Datainspektionen

Beslut
2011-04-01

Diarienr
1523-2010

Försäkringskassan
Klara Västra kyrkogata 11

103 51 Stockholm

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

Datainspektionens beslut

Försäkringskassan föreläggs att upphöra med att ge socialnämnderna åtkomst till uppgifter ur socialförsäkringsdatabasen via LEFI Online till dess att Försäkringskassan försäkrat sig om att handläggare hos socialnämnderna bara kan ta del av uppgifter om personer som är aktuella i ärenden hos nämnden.

Datainspektionen förutsätter att Försäkringskassan inte endast loggar vilken socialnämnd som haft åtkomst till vilka uppgifter och när, utan också att Försäkringskassan utför systematiska och återkommande loggkontroller av socialnämndernas åtkomst till personuppgifter på socialnämndnivå.

Ärendet avslutas.

Bakgrund

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

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

Redogörelse för tillsynsärendet
Datainspektionen har den 21 oktober 2010 genomfört en inspektion hos Försäkringskassan. Inspektionen är ett led i Datainspektionens projekt rörande informationsutbyte mellan myndigheter. Försäkringskassan har inte lämnat några synpunkter på inspektionsprotokollet, men har inkommit med svar på kompletterande frågor.

Skäl för beslutet

Lagstiftning
De registerförfattningar som Försäkringskassan vid inspektionstillfället har haft att följa är lagen (2003:763) om behandling av personuppgifter inom socialförsäkringens administration och förordningen (2003:766) om behandling av personuppgifter inom socialförsäkringens administration. Den 1 januari 2011 ersattes lagen av en reglering i 114 kap. socialförsäkringsbalken (2010:110). Detta innebar dock inga materiella förändringar. Personuppgiftslagen gäller om inte annat följer av registerförfattningarna.

Allmänt om informationsutbytet
LEFI Online är en automatiserad onlinetjänst som bland annat ger socialnämnder direktåtkomst till viss information som behövs i handläggning av ärenden hos nämnden. LEFI Online har två olika gränssnitt – system till systemgränssnittet och webbgränssnittet.

Kravet på försäkran från Socialnämnderna
Enligt bestämmelsen som sedan den 1 januari 2011 finns i 114 kap. 22 § socialförsäkringsbalken får en socialnämnd ha direktåtkomst först sedan Försäkringskassan har försäkrat sig om att handläggare hos socialnämnden bara *kan* ta del av uppgifter om personer som är aktuella i ärenden hos nämnden.

Vid inspektionen har framkommit att det inte finns några tekniska begränsningar i LEFI Online (varken i system till systemgränssnittet eller i webbgränssnittet) som begränsar sökbarheten till uppgifter om personer som är aktuella i ärenden hos en mottagande socialnämnd. Försäkringskassan har heller inte inhämtat någon försäkran från socialnämnderna.

Försäkringskassan har i ett yttrande till Datainspektionen gjort gällande att någon försäkran i enlighet med 114 kap. 22 § socialförsäkringsbalken inte är nödvändig därför att informationslämnande inte är att betrakta som direktåtkomst. Argumenten är att nämnderna endast kan ställa förbestämda frågor på ett förbestämt urval uppgifter utan någon möjlighet att på egen hand söka uppgifter i socialförsäkringsdatabasen. Innan svaret lämnas ut kontrolleras att information i svaret inte avviker från det som är tillåtet att utlämna enligt

gällande regelverk. Lösningen är tekniskt sett en asynkron lösning så fort frågan mottagits av Försäkringskassan och hanteras därmed inte internt som en online fråga. Frågeställaren saknar i detta skede möjlighet att påverka frågan och hur den hanteras. Tekniskt sett befinner sig frågeställaren i ett uppkopplat väntläge under den tid som Försäkringskassan behandlar frågan. För det fall att LEFI Online anses medge direktåtkomst har Försäkringskassan ansett att kravet på försäkran är uppfyllt genom den dokumentation som Försäkringskassan inhämtar från kommunerna vid anslutning. Dokumentationen innehåller uppgift om vilken chef inom kommunen som ansvarar för att fatta beslut om tilldelning av behörigheter samt de enskilda behörighetsbesluten.

Det finns inte någon legaldefinition av begreppet direktåtkomst och det har framförts att den tekniska utvecklingen har lett till att skillnaderna mellan direktåtkomst och annat uppgiftslämnande på automatisk väg blivit så små att det kan vara svårt att dra en gräns mellan direktåtkomst och andra former för utlämnande (prop. 2007/08:160 s. 58). Datainspektionen kan konstatera att Försäkringskassan även under bestämmelsens tillkomst ifrågasatte om ett förfarande som innehåller tekniska begräsningar och där frågorna och svaren är fördefinierade och begränsade till sin omfattning bör falla in under begreppet direktåtkomst. Regeringen bemötte vad Försäkringskassan framförde och fann att det saknades anledning att göra den bedömningen att regleringen innebär ett förfarande som inte är att betrakta som direktåtkomst (prop. 2007/08:160 s. 150).

Från integritetsskyddssynpunkt är det inte tillfredställande att handläggare hos socialnämnderna, genom LEFI Online på det sätt som sker, inte endast ges tillgång till uppgifter om personer som är aktuella i ett ärende utan även till uppgifter som rör befolkningen i övrigt. Datainspektionen kan också konstatera att lagstiftaren tydligt uttalat att kravet på utlämnande myndighet, att försäkra sig om begränsningar i åtkomsten hos socialnämnderna, ska gälla för den typ av utlämnande som det här är fråga om. Datainspektionen bedömer därför att Försäkringskassan har en skyldighet enligt 114 kap. 22 § socialförsäkringsbalken att inhämta en försäkran från socialnämnderna.

Av författningskommentaren till den aktuella bestämmelsen framgår att Försäkringskassan 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 (prop. 2007/08:160 s. 170). Datainspektionen anser därför att den dokumentation som Försäkringskassan inhämtar från socialnämnderna, rörande beslutsfattande chef och enskilda behörighetsbeslut, inte uppfyller kraven på försäkran om *teknisk begränsning* till åtkomst till uppgifter i aktuella ärenden.

Försäkringskassan föreläggs därför att upphöra med att ge socialnämnderna åtkomst till uppgifter ur socialförsäkringsdatabasen genom LEFI Online till dess att Försäkringskassan försäkrat sig om att handläggare hos socialnämnderna bara kan ta del av uppgifter om personer som är aktuella i ärenden nos nämnden.

Av förarbetena framgår att det är tillfyllest att Försäkringskassan från den mottagande socialnämnden *inhämtar en försäkran* om att kraven på tekniska begränsningar är uppfyllda (prop. 2007/08:160 s. 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).

Upplysningsvis har Datainspektionen i ett tillsynsbeslut mot Centrala studiestödsnämnden (CSN, dnr 1735-2010) ansett att det i princip är tillräckligt att inhämta en skriftlig försäkran från socialnämnderna. Däremot anser Datainspektionen att det kan finnas tillfällen då endast förekomsten av en underskriven försäkran från socialnämnden inte är tillräcklig. Utlämnande myndighet måste normalt kunna utgå ifrån att den socialnämnd, som skriver under en försäkran, faktiskt lever upp till de krav som ställs i försäkran. Men om det skulle framkomma omständigheter som ger utlämnande myndighet skälig anledning att misstänka att så inte är fallet anser Datainspektionen att myndigheten, 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 den utlämnande myndigheten, även på annat sätt, kunnat försäkra sig om att den mottagande socialnämnden har tillfredställande tekniska begränsningar. Anledningen till Datainspektionens ställningstagande är omständigheter som framkommit under en inspektion av Socialnämnden i Botkyrkas användning av Sambruks lösning, Multifråga (dnr 1579-2010). Både CSN och Socialnämnden i Botkyrka har förelagts att vidta åtgärder. Försäkringskassan bör i sitt kommande arbete beakta vad Datainspektionen anfört även i ovan nämnda ärenden.

Loggar och loggkontroller

I enlighet med 114 kap. 6 § socialförsäkringsbalken och 31 § personuppgiftslagen är Försäkringskassan, i egenskap av personuppgiftsansvarig för uppgifterna i socialförsäkringsdatabasen, skyldig att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas. I enlighet med Datainspektionens tidigare beslut mot Försäkringskassan är Försäkringskassan skyldig att utföra systematiska och återkommande åtkomstkontroller i syfte att upptäcka och beivra obehörig åtkomst av personuppgifter i myndighetens IT-system (se beslut 2009-06-23, dnr 1764-2008, som ska följas upp under 2011).

Vid inspektionen framkom att Försäkringskassan i sina loggar för system till systemgränssnittet kan se vid vilken tidpunkt en viss socialnämnd ställde en viss fråga och vilket svar som socialnämnden fick. I webbgränssnittet kan Försäkringskassan se samma information avseende den person som ställt frågan.

I propositionen om utökat elektroniskt informationsutbyte gjordes inga särskilda överväganden avseende 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).

Som ovan nämnts har Datainspektionens i tidigare beslut, avseende intern åtkomst hos Försäkringskassan, ansett att Försäkringskassan är skyldig att utföra systematiska och återkommande åtkomstkontroller i syfte att upptäcka och beivra obehörig åtkomst av personuppgifter. Datainspektionen anser att Försäkringskassan, mot bakgrund av säkerhetsbestämmelserna i 31 § personuppgiftslagen, måste ha kontroll över vilka uppgifter som lämnas ut och till vilken socialnämnd samt se till att logguppgifterna är så detaljerade att det är möjligt att bedöma huruvida det skulle kunna vara fråga om obehörig åtkomst. Försäkringskassan är därför skyldig att logga vilken socialnämnd som har ställt en viss fråga och när samt att utföra systematiska och återkommande loggkontroller. Datainspektionen anser att Försäkringskassan har en skyldighet att utföra loggkontroller av utlämnanden på socialnämndsnivå, men inte på handläggarnivå. Försäkringskassan bör nämligen 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 – som också har en skyldighet att utföra åtkomstkontroller.

Mot bakgrund av det anförda förutsätter Datainspektionen att Försäkringskassan inte endast loggar vilken socialnämnd som haft åtkomst till vilka uppgifter och när, utan också att Försäkringskassan utför systematiska och återkommande loggkontroller av socialnämndernas åtkomst till personuppgifter på socialnämndnivå, dvs. inte på handläggarnivå.

Kommunikationssäkerhet
Försäkringskassan har säkerställt att uppgifterna lämnas ut till identifierade socialnämnder och att uppgifterna skyddas vid överföringen. Datainspektio-

nen har därför inget att anmärka mot vad som framkommit avseende kommunikationssäkerheten.

Skärskilt om 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 en socialnämndshandläggare måste använda sig av personnummer när uppgifter söks i socialförsäkringsdatabasen. I svaret som handläggaren får står det angivet att personen har skyddad identitet. Det framgår i vilken kommun personen bor och personnummer på personens barn kan finnas med. Några namn eller adressuppgifter överförs aldrig.

Datainspektionen bedömer att utlämnandet av information om personer med skyddade personuppgifter är acceptabel under förutsättning att Försäkringskassan 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.

I tillsynsärendet har det framkommit att Försäkringskassan på sina blanketter anger att uppgifterna hanteras i Försäkringskassans datasystem och att mer information finns att läsa i broschyren ”Försäkringskassans personregister”.

Datainspektionen har i ett tidigare tillsynsärende mot Försäkringskassan (beslut 2007-03-07, dnr 1857-2005) framfört att uppdelning av informationen som Försäkringskassan valt inte torde strida mot personuppgiftslagen, så länge det sammantagna innehållet i informationen som ges, både på blanketten och i broschyren, uppfyller personuppgiftslagens krav. Ställningstagandet förutsätter att de registrerade alltid på ett enkelt sätt har tillgång till informationen i broschyren i samband med att personuppgifter lämnas.

Datainspektionen har inget att invända mot vad som vid denna inspektion framkommit avseende informationen som lämnas i blanketterna och broschyren. Datainspektionen utgår ifrån att Försäkringskassan även lämnar motsvarande information till den som använder Mina Sidor.

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:
Socialnämnden i Botkyrka Kommun, Kerstin Wexell, 147 785 Tumba