Umeå universitet
901 87 Umeå

Tillsyn enligt dataskyddsförordningen - Umeå universitets behandling av personuppgifter

Innehållsförteckning

Datainspektionens beslut

Datainspektionen konstaterar att Umeå universitet

- har skickat känsliga och integritetskänsliga personuppgifter genom okrypterad e-post och via öppet nät till Polismyndigheten den 5 februari 2019. Universitetet har därför behandlat personuppgifter i strid med artikel 5.1 f samt artikel 32.1 och 32.2 i dataskyddsförordningen[1] genom att inte ha vidtagit lämpliga tekniska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.
- inte har anmält personuppgiftsincidenten till Datainspektionen och inte dokumenterat omständigheterna kring incidenten då universitetet blev uppmärksammat på den. Universitetet har därför agerat i strid med artikel 33.1 och 33.5 i dataskyddsförordningen.
- vid behandlingen av känsliga och integritetskänsliga personuppgifter i molntjänsten Box, under tiden den 25 maj 2018 till våren 2019, inte har vidtagit lämpliga tekniska och organisatoriska åtgärder för att förhindra obehörigt röjande av eller obehörig åtkomst till personuppgifterna. Universitetet har därför behandlat personuppgifter i strid med artikel 5.1 f samt artikel 32.1 och 32.2 i dataskyddsförordningen.

Administrativ sanktionsavgift
Datainspektionen beslutar med stöd av artiklarna 58.2 och 83 i dataskyddsförordningen och 6 kap. 2 § dataskyddslagen (2018:218) att Umeå universitet ska betala en administrativ sanktionsavgift på 550 000 kronor.

[1] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Redogörelse för tillsynsärendet

Bakgrund

Datainspektionen inledde tillsyn mot Umeå universitet den 29 augusti 2019. Inspektionen hade fått information om att universitetet skickat känsliga personuppgifter till Polismyndigheten via okrypterad e-post. Till informationen bifogades Polismyndighetens skrivelse; Information om brister av hantering av handlingar.

Syftet med tillsynen är att undersöka om personuppgiftsbehandlingarna som beskrivs i Polismyndighetens skrivelse uppfyller kraven på säkerhet som ställs i artiklarna 5.1.f och 32 i dataskyddsförordningen.

Datainspektionen har dessutom granskat om Umeå universitet har följt bestämmelsen i artikel 33 i dataskyddsförordningen, som bland annat handlar om den personuppgiftsansvariges anmälningsskyldighet vid en personuppgiftsincident.

Vidare har Datainspektionen undersökt om hanteringen av känsliga personuppgifter i molntjänsten Box gjorts i enlighet med dataskyddsbestämmelserna.

Datainspektionens tillsyn utgår från den 25 maj 2018 då dataskyddsförordningen började tillämpas. Inspektionen har därför inte granskat den incident som inträffade före detta datum.

Tillsynen har utförts genom skriftlig kommunikation.

Vad som framkommit i ärendet

Polismyndighetens skrivelse
Av Polismyndighetens skrivelse framgår bland annat följande.

En forskargrupp vid Umeå universitet begärde ut samtliga förundersökningsprotokoll rörande våldtäkt mot män i Sverige från 2014. Den 18 juli 2016 lämnade Polismyndigheten ut handlingarna via bud.

I samband med en begäran om komplettering via mejl bifogade forskargruppen, den 19 november 2017, oavsiktligt ett av de förundersökningsprotokoll som tidigare lämnats ut av Polismyndigheten. Polismyndigheten kontaktade då forskargruppen och påpekade det olämpliga i att skicka känsligt material över oskyddade e-postkanaler. Forskargruppen beklagade det inträffade och hänvisade till den mänskliga faktorn.

I samband med ytterligare en begäran om komplettering bifogade forskargruppen, den 5 februari 2019, åter igen samma förundersökningsprotokoll. När Polismyndigheten ännu en gång kontaktade forskargruppen om detta medgavs att man även denna gång oavsiktligt bifogat det känsliga materialet i ett mejl.

Uppgifter från Umeå universitet
Umeå universitet var personuppgiftsansvarig när mejlen skickades till Polismyndigheten.

Den huvudansvarige forskaren lämnade sin anställning vid Umeå universitet den 31 augusti 2018 för anställning vid Uppsala universitet. I och med att den huvudansvarige forskaren bytte arbetsgivare och arbetsplats har projektet också bytt hemvist. Detta skedde dock efter de aktuella händelserna. Finansiären Forte[2] fattade beslut om byte av huvudman den 13 mars 2019 och Etikprövningsmyndigheten godkände ändringen som innebar byte av forskningshuvudman till Uppsala universitet den 10 maj 2019.

Forskningsprojektet vid Umeå universitet har godkänts av Etikprövningsmyndigheten och förundersökningsprotokollen har mottagits och lagrats utifrån ett allmänt intresse som tillåter personuppgiftsbehandling.

Händelseförloppet
I augusti 2016 fick forskargruppen de förundersökningsprotokoll som begärts. Handlingarna skickades i pappersform till Umeå universitet.

Samtliga polisanmälningar och förundersökningsprotokoll från 2014 skannades in och förvarades på en lösenordsskyddad filyta. En fysisk version låstes in i ett arkivrum. Förundersökningsprotokollen innehåller uppgifter

[2] Forskningsrådet för hälsa, arbetsliv och välfärd.

om bland annat misstanke om brott, namn, personnummer och kontaktuppgifter. Dessutom innehåller dessa protokoll uppgifter om sexualliv och hälsa, det vill säga känsliga personuppgifter.

Vid en begäran om komplettering som gjordes 2017 var inte avsikten att bifoga protokollet bland de andra handlingar som skickades till Polismyndigheten. Efter det inträffade har forskargruppen bland annat infört en rutin om att skanna känsligt material separat.

Forskargruppen har inte kunnat förklara varför gruppen, den 5 februari 2019, åter igen bifogat protokollet i ett mejl till Polismyndigheten.

Säkerhet vid utskick av förundersökningsprotokollen

Den felaktiga hanteringen har inskränkt sig till två tillfällen. I övrigt har projektets rutiner att låsa in fysiska dokument, att avskilja administrativa dokument från forskningsdata och att lösenordsskydda digitala dokument följts. Endast två forskare från universitetet har haft tillgång till det aktuella materialet.

Universitetet har bland annat regelverk och instruktioner för att säkerställa att behandling av personuppgifter vid universitet följer kraven som ställs i artikel 32 i dataskyddsförordningen. Universitetet har sedan 2014 en tydlig regel om att känsliga personuppgifter inte får skickas med e-post, i enlighet med dokumentet E-posttjänst vid Umeå universitet. Anställda får kontinuerlig utbildning och information i ämnet. Universitetet planerar även att rikta en särskild informationsinsats om behandling av personuppgifter i e-post till samtliga anställa vid universitetet.

Universitetet har begått ett misstag genom att skicka känsliga personuppgifter via e-post till Polismyndigheten. Personuppgiftsbehandlingarna i fråga kan därför inte sägas uppfylla de krav som ställs om lämpliga säkerhetsåtgärder enligt artikel 32 i dataskyddsförordningen.

Personuppgiftsincidenten

Umeå universitet fick kännedom om att känsliga personuppgifter skickats med e-post i samband med att myndigheten mottog Datainspektionens tillsynsskrivelse, den 30 augusti 2019.

Den 2 september 2019 utförde universitetet en analys av händelserna och kom då fram till att det var osannolikt att personuppgiftsincidenten skulle komma att medföra en risk för de registrerade. Universitetet har dokumenterat händelserna i Datainspektionens blankett för anmälan av personuppgiftsincident. Universitetet har i blanketten angett bland annat följande.

> Universitetet har bedömt att ingen anmälan ska skickas in till Datainspektionen. (...) Den 2 september inkom rekommenderat brev från Datainspektionen innehållande information om incidenterna. Umeå universitets bedömning är att det är osannolikt att incidenten medfört hög risk för enskildas fri- och rättigheter. Det finns inget som tyder på att det uppstått någon faktisk skada eller att någon obehörig tagit del av uppgifterna då protokollet i fråga har skickats till den myndighet som upprättat detsamma och till handläggare som haft till uppgift att hantera och till universitetet lämna ut samma typ av uppgifter.

Lagring och åtkomst i molntjänsten Box

Universitetet har skannat in 108 förundersökningsprotokoll från 2014 som sparats lokalt på en persondator för att sedan laddas upp hos molntjänstleverantören Box.

Användaren kan få tillgång till de lagrade uppgifterna i Box genom att logga in via ett webbgränssnitt internt via universitetets nätverk med singelfaktorsautentisering (det vill säga användarnamn och lösenord).

Det går även att logga in externt via internet på universitetets webbplats umu.se. Inloggningen sker då via valfri utrustning/nät. Användaren uppger först sin e-postadress och därefter sitt högskole-ID (användarnamn) och lösenord.

Användarkonton i Box är integrerade och kopplade mot högskole-ID som i sin tur är integrerade mot SWAMID. Med SWAMID erhålls en säker identifiering eftersom lösenord varken sparas eller skickas in till Box. Autentiseringen sker innan, genom att en ”ticket” skickas in till Box som bekräftar behörigheten.

All kommunikation är krypterad med 256 bitars SSL-kryptering (https).

All information lagras med 256-bitars kryptering. Det innebär att informationen inte är tillgänglig om någon utan behörighet skulle få åtkomst

till den. Även backuper krypteras. Box lagrar krypteringsnycklarna separat från data.

I forskningsprojektet ingår två forskare och det är endast de två som har haft behörighet och åtkomst till filytan som tillhandahålls av Box. Eftersom åtkomsten varit begränsad har inga särskilda rutiner upprättats.

Universitetet har ett personuppgiftsbiträdesavtal med SUNET (Swedish University computer Network) som bland annat gäller lagring av förundersökningsprotokollen. SUNET har i sin tur anlitat underbiträdet Box. Box lagrar informationen i USA och är ansluten till Privacy Shield samt har tecknat bindande företagsbestämmelser.

Förundersökningsprotokollen omfattas av sekretess enligt 35 kap. 1 § och 11 kap. 3 § offentlighets- och sekretesslagen (2009:400), OSL. Utgångspunkten är således att sekretess gäller för uppgifterna.

Information om att känsliga personuppgifter inte bör lagras i Box har publicerats på universitets intranät i september 2016.

Universitet har gjort bedömningen att det finns rättsliga och säkerhetsmässiga förutsättningar för att lagra såväl känsliga som sekretesskyddade uppgifter i Box. Universitetet har dock i samband med sin risk- och sårbarhetsanalys av försiktighetsskäl bedömt att så inte bör ske.

Universitetet har bedömt att filytan håller en tillfredsställande säkerhetsnivå. Bedömningen har utgått ifrån säkerhetsåtgärder såsom åtkomst, access och behörighetstilldelning samt säkerhet i kommunikation.

Motivering av beslut

Gällande regler

Den personuppgiftsansvariges ansvar
Dataskyddsförordningen är den primära rättsliga regleringen vid behandling av personuppgifter.

Den personuppgiftsansvarige ansvarar för att kunna visa att de grundläggande principerna i artikel 5 i dataskyddsförordningen följs (artikel 5.2).

Den personuppgiftsansvarige ansvarar för att genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. Åtgärderna ska genomföras med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers fri-och rättigheter. Åtgärderna ska ses över och uppdateras vid behov. Det framgår av artikel 24.1 i dataskyddsförordningen.

Rättslig grund
Av artikel 6 i dataskyddsförordningen framgår följande.

En behandling är endast laglig om ett av de angivna villkoren i artikeln är uppfyllt (punkt 1).

En behandling är laglig om den är nödvändig för att utföra en uppgift av allmänt intresse (punkt 1 e). Forskningsändamål anses vara en uppgift av allmänt intresse.

Uppgiften av allmänt intresse ska vara fastställd i enlighet med unionsrätten eller nationell rätt (punkt 3). För statliga universitet och högskolor är forskningsuppgiften fastställd i 1 kap. högskolelagen (1992: 1434).

Som huvudregel är det förbjudet att behandla känsliga personuppgifter, till exempel personuppgifter om hälsa och sexualliv. Det finns dock ett antal undantag från förbudet i artikel 9.2 i dataskyddsförordningen. Av artikel 9.2 j i dataskyddsförordningen följer att behandlingen ska vara nödvändig för forskningsändamål och ska omfattas av lämpliga skyddsåtgärder för den registrerades rättigheter och friheter i enlighet med artikel 89.1 i dataskyddsförordningen.

Dessutom kräver undantaget från detta förbud att nationell rätt innehåller bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades personliga integritet. I etikprövningslagen[3] fastställs en sådan

[3] Lagen (2003:460) om etikprövning.

lämplig och särskild åtgärd som krävs vid behandling av känsliga personuppgifter för forskningsändamål. Även bestämmelser om sekretess i OSL är exempel på sådan lämplig och särskild åtgärd.

I artikel 89.1 i dataskyddsförordningen anges särskilda villkor för behandling av personuppgifter för forskningsändamål. Där anges att behandlingen ska omfattas av lämpliga skyddsåtgärder i enlighet med förordningen.

Kravet på säkerhet vid behandling av personuppgifter
En grundläggande princip för behandling av personuppgifter är kravet på säkerhet enligt artikel 5.1 f i dataskyddsförordningen, som anger att personuppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

Av artikel 32.1 i dataskyddsförordningen följer att den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken med behandlingen. Det med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter.

Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandlingen medför, i synnerhet från 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. Det framgår av artikel 32.2 i dataskyddsförordningen.

I skäl 75 i dataskyddsförordningen anges att olika faktorer ska beaktas vid bedömningen av risken för fysiska personers rättigheter och friheter. Bland annat nämns personuppgifter som omfattas av tystnadsplikt, uppgifter om hälsa eller sexualliv. Vidare ska beaktas om behandlingen gäller personuppgifter om sårbara fysiska personer, framförallt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.

Även skäl 39 och 83 ger vägledning om den närmare innebörden av dataskyddsförordningens krav på säkerhet vid behandling av personuppgifter.

Om den personuppgiftsansvarige anlitar ett personuppgiftsbiträde för att genomföra en behandling ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier för att genomföra lämpliga tekniska och organisatoriska åtgärder. Det ska ske på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen och att den registrerades rättigheter skyddas. Det framgår av artikel 28.1 och skäl 81 i dataskyddsförordningen. Dessa bestämmelser anger också hur förhållandet mellan den personuppgiftsansvarige och personuppgiftsbiträdet ska regleras.

Skyldighet att anmäla och dokumentera personuppgiftsincidenter
Enligt artikel 4.12 i dataskyddsförordningen är en personuppgiftsincident 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. Enligt Artikel 29-gruppens vägledning WP250[4] kan obehörig eller olaglig behandling innefatta utlämnandet av personuppgifter (eller åtkomst till dessa) till mottagare som inte är behöriga att motta (eller få åtkomst till) uppgifterna, eller någon annan form av behandling som strider mot dataskyddsförordningen.

Av artikel 33.1 i dataskyddsförordningen framgår att den personuppgiftsansvarige, vid en personuppgiftsincident, ska anmäla incidenten till tillsynsmyndigheten utan onödigt dröjsmål, och om så är möjligt inte senare än 72 timmar efter att ha fått vetskap om den. Om det är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter behöver den inte anmälas. Om en personuppgiftsansvarig inte agerar snabbt och det blir uppenbart att en

[4] Artikel 29 – Arbetsgruppen för uppgiftsskydd, WP250rev.01; Riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679; antagna den 3 oktober 2017; senast granskade och antagna den 6 februari 2018; antagna av Europeiska dataskyddsstyrelsen, EDPB, under det första plenarsammanträdet den 25 maj 2018; s. 11–12. Arbetsgruppen inrättades enligt artikel 29 i direktiv 95/46/EG och var ett oberoende rådgivande EU-organ i frågor rörande dataskydd och integritet.

incident har ägt rum kan detta betraktas som en underlåtelse att agera i enlighet med artikel 33[5].

Följande anges i skäl 85.

> En personuppgiftsincident som inte snabbt åtgärdas på lämpligt sätt kan för fysiska personer leda till fysisk, materiell eller immateriell skada, såsom förlust av kontrollen över de egna personuppgifterna eller till begränsning av deras rättigheter, diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, obehörigt hävande av pseudonymisering, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, eller till annan ekonomisk eller social nackdel för den berörda fysiska personen. Så snart en personuppgiftsansvarig blir medveten om att en personuppgiftsincident har inträffat, bör den personuppgiftsansvarige därför anmäla personuppgiftsincidenten till tillsynsmyndigheten utan onödigt dröjsmål och, om så är möjligt, inom 72 timmar efter att ha blivit medveten om denna, om inte den personuppgiftsansvarige, i enlighet med ansvarsprincipen, kan påvisa att det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för fysiska personers rättigheter och friheter.

Enligt Artikel 29-arbetsgruppen ska en personuppgiftsansvarig anses ha fått vetskap om incidenten när den personuppgiftsansvarige är rimligt säker på att en säkerhetsincident har ägt rum som har medfört att personuppgifter äventyrats. Den personuppgiftsansvarige ska, enligt dataskyddsförordningen, vidta alla lämpliga tekniska skyddsåtgärder och alla lämpliga organisatoriska åtgärder för att omedelbart fastställa om en personuppgiftsincident har ägt rum och skyndsamt informera tillsynsmyndigheten och de registrerade.

I skäl 87 i dataskyddsförordningen anges vikten av att kunna fastställa en incident, bedöma risken för enskilda och sedan anmäla incidenten om så krävs.

I artikel 33.5 i dataskyddsförordningen regleras skyldigheten att dokumentera personuppgiftsincidenter. Den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, oavsett om incidenten ska anmälas till Datainspektionen eller inte. Dokumentationen ska innehålla information om omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av artikel 33 i dataskyddsförordningen.

---

[5] WP250, revo1, s. 13.

Dokumentationsskyldigheten i artikel 33.5 är även kopplad till ansvarsskyldigheten i artikel 5.2 i dataskyddsförordningen, det vill säga att den personuppgiftsansvarige ska ansvara för och kunna visa att de grundläggande principerna för dataskydd efterlevs. Det finns även en koppling mellan artikel 33.5 och bestämmelsen om ansvaret för personuppgiftsansvarige enligt artikel 24 i dataskyddsförordningen.[6]

Det kan tilläggas att det av Artikel 29- gruppens riktlinjer framgår att den personuppgiftsansvarige behöver ha rutiner för att upptäcka och åtgärda incidenter som rör personuppgifter, vilket är innebörden av artikel 33.5. Dessutom framgår att förmågan att snabbt upptäcka, åtgärda och rapportera en incident bör ses som viktiga inslag i de lämpliga tekniska och organisatoriska åtgärder som anges i artikel 32 i dataskyddsförordningen.

Överföring av personuppgifter till tredje land
I kapitel V i dataskyddsförordningen anges de möjligheter som finns för att föra över personuppgifter till ett tredjeland (ett land utanför EES).

Personuppgifter får föras över om EU-kommissionen har beslutat att det finns en adekvat skyddsnivå i mottagarlandet eller om det annars finns lämpliga skyddsåtgärder till exempel genom avtalsklausuler eller bindande företagsbestämmelser.[7]

Av skäl 101 och 116 i dataskyddsförordningen framhålls risken när personuppgifter överförs till länder utanför unionen och vikten av att skyddsnivån inte blir lägre vid sådana överföringar. Det gäller i synnerhet i fråga om skyddet för otillåten användning eller otillåtet utlämnande av denna information. Vidare framhålls den personuppgiftsansvariges och personuppgiftsbiträdets ansvar att se till att förordningen följs.

Datainspektionens bedömning

Personuppgiftsansvar
Datainspektionen konstaterar att Umeå universitet är personuppgiftsansvarig för de behandlingar av personuppgifter som

[6] WP250, revo1, s. 28.
[7] Se artiklarna 44—50 i dataskyddsförordningen.

aktualiserats i ärendet fram till dess projektet överflyttades till Uppsala universitet under våren 2019.

Behandling av personuppgifter i okrypterad e-post och öppet nät
Datainspektionen konstaterar att Umeå universitet, inom ramen för forskningsprojektet, har skickat ett förundersökningsprotokoll rörande våldtäkter mot män i ett okrypterat e-postmeddelande via ett öppet nät till Polismyndigheten. Något som också universitetet har medgett.

Förundersökningsprotokollet innehåller uppgifter om hälsa och sexualliv som är känsliga personuppgifter. Behandling av känsliga personuppgifter kan innebära betydande risker för den personliga integriteten och därför krävs ett starkt skydd vid behandling av sådana uppgifter. Förundersökningsprotokollet innehåller dessutom uppgifter om misstanke om brott och personnummer som är så kallade integritetskänsliga personuppgifter. Behandlingen av denna typ av personuppgifter är därför av sådan art att uppgifterna måste ha ett starkt skydd. Det innebär att om dessa personuppgifter skickas via e-post måste de skyddas på ett sådant sätt att obehöriga inte kan ta del av dem. Personuppgifterna kan till exempel skyddas genom kryptering.

Att skicka information med okrypterad e-post innebär att även andra än den avsedda mottagaren kan ta del av uppgifterna i e-postmeddelandet. Därmed säkerställs inte att bara den avsedda mottagaren tar del av personuppgifterna.

Universitetet har dessutom skickat personuppgifterna via ett öppet nät. Ett öppet nät, exempelvis internet, karaktäriseras av att andra kan ta del av uppgifter som kommuniceras i nätet. Det innebär att obehöriga har kunnat få åtkomst till de personuppgifter som universitetet överfört.

Som personuppgiftsansvarig ska Umeå universitet se till att de tekniska och organisatoriska åtgärderna säkerställer en säkerhetsnivå som är lämplig i förhållande till de risker för fysiska personers rättigheter och friheter som behandlingen medför (artikel 32.1). Personuppgifterna som behandlas måste till exempel skyddas mot obehörigt röjande eller obehörig åtkomst.

Vad som är lämplig säkerhetsnivå varierar i förhållande till riskerna, behandlingens art, omfattning, sammanhang och ändamål. Vid

bedömningen måste därför exempelvis beaktas vad det är för typ av personuppgifter som behandlas.[8]

Universitetet måste identifiera de möjliga riskerna för de registrerades rättigheter och friheter och bedöma sannolikheten för att riskerna inträffar och konsekvenserna i sådana fall.

I detta fall är det frågan om såväl känsliga som integritetskänsliga personuppgifter. Behandling av denna typ av uppgifterna kräver ett starkt skydd utifrån behandlingens art.

Sammantaget finner Datainspektionen att Umeå universitet har behandlat personuppgifter i strid med dataskyddsförordningen genom att universitetet inte har vidtagit lämpliga tekniska säkerhetsåtgärder för att skydda personuppgifterna i e-postmeddelandet utifrån uppgifternas känslighet och hur de kommunicerats okrypterat över öppet nät. Behandlingen har därför skett i strid med artikel 5.1 f samt artikel 32.1 och 32.2 i dataskyddsförordningen.

Personuppgiftsincidenten borde ha dokumenterats och anmälts
Enligt Umeå universitet fick universitetet kännedom om att känsliga personuppgifter skickats via okrypterad e-post i och med att universitetet fick Datainspektionens tillsynsskrivelse den 30 augusti 2019. Enligt universitetet dokumenterades också incidenten, den 2 september 2019, i Datainspektionens blankett för anmälan av personuppgiftsincident.

Vad gäller vetskapen om incidenten konstaterar Datainspektionen att det av Polismyndighetens skrivelse daterad den 3 april 2019, framgår att Polismyndigheten vid kontakt med universitetet påpekat det olämpliga i att skicka känsliga personuppgifter via okrypterad e-post. Datainspektionen bedömer därför att universitetet måste ha fått vetskap om den aktuella incidenten före den 30 augusti 2019 och åtminstone senast den 3 april 2019.

Avseende dokumentationen finner Datainspektionen således att universitetet inte dokumenterade omständigheterna kring personuppgiftsincidenten direkt efter att ha fått vetskap om den. Detta försvårar möjligheten att kontrollera efterlevnaden av artikel 33 i

[8] Se skäl 75 och 76 i dataskyddsförordningen.

dataskyddsförordningen. Att universitetet i efterhand har fyllt i Datainspektionens blankett om anmälan om personuppgiftsincident ändrar inte bedömningen att universitetet borde ha dokumenterat incidenten redan när Polismyndigheten kontaktade universitetet.
Vidare konstaterar Datainspektionen att universitetet inte har kommit in med en anmälan om personuppgiftsincident till Datainspektionen. Enligt universitetet berodde det på att det var osannolikt att incidenten skulle medföra hög risk för enskildas fri- och rättigheter. Datainspektionen vill understryka att det alltid finns en risk för att obehöriga kan ta del av personuppgifterna om de skickas okrypterat via öppet nät. Som Datainspektionen tidigare konstaterat gäller utskicket såväl känsliga som integritetskänsliga personuppgifter. Risken för de registrerades fri- och rättigheter är därför hög om denna typ av personuppgifter behandlas på ett sådant sätt så att de till exempel kommer obehöriga till del.

Sammantaget finner Datainspektionen att Umeå universitet har underlåtit att agera i enlighet med artikel 33.1 och 33.5 i dataskyddsförordningen.

Lagring av känsliga personuppgifter i en molntjänst i tredje land
Umeå universitet har använt sig av molntjänsten Box för att lagra 108 förundersökningsprotokoll rörande våldtäkt mot män.

En molntjänst är en internetbaserad it-tjänst som tillhandahålls av en extern leverantör. Tjänsten kan innefatta lagring men även andra funktioner, där dessa helt eller till vissa delar finns utanför den egna verksamhetens interna it-miljö[9]. I det här fallet ligger lagringen utanför universitetets interna it-miljö. Via personuppgiftsbiträdet SUNET anlitar Umeå universitet underbiträdet Box.

Dataskyddsförordningen ställer inte bara krav på att den personuppgiftsansvarige ska säkerställa lämplig säkerhet för personuppgifterna. Förordningen ställer även krav på att den personuppgiftsansvarige ser till att personuppgiftsbiträdet uppfyller en sådan säkerhetsnivå vid behandling av personuppgifter för den personuppgiftsansvariges räkning.

[9] För ytterligare definitioner se Article 29 Data Protection Working Party, 01037/12/EN WP 196, Opinion 05/2012 on Cloud Computing.

Den personuppgiftsansvarige ansvarar också för att den som personuppgiftsbiträdet i sin tur anlitar uppfyller kraven i dataskyddsförordningen.

Box levereras av ett amerikanskt företag som lagrar informationen i USA. Enligt universitetet var Box ansluten till Privacy Shield och hade tecknat bindande företagsbestämmelser.

Personuppgifter får föras över till tredje land endast om villkoren i kapitel V i dataskyddsförordningen är uppfyllda. Det gäller under förutsättning att den personuppgiftsansvarige och personuppgiftsbiträdet kan säkerställa att den skyddsnivå som förordningen ger fysiska personer inte undergrävs.

Enligt ett beslut från EU-kommissionen[10] har det varit tillåtet för personuppgiftsansvariga i EU att överföra personuppgifter till mottagare som har anslutit sig till Privacy Shield.

I det så kallade Schrems II-målet[11] från den 16 juli 2020 bedömde emellertid EU-domstolen att Privacy Shield-avtalet mellan EU och USA inte ger tillräckligt skydd för personuppgifter när dessa förs över till USA. Det innebär att det inte längre är tillåtet för personuppgiftsansvariga i EU att med stöd av Privacy Shield föra över personuppgifter till USA.

Schrems II- målet kan även komma att påverka överföringar av personuppgifter som sker med hjälp av bindande företagsbestämmelser. Det då ett tredje lands lagstiftning kan komma att påverka skyddet som ges genom dessa bestämmelser. EU-domstolen har fastslagit att det är den personuppgiftsansvarige som ska bedöma om skyddsnivån som krävs enligt EU-lagstiftningen följs i det berörda tredje landet.

Datainspektionen konstaterar att Umeå universitet upphörde att behandla de aktuella personuppgifterna i molntjänsten Box våren 2019. Då var det enligt EU-kommissionens beslut tillåtet att överföra personuppgifter till USA med stöd av Privacy Shield. Datainspektionen stannar därför i aktuellt

[10] Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna.
[11] Mål C-311/18 – Data Protection Commissioner mot Facebook Ireland och Maximillian Schrems.

ärende med att konstatera att Box uppges ha varit ansluten till Privacy Shield vid den tidpunkten och att behandlingen vid universitetet upphört före Schrems II-målet.

Förutom att den personuppgiftsansvarige ska ha stöd för att föra över personuppgifter till tredjeland, ansvarar den personuppgiftsansvarige också för att personuppsgiftsbiträdet behandlar uppgifterna på ett sätt som säkerställer lämplig säkerhet.

Att personuppgifter, liksom personuppgiftsbiträdet, befinner sig i tredje land kan öka risken för att fysiska personer inte kan utöva sina dataskyddsrättigheter, i synnerhet för att skydda sig från otillåten användning eller otillåtet utlämnande av denna information.[12]

I detta fall är det frågan om uppgifter som är skyddade av sekretess.

För att få behandla känsliga personuppgifter ställer dataskyddsförordningen krav på att den nationella rätten ska innehålla bestämmelser om lämpliga och särskilda åtgärder. Bestämmelserna om sekretess till skydd för den enskilde är sådan reglering som skyddar enskildas integritet vid hanteringen av allmänna handlingar.[13] Det innebär att sekretessen är en integritetsskyddande åtgärd som den personuppgiftsansvarige och personuppgiftsbiträdet har att följa. När personuppgifterna lagras hos en aktör som inte omfattas av sekretess, innebär det ett svagare integritetsskydd för uppgifterna, eftersom en lagreglerad tystnadsplikt som är straffsanktionerad ger ett starkare skydd än en avtalad tystnadsplikt.[14]

Eftersom Box är en aktör som inte omfattas av OSL får personuppgifterna ett svagare integritetsskydd.

Det finns även tekniska svagheter i den valda lagringen.

För att få åtkomst till förundersökningsprotokollen i Box, har universitetet använt sig av en så kallad singelfaktorsautentisering. I detta fall högskole-ID (användarnamn) och lösenord.

---

[12] Jfr skäl 101 och 116 i dataskyddsförordningen.

[13] Se propositionen Ny dataskyddslag (prop. 2017/18:105 s. 116).

[14] JO:s beslut den 9 september 2014, dnr 3032-2011.

Autentiseringen används för att den personuppgiftsansvarige ska kunna se till att endast behöriga användare får åtkomst till personuppgifter.

Singelfaktorsautentisering är en svag form av autentisering. Risken att någon kan få del av användarnamn och lösenord är stor. Dessutom är det inte säkert att den som har blivit bestulen kommer att upptäcka att så har skett om någon kommer över användarnamn och lösenord genom till exempel så kallad phishing (nätfiske).

En starkare autentisering ska försvåra för obehöriga att komma över de nödvändiga inloggningsuppgifter som behövs för att kunna autentisera sig. Starkare autentisering kan uppnås genom att man använder sig av mer än en faktor (något man vet, något man har och något man är). Exempelvis kan ”något man vet” vara ett användarnamn eller lösenord, ”något man har” kan vara ett smartkort eller mobiltelefon och ”något man är” kan vara ett fingeravtryck eller ansiktsdrag.

Användaren kan få tillgång till de lagrade uppgifterna i Box genom att logga in via ett webbgränssnitt internt via universitetets nätverk med singelfaktorsautentisering (det vill säga användarnamn och lösenord). Det går även att logga in externt via internet på universitetets webbplats umu.se. Inloggningen sker då via valfri utrustning och valfritt nät och användaren uppger först sin e-postadress och därefter sitt högskole-ID (användarnamn) och lösenord (det vill säga med singelfaktorsautentisering).

Eftersom åtkomst till de aktuella uppgifterna kan ske via det öppna nätet är exponeringsytan mot obehöriga mycket stor, vilket medför att risken för att uppgifterna kommer obehöriga till del ökar.

Umeå universitet har anfört att kommunikationen och lagringen av uppgifterna i förundersökningsprotokollen har krypterats i Box. Datainspektionen anser dock inte att det innebär att uppgifterna är tillräckligt skyddade mot obehörig åtkomst. Exempelvis kan den som olovligt kommit över användarnamn och lösenord utge sig som behörig och därmed ta del av uppgifterna i klartext.

Som tidigare angetts ska den personuppgiftsansvarige säkerställa en lämplig säkerhet i förhållande till risken med behandlingen. Det gäller även när

personuppgifterna behandlas av ett personuppgiftsbiträde. Den personuppgiftsansvarige måste därför göra en bedömning av de risker som kan uppstå i samband med behandlingen. När den personuppgiftsansvarige behandlar personuppgifter i en molntjänst behöver den ansvarige genomföra en lämplighetsbedömning som innefattar en riskanalys. På så sätt får den personuppgiftsansvarige ett underlag för att kunna fatta beslut om vilka lämpliga tekniska och organisatoriska åtgärder som behövs eller som bör krävas av personuppgiftsbiträdet. Det ger också den personuppgiftsansvarige en möjlighet att säkerställa en säkerhetsnivå som är lämplig.

Vid bedömning av säkerhetsnivån vid lagring och överföring av personuppgifter ska särskild hänsyn tas till om behandlingen medför risk för obehörigt röjande eller obehörig åtkomst.

Umeå universitet har uppgett att universitetet i samband med sin risk- och sårbarhetsanalys bedömde att känsliga personuppgifter inte bör lagras i Box av försiktighetsskäl. Denna information publicerades på universitetets intranät i september 2016. Trots det skannade universitetet in förundersökningsprotokollen och lagrade dem i Box.

Förundersökningsprotokollen rör våldtäkter mot män och personuppgifterna i dem är såväl känsliga, som integritetskänsliga. Uppgifterna omfattas dessutom av sekretess. Datainspektionens bedömning är att behandlingen av denna typ av personuppgifter innebär en hög risk för de enskildas integritet om personuppgifterna röjs eller om någon obehörig får åtkomst till dem. Behandlingen är därför av sådan art att den kräver en hög säkerhet.

Datainspektionen konstaterar att det har varit frågan om en behandling av personuppgifter i en molntjänst i USA som inte omfattas av bestämmelserna i OSL, och att säkerheten inte har varit tillräckligt hög för att förhindra obehörig åtkomst till uppgifterna. Dessutom konstaterar Datainspektionen att universitetet 2016 bedömde att behandlingen av känsliga personuppgifter i Box inte var lämpligt.

Datainspektionen finner sammanfattningsvis att Umeå universitet inte har vidtagit lämpliga tekniska och organisatoriska åtgärder för att förhindra obehörigt röjande av eller obehörig åtkomst till de känsliga och integritetskänsliga personuppgifterna som lagrats i Box. Universitetet har därigenom inte säkerställt en säkerhetsnivå som är lämplig i förhållande till

risken med att behandla de personuppgifter som det är frågan om i ärendet. Umeå universitet har därmed behandlat personuppgifterna i strid med artikel 5.1 f samt artikel 32.1 och 32.2 i dataskyddsförordningen.

Val av ingripande

Rättslig reglering
Datainspektionen har vid överträdelser av dataskyddsförordningen ett antal korrigerande befogenheter, bland annat reprimand, föreläggande och sanktionsavgifter. Det följer av artikel 58.2 a–j i dataskyddsförordningen.

Datainspektionen ska påföra sanktionsavgifter utöver eller i stället för andra korrigerande åtgärder som avses i artikel 58.2, beroende på omständigheterna i varje enskilt fall.

Medlemsstaterna får fastställa regler för om och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter.
Det framgår av artikel 83.7 i förordningen. Sverige har i enlighet med detta beslutat att Datainspektionen ska få ta ut sanktionsavgifter av myndigheter. För överträdelser av bland annat artiklarna 32 och 33 ska avgiften uppgå till högst 5 000 000 kronor. För överträdelser av bland annat artikel 5 i förordningen ska avgiften uppgå till högst 10 000 000 kronor. Det framgår av 6 kap. 2 § dataskyddslagen samt artikel 83.4 och 83.5 i dataskyddsförordningen.

Om en personuppgiftsansvarig eller ett personuppgiftsbiträde, med avseende på en och samma eller sammankopplade uppgiftsbehandlingar, uppsåtligen eller av oaktsamhet överträder flera av bestämmelserna i denna förordning får den administrativa sanktionsavgiftens totala belopp inte överstiga det belopp som fastställs för den allvarligaste överträdelsen. Det framgår av artikel 83.3 i dataskyddsförordningen.

Varje tillsynsmyndighet ska säkerställa att påförandet av administrativa sanktionsavgifter i varje enskilt fall är effektivt, proportionellt och avskräckande. Det anges i artikel 83.1 i dataskyddsförordningen.

I artikel 83.2 anges de faktorer som ska beaktas för att bestämma om en administrativ sanktionsavgift ska påföras, men också vad som ska påverka sanktionsavgiftens storlek.

Sanktionsavgiftens storlek
Universitetet har skickat ett förundersökningsprotokoll med personuppgifter om bland annat hälsa, sexualliv och misstanke om brott via okrypterad e-post och genom öppet nät. Personuppgifterna som behandlats är både känsliga och integritetskänsliga samt omfattas av bestämmelser om sekretess.
Polismyndigheten skickade uppgifterna till universitetet via bud, vilket borde gjort universitetet uppmärksamt på uppgifternas skyddsvärde. Trots detta underlät universitetet att vidta lämpliga tekniska säkerhetsåtgärder. Personuppgifterna skyddades därmed inte från risken att utsättas för bland annat obehörigt röjande och obehörig åtkomst. Datainspektionen finner att ingen annan bedömning kan göras än att överträdelsen skett genom oaktsamhet.

Dessutom har Umeå universitet lagrat ett stort antal, 108 stycken, förundersökningsprotokoll med känsliga och integritetskänsliga personuppgifter i molntjänsten Box. Detta utan att universitetet säkerställt en lämplig säkerhetsnivå för att kunna lagra denna typ av personuppgifter i Box. Universitetet underlät således även i denna del att vidta lämpliga tekniska säkerhetsåtgärder. Universitetet säkerställde inte heller att personuppgifterna omfattades av sådana lämpliga organisatoriska åtgärder som krävs enligt dataskyddsbestämmelserna.

I strid mot sin egen risk- och sårbarhetsanalys lagrade universitetet de känsliga personuppgifterna i Box. Datainspektionen anser att detta är en faktor som måste beaktas vid bedömning av sanktionsavgiftens storlek.

Vidare har universitetet underlåtit att anmäla personuppgiftsincidenten som uppstod vid utskicket i e-postmeddelandet till Datainspektionen. Inte heller dokumenterades omständigheterna kring incidenten då universitetet blev uppmärksammat på den.

Mot denna bakgrund finner Datainspektionen att Umeå universitet genom de aktuella personuppgiftsbehandlingarna har överträtt artikel 5.1 f, artikel 32.1 och 32.2 samt artikel 33.1 och 33.5 i dataskyddsförordningen. Datainspektionen anser därför att Umeå universitet ska påföras administrativa sanktionsavgifter för nämnda överträdelser.

Datainspektionen konstaterar att behandlingarna via e-post och lagringen i Box avser två sammankopplade uppgiftsbehandlingar enligt artikel 83.3 i dataskyddsförordningen. Detta då behandlingarna rör samma personuppgifter inom ett forskningsprojekt och avser överträdelse av samma bestämmelser det vill säga artikel 5.1 f samt 32.1 och 32.2 i förordningen.

Vid bestämmande av sanktionsavgiftens storlek beaktar Datainspektionen ovan angivna omständigheter och att den administrativa sanktionsavgiften ska vara effektiv, proportionell och avskräckande. Att Umeå universitet inte har uppfyllt säkerhetskraven är allvarligt då det är frågan om personuppgifter av sådan typ att uppgifterna kräver ett starkt skydd utifrån behandlingens art.

Datainspektionen bestämmer utifrån en samlad bedömning att Umeå universitet ska betala en administrativ sanktionsavgift på totalt 550 000 kronor. För utskicket i e-postmeddelandet och lagringen i molntjänsten Box ska universitetet betala en avgift på 450 000 kronor. För universitetets underlåtenhet att anmäla personuppgiftsincidenten till Datainspektionen och för att inte ha dokumenterat incidenten ska universitetet betala en avgift på 100 000 kronor.

Detta beslut har fattats av generaldirektören Lena Lindgren Schelin efter föredragning av juristen Linda Hamidi. Vid handläggning av ärendet har juristen Caroline Cruz Julander medverkat. Vid den slutliga handläggningen har enhetscheferna Katarina Tullstedt och Malin Blixt samt it-säkerhetsspecialisterna Johan Ma och Ulrika Sundling medverkat.

Lena Lindgren Schelin, 2020-12-10 (Det här är en elektronisk signatur)

Bilaga
Information om betalning av sanktionsavgift.

Kopia för kännedom till
Dataskyddsombudet.

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut ni överklagar och den ändring som ni begär. Överklagandet ska ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades. Om överklagandet har kommit in i rätt tid sänder Datainspektionen det vidare till Förvaltningsrätten i Stockholm för prövning.

Ni kan e-posta överklagandet till Datainspektionen om det inte innehåller några integritetskänsliga personuppgifter eller uppgifter som kan omfattas av sekretess. Myndighetens kontaktuppgifter framgår av beslutets första sida.