Beslut

Högskoledirektör

Diarienummer 20/703
2020-11-25

Rutin för identifiering och hantering av personuppgiftsincidenter

Inledning

Om en personuppgiftsincident inträffar ska vissa åtgärder vidtas för att snabbt minska eventuell skada. Denna rutin beskriver vad en personuppgiftsincident är och hur KMH ska hantera en sådan incident.

Vad är en personuppgiftsincident?

En personuppgiftsincident uppstår när de personuppgifter som behandlas av KMH, eller någon av KMH:s personuppgiftsbiträden, antingen:

- medvetet, omedvetet eller olagligt förstörs, förvanskas, försvinner eller ändras,
- eller när någon som inte har behörig tillgång till personuppgifterna får tillgång eller åtkomst till dessa, s.k. obehörig åtkomst,
- eller när personuppgifter på ett felaktigt sätt sprids eller publiceras internt eller externt, s.k. obehörigt röjande.

En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har blivit förstörda, gått förlorade eller kommit i orätta händer. Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fallen är det frågan om en personuppgiftsincident.

Personuppgifter är all slags information som kan knytas till en levande person. Det kan röra sig om namn, adress och

Kungl. Musikhögskolan
i Stockholm
Royal College of Music
+46 8 16 18 00
www.kmh.se

Valhallavägen 105
Box 27711
115 91 Stockholm
Sweden

personnummer. Även foton på personer klassas som personuppgifter.

Anmälan om personuppgiftsincidenter

Alla inom KMH som upptäcker eller har misstanke om att en personuppgiftsincident har inträffat, har en skyldighet att utan dröjsmål anmäla detta till närmaste chef. Ansvarig chef ska kontakta högskoleledningens samordnare som rådgör med högskoledirektören om vilken åtgärd som ska vidtas. Dataskyddsombudet ska informeras om det som inträffat. Om en personuppgiftsincident har inträffat ska detta i vissa fall även anmälas till Integritetsskyddsmyndigheten.

När KMH fått vetskap om att en personuppgiftsincident inträffat ska detta anmälas till Integritetsskyddsmyndigheten om det inte är osannolikt att incidenten medför en risk för fysiska personers rättigheter och friheter. För att avgöra om en anmälan ska göras ska högskoledirektören, eller den han utser, för varje incident göra en riskbedömning om hur incidenten påverkar fysiska personer. Om det konstateras att en anmälan ska göras ska detta ske utan dröjsmål, dock senast inom 72 timmar från det att incidenten upptäckts. Under dessa 72 timmar måste KMH dessutom besluta om vilka åtgärder som behövs för att hantera incidenten. Om det konstateras att en personuppgiftsincident har hänt men att det är osannolikt att incidenten medför en risk för fysiska personer finns det ingen skyldighet att anmäla detta till Integritetsskyddsmyndigheten. Incidenten ska ändå dokumenteras och dataskyddsombudet meddelas. Dokumentation om incidenten förs av dataskyddsombudet in i ett internt register över inträffade personuppgiftsincidenter. Registret finns hos dataskyddsombudet.

Hur bedömer man risken?

Vid en riskbedömning ska hänsyn tas till de specifika omständigheterna i samband med incidenten. Här ingår de potentiella effekternas svårighetsgrad och hur sannolika dessa effekter är. En personuppgiftsincident som inte snabbt åtgärdas på lämpligt sätt kan för fysiska personer leda till fysisk, materiell eller immateriell skada. Det kan röra sig om att den det gäller löper risk att förlora kontrollen över de egna personuppgifterna eller till att rättigheter begränsas. Det kan finns risk för identitetsstöld, bedrägeri och ekonomisk förlust. Vidare kan det leda till skadat anseende eller diskriminering, obehörigt hävande av pseudonymisering eller förlust av konfidentialitet om det rör personuppgifter som omfattas av tystnadsplikt. Slutligen kan personuppgiftsincident leda till

annan ekonomisk eller social nackdel för den det rör. Den övergripande frågan är vilka effekter incidenten riskerar att få för den som är berörd. Om incidenten rör känsliga personuppgifter ska risken för skada anses sannolik.

Riskbedömningen görs av högskoledirektören eller den han utsett. Dataskyddsombudet kan hjälpa till med riskbedömningen.

Hur görs anmälan och vad ska den innehålla?

En anmälan om personuppgiftsincident görs till Integritetsskyddsmyndigheten genom ett särskilt anmälningsformulär på deras webbplats. Anmälan ska innehålla bl.a. uppgifter om själva incidenten, kontaktuppgifterna för dataskyddsombudet eller andra kontaktpunkter där mer information kan erhållas, en beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten och vilka åtgärder som vidtagits eller kommer att vidtas. I anmälan ska också ange vad det är för typ av incident.

Information till de registrerade i samband med personuppgiftsincidenter

Förutom att Integritetsskyddsmyndigheten ska meddelas så kan enskilda personer behöva bli informerade om att det inträffat en personuppgiftsincident. Genom att underrätta de registrerade som drabbats om att en incident har inträffat kan KMH uppmärksamma dem på vilka risker incidenten medför och vilka åtgärder de kan vidta för att skydda sig mot potentiella konsekvenser.

KMH ska informera de registrerade om personuppgiftsincidenten om den sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Det är ett högre krav än vad som gäller för anmälan till Integritetsskyddsmyndigheten. Detta innebär att om de registrerade informeras ska alltid en anmälan till en Integritetsskyddsmyndigheten göras.

Det finns undantag från skyldigheten att informera de som drabbats i samband med incidenter. Information krävs inte om åtgärder vidtagits före personuppgiftsincidenten som gör att risken – trots incidenten – inte betraktas som hög. Eller att åtgärder vidtagits efter personuppgiftsincidenten som gör det osannolikt att en hög risk kommer att uppstå. Vidare kan ett undantag accepteras om det skulle innebära en orimligt stor ansträngning att informera samtliga berörda. I det senare fallet måste KMH i stället informera allmänheten eller se till att de som berörs informeras på ett lika

effektivt sätt. Om KMH anser att något av undantagen från att informera de berörda är uppfyllt, måste KMH inför Integritetsskyddsmyndigheten kunna lägga fram lämpliga bevis på att så är fallet.

Om man kommer fram till att de som drabbats bör underrättas ska detta ske så snart det är möjligt. Vad som är en rimlig tid beror på incidenten men om det finns ett behov av att snabbt mildra en omedelbar skaderisk ska de drabbade meddelas omedelbart.

Informationen till de som drabbats ska bestå av en tydlig och klar beskrivning av personuppgiftsincidenten. Kontaktuppgifter till dataskyddsombudet eller andra kontaktuppgifter där de drabbade kan få mer information ska ges. Informationen ska även omfatta en beskrivning av de troliga konsekvenserna av incidenten samt en beskrivning av hur KMH agerat eller vilka åtgärder som vidtagits för att åtgärda incidenten och mildra dess potentiella negativa effekter. Informationen bör också innehålla rekommendationer till vad de som berörs själva kan göra för att mildra de potentiella negativa effekterna.

Vad ska dokumenteras?

KMH ska dokumentera alla personuppgiftsincidenter. Syftet med dokumentationen är att göra det möjligt för Integritetsskyddsmyndigheten att kontrollera att KMH följer bestämmelserna om personuppgiftsincidenter i dataskyddsförordningen. Det är viktigt att dokumentationen innehåller omständigheterna kring incidenten, effekterna av den och vilka åtgärder som vidtagits. Bedömningen och agerandet ska motiveras. Detta är särskilt viktigt om man kommit fram till att incidenten sannolikt inte kommer att leda till en risk för enskildas rättigheter och friheter och någon anmälan inte görs. Dokumentationen ska sparas i särskilt register för incidentrapportering. Dataskyddsombudet ska kontaktas för närmare instruktioner.

Andra regelverk om incidentrapportering

Då en bedömning av personuppgiftsincidenten görs är det viktigt att ha i åtanke att det kan finnas en skyldighet att anmäla incidenten

även till andra myndigheter än Integritetsskyddsmyndigheten beroende på vilken typ av incident det rör sig om. Enligt förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, ska IT-incidenter rapporteras till Myndigheten för samhällsskydd och beredskap. Detta gäller för IT-incidenter som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller i tjänster som myndigheten levererar till en annan organisation.

Checklista

1. Vid misstanken om personuppgiftsincident, kontakta högskoleledningens samordnare Linda Nilsson, som i sin tur informerar högskoledirektör Peter Liljenstolpe och dataskyddsombudet Magnus Dyberg.
2. Genomför en riskbedömning för att utröna om någon personuppgiftsincident inträffat.
3. Anmäl personuppgiftsincident till Integritetsskyddsmyndigheten genom webbformulär om det konstaterats att den medför en risk för fysiska personers rättigheter och friheter. Anmälan ska göras inom 72 timmar.
4. Informera de registrerade om personuppgiftsincident om inte undantag föreligger.
5. Dokumentera personuppgiftsincident och informera dataskyddsombudet.
6. För in dokumentation om personuppgiftsincidenten i KMH:s interna registret för personuppgiftsincidenter.

Lagtexter och föreskrifter

Dataskyddsförordningen (GDPR The General Data Protection Regulation)

Riktlinjer om anmälan av personuppgiftsincidenter enligt GDPR. Från Artikel 29-gruppen. Riktlinjerna har godkänts av EDPB , Europeiska dataskyddsstyrelsen EDPB.

Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap