer: Integritet och konfidentialitet, ansvarsskyldighet, laglighet, ändamålsbegränsning, uppgiftsminimering, korrekthet, lagringsminimering.

3.1 Integritet och konfidentialitet:

Personuppgifterna ska skyddas bland annat mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelser. Den som behandlar personuppgifter ska därför vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna

3.2 Ansvarsskyldighet:

Den som behandlar personuppgifterna ansvarar för att kunna visa efterlevnad av dataskyddsförordningen. Detta kan till exempel göras genom att ha tydlig information till de registrerade, att dokumentera de behandlingar som pågår i organisationen samt att ha interna riktlinjer.

3.3 Laglighet:

Personuppgifter får behandlas endast om behandlingen har laglig/rättlig grund:

- Samtycke: varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade godtar behandling av sina personuppgifter eller
- Behandlingen är nödvändig för att:
  - fullgöra ett avtal;
  - fullgöra en rättslig förpliktelse;
  - skydda intressen som är av grundläggande betydelse för den registrerade eller annan fysisk person;
  - utföra en uppgift av allmänt intresse;
  - myndighetsutövning;
  - tillgodose ett berättigat intresse hos den personuppgiftsansvarig, om inte detta intresse övervägs av de registrerades integritetsintresse, s.k. intresseavvägning.

3.4 Ändamålsbegränsning:

- Personuppgifter ska samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål (inte för allmänt hållna).
- Personuppgifter får inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in.
- Personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen.

3.5 Uppgiftsminimering:

Personuppgifter som behandlas ska inte vara fler än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

3.6 Korrekthet:

- Personuppgifter som behandlas ska vara riktiga och aktuella.
- Alla rimliga åtgärder ska vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till behandlingens ändamål.

3.7 Lagringsminimering:

Personuppgifter ska inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till behandlingens ändamål. Arkivlagen (1990:782) och fastställda gallringsrutiner ska följas.

Vid överföring av personuppgifter till tredje land ska stor restriktivitet iakttas, konsultera med Dataskyddsombudet i förväg.

4. Organisation

4.1 Personuppgiftsansvarig

Luleå tekniska universitet är personuppgiftsansvarig avseende all personuppgiftsbehandling inom universitetet. Detta gäller oavsett om personuppgifterna hanteras internt på universitetet eller om de behandlas av någon utomstående organisation, på uppdrag av universitetet - ett s.k. personuppgiftsbiträde.

För att erbjuda integritetsskydd och tillmötesgå de registrerades rättigheter ska Luleå tekniska universitet säkerställa att följande finns på plats:

- Inbyggt dataskydd (Privacy by design) och dataskydd som standard (Privacy by default) i personuppgiftsbärande stödsystem – Artikel 25
- Avtal med personuppgiftsbiträden – Artikel 28
- Registerförteckning över behandlingar - Artikel 30
- Samarbete med tillsynsmyndigheten (Integritetsskyddsmyndigheten) - Artikel 31
- Säkerhet – Artikel 32
- Rutin för anmälan om incident till tillsynsmyndighet – Artikel 33
- Information till de registrerade - Artikel 34

- Rutin för konsekvensbedömningar – Artikel 35
- Utsett Dataskyddsombud - Artikel 37

4.2 Universitetets dataskyddsombud

Vid universitetet finns ett av rektor utsett och till Datainspektionen anmält Dataskyddsombud med roll och uppgifter enligt artiklarna 37–39 i Dataskyddsförordningen. I personuppgiftsombudets uppgifter vid universitetet ingår att:

- lämna råd och anvisningar som rör tillämpningen av regelverket,
- underlätta efterlevnad genom bl.a. konsekvensbedömningar och revisioner,
- ingripa vid felaktiga behandlingar,
- samråda med Datainspektionen,
- hjälpa registrerade att utöva sina rättigheter avseende personuppgiftsbehandling.

Dataskyddsombudet ska se till att universitetets medarbetare är informerade om reglerna för personuppgiftsbehandlingar och anmälningsskyldigheten avseende rättelse, radering och begränsning av behandling på begäran från den registrerade. Dataskyddsombudet har det övergripande tillsynsansvaret.

5. Universitetets förteckning över behandlingar av personuppgifter

Universitetet ska upprätthålla en förteckning över de behandlingar av personuppgifter som äger rum vid universitetet. LTU:s förteckning återfinns på internwebben i ett särskilt utvecklat verktyg för att fortlöpande anmäla nya och avanmäla avslutade personuppgiftsbehandlingar. Dataskyddsombudet finns för stöd och rådgivning när det gäller behandlingar av personuppgifter som ska anmälas/avanmälas i förteckningen.

Innehållet i förteckningen över behandlingar av personuppgifter ska omfatta:

- Namn och kontaktuppgifter för personuppgiftsansvarig och Dataskyddsombudet.
- Ändamålen med behandlingen.
- Beskrivning av kategorierna av registrerade och kategorierna av personuppgifter.
- Kategorierna av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inkl. mottagare i tredjeländer eller i internationella organisationer.
- I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation.
- Om möjligt, de förutsedda tidsfristerna för radering.
- Om möjligt, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna.

Ostrukturerat lagrade personuppgifter omfattas av den nya dataskyddsförordningen:

- Personuppgifter i e-post, Excel, Word, Powerpoint, html, fritextfält på webben, osv.
- E-postserver, gemensamma filytor, webben, lokal hårddisk, osv.
- Dokument sparade i pärmar och arkiv

Det innebär att förteckningen även ska innehålla behandlingar av ostrukturerade personuppgifter.

6. Personuppgiftsbehandlaren

Med personuppgiftsbehandlare menas samtliga anställda vid universitetet som behandlar personuppgifter och därvid exempelvis upprättar personregister för insamling, lagring, bearbetning, spridning av personuppgifter i samband med administration, i forskningsprojekt eller eljest.

Personuppgiftsbehandlaren svarar för:

- att behandlingen av personuppgifter överensstämmer med principerna i Dataskyddsförordningen,
- att behandlingen av personuppgifter anmäls till LTU:s förteckning över behandlingar av personuppgifter,
- att den behandling av personuppgifter som äger rum överensstämmer med det ändamål för vilket uppgifterna samlats in samt med det ändamål som angivits i förteckningen,
- att registreringar som inte längre behövs eller är inaktuella avvecklas samt att felaktiga uppgifter rättas.

Prefekter respektive chefen för verksamhetsstödet bär det övergripande ansvaret för behandling av personuppgifter på resultatenheterna.

7. Personuppgiftsbiträdesavtal

Om någon utanför LTU:s organisation behandlar personuppgifter för LTU:s räkning ska LTU upprätta ett personuppgiftsbiträdesavtal med denna aktör – personuppgiftsbiträdet - innefattande instruktioner och riktlinjer från LTU om hur personuppgifterna ska behandlas.

8. Registerutdrag

Universitetet är skyldigt att en gång per kalenderår kostnadsfritt – till den som skriftligen ansöker om det - lämna besked om personuppgifter som rör den sökande behandlas eller inte. I sådana fall ska personuppgiftsansvarig lämna information om bl.a. följande:

- Namn och kontaktuppgifter till personuppgiftsansvarig.
- Kontaktuppgifter till dataskyddsombudet.
- Ändamålen med behandlingen.
- Den rättsliga grunden för behandlingen.
- Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna.
- Att personuppgiftsansvarig avser att överföra personuppgifter till ett tredjeland.
- Den period under vilken personuppgifterna kommer att lagras eller de kriterier som används för att fastställa denna period.
- Information om den registrerades rättigheter.

Information behöver däremot inte lämnas om personuppgifter i löpande text.

Arkiv- och registratur ombesörjer sammanställning och utskick av sådana registerutdrag som enskilda personer begär. Informationen ska lämnas inom en månad från det att begäran gjordes. Om det finns särskilda skäl för det, får informationen dock lämnas senast fyra månader efter ansökan. Som exempel på särskilda skäl kan nämnas att personuppgifterna är krypterade, att sökmöjligheterna är begränsade eller att det rör sig om många uppgifter som är uppdelade på flera olika register eller databaser.

9. Registrerades rättigheter

Förutom rätt till information och tillgång till personuppgifter som behandlas hos personuppgiftsansvarig, har de registrerade rätt till att:

1. Utan onödigt dröjsmål få felaktiga eller ofullständiga personuppgifter rättade.
2. Utan onödigt dröjsmål få personuppgifter raderade om:
    - Personuppgifterna inte längre är nödvändiga.
    - Den registrerade återkallar samtycket.
    - Personuppgifterna har behandlats på olagligt sätt.
3. Begära begränsning av behandlingen om:
    - Personuppgifterna inte är korrekta.
    - Behandlingen är olaglig men den registrerade motsätter sig radering.
    - Personuppgifterna inte längre behövs men den registrerade behöver dessa för att kunna göra gällande rättsligt anspråk.
4. Få sina personuppgifter flyttade till en annan personuppgiftsansvarig.
5. När som helst göra invändningar mot behandlingen om personuppgiftsansvarig inte kan visa berättigade skäl för att behandla personuppgifterna.
6. Inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inkl. profilering, med undantag för avtal, uttryckligt samtycke, myndighetsutövning eller annan bestämmelse i nationell rätt.

Den registrerade har även rätt att lämna klagomål till Integritetsskyddsmyndigheten om personuppgifterna inte behandlas enligt ovan.

Den registrerade ska skicka en skriftlig och undertecknad begäran till LTU för att begära ut, ändra eller radera sina personuppgifter (återkalla samtycket).

10. Riskanalys och konsekvensbedömning av dataskydd

När personuppgiftsbehandlingen sannolikt kan medföra högre risker än normalt för att den enskildes fri- och rättigheter kränks vid personuppgiftsbehandling, bör personuppgiftsansvarig se till att en riskanalys och konsekvensbedömning avseende dataskydd genomförs och innehåller bedömning av riskens ursprung, art, särdrag och allvar (Se vidare i Riktlinjer för riskanalys och konsekvensbedömning vid behandling av personuppgifter LTU-1172-2018)

11. Personuppgiftsincidenter

Säkerhetsincidenter som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring, obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats, ska rapporteras, dokumenteras, åtgärdas samt anmälas (Se vidare i Riktlinjer för rapportering av personuppgiftsincidenter LTU-1171-2018).

12. Definitioner

Personuppgiftsansvarig – är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

Personuppgifter – Varje upplysning som avser en identifierad eller identifierbar fysisk person (en registrerad), där en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till ett namn, ett ID-nummer, en lokaliseringsuppgift eller online identifikatorer eller faktorer som är specifika för personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Känsliga personuppgifter – Uppgifter som rör ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa eller sexualliv samt genetiska och biometriska uppgifter.

Strukturerade/ostrukturerade personuppgifter – Personuppgifter anses vara strukturerade när de ingår i eller är avsedda att ingå i en struktur som gör det påtagligt enklare att söka efter eller sammanställa uppgifterna, exempelvis register. Samma regler gäller alla typer av personuppgifter – missbruksregeln är borttagen i Dataskyddsförordningen.

Behandling – En åtgärd eller kombination av åtgärder för personuppgifter, oavsett om de utförs automatiserat eller ej, t.ex. insamling, registrering, organisering, strukturering, lagring,

bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Tredjelandsöverföring – Tredjeland är länder som inte är medlemmar i EU eller EES. Tredjelandsöverföring innebär när personuppgifter som behandlas i ett EU eller EES land tillgängliggörs i ett land utanför EU/EES land. Det anses inte som en tredjelandsöverföring om uppgifterna publiceras på en webbplats på Internet och webbplatsen lagras hos en internetleverantör som är etablerad inom EU.