Pfizer AB
Box 501
183 25 Täby

Tillsyn enligt personuppgiftslagen (1998:204) – forskningsprojektet SWEGHO vid Pfizer AB

Datainspektionens beslut

Datainspektionen konstaterar att informationen om vem som är personuppgiftsansvarig för forskningsprojektet SWEGHO är otydlig. Enligt 25 § personuppgiftslagen (1998:204) ska informationen till registrerade omfatta uppgift om den personuppgiftsansvariges identitet. Datainspektionen förelägger Pfizer AB att i patientinformationen tydliggöra personuppgiftsansvaret för den aktuella studien.

Datainspektionen konstaterar att de uppgifter som i patientinformationen anges vara avidentifierade, är personuppgifter eftersom det är möjligt att härleda dem till nu levande fysisk person. Datainspektionen anser att informationen är missvisande och Datainspektionen förelägger Pfizer AB att justera patientinformationen så att det inte råder någon oklarhet om att det är personuppgifter som behandlas.

Datainspektionen konstaterar att Pfizer AB brister i skyddet av känsliga personuppgifter genom att i strid med kraven på lämpliga säkerhetsåtgärder i 31 § personuppgiftslagen lämna ut känsliga personuppgifter över öppet nät efter autentisering med enbart användarnamn och lösenord. Datainspektionen förelägger Pfizer AB att vid anslutning till känsliga personuppgifter via öppet nät införa stark autentisering.

Ärendet avslutas.

Bakgrund

Datainspektionen inledde tillsyn den 20 februari 2014 gentemot Pfizer AB för granskning av forskningsprojekt i vilka känsliga personuppgifter behandlas med stöd av samtycke. Pfizer AB ombads inkomma med en lista över pågående forskningsprojekt som behandlade denna kategori av personuppgifter.

Datainspektionen begärde därefter att Pfizer AB skulle lämna en närmare redogörelse för forskningsprojektet SWEGHO.

Pfizer AB har uppgett att syftet med SWEGHO är att följa patienter som har tillväxthormonbrist och har ordinerats läkemedlet Genotropin. Patienterna ingår i studien under 5 år med start 2013. De som deltar i studien är 18 år eller äldre. Pzifer AB genomförde en observationsstudie under åren 1994-2012 som kallades KIMS. Patienter som deltog i KIMS var patienter med diagnosen tillväxthormonbrist som antingen uppträtt under barnaåren eller i vuxen ålder. KIMS gav information om ovanliga biverkningar och information som kunde bidra till kostnadseffektiv och individualiserad behandling för patientgruppen. Samtliga patienter som deltog i KIMS var över 18 år. Patienter som deltog i KIMS erbjöds att delta i SWEGHO, samtidigt som nya patienter inkluderades. Det anges att personuppgifter i studien kan komma att överföras utanför EU/EES. De aktörer som personuppgifterna överförs till i USA har anslutit sig till Safe Harbour.

Pfizer AB har uppgett att uttryckligt samtycke från samtliga registrerade ska utgöra den lagliga grunden för behandlingen av känsliga personuppgifter i detta forskningsprojekt. Studien är granskad och godkänd av regionala etikprövningsnämnden i Uppsala.

Rättsregler

Personuppgiftslagen

Det är personuppgiftslagen som reglerar förutsättningarna för behandling av personuppgifter i forskningsverksamhet.

Personuppgiftsansvaret

Personuppgiftsansvarig är enligt 3 § personuppgiftslagen den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter, och personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning.
Vem som bestämmer över ändamålen avgörs genom en bedömning av de faktiska omständigheterna i det enskilda fallet. Avgörande för denna bedömning är bland annat varför behandlingen utförs och vem som är initiativtagare till behandlingen. Att bestämma över medlen för behandlingen avser främst att bestämma över de tekniska och organisatoriska medlen för behandlingen, dvs. ”hur” behandlingen ska gå till, till exempel vilka personuppgifter som ska behandlas, vilka tredje män som ska få tillgång till de behandlade personuppgifter och när uppgifter ska raderas.

Olika avtalskonstruktioner där personuppgiftsansvaret preciseras kan beaktas vid bedömningen men det är de faktiska omständigheterna i det enskilda fallet som är avgörande, dvs. vem eller vilka som faktiskt har bestämt över behandlingen, se *Personuppgiftslagen – En kommentar*, Öman och Lindblom, 4 uppl. 2011, s 93-94.

Vidare får ett personuppgiftsbiträde endast behandla uppgifter i enlighet med instruktioner från den personuppgiftsansvarige, se 30 § 1 st personuppgiftslagen. Den personuppgiftsansvarige kan överlåta den faktiska behandlingen av personuppgifter, men personuppgiftsansvaret kan aldrig överlåtas. Det är alltid den personuppgiftsansvarige som ytterst svarar för att personuppgiftslagen följs och att de registrerade behandlas korrekt.

Ansvaret är straff- och skadeståndssanktionerat. Den personuppgiftsansvarige är skadeståndsskyldig gentemot den registrerade, även för åtgärder som en medhjälpare eller ett personuppgiftsbiträde har utfört.

Känsliga personuppgifter

Enligt personuppgiftslagen är känsliga personuppgifter sådana som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt personuppgifter som rör hälsa eller sexualliv. Enligt huvudregeln i personuppgiftslagen är det förbjudet att behandla känsliga personuppgifter men det finns undantag. Känsliga personuppgifter får behandlas för forskningsändamål, enligt 19 § personuppgiftslagen, om behandlingen godkänts enligt lagen (2003:460) om etikprövning av forskning

som avser människor (etikprövningslagen). Efter en lagändring den 1 juni 2008 utvidgades etikprövningslagen så att all forskning som innefattar behandling av sådana personuppgifter som avses i 13 och 21 §§ personuppgiftslagen ska etikprövas, oavsett om forskningspersonen lämnat sitt uttryckliga samtycke till behandlingen eller inte.

Vid etikprövning av forskning som avser att behandla personuppgifter som antingen är känsliga eller som berör lagöverträdelser m.m. ska det i etikprövningsnämndens prövning ingå att bedöma förutsättningarna för behandlingen av personuppgifter och nämnden ska ange om det ställs krav på samtycke. Om etikprövningsnämnden godkänner en forskningsstudie med särskilda villkor avseende krav på samtycke krävs ett uttryckligt samtycke enligt 15 § personuppgiftslagen från de som deltar i forskningsstudien.

Samtycke och information

Av personuppgiftslagen framgår att ett giltigt samtycke enligt 3 och 15 §§ personuppgiftslagen förutsätter att deltagaren eller deras vårdnadshavare har fått information innan de lämnar sitt uttryckliga samtycke. Samtycket ska vara frivilligt, särskilt, informerat och en otvetydig viljeyttring. Att ett samtycke ska vara särskilt innebär att den enskilde ska informeras om en eller fler specificerade behandlingar och samtycket ska avse de specifika behandlingarna var för sig. I den information som deltagarna i en forskningsstudie får innan de lämnar sitt samtycke ska det finnas uppgift om den personuppgiftsansvariges identitet. Det innebär att man ska lämna uppgift om namn och kontaktuppgifter beträffande den normalt sett juridiska person som är personuppgiftsansvarig.

I förarbetena till etikprövningslagen uppges även att när forskaren med stöd av ett etikgodkännande enligt etikprövningslagen behandlar personuppgifter har forskaren att följa – förutom de villkor om t.ex. information till deltagarna som har uppställts i samband med etikgodkännandet – bestämmelserna i personuppgiftslagen, t.ex. om rättelse och så kallad registerutdrag (se prop. 2002/03:50 s 119-120). När det gäller rätten att ansöka om registerutdrag enligt 26 § personuppgiftslagen är det lämpligt att det framgår hur en ansökan om information ska göras, dvs. skriftligen hos den personuppgiftsansvarige. Beträffande rätten att få rättelse enligt 28 § personuppgiftslagen anser Datainspektionen att det är lämpligt att det framgår vart den registrerade kan vända sig för att utnyttja sin rättighet.

Tredje lands överföring

I en forskningsstudie måste den personuppgiftsansvarige även följa personuppgiftslagens regler om överföring av personuppgifter till tredje land när forskningen utförs. En överföring till tredje land sker när personuppgifter görs tillgängliga i ett land utanför EU/EES-området. Utgångspunkten är att det är förbjudet att föra över personuppgifter till tredje land om landet inte har en adekvat nivå för skyddet av personuppgifterna, 33 § personuppgiftslagen. Av 34 § personuppgiftslagen framgår att personuppgifter kan överföras till tredje land om den registrerade har gett ett informerat samtycke eller om överföringen är nödvändig i vissa särskilda situationer som anges i den aktuella bestämmelsen. Personuppgifter får också föras över till tredje land om det i annat fall är tillåtet enligt föreskrifter eller särskilda beslut av regeringen eller Datainspektionen, 35 § personuppgiftslagen samt 13-14 §§ personuppgiftsförordningen (1998:1191).

IT-säkerhet

I 31 § personuppgiftslagen ställs krav på att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de uppgifter som behandlas. Nivån på säkerhetsåtgärder bör klargöras utifrån en risk och sårbarhetsanalys. I bedömningen av lämpligt skydd ska hänsyn tas till tekniska möjligheter, kostnader, särskilda risker och hur känsliga uppgifterna som behandlas är. Personuppgifter ska skyddas från förstöring genom olyckshändelse eller otillåtna handlingar eller förlust genom olyckshändelse samt mot ändringar, otillåten spridning av eller otillåten tillgång till uppgifterna, särskilt om behandlingen innefattar överföring av uppgifter i ett nätverk, och mot varje annat slag av otillåten behandling.

Vid behandling av känsliga personuppgifter som kommuniceras över öppna nät (t.ex. Internet) ska kommunikationen krypteras på ett sådant sätt att obehöriga inte kan ta del av uppgifterna och åtkomst till de känsliga personuppgifterna ska föregås av stark autentisering. Stark autentisering är en säkerhetsåtgärd som ska tillämpas även om de känsliga personuppgifterna är kodade och kravet gäller för alla användare som har möjlighet att få åtkomst till de kodade personuppgifterna via öppet nät.

Det är Datainspektionen uppfattning att det följer av 31 § personuppgiftslagen att om känsliga personuppgifter lämnas ut över öppet nät, till exempel Internet, får det ske endast till identifierade användare vars identitet är

säkerställd med en teknisk funktion såsom asymmetrisk kryptering (t.ex. e-legitimation), engångslösenord eller motsvarande.

Skäl för beslutet

Personuppgiftsansvaret

Av patientinformationen kan utläsas att Pfizer AB är sponsor i den aktuella studien. Vidare framgår under punkten 7 att ”Sponsorn av studien är tillsammans med Institutionen personuppgiftsansvarig för de uppgifter som samlas in i SWEGHO och för den information som inhämtas från den tidigare studien KIMS.” Det är Pfizer AB som tillhandahåller datorstöd och patientinformationen inleds med att ”Sjukvården genomför studien på *uppdrag* av Pfizer AB”. I sammanhanget används också olika begrepp för aktörerna såsom ”kliniken”, ”prövaren”, ”institutionen”, ”ansvarig läkare”. Datainspektionen konstaterar att det är svårt att få klarhet i vem som är personuppgiftsansvarig för vad.

För Pfizer AB måste det givetvis stå klart vilken personuppgiftsbehandling som omfattas av Pfizer AB:s personuppgiftsansvar, dvs. för vilken personuppgiftsbehandling bestämmer Pfizer AB ändamålen och medel (se 3 § personuppgiftslagen). Personuppgiftsansvarets omfattning måste också framgå i informationen till patienterna, så att de registrerade kan ta tillvara sina rättigheter i samband med behandlingen så som nämnts ovan.

Av informationen i ärendet framgår att det är läkaren på kliniken som inhämtar samtycke från patienten. Datainspektionen konstaterar att det är otydligt i vilken egenskap som läkaren inhämtar samtycke från patienter och vem läkaren representerar.

Datainspektionen vill i sammanhanget också påpeka att en vårdgivare måste särskilja uppgifter som omfattas av patientdatalagen från uppgifter som behandlas för forskning. Det är också viktigt att det inte råder någon oklarhet om verksamheternas gränser i förhållande till sekretessreglerna.

Datainspektionen utgår därför från att Pfizer AB klargör omfattningen av personuppgiftsansvaret och gör nödvändiga ändringar i patientinformationen, så att det tydligt framgår för vilken personuppgiftsbehandling Pfizer AB är personuppgiftsansvarig.

Avidentifierade uppgifter

Pzifer AB samlar in information om graviditeter från kvinnor som är eller blir gravida medan de eller deras partner deltar i en Pziferstudie. I den aktuella studien vill företaget kunna inhämta information om en eventuell graviditet och dess utfall för att kunna utvärdera säkerheten och få veta mer om det läkemedel som används i studien påverkar graviditet eller det ofödda barnet. Av informationen till gravida studiepatienter/studiepatientens gravida partner (sid 2) framgår det att personuppgifterna i studien kommer att avidentifieras och sparas på ett sådant sätt så att varken patienten eller barnet kan identifieras utom i de fall Pzifer bland annat ska uppfylla sina regulatoriska rapporteringskrav. Vidare framgår det av informationen att den ansvarige läkaren i studien ansvarar för att den kodnyckel som gör det möjligt att koppla uppgifterna till patienten hålls konfidentiell. Datainspektionen ifrågasätter att uppgifterna är avidentifierade eftersom personer kan identifieras när företaget ska uppfylla sina regulatoriska rapporteringskrav och eftersom det finns en kodnyckel. All information som direkt eller indirekt kan hänföras till en fysisk person är en personuppgift. Kodade uppgifter omfattas därmed av lagen så länge det finns en kodnyckel bevarad med vars hjälp det är möjligt att identifiera enskilda individer. Det saknas i detta hänseende betydelse var och hos vem kodnyckeln förvaras. Det är därför missvisande att ange att uppgifterna är avidentifierade när kodnyckeln finns kvar. Datainspektionen utgår därför från att Pfizer AB på denna punkt gör nödvändiga ändringar i patientinformationen.

Säkerheten för behandling av personuppgifter

Av inlagan till Datainspektionen framgår att avidentifierade forskningsdata lagras i programvaran Viedoc, en webbaserad tjänst för kliniska prövningar och patientregister. Tjänsten utvecklas och driften sker i Sverige av företaget Pharma Consulting Group AB som enligt avtal med Pfizer AB tillhandahåller tjänsten och som också har en avtalsreglerad roll som personuppgiftsbiträde åt Pfizer AB. Det finns enligt Pzifer AB skriftligt personuppgiftsbiträdesavtal med Pharma Consulting Group AB. Nätverksförbindelse mellan användare och Viedoc är alltid krypterad. En användare får ett individuellt konto i systemet genom en kontrollerad ansökningsprocedur. Autentisering sker med ett unikt användarnamn och lösenord. Lösenordet måste uppnå en definierad komplexitetsnivå och bytas med en viss frekvens.

Mot bakgrund av uppgifter i ärendet konstaterar Datainspektionen att anslutning mot Viedoc brister då det inte sker med hjälp av stark autentisering trots att det är frågan om känsliga personuppgifter.

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 ni fick del av beslutet. 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. Vid den slutliga handläggningen har även it-säkerhetsspecialisten Fredrik Ekman deltagit.

Katarina Tullstedt

Salomeh Fanaei

Kopia till:

NN