HÖGSKOLAN I GÄVLE

STYRDOKUMENT

Dokumenttyp: Rutin
Ärendenummer: HIG-STYR 2022/61
Beslutat av: Förvaltningschef
Beslutsdatum: 2023-03-21
Giltighetstid: Tillsvidare

Rutin för hantering av personuppgiftsincidenter

Innehållsförteckning

Inledning **1**

Omfattning **1**

Vad är en personuppgift? **1**

Vad är en personuppgiftsincident? **1**

Exempel på personuppgiftsincidenter 2

Anmäla personuppgiftsincident till Integritetsskyddsmyndigheten (IMY) **2**

1. Av vem och hur ska anmälan göras? 2
2. Informera de registrerade 3
3. Dokumentation 4

Bilaga 1: Dokumentationsunderlag vid personuppgiftsincident **5**

Personuppgifterna och de registrerade 5
Konsekvenser 5
Information till de registrerade 5
Sen anmälan 6
Komplettering 6
Sekretess 6

Inledning

Högskolan ska se till att dataskyddsförordningen (GDPR) följs och arbeta proaktivt med att undvika personuppgiftsincidenter.

Rutinen omfattar Högskolans identifiering och hantering av personuppgiftsincidenter. Vidare klargör rutinen hur Högskolan skapar medvetenhet kring de risker som följer av personuppgiftsincidenter.

Omfattning

Rutinen omfattar hela Högskolan.

Vad är en personuppgift?

Personuppgifter är all information som kan knytas till en levande person. Det är till exempel:

- Namn
- Personnummer
- Adress
- Fotografi av en person
- Fingeravtryck
- Uppgift om en persons etniska ursprung
- Uppgift om en persons politiska åsikter

Vad är en personuppgiftsincident?

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors fri- och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks. Exempel:

- 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[1] har

- blivit förstörda
- gått förlorade på annat sätt
- kommit i orätta händer

Det spelar ingen roll om händelsen har skett oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter.

[1] Med registrerad person avses en person vars personuppgifter på något sätt behandlas, t ex samlas in, lagras, bearbetas med mera inom ramen för Högskolans verksamhet.

Högskolans dataskyddsombud svarar på frågor vid osäkerhet. Dataskyddsombuden kontaktas via registrator@hig.se. Dataskyddsombudsgruppen består av registratorer, säkerhetsansvarig, och informationssäkerhetsansvarig.

Exempel på personuppgiftsincidenter

- Någon obehörig part har fått tillgång till personuppgifter, till exempel om någon har skickat personuppgifter till mottagare som inte skulle ha uppgifterna.
- Datorer som innehåller personuppgifter har förlorats eller stulits.
- Någon har ändrat personuppgifter utan tillstånd.
- Personuppgifter är inte tillgängliga för den som behöver dem, och det leder till negativa effekter för de registrerade personerna.

Anmäla personuppgiftsincident till Integritetsskyddsmyndigheten (IMY)[2]

1. **Av vem och hur ska anmälan göras?**

Högskolan är i egenskap av personuppgiftsansvarig ansvarig för att upprätta anmälan. Personuppgiftsbiträden[3] är skyldiga att rapportera personuppgiftsincidenter till personuppgiftsansvarig.

Om incidenten rör ett system är det systemansvarig som gör anmälan. Om incidenten inte rör ett system, anmäler den som upptäckt incidenten.

Anmälan skickas till registrator@hig.se. Därigenom kontaktas dataskyddsombudsgruppen direkt, som bistår anmälaren med en första bedömning av om incidenten är allvarlig.

När en anmälan inkommer till registrator@hig.se kontaktar registrator även sakerhet@hig.se om incidenten rör t ex IT-system eller stulna datorer. Säkerhetsgruppen bedömer om tekniska säkerhetsåtgärder måste vidtas för att begränsa skada och risk, exempelvis om brandväggar behöver sättas upp eller en stulen dator låsas.

Allvarlig incident – anmälan till IMY

Om incidenten konstateras vara av en sådan art att den ska anmälas till IMY, görs en anmälan dit – beroende på vad som skett görs denna anmälan av systemansvarig (om det rör ett system) eller ansvarig chef för avdelningen där incidenten skett. Se bilaga 1 för dokumentationsunderlag.

En kopia av anmälan som skickas till IMY skickas till registrator@hig.se för diarieföring. När beslutet från IMY kommer ska även det diarieföras.

En personuppgiftsincident kan vara av sådan art att det inte är tydligt till exempel hur många som drabbats eller hur incidenten har skett, varvid en utredning måste genomföras för att klarlägga situationen. Även om incidenten kräver att Högskolan genomför en utredning av det inträffade, måste

---

[2] Tidigare Datainspektionen.

[3] Personuppgiftsbiträde är någon som behandlar personuppgifter åt annans räkning. Ett vanligt exempel är leverantörer eller andra lärosäten eller myndigheter som driftar molntjänster där Högskolan lagrar personuppgifter. Högskolan är fortfarande ansvarig, men personuppgiftsbiträdet lagrar uppgifterna vilket i sig är en personuppgiftsbehandling.

anmälan skickas till IMY inom 72 timmar. Anmälan till IMY kan vara inkomplett för att senare kompletteras efter genomförd utredning.

Utredning genomförs av ansvarig avdelning, alternativt systemansvarig om incidenten skett i ett IT-system. Högskolans dataskyddsombud är rådgivande, och nås via registrator@hig.se.

Innehåll i anmälan av personuppgiftsincident

Information om vad som ska ingå i en anmälan avseende personuppgiftsincidenter återfinns i IMYs e-tjänst för att rapportera personuppgiftsincidenter. Se bilaga 1 för dokumentationsunderlag vid personuppgiftsincident.

Sen anmälan

Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska Högskolan motivera förseningen. Anmälan syftar till att göra det möjligt för IMY att se och bevaka vilka åtgärder som vidtas för att motverka negativa effekter av det inträffade. Om det blir nödvändigt kan IMY också komma att utöva sina tillsynsbefogenheter för att få den som är ansvarig för behandlingen att vidta nödvändiga åtgärder.

Mindre allvarlig incident – hanteras internt

Anmälningsskyldigheten till IMY gäller inte om det är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Det är Högskolan som, enligt ansvarsprincipen, måste påvisa att det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för fysiska personers rättigheter och friheter.

Om incidenten i samråd med dataskyddsombudsgruppen konstateras vara av sådan art att den inte behöver anmälas till IMY, skrivs en intern rapport. Se bilaga 1 för dokumentationsunderlag, men använd endast punkt 3-6. Rapporten skickas till registrator@hig.se för diarieföring.

2. Informera de registrerade

Om personuppgiftsincidenten är allvarlig ska Högskolan utan onödigt dröjsmål även informera de registrerade om personuppgiftsincidenten. Detta gäller alltså om det är sannolikt att personuppgiftsincidenten leder till en hög risk för fysiska personers rättigheter och friheter. Den chef som är ansvarig för avdelningen där incidenten skett gör denna bedömning. Högskolans dataskyddsombud bistår med rådgivning i osäkra fall.

Högskolan ska bedöma både allvarligheten av den potentiella eller faktiska påverkan på personer som ett resultat av en personuppgiftsincident kan ha och sannolikheten för att detta inträffar.

- Hur allvarliga kan konsekvenserna bli?
- Hur sannolikt är det att enskilda personer drabbas?

Om personuppgiftsincidenten är allvarlig är risken högre. Om sannolikheten för konsekvenser är stor är risken också högre.

När risken är hög ska Högskolan genast informera de personer som har drabbats, särskilt om det finns ett behov av att mildra en omedelbar risk för skador. En av huvudorsakerna är att Högskolan ska kunna hjälpa individerna att vidta åtgärder för att skydda sig mot effekterna av en personuppgiftsincident.

Information till de registrerade

Högskolans information till de registrerade ska uppfylla IMYs minimikrav:

- Tydlig och klar beskrivning av orsaken till personuppgiftsincidenten.
- Namn och kontaktuppgifter till Högskolans kontaktperson i ärendet eller till en annan kontakt som är insatt i frågan och kan svara på frågor.
- Beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten.
- Beskrivning vad Högskolan har gjort, eller tänker göra, för att hantera personuppgiftsincidenten.
- I förkommande fall: Beskriv vad Högskolan har gjort för att mildra eventuella negativa effekter.

Om det går att avgöra vilka som drabbats, och det rör sig om en mindre mängd personer, kan de informeras via till exempel mejl eller brev. Om det rör sig om en stor mängd drabbade, eller det inte går att avgöra exakt vilka som har drabbats, kan information läggas ut på Högskolans webbsida.

Om information ska skickas ut till en mindre mängd personer, ska avsändare vara en person på Högskolan som kan besvara eventuella frågor från drabbade. Det kan därmed skifta beroende på vad situationen är, men exempelvis en systemansvarig om incidenten inträffade i ett system. Om information läggs ut på Högskolans webbsida, hänvisas eventuella frågor till funktionsmejl om sådan finns (t ex biblioteket@hig.se om incidenten skulle gälla bibliotekssystemet), och om ingen funktionsmejl finns används registrator@hig.se. Inkomna frågor till registraturen vidarebefordras till den person som kan besvara frågorna.

3. Dokumentation

Högskolan ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Ansvarig chef ansvarar för dokumentationen.

Med dokumentering avses här förutom anmälan till IMY eller den interna rapport som skrivs med stöd av bilaga 1 exempelvis en intern utredning om vad som inträffat och vad som har gjorts för att åtgärda det inträffade, eller korrespondens med en extern systemleverantör om behov av säkerhetsuppdateringar. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av Högskolans anmälningsskyldighet samt ytterligare skyldigheter som följer av anmälan om personuppgiftsincident.

Dokumentation skickas till registrator@hig.se för diarieföring i det ärende som skapats för personuppgiftsincidenten.

Bilaga 1: Dokumentationsunderlag vid personuppgiftsincident

Följande punkter skall användas vid dokumentation av personuppgiftsincident. Frågorna är baserade på vad IMY efterfrågar vid anmälan till dem. Vid intern anmälan, om en incidents inte bedömts vara så allvarlig att den måste anmälas till IMY, behöver endast frågor under punkt 3-6 besvaras.

1. Personuppgiftsansvarig

- Organisationens namn, kontaktuppgifter
- (Om sådana är involverade) Namn på personuppgiftsbiträden, underbiträden

2. Kontaktperson för anmälan

- Kontaktuppgifter till den person som IMY kan kontakta

3. Personuppgiftsincidenten

- Har personuppgiftsincidenten medfört en risk för de registrerades fri- och rättigheter?
- När inträffade personuppgiftsincidenten?
- När upptäckte ni personuppgiftsincidenten?
- Vad har hänt vid personuppgiftsincidenten?[4]
- Hur upptäckte ni personuppgiftsincidenten?
- Varför inträffade personuppgiftsincidenten enligt din eller organisationens uppfattning?
- Inom vilket verksamhetsområde inträffade personuppgiftsincidenten?

4. 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?

5. Konsekvenser

- Vad kan bli konsekvenserna av personuppgiftsincidenten?
- Hur allvarlig bedömer ni att personuppgiftsincidenten är?

6. Information till de registrerade

- Har ni informerat de registrerade om personuppgiftsincidenten? När?

[4] OBS, denna punkt ska inte vara alltför detaljerad. Lämna inte ut namn eller andra personuppgifter om de involverade, skriv t ex inte ”Kalle Kallesson, född 000101, lider av cancer och ett mejl till läraren om detta syntes av misstag på en skärm vid Zoom-föreläsning” utan istället ”En students hälsouppgifter har av misstag synts på en skärm vid Zoom-föreläsning”.

- Kommer ni att informera de registrerade? När? Om inte, varför kommer ni inte att informera de registrerade?

7. Sen anmälan

- Om anmälan kommer in senare än 72 timmar efter att ni upptäckte personuppgiftsincidenten ska ni beskriva varför.

8. Komplettering

- Om ni kommer att komplettera anmälan, beskriv varför.

9. Sekretess

- Om du har skrivit något som du anser bör omfattas av sekretess, beskriv det.