HÖGSKOLAN
I HALMSTAD

Hantering av personuppgiftsincidenter vid Högskolan i Halmstad

Fastställd av högskoledirektör 2018-06-21, dnr L 2018/83

Bakgrund

Dataskyddsförordningen, (EU) 2016/679, ställer krav på hur Högskolan i Halmstad hanterar personuppgiftsincidenter.

En personuppgiftsincident är, enligt förordningen, 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.

Exempel på personuppgiftsincidenter är om någon obehörig fått tillgång till personuppgifter, utrustning som innehåller personuppgifter stulits, någon obehörig har ändrat personuppgifter, eller om personuppgifter inte är tillgängliga för den som behöver dem, och det får negativa effekter för den registrerade.

Anmälan av personuppgiftsincident

Anställda, studenter, personuppgiftsbiträden och andra som upptäcker en personuppgiftincident ska snarast, dock inom 24 timmar, anmäla denna till epostadressen dataskydd@hh.se. Anmälan hanteras av arbetsgruppen för dataskydd. Arbetsgruppens beslut om eventuella vidare åtgärder ska dokumenteras.

Om arbetsgruppen bedömer att incidenten kommer att medföra en risk för de registrerade ska rapport skickas till tillsynsmyndigheten inom 72 timmar från att incidenten upptäcktes. Dröjer anmälan till tillsynsmyndigheten längre, ska anmälan ändå göras, men förseningen motiveras.

Anmälan till tillsynsmyndigheten ska utföras enligt tillsynsmyndighetens rutiner, och ska innehålla åtminstone följande uppgifter:

- Personuppgiftsansvarig:
    - Organisationens namn, kontaktuppgifter
- Namn på personuppgiftsbiträden, underbiträden
- Kontaktuppgifter till den person som Datainspektionen kan kontakta
- Beskrivning av personuppgiftsincidenten
    - Har personuppgiftsincidenten medfört en risk för de registrerades fri- och rättigheter?
    - När inträffade personuppgiftsincidenten och när upptäcktes den?
    - Vad har hänt vid personuppgiftsincidenten?
    - Hur upptäckte ni personuppgiftsincidenten?
    - Varför inträffade personuppgiftsincidenten enligt din eller organisationens uppfattning?
    - Inom vilken akademi/avdelning inträffade personuppgiftsincidenten?
- Personuppgifterna och de registrerade
    - Hur många registrerade har påverkats?
    - Hur många personuppgiftsposter har personuppgiftsincidenten påverkat?
    - Vilka grupper tillhör de registrerade?
    - Vilken sorts personuppgifter berörs av personuppgiftsincidenten?
    - Var personuppgifterna krypterade?

- Konsekvenser
    - Vad kan bli konsekvenserna av personuppgiftsincidenten?
    - Hur allvarlig bedömer ni att personuppgiftsincidenten är?
- Information till de registrerade
    - Har ni informerat de registrerade om personuppgiftsincidenten? När?
    - Kommer ni att informera de registrerade? När? Om inte, varför?
- Sen anmälan
    - Om anmälan kommer in senare än 72 timmar – beskriv varför den kommer sent.
- Om ni kommer att komplettera anmälan, beskriv varför.
- Om du har skrivit något som du anser bör omfattas av sekretess, specificera.

Informationen i anmälan får lämnas till tillsynsmyndigheten i omgångar, dock inom två veckor, om inte all information finns tillgänglig vid tiden för anmälan.

Högskolan ska dokumentera alla personuppgiftsincidenter (vad som hänt, eventuella effekter av incidenten och de åtgärder som vidtagits för att minska konsekvenser och upprepning). En sammanfattning av denna dokumentation ska bifogas den årliga rapporten till Högskolestyrelsen kring Högskolans informationssäkerhet.

Information till den registrerade

Om arbetsgruppen bedömer att incidenten sannolikt leder till en hög risk för de registrerades fri- och rättigheter ska även de registrerade snarast informeras.

Informationen ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och åtminstone innehålla

- en klar och tydlig beskrivning av orsaken till personuppgiftsincidenten,
- namn och kontaktuppgifter till dataskyddsombudet, eller till någon annan person som är insatt i frågan och kan svara på frågor,
- en beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten,
- en beskrivning vad Högskolan har gjort, eller tänker göra, för att hantera personuppgiftsincidenten, och i förekommande fall,
- en beskrivning av vad Högskolan har gjort för att mildra eventuella negativa effekter.

Högskolan behöver inte informera de registrerade om incidenten om

a) Högskolan har tillämpat lämpliga tekniska och organisatoriska skyddsåtgärder 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.
b) Högskolan har vidtagit ytterligare åtgärder som säkerställer att någon hög risk för de registrerades rättigheter och friheter sannolikt inte längre kommer att uppstå.
c) att informera skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.