Datainspektionen

Beslut
2011-04-01

Diarienr
1735-2010

Centrala Studiestödnämnden – CSN

851 82 Sundsvall

Tillsyn enligt personuppgiftslagen (1998:204) – Utökat elektroniskt informationsutbyte

Datainspektionens beslut

CSN har inhämtat en försäkran om tekniska begränsningar från anslutande socialnämnder. CSN föreläggs dock att upphöra med att lämna ut uppgifter om enskilda via direktåtkomst till Socialnämnden i Botkyrka till dess att CSN – även på annat sätt – försäkrat sig om att handläggare hos Socialnämnden i Botkyrka rent tekniskt inte ska ha möjlighet att söka på andra personer än sådana som är aktuella i ett ärende hos nämnden.

Datainspektionen utgår ifrån att CSN vidtar åtgärder för att försäkra sig om att de socialnämner som använder Sambruks lösning, Multifråga, har tekniska begränsningar på plats som förhindrar handläggare att söka på andra personer än sådana som är aktuella i ett ärende hos nämnden.

Datainspektionen kan konstatera att CSN loggar vilken socialnämnd som haft åtkomst till vilka personuppgifter och när, och förutsätter att CSN också utför systematiska och återkommande loggkontroller av socialnämndernas åtkomst till personuppgifter på socialnämndnivå.

Datainspektionen förutsätter att CSN genomför de planerade åtgärderna för att uppfylla kraven i 7 och 14 §§ studiestödsdataförordningen.

Ärendet avslutas.

Bakgrund

Den 1 januari 2009 trädde ett antal nya bestämmelser i kraft som innebär ett utökat elektroniskt informationsutbyte mellan myndigheter (se prop.

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

2007/08:160). Informationsutbytet ska huvudsakligen ske genom s.k. direktåtkomst. Datainspektionen inledde under 2010 ett projekt för att hos två statliga myndigheter och två socialnämnder granska hur informationsutbytet ser ut och om tillämpliga bestämmelser följs. Av särskilt intresse har varit systemens utformning och datakommunikation, information till registrerade och hanteringen av skyddade personuppgifter.

Redogörelse för tillsynsärendet

Datainspektionen har den 2 december 2010 genomfört en inspektion hos CSN. Inspektionen är ett led i Datainspektionens projekt rörande informationsutbyte mellan myndigheter.

Skäl för beslutet

Kravet på försäkran från socialnämnderna

Av andra stycket 13 § studiestödsdataförordningen framgår att en socialnämnd får ha direktåtkomst enligt första stycket först sedan CSN har försäkrat sig om att handläggare hos socialnämnden bara kan ta del av uppgifter om personer som är aktuella i ärenden hos socialnämnden.

För att uppfylla det kravet kräver CSN att socialnämnderna skriver under en skriftlig försäkran om att handläggare hos socialnämnden bara kan ta del av uppgifter om personer som är aktuella i ärenden hos socialnämnden. Försäkran lyder:

> ”Härmed försäkras att Socialnämnden i X kommun har vidtagit de tekniska och administrativa åtgärder som krävs för att säkra att anställda vid socialnämnden, vid direktåtkomst till personuppgifter som behandlas i CSN:s studiestödsverksamhet, bara kan ta del av uppgifter om personer som är aktuella i ärenden hos socialnämnden.”

Frågan är om detta är tillräckligt för att uppfylla förordningens krav.

Denna fråga behandlas inte närmare i förarbetena till studiestödsdatalagstiftningen (problematiken nämns endast vid ett tillfälle, se SOU 2007:64 s. 171). I den proposition som ligger till grund för bestämmelserna om socialnämndernas möjlighet till direktåtkomst hos ett antal olika myndigheter konstaterades att socialnämnderna borde ges möjlighet till direktåtkomst till uppgifter hos CSN, men något lagförslag lämnades inte eftersom CSN då saknade registerlagstiftning (prop. 2007/08:160 s. 151). Vad som anförs i den propositionen bör därför kunna ge ledning avseende det krav som andra stycket 13 § studiestödsdataförordningen ställer på CSN. Där framgår att utlämnande myndig-

het är skyldig att försäkra sig om att handläggare hos socialnämnderna rent tekniskt inte ska ha möjlighet att söka på andra personer än sådana som är aktuella i ett ärende hos den aktuella nämnden. Vidare framgår att det är tillräckligt att utlämnande myndighet från den mottagande socialnämnden inhämtar en försäkran om att dessa krav är uppfyllda (prop. 2007/08:160 s. 167, 169 och 170). Lagstiftaren har inte haft för avsikt att införa en skyldighet för utlämnande myndighet att genomföra faktiska kontroller av landets socialnämnder (prop. 2007/08:160 s. 150).

Datainspektionen anser därför att CSN, genom inhämtande av en sådan underskriven försäkran som CSN använder sig av, i princip uppfyller kravet i 13 § studiestödsdataförordningen.

I det här sammanhanget vill Datainspektionens göra CSN uppmärksam på vissa omständigheter som framkommit under Datainspektionens inspektion hos en av landets socialnämnder som använder Sambruks lösning, Multifråga. Vid inspektionen framkom att CSN har inhämtat en skriftlig försäkran från socialnämnden men att nämnden inte har några tekniska begränsningar på plats som gör det möjligt för handläggarna att endast söka på personer som är aktuella i ett ärende hos nämnden (Socialnämnden i Botkyrka kommun, dnr 1579-2010).

Datainspektionen anser att den beskrivna situationen visar att det kan finnas tillfällen då endast förekomsten av en underskriven försäkran från socialnämnden inte är tillräcklig. CSN måste normalt kunna utgå ifrån att den socialnämnd som skriver under en sådan försäkran som CSN använder sig av, faktiskt lever upp till de krav som ställs i försäkran. Men om det senare skulle framkomma omständigheter som ger CSN skälig anledning att misstänka att så inte är fallet anser Datainspektionen att CSN, också mot bakgrund av kravet på lämpliga säkerhetsåtgärder i 31 § personuppgiftslagen, har ett ansvar för att ta reda på hur det faktiskt förhåller sig och i tillämpliga fall begränsa åtkomsten till dess att CSN även på annat sätt kunnat försäkra sig om att den mottagande socialnämnden har tillfredställande tekniska begränsningar.

CSN föreläggs därför att upphöra med att tillhandahålla uppgifter via direktåtkomst till Socialnämnden i Botkyrka till dess att CSN på annat sätt försäkrat sig om att handläggare hos Socialnämnden i Botkyrka rent tekniskt inte ska ha möjlighet att söka på andra personer än sådana som är aktuella i ett ärende hos nämnden.

Upplysningsvis meddelar Datainspektionen att Socialnämnden i Botkyrka i beslut, med dnr 1579-2010, förelagts att införa tekniska begränsningar i Multifråga till pågående ärenden hos nämnden.

Datainspektionen antar att det finns andra kommuner än Socialnämnden i Botkyrka som fortfarande använder sig av Sambruks lösning. Eftersom det nu är känt för CSN att Multifråga inte innehåller några tekniska begränsningar utgår Datainspektionen ifrån att CSN vidtar åtgärder för att försäkra sig om att de socialnämner som använder Multifråga har tekniska begränsningar på plats som förhindrar handläggare att söka på andra personer än sådana som är aktuella i ett ärende hos nämnden.

Datainspektionen har inga anmärkningar i denna del utöver vad som nämnts ovan. Upplysningsvis anser dock Datainspektionen att integritetsskyddet skulle kunna stärkas ytterligare av att CSN för socialnämnderna beskrev de tekniska funktioner som behövs för att nämnderna ska uppfylla kraven på tekniska begränsningar.

Loggar och loggkontroller
Enligt 9 § studiestödsdatalagen måste CSN se till att elektronisk tillgång till personuppgifter dokumenteras. Myndigheten ska också systematiskt och återkommande kontrollera om någon obehörig åtkomst till uppgifterna har förekommit. Det finns möjlighet för regeringen eller den myndighet som regeringen bestämmer att meddela ytterligare föreskrifter om dokumentation och kontroll, men några sådana föreskrifter har inte meddelats.

Paragrafens rubrik talar om intern elektroniskt tillgång till personuppgifter, men av förarbetena till lagen framgår att dokumentationen även ska avse tillgång via direktåtkomst.

> ”Dokumentationen ska avse alla former av elektronisk tillgång som har förekommit, oavsett om det är personer som arbetar i CSN:s studiestödsverksamhet som internt har berett sig tillgång till uppgifterna eller om en utomstående har gjort det genom t.ex. direktåtkomst. CSN ska systematiskt och återkommande kontrollera om någon obehörig åtkomst till uppgifter har förekommit. Det är således inte tillräckligt att CSN endast kontrollerar loggarna när myndigheten av någon orsak har anledning att misstänka att obehörig åtkomst har förekommit.” (Se prop. 2008/09:96 s 84.)

CSN loggar vilken socialnämnd som har ställt en viss fråga och när, och inhämtar en försäkran från socialnämnderna innan de bereds direktåtkomst till uppgifter. Försäkran lyder:

> ”Socialnämnden försäkrar att behandlingshistorik förs som visar vilken anställd hos socialnämnden som har berett sig tillgång till personuppgifter som behandlas i CSN:s studiestödsverksamhet.”

Frågan är om CSN:s skyldighet att dokumentera och kontrollera tillgång till uppgifterna kan anses uppfylld genom att de loggar aktiviteten från varje socialnämnd och förlitar sig på att socialnämnderna för behandlingshistorik över sina anställdas åtkomst till uppgifterna i enlighet med den inhämtade försäkran från socialnämnderna.

I den ovan nämnda propositionen om utökat elektroniskt informationsutbyte gjordes inga särskilda överväganden om krav på åtkomstkontroll. I resonemangen kring kraven på hur utlämnande myndighet ska försäkra sig om att handläggare hos socialnämnderna endast kan ta del av uppgifter om personer i aktuella ärenden, framgår däremot att det inte är rimligt att uppställa krav på att de myndigheter som föreslås få rätt att medge socialnämnderna direktåtkomst själva ska vidta kontroller av landets alla socialnämnder och att någon skyldighet att genomföra några faktiska kontroller inte heller avses med förslaget (prop. 2007/08:160 s. 150).

CSN har en skyldighet att logga och åtkomstkontrollera vilka utomstående som berett sig tillgång till uppgifterna. Det är viktigt att myndigheten har kontroll över vilka uppgifter som lämnats ut och till vilken socialnämnd samt att logguppgifterna är så detaljerade att det är möjligt att bedöma huruvida det skulle kunna vara fråga om obehörig åtkomst. Därför står det klart att CSN är skyldig att logga vilken socialnämnd som har ställt en viss fråga och när, samt att utföra loggkontroller. CSN bör dock som utlämnande myndighet i många fall ha svårt att bedöma huruvida en enskild socialnämndhandläggares åtkomst till vissa uppgifter varit obehörig eller inte. En sådan bedömning förutsätter kännedom om handläggarens arbetsuppgifter etc. och bör därför endast kunna göras av den aktuella socialnämnden.

Datainspektionen bedömer därför att CSN – genom att systematiskt och återkommande kontrollera socialnämndernas åtkomst och genom inhämtandet av en försäkran om att socialnämnderna utför motsvarande kontroll av sina anställdas åtkomst till personuppgifter hos CSN – kan anses uppfylla sin skyldighet enligt 9 § studiestödsdatalagen och kraven på lämpliga säkerhetsåtgärder enligt 31 § personuppgiftslagen. Datainspektionen anser att integritetsskyddet skulle stärkas ytterligare om CSN kompletterade den inhämtade försäkran så att det framgår att socialnämnderna inte bara ska föra en behandlingshistorik, utan också att de är skyldiga att utföra verkningsfulla åtkomst-

kontroller av handläggarnas åtkomst till personuppgifter i CSN:s studiestödsverksamhet.

Datainspektionen kan konstatera att CSN loggar vilken socialnämnd som haft åtkomst till vilka personuppgifter och när, och förutsätter att CSN också utför systematiska och återkommande loggkontroller av socialnämndernas åtkomst till personuppgifter på socialnämndnivå, dvs. inte på handläggarnivå.

Kommunikationssäkerhet
I enlighet med 2 § studiestödsdatalagen och 31 § personuppgiftslagen är CSN, i egenskap av personuppgiftsansvarig för uppgifterna i sin verksamhet, skyldig att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder 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.

Under inspektionen har framkommit att CSN säkerställt att uppgifterna lämnas ut till identifierade socialnämnder och att uppgifterna skyddas vid överföringen. Datainspektionen har därför inget att anmärka mot vad som framkommit avseende kommunikationssäkerheten.

Typer av uppgifter
Av 10 § studiestödsdatalagen (2009:287) framgår att direktåtkomst och annat elektroniskt utlämnande utan den registrerades samtycke av personuppgifter som behandlas i CSN:s studiestödsverksamhet, är tillåtet bara i den utsträckning som anges i lag eller förordning och under förutsättning att utlämnandet är förenligt med lagens bestämmelser om ändamål, begränsningar i rätten att behandla personuppgifter, samtycke och sökbegrepp.

Av 13 § studiestödsdataförordningen (2009:321) första stycket framgår att socialnämnd får ha direktåtkomst till personuppgifter som behandlas i CSN:s studiestödsverksamhet i den utsträckning som anges i 2 § förordningen (2008:975) om uppgiftsskyldighet i vissa fall enligt socialtjänstlagen (2001:453).

Socialnämnden kan få uppgifter om studiemedel, studiehjälp och hemutrustningslån. CSN har till Datainspektionen gett in handlingar som beskriver vilka uppgifter som socialnämnder kan se vid direktåtkomst. Enligt dessa handlingar får socialnämnderna se namn, personnummer och uppgifter som bland

annat rör stödform, ärendets status, sökta tider och ansökans omfattning, beviljade tider och belopp, utbetalningsdatum och relaterade ärenden.

Datainspektionen bedömer att de uppgifter som socialnämnderna kan se överensstämmer med de uppgifter som socialnämnderna har rätt att ta del av enligt 2 § förordningen (2008:975) om uppgiftsskyldighet i vissa fall enligt socialtjänstlagen (2001:453).

Åtkomst till uppgifter till vilka den elektroniska tillgången har begränsats
Av 14 § studiestödsdataförordningen framgår att direktåtkomst inte får avse personuppgifter till vilka den direkta elektroniska tillgången har begränsats enligt 7 §. Av 7 § studiestödsdataförordningen framgår att direkt elektronisk tillgång till personuppgifter i ett ärende om studiestöd, som inte behövs för återbetalning eller återkrav av studiestöd, ska begränsas senast tre år efter utgången av det kalenderår då studiestöd senast beviljades i ärendet eller ansökan om studiestöd avslogs. Det framgår vidare att bara ett begränsat antal personer som arbetar i myndighens studiestödsverksamhet får ha sådan tillgång till personuppgifterna i ärendet. Behövs personuppgifterna för ett nytt ärende om studiestöd, får begränsningen upphävas.

CSN har uppgivit att det ännu inte finns någon teknisk begränsning för åtkomst till vissa äldre uppgifter i enlighet med 7 och 14 §§ studiestödsdataförordningen. Detta ska dock vara åtgärdat i maj 2011 då den interna elektroniska tillgången till dessa uppgifter ska ha begränsats.

Datainspektionen kan konstatera att CSN ännu inte har de tekniska förutsättningarna på plats som behövs för att uppfylla kraven i 7 och 14 §§ studiestödsdataförordningen. CSN har dock uppgivit att detta ska vara åtgärdat i maj 2011 då den interna elektroniska tillgången till dessa uppgifter ska ha begränsats. Datainspektionen förutsätter att CSN genomför de planerade åtgärderna enligt ovan och har i övrigt inget att invända.

Skyddade personuppgifter
Datainspektionen har i tidigare tillsynsbeslut uttalat att för att obehöriga inte ska komma åt skyddade personuppgifter är det bland annat viktigt att det vid myndigheter finns sekretessmarkeringar som syns tydligt vid sökningar i register, att all personal som hanterar personuppgifter ges grundlig information om skyddade personuppgifter och sekretessfrågor, att kretsen av personer som har tillgång till skyddade personuppgifter begränsas så mycket som möjligt, att skyddade personuppgifter inte sprids till områden där sekretess för uppgifterna inte föreligger och att myndigheten regelbundet följer upp att regler och rutiner kring skyddade personuppgifter efterlevs och respekteras.

I ärendet har det framkommit att när en socialnämndshandläggare ställer en fråga om någon som har skyddade personuppgifter visas de efterfrågade uppgifterna och samtidigt anges det att personen har skyddade personuppgifter.

Datainspektionen har inget att invända mot utlämnandet av skyddade personuppgifter under förutsättning att CSN försäkrat sig om att socialnämnderna endast kan söka efter personer i aktuella ärenden.

Information till registrerade
När personuppgifter behandlas har den personuppgiftsansvarige enligt 23-25 §§ personuppgiftslagen en omfattande skyldighet att självmant informera de registrerade om den behandling av personuppgifter som utförs, bland annat om mottagarna av uppgifterna.

Datainspektionen kan konstatera att den information som CSN lämnar i ansökningshandlingarna inte innehåller information om att uppgifter kan komma att lämnas ut till socialnämnder. Datainspektionen utgår ifrån att CSN uppdaterar informationen.

Ärendet avslutas.

Hur man överklagar
Om ni vill överklaga beslutet skall 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 generaldirektören Göran Gräslund i närvaro av chefsjuristen Hans-Olof Lindblom, teamledaren Britt-Marie Wester, IT-säkerhetsspecialisten Magnus Bergström samt juristerna Maria Bergdahl och Lena Carlsson, föredragande

Göran Gräslund

Lena Carlsson

Kopia till:
Försäkringskassan, chefsjuristen Eva Nordqvist, Klara Västra kyrkogata 11, 103 51 Stockholm

Socialnämnden i Botkyrka Kommun, Kerstin Wexell, 147 785 Tumba