REKOMMENDATIONER TILL NATIONELLA KVALITETSREGISTER INFÖR DATASKYDDSFÖRORDNINGEN

INLEDNING

Denna orientering syftar till att uppmärksamma i första hand centralt personuppgiftsansvariga myndigheter för Nationella Kvalitetsregister (CPUA-myndigheter) på konsekvenser för Nationella Kvalitetsregister när EU:s nya dataskyddsförordning träder i kraft den 25 maj detta år. Orienteringen riktar sig även till vårdgivare som rapporterar patientuppgifter till kvalitetsregister samt regionala registercentrum och cancercentrum (registercentrumorganisationen, RCO), vilka har till uppgift att stödja och utveckla kvalitetsregister.

Närmast berörda för nödvändiga anpassningsåtgärder är styrgrupper för Nationella Kvalitetsregister, registerhållare, registeransvariga hos vårdgivare och dataskyddsombud hos CPUA-myndigheten (normalt landstings- eller regionstyrelser). RCO bör ta en ledande roll för att genomföra rekommenderade åtgärder i samverkan med berörda vårdgivare och CPUA-myndigheter.

När dataskyddsförordningen träder i kraft gäller den som lag i Sverige och övriga EU:s medlemsländer. Vid samma tidpunkt upphör personuppgiftslagen och det nuvarande dataskyddsdirektivet. Förordningen kommer att innebära en hel del förändringar för de som behandlar personuppgifter, t.ex. kvalitetsregister, och stärkta rättigheter för den enskilde när det gäller den personliga integriteten.

Det finns inga övergångsregler utan dataskyddsförordningen kommer att gälla fr.o.m. den 25 maj. Den som behandlar personuppgifter men inte följer eller inte kan visa följsamhet till förordningens bestämmelser riskerar höga vitessanktioner.

Nationella och regionala kvalitetsregister regleras idag i 7 kap. patientdatalagen (2008:355; PDL). En särskild utredning, Socialdataskyddsutredningen (SOU 2017:66), har granskat patientdatalagen med anledning av dataskyddsförordningen. Utredningen har bedömt att PDL är i stort sett förenlig med förordningen och föreslagit endast mindre justeringar i lagen. Nuvarande reglering om kvalitetsregister i PDL kommer således att gälla efter den 25 maj med undantag för vissa redaktionella ändringar och en begränsning som behandlas nedan. Regeringen har i skrivande stund ännu inte presenterat en proposition med lagändringar i PDL.

FATTA BESLUT OM CPUA

För att veta bestämt vem som är personuppgiftsansvarig för ett Nationellt Kvalitetsregister och att det är en myndighet rekommenderas styrgrupper att som första åtgärd inför en anpassning av verksamheten till dataskyddsförordningen att kontrollera huvudmannaskapet för sitt eller sina Nationella Kvalitetsregister.

Enligt 7 kap. 7 § patientdatalagen får endast myndigheter inom hälso- och sjukvården vara personuppgiftsansvariga för central behandling av personuppgifter i ett nationellt eller regionalt kvalitetsregister. Kommunala bolag kan därmed inte vara personuppgiftsansvariga för kvalitetsregister. Som regel är landstingsstyrelser eller regionstyrelser personuppgiftsansvariga för kvalitetsregister. Även andra nämnder kan givetvis vara personuppgiftsansvariga.

Dataskyddsförordningen innebär en ny ordning med ett större ansvar för personuppgiftsbehandlingen och dataskyddet för personuppgifter. Det finns mot denna bakgrund anledning för varje styrgrupp att se över huvudmannaskapet för eget Nationellt Kvalitetsregister. Tre frågor ska kontrolleras:

- Är huvudmannen för ett kvalitetsregister en myndighet?
- Är det tydligt för rapporterande vårdgivare vem som är personuppgiftsansvarig för ett kvalitetsregister?
- Vilken organisatorisk enhet hos myndigheten ansvarar för ett kvalitetsregister?

Visar styrgruppens översyn att ansvarig huvudman inte är en myndighet är personuppgiftsbehandlingen i ett kvalitetsregister otillåten. Lösning: Byt huvudmannaskapet till en myndighet. Sondering om lämplig CPUA-myndighet bör ske med RCO. När en överenskommelse nåtts med ett landsting eller en region som ska ta över ansvaret för registret, kontakta dataskyddsombudet hos nuvarande huvudman eller övertagande landsting/region för rådgivning hur bytet ska genomföras, bl.a. med respekt för skyddet för de registrerades personliga integritet.

Om det är oklart för rapporterande vårdgivare vem som är personuppgiftsansvarig för ett kvalitetsregister, kan vårdgivarnas personuppgiftsbehandling (utlämnandebehandling) vara otillåten. Alla styrgrupper för Nationella Kvalitetsregister rekommenderas därför att driva frågan att få till stånd ett dokumenterat beslut om centralt personuppgiftsansvarig för kvalitetsregistret. Beslutet bör fattas i en landstingsstyrelse, regionstyrelse eller en sjukhusstyrelse när omständigheterna kring var det ligger/bör ligga har utretts. Informera om personuppgiftsansvarig på registrets hemsida och på www.kvalitetsregister.se. Informera också rapporterande vårdgivare. Se dessutom över informationen till registrerade och rutiner för informationsskyldigheten.

Det är lika viktigt att slå fast registrets organisatoriska tillhörighet i beslutet, dvs. vilken avdelning eller förvaltning inom CPUA-myndigheten som ansvarar för registret så att ansvaret är transparent inom myndigheten för både medarbetare och patienter/registrerade. Det är den organisatoriska enheten som ansvarar för registrets löpande verksamhet samt utser exempelvis styrgrupp och registerhållare. CPUA-myndighetens riktlinjer om exempelvis vilka kostnader som ska belasta verksamheten och jäv ska ju innefatta kvalitetsregistrets verksamhet.

Det finns ingen reglering som säger att ett sådant beslut måste fattas, eller fattas på ett särskilt sätt. Rekommendationen är emellertid att beslutet om centralt personuppgiftsansvarig för ett eller flera Nationella Kvalitetsregister inkluderar information om ansvarig organisatorisk enhet.

Saknas ett skriftligt beslut om ansvarig CPUA-myndighet och ansvarig organisatorisk enhet inom myndigheten för ett eller flera Nationella Kvalitetsregister, rekommenderas att ett sådant beslut fattas före den 25 maj 2018. Även uppdrag till styrgrupp och registerhållare kan behöva ses över med anledning av ett sådant beslut.

CPUA-MYNDIGHETENS SKYLDIGHETER

En rad nya skyldigheter i dataskyddsförordningen träffar CPUA-myndigheten. Landstingsstyrelsen eller regionstyrelsen är som regel CPUA-myndighet för Nationella Kvalitetsregister. I huvudsak följande skyldigheter måste iakttas:

1. Följa de grundläggande dataskyddsprinciperna
2. Se över rutiner för bevarande och gallring
3. Kunna visa ansvarsskyldighet
4. Utse dataskyddsombud
5. Etablera rutiner för hantering av personuppgiftsincidenter
6. Förteckning över kategorier av personuppgifter
7. Nya personuppgiftsbiträdesavtal med leverantörer
8. Etablera rutiner för att snabbt och smidigt tillgodose registrerads rättigheter
9. Etablera rutiner för att underrätta tredje part om rättelse och begränsning
10. Begränsningar att registrera genetiska uppgifter
11. Se över information till registrerade
12. Se över rutiner för samtycke
13. Utföra dataskyddskonsekvensbedömningar
14. Arbeta aktivt med skyddet för personuppgifter och iaktta inbyggt dataskydd och dataskydd som standard

I det följande kommenteras punkterna med åtföljande rekommendationer.

1. FÖLJA DE GRUNDLÄGGANDE DATASKYDDSPRINCIPERNA

Totalt innehåller dataskyddsförordningen *sex grundläggande dataskyddsprinciper* som ska genomsyra CPUA-myndighetens behandling av personuppgifter i kvalitetsregister. Dessa finns i art. 5 dataskyddsförordningen. Principerna är följande:

- Personuppgifter ska behandlas på *ett lagligt, korrekt och öppet sätt* i förhållande till den registrerade (principen om laglighet, korrekthet och öppenhet).
- Personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska inte anses vara oförenlig med de ursprungliga ändamålen (*principen om ändamålsbegränsning*).

- Personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (principen om uppgiftsminimering).
- Personuppgifter ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål (*principen om korrekthet*).
- Personuppgifter får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt denna förordning genomförs för att säkerställa den registrerades rättigheter och friheter (*principen om lagringsminimering*).
- Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (*principen om integritet och konfidentialitet*).

Använder CPUA-myndigheten ett personuppgiftsbiträde (se *Nya personuppgiftsbiträdesavtal med leverantörer*) ska myndigheten säkerställa att biträdet i motsvarande utsträckning följer dataskyddsprinciperna genom utfärdade instruktioner.

2. SE ÖVER RUTINER FÖR BEVARANDE OCH GALLRING

Personuppgifter i ett nationellt eller regionalt kvalitetsregister ska enligt 7 kap. 10 § första stycket PDL gallras när de inte längre behövs för det ändamål de behandlas för (systematiskt och fortlöpande utveckla och säkra vårdens kvalitet). Arkivmyndighet inom ett landsting eller en region (normalt landstings- eller regionstyrelsen) får dock enligt samma paragraf föreskriva att personuppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål.

Regleringen i 7 kap. 10 § PDL får anses utgöra ett undantag från principen om lagringsminimering i art. 5.1 e i dataskyddsförordningen (se *1. Följa de grundläggande dataskyddsprinciperna*). Principen innebär att personuppgifter inte får förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

Innebörden av 7 kap. 10 § PDL är att om uppgifter i ett kvalitetsregister ska användas för sekundära ändamål, t.ex. statistik och forskning (utöver systematisk och fortlöpande utveckling och säkring av vårdens kvalitet), vilka är normala användningsområden för alla kvalitetsregister, måste CPUA-myndigheten säkerställa att uppgifterna i registret bevaras för dessa ändamål i befintlig dokumenthanteringsplan (motsvarande). Annars följer det av både art. 5.1 e (principen om lagringsminimering) och 7 kap. 10 § PDL att uppgifterna i registret ska gallras när de inte längre är nödvändiga för ändamålet kvalitetsutveckling.

Saknas föreskrifter härom i dokumenthanteringsplan (motsvarande) för ett kvalitetsregister, men personuppgifterna i registret är avsedda att användas för att ta fram statistik över behandlingsåtgärder m.m. eller lämnas ut för forskning, ska CPUA-myndigheten, som tillika är arkivmyndighet, genomföra en bevarande- och gallringsutredningen och därefter föreskriva bevarandetid för personuppgifterna i registren för forskningsändamål eller statistiska ändamål.

3. KUNNA VISA ANSVARSSKYLDIGHET

En av nyheterna i dataskyddsförordningen är kravet på *ansvarsskyldighet*. Det innebär att den personuppgiftsansvarige, dvs. CPUA-myndigheten, inte bara ansvarar för att de grundläggande dataskyddsprinciperna följs utan ska också kunna ”*visa*” att de efterlevs (art. 5.2). Av art 24.1 framgår att CPUA-myndigheten också ska kunna visa att behandlingen är förenlig med övriga bestämmelser i förordningen. Eftersom PDL är ett utflöde av dataskyddsförordningen, får kravet på ansvarsskyldighet anses även omfatta den personuppgiftsbehandling som sker inom ramen för den lagen.

Det finns flera sätt att visa att man följer dataskyddsregleringen. Att ha riktlinjer, policys och instruktioner är ett sätt (art. 24.2; skäl 78). Att följa branschspecifika uppförandekoder för persondataskydd eller certifiera sig enligt etablerade standarder (och i framtiden enligt förordningen) är ytterligare sätt att visa ansvarsskyldighet.

I huvudsak handlar kravet på ansvarsskyldighet om att personuppgiftsansvarig ska ha tydliga rutiner för och dokumentation om åtgärder, överväganden och personuppgiftsbehandlingar. Dataskyddsförordningens bestämmelser om skadestånd och höga sanktionsavgifter har enbart till syfte att inpränta denna ansvarsskyldighet.

4. UTSE DATASKYDDSOMBUD

Dataskyddsförordningen ställer krav på att vissa organisationer ska utse ett dataskyddsombud. Även andra aktörer vars verksamhet involverar särskilt riskfylld behandling ska utse ett dataskyddsombud. Som exempel på sådan riskfylld behandling nämner förordningen regelbunden och systematisk övervakning av registrerade i stor skala eller omfattande behandling av känsliga personuppgifter (art. 37.1).

Det är viktigt att notera att rollen som dataskyddsombud inte är densamma som personuppgiftsombudet i nuvarande personuppgiftslagen. Dataskyddsombudet har en betydligt starkare och självständigare ställning. Den person som utses måste ha tillräcklig kunskap om dataskydd och få det stöd och de befogenheter i ett mandat från myndigheten som krävs för att kunna utföra sitt uppdrag på ett effektivt och oberoende sätt.

Personuppgiftsansvariga för Nationella Kvalitetsregister är som regel landstingsstyrelser eller regionstyrelser. De är myndigheter och ska ha ett utsett dataskyddsombud den 25 maj 2018. Det finns ingen övergångsperiod. Det är dock tillåtet för landsting eller regioner att utse ett gemensamt ombud för samtliga nämnder eller kommunala bolag eller flera ombud. Ett ombud kan vara anställd eller anlitas externt.

Artikel 29-arbetsgruppen har publicerat en vägledning om dataskyddsombud. Även SKL har publicerat en vägledning om dataskyddsombud, https://skl.se/download/18.2ced2eb215cc46662ca11a3a/1498030987866/Vägledning%20kring%20dataskyddsombud.pdf.

5. ETABLERA RUTINER FÖR PERSONUPPGIFTSINCIDENTER

Dataskyddsförordningen innehåller nya bestämmelser om vad personuppgiftsansvariga och personuppgiftsbiträden (leverantörer) måste göra om de blir utsatta för dataintrång eller på något annat sätt förlorar kontrollen över de uppgifter de behandlar. En sådan personuppgiftsincident ska anmälas av den personuppgiftsansvarige till Datainspektionen inom 72 timmar, om det inte är osannolikt att incidenten medför risker för enskildas fri- och rättigheter (art. 33.1). Personuppgiftsbiträdren ska enligt dataskyddsförordningen underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident, dvs. inom en betydligt kortare tidsfrist än 72 timmar (art. 33.2).

Om incidenten kan leda till att personer utsätts för allvarliga risker såsom diskriminering, id-stölder, bedrägerier eller finansiella stölder ska även de registrerade informeras om händelsen så att de kan vidta nödvändiga åtgärder (art. 34).

För att kunna leva upp till skyldigheten om rapportering av personuppgiftsincidenter enligt förordningen måste CPUA-myndigheten ha både en organisation för incidentberedskap och rutiner på plats för att kunna upptäcka, rapportera och utreda sådana incidenter som drabbar Nationella Kvalitetsregister. CPUA-myndigheten rekommenderas att bestämma var ansvaret för att göra en anmälan om incident till Datainspektionen ska ligga i registerorganisation så att anmälan kan göras i rätt tid. Rutiner för upptäckt och anmälan av personuppgiftsincidenter bör framgå av befintligt kvalitetsledningssystem. Eftersom registerhållaren dagligen arbetar med registret kan det vara lämpligt att utse denne att bära ansvaret för anmälan alternativt ansvarig verksamhetschef vid den organisatoriska enhet som ansvarar för registret inom myndigheten.

Anlitas leverantörer för drift av kvalitetsregister ska personuppgiftsbiträdesavtalet tydligt reglera deras roll vid incidenter och tidsfrister för rapportering till ansvarig mottagare hos CPUA-myndigheten.

Artikel 29-arbetsgruppen har publicerat en vägledning om personuppgiftsincidenter enligt dataskyddsförordningen

6. FÖRTECKNING ÖVER KATEGORIER AV PERSONUPPGIFTER

Dataskyddsförordningen (art. 30.1) kräver att varje personuppgiftsansvarig organisation ska föra ett register över personuppgiftsbehandlingar som utförs i den verksamhet som den personuppgiftsansvarige ansvarar för. När dataskyddsförordningen börjar gälla den 25 maj 2018 rekommenderas att denna förteckning finnas på plats hos CPUA-myndigheten, som regel en landstingsstyrelse eller regionstyrelse.

Det måste finnas rutiner för att kunna hålla förteckningen uppdaterad. Den ska vara skriftlig och helst i elektronisk form så att den är tillgänglig för organisationen. Förteckningen ska vid begäran kunna visas upp för Datainspektionen.

SKL har tagit fram en mall som kan användas för att föra denna förteckning, se https://skl.se/naringslivarbetedigitalisering/digitalisering/dataskyddsforordningengdpr/informationsinsatserkringdataskyddsforordningen.12704.html. Det finns även applikationer för detta ändamål som kan upphandlas.

7. NYA PERSONUPPGIFTSBITRÄDESAVTAL MED LEVERANTÖRER

Dataskyddsförordningen ställer krav på, liksom idag, att den personuppgiftsansvarige ska teckna ett personuppgiftsbiträdesavtal med den som behandlar personuppgifter för den personuppgiftsansvariges räkning, ett s.k. personuppgiftsbiträde. Som exempel på typiska personuppgiftsbiträden kan nämnas leverantörer av olika e-tjänster. Även Inera AB är ett personuppgiftsbiträde.

Dataskyddsförordningen ställer särskilda krav på innehållet i ett personuppgiftsbiträdesavtal (art. 28.3), bl.a. föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade samt den personuppgiftsansvariges skyldigheter och rättigheter, t.ex. att den personuppgiftsansvarige ska ha tillgång till all information hos leverantören för att kunna bedöma om denne lever upp till förordningens krav och att personuppgifter återlämnas alternativt raderas när uppdraget upphör.

En personuppgiftsansvarig får endast anlita personuppgiftsbiträden som kan ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i förordningen (art. 28.1). Vad det innebär i praktiken är något oklart.

Enligt skäl 81 i dataskyddsförordningen ska garantierna i synnerhet omfatta ”sakkunskap, tillförlitlighet och resurser för att genomföra tekniska och organisatoriska åtgärder som uppfyller kraven i förordningen, bl.a. vad gäller säkerhet i samband med behandlingen av uppgifter.” Vidare framgår det av skäl 81 att personuppgiftsbiträdets ”anslutning till en godkänd uppförandekod eller en godkänd certifieringsmekanism kan användas som ett sätt att påvisa att den personuppgiftsansvarige fullgör sina skyldigheter.” Om en leverantör är certifierad enligt etablerade standarder, t.ex. ISO/IEC 27001 Ledningssystem för informationssäkerhet, COBIT eller ITIL, torde således denne uppfylla kravet på ”tillräckliga garantier.

Enligt dataskyddsförordningen får ett personuppgiftsbiträde inte anlita ett underbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige (art. 28.2).

Som framgår rekommenderas CPUA-myndigheten att ha sett över sina personuppgiftsbiträdesavtal med leverantörer som driftar kvalitetsregister och kvalitetsregisterplattformar senast den 25 maj 2018, och i de fall nuvarande avtal inte uppfyller

förordningens krav på innehåll förhandla med motparten om nytt inom tidsgränsen. Instruktioner till personuppgiftsbiträdet om personuppgiftsbehandlingen ska vara skriftliga för att uppfylla kravet på ansvarsskyldighet.

8. ETABLERA RUTINER FÖR ATT SNABBT OCH SMIDIGT TILLGODOSE REGISTRERADS RÄTTIGHETER

Alla personuppgiftsansvariga måste ha en laglig (rättslig) grund för sin behandling av personuppgifter. Det är viktigt att ha klart för sig med vilken laglig grund man behandlar personuppgifter. Till exempel ska personuppgiftsansvariga bl.a. ange den lagliga grunden för personuppgiftsbehandlingen när man informerar registrerade. Dessutom är ett flertal av de registrerades rättigheter beroende av den rättsliga grunden för behandlingen.

De lagliga grunderna för behandling av personuppgifter i regionala och nationella kvalitetsregister är dels ”uppgifter av allmänt intresse” (art. 6.1 e), dels ”förebyggande hälso- och sjukvård och yrkesmedicin” (art. 9.2 h), dels lagstadgad tystnadsplikt för ”yrkesutövare” (art. 9.3), dels 2 kap. 4 § 1 i den föreslagna lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) och dels 7 kap. PDL.

Det innebär att enskilda personer och patienter kan åberopa följande rättigheter mot CPUA-myndigheten:

- Rätt att motsätta sig registrering i ett kvalitetsregister (efter att ha fått information om personuppgiftsbehandlingen)
- Efter att registrering har skett, rätt att få uppgifter utplånade ur registret så snart som möjligt.
- Rätt enligt 8 kap. 5 § PDL att få information om den direktåtkomst och elektroniska åtkomst som förekommit
- Rätt att få information (art. 13 och 14)
- Rätt att få tillgång till uppgifter (art. 15)
- Rätt till rättelse (art. 16)
- Rätt till begräsning av behandling (art. 18)

Rätten till begränsning är ny. Enligt art. 18 i dataskyddsförordningen har den registrerade rätt att under vissa förutsättningar kräva att behandlingen av personuppgifter begränsas, vilket har ersatt den åtgärd som enligt dataskyddsdirektivet benämns som blockering.

Den registrerade har rätt att kräva att behandlingen begränsas om han eller hon bestrider personuppgifternas korrekthet, under en tid som ger den personuppgiftsansvarige möjlighet att kontrollera om personuppgifterna är korrekta (art. 18.1 a). Begränsning kan också krävas om behandlingen är olaglig och den registrerade motsätter sig att personuppgifterna raderas och i stället begär en begränsning av deras användning (art. 18.1 b). Om den personuppgiftsansvarige inte längre behöver personuppgifterna för ändamålen med behandlingen, kan den registrerade kräva att behandlingen begränsas om han eller hon

behöver uppgifterna för att kunna fastställa, göra gällande eller försvara rättsliga anspråk (art. 18.1 c).

Rätten att bli bortglömd (art. 17) är inte tillämplig på kvalitetsregister eftersom PDL innehåller en motsvarande rätt att få bli utplånad. Rätten till dataportabilitet (art. 20) är inte heller tillämplig eftersom den rätten förutsätter att den lagliga grunden är antingen samtycke eller avtal; så är inte fallet med kvalitetsregister. Rätten till invändning (art. 21) är inte tillämplig eftersom PDL innehåller en motsvarande rätt att få motsätta sig registrering i kvalitetsregister.

Rätten att slippa bli föremål för automatiserade beslut som inbegriper profilering, vilket egentligen är ett förbud (art. 22), torde knappas aktualiseras för kvalitetsregister eftersom sådana register inte får användas för individnära vård och behandling.

Det rekommenderas att det finns rutiner i registerorganisationen för att kunna fånga upp och tillgodose enskildas rättigheter som åberopas mot CPUA-myndigheten. Rättigheterna kräver rutiner som väl kan liknas hanteringen vid en begäran att få del av allmän handling. Rutinerna bör lämpligen samordnas med andra personuppgiftsbehandlingar inom myndighetens verksamhet och med andra nämnder. Rapporterande vårdgivare ska givetvis även kunna hänvisa registrerade till rätt instans hos CPUA-myndigheten och tillhandahålla korrekta kontaktuppgifter. En registrad ska inte hamna i en situation där denne ”bollas” runt mellan olika organisatoriska enheter.

Beträffande dataskyddsförordningens rättigheter ska CPUA-myndigheten senast en månad efter att ha mottagit begäran tillhandahålla den registrerade information om de åtgärder som vidtagits (art. 12.3). Denna period får vid behov förlängas med ytterligare två månader, med beaktande av hur komplicerad begäran är och antalet inkomna begäranden. Den personuppgiftsansvarige ska underrätta den registrerade om en sådan förlängning inom en månad från det att begäran mottagits samt ange orsakerna till förseningen.

Om den registrerade lämnar en begäran om en rättighet i elektronisk form, *ska* informationen om möjligt tillhandahållas i elektronisk form, om den registrerade inte begär något annat (art. 12.3). CPUA-myndigheten bör därför erbjuda elektroniska möjligheter för registrerade att framföra sina rättigheter, t.ex. registerutdrag, genom identifiering med BankID, och lämna information i digital form på ett säkert sätt genom identifiering av mottagaren med BankID. Det finns ett flertal tjänster för utlämnande av elektroniska handlingar, s.k. digitala brevlådor, bl.a. Mina meddelanden, som tillhandahålls av Skatteverket. En allmän strävan bland vårdgivare och CPUA-myndigheter för kvalitetsregister bör vara att nyttja den infrastruktur som skapats nationellt för hälso- och sjukvården såsom Invånartjänsterna i 1177 Vårdguiden, t.ex. Journalen och invånarens 1177-konto. BankID är ett krav för inloggning.

Observera att registrerade alltid har rätt att åberopa en rättighet även om den är begränsad i svensk lagstiftning. Begäran ska alltid prövas av myndigheten oavsett om den är begränsad eller inte. Om den registrerade nekas en rättighet i sak, t.ex. rättelse, eller att rättigheten är beskuren i PDL, ska beslutet meddelas skriftligen med besvärshänvisning och i rekommenderat brev. Överklagandebestämmelser finns i förslaget till lag med kompletterande bestämmelser till EU:s dataskyddsförordning.

9. ETABLERA RUTINER FÖR ATT UNDERRÄTTA TREDJE PART OM RÄTTELSE OCH BEGRÄNSNING

Enligt art. 19 dataskyddsförordningen ska den personuppgiftsansvarige underrätta varje mottagare till vilken personuppgifterna har lämnats ut om eventuella rättelser eller radering av personuppgifter eller begränsningar av behandling, om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

Som framhållits är det enbart rätten till rättelse och begräsning som kan åberopas av en registrerad mot CPUA-myndighetens behandling av dennes personuppgifter i ett kvalitetsregister.

I majoriteten av de fall där uppgifter lämnas ut av ett kvalitetsregister, rör det sig om forskning. Anmälningsskyldigheten enligt art. 19 innebär att CPUA-myndigheten ska underrätta en forskningshuvudman om att uppgifter rättats eller begränsats på begäran av den registrerade. CPUA-myndigheten rekommenderas därför att ha rutiner och tekniska funktioner på plats för att dokumentera utlämnande av kvalitetsregisteruppgifter till tredje part för att kunna ha spårbarhet på mottagare som ska underrättas om en rättelse eller begräsning.

Kryptering och pseudonymisering utgör sådana säkerhetsåtgärder som nämns i art. 32 i dataskyddsförordningen och som ska vidtas i den mån det är lämpligt. Tillämpningen av pseudonymisering av personuppgifter kan minska riskerna för de registrerade som berörs och hjälpa personuppgiftsansvariga och personuppgiftsbiträden att fullgöra sina skyldigheter i fråga om dataskydd (skäl 32 i dataskyddsförordningen). Om uppgifterna som har lämnats ut av ett kvalitetsregister är pseudonymiserade, dvs. att inga namn och personnummer har lämnats ut till forskningshuvudmannen, torde skyldigheten enligt art. 19 bortfalla eftersom någon risk för enskildas fri- och rättigheter inte föreligger. Forskningshuvudmannen vet inte vems uppgifter som är rättade eller begränsade. Pseudonymisering utesluter dock inte att andra åtgärder för dataskydd kan behövas (skäl 32).

Kryptering och pseudonymisering är för övrigt åtgärder som tillgodoser principen om uppgiftsminimering i art. 5.1 c i dataskyddsförordningen eftersom sådana åtgärder innebär att den personuppgiftsansvarige inte behandlar fler direkt identifierande personuppgifter än vad som är nödvändigt för ändamålet med behandlingen. Krav på kryptering och pseudonymisering uppfyller också villkoren i principen om integritet och konfidentialitet i art. 5.1 f.

Nationella Kvalitetsregister bör vidare etablera en rutin för att vid beslut om rättelse av felaktig uppgift eller begränsning av behandling på grund av inkorrekta uppgifter informera den registrerade om den ”felaktiga” källan, dvs. rapporterande vårdgivare.

Art. 19 är också tillämplig på rapporterande vårdgivare. Har de rättat personuppgifter eller begränsat behandling av personuppgifter ska de underrätta kvalitetsregistret, som i samma utsträckning ska iaktta rättigheten, dvs. rätta uppgiften eller begränsa behandlingen.

10. BEGRÄNSNINGAR ATT REGISTRERA GENETISKA UPPGIFTER

Socialdataskyddsutredningen (SOU 2017:66) har föreslagit ändringar i 7 kap. 8 § 3 stycket PDL. Stycket reglerar idag begränsningar för kvalitetsregister att behandla andra känsliga uppgifter än hälsa samt uppgifter om lagöverträdelser m.m. Datainspektionens tillstånd krävs för att behandla andra uppgifter än hälsa och lagöverträdelser i ett kvalitetsregister.

Socialdataskyddsutredningen har föreslagit en annan formulering. Uppgifter om hälsa får registreras i regionala och nationella kvalitetsregister. Andra sådana känsliga personuppgifter får behandlas i nationella och regionala kvalitetsregister endast om regeringen eller den myndighet som regeringen bestämmer i enskilda fall medger det. I utredningens förslag finns en hänvisning i PDL till art. 9.1 som reglerar vad som utgör känsliga personuppgifter.

Som känsliga personuppgifter enligt dataskyddsförordningen avses personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Det har alltså tillkommit några nya kategorier av känsliga personuppgifter, nämligen genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person och uppgifter om sexuell läggning.

Förslaget från utredningen innebär en begräsning jämfört med idag för registrering av genetiska uppgifter eftersom dataskyddsförordningen gör åtskillnad mellan uppgifter om ”hälsa” och genetiska uppgifter.

I dagsläget registrerar ett flertal Nationella Kvalitetsregister genetiska uppgifter. Socialdataskyddsutredningen skriver att om genetiska uppgifter också utgör uppgift om hälsa, får sådana uppgifter registreras i kvalitetsregister utan särskilt tillstånd av regeringen eller den myndighet regeringen bestämmer. Utredningen anför dock att eftersom det inte har framkommit något behov av att behandla sådana personuppgifter om hälsa (sic!), som samtidigt omfattas av någon av de nya kategorierna av känsliga personuppgifter, saknas det dock anledning att införa ett sådant förtydligande i PDL (SOU 2017:66 s. 360).

Utredningen uttalande skapar osäkerhet om vad som gäller. CPUA-myndighet som idag registrerar eller avser att registrera genetiska uppgifter i Nationella Kvalitetsregister rekommenderas därför ansöka om tillstånd för behandling av genetiska uppgifter hos Datainspektionen den 25 maj 2018 eller kort därefter.

Det återstår att se om utredningens förslag består i regeringens förväntade proposition om ändringar i rådande registerförfattningar med anledning av dataskyddsförordningen eller om regeringen avser att göra förtydliganden i denna fråga avseende kvalitetsregister.

11. SE ÖVER INFORMATION TILL REGISTRERADE

Dataskyddsförordningen ställer krav på personuppgiftsansvariga att informera registrerade om behandling av personuppgifter (art. 12.1, 13 och 14). Eftersom öppenhet är en del av de grundläggande dataskyddsprinciperna i förordningen, får informationsskyldigheten anses ha

skärpts. En personuppgiftsansvarig måste därför kunna ”visa” att kravet på öppenhet är uppfyllt gentemot de registrerade (art. 5.2). Artikel 29-arbetsgruppen har för övrigt publicerat en vägledning om informationsskyldigheten enligt dataskyddsförordningen.

En informationsskyldighet regleras både i personuppgiftslagen och i PDL. Dataskyddsförordningen ställer dock fler krav än idag på innehållet i informationen till registrerade. Bland nyheterna kan nämnas att den personuppgiftsansvarige ska informera om kontaktuppgifter till dataskyddsombud, laglig (rättslig) grund för behandlingen, lagringsperioden och kriterier för fastställande av perioden, rätt att inge klagomål till tillsynsmyndigheten och, om uppgifterna samlas in från någon annan än den registrerade, varifrån uppgifterna kommer samt om ursprunget är allmänna källor. Därutöver ska den personuppgiftsansvarige också informera om vilka rättigheter den registrerade har (se art. 13 respektive 14).

Enligt PDL ska patienten också informeras om rätten att när som helst få uppgifter om sig själv utplånade ur kvalitetsregistret. Vidare, enligt det förslag till ändringar i PDL som lämnats av Socialdataskyddsutredningen,

- den uppgiftsskyldighet som kan följa av lag eller förordning,
- de sekretess- och säkerhetsbestämmelser som gäller för uppgifterna och behandlingen
- rätten enligt 8 kap. 5 § PDL att få information om den direktåtkomst och elektroniska åtkomst som förekommit,
- rätten enligt artikel 82 dataskyddsförordningen och 8 kap. 1 § lagen med kompletterande bestämmelser till EU:s dataskyddsförordning till skadestånd och
- vad som gäller i fråga om sökbegrepp, direktåtkomst och utlämnande av uppgifter på medium för automatiserad behandling

Både vårdgivare som registrerar uppgifter i kvalitetsregister och CPUA-myndigheten har en skyldighet att informera patienter om personuppgiftsbehandlingen i kvalitetsregister. Enligt artikel 12.1 ska informationen lämnas *skriftligen* till den registrerade, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form.

Av skäl 61 framgår att information om behandling av personuppgifter som rör den registrerade bör lämnas till honom eller henne vid den tidpunkt då personuppgifterna samlas in från den registrerade eller, om personuppgifterna erhålls från en annan källa, inom en rimlig period, beroende på omständigheterna i fallet. Om personuppgifter legitimt kan lämnas ut till en annan mottagare, bör de registrerade enligt skäl 61 informeras första gången personuppgifterna lämnas ut till denna mottagare.

Dataskyddsförordningen innehåller även undantag från informationsskyldigheten. Om den registrerade redan förfogar över informationen om personuppgiftsbehandlingen och vem som behandlar dennes personuppgifter behöver inte information lämnas (se art. 13 och 14). Undantaget är tillämpligt oavsett om uppgifterna samlats in från den registrerade eller från någon annan än den registrerade. Då måste den personuppgiftsansvarige kunna ”visa” att den registrerade redan har fått information om personuppgiftsbehandlingen, bl.a. på vilket sätt och

när, och att inte personuppgiftsbehandlingen förändrats sedan dess för att kunna undgå sin informationsplikt.

Sammantaget innebär förändringarna att registerorganisationen för ett Nationellt Kvalitetsregister rekommenderas se över informationen till registrerade före den 25 maj 2018 samt rutiner för att uppfylla informationsplikten. Både rapporterande vårdgivare och CPUA-myndigheten har ett ansvar i dessa delar. Styrgruppen för ett Nationellt Kvalitetsregister har ett samordnande ansvar. Även RCO kan bistå flera register med stöd och översyn. Eftersom patienten som regel har kontakt med bara rapporterande vårdgivare, och ska få information innan personuppgifter behandlas i ett kvalitetsregister (7 kap. 3 § PDL), ligger en stor del av ansvaret för att informera om registerbehandlingen i kvalitetsregister samt rätten att slippa förekomma där hos dessa.

Vårdgivare rekommenderas att uppfylla dataskyddsförordningens krav på informationsskyldigheten genom information i kallelse till vårdbesök. Med stöd av en kopia av kallelsen kan vårdgivaren ”visa” att patienten fått information om behandlingen av personuppgifter i ett kvalitetsregister.

Är kallelsen skriftlig kan den innehålla en kort skriftlig information om personuppgiftsbehandlingen i det specifika kvalitetsregister där patientens uppgifter registreras samt en länk till antingen vårdgivarens eller aktuellt registers hemsida där en fullständig information finns alternativt en adress där den fördjupade informationen kan beställas inför vårdbesöket. Vårdgivare ska också kunna lämna fullständig information vid vårdbesöket på den registrerades begäran, t.ex. i ett informationsblad.

Skickas kallelse till eller bekräftelse av vårdbesök per sms bör det likaledes innehålla kort information om behandlingen av personuppgifter i kvalitetsregister och en länk till vårdgivarens hemsida med allmän information om kvalitetsregister och enskildas rättigheter. Att använda en länk till det specifika register som registrerar uppgifter i sms kan röja vad för slags diagnos eller sjukdom individen söker vård för. Enligt Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården förutsätter påminnelser och kallelser i klartext över öppna nät att patienten bl.a. samtyckt till förfarandet och att sådana kallelser och påminnelser inte avslöja detaljer om patientens hälsotillstånd eller andra personliga förhållanden (3 kap. 17 §). Kallelse per sms torde kräva som kompletterande rutin – för att uppfylla informationsskyldigheten – att patienten vid första besök hos vårdgivaren alltid får en informationsfolder om det specifika kvalitetsregister som dennes uppgifter rapporteras till.

Om rapporterande vårdgivare uppfyller sin informationsplikt korrekt, dvs. ”skriftligen” till den registrerade och senast vid tidpunkten då uppgifterna samlas in, behöver enligt dataskyddsförordningen CPUA-myndigheten inte uppfylla sin informationsplikt eftersom den registrerade redan förfogar över informationen (art. 14.5). Det är dock lämpligt att presentera fullständig information om personuppgiftsbehandlingen på kvalitetsregistrets hemsida till vilken en vårdgivare kan hänvisa patienten om vårdgivaren saknar en egen hemsida med information eller om patienter söker efter eller begär information (art. 13). Det bör vara en

strävan för varje registerorganisation att erbjuda så många informationskanaler som möjligt för patienter. CPUA-myndigheten rekommenderas i samverkan med RCO att aktivt stödja rapporterande vårdgivare med underlag för att de ska kunna ge korrekt information om bl.a. registrets ändamål.

Om det inte är möjligt att lämna informationen innan personuppgiftsbehandlingen påbörjas, ska den lämnas så snart som möjligt därefter (7 kap. 3 § patientdatalagen). Situationen kan uppstå om patienten vårdas akut och uppgifter från vårdtillfället registreras i ett kvalitetsregister. Patienten kan vid vårdtillfället vara medvetslös och även vid rapporteringstillfället. En rekommenderad rutin är att ge patienten information om behandlingen av personuppgifter i ett kvalitetsregister vid utskrivning i form av en informationsfolder.

Informationen ska vara utformad på ett sätt som kan förstås av den registrerade. När det gäller patienter som inte talar svenska bör vårdgivare se till att någon översätter informationen eller att det finns skriftliga informationsblanketter på flera språk som tagits fram av CPUA-myndigheten, rapporterande vårdgivare och styrgrupp tillsammans. RCO kan också medverka i ett sådant arbete.

På www.kvalitetsregister.se kommer det att fr.o.m. mars finnas anpassade mallar till dataskyddsförordningen för att uppfylla informationsplikten för berörda rapporterande vårdgivare och kvalitetsregister.

12. SE ÖVER RUTINER FÖR SAMTYCKE

Enligt PDL får en vårdgivare registrera uppgifter i ett kvalitetsregister och CPUA-myndigheten behandla uppgifterna utan den registrerades samtycke, såvida denne har fått korrekt information om personuppgiftsbehandlingen före registrering sker. Bl.a. ska den registrerade få information om rätten att motsätta sig att förekomma i ett kvalitetsregister, s.k. opt-out. Denna ordning förväntas fortsatt gälla när dataskyddsförordningen träder i kraft (se Socialdataskyddsutredningens betänkande, SOU 2017:66).

För vuxna personer som har permanent nedsatt beslutsförmåga får personuppgifter behandlas i ett nationellt eller regionalt kvalitetsregister om 1. hans eller hennes inställning till sådan personuppgiftsbehandling så långt som möjligt klarlagts, och 2. det inte finns anledning att anta att han eller hon skulle ha motsatt sig personuppgiftsbehandlingen (7 kap. 2 a § PDL). Även beträffande denna kategori av patienter gäller att personuppgifter i ett kvalitetsregister ska så snart som möjligt utplånas, om det efter att personuppgiftsbehandlingen har påbörjats finns anledning att anta att den enskilde skulle motsätta sig den.

Personuppgiftsbehandling i regionala och nationella kvalitetsregister är således tillåten enligt PDL även utan den registrerades samtycke (prop. 2007/08:126 s. 188). Vissa kvalitetsregister inhämtar emellertid ett uttryckligt samtycke av registrerade för registrering av personuppgifter i kvalitetsregister. Samtycket ska enligt Socialstyrelsens föreskrifter (HSLF-FS 2016:40) dokumenteras eller registreras av vårdgivare i journalsystemet. Anledningen till användningen av samtycke är att regeringen har anfört i förarbetena till PDL att den omständigheten att det

inte uppställs krav på särskilt samtycke till registrering i kvalitetsregister givetvis inte innebär att vårdgivare inte får tillämpa en ordning där samtycke, uttryckligt eller inte, inhämtas (prop. 2007/08:126 s.189).

Det erinras att ett flertal krav ska vara uppfyllda för ett lagligt samtycke. Det ska vara informerat, frivilligt, otvetydigt och särskilt. Beträffande kravet på ”frivilligt” framgår av skäl 43 i dataskyddsförordningen att samtycke inte bör användas som laglig (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. I det senare fallet är det ”osannolikt att samtycket har lämnats frivilligt när det gäller alla förhållanden som denna särskilda situation omfattar”.

Om behandlingen i ett kvalitetsregister grundar sig på samtycke, ska den personuppgiftsansvarige dessutom kunna ”visa” att den registrerade har samtyckt till behandling av sina personuppgifter (art. 7.1). Eftersom personuppgiftsbehandlingen avser känsliga personuppgifter (hälsa) ska samtycket dessutom vara ”uttryckligt” (art. 9.2 a). Det innebär att samtycket måste komma till uttryck på ett särskilt tydligt sätt, helst i skriftlig form.

Till den lagliga grunden samtycke är vissa rättigheter knutna, bl.a. rätten till dataportabilitet (art. 20). Rättigheten innebär en rätt för den registrerade att själv kunna ladda ner uppgifter till sin egen dator som han eller hon själv tillhandahållit den personuppgiftsansvarige samt en rätt att få uppgifter överförda till en annan mottagare i ett ”strukturerat, allmänt erkänt och maskinläsbart format”. Denna rättighet, även om den formellt är tillämplig på CPUA-myndighetens personuppgiftsbehandling i ett kvalitetsregister om den lagliga grunden är ”samtycke”, kan dock inte åberopas av den registrerade/patienten. Det beror på att ett av rekvisiten, ”…personuppgifter som…han eller hon har tillhandahållit den personuppgiftsansvarige…” (art. 20.1), inte är uppfyllt. Det är ju vårdgivare som tillhandahåller CPUA-myndigheten uppgifter, inte den registrerade.

Samma bedömning gäller PROM-uppgifter (motsvarande). Sådana uppgifter får registreras av en patient i ett kvalitetsregister endast med vårdgivarens tillstånd eftersom det är bara vårdgivare enligt PDL som får registrera uppgifter i ett kvalitetsregister. Det är således inte den registrerade som själv tillför uppgifter till registret utan i juridisk mening enbart vårdgivaren. Vårdgivaren eller CPUA-myndigheten har alltid rätt att avbryta PROM-registrering (motsvarande).

Till den lagliga grunden samtycke är även rätten att bli bortglömd knuten (art. 17.1). Den registrerade har rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få sina personuppgifter raderade och den personuppgiftsansvarige ska vara skyldig att utan onödigt dröjsmål radera personuppgifter om bl.a. den registrerade återkallar det samtycke på vilket behandlingen grundar sig enligt artikel 6.1 a eller artikel 9.2 a och det finns inte någon annan rättslig grund för behandlingen. Eftersom vårdgivare och CPUA-myndigheten förfogar över en annan rättslig grund, nämligen ”uppgifter av allmänt intresse” i dataskyddsförordningen (art. 5.1 e), kan den registrerade nekas att bli bortglömd. En sådan begäran har emellertid av CPUA-myndigheten och rapporterande vårdgivare uppfattas som en begäran enligt 7 kap. 2 §

andra stycket PDL att slippa förekomma i registret och att få sina uppgifter utplånade. Det är lämpligt att även informera registrerade om denna uppfattning, om registrering i registret sker med stöd av ett samtycke.

Som framgår medför dataskyddsförordningen begränsade möjligheter för myndigheter, t.ex. CPUA-myndigheter och vårdmyndigheter, att behandla personuppgifter i kvalitetsregister med stöd av ett samtycke. Samtycke kräver vidare mer administration i form av hantering av skriftliga samtycken. CPUA-myndigheten riskerar vidare att handlägga ansökningar om rättigheter som egentligen inte är tillämpliga på behandlingen av personuppgifter i kvalitetsregister, men som måste besvaras och ger därmed upphov till onödig administration.

I många fall är sannolikt det samtycke som rapporterande vårdgivare inhämtar från patienter en kontrollåtgärd för att säkerställa att den enskilde förstått tidigare lämnad information (t.ex. i en kallelse) om att bl.a. registrering av hans eller hennes uppgifter kommer att ske i ett kvalitetsregister och de rättigheter som denne har. Ett slags integritetshöjande åtgärd, inte en ny laglig grund för behandling av personuppgifter. Dataskyddsförordningen hindrar inte sådana kontroller. Samtycket behöver inte vara ”uttryckligt”, och det räcker att dokumentera det i patientjournalen.

Det är CPUA-myndigheten tillsammans med rapporterande vårdgivare som äger frågan huruvida ett samtycke ska användas som laglig grund eller en integritetshöjande åtgärd för personuppgiftsbehandlingen i ett Nationellt Kvalitetsregister i dialog med ansvarig förvaltning för registret och styrgruppen för registret. Rekommendationen är att använda samtycke som en integritetshöjande funktion, dvs. kontrollera att en registrerad/patient förstått innebörden av den information han eller hon har fått, bl.a. rätten att slippa förekomma i ett kvalitetsregister. Samtycke som laglig grund bör inte användas för kvalitetsregister.

13. UTFÖRA DATASKYDDSKONSEKVENSBEDÖMNINGAR

Förordningen ställer särskilda krav på personuppgiftsansvariga som vill behandla personuppgifter på ett sätt som kan medföra stora integritetsrisker för enskilda. Om den personuppgiftsansvarige avser att utföra en riskfylld personuppgiftsbehandling, t.ex. en storskalig hantering av patientuppgifter, måste denne först göra en noggrann analys av vilka konsekvenser behandlingen kan få för enskilda, en s.k. dataskyddskonsekvensbedömning (art. 35). Artikel 29-arbetsgruppen har publicerat en vägledning för dataskyddskonsekvensbedömningar.

Sådan riskfylld behandling kan till exempel vara storskaliga register som innehåller känsliga personuppgifter, t.ex. patientuppgifter, profilering eller omfattande kameraövervakning på allmän plats. Även molntjänster med lagring av data utan för Sveriges gränser kan utgöra en riskfylld behandling. Om konsekvensbedömningen visar att risken för enskildas fri- och rättigheter är fortsatt hög, trots kompensatoriska åtgärder, måste den personuppgiftsansvarige samråda (förhandssamråd) med Datainspektionen innan behandlingen får påbörjas.

Enligt dataskyddsförordningen ska Datainspektionen och andra tillsynsmyndigheter i medlemsländerna upprätta och offentliggöra en förteckning över det slags

behandlingsverksamheter som omfattas av kravet på en konsekvensbedömning avseende dataskydd (art. 35.4). Datainspektionen får också upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som inte kräver någon konsekvensbedömning avseende dataskydd (art. 35.5). För närvarande saknas sådana förteckningar från Datainspektionen.

En konsekvensbedömning behöver enligt dataskyddsförordningen inte göras vid behandling som utförs med stöd av artikel 6.1 c eller e i dataskyddsförordningen (rättslig förpliktelse, allmänt intresse eller myndighetsutövning) om en konsekvensutredning redan har genomförts av lagstiftaren vid antagandet av den reglering som utgör den rättsliga grunden för behandlingen (art. 35.10).

Det skulle å ena sidan tala för att CPUA-myndigheten inte skulle behöva göra en konsekvensbedömning eftersom lagstiftaren i många avseenden tagit hänsyn till enskildas fri- och rättigheter beträffande regionala och nationella kvalitetsregister i PDL, t.ex. att enbart vårdgivare får ha direktåtkomst till de uppgifter som de själva registrerat om en patient och patientens rätt att motsätta sig registrering i ett kvalitetsregister.

Å andra sidan har denna konsekvensutredning gjorts mot dataskyddsdirektivet, inte mot den nya dataskyddsförordningen. Det skulle tala för att CPUA-myndigheten måste göra en konsekvensbedömning för varje register.

Frågan får bevakas av CPUA-myndigheten i det fortsatta lagstiftningsarbetet med anledning av dataskyddsförordningen. Om ingen klarhet i frågan lämnas av regeringen kan alternativt Datainspektionen förväntas tydliggöra skyldigheten i den förteckning som inspektionen ska offentliggöra enligt art. 35.4 över verksamheter som ska göra en dataskyddskonsekvensbedömning. SKL bevakar frågan, och eventuellt återkomma med information i denna fråga till registerorganisationen.

Det erinras för övrigt att personuppgiftsbiträden har en skyldighet att biträda personuppgiftsansvariga med konsekvensbedömningar (art. 28.3 f). Leverantörer som driftar kvalitetsregister på uppdrag av CPUA-myndigheten har således en skyldighet att biträde den senare med konsekvensbedömningar.

14. ARBETA AKTIVT MED SKYDDET FÖR PERSONUPPGIFTER OCH IAKTTA INBYGGT DATASKYDD OCH DATASKYDD SOM STANDARD

I dataskyddsförordningen finns en generell skyldighet för både personuppgiftsansvariga och personuppgiftsbiträden att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter samt för att i övrigt uppfylla kraven i förordningen både när beslut fattas om hur behandlingen ska genomföras och under hela den fortsatta behandlingen (art. 32). Vilka åtgärder som behövs beror på uppgifternas art, omfattning och syfte med behandlingen, liksom vilka risker för enskildas rättigheter och friheter som behandlingen kan innebära.

Åtgärderna kan till exempel vara pseudonymisering, som medför att uppgifterna inte går att koppla till en enskild person utan ytterligare information (nyckel) som hålls avskild, eller

dataminimering, det vill säga att endast behandla de uppgifter som är nödvändiga för varje enskilt ändamål. Det ställs även krav på kontinuitetsplanering och penetrationstester (art. 32.1 c och d).

Som vägledning för skyddet av personuppgifter i regionala och nationella kvalitetsregister rekommenderas CPUA-myndigheten att iaktta de grundläggande dataskyddsprinciperna i art. 5.1, t.ex. att inte samla in mer information än vad som behövs, inte ha kvar informationen längre än nödvändigt och inte använda uppgifterna till något annat än vad som var syftet när de samlades in. Genom att ta hänsyn till dessa principer när man utvecklar nya eller ändrar befintliga kvalitetsregister blir det enklare för både CPUA-myndigheten och rapporterande vårdgivare att uppfylla reglerna i förordningen. Att bygga in dataskydd i systemen kallas inbyggt dataskydd och regleras uttryckligen i förordningen (art. 25.1). Datainspektionen har publicerat en vägledning om inbyggt dataskydd som kan vara till hjälp, https://www.datainspektionen.se/Documents/faktablad-inbyggd-integritet.pdf.

Med dataskydd som standard avses att den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att – i standardfallet – säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter – i standardfallet – inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer (art. 25.2)

Vidare ställs det krav på skydd för personuppgifter i PDL och Socialstyrelsens föreskrifter om journalföring och behandling av personuppgifter inom hälso- och sjukvården (HSLF-FS 2016:40) som måste iakttas av både rapporterande vårdgivare och CPUA-myndigheten.

Manólis Nymark
Kansliet för Nationella Kvalitetsregister
Sveriges Kommuner och Landsting