SÖDERTÖRNS HÖGSKOLA | STOCKHOLM
sh.se

STYRDOKUMENT

Handläggningsordning för hantering av personuppgiftsincidenter

Dokumenttyp	Handläggningsordning
Beslutad av	Förvaltningschef
Beslutsdatum	2023-06-26
Diarienummer	2143-1.1.2-2023
Giltighetstid	2023-06-26 – tills vidare
Ersätter dokument	Rutin för personuppgiftsincident, dnr 2667-1.1.2-2019
Ansvarig avdelning	Avdelningen för verksamhetsutveckling och myndighetsstöd
Beskrivning	Denna handläggningsordning beskriver hur personuppgiftsincidenter ska hanteras på högskolan samt hur en eventuell anmälan till Integritetsskyddsmyndigheten ska genomföras.

Innehållsförteckning

1. Inledning

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter. Incidenten kan också leda till ett obehörigt röjande av eller obehörig åtkomst till personuppgifter.

Södertörns högskola ska enligt EU:s dataskyddsförordning (2016/679) ha rutiner på plats för att kunna upptäcka, utreda och rapportera personuppgiftsincidenter. Vissa personuppgiftsincidenter måste dessutom anmälas till Integritetsskyddsmyndigheten (IMY) **inom 72 timmar** från att incidenten upptäcktes.

Denna handläggningsordning beskriver hur personuppgiftsincidenter ska utredas, rapporteras och dokumenteras internt på högskolan samt hur en eventuell anmälan till IMY ska genomföras.

Handläggningsordningen utgör ett högskolegemensamt styrdokument, vilket innebär att samtliga medarbetare inom högskolan omfattas av handläggningsordningen.

2. Syfte

Syftet med denna handläggningsordning är att skapa en systematisk hantering av personuppgiftsincidenter samt utgöra ett stöd vid rapportering och utredning av personuppgiftsincidenter.

3. Hantering av personuppgiftsincidenter

Enligt rektorsbeslut från 2019, dnr 2534-1.9.3-2019, ska det finnas en utsedd GDPR-samordnare vid varje avdelning, institution och annan verksamhet (biblioteket, Enheten för verksamhetsplanering och projektledning och CBEES) på högskolan. Det är GDPR-samordnaren som har det samordnande ansvaret för att utreda och dokumentera personuppgiftsincidenter samt eventuellt anmäla incidenter till IMY. Det är dock den som upptäcker personuppgiftsincidenten som ansvarar för att rapportera incidenten internt på högskolan.

Nedan följer ett antal steg som ska följas vid hantering av en personuppgiftsincident.

3.1. Den som upptäcker eller misstänker en personuppgiftsincident ska rapportera incidenten till högskolans registrator

Den som upptäcker eller misstänker en personuppgiftsincident ska rapportera detta omedelbart till registrator@sh.se. E-postmeddelandet till registrator ska inte innehålla några känsliga personuppgifter eller sekretessbelagd information, utan endast det som framgår nedan.

- Namn på anmälaren och information om yrkestitel på anmälaren samt vilken avdelning, institution eller annan verksamhet (till exempel biblioteket, Enheten för verksamhetsplanering och projektledning och CBEES) anmälaren tillhör.

- En kort beskrivning av incidenten där det framgår när incidenten inträffade (datum och tid) och när den upptäcktes (datum och tid).

- Om incidenten har inträffat hos Södertörns högskola eller hos ett personuppgiftsbiträde till högskolan (till exempel en leverantör av ett system som högskolan har).

- Vilka persongrupper de drabbade tillhör (till exempel anställd eller student).

- Vad det är typ av personuppgifter (till exempel namn, personnummer, uppgift om hälsa).

- Antalet personer som berörs av incidenten (uppskatta antalet om det är osäkert hur många det är som berörs av incidenten).

3.2. Registrator registrerar ett ärende i högskolans diarium och utser aktuell GDPR-samordnare till handläggare

Registrator registrerar ett ärende i högskolans diarium och utser aktuell GDPR-samordnare till handläggare i enlighet med en särskild rutin som är framtagen för högskolans registratorer. Om aktuell GDPR-samordnare inte är närvarande utses samordnarens chef till handläggare.

3.3. GDPR-samordnaren skickar bekräftelse till registrator och utreder incidenten i samarbete med den som upptäckte incidenten

3.3.1. GDPR-samordnaren skickar bekräftelse till registrator

Så fort ärendet har tilldelats ansvarig GDPR-samordnare ska samordnaren skicka en bekräftelse till registrator och meddela att ärendet är mottaget.

3.3.2. GDPR-samordnaren utreder och tar ställning till om incidenten ska anmälas till IMY

GDPR-samordnaren ska i samarbete med den som anmält incidenten, skyndsamt utreda incidenten och göra en riskbedömning av incidenten. I riskbedömningen ska man bedöma om det är sannolikt att incidenten medför risker för personens fri- och rättigheter. I bedömningen ska det även utredas vilka åtgärder som kan vidtas för att hindra eventuella negativa konsekvenser för den enskilde, till exempel genom att göra personuppgifterna otillgängliga. Vilka faktorer som ska beaktas i en riskbedömning framgår av dokumentet

”Vägledning för att göra en riskbedömning av en personuppgiftsincident” som finns under Rättslig vägledning på medarbetarwebben. GDPR-samordnaren kan kontakta högskolans dataskyddsombud för vägledning i riskbedömningen.

GDPR-samordnaren kan behöva kontakta systemägaren eller systemledare om incidenten har inträffat i högskolans system. Det kan även bli aktuellt att kontakta leverantören av systemet. Om incidenten har inträffat hos ett personuppgiftsbiträde behöver GDPR-samordnaren samla in information om incidenten från biträdet. Beroende på vad incidenten avser kan det även bli aktuellt att kontakta Campus- och IT-avdelningen.

Efter att riskbedömningen har gjorts måste GDPR-samordnaren ta ställning till om incidenten ska anmälas till IMY eller inte. En anmälan till IMY måste göras **inom 72 timmar** från det att incidenten upptäcktes. Om man är osäker på om incidenten ska anmälas till IMY är det bättre att ta det säkra före det osäkra och anmäla incidenten.

Därefter behöver GDPR-samordnaren ta ställning till om personerna som drabbats av personuppgiftsincidenten ska informeras om incidenten (se nedan).

3.3.3. GDPR-samordnaren bedömer om personen eller personerna som drabbats av personuppgiftsincidenten ska informeras om incidenten

GDPR-samordnaren behöver ta ställning till om personen eller personerna som drabbats av personuppgiftsincidenten ska informeras om incidenten. Om incidenten sannolikt leder till en hög risk för de drabbade personernas fri- och rättigheter måste personerna få information om incidenten. Informationen ska ges utan onödigt dröjsmål, det vill säga så snart som möjligt. GDPR-samordnaren kan kontakta högskolans dataskyddsombud via dataskydd@sh.se för vägledning. Om GDPR-samordnaren bestämmer sig för att informera de drabbade ska informationen innehålla följande punkter.

- Tydlig beskrivning av personuppgiftsincidenten och orsaken till incidenten.
- Vilka de sannolika konsekvenserna är.
- Vilka åtgärder som har vidtagits eller som kommer att vidtas för att hantera incidenten. Ange även om åtgärder har vidtagits för att mildra eventuella konsekvenser.
- Övriga upplysningar, till exempel om de som drabbats av incidenten behöver vidta några åtgärder på egen hand.
- Namn och kontaktuppgifter till den som är insatt i ärendet samt högskolans dataskyddsombud (använd e-postadressen dataskydd@sh.se).

3.4. GDPR-samordnaren anmäler personuppgiftsincidenten till IMY och dokumenterar incidenten internt i högskolans framtagna beslutsmall (om personuppgiftsincidenten *inte* ska anmälas till IMY, gå vidare till avsnitt 3.5.)

3.4.1. GDPR-samordnaren anmäler incidenten via IMY:s webbplats och diarieför anmälan

Om GDPR-samordnaren bedömer att personuppgiftsincidenten ska anmälas till IMY ska detta göras **inom 72 timmar från det att incidenten upptäcktes**. Anmälan ska göras via IMY:s anmälningsformulär som finns på myndighetens webbplats. Länk finns här: https://www.imy.se/verksamhet/utfora-arenden/anmal-personuppgiftsincident/risk-for-registrerade/. Anmälan till IMY ska diarieföras. Vid diarieföring är det viktigt att uppge ärendets diarienummer.

Eftersom en inkommen anmälan till IMY i regel omfattas av svag sekretess är det viktigt att inte skriva för mycket om brister i högskolans it-säkerhet eller att skriva information som kan identifiera en enskild person.

Observera att om man inte har hunnit utreda incidenten fullt ut kan man komplettera anmälan till IMY i efterhand.

3.4.2. GDPR-samordnaren dokumenterar incidenten internt i högskolans framtagna beslutsmall

När anmälan till IMY har gjorts ska GDPR-samordnaren dokumentera incidenten internt genom att skriva ett beslut där det bland annat framgår vad som har hänt, vilka åtgärder som har vidtagits, att en anmälan till IMY har gjorts samt om den drabbade eller de drabbade har fått eller ska få information om incidenten. GDPR-samordnaren ska sedan föredra beslutet för prefekt, avdelningschef, bibliotekschef eller motsvarande som enligt högskolans besluts- och delegationsordning har befogenhet att fatta beslut om personuppgiftsincidenter. Beslutet ska diarieföras och skickas till högskolans dataskyddsombud för kännedom. Vid diarieföring är det viktigt att uppge ärendets diarienummer.

Under Rättslig vägledning på medarbetarwebben finns det en särskild beslutsmall för personuppgiftsincidenter som heter ”Beslutsmall för personuppgiftsincidenter”.

3.4.3. GDPR-samordnaren diarieför beslut från IMY

När IMY skickar beslut om anmäld personuppgiftsincident till högskolan ska ansvarig GDPR-samordnare diarieföra beslutet. Vid diarieföring är det viktigt att uppge ärendets dnr. Om beslutet innehåller information om att IMY har inlett en tillsyn mot högskolan ska GDPR-samordnaren kontakta högskolans dataskyddsombud.

3.5. Om personuppgiftsincidenten *inte* ska anmälas till IMY

3.5.1. GDPR-samordnaren dokumenterar incidenten internt i högskolans framtagna beslutsmall

Om personuppgiftsincidenten inte ska anmälas till IMY ska GDPR-samordnaren dokumentera incidenten internt genom att skriva ett beslut där det bland annat framgår vad som har hänt, vilka åtgärder som vidtagits och att en anmälan till IMY inte har gjorts samt en motivering till varför man valt att inte anmäla incidenten till IMY. Av beslutet ska det även framgå om de drabbade har fått eller ska få information om incidenten. GDPR-samordnaren ska sedan föredra beslutet för prefekt, avdelningschef, bibliotekschef eller motsvarande som enligt högskolans besluts- och delegationsordning har befogenhet att fatta beslut om personuppgiftsincidenter. Beslutet ska diarieföras och skickas till högskolans dataskyddsombud för kännedom. Vid diarieföring är det viktigt att uppge ärendets diarienummer.

Under Rättslig vägledning på medarbetarwebben finns det en särskild beslutsmall för personuppgiftsincidenter som heter ”Beslutsmall för personuppgiftsincidenter”.