Datainspektionen

Beslut
2017-04-21

Diarienr
2276-2016

Ert diarienr
2016/05877

E-hälsomyndigheten
Sankt Eriksgatan 117
113 43 Stockholm

Tillsyn enligt personuppgiftslagen (1998:204) - E-Hälsomyndighetens tjänst Hälsa För Mig

Datainspektionens beslut

Datainspektionen konstaterar att E-hälsomyndigheten inte beaktat att myndighetens personuppgiftsansvar avser all behandling av personuppgifter i tjänsten Hälsa För Mig i enlighet med 3 § personuppgiftslagen (1998:204). Det finns därmed risk för att E-hälsomyndigheten inte kommer att uppfylla sitt personuppgiftsansvar och att E-hälsomyndigheten ger fel information till de registrerade gällande personuppgiftsansvaret.

> Datainspektionen förelägger E-hälsomyndigheten att analysera sitt personuppgiftsansvar och innan personuppgifter behandlas i tjänsten Hälsa För Mig se till att nödvändiga åtgärder vidtagits så att E-hälsomyndigheten kan ta ansvar för att den behandling av personuppgifter som kommer att ske i tjänsten. E-hälsomyndigheten måste också se till att informationen till de registrerade gällande personuppgiftsansvaret är korrekt.

Datainspektionen konstaterar att E-hälsomyndigheten i tjänsten Hälsa För Mig kan komma att behandla personuppgifter i strid med 10 och 13 § personuppgiftslagen genom att inte ha ett rättsligt stöd för behandlingen av personuppgifter och genom att vid behandling av känsliga personuppgifter inte ha ett giltigt undantag från förbudet mot att behandla dessa.

> Datainspektionen förelägger E-hälsomyndigheten att, innan personuppgifter behandlas i tjänsten Hälsa För Mig, se till att det finns rättsligt stöd för behandlingen och om det är frågan om känsliga personuppgifter att det finns ett giltigt undantag från förbudet mot att behandla känsliga personuppgifter. Vid bedömningen ska beaktas kravet på samtycke, dvs. att samtycke ska vara en frivillig, särskild och otvetydig viljeyttring som den

registrerade personligen ger efter att ha fått information om den behandling som samtycket omfattar.

Datainspektionen konstaterar att E-hälsomyndigheten i tjänsten Hälsa För Mig kan komma att behandla personuppgifter i strid med 40 kap 5 § offentlighets- och sekretesslagen (2009:400) som anger att sekretess föreligger för personuppgifterna och 9 § personuppgiftslagen jämfört med 3 § förordningen (2013:1031) med instruktion för E-hälsomyndigheten som anger att E-hälsomyndigheten endast får behandla uppgifterna i tjänsten för teknisk lagring för den enskildes räkning. 9 § personuppgiftslagen stadgar att den personuppgiftsansvarige ansvarar för att behandlingen som sker är laglig och korrekt, att behandlingen sker bara för berättigade ändamål och att fler uppgifter inte behandlas än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

Datainspektionen förelägger E-hälsomyndigheten att se till att personuppgifterna på den enskildes konto inte röjs i strid med sekretessen.

Datainspektionen förelägger E-hälsomyndigheten att inte ge tillgång till personuppgifterna i Hälsa För Mig till andra än den enskilde kontoinnehavaren och de applikationsleverantörer som tillhandahåller applikationer i syfte att visa eller tillföra uppgifter till den enskildes konto.

Datainspektionen förelägger E-hälsomyndigheten att se till att inte andra uppgifter behandlas av applikationsleverantörerna än de som den enskilde kontoinnehavaren anvisat och att personuppgifterna inte behandlas för annat syfte än att visa eller tillföra uppgifter till den enskildes konto.

Datainspektionen konstaterar att E-hälsomyndigheten i prenumerationstjänsterna som ska överföra personuppgifter från vårdgivare, läkemedelsförteckningen och receptregistret kan komma att behandla personuppgifter i strid med 9 § personuppgiftslagen jämfört med 25 kap. 1 och 17 a §§ offentlighets- och sekretesslagen genom att E-hälsomyndigheten inte utformat prenumerationstjänsterna så att myndigheten tillsett att personuppgifterna bara behandlas på ett lagligt och korrekt sätt och inte i strid med bestämmelserna om sekretess. Datainspektionen konstaterar även

att det finns risk för att E-hälsomyndigheten kan komma att behandla personuppgifterna utan rättsligt stöd och utan att det finns ett giltigt undantag mot förbudet mot att behandla känsliga personuppgifter.

> Datainspektionen förelägger E-hälsomyndigheten att enbart behandla personuppgifter i en prenumerationstjänst om behandlingen som sker är laglig och korrekt och inte i strid med bestämmelserna om sekretess till skydd för den enskilde. E-hälsomyndigheten måste också se till att det finns rättsligt stöd för behandlingen och om det är frågan om känsliga personuppgifter att det finns ett giltigt undantag från förbudet mot att behandla känsliga personuppgifter.

Datainspektionen förutsätter att E-hälsomyndigheten i sina överväganden även beaktar EU:s dataskyddsförordning så att tjänsten Hälsa För Mig kommer att vara möjlig att nyttja även efter maj 2018.

Sammanfattning

E-hälsomyndigheten (EHM) har av regeringen fått i uppdrag att inrätta en tjänst för personliga hälsokonton (Konto). Tjänsten som har namnet Hälsa För Mig (Tjänsten) har ännu inte driftsatts. Hälsokontot ska kunna utgöra en lagringsplats för den enskildes samlade hälsouppgifter. Personuppgifter ska kunna tillföras både av den enskilde kontohavaren (Användaren) själv, genom applikationer som ansluts till Kontot och via prenumerationstjänster som överför uppgifter från vårdgivare och EHM:s egna register. Datainspektionen konstaterar att Hälsa För Mig kan komma att innehålla en stor del av Sveriges befolknings hälsouppgifter och bli en mycket stor samling känsliga personuppgifter. Avsikten är att fler än Användaren ska kunna få del av uppgifterna. Det kommer enligt EHM ske bland annat via applikationer som företag, organisationer, myndigheter eller andra som EHM tecknar avtal med kan ansluta till Tjänsten. Användaren kan också dela sitt Konto med andra kontoinnehavare. Det sammantagna resultatet blir att hälsouppgifter kan komma att löpande tillföras den enskildes Konto via prenumerationstjänsten och olika intressenter kan, med stöd av samtycke, sedan komma att ta del av dessa uppgifter. Det ska kunna ske även om Användaren inte själv har tagit del av uppgifterna. Känsliga personuppgifter kan därigenom riskera att få en oöverblickbar spridning.

EHM:s möjlighet att behandla personuppgifterna utgår från det uppdrag myndigheten har dvs. att tillhandahålla en lagringsplats för den enskildes hälsouppgifter. Enligt 2 kap. 10 § tryckfrihetsförordningen utgör handlingar i sådana utrymmen inte allmänna handlingar och EHM får inte för något annat syfte behandla uppgifterna utom för att lagra enskildas hälsouppgifter. EHM ska också enligt sin instruktion ge tredje part möjlighet att ansluta tillämpningar och tjänster till den elektroniska tjänsten. Eftersom Tjänstens syfte är att Användaren ska ha en yta för att hantera sina hälsouppgifter är det bara Användarens behov av olika funktioner för att behandla sina hälsouppgifter som tredje parternas anslutning kan avse. Om EHM lämnar eller ger tillgång till personuppgifter till tredje part för att tillgodose den tredje partens behov är det en behandling som inte är berättigad utifrån ändamålet och en behandling som går utöver att enbart lagra uppgifterna. Det är också i strid mot den sekretess som råder för uppgifterna. Datainspektionen konstaterar således att EHM inte kan ge tredje part möjlighet att för eget behov använda personuppgifterna i Tjänsten. Applikationsleverantörerna kan däremot, utifrån Användarens önskemål, bidra med uppgifter till Kontot och om Användaren väljer att använda en applikation kan Applikationsleverantören behandla uppgifterna för att visa uppgifterna i applikationen för Användaren.

EHM får således inte behandla uppgifterna i Tjänsten för egen del. Det är emellertid EHM som bestämt ändamål och medel med Tjänsten och som därmed är personuppgiftsansvarig för den behandling av personuppgifter som sker i Hälsa För Mig. EHM måste därför tillse att personuppgifterna inte används på något annat sätt än vad som är tillåtet. EHM har därmed också ett ansvar för att Applikationsleverantören bara får del av de uppgifter som behövs för den aktuella applikationen och att övriga personuppgifter skyddas från obehörig åtkomst och spridning. Det är också utifrån reglerna om sekretess enbart de uppgifter Användaren anger att de ska tillföra till applikationen som kan göras tillgängliga för Applikationsleverantören.

Om många väljer att använda Tjänsten kan Hälsa För Mig bli en mycket stor samling känsliga personuppgifter. Det kan ur olika aspekter ifrågasättas om inte en sådan stor samling känsliga personuppgifter behöver lagregleras. Om en vidare behandling än att ge den enskilde en lagringsplats för sina önskas så är det något som, enligt Datainspektionen, behöver lagregleras. I

sammanhanget bör också noteras att behovet av nationell reglering också kommer att påverkas av EU:s dataskyddsförordning.

Redogörelse för tillsynsärendet

Tillsynens omfattning
EHM har enligt sin instruktion i uppdrag att inrätta en tjänst för personliga hälsokonton - Hälsa För Mig. Datainspektionen har den 30 november 2016 inlett tillsyn mot EHM i syfte att utröna lagligheten vad gäller behandling av personuppgifter i Hälsa För Mig.

EHM har den 22 december 2016 inkommit med svar på Datainspektionens tillsynsfrågor och i samband därmed har EHM uppgett att eftersom Tjänsten inte är klar så är ett flertal funktioner och aspekter av såväl juridisk som säkerhetsmässig karaktär fortfarande under utarbetning. EHM har till svaret också bifogat bilagor bestående av utkast till användarvillkor inklusive hantering av personuppgifter, utkast till avtal Hälsa för mig Applikationsleverantör med bilaga Allmänna villkor Applikationsleverantörer.

Med hänsyn till att Tjänsten inte är i drift omfattar detta tillsynsbeslut enbart mer övergripande rättsliga aspekter gällande dataskydd. Datainspektionen har i denna tillsyn inte granskat säkerheten och inte frågor gällande användning av personuppgiftsbiträde.

Skäl för beslutet

Tillhandahållande av ett personligt hälsokonto

Bakgrund
Av 3 § första stycket i förordningen (2013:1031) med instruktion för E-hälsomyndigheten framgår följande:

> *Myndigheten ska tillhandahålla en elektronisk tjänst som ger enskilda personer möjlighet att i ett personligt hälsokonto kostnadsfritt lagra uppgifter om sin hälsa. Handlingar i ett personligt hälsokonto får endast förvaras hos myndigheten i form av teknisk lagring för enskilds räkning.*

EHM har uppgett att myndigheten kommer att erbjuda Hälsa För Mig till alla över 18 år som är svenska medborgare eller är folkbokförda i Sverige. Användaren måste ha en svensk e-legitimation för att kunna använda Tjänsten. Hälsa För Mig kommer enligt EHM att utgöra ett verktyg där Användaren kan samla, överblicka, lagra, dela och i övrigt administrera information om sin hälsa. Exempel på information som kan lagras i det personliga hälsokontot är t.ex. vikt, blodtryck, läkemedelsinformation och vaccinationer. Tjänsten kommer att öppnas tidigast under våren 2017. Den kommer då att ha ett begränsat antal funktioner och kommer stegvis att byggas ut. Det är frivilligt att använda Tjänsten.

EHM uppger att all information på Kontot kommer att ”ägas” av Användaren. EHM tar inte del av uppgifterna och använder dem inte för egen del.

Uppgifterna på Kontot kommer att samlas in av Användaren själv. Antingen genom att Användaren på egen hand lägger in uppgifterna i Kontots fritextfält eller ansluter sig till applikationer som information kan samlas in från. Användaren kan också välja att ansluta sig till en prenumerationstjänst (Prenumerationstjänsten) för att genom den kunna ”prenumerera” på uppgifter om sig själv från sin journal. Prenumerationstjänsten bygger på ett avtal mellan EHM och Inera. Inera kommer i sin tur att ha avtal med de vårdgivare som väljer att tillhandahålla tjänster inom ramen för Prenumerationstjänsten. Vårdgivaren beslutar om ett utlämnade i det enskilda fallet är möjligt enligt de regler som styr vårdgivarens verksamhet.

Vårdnadshavare kan samla information om sitt barn och vårdnadshavare kan prenumerera på uppgifter via Prenumerationstjänsten för sina barn om de är under 12 år. Även uppgifter om andra än Användaren själv och användarens barn kan komma att behandlas i Användarens Konto. Det kan t.ex. vara uppgift om läkare vars namn finns i inhämtade journaluppgifter. Det kan också vara uppgifter om anhöriga som Användaren själv infogar. EHM bedömer däremot det inte som troligt att vårdgivaren kommer lämna ut uppgifter om annan tredje part än om vårdpersonal eftersom uppgifter om andra förmodligen är belagda med sekretess hos vårdgivaren.

EHM har uppgett att EHM även kommer att erbjuda en möjlighet för Användaren att prenumerera på sin information från olika register hos EHM. I ett första steg från läkemedelsförteckningen med stöd av 7 § lagen (2005:258)

om läkemedelsförteckning och senare också från receptregistret med stöd av 11 § tredje stycket lagen (1996:1156) om receptregister.

Personuppgiftsansvar
Den personuppgiftsbehandling som EHM planerar att utföra regleras i personuppgiftslagen (1998:204).

Enligt 3 § personuppgiftslagen är den som ensam eller tillsammans med andra bestämmer ändamål och medel med behandlingen av personuppgifter personuppgiftsansvarig för behandlingen. Personuppgiftsansvarig kan också pekas ut i lag eller förordning.

Datainspektionen delar EHM:s uppfattning att EHM är personuppgiftsansvarig för behandlingen av personuppgifter i Hälsa För Mig. EHM har som myndighet fått i uppdrag att tillhandahålla en hälsotjänst för allmänheten. Ändamålet med tjänsten härrör från EHM:s instruktion och det är EHM som skapar medlet dvs. Tjänsten för att behandla uppgifterna. För de behandlingar av personuppgifter som en Användare utför i sitt Konto bestämmer EHM den yttre ramen för behandlingen, dvs. vad Tjänsten ska användas till, vad som är möjligt att utföra och hur det kan ske. Det betyder att det är EHM som bestämmer ändamål och medel för Tjänsten. Det inkluderar även de behandlingar som Användaren kan välja att göra och som sker på Användarens Konto.

Det är enligt EHM patienten som ”äger” personuppgifterna och som avgör vad som ska ske med dem. EHM har utifrån det resonemanget, enligt Datainspektionen, kommit att betrakta sitt personuppgiftsansvar som mer begränsat än vad det är. Dataskyddsreglerna handlar inte om ”ägandeskap” utan ansvaret finns hos den personuppgiftsansvarige och det kvarstår även om den registrerade samtycker till en behandling eller t.o.m. väljer själv att den ska ske. Användaren skulle också kunna ha ett ansvar för en sådan behandling, men enskilda fysiska personer som för privat bruk behandlar personuppgifter om andra omfattas inte av dataskyddsreglerna enligt 6 § personuppgiftslagen. Det s.k. privatundantaget kan inte åberopas av juridiska personer.

Prenumerationstjänsten har inrättats för att Tjänsten ska kunna få information överförd från vårdgivarna till Användarnas Konton. Prenumerationstjänsten är således en funktion för att Tjänsten ska fungera i

enlighet med EHM:s uppdrag. Vårdgivaren är enligt 2 kap. 6 § patientdatalagen (2008:355) personuppgiftsansvarig för de personuppgifter som behandlas inom hälso- och sjukvården. Vårdgivaren ansvarar således för att behandlingen av personuppgifterna är korrekt och lagenlig när uppgifterna överförs till Inera i syfte att de ska föras in på Användarens Konto. Det innebär emellertid inte att EHM inte har något ansvar. Enligt Högsta Förvaltningsdomstolens dom den 22 juni 2012 (mål 4453-10) som avsåg en elektronisk anmälan av tillfällig föräldrapenning via sms till Försäkringskassan och arbetsgivares anmälan av sjukfall via en s.k. Infratjänst, kan ett personuppgiftsansvar inledas innan uppgifterna kommit den ansvarige till del om denne bestämt ändamål och medel även för den initiala personuppgiftsbehandlingen. Vid en jämförelse kan konstateras att Prenumerationstjänsten är inrättad för att överföra hälsouppgifter till Tjänsten. Det är således EHM:s Tjänst som ska ha uppgifterna och EHM som utformat Prenumerationstjänsten. EHM har bestämt ändamål och medel och har därför ett personuppgiftsansvar även för Prenumerationstjänsten. Det hindrar emellertid inte att vårdgivare och Inera också är personuppgiftsansvariga för den behandling som de utför. För de behandlingar som sker hos annan och inte i EHM:s Tjänst eller verksamhet sträcker sig EHM:s personuppgiftsansvar, i enlighet med Högsta Förvaltningsrättens dom, till det som EHM kan råda över.

Grundläggande krav

Av 9 § första stycket personuppgiftslagen framgår de s.k. grundläggande kraven som gäller för behandling av personuppgifter. Kraven anger att behandlingen av personuppgifter ska vara laglig, korrekt och ske i enlighet med god sed. Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Uppgifterna får inte behandlas för något ändamål som är oförenligt med det ändamål för vilket personuppgifterna samlades in. De personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen, riktiga och om nödvändigt aktuella. Fler personuppgifter får inte behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Åtgärder ska vidtas för att rätta, blockera eller utplåna personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen och personuppgifter får inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Dessa grundläggande krav ska en personuppgiftsansvarig följa oavsett vilket rättsligt stöd behandlingen grundar sig på. Det innebär att dessa bestämmelser måste beaktas även om den registrerade samtyckt till behandlingen. EHM har överhuvudtaget inte fört några resonemang gällande de grundläggande kraven.

Rättsligt stöd
Den som behandlar personuppgifter måste också ha ett rättsligt stöd för behandlingen i tillämplig dataskyddslagstiftning. EHM har uppgett att det rättsliga stödet för behandling av personuppgifter i Tjänsten utgörs av Användarens samtycke.

Samtycke från den registrerade kan utgöra ett rättsligt stöd enligt 10 § personuppgiftslagen. Samtycke är enligt definitionen i 3 § personuppgiftslagen, 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. Samtycke är således individuellt och kan inte lämnas för andra. Beträffande barn är emellertid vårdnadshavarna legala ställföreträdare och har både rätt och skyldighet att företräda sitt barn i allehanda spörsmål, däribland inbegripet att bestämma i frågor som rör barnets personliga förhållanden (se 6 kap. 11 och 13 §§ föräldrabalken (1949:381)). När barnet blir äldre ska också barnets uppfattning beaktas.

Det räcker inte för kravet på frivillighet att det inte föreligger något tvång. Det måste vara frågan om en äkta valmöjlighet och samtycket ska utan problem gå att återkalla, se 12 § personuppgiftslagen. Att samtycket ska vara särskilt är sammankopplat med kravet på information. Den tänkta behandlingen ska vara tillräckligt preciserad så att den registrerade förstår vad samtycket omfattar.

Prenumerationstjänsten stödjer sig på Användarens samtycke. För att det ska vara möjligt krävs att samtycket inte är alltför generellt utan att Användaren kan förutse vilka uppgifter som kommer att behandlas och hur. Eftersom det är svårt att förutse vilka sjukdomar och hälsoproblem som en enskild person råkar ut för kan samtycket riskera att avse ett alltför ospecificerat område, jämför nedan gällande sekretess.

EHM har uppgett att beträffande personuppgifter som rör andra än Användaren utgörs det rättsliga stödet av intresseavvägning, enligt 10 § punkten f personuppgiftslagen. Någon intresseavvägning har emellertid inte presenterats.

Känsliga personuppgifter
Känsliga personuppgifter t.ex. personuppgifter om hälsa och sexualliv (13 § personuppgiftslagen) är förbjudna att behandla om behandlingen inte omfattas av ett undantag från förbudet (se 14-20 §§ personuppgiftslagen). Ett undantag från förbudet att behandla känsliga personuppgifter är, enligt 15 § personuppgiftslagen, den registrerades uttryckliga samtycke till behandlingen. Behandling av känsliga personuppgifter kan inte stödjas på en intresseavvägning, vilket innebär att EHM inte angett något undantag som medger behandling av känsliga personuppgifter om andra registrerade än Användaren.

Aktuella registerförfattningar
Hälsouppgifter som behandlas i offentlig eller offentlig finansierad verksamhet regleras i stor utsträckning av lag exempelvis regleras behandlingen av journaluppgifter i patientdatalagen. Enligt 5 kap. 5 § patientdatalagen får den enskilde medges direktåtkomst till uppgifter om den enskilde själv. Läkemedelsförteckningen och receptregistret förs av EHM. Prenumerationen av dessa uppgifter måste också vara förenlig med vad som föreskrivs i dessa bestämmelser. EHM har som stöd för att ge den enskilde uppgifter om sig själv hänvisat till 7 § lagen (2005:258) om läkemedelsförteckning i vilken det anges att *förskrivare, legitimerad sjuksköterska utan behörighet att förskriva läkemedel och farmaceut får under de förutsättningar som anges i 3 § andra och tredje styckena ha direktåtkomst till uppgifter i läkemedelsförteckningen. Den registrerade får ha direktåtkomst till uppgifter om sig själv.* EHM har även hänvisat till 11 § lagen (1996:1156) om receptregister som anger vilka som får ha direktåtkomst till uppgifterna i receptregistret, enligt följande. *Expedierande personal på ett öppenvårdsapotek får ha direktåtkomst till receptregistret för de ändamål som anges i 6 § första stycket 1, 2 och 8. Den som har legitimation för yrke inom hälso- och sjukvården får ha direktåtkomst till uppgifter om dosrecept. Den enskilde får ha direktåtkomst till uppgifter om sig själv.*

Sekretess
Den enskildes integritet inom hälso- och sjukvården skyddas också av sekretess, eller om det är ett privatorgan, av regler om tystnadsplikt. Den som lämnar ut eller låter någon ta del av en sekretessbelagd handling måste se till att det inte sker i strid med bestämmelser i offentlighets- och sekretesslagen (2009:400). Regler om sekretess till skydd för den enskilde verkar integritetshöjande och utgör därför ett skydd även vad gäller behandling av personuppgifter, även om reglerna i sig inte utgör dataskyddsregler. En myndighet ska också beakta att sekretess gäller enligt 21 kap. 7 § offentlighets- och sekretesslagen om det kan antas att ett utlämnande skulle medföra att uppgifterna behandlas i strid med personuppgiftslagen.

Enligt 12 kap. 2 § offentlighets- och sekretesslagen kan en enskild helt eller delvis häva sekretess som gäller till skydd för honom eller henne, om inte annat anges i lagen. Av lagkommentaren framgår att ett samtycke kan ges i förväg, med tanke på kommande situation. Ett samtycke får dock inte ges ett så generellt innehåll att den enskilde allmänt förklarar sig avstå från sekretessen hos en viss myndighet eller tjänsteman (se Lenberg m.fl., Offentlighets- och sekretesslagen, 1 juli 2016, Zeteo, kommentaren till 12 kap.2 § första stycket). Justitiekanslern har också i ett beslut uttalat att det inte är i alla situationer - eller rent av inte någonsin - möjligt att inhämta ett relevant samtycke i förväg när det gäller en akut vårdsituation eller när en patient i ett annat fall ska genomgå en operation (Justitiekanslerns beslut 2014-11-10, dnr 6764-13-31 och 8146-13-31).

Enligt EHM utlämnas vårduppgifter genom Prenumerationstjänsten från vårdgivaren till Inera, som sedan lämnar uppgifterna till EHM. EHM har uppgett att Användarens samtycke bryter sekretessen hos vårdgivaren. Datainspektionen konstaterar att eftersom det inte är möjligt att ge ett samtycke i förväg för alla olika typer av vårdsituationer måste prenumerationen vara begränsad så att den bara omfattar uppgifter som det är möjligt att i förväg bryta sekretessen för. Beträffande uppgifter om andra än Användaren och som det råder sekretess för, har EHM uppgett att EHM utgår från att vårdgivaren inte lämnar ut dessa uppgifter. Såsom angetts ovan har EHM ett ansvar att se till att Prenumerationstjänsten är utformad så att de personuppgifter som behandlas i den och som överförs till EHM:s Tjänst behandlas på ett lagligt och korrekt sätt. Det kan lämpligen ske i överenskommelsen mellan EHM, Inera och vårdgivarna.

Datainspektionens bedömning avseende det personliga hälsokontot
EHM har uppgett att det rättsliga stödet för behandlingen av personuppgifter på Kontot är samtycke från Användaren. Såsom angetts gällande samtycke finns det krav på information och frivillighet för att samtycke ska vara giltigt. Det är EHM:s ansvar att se till att samtycket från Användaren är giltigt.

Beträffande uppgifter om andra än Användaren såsom exempelvis uppgifter om vårdpersonal som kan förekomma i journaler, har EHM angett att dessa behandlas med intresseavvägning. EHM har inte beskrivit denna intresseavvägning närmare, men det är EHM:s ansvar att utföra en intresseavvägning innan uppgifter om vårdpersonal behandlas.

Enligt EHM kan även uppgifter om anhöriga till Användaren komma att behandlas i Kontot och torde då, såsom Datainspektionen uppfattat det, behandlas med stöd av intresseavvägning. Eftersom Kontot är avsett för hälsouppgifter bör det vara frågan om känsliga personuppgifter. För att behandla känsliga personuppgifter räcker det inte att det finns ett rättsligt stöd utan det måste också finnas ett undantag från förbudet mot att behandla känsliga personuppgifter. EHM har inte angett att det föreligger något undantag från förbudet gällande andra än Användarna. Det är EHM:s ansvar att se till att inte någon olaglig behandling sker. EHM måste därför kunna åberopa något undantag från förbudet att behandla känsliga personuppgifter för att behandla hälsouppgifter. Det gäller såväl uppgifter som tillförs av Användaren själv som uppgifter som kommer via prenumerationstjänsten eller via en applikation.

Mot denna bakgrund ska EHM föreläggas att, innan personuppgifter behandlas i tjänsten Hälsa För Mig, se till att det finns rättsligt stöd för behandlingen och om det är frågan om känsliga personuppgifter att det finns ett giltigt undantag från förbudet mot att behandla känsliga personuppgifter. Föreläggandet avser alla registrerade dvs. Användare, vårdpersonal, anhöriga eller andra vars uppgifter behandlas.

Enligt EHM utlämnas vårduppgifter genom Prenumerationstjänsten från vårdgivaren till Inera som sedan lämnar uppgifterna till Tjänsten med stöd av samtycke. För att det ska vara en laglig behandling krävs det att det, för såväl utlämnande av sekretessbelagda uppgifter som för behandling av känsliga personuppgifter, föreligger giltigt samtycke. EHM har även ett ansvar för att det i Prenumerationstjänsten inte behandlas uppgifter i strid mot gällande

bestämmelser. EHM får bara behandla personuppgifter om behandlingen är laglig och korrekt. För att EHM:s behandling ska anses laglig och korrekt måste det vara tillåtet för vårdgivarna att utlämna uppgifterna till Inera och även tillåtet för Inera att behandla uppgifterna och lämna dem vidare till EHM.

Mot denna bakgrund ska EHM föreläggas att enbart behandla personuppgifter i Prenumerationstjänsten om behandlingen som sker är laglig och korrekt och inte i strid med bestämmelserna om sekretess till skydd för den enskilde. EHM måste också se till att det finns rättsligt stöd för behandlingen och om det är frågan om känsliga personuppgifter att det finns ett giltigt undantag från förbudet mot att behandla känsliga personuppgifter.

Tillgång till hälsokontot för andra än Användaren

Bakgrund
I avsnittet ovan har Användarens användning av Kontot och Prenumerationstjänsterna analyserats. I detta avsnitt granskas hur andra än Användaren kan erhålla tillgång till Kontot.

I EHM:s instruktion 3 § stycket anges följande.

> *Myndigheten ska ge tredje part möjlighet att ansluta tillämpningar och tjänster till den elektroniska tjänsten. Anslutning av tillämpningar får enbart göras med den enskildes uttryckliga samtycke.*

EHM har uppgett att Användaren kan välja att ge en annan Användare åtkomst till delar eller hela informationen på Användarens Konto. Rätten kan antingen avse enbart att ta del av uppgifter eller att både ta del av uppgifter och att skriva. Det finns också möjlighet för Användaren att ge ett fullt s.k. ägarskap varvid den som får ett sådant s.k. ägarskap tilldelat sig har samma rättigheter på Kontot som Användaren själv.

Användaren på Kontot kan ansluta sig till olika applikationer från tredjepartsleverantörer (Applikationsleverantörer). Det kan exempelvis vara applikationer som tillhandahålls på webbplatser eller i s.k. smartphones. Applikationerna erbjuder olika funktioner och enligt de allmänna villkoren för Applikationsleverantörer kan företag, organisationer, myndigheter eller annan teckna avtal med EHM och efter godkännande av EHM ansluta

applikationer till Tjänstens elektroniska plattform. EHM tar ut en avgift av Applikationsleverantören per applikation som ansluts till plattformen.

I de allmänna villkoren anges även att Applikationsleverantören ska teckna avtal med Användaren och tydligt informera användaren om hur Användarens personuppgifter kommer att behandlas om Användaren använder applikationen. Applikationsleverantören ska också, enligt villkoren, inhämta samtycke från Användaren för att få åtkomst till personuppgifter som Användaren lagrar på sitt Konto och för att använda dessa uppgifter i applikationen. Användaren ska kunna lämna samtycke till att Applikationsleverantören får kontinuerlig åtkomst till sådana personuppgifter som Användaren lagrar på sitt Konto. Ett sådant samtycke ska vara giltigt i max tre månader och därefter måste det förnyas. Applikationsleverantören får inte låta tredje man nyttja Tjänsten om det inte uttryckligen angivits i avtalet med EHM.

Beträffande personuppgiftsbehandlingen anges i de allmänna villkoren att Applikationsleverantören är personuppgiftsansvarig för behandlingen av de personuppgifter som inhämtas via Tjänsten. Applikationsleverantören erinras om att behandling av känsliga personuppgifter normalt sett förutsätter att ett uttryckligt samtycke inhämtas från Användaren och att personuppgifterna skyddas på ett säkert sätt. Applikationsleverantören ansvarar för att alla sådana åtgärder vidtas. Applikationsleverantören ska enligt villkoren också åta sig att inte sälja, överlåta, upplåta eller överföra personuppgifterna som inhämtas via Tjänsten till tredje man för något kommersiellt syfte. Vad som avses med kommersiellt syfte anges inte och inte heller nämns någon begränsning avseende överföring av personuppgifterna till tredje land.

Applikationsleverantören åtar sig vidare att endast använda personuppgifterna som inhämtas via Tjänsten för marknadsföringsändamål, om en Användare uttryckligen har samtyckt till detta.
Applikationsleverantören erinras även om att en Användare kan lagra personuppgifter om annan person på sitt konto Hälsa För Mig. Applikationsleverantören åtar sig att inte samla in, sammanställa eller på annat sätt behandla personuppgifter om sådan annan person som en Användare lagrar på sitt Konto för annat syfte än att visa uppgifterna i Applikationen för Användaren.

Det framgår också av användarvillkoren mellan EHM och Användaren att om Användaren eller den person som Användaren valt att ge s. k. ägarskap genom delningsfunktionen, ansluter en applikation till Användarens information och Användaren lämnat sitt uttryckliga samtycke till att personuppgifterna lämnas ut och används i applikationen, så kommer mottagaren av Användarens personuppgifter att vara personuppgiftsansvarig för den fortsatta behandlingen i applikationen.

Personuppgiftsansvar
EHM har uppgett att EHM är ensam personuppgiftsansvarig för behandlingen av uppgifterna i Tjänsten. Samtidigt anger EHM att myndigheten inte ansvarar för vilka hälsouppgifter en Applikationsleverantör tillför Användarens Konto eller vilka hälsouppgifter som lämnas till en Applikationsleverantör.

Personuppgiftsansvaret kan inte överlåtas eller avtalas bort. Den enskildes samtycke påverkar inte heller var personuppgiftsansvaret är placerat. Det är EHM som skapat Tjänsten, som avgör dess utformning, som avtalar med Applikationsleverantörerna om att de får tillgång till Tjänsten och under vilka villkor. Datainspektionen kan således konstatera att EHM är personuppgiftsansvarig för all behandling som sker i Tjänsten, även för att Applikationsleverantörernas tillgång till personuppgifterna och behandling av dem är laglig. Det hindrar inte att även Applikationsleverantörerna kan ha ett personuppgiftsansvar för den behandling de utför.

Eftersom EHM inte beaktat hela sitt personuppgiftsansvar finns det risk för att EHM inte kommer att uppfylla det till fullo. Den enskilde registrerade riskerar också att få en felaktig bild gällande personuppgiftsansvaret.

Mot denna bakgrund, se även vad som anförts i det tidigare avsnittet gällande personuppgiftsansvaret, ska EHM föreläggas att analysera sitt personuppgiftsansvar och innan personuppgifter behandlas i tjänsten Hälsa För Mig se till att nödvändiga åtgärder vidtagits så att EHM kan ta ansvar för den behandling av personuppgifter som kommer att ske i tjänsten. EHM måste också se till att informationen till de registrerade gällande personuppgiftsansvaret är korrekt.

Grundläggande krav
I den personuppgiftsansvariges ansvar ingår att tillse att de grundläggande kraven i 9 § personuppgiftslagen uppfylls. EHM har därför ett ansvar för att den behandling som sker är laglig och korrekt. Att en behandling är laglig och korrekt innebär till exempel att de som behandlar uppgifterna följer de regelverk som gäller för den aktuella behandlingen. En vårdgivare som ska ta del av uppgifter från en annan vårdgivare i en vårdprocess ska således följa reglerna om sammanhållen journalföring i 6 kap. patientdatalagen. En forskningshuvudman som enligt ett etikgodkännande får behandla journaluppgifter för forskning, förutsatt att patientens samtycker och att uppgifterna är kodade, kan således inte inhämta journaluppgifter genom Tjänsten istället.

Ett grundläggande krav är att personuppgiftsbehandlingen inte omfattar mer än vad som är nödvändigt utifrån ändamålet. Det innebär bland annat att EHM ska se till att ingen får del av överskottsinformation i Tjänsten, som denne inte har ett berättigat ändamål att behandla. EHM har inte angett om det finns funktioner för att avgränsa behandlingarna eller selektera uppgifterna, förutom att EHM ska markera fält där det troligen finns uppgifter om andra än Användaren och på så sätt guida Applikationsleverantören till en korrekt hantering enligt avtalet. Datainspektionen konstaterar att en sådan guidning inte tillräcklig för att uppfylla kraven på uppgiftsminimering, särskilt inte med tanke på att det är frågan om känsliga personuppgifter.

Utgångspunkten för vad som får behandlas är således vad som är nödvändigt utifrån ändamålet. Av EHM:s instruktion framgår att EHM ska tillhandahålla ett personligt hälsokonto där den enskilde kan lagra sina hälsouppgifter. Handlingarna får endast förvaras hos EHM i form av teknisk lagring för den enskildes räkning. Ändamålet är att tillgodose Användarens behov och EHM ska anordna en plats för dessa uppgifter. I det följande stycket i instruktionen anges att EHM ska ge tredje part möjlighet att ansluta tillämpningar och tjänster till den elektroniska tjänsten. Det anges också att anslutning av tillämpningar enbart får göras med den enskildes uttryckliga samtycke.

Datainspektionen konstaterar att det av instruktionen inte framgår att dessa tredje parter för egen del får behandla uppgifterna på Kontot, att de får inhämta uppgifter från Kontot, att de får vidarebefordra uppgifter frånK eller att de får behandla uppgifterna för något annat syfte än att skapa funktioner

för Användaren. Eftersom ändamålet är att EHM ska lagra uppgifterna åt Användaren och ge Användaren tillgång till vissa tjänster, ingår det inte i ändamålen att EHM disponerar uppgifterna genom att ge andra tillgång till dem för andra syften än att enbart skapa tillämpningar och tjänster som Användaren kan nyttja i Kontot. Det är således inte ett berättigat ändamål för EHM att behandla personuppgifter i Tjänsten i syfte att ge andra än Användaren tillgång till enskildas hälsouppgifter.

Rättsligt stöd
För Applikationsleverantörernas behandling av personuppgifter har EHM angett att det rättsliga stödet är samtycke. Personuppgifter som rör annan än Användaren ska enligt avtal mellan EHM och Applikationsleverantören inte behandlas för annat syfte än att visa uppgifterna i Applikationen för användaren. Vilket det rättsliga stödet för denna behandling är anges inte.

För att ett samtycke ska vara giltigt ställs stora krav både på dess utformning och att det är frivilligt. För att det ska vara frivilligt måste det föreligga en äkta valbarhet. En arbetsgivare kan därför som regel inte stödja sig på samtycke vad gäller behandling av arbetstagares personuppgifter. På samma sätt kan en skola sällan stödja sig på samtycke i förhållande till en elev. Även i en privat relation kan det råda en ojämlikhet som innebär att ett samtycke inte är frivilligt, till exempel kan en förälder eller partner ha ett osunt kontrollbehov och tvinga till sig insyn. Att det föreligger faktisk frivillighet i den enskilda situationen är avgörande för att det ska vara frågan om ett giltigt samtycke.

Ett giltigt samtycke kräver också, såsom nämnts ovan, att den registrerade får information och att den är tillräckligt preciserad så att den registrerade förstår vad samtycket omfattar.

Ett samtycke berättigar bara till behandling av personuppgifter om den som har lämnat samtycket och inte till behandling av uppgifter om någon annan. Användaren kan således inte samtycka till behandling av andras personuppgifter. Användaren kan inte heller ge någon annan rättighet, genom s.k. ägarskap, att agera å Användarens vägnar. Ett sådant ägarskap utgör inte ett samtycke i enlighet med dataskyddsreglerna utan handlar om en överlåtelse av rättigheter. En sådan överlåtelse av rätten till integritet vid behandling av personuppgifter är inte möjlig. Datainspektionen anser att det är viktigt att EHM för alla former av samtycke analyserar de legala

förutsättningarna och ser till att aktuella samtycken utformas så att de uppfyller de rättsliga kraven.

Beträffande utrymmen som är till för den enskilde är det som tidigare konstaterats Användarens behov som ska tillgodoses och den behandling som ska ske där ska således ske på Användarens initiativ, varför det i det sammanhanget inte är frågan om samtycke i vanlig mening.

Vad gäller de personer som Användarna kan dela Konto med anges att det ska vara privatpersoner som själva har Konton i Tjänsten. Om dessa privatpersoner också måste ha en privat relation till Användaren eller om den kan vara yrkesmässig framgår inte. Är det en yrkesmässig behandling finns det givetvis samma krav på rättsligt stöd för att behandla personuppgifterna som i övrigt.

Känsliga personuppgifter
Behandling av känsliga personuppgifter är som redan tidigare nämnts enbart tillåtet om det föreligger ett undantag från förbjudet att behandla dessa. Samtycke kan utgöra ett undantag från förbudet, men samtycket ska då ges uttryckligen. Det finns också krav på starkare skydd för att få behandla känsliga personuppgifter.

Eftersom EHM inte anser sig vara personuppgiftsansvarig för den behandling som sker av Applikationsleverantörerna så har EHM inte tagit ansvar för att den behandling som Applikationsleverantörerna kan komma att utföra följer dataskyddsreglerna. Tjänsten kan komma att innehålla merparten av Sveriges befolknings journaluppgifter och läkemedelsuppgifter. Dessa uppgifter är strikt reglerade i tillämpliga registerförfattningar och sekretessbestämmelser och den tillåtna spridningen av dem är mycket begränsad.

Enligt Datainspektionen är det EHM som är personuppgiftsansvarig och som ansvarar för att dessa känsliga personuppgifter inte obehörigen varken sprids eller ges åtkomst till.

Sekretess
EHM har uppgett att Kontot utgör ett s.k. eget utrymme enligt 2 kap. 10 § tryckfrihetsförordningen. Det överstämmer också väl med första stycket i 3 § i EHM:s instruktion att handlingarna i det personligt hälsokonto endast får förvaras hos myndigheten i form av teknisk lagring för enskilds räkning. EHM

har vidare konstaterat att det av 2 kap. 10 § tryckfrihetsförordningen framgår att handlingar i ett sådant utrymme inte är att anse som allmänna handlingar hos myndigheten som bearbetar och lagrar dem. EHM har därefter dragit slutsatsen att det inte råder någon sekretess för handlingarna.

Enligt 40 kap. 5 § offentlighets- och sekretesslagen gäller dock sekretess enligt följande

> *Sekretess gäller i verksamhet för enbart teknisk bearbetning eller teknisk lagring för någon annans räkning av personuppgifter som avses i personuppgiftslagen (1998:204) för uppgift om en enskilds personliga eller ekonomiska förhållanden.*

Då något skaderekvisit inte ställs upp som villkor för sekretessen innebär det att det råder absolut sekretess gällande personuppgifterna som finns på Användarens Konto. Av kommentaren till offentlighets- och sekretesslagen (se Lenberg m.fl., Offentlighets- och sekretesslagen, 1 juli 2016, Zeteo, kommentaren till 40 kap.5 §) framgår att sekretessbestämmelsen i praktiken närmast är en tystnadspliktsbestämmelse, eftersom en handling som förvaras hos en myndighet endast som led i teknisk bearbetning eller teknisk lagring för annans räkning inte är att anse som en allmän handling hos den myndigheten enligt tryckfrihetsförordningen. Av kommentaren framgår också att en myndighet, hos vilken sekretess gäller enligt denna paragraf, givetvis får lämna ut uppgifter till uppdragsgivare och till andra i enlighet med myndighetens åtaganden enligt uppdraget. Någon rätt för myndigheten att vid sidan av ingångna överenskommelser lämna en uppgift finns inte.

Eftersom EHM inte anser att det råder någon sekretess för uppgifterna på Kontot, har EHM inte analyserat om det överhuvudtaget är möjligt för EHM att ingå avtal med andra aktörer att få tillgång till uppgifter för vilka det råder absolut sekretess. Datainspektionen konstaterar att tillämpliga bestämmelser gällande det egna lagringsutrymmet utgår från att alla aktiviteter som sker på ett enskilt Konto ska ske på Kontoinnehavarens initiativ, medan EHM utgår från att det räcker med Användarens samtycke eller någon som Användaren gett mandat att samtycka. Datainspektionen konstaterar att endast Användaren själv kan förfoga över denna sekretess och att Användaren på något sätt måste ge ett uppdrag till EHM för att de överhuvudtaget ska kunna ge någon annan tillgång till uppgifterna. Det räcker således inte med att Användaren samtycker, Användaren ska vara uppdragsgivare.

Direktåtkomst
Vad som benämns som direktåtkomst har varierat något över tid och i olika sammanhang, men oftast avses när någon får direkt tillgång till annans uppgiftssamling och på egen hand kan söka information, antingen i hela eller i begränsade delar av uppgiftssamlingen, utan att den som är ansvarig för uppgifterna gör någon särskild prövning, såsom exempelvis sekretessprövning, vid det enskilda tillfället. För att åtkomsten och den behandling den innebär ska vara laglig har istället generella bedömningar och åtgärder vidtagits, redan när direktåtkomsten tilläts. Inte sällan anses direktåtkomst så integritetskänsligt att det regleras särskilt i lag.

Till uppgifterna i Tjänsten kommer Användaren, de personer som Användaren delar Kontot med och Applikationsleverantörerna ha åtkomst utan att EHM gör någon prövning i det enskilda fallet. EHM har inte uttryckligen använt ordet direktåtkomst men det är svårt att förstå tillgången som dessa andra användare får till Kontot på annat sätt än att det är frågan om direktåtkomst.

EHM:s tjänst kommer sammantaget att kunna behandla en mycket stor mängd hälsouppgifter. Till denna uppgiftssamling planeras en generös tillgång ges till dem som Användaren delar uppgifter med och till dem som blir godkända som Applikationsleverantörer. Eftersom EHM inte anser sig vara personuppgiftsansvarig för denna behandling har EHM inte heller utformat krav och begränsningar för denna åtkomst. Tillgången ges således utan att behovet av att behandla uppgifterna anges eller relateras till det intrång i den personliga integriteten som behandlingen kan innebära. Inte heller anges någon begränsning av vem som kan få tillgång till uppgifterna eller hur tillgången ska begränsas till vad just den aktören ska få ha tillgång till. Det beskrivs inte heller hur en obefogad spridning av uppgifterna ska hindras.

Aktuella registerförfattningar
Såsom nämnts i det tidigare avsnittet regleras vårdgivares behandling av personuppgifter inom vården av patientdatalagen. Även läkemedelsförteckningen och receptregistret som förs av EHM regleras av särskilda registerförfattningar. I samtliga dessa registerförfattningar regleras direktåtkomst.

Enligt 5 kap. 5 § patientdatalagen får den enskilde medges direktåtkomst till uppgifter om den enskilde själv under vissa förutsättningar. Regeringen uttalade i förarbetena viss farhåga att ge den enskilde direktåtkomst: *Ett skäl som har anförts mot att ge patienter direktåtkomst till sina patientuppgifter är risken för att patienterna utsätts för påtryckningar från t.ex. anhöriga eller blivande arbetsgivare att visa dem uppgifterna. Det går naturligtvis inte att helt bortse från risken att några patienter kan komma utsättas för sådana påtryckningar. En sådan risk finns emellertid redan nu. En person kan t.ex. förmå en anhörig att ge honom eller henne fullmakt att begära ut journaluppgifter beträffande denne. (Prop. 2007/08:126 s. 159).*

Vårdgivare kan enligt reglerna om sammanhållen journalföring ges direktåtkomst till andra vårdgivares uppgifter om patienter se 6 kap. patientdatalagen. I 5 § i det aktuella kapitlet anges emellertid att en vårdgivare inte får behandla en annan vårdgivares uppgifter om en patient i systemet med sammanhållen journalföring under andra förutsättningar än dem som anges i 3 och 4 §§ även om patienten uttryckligen samtycker till det. I författningskommentaren till 6 kap. 5 § (Prop. 2007/08:126 s. 254) anges bland annat följande. *Enligt undantaget får en vårdgivare inte behandla en annan vårdgivares uppgifter om en patient i systemet med sammanhållen journalföring under andra förutsättningar än dem som anges i 3 och 4 §§ även om patienten uttryckligen samtycker till det. Bland annat därför att direktåtkomst är en särskilt integritetskänslig form av elektroniskt utlämnande av personuppgifter, har det ansetts viktigt att den inte används för andra ändamål än de angivna, inte ens med patientens samtycke.*

Såsom framgår av de tidigare citerade bestämmelserna i lagen om läkemedelsförteckningen och receptregisterlagen kan den enskilde och ett antal yrkesutövare ges direktåtkomst till dessa register. Datainspektionen kan konstatera att EHM har att följa vad som är reglerat gällande läkemedelsförteckningen och receptregistret för att ge direktåtkomst till dessa uppgifter. EHM har inte utvecklat hur Hälsa För Mig förhåller sig till dessa bestämmelser. Lagstiftarens restriktivitet avseende direktåtkomst i dessa registerförfattningar får antas uttrycka lagstiftarens uppfattning om i vilken utsträckning direktåtkomst kan medges dessa uppgifter. På motsvarande sätt har lagstiftaren reglerat direktåtkomst till de patientuppgifter som vårdgivarna behandlar. De proportionalitetsavvägningar lagstiftaren gjort visar att inte ens vårdpersonal som behöver uppgifterna i vården kan stödja sig på enbart samtycke från den enskilde för att få ta del av journaluppgifter.

Såsom EHM beskrivit Tjänsten kommer EHM att kunna behandla i princip samma uppgifter om den enskilde som vårdgivare behandlar om patienten och som EHM behandlar i läkemedelsförteckningen respektive receptregistret. Därtill kommer de uppgifter som Användaren eller Applikationsleverantören tillför. Om en vidare direktåtkomst till dessa uppgifter ska ges bör det ankomma på lagstiftaren att bedöma hur och för vilka dessa hälsouppgifter ska göras åtkomliga. Hälsouppgifter har många intressenter och det är viktigt att noga bedöma de risker som uppstår vid direktåtkomst och balansera dessa.

Datainspektionens bedömning avseende andra än Användarens tillgång till hälsokontot
Datainspektionen konstaterar att EHM:s personuppgiftsansvar även omfattar den behandling som sker i Kontot av de personer som Användaren delat sitt konto med genom den s.k. delningsfunktionen och den behandling som utförs av Applikationsleverantörerna.

I EHM:s personuppgiftsansvar ingår att se till att de grundläggande kraven uppfylls dvs. att behandlingen som utförs är laglig och korrekt och att den överensstämmer med de berättigade ändamål som ligger till grund för behandlingen. Datainspektionen anser att de ändamål som ligger till grund för behandlingen är att ge enskilda tillgång till egna hälsokonton och att till dessa ansluta vissa funktioner som tredje part tillhandahåller om Användaren begär det. Av instruktionen framgår också att EHM inte själva ska kunna behandla uppgifterna för annat än lagring för den enskildes räkning. I EHM:s uppdrag ingår således inte att sprida eller tillgängliggöra uppgifterna till tredje man.

EHM ansvarar också för att fler uppgifter inte behandlas än vad som är nödvändigt utifrån ändamålet. Det innebär att enbart de uppgifter som Användaren har behov av ska behandlas och uppgifterna ska bara behandlas om de behövs för att uppfylla Användarens behov. Uppgifter får således inte behandlas för att tillgodose någon annans behov.

Det måste finnas rättsligt stöd för behandlingen och om stödet är samtycke måste det vara ett giltigt samtycke. Eftersom det huvudsakligen är frågan om behandling av känsliga personuppgifter måste det finnas ett undantag från

förbudet mot att behandla dessa uppgifter. EHM har som personuppgiftsansvarig ett ansvar för att de samtycken som ges har föregåtts av tillräckligt preciserad och tydlig information för att Användaren ska veta vad samtycket innebär i det specifika fallet och att användaren också har lämnat samtycket helt frivilligt. Dessa krav omfattar även personuppgifter som rör annan registrerad än Användaren.

För personuppgifterna på Kontot råder absolut sekretess. Det innebär att EHM inte kan tillgängliggöra eller sprida uppgifterna annat än om det sker på uppdrag av Användaren.

Såsom Tjänsten är planerad kommer såväl personer som Användaren delar Kontot med och Applikationsleverantörer som fått Användarens samtycke, kunna få direktåtkomst till uppgifterna på Kontot. Direktåtkomst anses vara en särskilt integritetskänslig form av utlämnande. Genom att ge direktåtkomst ger EHM tillgång till personuppgifterna för vilka det råder sekretess. EHM har som redan nämnts inte rätt att disponera över uppgifterna utan ska enbart lagra dem för den enskildes räkning. Att Användaren samtycker till en behandling är inte detsamma som att Användaren har ett eget intresse av denna behandling. Direktåtkomst till Användarens personuppgifter kan således bara ske för att uppfylla Användarens eget behov och till uppgifter som Användaren anvisat. Det är EHM:s ansvar att se till att det föreligger ett giltigt samtycke, att uppgifterna inte används på något annat sätt än vad Användaren angett, att tillgång bara ges till de uppgifter som behövs för att uppfylla uppdraget.

Beträffande möjligheten att dela information med andra privatpersoner så är inte det angivet i EHM:s instruktion. Det är frågan om en direktåtkomst till känsliga personuppgifter som går utöver vad som gäller i aktuella registerförfattningar. Funktionen är inte begränsad till viss kategori utan i princip kan även yrkesverksamma som själva har ett Konto, erhålla tilldelning av Konton från kunder, klienter, patienter, forskningsobjekt osv. Dessa yrkesverksamma skulle kunna få del av en stor mängd Konton. En sådan behandling har EHM inte stöd för. Att den enskilde kan överlåta sina rättigheter till en annan i delningsfunktionen genom ett s.k. ägarskap är inte förenligt med vare sig med gällande dataskyddsregler eller med den sekretess som råder för Tjänsten. EHM har inte heller angett att de kontrollerar att delningen av Kontot sker frivilligt. Uppgifterna på Kontot kan dessutom innehålla betydligt mer information än vad Användaren själv är medveten om

eftersom hälsouppgifter är tänkta att överföras löpande via prenumerationstjänsterna. Det innebär att EHM kan komma att ge tillgång till uppgifter för vilka det råder sekretess och som Användaren själv inte önskar delge andra. Enligt Datainspektionen har den delningsfunktion som EHM utformat inte stöd i gällande regler.

Mot denna bakgrund ska EHM föreläggas att se till att personuppgifterna på den enskildes konto inte röjs i strid med sekretessen och att inte ge tillgång till personuppgifterna i Hälsa För Mig till andra än den enskilde kontoinnehavaren och de applikationsleverantörer som tillhandahåller applikationer i syfte att visa eller tillföra uppgifter till den enskildes konto. EHM ska också föreläggas att se till att inte andra uppgifter behandlas av applikationsleverantörerna än de som den enskilde kontoinnehavaren anvisat och att personuppgifterna inte behandlas för annat syfte än att visa eller tillföra uppgifter till den enskildes konto.

Övrigt

EU:s dataskyddsförordning
Från och med den 25 maj 2018 kommer personuppgiftslagen ersättas av EU:s dataskyddsförordning. Dataskyddsförordningen kommer att ha företräde framför nationell rätt, vilket innebär att om nationell lagstiftning inte överensstämmer med förordningen, ska förordningens bestämmelser tillämpas. Dataskyddsförordningen lämnar dock visst utrymme för, och påbjuder även i vissa fall, nationella regler. Det kommer därför fortsatt finnas nationella dataskyddsregler, men dessa måste vara anpassade till förordningen.

Dataskyddsförordningen innehåller i stora drag samma bestämmelser som dagens dataskyddsregler, men det finns skillnader som är viktiga att notera. De grundläggande kraven i 9 § personuppgiftslagen återfinns i de grundläggande principerna för behandling i artikel 5. Det som är särskilt värt att notera gällande artikel 5 är att kravet på öppenhet gentemot den registrerade har stärkts. Integritet och konfidentialitet har lyfts in i de grundläggande principerna. Ett nytt krav har tillkommit som anger att den personuppgiftsansvarig inte bara ansvarar för att de grundläggande principerna följs utan också ska kunna visa att de efterlevs, s.k. ansvarsskyldighet.

Det rättsliga stödet i 10 § personuppgiftslagen motsvaras av kravet på laglig grund för behandling i artikel 6. I skäl 42 och 43 beskrivs närmare vad kraven på frivillig, specifik, informerad och otvetydig viljeyttring vid samtycke innebär. Skäl 43 har följande lydelse. *För att säkerställa frivillighet bör det inte utgöra giltig rättslig grund för behandling av personuppgifter i ett särskilt fall där det råder betydande ojämlikhet mellan den registrerade och den personuppgiftsansvarige, särskilt om den personuppgiftsansvarige är en offentlig myndighet och det därför är osannolikt att samtycket har lämnats frivilligt när det gäller alla förhållanden som denna särskilda situation omfattar. Samtycke antas inte vara frivilligt om det inte medger att separata samtycken lämnas för olika behandlingar av personuppgifter, trots att detta är lämpligt i det enskilda fallet, eller om genomförandet av ett avtal – inbegripet tillhandahållande av en tjänst – är avhängigt av samtycket, trots att samtycket inte är nödvändigt för ett sådant genomförande.* Vidare begränsas i artikeln offentliga myndigheters möjlighet att använda intresseavvägning.

Förbudet mot att behandla särskilda kategorier av uppgifter s.k. känsliga personuppgifter regleras i artikel 9 och de registrerades rättigheter återfinns i kapitel III. Förordningen lämnar ett visst utrymme för att inskränka de rättigheter som anges i kapitel III, men ställer krav på lagstiftningens utformning och innehåll. Dessa krav framgår av artikel 23. Skyldigheterna regleras i kapitel IV som har rubriken *Personuppgiftsansvarig och personuppgiftsbiträde*. I det kapitlet kan särskilt nämnas artikel 32 som reglerar säkerhet i samband med personuppgiftsbehandling och artikel 35 som reglerar konsekvensbedömning avseende dataskydd. I kapitel V regleras överföring av personuppgifter till tredjeländer eller internationella organisationer.

För att EHM ska kunna erbjuda Tjänsten även efter den 25 maj 2018 måste reglerna i dataskyddsförordningen beaktas. Det är även väsentligt att överväga behovet av nationell lagstiftning utifrån dataskyddsförordningen.

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. 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 enhetschef Katarina Tullstedt. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom och juristen Lena Carlsson deltagit.

Kristina Svahn Starrsjö

Katarina Tullstedt

Kopia till:

Socialdepartementet för kännedom