Målnummer: 4453-10 **Avdelning:** 1

Avgörandedatum: 2012-06-05

Rubrik: Försäkringskassan har vid tillhandahållande av elektroniska självbetjäningstjänster ansetts personuppgiftsansvarig för den behandling som sker innan uppgifterna blir tillgängliga för kassan.

Lagrum:
- 3 §, 6 §, 31 §, 32 § och 43 b § personuppgiftslagen (1998:204)
- Punkt 46 och punkt 47 i ingressen till Europaparlamentets och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter

Rättsfall:

REFERAT

Datainspektionen beslutade den 20 december 2008 att förelägga Försäkringskassan att genomföra en risk- och sårbarhetsanalys av sin sms-tjänst för anmälan av tillfällig föräldrapenning samt av Infratjänsten som används vid arbetsgivares anmälan av anställdas sjukdomsfall, samt att underrätta Datainspektionen om resultatet av analyserna och vilka slutsatser som Försäkringskassan drar av analyserna. Beslutet grundades på att Försäkringskassan ansågs personuppgiftsansvarig för personuppgiftsbehandlingen i de aktuella självbetjäningstjänsterna enligt 31 § personuppgiftslagen (1998:204), PuL.

Försäkringskassan överklagade Datainspektionens beslut hos länsrätten och yrkade att beslutet avseende risk- och sårbarhetsanalys av kassans sms-tjänst och Infratjänst skulle upphävas. Försäkringskassan anförde bl.a. följande. Kassan är inte ansvarig för behandlingen av personuppgifter förrän vid den tidpunkt då sms-meddelandet nått Försäkringskassan respektive när arbetsgivarens uppgifter passerat kassans brandvägg, eftersom det är först då som Försäkringskassan har bestämt ändamålen med behandlingen och hur denna ska gå till. När det gäller sms-tjänsten är det innan den tidpunkt som sms-meddelandet når Försäkringskassan fråga om en sådan behandling av rent privat natur som enligt 6 § PuL är undantagen från lagens tillämpningsområde. Om behandlingen inte skulle anses vara undantagen från lagens tillämpningsområde kan Försäkringskassan ändå inte göras ansvarig för tekniska och organisatoriska åtgärder vad gäller personuppgifter som förmedlas av en tredje part förrän personuppgifterna nått Försäkringskassan. Vad gäller arbetsgivarnas nyttjande av Infratjänsten faller det på sin egen orimlighet att kassan ska ansvara för det som sker inom företaget. Den behandling av personuppgifter som arbetsgivaren utför för att ta fram information till kassan faller på arbetsgivarens ansvar. Inte heller kan kassan ta ansvar för den information som arbetsgivaren skickar, bl.a. för att innehållet kan vara av varierande art och kvalitet.

Datainspektionen vidhöll sitt beslut och bestred bifall till överklagandet.

Länsrätten i Stockholms län (2009-01-28, ordförande Lundholm) yttrade: Den grundläggande frågan i målet är vid vilken tidpunkt Försäkringskassan kan anses personuppgiftsansvarig för de uppgifter som försäkrade och arbetsgivare

lämnar via de aktuella tjänsterna. - En personuppgift är information/fakta om en levande fysisk person. Genom att t.ex. samla in information behandlas informationen. Den som bestämmer ändamålet med och medlen för denna behandling är personuppgiftsansvarig. - I likhet med Datainspektionen finner länsrätten att undantaget för privat behandling av uppgifter enligt 6 § PuL inte är tillämpligt på sådana uppgifter som lämnas till myndigheter för att ligga till grund för den myndighetens verksamhet. Däremot torde själva författandet av ett sådant meddelande falla under undantaget i 6 § PuL (jfr prop. 1997/98:44 s. 54). - Det är Försäkringskassan som bestämt ändamålet med behandlingen av personuppgifterna, nämligen att anmäla olika former av sjukfall. Det är också Försäkringskassan som bestämt medlen för behandlingen. Försäkringskassan har genom att låta försäkrade och arbetsgivare använda sig av sms respektive Infratjänsten för dessa anmälningar öppnat en ny kommunikationsväg mellan försäkrade, arbetsgivare och kassan. Vid skapandet av en sådan kommunikationsväg bör hanteringens risker i förhållande till den enskildes integritet beaktas, även om den fysiska hanteringen av informationen faller utanför myndigheternas kontroll, vilket är fallet i relation till t.ex. den enskildes mobiltelefonileverantör. Detta innebär inte nödvändigtvis att Försäkringskassans tjänster inte kan nyttjas eller att Försäkringskassan ska vidta åtgärder gentemot enskildas mobiltelefonleverantörer. Däremot ska tjänsterna, dvs. insamlingen/anmälningen av sjukfall, utifrån förhållandena och omständigheter uppfylla kraven i PuL. - Länsrätten instämmer således i Datainspektionens bedömning att den omständigheten att Försäkringskassan tillhandahåller tjänster, som förutsätter underliggande kommunikationstjänster från exempelvis teleoperatörer, inte fråntar Försäkringskassan ett personuppgiftsansvar enligt PuL. - Mot bakgrund härav finner länsrätten att det saknas anledning att invända mot Datainspektionens föreläggande. Överklagandet ska följaktligen avslås. - Länsrätten avslår överklagandet.

Försäkringskassan överklagade länsrättens dom hos kammarrätten och yrkade att domen och Datainspektionens beslut skulle upphävas. Kassan anförde bl.a. följande. Försäkringskassan är inte personuppgiftsansvarig för den behandling av personuppgifter som sker innan uppgifterna når kassans elektroniska mottagningsställen. Dessförinnan har kassan inte behandlat uppgifterna. Det finns dessutom inga praktiska möjligheter för kassan att före denna tidpunkt ta ett personuppgiftsansvar. Den behandling av sms-tjänster som sker innan sms-meddelandet når Försäkringskassans elektroniska mottagningsställen är en sådan behandling av personuppgifter som en fysisk person utför som ett led i en verksamhet av rent privat natur, varför PuL inte är tillämplig. Försäkringskassan åberopade ett utlåtande av jur.kand., expert på personuppgiftslagen, Sören Öman, dagtecknat den 3 mars 2009.

Datainspektionen bestred bifall till överklagandet och anförde i huvudsak följande. Försäkringskassans sms-tjänst för anmälan av tillfällig föräldrapenning (sms-tjänsten) och tjänsten för arbetsgivares anmälan av sjukdomsfall över infratjänsten (Infratjänsten) är exempel på sådana e-tjänster som är en väsentlig del i utvecklingen av e-förvaltningen. Syftet är att underlätta för enskilda att kommunicera med myndigheter. Att myndigheter måste ta ett ansvar för säkerheten i dessa e-tjänster inklusive de överföringssätt som myndigheterna anvisar för enskildas kommunikation med e-tjänsten är i det närmaste en självklar utgångspunkt för utvecklingen av e-förvaltningen. Denna utgångspunkt framgår exempelvis av 3 § lagen (2004:115) om självbetjäningstjänster via Internet inom socialförsäkringens administration. Inrättandet av en e-tjänst, såsom Försäkringskassans sms-tjänst och Infratjänst, innebär ett anvisande av en överföringsmetod och det ingår i den personuppgiftsansvariges skyldigheter att bedöma om överföringsmetoden är tillräckligt säker för den avsedda behandlingen av personuppgifter. Ansvaret omfattar sålunda mer än den faktiska behandlingen. Skyldigheten att vidta lämpliga säkerhetsåtgärder enligt 31 § PuL är en sådan planeringsåtgärd som åligger den personuppgiftsansvarige. Det är riktigt att man inte kan vara personuppgiftsansvarig för åtgärder som någon annan vidtar självständigt, för egen räkning och på eget initiativ. De som använder Försäkringskassans sms-

tjänst och Infratjänst har emellertid inte någon självständighet i förhållande till ändamålet och medlen för behandlingen. Uppgifterna som förekommer i anmälningarna som görs med dessa tjänster är förutbestämda och förutsägbara av Försäkringskassan. Det är därför kassan som kan bedöma om de anvisade överföringssätten har tillräckligt hög säkerhet. Användaren har ingen möjlighet att påverka beslut om vilka säkerhetsåtgärder som ska vidtas. Denne kan endast avstå från att använda tjänsterna.

Kammarrätten i Stockholm (2010-06-22, Wahlqvist, Trägård, Råberg, referent) yttrade: Datainspektionen har såsom tillsynsmyndighet enligt 32 § PuL att i enskilda fall besluta om vilka säkerhetsåtgärder som den personuppgiftsansvarige ska vidta enligt 31 § samma lag. Kammarrätten bedömer att en risk- och sårbarhetsanalys får anses vara en sådan säkerhetsåtgärd. - Enligt förklaringssats 46 till dataskyddsdirektivet förutsätter skyddet för de registrerades fri- och rättigheter såvitt avser behandling av personuppgifter att lämpliga tekniska och organisatoriska säkerhetsåtgärder vidtas både när systemet för behandling utformas och när själva behandlingen sker. Detta stöder uppfattningen att säkerhetsåtgärder enligt 31 § PuL kan behöva vidtas redan innan den personuppgiftsansvarige förfogar över personuppgifterna. - Sms-tjänsten och Infratjänsten skiljer sig från mer allmänna kommunikationsvägar såsom traditionell post eller e-post genom att Försäkringskassan aktivt möjliggör användningen av dem och styr över deras funktioner. Kassan får därför enligt kammarrättens mening anses samla in personuppgifter genom de aktuella tjänsterna redan när uppgifterna skickas från de enskilda och deras arbetsgivare, trots att Försäkringskassan då ännu inte förfogar över uppgifterna. - Syftet med säkerhetsåtgärder är enligt 31 § PuL att 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 personuppgifter och hur pass känsliga de behandlade personuppgifterna är. Åtgärder enligt 31 § PuL får i första hand förutsättas gälla säkerheten i de led där den personuppgiftsansvarige förfogar över personuppgifterna, dvs. inom det egna datasystemet och den egna verksamheten. När det gäller en risk- och sårbarhetsanalys kan dock en sådan, som även omfattar leden innan en personuppgift lagrats av den personuppgiftsansvarige, vara nödvändig i syfte att skydda de uppgifter som överförs. - Det har inte kommit fram att en sådan risk- och sårbarhetsanalys, som Datainspektionen har förelagt Försäkringskassan att genomföra, är kostsam eller på annat sätt mindre lämplig. Kammarrätten kommer, med beaktande av det anförda, till samma slutsats som underinstanserna, dvs. att Datainspektionen har haft fog för sitt föreläggande. Överklagandet ska därför avslås. - Kammarrätten avslår överklagandet.

Försäkringskassan överklagade kammarrättens dom och yrkade att Högsta förvaltningsdomstolen skulle upphäva kammarrättens och länsrättens domar samt Datainspektionens beslut. Försäkringskassan anförde följande. Försäkringskassan har i samband med inrättandet av de aktuella tjänsterna givetvis gjort bedömningen att de noga preciserade uppgifter, som är de enda som kan lämnas inom ramen för tjänsterna, bör kunna få lämnas av enskilda som så önskar utan att det för den enskildes överföring till Försäkringskassan krävs några ytterligare säkerhetsåtgärder. Statliga myndigheter bör inte därutöver behöva lägga ned resurser på att analysera risker som hänför sig till sådant som de inte kan åtgärda. I förvaltningslagen (1986:223) infördes 2003 en skyldighet för myndigheterna att se till att medborgarna kan kommunicera med dem med hjälp av e-post. I lagstiftningsärendet redovisades inte någon risk- och sårbarhetsanalys avseende förmedlingen av meddelanden från medborgarna till myndigheterna (prop. 2002/03:62).

Datainspektionen bestred bifall till överklagandet och anförde följande. För att skapa ett lämpligt skydd för behandlade personuppgifter ska den personuppgiftsansvarige vid en samlad bedömning bl.a. ta hänsyn till hur pass känsliga personuppgifterna är, vilka risker som finns med behandlingen samt

vilka tekniska möjligheter som finns tillgängliga på marknaden och kostnaden för dessa. Den säkerhetsbedömning Försäkringskassan redovisar i överklagandet kan inte jämställas med en sådan risk- och sårbarhetsanalys som krävs för att bestämma vilken säkerhetsnivå som är lämplig och vilka eventuella åtgärder som ska vidtas.

Högsta förvaltningsdomstolen (2012-06-05, Melin, Sandström, Almgren, Brickman, Jäderblom) yttrade:

Skälen för avgörandet

Rättslig reglering

I 3 § PuL definieras begreppet behandling av personuppgifter som varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring. Enligt samma lagrum avses med personuppgiftsansvarig den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

Enligt 6 § PuL gäller lagen inte för sådan behandling av personuppgifter som en fysisk person utför som ett led i en verksamhet av rent privat natur.

Den personuppgiftsansvarige ska enligt 31 § första stycket PuL vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av

a) de tekniska möjligheter som finns,

b) vad det skulle kosta att genomföra åtgärderna,

c) de särskilda risker som finns med behandlingen av personuppgifterna, och

d) hur pass känsliga de behandlade personuppgifterna är.

Datainspektionen får i egenskap av tillsynsmyndighet enligt 32 § PuL i enskilda fall besluta om vilka säkerhetsåtgärder som den personuppgiftsansvarige ska vidta enligt 31 §.

Datainspektionen har enligt 43 § b PuL rätt att för sin tillsyn på begäran få upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna.

I punkt 46 i ingressen till Europaparlamentets och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet) anges följande. Skyddet för de registrerades fri-och rättigheter förutsätter såvitt avser behandling av personuppgifter att lämpliga tekniska och organisatoriska åtgärder vidtas både när systemet för behandlingen utformas och när själva behandlingen sker, särskilt för att garantera säkerheten och för att på så sätt hindra all otillåten behandling. Det åligger medlemsstaterna att säkerställa att de registeransvariga respekterar dessa åtgärder. Åtgärderna ska garantera en lämplig säkerhetsnivå med hänsyn till den nuvarande utvecklingsnivån och till kostnaderna för genomförandet under hänsynstagande till de risker behandlingen innebär och arten av de uppgifter som ska skyddas.

I punkt 47 i ingressen till dataskyddsdirektivet anges bl.a. följande. När ett meddelande som innehåller personuppgifter översänds genom förmedling av en organisation för telekommunikation eller elektronisk post, vars enda ändamål

är att översända sådana meddelanden, blir det normalt den från vilken meddelandet härrör och inte den person som erbjuder nämnda tjänst som anses ansvara för behandlingen av personuppgifterna.

Högsta förvaltningsdomstolens bedömning

Försäkringskassan tillhandahåller elektroniska självbetjäningstjänster i form av anmälan av tillfällig föräldrapenning via sms och av arbetsgivares anmälan av sjukfall via en s.k. Infratjänst. I båda fallen är det fråga om att enskilda personer lämnar uppgifter genom elektroniska kommunikationskanaler via olika operatörer. Uppgifterna är inte tillgängliga för Försäkringskassan förrän de når kassans elektroniska mottagningsställen.

För att Försäkringskassan ska betraktas som personuppgiftsansvarig redan innan uppgifter blir tillgängliga för kassan krävs att kassan har bestämt ändamålen med och medlen för behandlingen av dem.

Varken personuppgiftslagen, dess förarbeten eller dataskyddsdirektivet anger hur en avgränsning av personuppgiftsansvaret ska göras.

Försäkringskassan har bestämt ändamålet med behandlingen av personuppgifterna, nämligen att anmäla olika typer av sjukfall. Försäkringskassan har också bestämt medlen för behandlingen av personuppgifter genom att anvisa de kommunikationsvägar som gäller för anmälningarna. I 3 § PuL anges visserligen inte - när det gäller vem som ska anses vara personuppgiftsansvarig - att denne själv måste genomföra behandlingen av uppgifter. Det måste emellertid förutsättas att det för sådant ansvar krävs att den som bestämt ändamål och medel för behandlingen också utför denna, dvs. vidtar åtgärder som innefattar behandling enligt 3 §, eller att sådana åtgärder utförs för dennes räkning.

Den serie av åtgärder i fråga om personuppgifter som vidtas i de aktuella fallen kan betraktas som led i Försäkringskassans behandling av uppgifter i enskilda ärenden. Det gäller trots att Försäkringskassan saknar möjlighet att påverka hur uppgifterna hanteras innan de blir tillgängliga för kassan. Det gäller också oberoende av om någon eller några av åtgärderna skulle utgöra behandling av personuppgifter även hos någon annan. Inte heller vad som uttalas i punkt 47 i ingressen till dataskyddsdirektivet leder till någon annan bedömning. Tvärtom anges det i denna punkt att personuppgiftsansvaret inte upphör att gälla enbart på grund av att den ansvarige saknar faktisk möjlighet att förfoga över uppgifterna i samband med överföring av dem.

Att Försäkringskassan saknar faktisk möjlighet att påverka hur uppgifterna hanteras innan de blir tillgängliga hos kassan kan innebära svårigheter vid bedömningen av de skyldigheter och sanktionsmöjligheter som föreskrivs i PuL och som tar sikte på personuppgiftsansvaret. Det hindrar emellertid inte att Försäkringskassan åläggs att redovisa säkerheten vid behandlingen av personuppgifter enligt 43 § b PuL. Detta gäller trots att en sådan redovisning möjligen kan komma att vara ofullständig i vissa hänseenden när det gäller säkerheten för personuppgifter hos operatörer eller avsändare. Överklagandet ska således avslås.

Högsta förvaltningsdomstolens avgörande

Högsta förvaltningsdomstolen avslår överklagandet.

Föredraget 2012-05-02, föredragande Samuelsson, målnummer 4453-10

Sökord: EU-rätt; Personuppgiftslagen

Litteratur: Personuppgiftslagen - En kommentar, Sören Öman och Hans-Olof Lindblom, 4 u. 2011 s. 99; SOU 1997:39 s. 333