Ansvarig enhet
Universitetskansliet

Datum
2018-05-14

Dnr
LTU-1172-2018

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

Riktlinjer för riskanalys och konsekvensbedömning vid behandling av personuppgifter

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 med träder i kraft som svensk lagstiftning den 25 maj 2018.

Syftet med dessa riktlinjer är att ge vägledning för hur riskanalys och konsekvensbedömning ska genomföras och vad den ska innehålla, så att lagstadgade krav efterlevs.

2. Riskanalys och konsekvensbedömning

2.1 Allmänt

Riskanalys ska göras för att säkerställa att personuppgiftsbehandling (behandling) inte är förenad med särskilda risker för enskildas fri- och rättigheter. Konsekvensbedömning ska göras för att minimera hög risk för enskilda personers fri- och rättigheter.

2.2 Omfattning

Riktlinjen gäller för riskanalys och konsekvensbedömning innan en ny behandling inleds, om risken med pågående behandling har ändrats samt för befintliga behandlingar som saknar tidigare genomförda riskanalyser och konsekvensbedömningar.

2.3 Ansvarig

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

2.4 Tillämpning

2.4.1 Huvudregel

Huvudregeln är att riskanalys ska göras så tidigt som möjligt för att säkerställa att behandling inte innebär risker att enskildas fri- och rättigheter kränks. Om behandling sannolikt leder till en hög risk för enskilda personers fri- och rättigheter ska en konsekvensbedömning göras.

2.4.2 Riskanalys

Riskanalys ska genomföras för att analysera och dokumentera vilka risker behandlingen kan innebära och för att föreslå lämpliga säkerhetsåtgärder. Utifrån riskanalysen ska det dokumenteras och bedömas om en konsekvensbedömning behöver göras eller inte. Om ett beslut innebär att en konsekvensbedömning inte ska göras ska anledningarna till beslutet dokumenteras och motiveras. I konsekvensbedömning ska alltid genomföras i tveksamma fall.

Riskanalysen ska utgå från den enskildes personliga integritet och innehålla en beskrivning av:

- Händelsen och varför den innebär en potentiell risk.
- Hur sannolikt det är att händelsen inträffar.
- Hur allvarliga konsekvenserna blir om händelsen inträffar.

Förutom risken för den enskildes personliga integritet ska risken för överträdelse av andra grundläggande rättigheter bedömas, till exempel:

- Yttrandefrihet
- Tankefrihet
- Fri rörlighet
- Förbud mot diskriminering
- Rätt till frihet, samvete och religion

2.4.3 Konsekvensbedömning

Om behandlingen sannolikt leder till en hög risk för enskilda personers fri- och rättigheter ska en konsekvensbedömning utföras. Nedan följer exempel på behandlingar när konsekvensbedömning behöver utföras (exempel 3-11 är från Artikel 29-gruppen):

1. Automatiskt beslutsfattande som grundar sig på en systematisk och omfattande bedömning av människors personliga aspekter, till exempel profilering.
2. Behandling av uppgifter om lagöverträdelser eller känsliga personuppgifter, till exempel uppgifter om hälsa, religiös tro, politisk uppfattning eller etniskt ursprung, i stor omfattning.
3. Behandlingen innebär element av bedömning eller värdering (t.ex. automatiserade kreditbedömningar).
4. Behandlingen syftar till att fatta automatiserade beslut med rättsliga följder eller liknande för den registrerade (t.ex. om behandlingen riskerar att leda till att vissa personer utesluts eller diskrimineras).

5. Behandlingen omfattar känsliga personuppgifter (inbegriper även typer av personuppgifter som inte räknas upp i dataskyddsförordningens artikel 9.1, t.ex. betaluppgifter som kan användas för att begå bedrägeri).
6. Behandlingen innebär att personuppgifter behandlas i stor skala (med beaktande av antalet registrerade som berörs, volymen av uppgifter eller bredden av personuppgiftstyper, behandlingens varaktighet och den geografiska omfattningen av personuppgiftsbehandlingen).
7. Behandlingen innefattar samkörning av uppgifter mellan olika register.
8. Behandlingen om fattar personuppgifter om särskilt utsatta eller skyddsvärda typer av registrerade.
9. Personuppgifterna behandlas på ett innovativt sätt (innefattande behandling med ny teknik) eller för att tillämpa tekniska eller organisatoriska lösningar (t.ex. vid kombinerande av fingeravtryck och ansiktsavläsning för fysisk behörighetskontroll).
10. Personuppgifter ska föras över till ett land utanför EES.
11. Personuppgiftsbehandlingen i sig förhindrar registrerade från att utöva en rättighet eller att använda en tjänst eller ett avtal.

Datainspektionen kan komma att ta fram fler exempel på behandlingar som omfattas av kravet på konsekvensbedömningar.

Konsekvensbedömning ska **alltid** innehålla följande fyra delar:

1. Systematisk beskrivning av den planerade behandlingen och dess syfte.
2. Bedömning av om behandlingen är nödvändig och proportionerlig i förhållande till dess syfte.
3. Bedömning av riskerna för de registrerades rättigheter och friheter.
4. Åtgärder som planeras för att hantera riskerna och för att vida att lagstiftningen efterlevs.

Den personuppgiftsansvarige ska **alltid** samråda med Integritetsskyddsmyndigheten före behandlingen när konsekvensbedömningen visar att den skulle leda till en hög risk om inte riskminimerande åtgärder vidtas. Dataskyddsombudet ska **alltid** kontaktas för rådgivning. Sanktionsavgifter kan påföras om dataskyddsombudet inte rådfrågats, om den personuppgiftsansvarige inte samrått med tillsynsmyndigheten samt om de fyra obligatoriska delarna i konsekvensbedömningen inte inkluderats.

Det kommer att finnas en e-tjänst för att begära förhandssamråd på Datainspektionens webbplats.

Synpunkter, om vilka möjliga risker och konsekvenser som kan finnas med behandlingen ska inhämtas från de registrerade eller deras företrädare, när det är lämpligt. Är det inte lämpligt att inhämta eller följa synpunkter från de registrerade ska det motiveras. Om den personuppgiftsansvarige och de registrerade inte har samma syn på behandlingen ska det dokumenteras. Detta gäller särskilt om den personuppgiftsansvarige väljer att gå vidare med behandlingen.

2.4.4 En konsekvensbedömning för flera behandling

En enda konsekvensbedömning kan användas för att bedöma flera behandlingar som liknar varandra vad gäller art, omfattning, innehåll, ändamål och risker. Om man vill införa en behandling som liknar en annan där det redan finns en konsekvensbeskrivning kan den första bedömningen användas som referens i den nya konsekvensbedömningen. Att liknande teknik används för att samla in samma typ av uppgifter för samma ändamål kan också leda till att endast en konsekvensbedömning behöver göras. Det ska motiveras varför en enda konsekvensbedömning har använts.

2.4.5 Kontinuerlig omprövning av konsekvensbedömning

Bedömning av riskerna ska omprövas flera gånger under behandlingsprocessen. Detta gäller särskilt när behandlingen förändras på ett sätt som kan påverka risken, till exempel om fler uppgifter samlas in. Detta gäller även framtagningar av nya tekniska lösningar.

2.4.6 Roller och ansvar under konsekvensbedömningen

Följande roller har ansvar under genomförande av konsekvensbedömningen

- Personuppgiftsansvarige (dvs. universitetet) har yttersta ansvaret för att en konsekvensbedömning genomförs
- Dataskyddsombudet har ansvar för att ge råd och övervaka.
- Personuppgiftsbiträde ansvarar för att hjälpa till och bidra med information om behandlingen helt eller delvis ska genomföras av personuppgiftsbiträdet.
- Den registrerade har ansvar för att lämna synpunkter när det är lämpligt.