AB3

Datainspektionen

Fotokopians överensstämmelse med originalet intygas:

Beslut 2017-06-22

Diarienr 2407-2016

Blekinge Tekniska Högskola
371 79 Karlskrona

Tillsyn enligt personuppgiftslagen (1998:204) - angående behandling av personuppgifter i Nais

Datainspektionens beslut

Datainspektionen konstaterar att Blekinge Tekniska Högskola behandlar personuppgifter i strid med 15 § personuppgiftslagen (1998:204) eftersom samtycket inte kan anses vara frivilligt.

Datainspektionen förelägger Blekinge Tekniska Högskola att upphöra att behandla känsliga personuppgifter med stöd av 15 § personuppgiftslagen och att utreda om något annat undantag kan bli tillämpligt vid behandling av känsliga personuppgifter.

Datainspektionen konstaterar att uppgift om den personuppgiftsansvariges identitet, i strid med 25 § personuppgiftslagen, saknas i den information som den registrerade får.

Datainspektionen förelägger Blekinge Tekniska Högskola att komplettera informationen så att det är tydligt för den registrerade vem som är personuppgiftsansvarig.

Datainspektionen konstaterar att Blekinge Tekniska Högskolas behandling av personuppgifter i Nais i samband med handläggning av ansökan om särskilt pedagogiskt stöd inte uppfyller säkerhetskraven i 31 § personuppgiftslagen beträffande åtkomst till känsliga personuppgifter över öppet nät.

Datainspektionen förelägger Blekinge Tekniska Högskola mot bakgrund av detta att vidta åtgärder för att säkerställa att endast de avsedda mottagarna kan ta del av personuppgifter i Nais, exempelvis genom att använda e-

legitimation för samtliga användare som har åtkomst till uppgifter som rör studenternas personliga förhållanden via internet.

Datainspektionen förelägger Blekinge Tekniska Högskola att skicka in en åtgärdsplan som beskriver vilka åtgärder Blekinge Tekniska Högskola har vidtagit eller ska vidta för att rätta till de brister som framgår av Datainspektionens beslut rörande det rättsliga stödet. Av planen ska även framgå när åtgärderna ska vidtas. Åtgärdsplanen ska ha kommit in till Datainspektionen senast 18 september 2017.

Datainspektionen förutsätter att Blekinge Tekniska Högskola klargör vilken annan rättslig grund än samtycke som utgör det rättsliga stödet enligt 10 § personuppgiftslagen.

Redogörelse för tillsynsärendet

Datainspektionen har mottagit klagomål som gör gällande att det på webbplatsen https://www.nais.uhr .se inte finns upplysning till de registrerade hur deras personuppgifter behandlas och vem som har tillgång till uppgifterna. Datainspektionen beslutade mot bakgrund av klagomålet att inleda tillsyn mot Universitets- och högskolerådet (UHR). UHR visade sig dock vara personuppgiftsbiträde till respektive lärosäte. I ärendet framkom också att 27 lärosäten är anslutna till Nationellt administrations- och informationssystem för samordnare av särskilt pedagogiskt stöd, Nais varav Blekinge Tekniska Högskola är en av dem. Datainspektionen har mot den bakgrunden inlett tillsyn mot Blekinge Tekniska Högskola.

Skäl för beslutet

Personuppgiftsansvar

Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter är personuppgiftsansvarig för behandlingen. Personuppgiftsansvarig är normalt den juridiska person eller den myndighet som behandlar personuppgifter i sin verksamhet och som bestämmer vilka uppgifter som ska behandlas och vad uppgifterna ska användas till. Blekinge Tekniska Högskola (BTH) har uppgett sig vara personuppgiftsansvarig för behandling av personuppgifter i Nais.

Rättsligt stöd

För att en behandling över huvud taget ska vara tillåten måste den personuppgiftsansvarige finna ett stöd för behandlingen i 10 § personuppgiftslagen. Vid behandling av känsliga personuppgifter måste behandlingen dessutom vara tillåten enligt bestämmelserna i 13- 20 §§ personuppgiftslagen. Känsliga personuppgifter är enligt personuppgiftslagen sådana som avslöjar, ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter som rör hälsa eller sexualliv. Enligt 13 § personuppgiftslagen finns ett principiellt förbud mot behandling av känsliga personuppgifter. I 14- 20 §§ personuppgiftslagen anges när känsliga personuppgifter trots förbudet får behandlas. Vid behandling av känsliga personuppgifter, i det här fallet uppgifter om funktionsnedsättning, måste således den personuppgiftsansvarige finna ett stöd för behandlingen i något av undantagen.

BTH har uppgett att det rättsliga stödet vid registrering av enskildas uppgifter om funktionsnedsättning (bl.a. intyg på funktionsnedsättningen som studenten ska bifoga) sker genom att studenten samtycker till behandlingen enligt 15 § personuppgiftslagen. Datainspektionen uppfattar att BTH med svaret menar att samtycke utgör både det rättsliga stödet enligt 10 § och undantag för behandling av känsliga personuppgifter enligt 15 §.

Vidare uppges att BTH rapporterar in statistikuppgifter till Stockholms universitet (SU) som har ett särskilt åtagande att fördela bidrag för ett särskilt pedagogiskt stöd för studenter med funktionshinder i studiesituationen och i mån av behov fördela de nationella medel som anvisas för ändamålet. Statistiken som BTH anger sig rapportera till SU består av uppgift om antal studenter, fördelning av funktionsnedsättning samt kön och sker med stöd av 19 § 2 st. personuppgiftslagen.

För att ett samtycke ska kunna tillämpas enligt personuppgiftslagen måste samtycket vara frivilligt och informerat. Behandlingen innefattar här myndighetsutövning gentemot den enskilda eftersom högskolan fattar ett beslut om studenten kan få ett särskilt pedagogiskt stöd. Är situationen sådan att den registrerade i praktiken inte kan avstå en behandling, kan samtycket inte vara "frivilligt". Även förhållandet mellan den som behandlar uppgifterna och den registrerade påverkar möjligheten till frivilligt samtycke. För att ett

samtycke ska vara att anse som frivilligt kan det inte finnas ett beroendeförhållande såsom det finns vid exempelvis myndighetsutövning.

Detta har kommit till uttryck ännu tydligare i den kommande dataskyddsförordningen som ersätter personuppgiftslagen från och med 25 maj 2018. I dataskyddsförordningen anges att för att säkerställa att det är frågan om ett frivilligt samtycke bör det inte utgöra den rättsliga grunden för behandlingen i fall där det råder ojämlikhet mellan den registrerade och den personuppgiftsansvarige, särskilt om den personuppgiftsansvarige är en offentlig myndighet (se skäl 43 dataskyddsförordningen). Datainspektionens bedömning är att det inte är möjligt att i denna situation få ett samtycke som uppfyller kraven på frivillighet. BTH behöver därför ha en annan rättslig grund än samtycke för behandlingen och ett annat undantag för att få behandla känsliga personuppgifter.

Datainspektionen förelägger BTH att upphöra att behandla känsliga personuppgifter med stöd av 15 § personuppgiftslagen och att utreda vilket annat undantag som kan bli tillämpligt vid behandling av känsliga personuppgifter. Det är viktigt att notera att när det gäller den personuppgiftsbehandling som erfodras måste den från och med 25 maj 2018 ske i enlighet med den kommande dataskyddsförordningen.

Informationsskyldighet

När personuppgifter samlas in och behandlas måste de personer som registreras bli informerade om detta. Det är den personuppgiftsansvarige som ska se till att den registrerade får den information som krävs. Enligt personuppgiftslagen finns det en långtgående informationsskyldighet för den personuppgiftsansvarige att informera den registrerade om behandlingen (23-24 §§). Av informationen ska framgå uppgift om den personuppgiftsansvariges identitet, uppgift om ändamålen med behandlingen och all övrig information som behövs för att den registrerade ska kunna ta tillvara sina rättigheter i samband med behandlingen, såsom information om mottagarna av uppgifterna, skyldighet att lämna uppgifter och rätten att ansöka om information och få rättelse (25 §).

BTH har bifogat den information om personuppgiftsbehandlingen som den registrerade får i samband med ansökan om särskilt pedagogiskt stöd. Av den framgår bl.a. uppgift om vilka personuppgifter som behandlas, vilka som har

åtkomst till uppgifterna, vad personuppgifterna kommer att användas till samt vilka rättigheter den som ansöker om särskilt pedagogiskt stöd har.

Datainspektionen konstaterar att uppgift om den personuppgiftsansvariges identitet saknas i den information som den registrerade får. Datainspektionen förelägger BTH att i enlighet med 25 § personuppgiftslagen komplettera informationen så att det är tydligt för den registrerade vem som är personuppgiftsansvarig och således vem som den registrerade kan vända sig för att tillvarata sina rättigheter.

Säkerhet

BTH uppger vidare att samordnaren och administratören, det vill säga chefen för studerandeavdelningen, har åtkomst till personuppgifter i systemet via internet. För åtkomst till personuppgifter i systemet krävs inloggning med lösenord.

De personuppgifter som behandlas när en student gör en ansökan om särskilt pedagogiskt stöd är namn, personnummer, kontaktuppgifter (e-post och telefonnummer), "godkännande av PuL" samt intyg på funktionsnedsättningen.

Enligt 31 § personuppgiftslagen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur pass känsliga de behandlade personuppgifterna är.

Den skyldighet som den personuppgiftsansvarige har för att vidta säkerhetsåtgärder innebär att när känsliga eller integritetskänsliga behandlas ska uppgifterna skyddas på ett sådant sätt att obehöriga inte kan ta del av dem. När sådana personuppgifter kommuniceras via internet ska den personuppgiftsansvarige därför använda stark autentisering vid åtkomst till uppgifterna, exempelvis e-legitimation, engångslösenord eller motsvarande. Datainspektionen har tagit fram riktlinjer för personuppgiftsbehandling i skolverksamhet, *Checklista för skolor*, som beskriver kraven för åtkomst till särskilt integritetskänsliga personuppgifter via webbaserade IT-system. Checklistan finns på följande länk: http://www.datainspektionen.se/lagar-

och-regler/personuppgiftslagen/skolor/checklista-for-hantering-av-personuppgifter/.

Datainspektionen konstaterar att det enligt 31 § personuppgiftslagen gäller samma säkerhetskrav för samtliga användare som har åtkomst till känsliga personuppgifter vid inloggning till webbaserade IT-system. Högskolans behandling av personuppgifter i Nais i samband med handläggning av ansökan av särskilt pedagogiskt stöd uppfyller därmed inte säkerhetskraven i personuppgiftslagen beträffande åtkomst till känsliga personuppgifter över internet. Datainspektionen förelägger Blekinge Tekniska Högskola mot bakgrund av detta att vidta åtgärder för att säkerställa att endast de avsedda mottagarna kan ta del av personuppgifter i Nais, exempelvis genom att använda e-legitimation för samtliga användare som har åtkomst till uppgifter som rör studenternas personliga förhållanden via internet.

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. 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 juristen Salomeh Fanaei.

Katarina Tullstedt

Salomeh Fanaei

Vid den slutliga handläggningen av ärendet har även it-säkerhetsspecialisten Magnus Bergström deltagit.

Kopia till:

Personuppgiftsombudet.