



Vägledning för att göra en riskbedömning av en personuppgiftsincident

Om en personuppgiftsincident har inträffat ska högskolan bedöma om incidenten sannolikt innebär en risk för de drabbades fri- och rättigheter. Bedömningen ska sedan ligga till grund för att avgöra om incidenten behöver anmälas till Integritetsskyddsmyndigheten (IMY) och om de som drabbats av incidenten behöver informeras om händelsen. Vid bedömningen ska högskolan ta hänsyn till vilka konsekvenser som kan uppkomma för de drabbades fri- och rättigheter till följd av incidenten samt hur sannolikt det är att incidenten inträffar.

Är det osannolikt att personuppgiftsincidenten medför några risker för de drabbades fri- och rättigheter behöver incidenten inte anmälas IMY.

Nedan finns ett antal faktorer som ska beaktas i riskbedömningen.

1. Vad är det för typ av personuppgiftsincident?

Utred vad det är för typ av personuppgiftsincident. Vilken typ av incident det är fråga om har betydelse för vilka risker som kan uppkomma samt vilka konsekvenser som de drabbade kan utsättas för. Ett felaktigt brevutskick med känsliga uppgifter kan exempelvis få andra konsekvenser än en incident som innebär att en persons medicinska uppgifter har raderats eller inte längre är tillgängliga.

2. Personuppgifternas karaktär, känslighet och mängd

Ta reda på vad det är för typ av personuppgifter som omfattas av personuppgiftsincidenten. Personuppgifternas karaktär och känslighet kan påverka vilken skada som kan uppkomma för de som drabbats av incidenten. Till exempel kan identitetshandlingar och finansiella uppgifter tillsammans användas för identitetsstöld. I vissa fall kan en kombination av personuppgifter vara känsligare än endast en typ av personuppgifter. Om det rör sig om en större mängd personuppgifter kan incidenten innebära större effekter på de drabbades fri- och rättigheter.

3. Hur enkelt är det att identifiera enskilda personer?

Utred hur enkelt det är att identifiera enskilda personer. Hur enkelt det är att identifiera personer med hjälp av de uppgifter som personuppgiftsincidenten omfattar kan få betydelse för vilka konsekvenser incidenten kan medföra. Hur enkelt uppgifterna, direkt eller indirekt,

kan användas för att identifiera en enskild person kan exempelvis påverkas av om personuppgifterna skyddats genom kryptering eller pseudonymisering

4. Vilka personer är det som har drabbats av personuppgiftsincidenten?

Utred vilka personer som omfattas av personuppgiftsincidenten. En personuppgiftsincident kan få allvarigare konsekvenser om den drabbar särskilt skyddsvärda personer, exempelvis barn eller andra personer i sårbarare eller svagare ställning. Det kan även finnas andra faktorer hos personen som kan påverka vilken effekt en incident får för den som drabbats. Därför är det viktigt att ta hänsyn till vilka personerna är och om det finns egenskaper hos dem som kan få betydelse för riskbedömningen.

5. Hur allvarliga är konsekvenserna?

Utred hur allvarliga konsekvenserna är eller kan bli till följd av personuppgiftsincidenten. En incident är särskilt allvarlig om det finns en risk att incidenten leder till exempelvis identitetsstöld, bedrägeri eller skadlig ryktesspridning.

Hur allvarliga konsekvenserna är beror på vad det är för typ av incident. Det har till exempel betydelse om högskolan vet om att personuppgifterna hamnat hos personer vars avsikter är okända eller skadliga. Om uppgifterna istället skickats till en mottagare som är betrodd kan risken för de drabbade anses vara lägre.