Roche AB
Box 437 27
100 47 Stockholm

Tillsyn enligt personuppgiftslagen (1998:204) - två forskningsprojekt vid Roche AB

Datainspektionens beslut

Datainspektionen förelägger Roche AB att justera informationen till patienter enligt följande:

- Datainspektionen konstaterar att informationen om vem som är personuppgiftsansvarig är missvisande eller otydlig. Enligt 25 § personuppgiftslagen (1998:204) ska informationen till registrerade omfatta uppgift om den personuppgiftsansvariges identitet. Datainspektionen förelägger Roche AB att i patientinformationen tydliggöra personuppgiftsansvaret för båda studierna.
- Av patientinformationen ska framgå huruvida personuppgifterna kan komma att överföras till tredje land i studien PrefMab.
- Datainspektionen konstaterar att de uppgifter som i patientinformationen till studien Arthur 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 Roche AB att justera patientinformationen så att det inte råder någon oklarhet om att det är personuppgifter som behandlas.
- Äldre barn/ungdomar som är föremål för studien Arthur, ska ges fullständig information i enlighet med 25 § personuppgiftslagen vilket innebär att i den granskade informationen ska tilläggas uppgift om den personuppgiftsansvariges identitet och rätten att ansöka om registerutdrag och rättelse.

Datainspektionen erinrar Roche AB att ett giltigt samtycke enligt personuppgiftslagen förutsätter att patienter/vårdnadshavare i studien Arthur har fått information innan studien startar.

Ärendet avslutas.

Bakgrund

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

Datainspektionen begärde därefter att Roche AB skulle lämna en närmare redogörelse för följande forskningsprojekt:

- PrefMab, MO28457 (PrefMab)
- Arthur, WA28029 (Arthur)

Studien PrefMab riktar sig till patienter med cancer i lymfkörteln. Syftet med studien är att undersöka möjligheten att ge läkemedlet MabThera genom en injektion i underhuden istället för genom intravenös dropp. Patienten ska i studien ge information om vilket sätt man föredrar att få läkemedlet. Deltagare i studien är enligt etikansökan mellan 18 och 80 år. Av patientinformationen framgår att personuppgifterna kan komma att skickas utomlands. Det anges i patientinformation till studien PrefMab under rubriken patientsamtycke- studie MO28457 att genom att patienten signerar information ges samtidigt samtycke till att personuppgifterna bland annat kan analyseras av företag som Roche AB samarbetar med och några av dessa kan finnas i andra länder. Studien är granskad och godkänd av regionala etikprövningsnämnden i Göteborg.

Forskningsstudien Arthur syftar till att utreda huruvida läkemedlet tocilizumab kan ges med längre tid mellan behandlingarna vid behandling av juvenil idiopatisk artrit. Barn i åldrarna 2-17 år deltar i studien. Av informationen till vårdnadshavare till barn i studien kan utläsas att insamlad data under studien om barnet kommer att bearbetas av F. Hoffman- La Roche eller dess samarbetspartner i Sverige eller utomlands. I forskningsstudien

Arthur anges att samtycket även omfattar behandling av personuppgifter utanför EU. Studien är granskad och godkänd av regionala etikprövningsnämnden i Stockholm.

Roche AB har uppgett att uttryckligt samtycke från samtliga registrerade ska utgöra den lagliga grunden för behandlingen av känsliga personuppgifter i de i ärendet aktuella forskningsprojekten.

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

Forskningsprojekt PrefMab

I patientinformationen anges att kontaktperson på Roche AB är personuppgiftsansvarige NN. Personuppgiftsansvarig är enligt definitionen i 3 § personuppgiftslagen den person som bestämmer ändamål och medel med behandlingen. Behandlas personuppgifter i en verksamhet så är det den juridiska personen som är personuppgiftsansvarig. Det är således inte verksamhetsansvarig, personuppgiftsombudet, forskaren eller någon annan anställd som är personuppgiftsansvarig. Datainspektionen anser att det är positivt att Roche AB angett en kontaktperson, men att det är missvisande att ange att kontaktpersonen är personuppgiftsansvarig.

Enligt patientinformationen kan personuppgifter överföras till Roche AB och samarbetande organisationer i Sverige eller utomlands. I avsnittet patientsamtycke ger patienten ett medgivande till att personuppgifter analyseras av Roche AB eller samarbetande företag och att några av dessa kan finnas i andra länder (PrefMab sid 4 och 6). För att en patient ska kunna lämna ett giltigt samtycke till överföring av personuppgifter till tredje land måste patienten få information om överföringen. Att uppgifterna skickas

utomlands eller till andra länder betyder inte att de nödvändigtvis skickas till tredje land. Datainspektionen konstaterar att information om uppgifter i studien PrefMab kommer att överföras till tredje land saknas.

Vidare framgår att för att kvalitetskontrollera studien kommer så kallad monitorering utföras av representant från Roche. Den personuppgiftsansvarige dvs. Roche AB har bevisbördan för att den registrerade har fått den information som krävs och det är därför i dennes intresse att den informationen som lämnas är begriplig för den registrerade. Datainspektionen anser att facktermer såsom ”monitorering” behöver förklaras för patienter (se *Personuppgiftslagen - En kommentar,* Öman och Lindblom, 4 uppl. 2011, s 390).

Forskningsprojektet Arthur

Avidentifiering
I avsnittet ”Hantering av data och sekretess” anges att all information *avidentifieras* innan den överförs. Meningen i sig är ofullständig då det saknas information om vart uppgifterna överförs (se Arthur sid 9 andra meningen). Beträffande avidentifieringen får patienten information om att barnets personuppgifter får en kod som endast läkaren kan identifiera och att nyckeln till denna kod förvaras under och *efter* studien på kliniken och är endast tillgänglig för ansvarig läkare. 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 saknar betydelse var och hos vem kodnyckeln förvaras. Så länge kodnyckeln finns kvar är uppgifterna således personuppgifter för att de kan härledas till en person. Det är därför missvisande att ange att uppgifterna är avidentifierade när kodnyckeln finns kvar.

Personuppgiftsansvaret
Under rubriken ”personuppgiftsansvarig” anges att Landstinget i Stockholms län samt Roche AB är personuppgiftsansvariga för denna studie.

Datainspektionen konstaterar att det är svårt att få klarhet i vem som är personuppgiftsansvarig för vad.

För Roche AB måste det givetvis stå klart vilken personuppgiftsbehandling som omfattas av Roche AB:s personuppgiftsansvar, dvs. för vilken personuppgiftsbehandling bestämmer Roche AB ändamålen och medel (se 3 § personuppgiftslagen). Personuppgiftsansvarets omfattning måste också framgå av 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 ansvarig läkare ger information till patienten och 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 Roche AB klargör omfattningen av personuppgiftsansvaret i studien Arthur och gör nödvändiga ändringar i patientinformationen, så att det tydligt framgår för vilken personuppgiftsbehandling Roche AB är personuppgiftsansvarig.

Information
Datainspektionen konstaterar att patientinformation till vårdnadshavare och äldre barn/ungdomar är daterade efter att Datainspektionens tillsyn inleddes. Den av Roche AB inlämnade patientinformation och samtycke för studien Arthur är daterad 16 april 2014. Även medgivandeformuläret (för äldre barn/ungdomar) är daterad 16 april 2014. Samtidigt framgår av utredningen i ärendet att studierna startades innan 2014. För att samtycket ska vara giltigt enligt personuppgiftslagen ska den registrerade ha fått tillräcklig information om behandlingen. Informationen måste lämnas innan patienten kan ge sitt samtycke till att delta i studien.

Medgivandeformulär (för äldre barn/ungdomar)
För att äldre barn ska kunna lämna ett giltigt samtycke ska informationen innehålla alla nödvändiga uppgifter i enlighet med 25 § personuppgiftslagen och på ett sätt som är begripligt för äldre barn. Datainspektionen konstaterar att det i medgivandeformuläret för äldre barn/ungdomar saknas information om vem som är personuppgiftsansvarig och övrig information som behövs för

att den registrerade ska kunna ta tillvara sina rättigheter i samband med behandlingen såsom rätten att ansöka om registerutdrag och rätten att få rättelse.

Säkerheten vid behandling av personuppgifter i båda studierna

Datainspektionen konstaterar att Roche AB inte har besvarat frågorna om IT-säkerheten. Med anledning av detta kan Datainspektionen inte uttala sig om Roche AB lever upp till säkerhetskraven i 31 § personuppgiftslagen.

Datainspektionen anser att det är anmärkningsvärt att Roche AB inte besvarat Datainspektionens frågor gällande IT-säkerheten mot bakgrund av att Datainspektionen enligt 43 § personuppgiftslagen har rätt att för sin tillsyn på begäran få upplysningar om och dokumentation gällande behandlingen av personuppgifter och säkerheten vid denna.

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, samma adress som ovan.