Datainspektionen

Datum	Diarienr
2014-11-17	1713-2013

Uppsala Universitet
Box 256
751 05 Uppsala

Tillsyn enligt personuppgiftslagen (1998:204) – Hantering av känsliga personuppgifter via e-post

Datainspektionens beslut

Datainspektionen förelägger Uppsala universitet att senast den 13 februari 2015 inkomma med en skriftlig policy för hur forskare får hantera känsliga personuppgifter i e-post.

Bakgrund

Datainspektionen inledde den 25 maj 2011 en inspektion av Uppsala universitets rutiner för hantering av personuppgifter via e-post, särskilt inom ramen för kliniska prövningar, diarienummer 752-2011. Datainspektionen konstaterade i beslut den 24 februari 2012 att det inte fanns några dokumenterade rutiner angående kommunikation av känsliga personuppgifter via e-post inom ramen för kliniska prövningar vid Uppsala universitet. Datainspektionen konstaterade vidare att det fanns grundläggande oklarheter kring skyddet för känsliga personuppgifter i e-post inom ramen för kliniska prövningar vid Uppsala universitet. Datainspektionen förelade därför Uppsala universitet att upprätta en skriftlig policy för hur och under vilka omständigheter universitetets forskare får hantera känsliga personuppgifter i e-post.

Redogörelse för tillsynsärendet

Datainspektionen beslutade den 24 oktober 2013 att följa upp ärendet och begärde att den skriftliga policyn skulle ges in. Uppsala Universitet inkom den 30 oktober 2013 med ett yttrande och bifogade handboken *Hanterig av allmänna handlingar vid universitetet* daterad maj 2006 och uppdaterad maj 2013 (handboken).

Postadress: Box 8114, 104 20 Stockholm
Besöksadress: Drottninggatan 29, plan 5
Webbplats: www.datainspektionen.se
E-post: datainspektionen@datainspektionen.se
Telefon: 08-657 61 00
Telefax: 08-652 86 52

Datainspektionen ställde en fråga, i ett kompletterande yttrande den 12 december 2013, om handboken skulle avses vara en skriftlig policy för hur universitetets forskare får hantera känsliga personuppgifter i e-post.

Universitetet inkom med ett svar den 2 december 2013 som innehöll ett utdrag ur handboken och bifogade dokumenten *Riktlinjer för säkerhetsarbete vid Uppsala universitet* och *Riktlinjer inom IT-området*, reviderad 2013-10-30.

Utdraget ur handboken lyder som följer.

> *När känsliga personuppgifter kommuniceras via öppna nät t.ex. via e-post, ska uppgifterna vara krypterade på ett sådant sätt att endast avsedda mottagare kan ta del av uppgifterna. Kryptering kan göras med tekniker för att säkra kommunikationsprotokoll (SSL/TLS motsv.)*

Skäl för beslutet

Datainspektionens föreläggande den 24 februari 2012 innebar att Uppsala Universitet skulle upprätta en skriftlig policy för hur och under vilka omständigheter universitetets forskare får hantera känsliga personuppgifter i e-post. Syftet med policyn är att den enskilde forskaren ska förstå vilka uppgifter som är känsliga och hur dessa ska hanteras om de ska skickas via e-post.

Datainspektionen anser att Uppsala universitets rutiner för e-post är otydliga och ofullständiga då det enligt Datainspektionens uppfattning krävs betydande förhandskunskaper och tekniska hjälpmedel för att användare, utifrån de ingivna dokumenten, ska förstå vad som förväntas av den enskilde forskaren när det gäller hantering av känsliga personuppgifter i e-post.

Att enbart ange att känsliga personuppgifter som kommuniceras via öppna nät ska krypteras kan inte anses som tillräckligt i en policy riktad till användarna. Datainspektionen vill erinra om att även andra personuppgifter kan omfattas av kravet på kryptering. Vid bedömning enligt 31 § personuppgiftslagen av *hur pass* känsliga uppgifterna är ska särskilt beaktas om personuppgifterna definieras som känsliga i 13 § personuppgiftslagen eller *på annat sätt* är integritetskänsliga, till exempel genom att behandlingen av dem omfattas av särreglering, samt om de omfattas av tystnadsplikt eller sekretess enligt offentlighets- och sekretesslagen (2009:400) eller annan lagstiftning.

Det måste också tydligare framgå vad som avses med kryptering och hur användaren kan se till att kryptering sker. Att uppge att användarna ska använda SSL/TLS är inte någon tydlig instruktion. SSL/TLS är ett sätt att kryptera förbindelsen (skydda kommunikationen) mellan e-post servern och anslutande klient. Det innebär i sig inte att innehållet i e-post meddelandet är skyddat så

att endast avsedd mottagare kan ta del av informationen. Det är dessutom något som den enskilde användaren sällan kan påverka.

Datainspektionen konstaterar sammanfattningsvis att rutinerna kring universitetets e-posthantering behöver utvecklas och förtydligas.

Av policyn bör det framgå vad den avser, vem/vilka som berörs, när och hur den ska tillämpas. Vilka medel och metoder det finns för att tillämpa policyn och gärna en steg för steg instruktion som hjälper användarna att göra rätt.

Rutiner och instruktioner ska enligt Datainspektionens uppfattning vara utformade så att den personuppgiftsansvarige och befattningshavare under dess ledning kan följa gällande rätt. Det är därför viktigt att rutiner och instruktioner är så tydliga att missförstånd och misstag kan undvikas.

Datainspektionen konstaterar att Uppsala universitet inte följt föreläggandet från den 24 februari 2012. Datainspektionen förelägger därför Uppsala universitet att inkomma med en skriftlig policy för hur och under vilka omständigheter universitetets forskare får hantera känsliga personuppgifter i e-post.

Hur man överklagar
Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Överklagandet ska ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades för att kunna prövas. Datainspektionen sänder överklagandet vidare till Förvaltningsrätten i Stockholm för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Detta beslut har fattats av enhetschefen Katarina Tullstedt efter föredragning av IT-säkerhetsspecialisten Fredrik Ekman. I ärendets slutgiltiga handläggning har också IT-säkerhetsspecialisten Magnus Bergström deltagit.

Katarina Tullstedt

Fredrik Ekman

Kopia till:
Personuppgiftsombudet, via e-post.