UPPSALA
UNIVERSITET

2018-05-24

Hantering av personuppgiftsincidenter

Den 25 maj 2018 ersätts svenska personuppgiftslagen (PUL) av Europeiska Unionens dataskyddsförordning, på engelska kallad *General Data Protection Regulation* (GDPR)[1]. Genom förordningen införs en skyldighet för den som är personuppgiftsansvarig[2] att anmäla till Datainspektionen om det inträffat en personuppgiftsincident.

Den personuppgiftsansvarige är även skyldig att informera den registrerade[3] om den inträffade personuppgiftsincidenten. Även personuppgiftsbiträden[4] har en skyldighet att rapportera personuppgiftsincidenter, men då till den personuppgiftsansvarige som ska anmäla incidenten till datainspektionen. Hur personuppgiftsbiträdes ansvar ser ska regleras i ett så kallat personuppgiftsbiträdesavtal, PUBA.

Uppsala universitet kan agera som personuppgiftsansvarig eller som personuppgiftsbiträde och har därmed ansvar för att anmäla antingen till den personuppgiftsansvarige eller till Datainspektionen, beroende av hur det enskilda fallet ser ut.

Rutiner

Uppsala universitet måste ha tydliga och effektiva rutiner för att kunna uppfylla dataskyddsförordningens krav på anmälan av personuppgiftsincidenter. För att fastställa om en personuppgiftsincident har ägt rum och vid behov skyndsamt informera Datainspektionen och den registrerade krävs även en redovisning av hur lämpliga tekniska och organisatoriska åtgärder har vidtagits.

Det är av stor vikt att ha säkerhetslösningar på plats för att undvika incidenter. Detta kan uppnås genom att säkerställa att IT-system innehåller funktioner som uppmärksammar incidenter snabbt och ger en god överblick över sådan information som ska rapporteras till Datainspektionen för att hinna göra anmälan i tid. Vidare ska personuppgiftsbiträdesavtal reglera hur personuppgiftsincidenter ska anmälas till Uppsala universitet. Enligt dagens lösning är IT-avdelningen ansvarig för att sammanställa och rapportera den information som krävs för dataskyddsombudet ska kunna göra en bedömning av om personuppgiftsincidenten medför en hög risk för fysiska personers rättigheter och friheter.

---

[1] Europaparlamentets 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).

[2] Personuppgiftsansvarig är den som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen.

[3] De vars personuppgifter blir behandlade kallas för de registrerade.

[4] Personuppgiftsbiträde är en aktör som behandlar personuppgifter för någon annans räkning.

UPPSALA
UNIVERSITET

2018-05-24

Personuppgiftsincident

En personuppgiftsincident definieras i dataskyddsförordningen som en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.[5] Blir du medveten om en incident av detta slag är det viktigt att du skyndsamt kontaktar IT-avdelningen på it-incident@uu.se. IT-avdelningen kommer i sin tur att avgöra om incidenten ska anmäla till Datainspektionen.

Anmälan och dess innehåll

Kravet på att en anmälan ska göras till Datainspektionen syftar till att på ett snabbt och lämpligt sätt åtgärda och minska risken för att den registrerade lider fysisk, materiell eller immateriell skada. Dessa skador kan t.ex. vara förlust av kontrollen över de egna personuppgifterna, begränsning av de registrerades rättigheter, diskriminering, identitetsstöld, bedrägeri, skadat anseende eller ekonomisk förlust.[6]

Vid upptäck av en personuppgiftsincident ska Uppsala universitet, utan onödigt dröjsmål och inom 72 timmar göra en anmälan till Datainspektionen. Om det inte är möjligt att lämna *all* information inom 72 timmar kan man dela upp det och lämna uppgifter vid olika tillfällen allt eftersom det blir möjligt. Det är viktigt att förse Datainspektionen med så mycket information som möjligt så skyndsamt som möjligt.

Hinner universitetet inte göra anmälan alls inom 72 timmar ska man informera Datainspektionen och ange skälen för förseningen. I de fall universitetet är personuppgiftsbiträde ska den personuppgiftsansvarige underrättas utan onödigt dröjsmål efter att ha fått vetskap om personuppgiftsincidenten. Det personuppgiftsbiträdesavtal som reglerar behandlingen som biträdet utför åt den ansvarige reglerar mer detaljerat vilka skyldigheter biträdet har vid en personuppgiftsincident.

En anmälan ska enligt förordningen innehålla:

- Vilken typ av incident det är fråga om.
- Vilka kategorier av personer som kan komma att beröras.
- Hur många personer incidenten berör.
- Vilka konsekvenser incidenten kan få.

[5] Behandling innebär en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom 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.
[6] Skäl 85 dataskyddsförordningen.

- Vilka åtgärder man vidtagit för att motverka eventuella negativa konsekvenser för de registrerade.

Information till de som kan drabbas

Om incidenten sannolikt leder till en hög risk för den registrerades rättigheter och friheter, ska de registrerade utan onödigt dröjsmål informeras om personuppgiftsincidenten. Syftet med att informera är att den registrerade ska kunna vidta försiktighetsåtgärder.

Huruvida incidenten sannolikt innebär en risk för de registrerade och riskens allvar bör bedömas utifrån behandlingens art, omfattning, sammanhang och ändamål. Utvärderingen av huruvida personuppgiftsbehandlingen medför hög risk ska ske objektivt. Med hög risk avses enligt dataskyddsförordningen en särskild risk för menlig inverkan på registrerades rättigheter och friheter. Denna bedömning görs av IT-avdelningen efter att anmälan skett till it-incident@uu.se.

När Uppsala universitet anser att skyldigheten att informera de registrerade föreligger, ska informationen innehålla:

- En tydlig och klar beskrivning av personuppgiftsincidentens art.
- Namnet på och kontaktuppgifterna till Dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas.
- De sannolika konsekvenserna av personuppgiftsincidenten.
- En beskrivning av de åtgärder som den personuppgiftsansvariga har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet (när så är lämpligt), åtgärder för att mildra dess potentiella negativa effekter.

Uppsala universitet behöver dock inte informera de registrerade om någon av följande omständigheter föreligger:

- Om universitet har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som ska göra uppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till personuppgifterna, såsom kryptering.
- Om universitetet har vidtagit ytterligare åtgärder som säkerställer att den höga risken för registrerades rättigheter och friheter sannolikt inte längre kommer att uppstå.
- Om det skulle innebära en oproportionell ansträngning. I så fall ska universitetet i stället informera allmänheten eller vidta en liknande åtgärd genom vilken de registrerade informeras på ett lika effektivt sätt.

UPPSALA
UNIVERSITET

2018-05-24

Krav på dokumentation

Alla personuppgiftsincidenter ska dokumenteras, då särskilt omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen är avgörande för att universitetet ska kunna visa för Datainspektionen att myndigheten har vidtagit de åtgärder som krävs för att leva upp till de skyldigheter som följer av dataskyddsförordningen.

Dokumentationen kan användas som underlag för hur säkerheten i verksamheten kan förbättras. Man kan då säkerställa att nödvändiga åtgärder vidtagits i syfte att förhindra nya och liknande incidenter.

Upprättande av rutiner

För att följa dataskyddsförordningens bestämmelser är det viktigt att upprätta rutiner för att upptäcka, rapportera och utreda personuppgiftsincidenter. Ett led i detta arbete är att utse en eller flera personer som ska hantera personuppgiftsincidenter och ansvara för att hanteringen går rätt till.

Man bör fastställa format och förfaranden för anmälan av personuppgiftsincidenter. När detta görs bör man ta hänsyn till omständigheterna kring incidenten, däribland om personuppgifterna är skyddade av lämpliga tekniska skyddsåtgärder, som betydligt begränsar sannolikheten för identitetsbedrägeri eller andra former av missbruk.

Anmälan av personuppgiftsincidenter

Om du misstänker eller upptäcker en personuppgiftsincident är det viktigt att du så fort som möjligt meddelar detta till it-incident@uu.se så att IT-avdelningen kan utreda och vid behov anmäla detta till Datainspektionen. Märk ditt e-postmeddelande med PERSONUPPGIFTSINCIDENT och var tydlig med dina kontaktuppgifter så att Dataskyddsombudet kan komma i kontakt med dig.