UPPSALA
UNIVERSITET

2018-05-24

Dataskyddsförordningens grundläggande principer

Den 25 maj 2018 ersätts svenska personuppgiftslagen (PUL) av Europeiska Unionens dataskyddsförordning, på engelska kallad ***General Data Protection Regulation (GDPR)***[1]**.** Dataskyddsförordningen ställer högre krav på behandling av personuppgifter, och sanktionerna vid överträdelser är betydligt hårdare än dagens reglering. Om Uppsala universitet inte följer de grundläggande principerna i dataskyddsförordningen i sin behandling av personuppgifter innebär det att en sådan överträdelse kan under vissa omständigheter medföra att de högre administrativa sanktionsavgifterna utdöms.

Här nedan finner du information om vilka principer som gäller och ska appliceras på alla personuppgiftsbehandlingar. Ha alltid dessa i bakhuvudet när du hanterar personuppgifter, som en vägledning.

Principerna

All behandling av personuppgifter måste, utöver att ha minst en laglig grund, även uppfylla de grundläggande principer som anges i dataskyddsförordningen. Principerna innebär bland annat att personuppgifter bara får samlas in för berättigade ändamål som inte är alltför allmänt hållna och att mängden uppgifter ska begränsas till vad som är nödvändigt för ändamålen. Uppgifterna får inte senare behandlas på ett sätt som är oförenligt med dessa ändamål och inte heller sparas längre än nödvändigt. Den som behandlar personuppgifter ska kunna visa att principerna följs. Principerna ska iakttas vid all behandling. Den som behandlar personuppgifter måste därför ha rutiner för att se till att de följs.

De sex grundläggande principerna är:

- Principen för laglighet, korrekthet och öppenhet
- Principen om ändamålsbegränsning
- Principen för uppgiftsminimering
- Principen om riktighet
- Principen om lagringsminimering, och
- Principen för integritet och konfidentialitet.

Laglighet, korrekthet och öppenhet (Eng. lawfulness, fairness and transparency)

Personuppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.

Kravet på att behandlingen av personuppgifter ska vara **laglig** innebär bland annat att det måste finnas en rättslig grund för behandlingen.

[1] Europarlamentets och Rådets förordning (EU) 2016/79 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Kravet på en **korrekt behandling** förutsätter att de registrerade får kännedom om behandlingen, det vill säga att de informeras i enlighet med regleringen i dataskydds-förordningen. Korrekthet skulle även kunna innebära att man inte får använda dolda arrangemang för att samla in uppgifter utan att den registrerade känner till det. t.ex. telefonavlyssning eller utvecklar och använder hemliga behandlingsmetoder.

Kravet på **öppenhet** innebär bland annat att det ska vara klart och tydligt för en registrerad person hur hans eller hennes personuppgifter samlas in och i övrigt behandlas. De registrerade måste därför få information om behandlingen, exempelvis efter begäran om registerutdrag få informationen på ett lättillgängligt sätt och formulerat med ett klart och tydligt språk.

Ändamålsbegränsning (Eng. purpose legitima)

Alla personuppgifter ska enligt dataskyddsförordningen bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. De på förhand fastställda ändamålen är det som sätter ramarna för behandlingen. De ska vara tydliga och legitima och ha bestämts vid den tidpunkt då personuppgifterna samlades in. Det finns inte någon möjlighet att skjuta upp bestämmandet av ändamålet till ett senare tillfälle och ett ändamål kan inte läggas till efteråt.

Ändamålen ska dokumenteras skriftligt och den registrerade ska få information om ändamålen både när uppgifterna samlas in och annars när denne begär det. Om de insamlade personuppgifterna senare ska behandlas för andra ändamål som är förenliga med de ursprungliga ändamålen måste de registrerade också informeras om detta. De insamlade personuppgifterna får behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål utan att det anses oförenligt med de ursprungliga ändamålen om det finns lämpliga skyddsåtgärder för de registrerades rättigheter.

Ändamålen kan även finnas i lagstiftning i vissa fall varvid den personuppgiftsansvarige har att följa den regleringen. Oavsett om ändamålen fastställts i författning eller inte är det dock alltid den personuppgiftsansvarige som ansvarar för, och ska kunna visa, att de grundläggande principerna följs. Det är den personuppgiftsansvarige som är ansvarig för att behandlingen enbart sker för de angivna ändamålen. Vid en tvist är det denne som har bevisbördan eftersom det är den personuppgiftsansvarige som i första hand bestämmer ändamålen.

Uppgiftsminimering (Eng. data minimisation)

Principen om uppgiftsminimering innebär att personuppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Det är med andra ord inte tillåtet att samla in personuppgifter för obestämda framtida behov. Insamlade personuppgifter får inte heller behandlas om de till exempel är så gamla att de inte längre är relevanta för de ursprungliga ändamålen.

Att personuppgifterna inte ska vara för omfattande i förhållande till de ändamål för vilka de behandlas innebär att de ska vara begränsade till vad som är nödvändigt för de ändamål som de behandlas för. Detta kräver i synnerhet att det tillses att den period under vilken

personuppgifterna lagras är begränsad till ett strikt minimum. Samla varken in mer eller mindre personuppgifter, eller ovidkommande uppgifter, än vad som verkligen behövs i förhållande till ändamålet med behandlingen. Ett rättesnöre kan vara att du ska kunna förklara varför de olika uppgifterna behövs för att uppfylla ändamålen med behandlingen.

Detta kan även i praktiken betyda att den personuppgiftsansvarige som t.ex. använder fritextfält för något visst ändamål via internet bör utfärda skriftliga instruktioner om vilken information som är relevant att lämna i fältet. För att säkerställa att personuppgifter inte sparas längre än nödvändigt finns inom Uppsala universitet tidsfrister för radering för regelbunden kontroll.

Korrekthet (eng. accuracy)

Personuppgifter ska vara korrekta och uppdaterade. Den som behandlar personuppgifter måste vidta alla rimliga åtgärder för att säkerställa att felaktiga personuppgifter raderas eller rättas utan dröjsmål. Om det krävs för ändamålen ska personuppgifterna dessutom vara uppdaterade. Det betyder att den personuppgiftsansvariga behöver vara aktiv för att säkerställa personuppgifternas kvalitet och att inte vänta med att agera förrän den registrerade utnyttjar sin rätt till rättelse av bl.a. felaktiga personuppgifter. Omständigheterna i varje enskilt fall såsom t.ex. ändamålen med behandlingen, hur många personuppgifter som behandlas och vilka konsekvenser en felaktig uppgift kan få för den registrerade kan vara faktorer som beaktas. Om det är nödvändigt att uppgifterna är uppdaterade torde avgöras med hänsyn till ändamålen med behandlingen.

Lagringsminimering (eng. storage limitation)

Personuppgifter får inte sparas, det vill säga förvaras i en form som möjliggör identifiering av den registrerade, under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. När personuppgifterna inte längre behövs för de ändamålen ska de raderas eller avidentifieras. För att säkerställa att personuppgifter inte sparas längre än nödvändigt bör den som behandlar personuppgifter införa tidsfrister och rutiner för radering eller avidentifiering.

De insamlade personuppgifterna får lagras under längre tid för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål om det finns lämpliga skyddsåtgärder för de registrerades rättigheter.

Det krävs också enligt dataskyddsförordningen att den personuppgiftsansvarige ska tillhandahålla information till de registrerade bl.a. den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period. Detta gäller oavsett om personuppgifterna kommer från den registrerade själv eller inte, dvs. om de har erhållits från någon annan. Samma information ska även ges om den registrerade begär ett registerutdrag.

UPPSALA
UNIVERSITET

2018-05-24

Integritet och konfidentialitet (Eng. integrity and confidentiality)

Personuppgifterna ska skyddas bland annat mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Den som behandlar personuppgifter ska därför vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna. Personuppgifter ska således behandlas på ett sätt som säkerställer lämplig säkerhet och konfidentialitet för personuppgifterna samt förhindrar obehörigt tillträde till och obehörig användning av personuppgifter och den utrustning som används för behandlingen.

Integritet i detta sammanhang är en säkerhetsprincip med innebörden att personuppgifterna inte förändras eller förstörs av misstag varken av en obehörig person eller av processen. Konfidentialitet är också en säkerhetsprincip som innebär att informationen inte görs tillgänglig eller avslöjas för obehörig person eller process. Båda begreppen ingår i generell informationssäkerhet.

Ansvarsskyldighet (Eng. accountability)

Den som behandlar personuppgifter ansvarar för att principerna om personuppgiftsbehandling följs och måste kunna visa på vilket sätt man följer dem. Det finns flera sätt att visa detta, till exempel genom att ha tydlig information till de registrerade, att dokumentera de behandlingar som pågår i organisationen och de överväganden man har gjort samt att ha dokumenterade interna riktlinjer för dataskyddet, en dataskyddspolicy. Dataskyddsombudet kontrollerar organisationens efterlevnad av förordningen och de interna riktlinjerna, vilket också är ett sätt att uppfylla kravet på ansvarsskyldighet.