Karolinska institutet
171 77 Stockholm

Tillsyn enligt personuppgiftslagen (1998:204) LifeGene - direktåtkomst, säkerhet för känsliga personuppgifter samt samtycke och information

Datainspektionens beslut

Datainspektionen konstaterar att Karolinska institutet:

- i strid mot förbudet i 11 § lagen (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa, genom direktåtkomst lämnar ut personuppgifter i registret LifeGene,

- brister i skyddet av känsliga personuppgifter genom att i strid med kraven på lämpliga säkerhetsåtgärder i 31 § personuppgiftslagen (1998:204) lämnar ut känsliga personuppgifter över öppet nät efter autentisering med enbart användarnamn och lösenord, och

- brister i informationsmaterialet om LifeGene. Informationen uppfyller inte kraven i 14 § lagen (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa avseende för vilka *ändamål* behandlingen av personuppgifter kan komma att ske, vilka uppgifter som får registreras, de *sekretess- och säkerhetsbestämmelser* som gäller för registret och *hur länge* uppgifterna kommer att sparas.

Datainspektionen konstaterar även att deltagare som registrerats innan lagens ikraftträdande inte har fått fullständig information eller lämnat samtycke enligt 14 § lagen (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa.

Datainspektionen förelägger Karolinska institutet att

1. Upphöra med utlämnande genom direktåtkomst till personuppgifter i registret LifeGene.
2. Upphöra att lämna ut känsliga personuppgifter i registret LifeGene över öppet nät efter autentisering med enbart användarnamn och lösenord.
3. Uppdatera sin information till registrerade med följande.
    a. Uppgift om ändamålen med registret,
    b. de sekretess- och säkerhetsbestämmelser som gäller för registret, och
    c. uppgift om hur länge uppgifterna sparas.
4. Delge de deltagare som registrerats före lagens ikraftträdande den uppdaterade informationen.
5. Inhämta ett uttryckligt samtycke från de deltagare som registrerats före lagens ikraftträdande.

Datainspektionen förutsätter att Karolinska institutet tar fram rutiner för att i registret LifeGene gallra uppgifter om de deltagare som, efter att ha tagit del av den uppdaterade informationen inte lämnar sitt samtycke till behandlingen av personuppgifter.

Föreläggandet i punkten 2 ska enligt 51 § andra stycket personuppgiftslagen (1998:204) gälla även om beslutet överklagas.

Ärendet avslutas, men kan komma att följas upp.

Redogörelse för tillsynsärendet

Datainspektionen beslutade den 7 mars 2014, att inleda tillsyn mot Karolinska institutet. Bakgrunden och frågorna framgår av tillsynsskrivelsen. Karolinska institutet inkom den 31 mars 2014 med ett yttrande med svar på Datainspektionens frågor. Till yttrandet bifogades en *informationsbroschyr* om LifeGene, version 2014-01-23 (bilaga 1), blanketten *Informerat samtycke* (bilaga 2), *samtyckesinformation* (bilaga 3), *Ärende- och mailhantering LifeGene Servicecenter* (bilaga 4), *Erinran om informationssäkerhet och ansvar i LifeGene* (bilaga 5) och *Riktlinjer och regler för informationssäkerhet vid Karolinska institutet* (bilaga 6). Karolinska institutet kontaktade också Datainspektionen i ärendet den 24 november 2014.

Skäl för beslutet

Om inget annat anges avses i detta beslut med *lagen*, lag (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa och med *propositionen*, regeringens proposition 2012/13:163 Vissa register för forskning om vad arv och miljö betyder för människors hälsa.

Karolinska institutet får enligt vad som anges i bilagan till förordningen (2013:833) om vissa register för forskning om vad arv och miljö betyder för människors hälsa som personuppgiftsansvarig behandla personuppgifter i registret LifeGene i enlighet med 2 § lagen. Lagen och den förordningen trädde ikraft i december 2013.

Direktåtkomst

Utgångspunkter för Datainspektionens bedömning
När en person begär att ta del av en allmän handling är det fråga om ett utlämnande enligt 2 kap. tryckfrihetsförordningen. Ett sådant utlämnande kräver i första hand en sekretessprövning. Även om sekretess inte hindrar ett utlämnande kan dataskyddsregler innebära hinder för ett elektroniskt utlämnande. De elektroniska utlämnandena kan ske på vad som brukar benämnas medium för automatiserad behandling eller genom direktåtkomst.

Beträffande den registrerade anges uttryckligen i 7 § tredje stycket i lagen att personuppgifter som registrerats enligt lagen alltid får lämnas ut till den registrerade själv.

Beträffande formen för elektroniskt utlämnande anges i lagens 11 § att utlämnande genom direktåtkomst till personuppgifter inte får förekomma.

Karolinska institutet medger deltagare möjligheten att via en ”personlig hemsida” på egen hand söka efter uppgifter om sig själva som finns i registret LifeGene. Karolinska institutet uppger i yttrandet att de inte anser att det är frågan om direktåtkomst och beskriver förfarandet på följande sätt.

> *”Karolinska anser att deltagarna inte ges direktåtkomst till sina personuppgifter. Deltagare får vid besök på Testcenter ange om de vill ha tillgång till sina provsvar. LifeGene lägger då upp ett dokument på deltagarens personliga hemsida där deras respektive provsvar läggs in. Deltagaren kan inte själv gå in och söka på sina resultat i databasen.*

> *LifeGene har kontroll på vilka uppgifter som lämnats ut. Systemet för webbplatsen frågar via två olika web service anrop den centrala databasen om information om en specifik deltagare. Svar på den specifika frågan hämtas från den centrala databasen och lämnas ut till deltagaren via deras personliga hemsida."*

Beträffande direktåtkomst anges i propositionen (s. 44) följande.

> *"Begreppets [direktåtkomst] grundläggande innebörd är vanligtvis att någon har direkt tillgång till någon annans register eller databaser och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i registret eller databasen. I begreppet direktåtkomst ligger också att den som är ansvarig för registret eller databasen inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst tillfälle tar del av (se t.ex. prop. 2004/05:164 s. 83)".*

Den andra formen av utlämnande benämns vanligen utlämnande på medium för automatiserad behandling och innebär, förenklat uttryckt, elektroniskt utlämnande utan möjlighet för mottagaren att själv bereda sig tillgång till uppgifterna t.ex. genom att utlämnandet sker via e-post, på cd-rom eller genom filöverföring från ett datorsystem till ett annat. Själva utlämnandet sker således genom en aktiv handling hos den utlämnande myndigheten.

Datainspektionens bedömning
Det kan konstateras att uppgifterna om en deltagare i registret LifeGene, som ett sekundärt ändamål får behandlas för att lämnas ut till deltagaren själv. Beträffande formen för utlämnandet innehåller lagen en tydlig begränsning. Utlämnande genom direktåtkomst till personuppgifter i registret får inte förekomma (11 § lagen). Av förarbetena framgår att lagstiftaren infört detta förbud i fullt medvetande om att utlämnande av personuppgifter till enskilda genom direktåtkomst tillåtits i annan lagstiftning såsom i 5 kap. 5 § patientdatalagen (2008:355) och 12 § studiestödsdatalagen (2009:287), se propositionen s. 45.

Karolinska institutet har gett deltagare möjligheten att via en "personlig hemsida" på egen hand söka efter de uppgifter om sig själva som finns i registret LifeGene. Formen för utlämnandet skiljer sig inte på något väsentligt vis från hur vårdgivarna, med stöd av bestämmelserna om direktåtkomst i

patientdatalagen, lämnar ut vårddokumentation till patienter via s.k. e-tjänster.

Karolinska institutet saknar kontroll över vilka uppgifter ur registret LifeGene som lämnas ut till deltagaren vid ett visst tillfälle. Det är deltagaren som fritt söker fram de uppgifter som finns i registret LifeGene om deltagaren, vid tidpunkter som denne själv väljer och avseende de uppgifter som deltagaren vid varje tillfälle vill ta del av.

Datainspektionen konstaterar således att Karolinska institutet ger deltagarna direktåtkomst till uppgifter i registret LifeGene utan att ha lagligt stöd för det. Direktåtkomsten måste därför upphöra.

Säkerhet för känsliga personuppgifter

Utgångspunkter för Datainspektionens bedömning
Den personuppgiftsansvarige ska, enligt 31 § första stycket personuppgiftslagen, 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, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur pass känsliga de behandlade personuppgifterna är.

Enligt förarbetena till 31 § personuppgiftslagen ska paragrafen ha samma innebörd som artikel 17.1 och 17.2 i EG-direktivet (95/46/EG), se s. 136 i prop. 1997/98:44. Första stycket i artikel 17.1 talar om vad säkerhetsåtgärderna ska åstadkomma. Åtgärderna ska skydda personuppgifter 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.

Datainspektionens bedömning
Överföring av personuppgifter via ett öppet nät, till exempel internet, innebär särskilda risker för att uppgifterna förstörs, ändras eller förvanskas och för obehörig åtkomst. Ett öppet nät karaktäriseras av att fler än den personuppgiftsansvarige kan ta del av uppgifter som kommuniceras i nätet eller nå resurser som är tillgängliga via det. Mot denna bakgrund anser

Datainspektionen 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 (jämför Kammarrättens i Stockholm dom 2013-03-06 i mål nr. 2415-12 som gällde utlämnande över öppet nät av uppgifter av känslig natur).

De personuppgifter som behandlas i registret LifeGene är känsliga enligt definitionen i 13 § personuppgiftslagen och särregleras genom den i det här ärendet aktuella lagen och tillhörande förordning. Uppgifterna i LifeGene omfattas även av sekretess. Karolinska institutets elektroniska utlämnande av personuppgifterna i registret LifeGene via webbplatsen www.lifegene.se sker över ett öppet nät. För tillgång till personuppgifter om sig själva i registret LifeGene har deltagarna endast autentiserats med användarnamn och lösenord. Lösenorden har dessutom skickats till deltagarna med oskyddad e-post, vilket avsevärt ökar risken för otillåten spridning av och otillåten tillgång till uppgifterna.

Datainspektionen konstaterar således att Karolinska institutet förutom att medge en olaglig direktåtkomst till uppgifter i registret LifeGene även brister i skyddet av uppgifterna genom att i strid med kraven på lämpliga säkerhetsåtgärder i 31 § personuppgiftslagen lämnar ut känsliga personuppgifter över öppet nät efter inloggning med endast användarnamn och lösenord.

Datainspektionen anser därför att Karolinska institutet måste upphöra att medge åtkomst till känsliga personuppgifter i registret LifeGene över öppet nät efter autentisering med enbart användarnamn och lösenord.

I samband med att Datainspektionen inledde tillsyn i mars 2014 uppmärksammade Karolinska institutet på egen hand behovet av stark autentisering. Trots det ligger känsliga personuppgifter i registret LifeGene fortfarande åtkomliga via internet efter autentisering med endast användarnamn och lösenord och har gjort så under ärendets hela handläggning. Det innebär en stor risk för att känsliga personuppgifter ska komma i orätta händer. Särskilt som lösenorden för åtkomsten skickats till deltagarna med oskyddad e-post.

Beslutet ska därför, i den här delen, gälla även om det överklagas, se 51 § andra stycket personuppgiftslagen.

Samtycke och information

Utgångspunkter för Datainspektionens bedömning
I lagens 5-8 §§ finns detaljerade bestämmelser om *ändamålen* för vilka personuppgifter får behandlas i de register som omfattas av lagen.

Av 14 § i lagen framgår att personuppgifter inte får samlas in, i syfte att de ska registreras i ett register som förs enligt denna lag, utan att den som uppgifterna avser uttryckligen har samtyckt till att personuppgifter behandlas. Innan en person lämnar sitt samtycke ska han eller hon ha informerats bland annat om för vilka *ändamål* behandling kan ske och vilka uppgifter som får registreras, de *sekretess- och säkerhetsbestämmelser* som gäller för registret och *hur länge* uppgifterna sparas.

I propositionen framgår bland annat följande (s. 52).

> *”Den enskilde måste få tillräckligt mycket information för att kunna avgöra vilka integritetsrisker som är förknippade med att lämna eller på annat sätt medverka till uppgifter i syfte att uppgifterna ska registreras i ett register som förs enligt den föreslagna lagen, så att den enskilde kan avgöra om denne vill medverka eller inte.”*
>
> *”Den enskilde ska vidare informeras om att endast sådana uppgifter som inte är direkt hänförliga till den enskilde kommer att lämnas ut till sådana forskningsprojekt, men att uppgifterna kan vara försedda med löpnummer i syfte att uppgifterna ska kunna uppdateras inom ramen för ett forskningsprojekt. Den enskilde ska även informeras om att en s.k. kodnyckel […] kan komma att lämnas ut till andra registerförande myndigheter i syfte att dessa ska kunna lämna uppgifter om samma personer till sådana etikgodkända forskningsprojekt som har fått uppgifter från nu aktuellt register, i syfte att uppgifterna från de olika registren ska kunna sambearbetas i forskningsprojekten.*

Karolinska institutet har i sitt yttrande svarat följande på frågan om hur Karolinska institutet beaktat kraven på information och samtycke i lagens 14 §.

”Det mejl som skickades ut den 20 december [2013] skickades ut till redan registrerade deltagare i LifeGene. Dessa har redan erhållit och inhämtat information och samtyckt i samband med att de valde att delta i studien. I det informationsmaterialet finns information enligt 14 § [lagen], se bilaga 1. Informationsmaterialet finns även på nätet. För de deltagare som tidigare besökt Testcenter för bastest finns även skriftligt samtycke inhämtat. Se bilaga 2. De som spontant, utan separat inbjudan, väljer att registrera sig i LifeGene gör detta på www.lifegene.se där all information i enlighet med 14 § [lagen] finns tillgänglig för deltagaren. Se bilaga 3.”

Av informationsbroschyren om LifeGene (bilaga 1 till yttrandet) framgår, som Datainspektionen uppfattar det, avseende *ändamålet* med behandlingen bland annat att LifeGene är ett forskningsprojekt och en studie som ämnar skapa underlag för olika forskningsprojekt och att målet är att skapa nya verktyg för att förebygga, diagnostisera och behandla sjukdomar som exempelvis allergier, depression, infektioner, hjärt- och kärlsjukdom och cancer. Vidare framgår att det är viktigt att känna till förekomsten av vanliga hälsoproblem för att kunna studera hälsoutvecklingen och kunna finna viktiga samband som kommer studeras kring hur arv, miljö och livsstil påverkar vår nutida och framtida hälsa. Därefter exemplifieras det med ett antal tänkbara forskningsfrågeställningar.

De *sekretess- och säkerhetsbestämmelser* som gäller för uppgifter i registret LifeGene framgår av samma informationsbroschyr enligt följande.

”Dina personuppgifter kommer att behandlas i enlighet med offentlighets- och sekretesslagen (2009:400) och med starka säkerhetsrutiner för att bevara din anonymitet. Information som kan användas för att identifiera dig [...] hålls alltid åtskild från andra data om dig[...]. Även dina svar och dina resultat kommer att behandlas utifrån offentlighets- och sekretesslagen vilket innebär att inga obehöriga kan ta del av dem. De blod- och urinprover du lämnar förses med en unik kod så att de inte kan identifieras av obehöriga. Alla som arbetar med LifeGene har tystnadsplikt.”

I samma informationsbroschyr (bilaga 1 till yttrandet), finns flera referenser som innebär att personuppgifter kommer att behandlas ”under lång tid”, men inget närmare om *hur länge* uppgifterna får sparas.

I bilaga 2 till yttrandet, blanketten Informerat samtycke, finns information om att deltagande är frivilligt, att Karolinska institutet är personuppgiftsansvarig och om rätten till skadestånd och att få uppgifter utplånade. I övrigt hänvisas till ”den information jag tagit del av”.

I bilaga 3 till yttrandet, Samtyckesinformation, framgår, som Datainspektionen uppfattar det, avseende *ändamålet* med registret LifeGene att *”vi samlar in uppgifter för framtida forskning. Alla forskare som får ta del av uppgifter från LifeGene behöver ett etikgodkännande och ett godkännande från LifeGene”*.

Angående de *sekretess- och säkerhetsbestämmelser* som gäller står i bilaga 3 till yttrandet följande.

> *”Att deltagarnas personuppgifter, som personnummer, namn och adresser, samt information om deras hälsa, arv och levnadsvanor lagras på ett säkert sätt. Vid framtida forskning är all information som forskaren tar del av kodad vilket innebär att informationen inte direkt kan knytas till en individ. Alla som arbetar, praktiserar eller har uppdrag inom LifeGene har tystnadsplikt. Sekretess och tystnadsplikt gäller alla muntliga och skriftliga deltagaruppgifter, oavsett om de finns på papper, i en dator eller på annat sätt”.*

I bilaga 3 till yttrandet står också att *”dina personuppgifter kommer att sparas i 30 år”*.

Personuppgifter som behandlas enligt lagen får inte samlas in utan att deltagaren uttryckligen har lämnat sitt samtycke (14 § lagen). Enligt 3 § personuppgiftslagen avses med samtycke varje slag av frivillig, särskild och otvetydig viljeyttring genom vilken den registrerade, efter att ha fått information, godtar behandling av personuppgifter som rör honom eller henne. I förhållande till den definitionen har det i 14 § lagen preciserats dels vad den registrerades frivilliga och särskiljda viljeyttring ska avse (behandling av personuppgifter i enlighet med lagen), dels att den registrerades otvetydiga viljeyttring ska vara uttrycklig (propositionen s. 84). Kravet på utrycklighet innebär att viljeyttringen ska lämnas på ett tydligt iakttagbart sätt som inte lämnar något utrymme för tvekan om innebörden i samtycket.

Datainspektionens bedömning
Att korrekt information enligt 14 § andra stycket i lagen har lämnats innan samtycke inhämtas är en rättslig förutsättning för att samtycket ska vara giltigt och därmed att behandlingen av personuppgifter i registret LifeGene ska vara laglig.

Vad gäller den information som Karolinska institutet gett in i ärendet avseende *ändamålen* för vilka personuppgifterna kan behandlas saknas en tydlig koppling till ändamålsbestämmelserna i lagen. Det informeras till exempel om *att* uppgifterna kodas så att de inte kan identifieras av obehöriga, men inte att kodnyckeln under vissa förutsättningar kan komma att lämnas ut, jämför s. 52 i propositionen.

Att enbart hänvisa till offentlighets- och sekretesslagen, att informera om *att* det finns en tystnadsplikt och att uppgifterna omfattas av ”starka säkerhetsrutiner” eller att de behandlas ”på ett korrekt och säkert sätt” är inte tillräckligt för att uppfylla kravet på information om *de sekretess- och säkerhetsbestämmelser* som gäller för uppgifterna i registret.

För att uppfylla informationsplikten om *hur länge* uppgifterna sparas räcker det med att upplysa om innebörden av den gallringsbestämmelse som lagen innehåller (se propositionen s. 53 och 12 § lagen). Att enbart hänvisa till att uppgifterna sparas ”under lång tid” kan inte anses tillräckligt. Endast i samtyckesinformationen (bilaga 3 till yttrandet), som enligt Karolinska institutets yttrande delges de som spontant väljer att registrera sig i LifeGene, finns en närmare tidsangivelse.

Datainspektionen konstaterar således att det finns brister i det i ärendet ingivna informationsmaterialet. Det gäller särskilt de ingivna bilagorna 1 och 2. Dessutom har de deltagare som registrerats innan lagen trädde ikraft inte nåtts av fullständig information eller kunnat lämna sitt samtycke enligt 14 § i lagen.

Datainspektionen konstaterade i beslut i ärende 766-2011 den 19 december 2011 att personuppgiftslagens krav samt avsaknaden av en särreglering utgjorde hinder för att inom projektet LifeGene skapa en databas av detta slag. Det ledde till att särreglering infördes i form av den nu gällande tillfälliga lagen och därtill hörande förordning. Lagen är tydlig med att information ska ha lämnats och samtycke ska inhämtats innan registrering i registret påbörjas.

Lagen, som trädde ikraft den 1 december 2013, saknar övergångsbestämmelser eller andra hänvisningar till vad som ska gälla för de personuppgifter som samlades in före lagens ikraftträdande. Datainspektionen konstaterar att avsikten med den tillfälliga lagen är att, under de begränsningar som lagen innehåller, tillåta behandling av personuppgifter i registret LifeGene. Datainspektionen gör därför bedömningen att bristen på information och uttryckligt samtycke avseende tidigare insamlade personuppgifter kan åtgärdas genom att nu ge deltagare som registrerats i registret LifeGene före lagens ikraftträdande korrekt och fullständig information enligt 14 § i lagen och därefter inhämta ett uttryckligt samtycke från dessa.

Karolinska institutet måste därför uppdatera informationen till deltagarna, delge de deltagare som registrerats före lagens ikraftträdande den nya informationen och inhämta ett uttryckligt samtycke från dessa.

Datainspektionen förutsätter att Karolinska institutet tar fram rutiner för att i registret LifeGene gallra uppgifter om de deltagare som, efter att ha tagit del av den uppdaterade informationen inte lämnar ett giltigt samtycke till behandlingen av 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 beslutet meddelades för att kunna prövas. 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 generaldirektören Kristina Svahn Starrsjö efter föredragning av IT-säkerhetsspecialisten Magnus Bergström. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom och enhetschefen Katarina Tullstedt deltagit.

Kristina Svahn Starrsjö

Magnus Bergström