Ansvarig enhet
Universitetskansliet

Datum
2018-05-14

Dnr
LTU-1171-2018

Beslutsfattare: Rektor	Beslutsdatum: 2018-05-14
Dokumenttyp: Riktlinje	Träder i kraft: 2018-05-14
Giltighetstid: tillsvidare	Bör uppdateras före: 2019-05-14

Riktlinjer för rapportering av personuppgiftsincidenter

1. Inledning och syfte

General Data Protection Regulation (GDPR) är en dataskyddsförordning som beslutades av EU under år 2016 och som ersätter den svenska personuppgiftslagen (PUL). GDPR träder i kraft som svensk lagstiftning den 25 maj 2018.

Syftet med dessa riktlinjer är att ge vägledning för hur personuppgiftsincidenter som sannolikt medför risker för fysiska personers fri- och rättigheter ska rapporteras/anmälas till Datainspektionen.

2. Rapportering av personuppgiftsincidenter

2.1 Omfattning

Riktlinjen omfattar rapportering av personuppgiftsincidenter som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring, obehörigt röjande eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats, när det inte är osannolikt att personuppgiftsincidenter medför risker för fysiska personers fri- och rättigheter.

2.2 Ansvarig

I enlighet med gällande delegationsordning bär prefekterna och chefen för verksamhetsstödet ansvaret för behandlingen av personuppgifter inom institutionen respektive verksamhetsstödet.

2.3 Personuppgiftsincident

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust, ändring, obehörigt röjande eller åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

En personuppgiftsincident kan medföra risker för människors fri- och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks, t.ex.

- Diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning

- Finansiell förlust
- Brott mot sekretess eller tystnadsplikt.

En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har blivit förstörda, gått förlorade på annat sätt eller kommit i orätta händer.

2.4 Tillämpning

2.4.1 Huvudregel

Vid en personuppgiftsincident ska den personuppgiftsansvarige anmäla incidenten till Datainspektionen inte senare än 72 timmar efter att ha fått vetskap om incidenten. Incidenten ska anmälas när det inte är osannolikt att den medför risk för fysiska personers fri- och rättigheter. Om anmälan inte görs inom 72 timmar ska en motivering till förseningen anges.

Denna regel gäller även om incidenten har inträffat hos ett personuppgiftsbiträde.

Universitetet ska dokumentera alla personuppgiftsincidenter, omständigheterna kring varje incident, dess konsekvenser och korrigerande åtgärder som har vidtagits. En personuppgiftsincident som inte har hanterats på ett lämpligt sätt kan leda till sanktionsavgifter och påverka förtroendet för universitetet.

Varje medarbetare som upptäcker en incident ska anmäla detta till Datainspektionen. Anmälan kan göras via en e-tjänst på Datainspektionens webbsida. Vid frågor om tillvägagångssättet vid anmälan går det att vända sig till Dataskyddsombudet på adressen dataskydd@ltu.se.

2.4.2 Anmälan om personuppgiftsincident

Anmälan om personuppgiftsincident ska åtminstone innehålla följande information:

- Personuppgiftsincidentens art, kategorier och ungefärliga antalet av både registrerade och personuppgiftsposter som berörs
- Namnet och kontaktuppgifter till Dataskyddsombudet eller annan som har information om personuppgiftsincidenten
- Sannolika konsekvenser av personuppgiftsincidenten
- Åtgärder som har vidtagits eller föreslagits, inklusive åtgärder för att mildra incidentens potentiella negativa effekter, när lämpligt.

2.4.3 Information till den registrerade

Om personuppgiftsincidenten sannolikt leder till risker för fysiska personers fri- och rättigheter, ska universitetet utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten. Information till den registrerade ska innehålla en tydlig och klar beskrivning av incidentens art samt:

- Namnet och kontaktuppgifterna till Dataskyddsombudet eller annan som har information om personuppgiftsincidenten
- Beskrivning av konsekvenserna av personuppgiftsincidenten
- Beskrivning av åtgärder som har vidtagits eller föreslagits

Information till den registrerade krävs inte om något av följande villkor är uppfyllda:

- Universitetet har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder som har tillämpats på personuppgifterna som påverkades av inträffad personuppgiftsincident (t.ex. kryptering)
- Universitetet har vidtagit ytterligare åtgärder som säkerställer att den höga risken för registrerades fri- och rättigheter sannolikt inte längre kommer att uppstå
- Information till den registrerade skulle inbegripa oproportionell ansträngning.