Södermalms stadsdelsnämnd
Box 4270
102 66 Stockholm

Tillsyn enligt personuppgiftslagen (1998:204) - avseende behörighetsstyrning i ParaGå

Datainspektionens beslut

Datainspektionen konstaterar att Södermalms stadsdelsnämnd behandlar personuppgifter i strid med 6 § lagen (2001:454) om behandling av personuppgifter inom socialtjänsten genom att i systemet ParaGå ge anhörigvårdare behörighet till fler personuppgifter än vad som är nödvändigt för att de ska kunna utföra sina arbetsuppgifter inom socialtjänsten.

Datainspektionen förelägger därför Södermalms stadsdelsnämnd att tillse att anhörigvårdare inte kan ta del av fler uppgifter än de behöver för att ge vård och omsorg till sina respektive anhöriga.

Datainspektionen konstaterar att Södermalms stadsdelsnämnd inte vidtar nödvändiga säkerhetsåtgärder enligt 31 § personuppgiftslagen (1998:204) för att skydda de personuppgifter som behandlas i ParaGå genom att inte ha loggar över vilka åtgärder som vidtas i systemet och därmed inte heller logguppföljning för att kontrollera om någon obehörig behandlar personuppgifter i ParaGå.

Datainspektionen förelägger därför nämnden att införa loggar över vilka åtgärder som vidtagits i systemet. Nämnden föreläggs även skapa en rutin för regelbunden logguppföljning.

Datainspektionen konstaterar att åtkomst till uppgifter som registrerats i ParaGå är åtkomliga över öppet nät efter autentisering med användarnamn och lösenord. Det uppfyller inte kraven på stark autentisering.

Datainspektionen förelägger Södermalms stadsdelsnämnd att vid åtkomst över öppet nät säkerställa att den autentiseringsmetod som används uppfyller kraven på stark autentisering.

Ärendet avslutas.

Redogörelse för tillsynsärendet

Datainspektionen har mottagit klagomål som gör gällande att it-systemet ParaGå saknar tekniska spärrar för att anpassa behörigheten samt att anhörigvårdare har tillgång till fler uppgifter än uppgifter om den anhörige. Datainspektionen har med anledning av klagomålet inlett tillsyn mot Södermalms stadsdelsnämnd som använder ParaGå inom hemtjänstverksamheten.

Datainspektionen har genomfört en inspektion i syfte att granska nämndens behandling av personuppgifter i ParaGå. Syftet med inspektionens var närmare bestämt att kontrollera åtkomstmöjligheterna till personuppgifter i ParaGå samt tekniska och organisatoriska åtgärder för behörighetsstyrning. Nämnden bedriver hemtjänstverksamhet under namnet Södertjänst. Datainspektionen har under inspektionen intervjuat representanter från Södertjänst och nämndens personuppgiftsombud. Datainspektionen tog på plats del av personuppgiftsbehandling i ParaGå. Datainspektionen har fört protokoll under inspektionen och gett nämnden tillfälle att yttra sig över protokollet och svara på ett antal kompletterande frågor.

ParaGå är en it-plattform inom vård och omsorg och hemtjänstpersonalen har endast tillgång till ParaGå genom tjänstemobilen som inte får användas privat. Tjänstetelefonen är inte personligt knuten till en anställd på så sätt att det endast är den som har fått telefonen tilldelad till sig som kan logga in och ta del av uppgifter i ParaGå. Timvikarier får använda sig av lånetelefoner . ParaGå är kopplat till ett system som heter ParaSol. Uppgifter som förs in i ParaGå överförs även till ParaSol. Uppgifter som personal kommer åt via ParaGå är uppgifter som är registrerade i ParaSol. ParaGå används för att säkerställa att hemtjänstpersonal är hos kunden och utför de insatser som kunden är berättigad till. I ParaGå dokumenteras vidtagna åtgärder och avvikelser (så kallade journalanteckningar). Uppgifter om ca 700-800 kunder är nåbara via ParaGå inom Södertjänst.

Skäl för beslutet

Tillämpliga bestämmelser

I socialtjänstlagen (2001:453) regleras enskildas rätt att få den hjälp och stöd som de behöver. Bestämmelser om behandling av personuppgifter finns i lagen (2001:454) och förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten och i personuppgiftslagen (1998:204), PuL.

Det är vårdbiträden och undersköterskor som anställs inom hemtjänsten i Södermalm. Även de som vårdar anhöriga i hemmet, anhörigvårdare, är anställda av stadsdelsförvaltningen. Under inspektionen uppgav nämnden att hälso- och sjukvårdslagen inte är tillämplig på den verksamhet som nämnden bedriver, utan dokumentation i ParaGå sker i enlighet med socialtjänstlagen. Mot bakgrund av de uppgifter som framkommit i ärendet delar Datainspektionen denna bedömning.

Personuppgiftsansvarig

Enligt 11 § förordning om behandling av personuppgifter inom socialtjänsten är en kommunal myndighet personuppgiftsansvarig för den behandling av personuppgifter inom socialtjänsten som myndigheten utför. Nämnden är således personuppgiftsansvarig för behandlingen av personuppgifter i ParaGå.

Vilka typer av uppgifter behandlas i ParaGå

Datainspektionen konstaterar att de personuppgifter som registreras i ParaGå kan vara känsliga enligt 13 § PuL eller annars integritetskänsliga enligt 31 § PuL.

Känsliga personuppgifter definieras som uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i förening samt personuppgifter som rör hälsa eller sexualliv (13 § PuL). Även andra uppgifter kan anses så integritetskänsliga att de kräver höjd säkerhet. I Datainspektionens Allmänna råd ”Säkerhet för personuppgifter” anges exempelvis att uppgifter angående ekonomisk hjälp eller vård inom socialtjänsten är exempel på personuppgifter som normalt är att anse som känsliga så att säkerheten behöver skärpas (s. 18).

De personuppgifter om kunder som registreras i ParaGå är personnummer, namn, adress, åtgärdsplan och vidtagna åtgärder. Av åtgärdsplanen framgår vilka åtgärder som ska vidtas hos kunden. Åtgärdsplanen är upprättad tillsammans med kunden. I ParaGå finns även fritextfält för journalanteckningar och arbetsanteckningar. De exempel på journalanteckningar som Datainspektionen har tagit del av vid inspektionen talar för att de uppgifter som registreras är känsliga personuppgifter t.ex. uppgift om att en kund har fått viss medicin eller inkontinensskydd. Datainspektionen konstaterar mot bakgrund av detta att det i ParaGå registreras uppgifter som rör hälsa vilket således är registrering av känsliga personuppgifter.

I ParaGå registreras även uppgifter om anställda exempelvis framgår det vilken anställd som skrivit/rapporterat uppgifter om en kund i systemet. Även GPS-uppgifter sparas i ParaGå. De anställda får information om hur ParaGå fungerar i samband med anställningen. Det finns en skriftlig användarmanual för ParaGå tillgänglig för personalen.

IT-säkerhet

Av 31 § PuL framgår att den personuppgiftsansvarige ska 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, kostnaden för åtgärderna, särskilda risker med behandlingen och hur pass känsliga uppgifterna är.

Vid bedömning av hur pass känsliga uppgifterna hos socialtjänsten är ska särskilt beaktas om personuppgifterna definieras som känsliga i personuppgiftslagen, om de omfattas av tystnadsplikt eller sekretess enligt offentlighets- och sekretesslagen (2009:400) eller annan lagstiftning samt om de är att anse som ömtåliga enligt lagen om behandling av personuppgifter inom socialtjänsten.

Kraven på lämpliga tekniska och organisatoriska åtgärder ligger till grund för de följande underrubrikerna behörighetsstyrning, behandlingshistorik och logguppföljning samt autentiseringen.

Behörighetsstyrning

Datainspektionen konstaterar att nämnden behandlar personuppgifter i strid med 6 § lagen om behandling av personuppgifter inom socialtjänsten genom

att ge anhörigvårdare behörighet till fler personuppgifter än vad som är nödvändigt för att anhörigvårdare ska kunna utföra sina arbetsuppgifter inom socialtjänsten

Enligt personuppgiftslagen gäller att personuppgifter får samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål samt att uppgifterna senare inte får behandlas får något ändamål som är oförenligt med det för vilket uppgifterna har samlats in (9 §). Den personuppgiftsansvarige ska själv, redan när uppgifterna samlas in, ange särskilda ändamål för sin behandling av personuppgifterna. Dessa ändamål sätter sedan gränserna för hur uppgifterna får behandlas. Personuppgiftslagen innehåller en uppräkning av när behandlingen av personuppgifter är tillåten (10 §). Det är bl.a. tillåtet att behandla personuppgifter efter den registrerades samtycke. I vissa fall får personuppgifter hanteras utan samtycke. En förutsättning i samtliga fall är att behandlingen är nödvändig för ändamålet.

Personuppgiftslagen är subsidiär vilket innebär att om det i annan lag eller förordning finns bestämmelser som avviker från personuppgiftslagen ska de bestämmelserna gälla (2 §). Enligt lagen om behandling av personuppgifter inom socialtjänsten får personuppgifter bara behandlas om behandlingen är nödvändig för att arbetsuppgifter inom socialtjänsten ska kunna utföras (6 §). Av paragrafens *första stycke*, som ersätter 10 § PuL, följer att samtliga kategorier av personuppgifter i och för sig får behandlas. Bestämmelsen innebär emellertid att det läggs fast en yttersta ram när behandling av personuppgifter är tillåten. Personuppgifter får behandlas bara om behandlingen är nödvändig för att arbetsuppgifterna inom socialtjänsten ska kunna utföras. Endast sådan behandling kan anses berättigad. Detta framgår av rubriken till paragrafen. Regeringen eller den myndighet som regeringen bestämmer har därutöver rätt att meddela de föreskrifter om begränsningar som är nödvändiga i detta hänseende (jfr 12 § förordningen [2001:637] om behandling av personuppgifter inom socialtjänsten). Av 12 § förordning om behandling av personuppgifter inom socialtjänsten framgår att en kommunal myndighet får behandla personuppgifter för bland annat handläggning av ärenden om bistånd och annat stöd samt genomförande av beslut om bistånd, stödinsatser, vård och behandling samt annan social service som följer av bestämmelserna i socialtjänstlagen (p. 1).

Hemtjänsten inom nämnden är uppdelad i fyra administrativa delar – nord, syd, öst och väst. En kund tillhör en viss enhet beroende på var denne bor och

i ParaGå kan man tilldelas behörighet till respektive enhet. Under inspektionen framkom att behörighetsstyrningen utgår från hur Södertjänst valt att organisera sig. Hemtjänstpersonalen arbetar över enhetsgränserna och har därför tillgång till uppgifter om kunderna inom samtliga geografiska områden. Anhörigvårdare tilldelas behörighet till den geografiska enhet som dennes anhörige tillhör (nord/syd/öst/väst) och har därmed tillgång till uppgifter om samtliga kunder i den geografiska enheten. I systemet är det tekniskt möjligt att begränsa åtkomsten gruppvis men inte enbart till en kund.

Datainspektionen konstaterar att hemtjänstpersonalen ges en bred behörighet och att det i ParaGå finns känsliga personuppgifter men mot bakgrund av att hemtjänstpersonalen arbetar över enhetsgränserna konstaterar Datainspektionen att det är rimligt att personalen har teknisk tillgång till kunder inom samtliga geografiska områden. Däremot krävs det för att faktiskt få ta del av uppgifterna att det är nödvändig för att arbetsuppgifter inom hemtjänsten ska kunna utföras. För att minska risken för intrång i systemet måste nämnden således ge personalen anvisningar om hur ParaGå får användas så att både sekretess- och dataskyddsreglerna följs. Det kan vara lämpligt att dokumentera i en it-policy, vad som är tillåtet, vilka konsekvenserna blir om man bryter mot en regel och hur efterlevnaden av reglerna följs upp (se Datainspektionens Allmänna råd ”Säkerhet för personuppgifter” sid 13).

Vad gäller anhörigvårdare, som bara utför arbetsuppgifter hos sin anhörige, gör Datainspektionen en annan bedömning. Av de uppgifter som framkommit i ärendet behöver anhörigvårdare endast ha tillgång till uppgifter om sin anhörige. Det synes således inte finnas något behov för anhörigvårdare att ha behörighet till andra kunder för att genomföra de arbetsuppgifter som anhörigvårdaren ska utföra. Datainspektionen förelägger därför nämnden att tillse att anhörigvårdare inte kan ta del av fler uppgifter än de behöver för att ge vård och omsorg till sina respektive anhörige.

Behandlingshistorik och logguppföljning

Datainspektionen konstaterar att nämnden inte vidtar nödvändiga säkerhetsåtgärder enligt 31 § PuL för att skydda de personuppgifter som behandlas i ParaGå genom att inte ha loggar över vilka åtgärder som vidtagits i systemet och genom att inte genomföra logguppföljning för att kontrollera om någon obehörigen tar del av personuppgifter i ParaGå.

Krav på logguppföljning inom socialtjänsten följer av säkerhetskraven i 31 § PuL. Enligt den bestämmelsen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Av Datainspektionens Allmänna råd ”Säkerhet för personuppgifter” framgår att ett system för behörighetskontroll bör upprättas för att förhindra obehörig användning eller åtkomst. Ett sådant system bör omfatta möjligheter att identifiera användare och bekräfta användares identitet. Systemet bör kunna kontrollera användningen så att endast de som behöver uppgifter för sitt arbete får åtkomst till åtkomstskyddade personuppgifter. Det bör finnas rutiner för tilldelning och kontroll av behörigheter. För att åtkomsten ska kunna kontrolleras bör det, beroende på känsligheten hos personuppgifterna finnas en behandlingshistorik (loggar) som sparas en viss tid. En behandlingshistorik bör följas upp och skyddas mot otillåtna förändringar. En behandlingshistorik bör normalt vara så detaljerad att den kan användas för att utreda felaktig eller obehörig användning av personuppgifter. Behandlingshistoriken bör, beroende på känsligheten hos personuppgifterna, ange till exempel läsning, ändring, utplåning eller kopiering av personuppgifter (sid 21-22).

Som tidigare nämnts registreras både känsliga och integritetskänsliga personuppgifter i ParaGå. Utgångspunkten för säkerhetsarbetet är att ju känsligare personuppgifter som behandlas desto högre krav på säkerhet. Mot bakgrund av att hemtjänstpersonalen ges en relativt bred behörighet till de personuppgifter som finns i ParaGå är det viktigt att det finns en behandlingshistorik för att kunna kontrollera att personuppgifter behandlas i enlighet med gällande bestämmelser och den aktuella it-policyn. Det är också viktigt att genomföra loggуppföljning, för att på förekommen anledning eller genom stickprover kontrollera om det sker obehöriga slagningar. För att obehörig åtkomst ska upptäckas och för att loggуppföljningar ska få en preventiv effekt behövs rutiner för loggуppföljningar och tydlig information bör ges till personalen.

Nämnden har uppgett att det inte finns några loggar över vilka åtgärder som vidtas i ParaGå. Det sker inga loggkontroller i systemet för att kontrollera om någon obehörig tar del av personuppgifter i ParaGå.

Datainspektionen förelägger därför nämnden att införa behandlingshistorik över vilka åtgärder som vidtagits i systemet. Nämnden ska även skapa en rutin

för att följa upp behandlingshistoriken och föra regelbundna kontroller av loggarna för att att se till att det inte sker en obehörig behandling av personuppgifter. I syfte att förhindra otillåten spridning av eller otillåten tillgång till uppgifterna bör nämnden även på ett tydligt sätt informera personalen om vilken loggning och logguppföljning som kan förekomma.

Autentisering
Datainspektionen konstaterar att åtkomst till uppgifter som registrerats i ParaGå är åtkomliga över öppet nät efter autentisering med användarnamn och lösenord. Det uppfyller inte kraven på stark autentisering.

Om (integritets-) känsliga personuppgifter får lämnas ut över öppet nät, till exempel Internet, ska användarnas identitet säkerställas med en teknisk funktion som ger en stark autentisering (31 § PuL). Stark autentisering används som ett samlingsnamn för tekniska funktioner som säkerställer en användares identitet genom användarcertifikat, engångslösenord eller motsvarande, det vill säga en högre grad av verifiering av en uppgiven identitet än enbart användarnamn och lösenord. Om en autentiseringslösning innefattar fler än en faktor sägs vanligen att den kan uppnå en stark autentisering av användaren. Önskvärda egenskaper hos starka autentiseringslösningar innefattar att användaren ska kunna förlora kontrollen över en faktor utan att säkerheten för skyddsobjektet helt går förlorad samt att det ska gå att upptäcka och vidta åtgärder om det händer. Stark autentisering kan uppnås med hjälp av en mobil enhet om den mobila enheten i sig är en förutsättning för att användaren ska kunna bereda sig åtkomst till systemet med hjälp av sitt användarnamn och lösenord och det finns en koppling mellan användaren och enheten.

Inloggning i ParaGå sker via öppet nät med användarnamn och lösenord. Användarnamnet skapas av programmet vid registrering av användaren och ett tillfälligt lösenord skapas. Programmet kräver att lösenordet byts när man börjar använda ParaGå. Administrativ personal har åtkomst till en webbversion av ParaGå som är ett administrationsverktyg. ParaGå Web erbjuds även som en tjänst via internet.

Datainspektionen förelägger nämnden mot bakgrund av detta att säkerställa att den autentiseringsmetod som används uppfyller kraven på stark autentisering.

Övrigt

Under inspektionen framkom att det till systemet finns en applikation som kallas omsorgsdagboken som möjliggör att kunder och anhöriga till kunder får tillgång till journalanteckningar via nätet. Datainspektionen har inte i detta ärende inspekterat omsorgsdagboken, men förutsätter att nämnden utifrån den information som framkommit i detta ärende analyserar tillgång och säkerhet även för denna applikation.

Datainspektionens tillsyn och beslut utgår från bestämmelser om dataskydd dvs. regler kring personuppgiftsbehandling. Eftersom många uppgifter som behandlas inom hemtjänsten även omfattas av sekretess måste nämnden också analysera att samtlig hantering av uppgifter som kan omfattas av sekretess också följer gällande sekretessbestämmelser.

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 via e-post.