Datainspektionen

Beslut
2007-12-20

D n r
998-2007

Er beteckning
41791-2007

Försäkringskassan
103 51 Stockholm

Beslut efter tillsyn enligt personuppgiftsiagen (1998:204)

Datainspektionens beslut

1. Rutiner för information till de registrerade och rättelse

Datainspektionen vidtar i dagsläget inga åtgärder beträffande Försäkringskassans tillämpning av bestämmelserna i PuL om information till de registrerade och rättelse. Datainspektionen kommer att följa upp ärendet på denna punkt.

Datainspektionen utgår från att Försäkringskassan vid utarbetandet av sina rutiner beaktar Datainspektionens synpunkter nedan i skälen för detta beslut.

2. Rättelse i medicinska utredningar

Datainspektionen vidtar i dagsläget inga åtgärder beträffande Försäkringskassans hantering av begäran om rättelse i medicinska utredningar.

Datainspektionen utgår från att Försäkringskassan vid utarbetandet av sina rutiner beaktar Datainspektionens synpunkter nedan i skälen för detta beslut.

3. Sms-tjänsten för anmälan av tillfällig föräldrapenning

Försäkringskassan har personuppgiftsansvar för personuppgiftsbehandlingen i sms-tjänsten för anmälan av tillfällig föräldrapenning.

Datainspektionen förelägger Försäkringskassan att genomföra en risk- och sårbarhetsanalys av sin sms-tjänst för anmälan av tillfällig föräldrapenning, samt att underrätta Datainspektionen om resultatet av analysen och vilka slutsatser som Försäkringskassan drar av analysen.

4. **Arbetsgivares anmälan av sjukdomsfall över Infratjänsten**

Försäkringskassan har personuppgiftsansvar för personuppgiftsbehandlingen i Infratjänsten som används för anmälan av anställdas sjukdomsfall.

Datainspektionen förelägger Försäkringskassan att genomföra en risk- och sårbarhetsanalys av Infratjänsten som används vid arbetsgivares anmälan av anställdas sjukdomsfall, samt att underrätta Datainspektionen om resultatet av analysen och vilka slutsatser som Försäkringskassan drar av analysen.

Bakgrund

Datainspektionen har inspekterat tre av Försäkringskassans kontor: länskontoret i Västmanlands län, länskontoret i Stockholms län och Försäkringskassans huvudkontor.

Vid inspektionerna och i efterföljande kontakt med Försäkringskassans huvudkontor har i huvudsak följande framkommit.

1. Rutiner för information till de registrerade och rättelse

Det finns inom Försäkringskassan några dokument som beskriver när och hur handläggare ska beställa information till den registrerade (s.k. registerutdrag) ur Försäkringskassans system. Det finns dock inget dokument som behandlar gränsdragningen mellan partsinsyn, offentlighetsprincipen och registerutdrag. Det saknas helt och hållet dokument om Försäkringskassans rättelsemöjligheter.

Försäkringskassan har således ännu inte tagit fram den enhetliga rutin för rättelser som Försäkringskassan i samband med Datainspektionens tidigare inspektion i december år 2005 (dnr 1857-2005) planerade att genomföra.

Försäkringskassan ska emellertid under hösten 2007 ta fram styrdokument för när registerutdrag och rättelse ska göras.

Försäkringskassan känner inte till att det inom Försäkringskassan någonsin har meddelats ett formenligt beslut om registerutdrag eller rättelse.

Registerutdrag skickas både från centrala register och från lokala register. Ett dagboksblad (en innehållsförteckning) är den enda information som lokalt lämnas ut från Försäkringskassans ärendehanteringssystem, ÄHS. Önskar en registrerad mer information om en viss handling, kan han eller hon få det efter särskild framställan.

Försäkringskassan anser sig inte behöva lämna ut innehållet i de handlingar som finns i s.k. elektroniska aktregister. Detta med anledning av förarbetena till 27 § lagen (2003:763) om behandling av personuppgifter inom socialförsäkringens administration (SofdL), där följande sägs: "För sådana handlingar som avses i 11 § socialförsäkringsregisterlagen – dvs. handlingar i

elektroniska akter m.m. – gäller dock i dag den begränsningen att uppgifter i sådana handlingar inte behöver tas med i information enligt 26 § personuppgiftslagen. Däremot skall av informationen framgå vilka handlingar avseende den registrerade som finns i registret." (Prop. 2002/03:135 sid. 116f) Försäkringskassan anser att det av specialmotiveringen (a a sid. 135) framgår att den i propositionen föreslagna regleringen motsvarar vad som då gällde enligt 20 § socialförsäkringsregisterlagen. Enligt Försäkringskassan innebär detta att någon förändring inte varit avsedd.

Försäkringskassan skiljer mellan en situation då en person begär partsinsyn enligt förvaltningslagen och far betala för kopiorna enligt avgiftsförordningen, samt en situation då en person begär att få ett gratis registerutdrag. Partsinsynen ger tillgång till allt som finns i akten, medan det centrala registerutdraget ger tillgång till det som finns i de centrala databaserna.

2. Rättelse i medicinska utredningar

När den försäkrade påpekar sakfel i en försäkringsmedicinsk utredning som på uppdrag av Försäkringskassan utförts av ett utomstående företag, behandlas detta påpekande förmodligen på olika sätt, beroende på vad det rör sig om för felaktighet. Försäkringskassan kan vända sig till det företag som utfört utredningen, eller hänvisa den försäkrade till företaget för att fa till stånd en rättelse. Det företag som utfört utredningen har ett eget personuppgiftsansvar för de personuppgifter som företaget behandlar. Försäkringskassan gör inga rättelser i dessa utredningar, men beroende på omständigheterna och vad saken gäller kan en uppgift justeras eller kommenteras i ärendets journal.

3. Sms-tjänsten för anmälan av tillfällig föräldrapenning

Det är möjligt att via sms till Försäkringskassan anmäla tillfällig föräldrapenning (vård av sjukt barn). Vårdnadshavaren sms:ar bokstäverna TFP och sitt personnummer följt av barnets personnummer till telefonnummer 71020.

Denna möjlighet beskrivs på en förteckning på Försäkringskassans webbplats över Försäkringskassans självbetjäningstjänster för anmälan och begäran av tillfällig föräldrapenning. De andra självbetjäningstjänsterna för anmälan och begäran av tillfällig föräldrapenning är:
- Anmälan och begäran på nätet med e-legitimation,
- Anmälan på nätet utan e-legitimation,
- Anmälan per automatisk telefonsvarare.

När Försäkringskassan har fått in en sms-anmälan om tillfällig föräldrapenning, skickas ett maskinellt genererat svarsmeddelande till det mobiltelefonnummer från vilket anmälan gjordes. Det finns 14 olika svarsmeddelanden som Försäkringskassan kan skicka i samband med anmälan av tillfällig föräldrapenning via sms. Ett svarsmeddelande kan exempelvis upplysa om att anmälan har registrerats, att barnets eller vårdnadshavarens personnummer är felaktigt, att "sms-tjänsten har stängt" och anmälan måste göras på annat sätt, och liknande.

Försäkringskassan behandlar i mottagande system uppgift om källa (sms plus uppringande telefonnummer), datum, tid, servicekod (vad som beställts), personnummer, aktuellt försäkringskassekontor, och status (OK eller inte). Uppgifterna sparas i två månader för felsökning.

När Försäkringskassan fått in en sms-anmälan om tillfällig föräldrapenning som godkänns av systemet, skickas det automatiskt ut en blankett per post till vårdnadshavaren för begäran om tillfällig föräldrapenning. Denna begäran förväntas vårdnadshavaren skicka tillbaka till Försäkringskassan. Om begäran inte inkommer, avslutas försäkringsärendet efter 180 dagar. Avslutningsanledningen blir "ej avhörd".

Sms:et har rättsverkan i ärenden om tillfällig föräldrapenning, på samma sätt som en anmälan per telefon har det.

För barn över 12 år kan sms-tjänsten inte användas. Det finns ingen autentiseringskontroll, dvs. det går att sms:a in en helt främmande persons personnummer. Försäkringskassan är medveten om att ett sms för anmälan av tillfällig föräldrapenning kan utgöra en känslig personuppgift.

Det är även möjligt att via sms anmäla ersättning för ledighet i samband med barns födelse (så kallade pappadagar) och beställa ett europeiskt sjukförsäkringskort.

4. Arbetsgivares anmälan av sjukdomsfall över Infratjänsten

En arbetsgivare kan, förutom per telefon eller vanligt brev, fullgöra sin anmälningsskyldighet av anställdas sjukdomsfall elektroniskt genom e-post samt genom manuell eller automatisk filöverföring.

Försäkringskassan uppmanar inte arbetsgivare att göra anmälan genom e-post och har tagit bort informationen om denna möjlighet från sin webbplats.

Arbetsgivarnas möjlighet att fullgöra anmälningsskyldigheten genom manuell eller automatisk filöverföring beskrivs på Försäkringskassans webbplats, där dessa möjligheter nämns under rubriken Sjukanmäl genom självbetjäning.

Oavsett om manuell eller automatisk filöverföring väljs, överför arbetsgivaren endast personnummer och datum (fr.o.m.-t.o.m.) till Försäkringskassan. När Försäkringskassan tagit emot uppgifterna skickar man ut ansökningsblanketter till de anställdas folkbokföringsadresser.

Vid manuell filöverföring sker alla överföringar krypterat.

Vid automatisk filöverföring över Infratjänsten krävs att arbetsgivaren har ett avtal med en infratjänstleverantör som sköter kopplingen mellan arbetsgivarens och Försäkringskassans system. För offentlig sektor finns ramavtal med leverantörerna TietoEnator och WM-data. Försäkringskassan känner inte till vilken säkerhet TietoEnator och WM-data tillämpar för uppgifter som dessa

förmedlar mellan arbetsgivaren och Försäkringskassan. Försäkringskassan anser att säkerheten är en fråga för arbetsgivaren som har ett avtal med leverantören, och inte för Försäkringskassan. Arbetsgivaren skickar filerna på egen risk. Först när uppgifterna kommit innanför Försäkringskassans brandvägg, anser Försäkringskassan att man har ett ansvar för behandlingen.

Skäl för beslutet

1. Rutiner för information till de registrerade och rättelse

Rutiner för information till de registrerade och rättelse

Försäkringskassans handläggare måste tillämpa och behärska flera olika regelverk. Först och främst den materiella socialförsäkringslagstiftning som är aktuell i ett ärende. Men handläggaren måste även tillämpa flera andra regelverk parallellt:
– förvaltningslagen som reglerar rätten till partsinsyn och Försäkringskassans kommuniceringsskyldighet,
– lagen om allmän försäkring som, vanligen, reglerar ändringar, omprövningar och överklaganden av Försäkringskassans beslut, samt
- PuL som reglerar de registrerades rätt till information (s.k. registerutdrag) och rättelse.

Det förekommer att Datainspektionen far frågor och klagomål från allmänheten angående Försäkringskassans tillämpning av ovan nämnda lagar (se exempelvis Datainspektionens dnr 947-2007). Det har framkommit att Försäkringskassans handläggare inte alltid tydligt skiljt mellan de olika regelverken.

Med hänsyn härtill och till vad som framkommit i tillsynsärendet anser Datainspektionen att det finns ett stort behov av tydliga och enhetliga rutiner hos Försäkringskassan.

Eftersom Försäkringskassan nu har påbörjat sitt arbete med att ta fram sådana rutiner finns det inte någon anledning för Datainspektionen att vidta några ytterligare åtgärder. Datainspektionen kommer dock att följa upp om några rutiner har tagits fram.

Vad informationen enligt 27 § SofdL (registerutdraget) ska omfatta

I 27 § SofdL anges följande. Personuppgifter i handlingar som kommit in i ett ärende eller upprättats i ett ärende behöver inte tas med i information enligt 26 § PuL om den registrerade tagit del av handlingens innehåll. Av informationen skall det dock framgå vilka sådana handlingar som behandlas. Om den registrerade begär information om uppgifter i en sådan handling och anger vilken handling som avses, skall dock informationen omfatta dessa uppgifter, om inte annat följer av bestämmelser om sekretess. I sistnämnda fall skall begränsningen i 26 § PuL om att information bara behöver lämnas gratis en gång per kalenderår gälla varje handling för sig.

Bestämmelsen i 27 § SofdL utgör en särreglering i förhållande till PuL och undantar vissa uppgifter som annars enligt PuL vid en första begäran måste lämnas ut till den registrerade. Undantagets omfattning anges tydligt i laxtexten: Personuppgifter i handlingar som kommit in i ett ärende eller upprättats i ett ärende behöver inte tas med i information enligt 26 § PuL om den registrerade tagit del av handlingens innehåll. Det som avgör vad som ska tas med i registerutdraget är således vad den registrerade kan anses ha tagit del av. Datainspektionen anser att det förarbetsuttalande som Försäkringskassan åberopar inte ändrar innebörden av lagens uttryckliga och tydliga lydelse. Försäkringskassans nuvarande tillämpning 27 § SofdL kan därför i vissa fall leda till en otillåten inskränkning av den registrerades rätt till information.

Försäkringskassan måste ta ställning till hur myndigheten ska bedöma vilka handlingar den registrerade tagit del av.

Datainspektionen förutsätter att Försäkringskassan beaktar Datainspektionens synpunkter i denna fråga och att Försäkringskassan i sina kommande riktlinjer presenterar en vägledning som inte bygger på Försäkringskassans nuvarande tolkning av 27 § SofdL, och som istället klargör för handläggarna hur de ska göra bedömningen av vad den registrerade kan anses ha tagit del av.

2. **Rättelse i medicinska utredningar**

I 30 § SofdL anges följande. Bestämmelserna i PuL om rättelse och skadestånd gäller vid behandling av personuppgifter enligt denna lag eller föreskrifter som har meddelats i anslutning till denna lag.

Av 9 och 28 §§ PuL framgår bl.a. att felaktiga personuppgifter ska rättas.

Den omständigheten att det rör sig om påstådda felaktigheter i utredningar som kommit in till Försäkringskassan, medför inte att det saknas skyldighet för Försäkringskassan att vidta rättelse eller att i beslut med besvärshänvisning neka rättelse av den påstådda felaktiga uppgiften. Försäkringskassan kan därför inte nöja sig med att hänvisa till den som genomfört den aktuella utredningen.

Denna bedömning avser dock endast påstådda felaktigheter enligt PuL. Försäkringskassans skyldighet att meddela beslut enligt 30 § SofdL aktualiseras således inte när den registrerade ifrågasätter medicinska bedömningar. Kritik mot medicinska bedömningar noteras i stället av Försäkringskassan i samband med kommunicering av underlaget inför beslut om försäkringsförmån.

Om rättelse vidtas måste Försäkringskassan i regel underrätta tredje man, exempelvis den som utfärdat intyget, om den felaktiga uppgiften även finns kvar hos denne.

Det finns som sagt inget undantag i Försäkringskassans skyldighet att korrigera felaktiga personuppgifter endast av den anledningen att de finns i ett intyg som kommit in till Försäkringskassan. Däremot finns det bestämmelser om arkivering och gallring som reglerar på vilket sätt Försäkringskassan ska korrigera felaktiga personuppgifter. Frågan behandlas i PuLs förarbeten.

"En myndighet har således enligt den nya persondatalagen frihet att välja om felaktiga, missvisande eller ofullständiga uppgifter skall rättas, utplånas eller blockeras. Detta innebär att myndigheten givetvis inte far välja att *utplåna* t.ex. en uppgift i en allmän handling, om det skulle strida mot andra bestämmelser. Valet av korrigeringsmetod kan således styras av andra bestämmelser som myndigheten har att rätta sig efter. (...) Att en uppgift *rättas* innebär att den ursprungliga, felaktiga, missvisande eller ofullständiga uppgiften ersätts av en uppgift om de rätta förhållandena eller att uppgifterna annars kompletteras. Det finns inte något krav på att den felaktiga uppgiften skall utplånas. Det bör vara upp till den som är ansvarig för behandlingen att avgöra hur rättelsen skall göras. Det enda kravet är – om den felaktiga uppgiften inte utplånas – att det i alla sammanhang klart skall framgå att den felaktiga uppgiften har ersatts av en annan uppgift och vilka de rätta förhållandena är. Något hinder mot att med stöd av offentlighetsprincipen lämna ut den (tydligt markerade) felaktiga uppgiften jämte de riktiga uppgifterna och upplysning om den rättelse som skett finns inte. Det torde vara denna rättelsemetod som myndigheter i allmänhet bör använda."
(SOU 1997: 39, *Integritet • Offentlighet • Informationsteknik,* sid. 217f)

Datainspektionen förutsätter att Försäkringskassan beaktar Datainspektionens synpunkter i denna fråga och att Försäkringskassan i sina kommande riktlinjer presenterar en vägledning som inte bygger på Försäkringskassans nuvarande tolkning av 30 § SofdL, utan som istället klargör för handläggarna hur de ska göra bedömningen av i vilka situationer beslut om rättelse enligt 30 § SofdL ska meddelas.

Datainspektionen anser inte att det för närvarande finns skäl att vidta några ytterligare åtgärder.

3. Sms-tjänsten för anmälan av tillfällig föräldrapenning

Av huvudregeln i 4 kap. 15 § första meningen AFL framgår att en förälder, för att kunna få tillfällig föräldrapenning, senast den aktuella frånvarodagen måste anmäla att han eller hon kommer att göra anspråk på tillfällig föräldrapenning för dagen ifråga.

Försäkringskassan anser sig inte ansvara för den behandling av personuppgifter som sker innan sms:et med anmälan om tillfällig föräldrapenning når Försäkringskassan. Försäkringskassan har hävdat att det dessförinnan är fråga om en sådan behandling av rent privat natur som enligt 6 § PuL är undantagen från lagens tillämpningsområde.

Enligt 6 § Pul gäller denna lag inte för sådan behandling av personuppgifter som en fysisk person utför som ett led i en verksamhet av rent privat natur. Med "rent privat natur" menas enligt förarbetena t.ex. att enskilda för rent privat bruk kan föra en elektronisk dagbok eller registrera sina grannar eller släktingar (prop. 1997/98:44, sid. 117).

I förarbetena berörs även enskilda personers kommunikationer med myndigheter, bl.a. sägs följande. "Om myndigheter, företag eller organisationer

vidarebefordrar personuppgifter med e-post saknas anledning att inte låta lagens bestämmelser om behandling av personuppgifter bli tillämpliga. Detsamma gäller om enskilda med användande av e-post lämnar personuppgifter som myndigheterna samlar in exempelvis för statistik."(SOU 1997:37, sid. 1990

Mot bakgrund härav anser Datainspektionen att undantaget i 6 § PuL för rent privat behandling av personuppgifter, inte omfattar enskilda personers nyttjande av myndigheters automatiserade självbetjäningstjänster. När Försäkringskassan ställer en sms-självbetjäningstjänst till allmänhetens förfogande för anmälan av tillfällig föräldrapenning, anser Datainspektionen att Försäkringskassan samlar in personuppgifter på ett sätt som gör att PuL blir tillämplig och att Försäkringskassan är personuppgiftsansvarig för behandlingen.

Det innebär att Försäkringskassan ska tillämpa säkerhetsbestämmelserna i 31 § PuL. Av 31 § första stycket PuL framgår att den personuppgiftsansvarige skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna skall åstadkomma en säkerhetsnivå som är lämplig med beaktande av följande: 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.

Det sagda innebär inte nödvändigtvis att Försäkringskassan bör upphöra med den aktuella sms-tjänsten, eller att Försäkringskassan måste omgärda sms-tjänsten med omfattande och dyrbara säkerhetsarrangemang.

Försäkringskassan måste emellertid göra den i 31 § PuL föreskrivna bedömningen av vilka säkerhetsåtgärder som är lämpliga för den aktuella personuppgiftsbehandlingen. Detta har Försäkringskassan inte gjort, eftersom man ansett att PuL överhuvudtaget inte är tillämplig på sms-tjänsten innan personuppgifterna mottagits av Försäkringskassan.

Datainspektionen anser därför att det finns skäl att förelägga Försäkringskassan att genomföra en risk- och sårbarhetsanalys av sin sms-tjänst för anmälan av tillfällig föräldrapenning, samt att underrätta Datainspektionen om resultatet av analysen och vilka slutsatser som Försäkringskassan drar av analysen.

4. Arbetsgivares anmälan av sjukdomsfall över Infratjänsten

Av bl.a. 12 § lagen (1991:1047) om sjuklön framgår att arbetsgivaren är skyldig att till Försäkringskassan anmäla anställdas sjukdomsfall inom sju dagar efter sjuklöneperiodens slut, det vill säga under sjukdag 15-21.

Genom Försäkringskassans självbetjäningstjänst kan arbetsgivare med hjälp av bl.a. Infratjänsten fullgöra sin lagstadgade anmälningsskyldighet av anställdas sjukdomsfall.

När Försäkringskassan ställer en självbetjäningstjänst till arbetsgivarnas förfogande för anmälan av anställdas sjukdomsfall, anser Datainspektionen att Försäkringskassan samlar in personuppgifter på ett sätt som gör att Försäkringskassan får ansvar för de personuppgifter som behandlas i självbetjäningstjänsten.

Det innebär att Försäkringskassan ska tillämpa säkerhetsbestämmelserna i 31 § PuL. Av 31 § första stycket 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 följande: 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.

Försäkringskassan måste göra den i 31 § PuL föreskrivna bedömningen av vilka säkerhetsåtgärder som är lämpliga för personuppgiftsbehandlingen i Infratjänsten vid arbetsgivares anmälan av anställdas sjukdomsfall. Detta har Försäkringskassan inte gjort, eftersom man ansett att Försäkringskassan inte ansvarar för behandlingen innan uppgifterna passerat Försäkringskassan brandvägg.

Datainspektionen vill i sammanhanget erinra om att känsliga personuppgifter ska vara krypterade vid överföring via öppna nät.

Datainspektionen anser därför att det finns skäl att förelägga Försäkringskassan att genomföra en risk- och sårbarhetsanalys av Infratjänsten som används vid arbetsgivares anmälan av anställdas sjukdomsfall, samt att underrätta Datainspektionen om resultatet av analysen och vilka slutsatser som Försäkringskassan drar av analysen.

ÖVERKLAGANDE AV BESLUTET

Om ni vill överklaga beslutet skall Ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som Ni begär. Inspektionen måste ha fatt Ert överklagande inom tre veckor från den dag beslutet meddelades, annars kan överklagandet inte prövas. Datainspektionen sänder överklagandet vidare till Länsrätten i Stockholms län för prövning, om inspektionen inte själv ändrar beslutet på det sätt Ni har begärt.

Beslut i detta ärende har fattats av generaldirektören Göran Gräslund i närvaro av datarådet Katja Isberg Amnäs, IT-säkerhetsspecialisten Magnus Bergström och juristen Erik Janzon, föredragande.

Göran Gräslund

Erik Janzon