Rekommendationer till Nationella kvalitetsregister om dataskyddsförordningen GDPR

Manólis Nymark

Nationellt system
för kunskapsstyrning
Hälso- och sjukvård
SVERIGES REGIONER I SAMVERKAN

Inledning

Denna orientering syftar till att uppmärksamma i första hand centralt personuppgiftsansvariga myndigheter (CPUA-myndigheter) för Nationella Kvalitetsregister på EU:s dataskyddsförordning (dataskyddsförordningen). 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.

Dataskyddsförordningen gäller som lag i Sverige och EU:s övriga medlemsländer. Den kompletteras av lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) och särskilda registerförfattningar, till exempel patientdatalagen (PDL) (2008:335; PDL). 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. PDL. En särskild utredning, Socialdataskyddsutredningen (SOU 2017:66), granskade patientdatalagen med anledning av dataskyddsförordningen. Utredningen bedömde att PDL i stort sett är förenlig med förordningen och föreslog endast mindre justeringar i lagen för att anpassa den.

Manólis Nymark, jurist, Stödfunktionen för Nationella kvalitetsregister

2023-12-01

Stockholm

Innehållsförteckning

Fatta beslut om CPUA-myndighet

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 regionstyrelser personuppgiftsansvariga för kvalitetsregister. Även andra nämnder kan givetvis vara personuppgiftsansvariga.

Dataskyddsförordningen innebär ett skärpt ansvar för personuppgiftsbehandlingen och dataskyddet för personuppgifter. Det finns mot denna bakgrund anledning för varje styrgrupp att se över huvudmannaskapet för eget Nationellt Kvalitetsregister. Fyra frågor ska kontrolleras:

- Är huvudmannen för ett kvalitetsregister en myndighet?
- Är det tydligt för rapporterande vårdgivare vem som är personuppgiftsansvarig för ett kvalitetsregister?
- Är det tydligt för patienter 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. Lösningen är att byta huvudmannaskapet till en myndighet. Sondering om lämplig CPUA-myndighet bör ske med RCO. När en överenskommelse nåtts med en region som ska ta över ansvaret för registret, kontakta dataskyddsombudet hos nuvarande huvudman eller övertagande region för rådgivning hur bytet ska genomföras, bland annat 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 av regionstyrelsen eller en sjukhusstyrelse när omständigheterna kring var det ligger eller bör ligga har utretts. Informera om personuppgiftsansvaret 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, det vill säga vilken avdelning eller förvaltning inom CPUA-myndigheten som ansvarar för registret så att ansvaret är transparent inom myndigheten för både medarbetare och patienter och 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 för 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.

CPUA-myndighetens skyldigheter

CPUA-myndigheten har en rad skyldigheter enligt dataskyddsförordningen. Regionstyrelsen är som regel CPUA-myndighet för Nationella Kvalitetsregister. I huvudsak måste följande skyldigheter iakttas:

- Följa de grundläggande dataskyddsprinciperna
- Se över rutiner för bevarande och gallring
- Kunna visa ansvarsskyldighet
- Utse dataskyddsombud
- Etablera rutiner för hantering av personuppgiftsincidenter
- Upprätta en förteckning över kategorier av personuppgifter
- Teckna ett personuppgiftsbiträdesavtal med leverantören
- Etablera rutiner för att snabbt och smidigt tillgodose registrerads rättigheter
- Etablera rutiner för att underrätta tredje part om rättelse och begränsning
- Iaktta begränsningar att registrera genetiska uppgifter
- Se över information till registrerade
- Se över rutiner för samtycke
- Utföra dataskyddskonsekvensbedömningar
- 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

Dataskyddsförordningen innehåller ett flertal grundläggande dataskyddsprinciper som ska genomsyra CPUA-myndighetens behandling av personuppgifter i kvalitetsregister. Dessa finns i artikel 5 dataskyddsförordningen. Principerna är följande:

Personuppgifter:

- ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (principerna om laglighet, korrekthet och öppenhet).
- 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).
- ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (principen om uppgiftsminimering).
- ska vara riktiga 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 riktighet).
- 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).
- 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 Teckna ett personuppgiftsbiträdesavtal med leverantören) ska myndigheten säkerställa att biträdet i motsvarande utsträckning följer dataskyddsprinciperna genom utfärdade instruktioner.

2. 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 primära ändamålet att systematiskt och fortlöpande utveckla och säkra vårdens kvalitet. Arkivmyndigheten inom en region (normalt regionstyrelsen) får dock enligt samma paragraf föreskriva att personuppgifter får bevaras för arkivändamål av allmänt intresse, vetenskapliga eller historiska ändamål eller statistiska ändamål.

Regleringen i 7 kap. 10 § PDL får anses utgöra ett undantag från principen om lagringsminimering i artikel 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, till exempel. statistik eller forskning , vilka är tillåtna användningsområden för 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 kvalitetssäkring.

Saknas föreskrifter härom i dokumenthanteringsplan (motsvarande) för ett kvalitetsregister, men personuppgifterna i registret är avsedda att användas för att ta fram statistik över behandlingsåtgärder med mera 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, CPUA-myndigheten, inte bara ansvarar för att de grundläggande dataskyddsprinciperna följs utan ska också kunna ”visa” att de efterlevs (artikel 5.2). Av artikel 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 (artikel 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 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 (artikel 37.1). Under alla omständigheter ska myndigheter alltid ha ett dataskyddsombud.

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

Europeiska dataskyddsstyrelsen (EDPB) har publicerat en vägledning om dataskyddsombud, läs mer på deras webbplats: https://edpb.europa.eu/edpb_en

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 Integritetsskyddsmyndigheten inom 72 timmar, om det inte är osannolikt att incidenten medför risker för enskildas fri- och rättigheter (artikel 33.1). Personuppgiftsbiträdren ska enligt dataskyddsförordningen underrätta den

personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident, det vill säga inom en betydligt kortare tidsfrist än 72 timmar (artikel 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 (artikel 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 Integritetsskyddsmyndigheten ska ligga i registerorganisation så att anmälan kan göras i rätt tid. Rutiner för upptäckt och anmälan av personuppgiftsincidenter bör framgå av befintligt kvalitetsledningssystem.

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

Europeiska dataskyddsstyrelsen (EDPB) har publicerat en vägledning om personuppgiftsincidenter enligt dataskyddsförordningen. Läs mer på deras webbplats: läs mer på deras webbplats: https://edpb.europa.eu/edpb_en

6. Upprätta förteckning över kategorier av personuppgifter

Dataskyddsförordningen (artikel 30.1) kräver att varje personuppgiftsansvarig organisation ska föra ett register över personuppgiftsbehandlingar som utförs i den verksamhet som den personuppgiftsansvarige ansvarar för.

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 Integritetsskyddsmyndigheten.

7. Teckna ett personuppgiftsbiträdesavtal med leverantörer

Dataskyddsförordningen ställer krav på att den personuppgiftsansvarige ska teckna ett personuppgiftsbiträdesavtal med den som behandlar personuppgifter för den personuppgiftsansvariges räkning, ett så kallat personuppgiftsbiträde. Som exempel på typiska personuppgiftsbiträden kan nämnas leverantörer av olika digitala tjänster. Även Inera AB är ett personuppgiftsbiträde.

Dataskyddsförordningen ställer särskilda krav på innehållet i ett personuppgiftsbiträdesavtal (artikel 28.3), bland annat föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade samt den

personuppgiftsansvariges skyldigheter och rättigheter, till exempel 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 (artikel 28.1). 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, bland annat 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, till exempel 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 (artikel 28.2). Instruktioner till personuppgiftsbiträdet om personuppgiftsbehandlingen ska vara skriftliga för att uppfylla kravet på ansvarsskyldighet.

SKR-koncernen har publicerat ett personuppgiftsbiträdesavtal som är anpassat för regioner och kommuners anlitande av personuppgiftsbiträden. Läs mer på www.skr.se

8. Rutiner för att snabbt och smidigt tillgodose registrerades rättigheter

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

Den rättsliga grunderna för behandling av personuppgifter i regionala och nationella kvalitetsregister är dels ”uppgifter av allmänt intresse” (art. 6.1 e) och dels 7 kap. PDL. Därutöver är villkoren för att behandla känsliga personuppgifter uppfyllda genom 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 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)

I det följande kommenteras några rättigheter

Enligt artikel 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 benämndes 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 (artikel 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 (artikel 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 (artikel 18.1 c).

Rätten att bli bortglömd (artikel 17) är inte tillämplig på kvalitetsregister eftersom PDL innehåller en motsvarande rätt att få bli utplånad. Rätten till dataportabilitet (artikel. 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 (artikel 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 (artikel 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 liknar 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 (artikel 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 (artikel 12.3). CPUA-myndigheten bör därför erbjuda elektroniska möjligheter för registrerade att framföra sina

rättigheter, till exempel 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, så kallade digitala brevlådor som kan användas.

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, till exempel rättelse, eller att rättigheten är beskuren i PDL, ska beslutet meddelas skriftligen med besvärshänvisning och i rekommenderat brev. Överklagandebestämmelser finns i lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen).

9. Etablera rutiner för att underrätta tredje part om rättelse och begränsning

Enligt artikel 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 artikel 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 artikel 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, det vill säga att inga namn och personnummer har lämnats ut till forskningshuvudmannen, torde skyldigheten enligt artikel 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 artikel 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 artikel 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, det vill säga rapporterande vårdgivare.

Artikel 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, det vill säga rätta uppgiften eller begränsa behandlingen.

10. Iaktta begränsningar för att registrera genetiska uppgifter

Enligt 7 kap. 8 § tredje stycket PDL får uppgifter om hälsa behandlas i nationella och regionala kvalitetsregister. Av bestämmelsen framgår också att andra känsliga personuppgifter får behandlas i nationella och regionala kvalitetsregister endast om regeringen eller den myndighet som regeringen bestämmer i enskilda fall medger det. 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. Dataskyddsförordningen gör alltså skillnad på uppgifter om ”hälsa” respektive ”genetiska uppgifter”.

I dagsläget registrerar ett flertal Nationella Kvalitetsregister genetiska uppgifter. För att få behandla genetiska uppgifter i ett kvalitetsregister behövs därför som huvudregel ett medgivande från Integritetsskyddsmyndigheten. När genetiska uppgifter innefattas i uppgifter om en persons hälsotillstånd, är det Integritetsskyddsmyndighetens bedömning, att det inte krävs ett särskilt medgivande från myndigheten för att få behandla dessa uppgifter. Det innebär att den som är personuppgiftsansvarig för ett kvalitetsregister inte behöver ansöka om ett medgivande hos Integritetsskyddsmyndigheten för att få behandla genetiska uppgifter, om dessa uppgifter också är uppgifter om hälsa.

Integritetsskyddsmyndighetens uttalande finns här www.imy.se

11. Information till registrerade

Dataskyddsförordningen ställer krav på personuppgiftsansvariga att informera registrerade om behandling av personuppgifter (artikel 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 (artikel 5.2).

Bland annat ska den personuppgiftsansvarige informera registrerade patienter om kontaktuppgifter till dataskyddsombud, 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 artikel 13 respektive 14).

Enligt PDL ska patienten också informeras om:

- Rätten att när som helst få uppgifter om sig själv utplånade ur kvalitetsregistret,
- den uppgiftsskyldighet som kan följa av lag eller förordning,
- de sekretess- och säkerhetsbestämmelser som gäller för uppgifterna och behandlingen,
- rätten enligt 4 kap. 4 § PDL att i vissa fall begära att uppgifter spärras,
- rätten enligt 7 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 i dataskyddsförordningen 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 artikel 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, bland annat på vilket sätt och när, och att inte personuppgiftsbehandlingen förändrats sedan dess för att kunna undgå sin informationsplikt.

Både rapporterande vårdgivare och CPUA-myndigheten har ett ansvar för att informera registrerade. Styrgruppen för ett Nationellt Kvalitetsregister har ett samordnande ansvar. Även RCO kan bistå flera register med stöd och översyn. Eftersom patienter 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.

Stödfunktionen för Nationella kvalitetsregister har publicerat en vägledning om information till registrerade i kvalitetsregister och mallar för att uppfylla informationsskyldigheten, både på svenska och ett flertal andra språk. www.kvalitetsregister.se

12. 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. Bland annat ska den registrerade få information om rätten att motsätta sig att förekomma i ett kvalitetsregister, så kallad opt-out.

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 vårdgivare får använda samtycke, trots att det inte behövs (prop. 2007/08:126 s.189).

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 (artikel. 7.1). Eftersom personuppgiftsbehandlingen avser känsliga personuppgifter (hälsa) ska samtycket dessutom vara ”uttryckligt” (artikel 9.2 a). Det innebär att samtycket måste komma till uttryck på ett särskilt tydligt sätt, helst i skriftlig form.

Till den rättsliga grunden samtycke är vissa rättigheter knutna, bland annat rätten till dataportabilitet (artikel 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…” (artikel 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 ska som regel registreras av vårdgivare i kvalitetsregister och inte av CPUA-myndigheten (se SKR publikation

Patientrapporterade mått – insamling och ansvar). Det är således inte den registrerade som själv tillför uppgifter till registret utan i juridisk mening enbart vårdgivaren.

Till den rättsliga grunden samtycke är även rätten att bli bortglömd knuten (artikel. 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 bland annat 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 (artikel 5.1 e), kan den registrerade nekas att bli bortglömd. En sådan begäran har emellertid av CPUA-myndigheten och rapporterande vårdgivare uppfattats 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, till exempel 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 (till exempel i en kallelse) om att bland annat registrering av hans eller hennes uppgifter kommer att ske i ett kvalitetsregister och de rättigheter som denne har. En slags integritetshöjande åtgärd, men inte en ny rättslig 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 rättslig grund eller som en integritetshöjande åtgärd för personuppgiftsbehandlingen i ett Nationellt Kvalitetsregister i dialog med dataskyddsombudet och styrgruppen för registret. Rekommendationen är att använda samtycke enbart som en integritetshöjande funktion, det vill säga kontrollera att en registrerad/patient förstått innebörden av den information han eller hon har fått, bland annat rätten att slippa förekomma i ett kvalitetsregister. Samtycke som laglig grund bör inte användas för kvalitetsregister eftersom det inte behövs.

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, till exempel en storskalig hantering av patientuppgifter, måste denne först göra en noggrann analys av vilka konsekvenser behandlingen kan få för enskilda, en så kallad dataskyddskonsekvensbedömning (art. 35). SKR har publicerat en mall för dataskyddskonsekvensbedömningar för vård- och omsorgsverksamhet www.skr.se

Sådan riskfylld behandling kan till exempel vara storskaliga register som innehåller känsliga personuppgifter, till exempel 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 Integritetsskyddsmyndigheten innan behandlingen får påbörjas.

Enligt dataskyddsförordningen ska Integritetsskyddsmyndigheten och andra tillsynsmyndigheter i medlemsländerna upprätta och offentliggöra en förteckning över det slags behandlingsverksamheter som omfattas av kravet på en konsekvensbedömning avseende dataskydd (artikel. 35.4). Integritetsskyddsmyndigheten har publicerat en sådan förteckning över när en dataskyddskonsekvensbedömning ska göras https://www.imy.se

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 (artikel. 35.10).

Det krävs inte heller någon konsekvensbedömning för behandlingar som har kontrollerats av en tillsynsmyndighet eller ett dataskyddsombud i enlighet med artikel 20 i det tidigare dataskyddsdirektivet och vars genomförande inte har ändrats sedan föregående kontroll.

Samtliga Nationella Kvalitetsregister är äldre än dataskyddsförordningen och omfattas av PDL:s reglering sedan 2008. Även om en konsekvensbedömning genomförts före dataskyddsförordningens ikraftträdande, eller en kontroll av tillsynsmyndigheten eller ett dataskyddsombud genomförts i ett tidigare skede, rekommenderas Nationella Kvalitetsregister att upprätta eller kontinuerligt se över befintlig konsekvensbedömning. Fokus ska läggas på tekniska och organisatoriska åtgärder. Behovs- och proportionalitetsbedömningen har regering och riskdag redan gjort i samband med beredning och beslut om att anta PDL.

Det erinras för övrigt att personuppgiftsbiträden har en skyldighet att biträda personuppgiftsansvariga med konsekvensbedömningar (artikel 28.3 f). Leverantörer som tillhandahåller 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 (artikel 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 (artikel 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 artikel 5.1, såsom 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 (artikel 25.1). Europeiska dataskyddsstyrelsen (EDPB) har publicerat en vägledning om inbyggt dataskydd och dataskydd som standard som kan vara till hjälp, https://edpb.europa.eu

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 (artikel 25.2).

Stödfunktionen för Nationella kvalitetsregister

adminkvalitetsregister@skr.se