ACTA IURIDICA RESOVIENSIA Nr 4(39)/2022
ISSN 2720-0574 DOI: 10.15584/actaires.2022.4.21

Joanna Anna Wolska

Podhalańska Państwowa Uczelnia Zawodowa w Nowym Targu
ORCID: 0000-0002-5780-4005

BRAK KODEKSU BRANŻOWEGO W SYSTEMIE OCHRONY ZDROWIA A OCHRONA DANYCH OSOBOWYCH PACJENTA

Wprowadzenie

Rozporządzenie Parlamentu Europejskiego i Rady (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[1] dotyczy wszystkich podmiotów, które przetwarzają dane osobowe osób fizycznych w związku z prowadzoną działalnością zawodową, zarobkową, statutową. Zostało skierowane do wielu branż, a jak wiadomo, każda branża jest inna, nie można porównać prowadzenia jakiegokolwiek sklepu internetowego z wykonywaniem działalności leczniczej. W jaki sposób należy zatem dokonywać wykładni przepisów w tak różnych obszarach działalności, gdy RODO przewiduje przepisy wspólne dla wszystkich? Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu rozporządzenia. Taki kodeks branżowy ma pomóc określić minimalne wymogi związane z ochroną danych osobowych w placówkach ochrony zdrowia, które należy spełnić, by być w zgodności z RODO. Założeniem jest uszczegółowienie kwestii dotyczących m.in. zbierania i udostępniania danych (obowiązek informacyjny), zabezpieczenia danych, w tym stosowania środków technicznych, które mają na celu ochronę danych osobowych przed ich ujawnieniem osobom nieupoważnionym. Praktycznie przepisy RODO są stosowane od 4 lat. Czy dotychczas jakikolwiek kodeks branżowy obowiązuje, w tym także w zakresie ochrony zdrowia w Unii Europejskiej? Wydaje się, że przepisy RODO stosowane bez odpowiedniej wykładni uniemożliwiają prowadzenie działalności leczniczej, która wiąże się z przetwarzaniem danych wrażliwych. Czy zatem pacjent

[1] Dz. Urz. UE. L. z 2016 r., nr 119/1 (dalej: RODO).

w obecnie obowiązującym stanie prawnym ma zapewnioną odpowiednią ochronę? Czy istnieje mechanizm, który pomoże w prawidłowym stosowaniu RODO w tym zakresie?

Ochrona danych osobowych w systemie ochrony zdrowia

Każdy domaga się, aby jego prawo do prywatności było przestrzegane. Nie życzymy sobie, aby ktoś wchodził nam do mieszkania czy korzystał z naszych rzeczy, czytał nasze listy czy maile. W ślad za prawem do prywatności w wyniku informatyzacji przy przetwarzaniu danych osobowych w aktach prawnych, w szczególności europejskich, wyodrębniono właśnie prawo do ochrony danych osobowych. Informatyzacja z jednej strony usprawnia obieg informacji, ale jest to „miecz obosieczny", bowiem umożliwia też kradzież takich danych[2].

Ubiegając się o udzielenie świadczenia zdrowotnego, pacjent musi się liczyć z tym, że bez podania swoich danych osobowych świadczenia nie otrzyma. Gdy jednak pacjent ujawni swoje dane osobowe i poda dodatkowe informacje dotyczące jego stanu zdrowia, powstaje kolejne pytanie: kto, w jakich sytuacjach i zakresie będzie mógł się o tym dowiedzieć?

Parę lat temu autobus z dziećmi jadącymi na ferie zimowe miał wypadek na południu Polski. Ranni zostali przewiezieni do różnych, oddalonych o kilkadziesiąt kilometrów od siebie szpitali. Rodzice dzwonili do placówek, by dowiedzieć się, gdzie znajdą swoje dziecko, by jak najszybciej do niego dotrzeć. Co powinna była odpowiedzieć osoba odbierająca telefon z pytaniem, czy dziecko znajduje się na oddziale i co mu dolega? Odpowiedź na powyższe pytanie stanowi pretekst do przedstawienia problematyki ochrony danych osobowych w systemie ochrony zdrowia. Na podstawie choćby tego przykładu wyraźnie widać, że codzienne sytuacje mogą stanowić problem dla osób wykonujących działalność leczniczą. Tak jest, zwłaszcza gdy przepisy nie dają konkretnych odpowiedzi na pytanie, jak w danym przypadku postępować. Osoba wykonująca zawód medyczny ma przede wszystkim leczyć, a nie zajmować się interpretacją przepisów. Czy ustawodawca unijny o fakcie tym pamiętał, tworząc regulacje dotyczące ochrony danych osobowych?

RODO jest stosowane od 25 maja 2018 r. Jest to pierwszy bezpośrednio wiążący[3] akt prawa unijnego, w którym w sposób kompleksowy uregulowano problematykę ochrony danych osobowych. Skuteczne stosowanie RODO mogło jednak

[2] A. Mednis [w:] *System Prawa Medycznego*, t. III: *Organizacja systemu ochrony zdrowia*, red. D. Bach-Golecka, R. Stankiewicz, Warszawa 2020, s. 932–934, nb. 1–5.

[3] Art. 288 akapit 2 TFUE (Dziennik Urzędowy C 326, 26 października 2012 r., P. 0001–0390). Także: wyrok TSUE z 14 grudnia 1971 r., C-43/71, *Politi przeciwko Ministrowi Finansów Republiki Włoskiej*, EU:C:1971:122.

zostać zapewnione dopiero poprzez odpowiednie regulacje krajowe[4]. Polski ustawodawca zdecydował o uchwaleniu nowej ustawy o ochronie danych osobowych[5]. Pamiętać trzeba, po pierwsze, o tym, że rozporządzenia organów unijnych mają pierwszeństwo stosowania, ponieważ stanowią akt wyższej rangi niż polska ustawa (art. 91 ust. 2 Konstytucji RP[6]). Po drugie, jak wynika z art. 2 ust. 2 TFUE[7], w przypadku kompetencji dzielonych państwa członkowskie wykonują swoją kompetencję jedynie w takim zakresie, w jakim Unia nie wykonała swojej kompetencji[8]. Co do zasady od momentu wiążącego stosowania przepisów RODO polskie regulacje, które były z nimi sprzeczne, powinny zostać zastąpione właściwymi przepisami RODO. Inaczej jest jedynie w takiej sytuacji, gdy ustawodawca unijny pozostawił swobodę regulacji ustawodawcy krajowemu w tym zakresie[9].

W Polsce RODO spowodowało poruszenie przede wszystkim dlatego, że za jego pośrednictwem nałożono nowe obowiązki na administratorów danych i wprowadzono możliwość wymierzenia wysokich kar finansowych za naruszenie przepisów rozporządzenia[10]. Miało to związek z „podejściem opartym na ocenie ryzyka (ang. *risk-based approach*)". Polega to na tym, że to administrator i podmiot przetwarzający muszą zapewnić bezpieczeństwo danych przy wdrożeniu odpowiednich środków technicznych i organizacyjnych[11]. RODO dotyczy wszystkich podmiotów, które przetwarzają dane osobowe osób fizycznych w związku z prowadzoną działalnością zawodową lub handlową[12]. Zostało tym samym skierowane do wielu branż, a każda branża jest inna, nie można porównać np. prowadzenia księgarni internetowej z wykonywaniem działalności leczniczej. Nadzwyczajna sytuacja epidemiczna nie wyłączyła ani nie spowodowała zawieszenia stosowania przepisów o ochronie danych osobowych. Przecież art. 51 ust. 1 Konstytucji RP gwarantuje, że nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. W systemie ochrony zdrowia pandemia z jednej strony przyczyniła się do wdrożenia procedur zgodnych z RODO (zachowywanie odległości między pacjentami przy rejestracji z racji dystansu społecznego, umawianie pacjentów na godziny, by uniknąć ich kumulacji w poczekalni, brak

[4] Motyw 8 RODO: „W zakresie, w jakim niniejsze rozporządzenie dopuszcza doprecyzowanie lub zawężenie jego przepisów przez prawo państw członkowskich, mogą one – o ile jest to niezbędne, by krajowe przepisy były spójne i zrozumiałe dla osób, do których mają zastosowanie – włączyć elementy niniejszego rozporządzenia do swego prawa krajowego".

[5] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019, 1781).

[6] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997, nr 78, poz. 483).

[7] Traktat o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE. C. z 2012 r., nr 326/01).

[8] Por. np. kompetencję wyłączną w art. 51 RODO: „każde państwo członkowskie zapewnia/wskazuje".

[9] Por. np. art. 9 ust. 4 RODO: „państwa członkowskie mogą".

[10] Zob. art. 83 RODO.

[11] A. Mednis [w:] *System Prawa Medycznego*, t. III: *Organizacja systemu ochrony zdrowia*, red. D. Bach-Golecka, R. Stankiewicz, Warszawa 2020, s. 941, nb. 24.

[12] Motyw 18 RODO.

omawiania sytuacji zdrowotnej i podawania danych osobowych przy osobach postronnych) i rozwiązań z zakresu e-medycyny (e-recepta, e-skierowanie, pacjent.gov.pl itp.). Z drugiej strony czy zagwarantowano rozwiązania zgodne z RODO przy korzystaniu z tzw. teleporady?

Dane osobowe i dane medyczne

Z przepisów rozporządzenia wynika, że do przetwarzania danych wrażliwych wymagana jest świadoma, dobrowolna, konkretna i jednoznaczna zgoda, która powinna zostać wyrażona przed przetwarzaniem danych[13]. W przeciwnym razie gdy dane osobowe będą przetwarzanie bez ważnej podstawy prawnej, może to skutkować nałożeniem kary finansowej (art. 83 RODO), a także może być przyczyną roszczeń cywilnoprawnych (art. 82 RODO) oraz odpowiedzialności karnej (art. 107 ustawy[14]). Nie wolno zbierać danych „na zapas", dane zbędne należy usunąć[15].

Definicja danych osobowych znajduje się w art. 4 pkt 1 RODO. Są to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie takiego identyfikatora, jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Dane medyczne stanowią kategorię danych o osobach, przy czym dotyczą zdrowia i leczenia ludzi, a więc są danymi wrażliwymi[16], bowiem odnoszą się do „intymnej sfery życia jednostki"[17]. RODO nie odwołuje się do pojęcia *dane medyczne*, natomiast w art. 4 pkt 15 formułuje definicję „danych dotyczących zdrowia". Są to dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o stanie

[13] Więcej na ten temat zob. dokument opracowany przez Europejską Radę Ochrony Danych: Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679, v.1.1, przyjęty 4 maja 2020 r., https://uodo.gov.pl/pl/10/428 (1.02.2022) przez stronę internetową UODO. „Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania Grupy zostały określone w przepisach art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE".

[14] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019, poz. 1781), dalej: ustawa.

[15] A. Mednis [w:] *System Prawa Medycznego*, t. III: *Organizacja systemu ochrony zdrowia*, red. D. Bach-Golecka, R. Stankiewicz, Warszawa 2020, s. 940, nb. 21.

[16] M. Jagielski [w:] *Ochrona danych osobowych*, red. P. Litwiński, Warszawa 2018, s. 7.

[17] A. Mednis [w:] *System Prawa Medycznego*, t. III: *Organizacja systemu ochrony zdrowia*, red. D. Bach-Golecka, R. Stankiewicz, Warszawa 2020, s. 941, nb. 26.

jej zdrowia. Według motywu 35 z RODO do tej kategorii należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dotyczą, ujawniające informacje o jej przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia. Do danych takich należą informacje o konkretnej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej. Bliższe doprecyzowanie znajduje się w dyrektywie Parlamentu Europejskiego i Rady 2011/24/UE[18].

Dane medyczne jako dane wrażliwe w świetle prawa są chronione podwójnie, bo w ramach tajemnicy medycznej[19], a także prawem ochrony danych osobowych. Przy czym gdy tajemnica posiada „wyższy poziom ochrony niż RODO, ma ona pierwszeństwo przed przepisami rozporządzenia"[20]. Brak takich przepisów powodowałby, że dokumentacja medyczna mogłaby zostać znaleziona wszędzie, np. na śmietniku. Same dane o stanie zdrowia, z których nie wynika, kogo dotyczą, nie stanowią danych osobowych w rozumieniu rozporządzenia[21]. Z jednej strony szczególna kategoria danych medycznych powinna podlegać kontroli jak każde dane osobowe przed ich niekontrolowanym przetwarzaniem, a także ich nadmiernym utajnieniem (ochrona prywatności, zapewnienie intymności). Z drugiej strony bezwzględny zakaz udostępniania danych bez zgody osoby, której dane dotyczą, może być równoznaczny z zagrożeniem jej życia lub zdrowia[22] (np. osoba nieprzytomna, na temat której jej znajomy może poinformować, jakie leki przyjmuje). Same przepisy rozporządzenia ze względu na fakt, że stanowić miały kompromis pomiędzy brakiem kontroli przetwarzania danych osobowych a ich utajnianiem, nie są odpowiedzią na powstałe w praktyce wątpliwości, z którymi zmaga się personel medyczny przy udzielaniu świadczeń zdrowotnych lub informowaniu o nich.

Kodeksy postępowania

Wyrazem elastyczności w podejściu do przestrzegania przepisów rozporządzenia w różnych branżach jest rozwiązanie zawarte w rozdziale IV sekcji 5. Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają w przepisie art. 40 ust. 1 RODO do sporządzania kodeksów po-

[18] Dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE z 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej (Dz. Urz. L 88 z 4 kwietnia 2011 r., s. 45).

[19] Np. art. 40 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz.U. 2021, poz. 790) – tajemnica lekarska, art. 17 ustawy z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej (Dz.U. 2021, poz. 479) – tajemnica pielęgniarki i położnej.

[20] A. Mednis [w:] *System Prawa Medycznego*, t. III: *Organizacja systemu ochrony zdrowia*, red. D. Bach-Golecka, R. Stankiewicz, Warszawa 2020, s. 942, nb. 27.

[21] M. Jagielski [w:] *Ochrona danych osobowych*, red. P. Litwiński, Warszawa 2018, s. 10.

[22] *Ibidem*.

stępowania mających pomóc we właściwym stosowaniu rozporządzenia, z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania danych, ponieważ od początku było wiadomo, że każda branża jest inna. Postawiono nawet tezę, że „kodeksy postępowań to jeden z najważniejszych mechanizmów zaproponowanych przez RODO. Idea jest zaczerpnięta z systemów zarządzania, np. rodziny ISO"[23], przy czym zagadnienia te należy stanowczo oddzielić od siebie. Wdrożenie systemów z rodziny ISO dotyczących danych nie oznacza zgodności z RODO, choć może stanowić ułatwienie przy interpretacji przepisów[24].

Autorami kodeksów mają być zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające (art. 40 ust. 2 RODO) celem stworzenia samoregulacji należącej do kategorii *soft law*[25]. Samoregulacja „w kontekście gospodarki oznacza ogólnie, że podmioty gospodarcze przyjmują pewne zasady postępowania między sobą lub w stosunku do stron trzecich na rynku oraz w społeczeństwie i uzgadniają ich przestrzeganie między sobą bez żadnych zewnętrznych mechanizmów przymusu"[26]. Natomiast idea *soft law* polega na kompromisie, ponieważ podmioty chcące skorzystać z tego typu regulacji jednocześnie godzą się na związanie postanowieniami w tym prawie zawartymi. Brak jest w tym wypadku sformalizowanych, władczych procedur legislacyjnych i obecności zinstytucjonalizowanego przymusu w razie jego nieprzestrzegania[27]. To tak jak przystąpienie do gry – możemy stać się graczem, jeśli zgodzimy się przestrzegać reguł gry ze wszystkimi tego konsekwencjami (np. wykluczeniem z dalszego uczestnictwa przy graniu nie *fair*). Innymi słowy, przyjęcie kodeksu postępowania, choć dobrowolne, wiąże się z kontrolą jego przestrzegania i ewentualnymi negatywnymi konsekwencjami w przypadku nieprzestrzegania go (samoregulacyjny charakter)[28]. Przyjęcie tego typu rozwiązania stanowi „rękojmię stosowania reguł ochrony danych zawartych w kodeksie" oraz przykład aktywnego wdrażania RODO przez administratorów danych[29]. „Jeżeli jednak kodeks postępowania wprowadza wyższy standard ochrony danych osobowych niż przewidziany w powszechnie obowiązujących przepisach o ochronie danych osobowych, to jego naruszenie będzie rodziło

[23] A. Czarnowski [w:] *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, red. M. Gawroński, Warszawa 2018, s. 626.

[24] Bliżej na ten temat zob. *ibidem*, s. 626–631.

[25] U. Góral, P. Makowski [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, art. 40, s. 819, nb. 1.

[26] Pkt 3.2 opinii Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie samoregulacji i współregulacji we wspólnotowych ramach prawnych (opinia z inicjatywy własnej) (Dz. Urz. UE C 291 z 2015 r., s. 29).

[27] Por. P. Skuczyński, *Soft law w perspektywie teorii prawa* [w:] *System prawny a porządek prawny*, red. O. Bogucki, S. Czepita, Szczecin 2008, s. 334.

[28] U. Góral, P. Makowski [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 827, nb. 11.

[29] *Ibidem*, s. 820–821, nb. 3.

odpowiedzialność na zasadach określonych w kodeksie”[30]. Główny cel kodeksu postępowania, oprócz wspomnianej wcześniej samokontroli, to doprecyzowanie przepisów RODO pod względem rzetelnego i przejrzystego przetwarzania z dostosowaniem do specyfiki różnych sektorów dokonujących przetwarzania danych osobowych[31]. Powinien stanowić swoistą „instrukcję obsługi” dla osób wykonujących zawody medyczne i przetwarzających dane pacjentów, np. odpowiadać na pytania[32]:

1. W jaki sposób zapewnić anonimowość pacjentów w trakcie rejestracji przed wizytą?
2. W jaki sposób w czasie wzywania pacjentów do gabinetów można zapewnić im anonimowość, gdy placówka nie ma środków na wdrożenie elektronicznego systemu identyfikacji pacjentów (numerki wyświetlane nad gabinetami), a na korytarzu przebywa czasami ogromna liczba oczekujących?
3. Czy placówka zdrowia może na drzwiach gabinetów lekarskich zamieszczać imiona, nazwiska oraz specjalizacje lekarzy lub innych osób wykonujących zawód medyczny, przyjmujących pacjentów?
4. Czy lekarz lub inna osoba wykonująca zawód medyczny może na sali chorych rozmawiać z pacjentem o jego chorobie, gdy nie ma gwarancji, że nie słyszą tego inni pacjenci, a stan zdrowia pacjenta pozwala na przeprowadzenie takiej rozmowy poza salą chorych?
5. Czy RODO znajduje zastosowanie do wszelkich przypadków rozmów prowadzonych z pacjentem zarówno przez personel medyczny, jak i administrację szpitala?
6. Czy lekarz i personel medyczny na sali chorych może zwracać się do pacjentów po imieniu i nazwisku?
7. Czy możliwe jest oznaczanie produktów leczniczych imieniem i nazwiskiem pacjenta?
8. Czy podmiot leczniczy może uzależnić wgląd do dokumentacji medycznej osoby trzeciej od posiadania upoważnienia udzielonego przez pacjenta, którego dotyczy dokumentacja, opatrzonego własnoręcznym podpisem albo złożonym w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym?

---

[30] P. Drobek [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. D. Lubasz, Warszawa 2019, art. 27, s. 184, nb. 6.

[31] K. Iwańska [w:] *Ochrona danych medycznych. RODO w ochronie zdrowia*, red. M. Jackowski, Warszawa 2018, s. 224.

[32] Pytania pochodzą z projektu Kodeksu Postępowania dla Sektora Ochrony Zdrowia wydanego zgodnie z art. 40 RODO dotyczących podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających autorstwa: Polskiej Federacji Szpitali, Fundacji Telemedyczna Grupa Robocza, Pracodawców Medycyny Prywatnej, Konfederacji Lewiatan, Polskiej Izby Informatyki i Telekomunikacji, Federacji Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie oraz innych podmiotów tworzących Komitet sterujący, https://www.oil.szczecin.pl/upload/files/KODEKS%20POSTEPOWANIA%20DLA%20SEKTORA%20OCHRONY%20ZDROWIA.pdf (17.02.2022).

9. Czy podmiot leczniczy może wykorzystywać utrwaloną już metodę ujawniania informacji o stanie zdrowia w zakresie temperatury pacjenta na tzw. kartach przyłóżkowych (kartach zamieszczonych przy łóżkach szpitalnych pacjentów)?
10. Czy podmiot leczniczy może udostępniać telefonicznie informacje o fakcie hospitalizacji pacjentów o wskazanej przez rozmówcę tożsamości, gdy nie ma pewności co do tożsamości rozmówcy, ale udzielenie takich informacji może mieć wpływ na stan zdrowia bądź życie pacjenta?

Warto podkreślić w tym miejscu, że w motywie 148 preambuły do RODO uznano, że przy stosowaniu sankcji za naruszenie rozporządzenia użycie kodeksów postępowania powinno być brane pod uwagę. Przykładowo w treści rozporządzenie w art. 83 ust. 2 lit. j RODO regulującym nakładanie administracyjnych kar pieniężnych wskazano, że przy podejmowaniu decyzji, czy nałożyć karę, a jeśli tak, to w jakiej wysokości, organ powinien wziąć pod uwagę m.in. stosowanie zatwierdzonych kodeksów postępowania.

Sytuacja w Polsce

W Polsce Prezes Urzędu Ochrony Danych Osobowych (UODO) jest w rozumieniu rozporządzenia krajowym organem nadzorczym (art. 34 ust. 2 ustawy). To jemu przysługuje kompetencja do zatwierdzenia projektu kodeksu, jego rejestracji i publikacji (art. 40 ust. 5 i 6 RODO). Monitorowaniem zatwierdzonych kodeksów postępowania zajmuje się jednak nie on, a podmiot, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie będącej przedmiotem kodeksu i został przez niego akredytowany w tym celu. Wiedza fachowa w tym znaczeniu to nie tylko wiedza odnośnie do ochrony danych osobowych w ogóle, ale konkretnie wiedza w tym zakresie dla sektora, który dany kodeks obejmuje swoją regulacją (art. 41 ust. 1 *in fine* RODO). Warunki, jakie musi spełnić podmiot, aby mógł zostać akredytowany, określone zostały w art. 41 ust. 2 RODO. Należą do nich:

- wykazanie niezależności i wiedzy fachowej w dziedzinie będącej przedmiotem kodeksu,
- dysponowanie procedurami, które pozwalają mu ocenić zdolność konkretnych administratorów i podmiotów przetwarzających do stosowania kodeksu, monitorować przestrzeganie przez nich jego przepisów oraz okresowo dokonywać przeglądu jego funkcjonowania,
- dysponowanie procedurami i strukturami, które pozwalają rozpatrywać skargi na naruszenie kodeksu przez administratora lub podmiot przetwarzający lub na sposób wdrożenia lub wdrażania kodeksu przez administratora lub podmiot przetwarzający oraz które pozwalają zapewnić przejrzystość tych procedur i struktur dla osób, których dane dotyczą, i opinii publicznej,

– wykazanie w sposób satysfakcjonujący właściwemu organowi nadzorczemu, że jego zadania i obowiązki nie powodują konfliktu interesów.

Dokonanie akredytacji nie wpływa na zadania i uprawnienia organu nadzorczego (art. 41 ust. 1 RODO), Prezes UODO może monitorować przestrzeganie przepisów rozporządzenia[33]. Wynika z tego, że w istocie kodeks branżowy jest „instrumentem samoregulacyjnym o charakterze koregulacyjnym"[34]. „Współregulacja ogólnie rozumiana jest jako forma regulacji zainteresowanych stron, promowana, ukierunkowywana, prowadzona lub kontrolowana przez stronę trzecią – czy to organ urzędowy, czy niezależny organ regulacyjny, posiadający zwykle uprawnienia w zakresie kontroli i nadzoru, a niekiedy nawet nakładania sankcji"[35]. To, w jaki sposób monitorowanie ma przebiegać, powinno się znaleźć w treści kodeksu postępowania (art. 40 ust. 4 RODO).

W Polsce od momentu stosowania przepisów RODO wkrótce miną 4 lata[36], a mimo to żaden kodeks branżowy nie został zatwierdzony, a więc przyjęty do stosowania, w tym także w zakresie ochrony zdrowia. „Organ nadzorczy pozytywnie zaopiniował dwa projekty kodeksów postępowania, tj.:

1. projekt Kodeksu postępowania dot. ochrony danych przetwarzanych w małych placówkach medycznych (Porozumienie Zielonogórskie),
2. projekt Kodeksu postępowania dla sektora ochrony zdrowia dotyczący podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających (Polska Federacja Szpitali)"[37].

Gdzie w takim razie jest problem? Przy opracowywaniu kodeksu branżowego na pewno nie pomogła pandemia, kiedy to system ochrony zdrowia stanął przed obliczem bezprecedensowego wyzwania. Nie chodzi w tym wypadku o sam nieznany dotychczas koronawirus, ale także o zmiany w przepisach i procedurach, które często ulegały modyfikacjom, aby do rozprzestrzeniania się COVID-19 nie dochodziło. Doprowadzenie do końca nawet już rozpoczętych konsultacji uległo przesunięciu w czasie. Wiadomo, że przepisy RODO stosowane bez odpowiedniej wykładni uniemożliwiałyby prowadzenie działalności leczniczej, która wiąże się z przetwarzaniem danych wrażliwych. Powstaje pytanie, czy zatem pacjent w obecnie obowiązującym stanie prawnym ma zapewnioną dostateczną ochronę jego danych osobowych, skoro wykładnia dokonywana jest bez branżowych wskazań.

---

[33] P. Fajgielski, *Ogólne rozporządzenie o ochronie danych, ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022, s. 501, nb. 3.

[34] U. Góral, P. Makowski [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 829, nb. 12.

[35] Pkt 3.4 opinii Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie samoregulacji i współregulacji we wspólnotowych ramach prawnych (opinia z inicjatywy własnej).

[36] Artykuł oddany do publikacji w marcu 2022 r.

[37] https://uodo.gov.pl/pl/426/1110 (17.02.2022).

Od czasu wejścia w życie RODO co jakiś czas pojawiają się doniesienia, że już wszystko jest „prawie gotowe". Przykładowo pod koniec września 2019 r. informowano, że dwa kodeksy branżowe dotyczące ochrony danych osobowych w ochronie zdrowia zostały złożone do UODO. Jak wyżej wspomniano, jeden złożyła Polska Federacji Szpitali, a drugi – Federacja Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie[38]. Doniesienia ponad rok później, bo z listopada 2020 r., wskazywały, że Prezes UODO czeka na zaakceptowanie przez Europejską Radę Ochrony Danych wymogów dla podmiotów monitorujących kodeksy[39]. „W roku 2020 UODO przygotował wymogi akredytacji podmiotów monitorujących przestrzeganie postanowień kodeksów postępowania, które zostały poddane konsultacjom z zainteresowanymi, a następnie zostały przedstawione do zaopiniowania przez Europejską Radę Ochrony Danych. Po uwzględnieniu zaleceń EROD, organ nadzorczy udostępnił na swoich stronach internetowych aktualną wersję dokumentu: Wymogi akredytacji podmiotów monitorujących przestrzeganie postanowień kodeksów postępowania z 13.01.2021 r. (https://uodo.gov.pl/pl/file/3391, dostęp: 21.06.2021 r.)"[40]. Procedura ta przebiegała zgodnie z art. 41 ust. 3 RODO. Pod koniec maja 2021 r. poinformowano, że zgłosili się dwaj przedsiębiorcy chcący monitorować RODO w podmiotach leczniczych, jednak doprecyzowania wymaga nadal kwestia monitorowania podmiotów publicznych[41]. Wynika to z art. 41 ust. 6 RODO, który wyłącza stosowanie regulacji dotyczącej monitorowania zatwierdzonych kodeksów postępowania, gdy przetwarzanie danych następuje przez organy i podmioty publiczne.

Podsumowanie i wnioski

Na koniec, odpowiadając na zadane wcześniej pytania, trzeba wskazać, że bez przyjętego kodeksu branżowego w obszarze ochrony zdrowia nie można mówić o zagwarantowaniu dostatecznej ochrony danych osobowych pacjentów. Obecnie stosowane są różne praktyki w tym zakresie, nie wszystkie prawidłowe i zgodne z RODO. Warto np. zapoznać się z rozwiązaniami zaproponowanymi w projekcie Kodeksu Postępowania dla Sektora Ochrony Zdrowia wydanego zgodnie z art. 40

[38] A. Pochrzęst-Motyczyńska, *Kodeksy RODO dla ochrony zdrowia już prawie gotowe*, https://www.prawo.pl/zdrowie/jesienia-mozliwe-uchwalenie-kodeksow-rodo-dla-ochrony-zdrowia,478072.html (20.02.2022).

[39] J. Ojczyk, *RODO. Wkrótce ma być zatwierdzony pierwszy kodeks branżowy*, https://www.prawo.pl/biznes/rodo-kodeksy-branzowe-i-wytyczne-dla-podmiotow-monitorujacych,504522.html (20.02.2022).

[40] P. Fajgielski, *Ogólne rozporządzenie*…, s. 502, nb. 5.

[41] J. Ojczyk, *Dwie firmy chcą monitorować RODO w podmiotach medycznych*, https://www.prawo.pl/zdrowie/podmioty-monitorujace-kodeksy-postepowania-w-ochronie-zdrowia,508506.html (20.02.2022).

RODO dotyczących podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających autorstwa: Polskiej Federacji Szpitali, Fundacji Telemedyczna Grupa Robocza, Pracodawców Medycyny Prywatnej, Konfederacji Lewiatan, Polskiej Izby Informatyki i Telekomunikacji, Federacji Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie oraz innych podmiotów tworzących Komitet sterujący, gdzie w załączniku nr 3 pt. „Zasady postępowania w wybranych sytuacjach związanych ze zwiększonym ryzykiem naruszenia praw Pacjentów w związku z przetwarzaniem danych osobowych" znajduje się m.in. odpowiedź na zadane na początku pytanie: „Czy podmiot leczniczy może udostępniać telefonicznie informacje o fakcie hospitalizacji pacjenta o wskazanej przez rozmówcę tożsamości, gdy nie ma pewności co do tożsamości rozmówcy, ale udzielenie takich informacji może mieć wpływ na stan zdrowia bądź życie pacjenta?". Przy czym należy pamiętać, tak jak wskazano powyżej, że nie jest to powszechnie obowiązująca wykładnia przepisów ani tym bardziej regulacja prawna, a jedynie niezatwierdzony projekt, który nawet po dokonaniu stosownego zatwierdzenia należeć będzie do kategorii *soft law*. Takie swoiste wytyczne mają stanowić gotowe rozwiązanie dla często występujących w praktyce sytuacji. Mają one zaoszczędzić czas personelu medycznego, który sam nie musi wyinterpretować właściwej procedury postępowania. Wynika to z faktu, że taka interpretacja musi zostać dokonana na podstawie licznych norm prawa powszechnie obowiązującego, uregulowanego często w kilku aktach prawnych. Podkreślić należy, że niezależenie od przyjętych rozwiązań przepisy RODO nie mogą dezorganizować bądź ograniczać procesu udzielania świadczeń zdrowotnych. Ratowanie życia i zdrowia ludzkiego jest priorytetem i w takiej sytuacji może być poświęcone dobro nawet w postaci danych osobowych. Zawsze trzeba pamiętać o tym, że wykorzystywanie danych pacjenta powinno następować z poszanowaniem jego prywatności, intymności oraz godności, w tym jego prawa do zachowania w tajemnicy informacji z nim związanych zgodnie z ustawą o prawach pacjenta i Rzeczniku Praw Pacjenta. Podmioty lecznicze zainteresowane konkretnymi rozwiązaniami i przystąpieniem do zatwierdzonych kodeksów postępowania muszą sprawdzać informacje dotyczące prac nad projektami, które są dostępne na stronie internetowej UODO[42]. Na dzień oddania artykułu do publikacji nie można niestety stwierdzić, kiedy nastąpi finał prac. Z problemem tym borykają się również inne kraje członkowskie, których kodeksy branżowe w zakresie ochrony zdrowia także jeszcze nie zostały zatwierdzone.

Bibliografia

Czarnowski A. [w:] *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, red. M. Gawroński, Warszawa 2018.

[42] https://uodo.gov.pl/pl/426 (20.03.2022).

Drobek P. [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. D. Lubasz, Warszawa 2019.
Fajgielski P., *Ogólne rozporządzenie o ochronie danych, ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022.
Góral U., P. Makowski [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.
Iwańska K. [w:] *Ochrona danych medycznych. RODO w ochronie zdrowia*, red. M. Jackowski, Warszawa 2018.
Jagielski M. [w:] *Ochrona danych osobowych medycznych*, red. P. Litwiński, Warszawa 2018.
Mednis A. [w:] *System Prawa Medycznego*, t. III: *Organizacja systemu ochrony zdrowia*, red. D. Bach-Golecka, R. Stankiewicz, Warszawa 2020.
Ojczyk J., *Dwie firmy chcą monitorować RODO w podmiotach medycznych*, https://www.prawo.pl/zdrowie/podmioty-monitorujace-kodeksy-postepowania-w-ochronie-zdrowia,508506.html (20.02.2022).
Ojczyk J., *RODO. Wkrótce ma być zatwierdzony pierwszy kodeks branżowy*, https://www.prawo.pl/biznes/rodo-kodeksy-branzowe-i-wytyczne-dla-podmiotow-monitorujacych,504522.html (20.02.2022).
Pochrzęst-Motyczyńska A., *Kodeksy RODO dla ochrony zdrowia już prawie gotowe*, https://www.prawo.pl/zdrowie/jesienia-mozliwe-uchwalenie-kodeksow-rodo-dla-ochrony-zdrowia,478072.html (20.02.2022).
Skuczyński P., *Soft law w perspektywie teorii prawa* [w:] *System prawny a porządek prawny*, red. O. Bogucki, S. Czepita, Szczecin 2008.

Streszczenie

Rozporządzenie Parlamentu Europejskiego i Rady (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 (RODO) dotyczy wszystkich podmiotów, które przetwarzają dane osobowe osób fizycznych w związku z prowadzoną działalnością zawodową, zarobkową, statutową. Zostało skierowane do wielu branż, a jak wiadomo, każda branża jest inna, nie można porównać prowadzenia sklepu internetowego z wykonywaniem działalności leczniczej. Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu rozporządzenia. Kodeks branżowy ma podawać minimalne wymogi związane z ochroną danych osobowych w placówkach ochrony zdrowia, które należy spełnić, by być w zgodności z RODO. Założeniem jest uszczegółowienie kwestii dotyczących m.in. zbierania danych, czynienia zadość obowiązkowi informacyjnemu, sposobu zastosowania środków technicznych, aby do naruszenia danych osobowych nie dochodziło. Praktycznie przepisy RODO są stosowane od 4 lat, a do tego czasu żaden kodeks branżowy nie obowiązuje, w tym także w zakresie ochrony zdrowia. Przepisy RODO stosowane bez odpowiedniej wykładni uniemożliwiałyby prowadzenie działalności leczniczej, która wiąże się z przetwarzaniem danych wrażliwych. Czy zatem pacjent w obecnie obowiązującym stanie prawnym ma zapewnioną odpowiednią ochronę?

Słowa kluczowe: RODO, dane medyczne, ochrona zdrowia, działalność lecznicza, pacjent, kodeks branżowy

LACK OF A CODE OF CONDUCT IN THE HEALTH CARE SYSTEM AND THE PROTECTION OF PATIENT'S PERSONAL DATA

Summary

The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) shall concern all those who process personal data of natural persons with regard to their professional, commercial and statutory activities. It was addressed to many industries, and as it is well known each industry is different, running an online store cannot be compared with the provision of health care or treatment. The Member States, the supervisory authorities, the European Data Protection Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation. The code of conduct is to provide the minimum requirements related to the protection of personal data in health care facilities that must be met in order to demonstrate compliance with the GDPR. The purpose of the code is, inter alia, the collection of the personal data, fulfilling the obligation to inform and the use of technical means to prevent personal data breach. Almost four years have passed since the application of the GDPR regulations and no code of conduct has been adopted for application, including the health protection. The GDPR applied without proper interpretation would make it impossible to conduct medical treatment which involve sensitive data processing. In the current legal situation is a patient provided with adequate protection?

Keywords: GDPR, medical data, health protection, medical activity, patient, code of conduct