Förändringar för hälso- och sjukvården genom EU: s dataskyddsförordningen (förordningen) GDPR

Inledning

Att förstå EU: s nya dataskyddsförordning (förordningen) är viktigt för varje organisation t.ex. vårdgivare som hanterar personuppgifter. Förordningen stärker dataskyddet genom att sätta mer fokus på ansvar och säkerhet. De som behandlar personuppgifter kommer nu att tvingas inte bara att följa den nya lagstiftningen utan också visa att de har uppfyllt kraven.

Med behandling av personuppgifter avses varje åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Den nya förordningen antogs den 27 april 2016 och måste genomföras i hela EU senast den 25 maj 2018.

Bakgrund

Den nya förordningen har i princip samma mål som EU: s direktiv om dataskydd från 1995 och syftar till att göra skyddet mer lämpat för dagens tekniska miljö och att säkerställa samma skyddsnivå för dataskydd inom EU.

Genom den nya förordningen ges mindre tolkningsutrymme på nationell nivå. Inom området hälso- och sjukvård kommer det dock fortfarande att finnas vissa möjligheter att ha kompletterande lagstiftning, vägledningar och regler, eftersom det är ett område där EU tillåter en nationell lagstiftning.

Användningen av personuppgifter är avgörande inte bara för att tillhandahålla högkvalitativ hälso- och sjukvård till patienter, men också för förvaltningen av hälso- och sjukvårdens system och för medicinsk forskning.

De som arbetar inom hälso- och sjukvården använder personuppgifter inte bara för vården av enskilda patienter utan också till att:

• bättre förstå sjukdomar och förbättra behandlingar

• förstå mönster och trender inom offentlig hälso- och sjukvård

• planera tjänster som gör det bästa av begränsade resurser

• kontrollera säkerheten hos läkemedel och behandlingar, och

• jämföra kvaliteten på hälso- och sjukvården i olika områden.

De viktigaste förändringarna för hälso- och sjukvården i den nya dataskyddsförordningen

I artikel 4 (5) nämns pseudonymisering och därmed avses behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.

Enligt skäl 26[1] är uppgifter som har genomgått pseudonymisering, men som ändå kan tillskrivas en fysisk person med hjälp av ytterligare information, att se som identifierbara. För att avgöra om en person är identifierbar bör hänsyn tas till alla rimliga medel som kan komma att användas, såsom att peka ut, antingen av den registeransvarige eller av någon annan person, för att identifiera personen direkt eller indirekt. Att fastställa om medel som kan användas för att identifiera den enskilde är rimliga, bör hänsyn tas till alla objektiva faktorer, såsom kostnaderna för och den tid som krävs för identifiering, med hänsyn tagen till både tillgänglig teknik vid tidpunkten för behandlingen och teknisk utveckling.

Skäl 26 kan tolkas som om att alla pseudonymiserade uppgifter bör betraktas som personuppgifter.

Genom förordningen införs också nya definitioner (artikel 4) för personuppgifter som rör hälsa, genetiska data och biometriska uppgifter:

- uppgifter om hälsa: personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus,
- genetiska uppgifter: alla personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken för en fysisk person, vilka ger unik information om denna fysiska persons fysiologi eller hälsa och vilka framför allt härrör från en analys av ett biologiskt prov från den fysiska personen i fråga,

[1] Ett skäl i ett EU direktiv eller förordning är en förklarande text som är en del av den lagstiftning som anger skälen till bestämmelserna i en artikel.

- personuppgiftsincident; en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats

Principer för behandling av personuppgifter (artikel 5)

Principerna för behandling personuppgifter är i stort sett densamma som i direktivet från 1995, dock finns ett ökat fokus på öppenhet och på att säkerställa att lämpliga säkerhetsåtgärder vidtas.

De registeransvariga förväntas nu inte bara följa principerna, men ska också kunna visa att regelverket efterlevs på ett ansvarsfullt sätt. Det är en viktig och betydande förändring från passiv till aktiv efterlevnad som vårdgivarna bör uppmärksamma.

Ett sätt att visa att personuppgifts behandling är i överensstämmelse med lagstiftningen kan vara att anta uppförandekoder, interna riktlinjer och förfaranden.

De viktigaste principerna för skydd av personuppgifter i artikel 5 är; laglighet, korrekthet och öppenhet, ändamålsbegränsning, uppgiftsminimering, korrekthet, lagringsminimering, integritet och konfidentialitet samt ansvarsskyldighet.

Laglig behandling (artikel 6)

Den rättsliga grunden för laglig behandling av personuppgifter är i stort sett den samma som i direktivet från 1995. En viktig förändring är dock att som laglig behandling räknas inte längre den intresseavvägning som myndigheter tidigare kunde åberopa som grund för sin behandling när de utför sina uppgifter. Enligt förordningen måste myndigheter (inklusive offentliga sjukhus och övriga vårdgivare) numera kunna ange en laglig grund för sin behandling.

I Sverige finns den lagliga grunden för behandling av personuppgifter inom hälso- och sjukvården huvudsakligen i patientdatalagen. Medlemsländerna kan välja att ha en nationell lagstiftning för behandling av personuppgifter i hälso- och sjukvården.

Andra lagliga grunder för att behandla personuppgifter i förordningen:

• den registrerade har gett sitt medgivande

• behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part

• behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den registeransvarige

• behandlingen är nödvändig för att skydda vitala intressen för den registrerade eller en annan fysisk person (liv eller död)

• behandlingen är nödvändig för att utföra uppgifter av allmänt intresse eller vid myndighetsutövning.

En annan mycket viktig förändring gäller behandling för ett annat ändamål än det för vilket personuppgifterna ursprungligen har samlats in. Vårdgivarna och andra behöver analysera de nya kraven för att definiera när deras ytterligare syfte för behandling av personuppgifter kan anses vara "kompatibla". Dessa krav anges i artikel 6 (4) i förordningen.

Behandling av särskilda kategorier av personuppgifter (artikel 9)

Liksom i direktivet från 1995 utgör hälsodata en särskild kategori av data och bearbetning är därför i princip förbjuden. Andra förbjudna former av bearbetning av personuppgifter gäller: genetisk information, biometriska uppgifter och uppgifter om sexuella uppgifter läggning.

Det är värt att notera att det finns ett ökat utrymme och flexibilitet jämfört med direktivet från 1995. Numera nämns särskilt tillhandahållande och förvaltning av hälso- och sjukvårdstjänster och folkhälsoområdet som skäl för att lyfta förbudet mot behandling av särskilda kategorier av uppgifter. Detta kan underlätta samarbetet mellan offentlig och privat vård.

Villkor för samtycke (Artikel 7)

Förutsättningarna för samtycke har tydliggjorts ytterligare. Om behandlingen grundar sig på samtycke, ska den personuppgiftsansvarige kunna visa att den registrerade har samtyckt till behandlingen av sina personuppgifter. Med samtycke avses i förordningen varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.

För bearbetning av särskilda kategorier av uppgifter enligt artikel 9, måste den registrerade ge sitt uttryckliga medgivande. När samtycke används som rättslig grund, är det viktigt att notera att den "dubbla samtyckes mekanismen” ligger i linje med direktivet från 1995.

Otvetydigt samtycke krävs för behandling av personuppgifter och uttryckligt samtycke kommer att krävas för behandling av särskilda former av data (dvs. hälsouppgifter och genetiska data).

För hälso- och sjukvården är, de viktigaste undantagen från förbudet mot behandling av särskilda former av personuppgifter följande:

• uttryckligt medgivande

• skydda vitala intressen (liv eller död scenarier)

• viktigt allmänt intresse

• förebyggande yrkesmedicin, medicinska diagnoser, tillhandahållande av vård och omsorg eller behandling eller administration av hälso- eller omsorg och systemen som bygger på nationell lagstiftning eller EU-lagstiftning

• allmänt intresse när det gäller folkhälsan

• arkivering av allmänt intresse, vetenskaplig och historisk forskning, statistiska ändamål (med förbehåll för artikel 89 och nationell eller EU-lag).

Artikel 9 (3) i förordningen möjliggör en utvidgning av tillämpningsområdet för yrkesverksamma med tystnadsplikt enligt unionsrätten eller nationell lagstiftning att få tillgång till data för att tillgodose nya arbetssätt och nya vårdmodeller som användes i hela Europa.

För närvarande kan hälsouppgifter endast behandlas av "hälso- och sjukvårdpersonal enligt nationell lagstiftning eller bestämmelser som antagits av behöriga nationella myndigheter, till tystnadsplikt eller av en annan person som är ålagd en liknande tystnadsplikt ".

Med den nya förordningen utvidgas tillämpningsområdet till att omfatta ett bredare spektrum av individer som kan tillåtas bearbeta hälsodata. Närmare bestämt säger den nya texten att hälsodata och andra känsliga kategorier av uppgifter får behandlas för förebyggande yrkesmedicin, medicinska diagnoser, tillhandahållande av vård och omsorg, eller behandling eller administration av hälso- eller omsorgssystemen när dessa uppgifter behandlas "av eller under överinseende av en professionell som omfattas av tystnadsplikt enligt Unionens eller medlemsstaternas lagstiftning eller regler som fastställts av behöriga nationella organ, eller av en annan person som är ålagd tystnadsplikt enligt unionen eller medlemsstaternas lagstiftning eller regler som fastställts av behöriga nationella organ ".

Det finns en bestämmelse i förordningen (artikel 9 (4)) som möjliggör för varje land att "bibehålla eller införa ytterligare villkor, inklusive begränsningar, när det gäller behandling av genetisk information, biometriska data eller hälsouppgifter".

Inverkan på forskningen

I stort sett kommer den nya lagstiftningen upprätthålla status quo för forskning inom många områden. Ytterligare behandling för vetenskaplig forskning, statistiska eller historiska ändamål som "inte är oförenliga" med de ursprungliga ändamål för vilka

uppgifterna behandlas är tillåten. Ytterligare behandling för forskning är därför tillåtet, i enlighet med direktivet från 1995.

I artikeln om behandling för historiska, statistiska och vetenskapliga forskningsändamål (artikel 89) införs dubbla garantier och undantag som kan användas för att stödja forskningen. Detta kräver dock att medlemsstaterna lagstiftar om undantagen.

För att underlätta gränsöverskridande forskning och uppmuntra medlemsstaterna att samarbeta krävs dock viss likhet mellan de nationella tillvägagångssätten.

De garantier som införs bör också ta hänsyn till och arbeta med nuvarande tillsynsstrategier, såsom etisk kommitté godkännande. Vägledning och slutsatserna om pseudonymisering kommer också att vara av avgörande betydelse för forskare.

Registrerades rättigheter (kapitel III)

Kapitlet om rättigheter för den registrerade har stärkts avsevärt i förordningen, även om de grundläggande principerna i detta kapitel i stort överensstämde med bestämmelserna i direktivet från 1995.

Information från hälso- och sjukvården måste vara transparent, begriplig och lättillgänglig (en detaljerad förteckning över de uppgifter som ska lämnas återfinns i artiklarna 13 och 14). Informationen till de registrerade kan också tillhandahållas i kombination med standardiserade ikoner när kommissionen inför dem genom delegerade akter (artikel 12 (8)).

Rätten till rättelse och radering (Artikel 16)

Den registrerade ska ha rätt att från den registeransvarige utan onödigt dröjsmål få rättelse av personuppgifter som rör honom eller henne som är felaktiga. Med beaktande av ändamålet med behandlingen, ska den registrerade ha rätt att komplettera ofullständiga personuppgifter, bland annat genom ett kompletterande utlåtande.

När det gäller praktiska konsekvenser att detta beror det på hur "riktiga" eller "felaktig uppgifter" definieras, t.ex. om en anteckning i en patientjournal eller läkarintyg kan anses "felaktig" om patienten inte håller med det. Men i praktiken är det svårt att bevisa att ett yttrande är felaktigt.

Rätten att glömmas bort och radering av data (artikel 17) gäller inte för patientjournaler, för folkhälsoändamål eller för forskningsändamål. I Sverige finns dock sedan länge en möjlighet att få felaktig uppgifter i en patientjournal förstörda om de inte behövs för patientens vård.

Rätten till uppgifter om portabilitet (artikel 20) är en helt ny rättighet och detta måste beaktas även av hälso- och sjukvården.

De registrerade kommer att ha rätt att få del av uppgifter som behandlas med stöd av samtycke som laglig grund för bearbetning i en strukturerad samling i ett maskinläsbart format. Detta kan innebära vårdgivare kan ställas inför krav från patienter att få (kopia) av sin patientjournal i ett lämpligt format så att de kan välja att gå till en annan leverantör av vård (till exempel en privatvårdgivare) eller att få vård i ett annat europeiskt land.

Som med direktivet från 1995, finns det vissa situationer då det anses nödvändigt och proportionerligt för att begränsa registrerades rättigheter. Artikel 23 i förordningen gäller de situationer när begränsningarna kan vara lämpliga av säkerhets- och försvarsskäl.

Sådana begränsningar måste ha stöd i EU:s eller medlemsstaternas lagstiftning. Listan över potentiella begränsningar innefattar en begränsning för allmänheten i syfte att "förebygga, utreda, avslöja och åtala överträdelser av etiska regler för reglerade yrken". Den innehåller också en begränsning för "andra viktiga mål för allmänna intressen i unionen eller medlemsstaten, i synnerhet ett viktigt ekonomiskt eller finansiellt intresse ... inklusive folkhälsa och social trygghet".

En särskild utmaning för hälso- och vården kommer vara att kopior av journaler ska tillhandahållas gratis. Avgifter kan endast ta ut för ytterligare kopior (artikel 15 (3)) eller där en begäran om information är "uppenbart ogrundad eller överdriven" (artikel 12 (5)).

Allmänna skyldigheter för registeransvariga och processorer (kapitel IV)

Detta är i grunden ett nytt kapitel som tidigare låg i de nationella regeringarna som utarbetades för genomförande av direktivet från 1995.

I detta kapitel införs en ny skyldighet att dataskydd ”vid design” ska vara standard. Det är ett förhållningssätt till projekt som främjar integritet och dataskydd följs från början. Tanken är att dataskydd ska övervägas från början av ett projekt (artikel 25) och inte först i slutet.

Med tanke på kravet på registeransvariga att visa överensstämmelse med förordningen (artikel 5), är denna skyldighet ett viktigt nytt krav.

Förordningen ger tydligare definitioner av "personuppgiftsansvarig" (artikel 24), ”gemensamt personuppgiftsansvariga" (artikel 26) och "personuppgiftsbiträden" (artikel 28) i detta kapitel än i direktivet från 1995.

Dataskyddsombud (personuppgiftsombud) är nu obligatorisk för myndigheter (artikel 37-39) och för företag vars verksamhet medför särskilt riskfylld behandlingar.

Exempel på s.k. riskfyllda behandlingar, regelbunden och systematisk övervakning av registrerade i stor skala eller omfattande behandling av känsliga personuppgifter.

Enligt förordningen är det obligatoriskt att göra en bedömning av storskalig hantering av särskilda kategorier av personuppgifter (dvs. hälsouppgifter och genetiska data) (artikel 35).

Det är också viktigt att notera att "en enda bedömning kan ta upp liknande behandlingar som innebär liknande höga risker". Detta kan avsevärt bidra till att minska den administrativa bördan för vårdgivarna de när ska utför en sådan bedömning.

En anmälan av personuppgiftsincident (artikel 33) till tillsynsmyndigheten ska normalt ske inom 72 timmar och till den registrerade utan onödigt dröjsmål. Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident.

Artikel 30 säkerställer kravet att upprätthålla ett register över alla databehandling.

Det finns intressanta möjligheter för hälso- och sjukvården att ha självreglerande uppförandekoder (artikel 40) som kan ha allmän giltighet i hela EU under vissa förutsättningar.

Det kommer finnas möjlighet att ansöka om certifiering av överensstämmelse med förordningen - det kan vara av intresse för vårdgivare. Denna certifieringsprocess kommer att utarbetas under 2016 av Europeiska dataskyddsstyrelsen (för närvarande arbetsgruppen 29) och de nationella tillsynsmyndigheterna.

Striktare tillämpning av reglerna

Artikel 82 om rätten till ersättning och ansvar är kraftfullare än motsvarande bestämmelser i direktivet från 1995. Varje person som har drabbats av materiella eller immateriella skador som resultat av ett åsidosättande av förordningen, ska ha rätt till ersättning från den registeransvarige eller processorn för skadan.

En personuppgiftsansvarig eller ett personuppgiftsbiträde kan undgå ansvar om de kan bevisa att de inte på något sätt ansvariga för den händelse som orsakade skadan. Administrativa sanktioner kan också införas av de nationella tillsynsmyndigheterna i fall av bristande efterlevnad av förordningen.

Beroende på hur allvarlig överträdelsen är kan sanktionsavgifter uppgå till 4 procent av den totala årliga omsättningen eller 20 miljoner euro.