SAMORZĄD I ADMINISTRACJA

Branża medyczna już pisze własny kodeks ochrony danych osobowych

Zofia Jóźwiak
zofia.jozwiak@infor.pl

Podmioty zajmujące się ochroną zdrowia będą świecić przykładem? Wiele wskazuje na to, że tak. Bo nie czekając na wejście unijnego rozporządzenia RODO dotyczącego ochrony danych osobowych ani nowej polskiej ustawy w tym zakresie, branża już przygotowuje własne przepisy – kodeks dla sektora ochrony zdrowia dotyczący ochrony danych osobowych. To najprawdopodobniej pierwsza taka inicjatywa w UE, jeśli chodzi o tę branżę. Warta rozpropagowania, bowiem z kodeksem przystosowanym do specyfiki określonej grupy podmiotów będzie prościej dostosować się do RODO niż zastanawiać się za każdym razem samodzielnie, czy w konkretnym przypadku rozporządzenie trzeba stosować, a jeśli tak, to w jaki sposób. Dla firm zajmujących się ochroną zdrowia ma to tym większe znaczenie, że dysponują one danymi szczególnie wrażliwymi, tym samym bardziej niż inne są narażone na ewentualne spory z osobami, których prywatność zostanie naruszona.

Ostatecznego kształtu kodeksu jeszcze nie znamy, a jak wiadomo diabeł tkwi w szczegółach. Jednak biorąc pod uwagę strony zainteresowane inicjatywą, wydaje się, że są szanse na dobrą i spełniającą potrzeby wszystkich regulację. Bo wśród deklarujących udział w pracach lub przynajmniej poparcie, są i przedstawiciele dużych szpitali i mniejszych podmiotów skupionych w Porozumieniu Zielonogórskim, przedstawiciele strony rządowej i samorządów, a także powiązane z branżą medyczną korporacje, np. aptekarska. Przygotowanie branżowego dokumentu zajmie wprawdzie trochę czasu, ale zapewne ułatwi dostosowanie się do nowych ogólnounijnych przepisów, które nie zawsze są dopasowane do potrzeb podmiotów medycznych. Jeżeli wszystko pójdzie dobrze, to zakończenie prac nad kodeksem i przedstawienie projektu głównemu inspektorowi ochrony danych osobowych powinno nastąpić pod koniec tego roku. To znaczy, że jest szansa, by regulacja była gotowa przed 25 maja, czyli przed datą wejścia RODO w UE. ©℗

PIOTR NAJBUK
prawnik i lekarz w Domański Zakrzewski Palinka sp. k.

JĘDRZEJ STĘPNIOWSKI
prawnik w Domański Zakrzewski Palinka sp. k.

PAWEŁ KAŹMIERCZYK
prawnik w Domański Zakrzewski Palinka sp. k.

Sektorowe przepisy zmniejszą ryzyka prawne

Dziś bezpieczeństwo danych osobowych pacjentów pozostawia wiele do życzenia. Wejście w życie unijnego rozporządzenia RODO powinno to zmienić, zwłaszcza jeśli podmioty medyczne przygotują własne, precyzyjne regulacje w tym zakresie

Od 25 maja 2018 r. w całej Unii Europejskiej, w tym w Polsce, trzeba będzie obowiązkowo stosować się do rozporządzenia (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (tzw. ogólne rozporządzenie o ochronie danych, w skrócie RODO). Ta regulacja wprowadzi wiele nowych praw i obowiązków związanych z przetwarzaniem danych osobowych oraz zmodyfikuje znane już rozwiązania prawne.

Jedną z ważniejszych zmian jest dopuszczenie przez unijnego prawodawcę przyjmowania kodeksów postępowania przez zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające. Takie zbiory przepisów będą następnie zatwierdzane przez organ nadzorczy. Należy podkreślić, że kodeksy choć są elementem samoregulacji branżowej, to ze względu na ich formalne zatwierdzenie przez organ nadzorczy staną się quasi-prawem ograniczającym ryzyka prawne administratorów danych je stosujących. Choć nowe przepisy zaczną obowiązywać za dopiero za dziewięć miesięcy, już obecnie trwają prace nad wykorzystaniem tego typu rozwiązań w sektorze ochrony zdrowia.

Prace już trwają

Kodeks dla ochrony zdrowia ma nie tylko uporządkować i doprecyzowywać dotychczasowe, rozproszone po wielu aktach prawnych regulacje, ale także stanowić ważne narzędzie w implementacji RODO, dostępne dla wszystkich podmiotów wykonujących działalność leczniczą. 26 lipca 2017 r. w tej sprawie odbyło się już spotkanie przedstawicieli strony publicznej (Centrum Systemów Informacyjnych Ochrony Zdrowia, Ministerstwo Zdrowia, Centrum Monitorowania Jakości w Ochronie Zdrowia) z reprezentantami organizacji branżowych zainteresowanych współtworzeniem samoregulacji dla ochrony zdrowia (m.in. Polskiej Federacji Szpitali, Fundacji Telemedyczna Grupa Robocza, Pracodawców Medycyny Prywatnej, Konfederacji Lewiatan, Polskiej Izba Informatyki i Telekomunikacji, Federacji Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie). Inicjatywa powstania branżowej regulacji uzyskała poparcie również władz województwa wielkopolskiego, fundacji My Pacjenci oraz Urszuli Jaworskiej, a także Naczelnej Izby Pielęgniarek i Położnych, Naczelnej Izby Aptekarskiej, Krajowej Izby Diagnostów Laboratoryjnych, Krajowej Rady Fizjoterapeutów. Przy czym inicjatorem i partnerem merytorycznym prac nad kodeksem jest kancelaria DZP.

W czasie spotkania m.in. podpisano list intencyjny, w którym wskazano, że jego sygnatariusze „widzą zasadność stworzenia oraz deklarują chęć współpracy nad opracowaniem kodeksu branżowego dla sektora ochrony zdrowia dotyczącego ochrony danych osobowych, który może pozwolić na osiągnięcie (...) celu nadrzędnego – dobra pacjenta". Zgodnie z harmonogramem zakończenie prac nad kodeksem i przedstawienie jego projektu głównemu inspektorowi ochrony danych osobowych powinno nastąpić pod koniec tego roku.

> Pod koniec roku główny inspektor ochrony danych osobowych powinien otrzymać projekt branżowego kodeksu dla sektora ochrony zdrowia

Nowe możliwości samoregulacji

Rozporządzenie RODO, którego jednym z głównych celów jest zapewnienie większej harmonizacji prawa ochrony danych osobowych w Unii Europejskiej, wprowadza nowe prawa i obowiązki związane m.in. z większą odpowiedzialnością podmiotów zaangażowanych w proces przetwarzania danych

Przykładowo, RODO rozwija i precyzuje zasady powierzania przetwarzania danych osobowych. Tego w obowiązujących jeszcze przepisach (dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, na których opiera się obecnie obowiązująca ustawa o ochronie danych osobowych) nie ma. Wyraźnie reguluje też kwestie korzystania przez podmiot przetwarzający z pomocy podwykonawców.

OPINIE EKSPERTÓW

Szpitale ograniczone budżetami

LIGIA KORNOWSKA

zarządzająca Polskiej Federacji Szpitali

Wprowadzenie RODO zmieni istotnie dotychczasową sytuację prawną w zakresie ochrony danych osobowych, w tym danych medycznych, nakładając nowe obowiązki i zwiększając krytycznie sankcje finansowe. Dane medyczne są co najmniej tak wrażliwe, jak np. dane bankowe. O ile jednak banki od lat przeznaczają ogromne fundusze na prace całych działów dedykowanych ochronie danych osobowych i cyberbezpieczeństwu, co i tak nie chroni ich całkowicie przed wyciekiem, tak chronicznie niedofinansowane szpitale stoją przed wyzwaniem dostosowania się do nowych przepisów w ramach obecnego budżetu. Brak środków finansowych lub brak świadomości w zakresie bezpieczeństwa danych nie będzie okolicznością łagodzącą w przypadku ewentualnego naruszenia. Dlatego tak ważne jest powstanie kodeksu branżowego w ochronie zdrowia. Umożliwi to interesariuszom sektora i stronie rządowej wypracowanie wspólnych rozwiązań, które jednocześnie zadbają o odpowiednie bezpieczeństwo danych wrażliwych i nie będą zbyt obciążające czy też wręcz niemożliwe do spełnienia dla podmiotów działających w ochronie zdrowia. Polska Federacja Szpitali, będąc najbardziej reprezentatywną organizacją szpitali w Polsce, popiera tę inicjatywę i deklaruje pełną współpracę przy tworzeniu kodeksu na każdym jego etapie powstawania. ©℗

Małe poradnie potrzebują pomocy

TOMASZ ZIELIŃSKI

ekspert Federacji Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie

Stworzenie kodeksu branżowego dla ochrony zdrowia to ciekawa inicjatywa. Federacja Porozumienie Zielonogórskie zdecydowała się wziąć udział w tworzeniu kodeksu, aby chronić interesy podmiotów, które mają ograniczone zasoby kadrowe i finansowe. Chcemy, na tyle ile to możliwe, ograniczyć problemy w interpretacji i stosowaniu prawa przez administratorów danych w małych poradniach POZ, które reprezentujemy. Dotychczasowe regulacje nastręczały wielu problemów, a nowe ze zwiększonymi sankcjami finansowymi stanowią duże zagrożenie, dlatego z nadzieją na wypracowanie akceptowalnego modelu doprecyzowania RODO dla podmiotów leczniczych, Porozumienie Zielonogórskie poparło pomysł utworzenia kodeksu branżowego. ©℗

Wytyczne muszą być jasne

MACIEJ SYTEK

członek zarządu województwa wielkopolskiego

Kodeks branżowy jest niezwykle ważną inicjatywą w kontekście nadchodzących zmian przepisów, jak również coraz większych zagrożeń związanych z bezpieczeństwem danych medycznych pacjentów. Samorząd województwa wielopolskiego i ja osobiście jesteśmy szczególnie zainteresowani wypracowaniem rozwiązań, które zapewnią jasne wytyczne przetwarzania danych medycznych, gwarantujące z jednej strony ochronę prywatności i godności pacjentów, a z drugiej umożliwiające efektywne udzielanie świadczeń zdrowotnych. W kontekście nowych wyzwań dotyczących przetwarzania danych medycznych samorząd województwa wielkopolskiego występuje w podwójnej roli: jako właściciel, podmiot tworzący dla 21 szpitali na terenie regionu, jak również jako podmiot realizujący niezwykle ambitny projekt stworzenia platformy regionalnej wymiany danych medycznych, który ma objąć wszystkie szpitale na obszarze województwa. Liczę na to, że kodeks branżowy będzie pomocny na dwóch poziomach – na poziomie konkretnej placówki medycznej, której personel będzie miał wskazówki, jak przetwarzać dane medyczne w świetle nowych przepisów, ale również na poziomie platformy regionalnej – bezpieczeństwo danych na platformie zależeć będzie od poziomu bezpieczeństwa danych w korzystających z niej placówkach. ©℗

Taniej, szybciej, efektywniej

MARCIN SERAFIN

partner w Kancelarii Maruta Wachta

Kodeksy postępowania (oraz kodeksy dobrych praktyk) to bardzo dobre narzędzia, które w nowoczesny sposób pozwalają osiągać te same cele co przepisy prawa. W odróżnieniu od przepisów ustawowych czy unijnych, pozwalają na dostosowanie środków prawnych do specyfiki danego sektora. W ten sposób te same cele regulacyjne mogą być zrealizowane taniej, szybciej i efektywniej niż tekst ustawy jednolity dla wszystkich. Taka samoregulacja to przyszłość tworzenia prawa i to nie tylko w obszarze danych osobowych.
RODO w bardzo wielu miejscach podkreśla rolę kodeksów postępowania, jednak w sposób dość ogólny. Na pewno polska ustawa uzupełniająca regulacje RODO powinna określić takie zagadnienia, jak zasady zaangażowania organu krajowego w proces inicjowania i prace nad kodeksami, bardziej konkretne oczekiwania co do treści kodeksów, zasady prowadzenia dialogu pomiędzy organem ochrony danych a wnioskodawcami kodeksów czy wreszcie kwestie związane z mechanizmami ich zatwierdzania i weryfikacji stosowania. RODO nie rozstrzyga też kwestii publikacji kodeksu i to również mogłoby zostać ustawowo przesądzone. Z kodeksami postępowania łączy się mechanizm monitorowania sposobu ich wykonywania przez podmiot akredytowany i sposoby oraz wymagania co do takiego monitoringu również mogłoby być przedmiotem regulacji polskiej ustawy. Odpowiednie wdrożenie takich mechanizmów pozwoli odciążyć organ krajowy, przerzucając istotny ciężar monitorowania zgodności działania z RODO na podmioty akredytowane. Wszystkie te elementy dają nadzieję na skuteczniejsze i precyzyjniejsze wdrożenie ogólnych wymagań RODO, do których dostosowanie własnej działalności spędza sen z powiek niejednemu przedsiębiorcy. ©℗

Administrator przed rozpoczęciem przetwarzania danych będzie musiał dokonać oceny tych operacji dla ochrony danych osobowych, w sektorach, w których przetwarzane są dane wrażliwe.

Niektóre sektory muszą przy tym postępować szczególnie uważnie. Chodzi przede wszystkim o te, w ramach których przetwarzane są dane wrażliwe, np. o sektor ochrony zdrowia.

W świetle nowych unijnych przepisów administrator przed rozpoczęciem przetwarzania danych osobowych będzie zobowiązany do dokonania oceny skutków planowanych operacji. Dotyczyć to będzie sytuacji, w których dany rodzaj przetwarzania (w szczególności z użyciem nowych technologii) ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Ponadto – ze względów bezpieczeństwa – RODO wymaga, by administrator i podmiot przetwarzający wyznaczyli inspektora ochrony danych (dalej: IOD) zawsze wtedy, gdy przetwarzania dokonuje organ lub podmiot publiczny. IOD musi być wyznaczony także wtedy, gdy główna działalność administratora (lub podmiotu przetwarzającego) polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego, systematycznego i na dużą skalę monitorowania osób, których dane dotyczą. Inspektora trzeba mieć także wtedy, gdy główne zadanie polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, w tym tych o stanie zdrowia. Oznacza to, że w zasadzie każdy podmiot leczniczy prowadzący działalność na większą skalę (zarówno publiczny, jak i prywatny) będzie zobowiązany do powołania IOD. Inspektor może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.

Przy czym wiele nowych wymogów, a ponadto dotkliwe sankcje za ich naruszenie, to istotne ryzyko prawne dla podmiotów przetwarzających dane, w szczególności w początkowym okresie wdrażania przepisów. Dlatego też unijny prawodawca dopuszcza także nowe możliwości certyfikacji i samoregulacji branżowych, które ułatwić mogą przyjęcie nowych rozwiązań i zapewnić zgodność z wymogami rozporządzenia.

I tak zgodnie z art. 40 ust. 1 RODO państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja wręcz zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu RODO – z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

Zasady tworzenia kodeksów branżowych przewidziane w RODO staną się wiążącym prawem – unijne rozporządzenie obowiązuje bowiem bezpośrednio na terenie wszystkich państw członkowskich UE. I choć część jego aspektów zostanie doprecyzowana i uregulowana w prawie krajowym, to podstawowe zapisy dotyczące skutków i charakteru kodeksów znalazły się już w samym rozporządzeniu i będą jednolite na terenie całej Unii. To zaś powinno przełożyć się na większą popularność tego typu rozwiązań w całej Europie. Na popularność kodeksów wpłyną zapewne również potencjalne zalety, jakie się z nimi wiążą.

Sam proces przygotowania projektu kodeksu branżowego nie został szczegółowo uregulowany w RODO. Rozporządzenie stanowi jedynie, że podmioty chcące go opracować (a także zmienić lub rozszerzyć zakres dotychczas obowiązującego dokumentu), są zobowiązane przedłożyć projekt kodeksu organowi nadzorczemu. W przypadku kodeksu branżowego obowiązującego wyłącznie na terytorium Polski organem tym będzie GIODO, a po wejściu w życie nowej ustawy o ochronie danych osobowych prezes Urzędu Ochrony Danych Osobowych. Po przedłożeniu projektu organ nadzorczy wydaje opinię o zgodności projektu kodeksu z RODO i go zatwierdza, o ile uzna, że stanowi on odpowiednie zabezpieczenie. Następnie organ nadzorczy rejestruje i publikuje kodeks.

Jak to będzie wyglądać w praktyce

Zgodnie z art. 41 ust. 1 RODO, zatwierdzony kodeks postępowania podlega monitorowaniu przez podmiot, który dysponuje odpowiednim poziomem wiedzy w dziedzinie będącej przedmiotem kodeksu i został akredytowany w tym celu przez organ ochrony danych osobowych. Takim podmiotem może być Urząd Ochrony Danych Osobowych (będzie to następca GIODO po wejściu w życie rozporządzenia), ale i specjalnie do tego celu powołana fundacja lub spółka). Ponadto, zgodnie z art. 41 ust. 4 RODO, podmiot monitorujący będzie musiał podejmować aktywne działania wobec tych sygnatariuszy kodeksu, którzy nie przestrzegają jego zapisów. To znaczy zawieszać lub wykluczać podmioty dopuszczające się najpoważniejszych naruszeń spośród stosujących kodeks. Informacja o powodach takiego działania powinna być także skierowana do organu nadzorczego.

Żeby podmiot monitorujący kodeks uzyskał stosowną akredytację, zgodnie z art. 41 ust. 2 będzie on musiał:

- wykazać organowi ochrony danych osobowych niezależność i odpowiedni poziom wiedzy w dziedzinie będącej przedmiotem kodeksu;
- wdrożyć procedury pozwalające na: ocenę zdolności konkretnych administratorów i podmiotów przetwarzających do stosowania kodeksu, monitorowanie przestrzegania przez nich jego przepi-

WAŻNE Od 25 maja 2018 r., czyli od wejścia w życie rozporządzenia RODO, przestaną obowiązywać normy wynikające z dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, na których opiera się obecnie obowiązująca ustawa o ochronie danych osobowych.

Ramka

Nowe-stare rozwiązanie

Mechanizm tworzenia kodeksów dobrych praktyk w zakresie ochrony danych osobowych przewidziano już w przyjętej w 1995 roku i wciąż jeszcze obowiązującej unijnej dyrektywie 95/46/WE
Zgodnie z art. 27 tego aktu państwa członkowskie UE oraz Komisja Europejska mają zachęcać do przyjmowania kodeksów dobrych praktyk zarówno na poziomie krajowym, jak i europejskim oraz umożliwiać przedstawienie ich do akceptacji krajowym organom ochrony danych lub Grupie Roboczej Art. 29 (niezależne ciało doradcze powołane na mocy dyrektywy 95/46/WE, w którego skład wchodzą przedstawiciele krajowych organów ochrony danych osobowych ze wszystkich państw członkowskich UE, przedstawiciel Europejskiego Inspektora Ochrony Danych Osobowych oraz przedstawiciel Komisji Europejskiej).
Celem tworzenia kodeksów dobrych praktyk – w myśl dyrektywy – jest ułatwienie stosowania przepisów z zakresu ochrony danych osobowych obowiązujących w państwach członkowskich oraz samej dyrektywy. W praktyce jednak, znaczenie kodeksów dobrych praktyk pod rządami dyrektywy 95/46/WE jest stosunkowo niewielkie. Dość powiedzieć, że omawiany przepis nie został nawet implementowany do polskiej ustawy o ochronie danych osobowych. Co ciekawe, mimo braku podstawy prawnej dla stworzenia kodeksów w polskiej ustawie, generalny inspektor ochrony danych osobowych zawarł porozumienia dotyczące stworzenia takich dokumentów, m.in. z Polskim Związkiem Motoryzacyjnym czy też reprezentantami organizacji IAB Polska (Związek Pracodawców Branży Internetowej). ©℗

sów oraz okresowe dokonywanie przeglądu jego funkcjonowania;
- dysponować procedurami i strukturami pozwalającymi rozpatrywać skargi na naruszenie kodeksu przez administratora lub podmiot przetwarzający lub na sposób wdrożenia lub wdrażania kodeksu przez ww. podmioty oraz które pozwalają zapewnić przejrzystość tych procedur i struktur dla osób, których dane dotyczą, a także opinii publicznej;
- wykazać właściwemu organowi nadzorczemu, że jego zadania i obowiązki nie powodują konfliktu interesów.

Szczegółowe przepisy dotyczące sposobu uzyskania akredytacji przez podmiot monitorujący (w tym regulacja dotycząca kosztów uzyskania akredytacji) znajdą się w nowej, polskiej ustawie o ochronie danych osobowych. Jednak projekt ustawy w brzmieniu opublikowanym w marcu br. nie zawierał przepisów odnoszących się do akredytacji podmiotów monitorujących przestrzeganie kodeksów postępowania.

WAŻNE **Przepisy unijnego rozporządzenia ogólnego w sprawie ochrony danych osobowych wprowadzają możliwość przygotowania branżowych kodeksów postępowania. Celem tego typu regulacji jest doprecyzowanie w poszczególnych branżach przepisów RODO.**

Medyczna specyfika

Tak jak pisaliśmy, kodeksy postępowania powinny przede wszystkim jak najpełniej uwzględniać specyfikę sektorową. I tak podmioty wykonujące działalność leczniczą oraz firmy i instytucje z ich otoczenia w codziennej pracy przetwarzają duże ilości danych osobowych, w tym m.in. medycznych, czyli danych o szczególnym charakterze, niezwykle wrażliwych, wymagających w związku z tym zapewnienia szczególnej ochrony. Ochrona zdrowia jest również działalnością regulowaną na poziomie rożnych aktów normatywnych, od konstytucji począwszy, a skończywszy na obwieszczeniach i zarządzeniach prezesa NFZ. Dlatego też szczególnie ważne jest stworzenie regulacji dedykowanej ochronie zdrowia.

I tak w opinii Grupy Roboczej Art. 29 „wszelkie dane zawarte w dokumentacji medycznej, w elektronicznej dokumentacji zdrowotnej oraz w systemach EHR należy traktować jako dane sensytywne, a więc dane szczególnie chronione" (tak wynika z dokumentu roboczego w sprawie przetwarzania danych osobowych dotyczących zdrowia w elektronicznej dokumentacji zdrowotnej [EHR] przyjętego 15 lutego 2007 r., 00323/07/PL, WP 131). System EHR (ang. electronic health record), czyli elektroniczny rekord pacjenta – zawiera wszystkie dane o konkretnym chorym, które swobodnie można wymieniać pomiędzy usługodawcami medycznymi (przykładowo lekarzem rodzinnym, szpitalem, domem opieki).

Za dane medyczne należy więc przyjąć wszelkie informacje odnoszące się do stanu zdrowia osoby fizycznej, w tym np. o chorobach pacjenta, procedurach diagnostycznych i terapeutycznych, z których on skorzystał, a także inne dane mające wyraźny i bliski związek z opisem stanu zdrowia danej osoby, np. dotyczące przyjmowanych leków, zażywania przez nią alkoholu lub narkotyków, jak również genetyczne, znajdujące się w dokumentacji medycznej. Podsumowując – danymi medycznymi mogą być więc nie tylko dane o stanie zdrowia, ale także inne dane wrażliwe mogące mieć wpływ na stan zdrowia.

Dane medyczne są powszechnie przetwarzanie w codziennej pracy podmiotów wykonujących działalność leczniczą, m.in. w prowadzonej przez nie dokumentacji medycznej. O ile w dalszym ciągu większość dokumentacji ma formę papierową, to postępujący proces informatyzacji sektora ochrony zdrowia powoduje, że coraz większa ilość danych medycznych powstaje w formie cyfrowej. W związku bowiem z przyjętą przez Sejm 20 lipca 2017 r. nowelizacją ustawy o systemie informacji w ochronie zdrowia (Dz.U. z 2017 r. poz. 1524) od 1 stycznia 2019 r. dokumentacja medyczna ma być już powszechnie prowadzona w formie elektronicznej (e-recepty mają być obowiązkowe począwszy od 1 stycznia 2020, a e-skierowania – rok później). Wiąże się to z nowymi wyzwaniami prawno-organizacyjnymi, którym można będzie łatwiej sprostać m.in. dzięki wykorzystaniu kodeksu.

Dotychczasowe doświadczenia nie napawają optymizmem

Problem zapewnienia odpowiedniego poziomu ochrony danych o stanie zdrowia nie jest nowym tematem wynikającym z wdrożenia RODO. Z tym że po zmianie przepisów brak działań w tym zakresie będzie się wiązał z poważnymi konsekwencjami, w tym finansowymi

Zaprezentowane przez Najwyższą Izbę Kontroli wyniki kontroli „Tworzenie i udostępnianie dokumentacji medycznej" potwierdziły istotne problemy z przestrzeganiem zasad prowadzenia dokumentacji medycznej i ochrony danych osobowych. Na 24 zbadanych wówczas (kontrolą NIK objęto funkcjonowanie w latach 2013-2015 świadczeniobiorców z 7 województw), aż 21 prowadziło dokumentację z naruszeniem prawa. Blisko połowa placówek nie zapewniała też należytego poziomu ochrony informacji o stanie zdrowia pacjentów. Zdarzało się, że dokumenty zawierające wrażliwe dane pacjentów leżały np. w kartonowych pudłach na podłodze lub w pozbawionych zamków szafach stojących w publicznie dostępnym korytarzu. NIK stwierdziła ponadto, że do czasu zakończenia kontroli żaden z objętych nią świadczeniodawców nie wdrożył systemu informatycznego dla tego rodzaju dokumentacji w postaci elektronicznej.

Jeżeli do takich naruszeń doszłoby pod rządami RODO, to mogłyby one mieć dla pomiotu leczniczego dużo poważniejsze konsekwencje niż obecnie. Unijne rozporządzenie zakłada bowiem z jednej strony wprowadzenie mechanizmów ujawniania naruszeń bezpieczeństwa danych osobowych (obowiązek poinformowania organu nadzoru i pacjenta), a z drugiej możliwość łatwego egzekwowania swoich praw przez osoby, których dane dotyczą. Nie bez znaczenia są również ogromne potencjalne kary administracyjne, które mogą zostać nałożone na administratora danych.

Zyska nie tylko pacjent

Korzyści wynikające z przyjęcia kodeksu dedykowanego ochronie zdrowia będą odczuwalne przede wszystkim przez pacjentów. Ich wprowadzenie oznacza zwiększenie bezpieczeństwa i ochrony danych osobowych osób korzystających z placówek medycznych, m.in. dzięki lepszej kontroli egzekwowania przepisów, a także wprowadzeniu najnowszych standardów ochrony danych wrażliwych. Przyjęcie branżowej samoregulacji da też pacjentom bezpośrednie narzędzia – wprowadzone mechanizmy doprecyzowujące ogólne przepisy RODO pozwolą im łatwiej wyegzekwować prawa względem swoich danych medycznych.

Jednak opracowanie branżowych zasad, dzięki zwiększeniu bezpieczeństwa prawnego podmiotów leczniczych, pozytywnie wpłynie też na wprowadzanie nowoczesnych systemów teleinformatycznych usprawniających opiekę nad pacjentem oraz zwiększających komfort jego terapii. Stworzy również dobre warunki dla rozwoju telemedycyny i e-zdrowia w Polsce. Kodeks będzie miał też dobry

Główne zalety opracowania kodeksów branżowych ©℗

POTWIERDZENIE ROZLICZALNOŚCI

Przede wszystkim przepisy RODO kładą istotny nacisk na tzw. rozliczalność, czyli zdolność administratorów danych oraz podmiotów przetwarzających dane do wykazania, że podejmowane przez nich działania są zgodne z unijnymi wymogami. Jednym zaś z mechanizmów wykazywania takiej zgodności (rozliczalności) jest przestrzeganie przez administratora danych oraz podmioty przetwarzające zapisów zatwierdzonego kodeksu postępowania.

DOPRECYZOWANIE NIEJASNYCH OBOWIĄZKÓW – OBNIŻENIE RYZYKA PRAWNEGO I OBCIĄŻEŃ REGULACYJNYCH

Przepisy RODO, mimo że mają stosunkowo ogólny charakter, to nakładają na administratorów danych i podmioty przetwarzające wiele nowych, nieistniejących w obecnych regulacjach o ochronie danych osobowych obowiązków, których realizacja może nastręczać pewnych trudności. W tym kontekście doprecyzowanie w ramach określonego kodeksu branżowego sposobu rozumienia poszczególnych przepisów RODO i realizacji obowiązków z nich wynikających może stanowić duże ułatwienie dla administratorów danych.

MIARKOWANIE SANKCJI

W myśl art. 83 RODO fakt przestrzegania zatwierdzonego kodeksu postępowania przez administratora danych będzie także uwzględniany przez organ ochrony danych osobowych przy określaniu wysokości administracyjnej kary pieniężnej za ewentualne naruszenia przepisów RODO. Ze względu na istotną wysokość sankcji finansowych przewidzianych w przepisach rozporządzenia – nawet do 20 mln euro lub do 4 proc. obrotu globalnego – możliwość wpływu na wysokość nakładanej kary będzie działać zachęcająco na administratorów danych do korzystania z kodeksu. W tym miejscu warto jednak zauważyć, że sposób sformułowania art. 83 RODO nie przesądza jednoznacznie, że fakt przestrzegania zatwierdzonego kodeksu postępowania przez przedsiębiorcę będzie traktowany wyłącznie jako okoliczność łagodząca.

MONITOROWANIE PRZESTRZEGANIA PRZEPISÓW

Zakres regulacji zatwierdzonych kodeksów postępowania może być w praktyce bardzo szeroki i może odnosić się do wszystkich elementów związanych z przetwarzaniem danych osobowych i wynikających z przepisów RODO. Dokument ten obejmuje również mechanizmy pozwalające podmiotowi akredytowanemu monitorowanie przestrzegania przepisów kodeksu.

PRZYKŁADOWY ZAKRES REGULACJI POWINIEN OKREŚLAĆ:

- zasady rzetelnego i przejrzystego przetwarzania oraz zbierania danych osobowych;
- zasady pseudonimizacji* danych osobowych;
- sposób przekazywania informacji opinii publicznej, a także osobom, których dane dotyczą;
- prawa przysługujące osobom, których dane są zbierane i przetwarzane;
- zasady informowania i ochrony dzieci oraz sposób pozyskiwania zgody osoby sprawującej władzę lub opiekę nad dzieckiem;
- środki i procedury zapewniające bezpieczeństwo przetwarzania danych;
- zgłaszanie organowi nadzorczemu naruszeń ochrony danych osobowych oraz zawiadamiania o takich naruszeniach osób, których dane dotyczą;
- przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych;
- rodzaj postępowań pozasądowych oraz inne tryby rozstrzygania sporów.
- określać prawnie uzasadnione interesy administratorów danych w konkretnych kontekstach.

*Pseudonimizacja to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie – czyli tej, której dane dotyczą – bez użycia dodatkowych informacji. Ponadto dane te są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.)

AGP

wpływ na medycynę jako naukę – uwzględnienie specyfiki branży sprawi, że wprowadzanie RODO ułatwi przetwarzanie danych medycznych w celach naukowych. A jest to szczególnie istotne w przypadku badania i terapii chorób rzadkich (tzw. secondary use of data).

Przyjęcie kodeksu zapewni wreszcie korzyść także podmiotom funkcjonującym w systemie ochrony zdrowia i przetwarzających w związku z tym dane medyczne. Przez doprecyzowanie ogólnych przepisów RODO i możliwe najpełniejsze dostosowanie przyjętych rozwiązań do specyfiki branży nastąpi obniżenie ryzyka prawnego związanego z możliwymi różnicami interpretacyjnymi nowych przepisów oraz brakiem stabilnego orzecznictwa w tym zakresie. W związku z tym nastąpi redukcja ryzyka poniesienia sankcji finansowych.

Ponadto samoregulacja da możliwość sformułowania przepisów w sposób możliwie najmniej dotkliwy dla administratorów danych. Oczywiście z zachowaniem odpowiedniego poziomu ochrony praw i wolności osób, których dane dotyczą, co zapewni zarazem lepsze dostosowanie do specyfiki branży, oznaczające obniżenie kosztów regulacyjnych i administracyjnych spełnienia obowiązków ochrony danych.

Powyższe przyczyni się m.in. do obniżenia ryzyka prawnego, a co za tym idzie dużo większego otwarcia rynku ochrony zdrowia na nowe technologie w sposób bezpieczny dla danych osobowych pacjenta i spójny z polityką publiczną w tym zakresie. Kodeks jest ponadto formą stosunkowo elastyczną, możliwe jest zaproponowanie w nim najnowszych wytycznych i standardów bezpieczeństwa, a zatem zapewnienie większego bezpieczeństwa danych. Jest to szczególnie istotne w kontekście rozwoju nowych technologii, które mogą wprowadzać rozwiązania zapewniające coraz wyższy poziom ochrony.

Kodeks postępowania dla ochrony zdrowia to wreszcie wiele korzyści systemowych, szczególnie istotnych z perspektywy generalnego inspektora ochrony danych osobowych oraz ministra zdrowia.

Wiele ustaw pod lupą

Dotychczasowe trudności związane z przestrzeganiem zasad ochrony danych pacjentów mogą wynikać – o czym już wspominaliśmy – ze stosunkowo dużego rozproszenia regulacji, które zawarte są w szeregu aktów pranych. Normy ogólne ochrony danych są bowiem modyfikowane szczegółowymi regulacjami prawa medycznego odnoszącymi się do prowadzenia dokumentacji wykorzystywanej w ochronie zdrowia. Ponadto, w związku z procesem informatyzacji tego sektora, wiele przepisów ma charakter techniczny, a ich zrozumienie wymaga doświadczenia w zakresie nowych technologii. TABELA

Potrzebne otwarcie na nowoczesne technologie

Nowe technologie są i będą coraz powszechniej wykorzystywane w ochronie zdrowia. Ich rozwój możliwy jest przede wszystkim dzięki cyfryzacji informacji o stanie zdrowia pacjentów. Dlatego też elektroniczna dokumentacja medyczna staje się europejskim standardem, który obejmie docelowo wszystkie kraje UE. Sprzyja to szybkiemu rozwojowi nowych technologii medycznych, które coraz częściej i w coraz większym zakresie przetwarzają dane pacjentów.

Biorąc to pod uwagę, a także uwzględniają postulaty zawarte zarówno w najważniejszych dokumentach strategicznych Unii Europejskiej, jak i dokumentach pochodzących od polskich organów administracji, wydaje się uzasadnione, by zapisy kodeksu odnosiły się m.in. do kwestii świadczenia usług zdrowotnych z wykorzystaniem nowoczesnych technologii (e-zdrowie, telemedycyna, m-zdrowie). Dzięki temu zapisy kodeksu będą właściwie uwzględniać współczesny stan rozwoju medycyny oraz technologii ICT (internet, sieć bezprzewodowa i Bluetooth, telefonia stacjonarna, a także komórkowa i satelitarna, technologia komunikacji dźwięku i obrazu oraz radio, telewizja (pamięci przenośne, dyski twarde, taśmy, komputery, serwery, sieci komputerowe itp.). Jest to szczególnie ważne, gdyż technologie ICT już teraz obejmują całą gamę aplikacji informatycznych oraz złożonych systemów IT umożliwiających realizację przetwarzania i przesyłania danych na wyższym poziomie abstrakcji niż poziom sprzętowy. ©℗

WAŻNE **Kodeks da możliwość sformułowania przepisów w sposób najmniej dotkliwy dla administratorów danych, jednocześnie z zachowaniem odpowiedniego poziomu ochrony praw i wolności osób, których dane dotyczą. Zapewni zarazem lepsze dostosowanie do specyfiki branży, oznaczające obniżenie kosztów regulacyjnych i administracyjnych spełnienia obowiązków ochrony danych.**

Kodeks w sektorze ochrony zdrowia – a co w nim?

MC

Etapy tworzenia regulacji

ETAP 1 Stworzenie kodeksu branżowego na forum organizacji zrzeszającej administratorów danych i/lub podmioty przetwarzające

ETAP 2 Przedłożenie projektu kodeksu organowi nadzorczemu

ETAP 3 Opinia o zgodności projektu z RODO

ETAP 4 Rejestracja i publikacja kodeksu przez organ nadzorczy

Postanowienia kodeksu zawierać...

POWINNY:

- Doprecyzować regulacje RODO
- Uwzględniać i wykorzystywać efekty prac Centrum Systemów Informacyjnych Ochrony Zdrowia (wytyczne i rekomendacje dotyczące przetwarzania danych medycznych)
- Być spójne z postanowieniami innych branżowych kodeksów postępowania
- Być elastyczne, niedyskryminujące, promujące wysoki standard ochrony przetwarzania danych
- Cyklicznie być przeglądane i aktualizowane

NIE POWINNY:

- Powielać lub być sprzeczne z regulacjami branżowymi
- Być sprzeczne z przepisami unijnymi
- Stanowić doprecyzowania regulacji branżowych dotyczących przetwarzania danych zawartych w dokumentacji medycznej, chyba że regulacje branżowe stanowią jednocześnie doprecyzowanie RODO

Dobrze przygotowana i wspólnie uzgodniona samoregulacja w tym zakresie to m.in.:

- lepsza ochrona danych medycznych pacjentów
- wprowadzenie elementu samoregulacji w dziedzinie ochrony danych osobowych, co wiąże się z wypracowaniem rozwiązania akceptowalnego dla adresatów przepisów i zwiększającego compliance (zapewnienie zgodności działalności z regulacjami prawnymi, normami bądź zestawami zaleceń)
- wykorzystanie transparentnego mechanizmu współpracy między stroną publiczną a organizacjami branżowymi
- łatwiejsza i bardziej efektywna kontrola przestrzegania zasad ochrony danych osobowych przez podmioty z branży medycznej
- poszerzanie świadomości branży na temat problematyki ochrony danych osobowych
- skorzystanie ze specjalistycznej wiedzy branży, dzięki czemu wypracowane wytyczne będą najbardziej spójne ze stosowanymi rozwiązaniami technologicznymi
- wykorzystanie wsparcia w postaci zasobów merytorycznych, finansowych i czasowych branży
- wypracowanie rozwiązania spójnego systemowo z kodeksem tworzonym przez Polską Izbę Informatyki i Telekomunikacji

20 mln euro

lub do 4 proc. wartości rocznego światowego obrotu przedsiębiorstwa grozi maksymalnie za naruszenie niektórych przepisów RODO

Shutterstock

21,5 tys.

tyle podmiotów leczniczych zostało zarejestrowanych w Rejestrze Podmiotów Wykonujących Działalność Leczniczą

Tabela Jakie akty prawne powinna zawierać regulacja?

©℗

Akt prawny	Zakres
Ustawa z 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (tj. Dz.U. z 2017 r. poz. 125 ze zm).	Prawo dostępu lekarzy i lekarzy dentystów do dokumentacji medycznej pacjenta, zasady uzyskiwania zgody pacjenta. Ustawa nakłada obowiązek zachowania tajemnicy zawodowej, prowadzenia dokumentacji i informowania o udzielanych świadczeniach (art. 32, 40 i 41).
Ustawa z 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (t.j. Dz.U. z 2016 r. poz. 1793 ze zm.).	Prawa i obowiązki Narodowego Funduszu Zdrowia, ministra zdrowia oraz świadczeniodawców w zakresie przetwarzania danych osobowych na potrzeby ewidencjonowania świadczeń zdrowotnych (art. 188–192a).
Ustawa z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2017 r. poz. 750).	Minimalne wymogi dla systemów informatycznych przeznaczonych do realizowania zadań publicznych.
Ustawa z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz.U. z 2016 r. poz. 186 ze zm.).	W szczególności – lecz nie wyłącznie – w zakresie, w jakim określa ona prawa pacjenta do informacji, tajemnicy informacji z nim związanych, dokumentacji medycznej oraz zasady przechowywania dokumentacji medycznej (rozdziały 3, 4 i 7 ustawy).
Ustawa z 15 kwietnia 2011 r. o działalności leczniczej (tj. Dz.U. z 2016 r. poz. 1638 ze zm.).	W zakresie, w jakim określa ona zasady funkcjonowania podmiotów wykonujących działalność leczniczą.
Ustawa z 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (t.j. Dz.U. z 2016 r. poz. 1535 ze zm.).	Zasady funkcjonowania rejestrów medycznych i zasady wymiany informacji między podmiotami przekazującymi dane do rejestrów.
Ustawa z 15 lipca 2011 r. o zawodach pielęgniarki i położnej (t.j. Dz.U. z 2016 r. poz. 1251 ze zm.).	Prawo dostępu pielęgniarek oraz położnych do dokumentacji medycznej pacjenta i nakłada na pielęgniarki oraz położne obowiązek zachowania tajemnicy zawodowej, prowadzenia dokumentacji medycznej i informowania pacjenta o udzielanych świadczeniach (art. 14 oraz art. 16–18 ustawy).
Ustawa z 25 września 2015 r. o zawodzie fizjoterapeuty (Dz.U. z 2015 r. poz. 1994 ze zm).	Prawo dostępu fizjoterapeuty do dokumentacji medycznej pacjenta i nałożenie na fizjoterapeutę obowiązku zachowania tajemnicy zawodowej, prowadzenia dokumentacji medycznej oraz informowania pacjenta o udzielanych świadczeniach (art. 7 i art. 9 ustawy).
Rozporządzenie ministra zdrowia z 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzoru dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. z 2015 r. poz. 2069).	W zakresie, w jakim doprecyzowuje RODO.
Rozporządzenie ministra spraw wewnętrznych i administracji z 25 lutego 2016 r. w sprawie rodzajów, zakresu i wzorów oraz sposobu przetwarzania dokumentacji medycznej w podmiotach leczniczych utworzonych przez ministra właściwego do spraw wewnętrznych (Dz.U. z 2016 r. poz. 249).	W zakresie, w jakim doprecyzowuje RODO.
Rozporządzenie ministra sprawiedliwości z 26 lutego 2016 r. w sprawie rodzajów i zakresu dokumentacji medycznej prowadzonej w podmiotach leczniczych dla osób pozbawionych wolności oraz sposobu jej przetwarzania (Dz.U. z 2016 r. poz. 258).	W zakresie, w jakim doprecyzowuje RODO.

(przykładowy zakres)