DOI: 10.24292/01.OT.300319.08

Ochrona danych osobowych – od czego zacząć?

Personal data protection – where to start?

Tomasz Osiej

Omni Modo sp. z o.o. w Warszawie
Prezes Zarządu: mec. Tomasz Osiej

NAJWAŻNIEJSZE

Niniejszy artykuł przedstawia podstawowe wymogi RODO, które muszą zostać wdrożone przez lekarzy w ramach prywatnej praktyki.

HIGHLIGHTS

This article presents the basic GDPR requirements that have to be implemented by the physicians within private medical practice.

STRESZCZENIE

Niniejszy artykuł skupia się na wymogach ogólnego rozporządzenia o ochronie danych w odniesieniu do prywatnych praktyk lekarskich. Rozpoczyna się od opisania 2 podstawowych funkcji, które może pełnić podmiot przetwarzający dane osobowe, tj. administratora oraz podmiotu przetwarzającego. Następnie przyporządkowano ww. role do lekarzy w zależności od charakteru ich pracy (w szpitalu lub w ramach prywatnej praktyki lekarskiej), wraz z opisem podstaw przetwarzania danych osobowych w sektorze ochrony zdrowia. Ostatnia część zawiera najważniejsze elementy ochrony danych, od których powinien zacząć każdy lekarz. Są nimi: wdrożenie odpowiednich technicznych oraz organizacyjnych środków bezpieczeństwa, przekazanie dokładnego obowiązku informacyjnego pacjentom, jak również wprowadzenie podstawowej dokumentacji dotyczącej danych osobowych, tj. rejestru czynności przetwarzania danych oraz procedury zgłaszania naruszeń ochrony danych osobowych.

Słowa kluczowe: ochrona danych osobowych, opieka zdrowotna, prywatna praktyka lekarska, administrator, podmiot przetwarzający, ogólne rozporządzenie o ochronie danych (RODO), podstawa prawna

ABSTRACT

The present article focuses on the main General Data Protection Regulation requirements for private medical practices. It starts with description of 2 basic capacities in which an entity processing personal data can act, i.e. the controller or processor. Then, aforementioned roles are allocated to the physicians depending on the nature of their work (hospital or private medical practice), together with the description of legal basis for personal data processing in healthcare sector. The last part contains the most important elements of data protection that any physician should start with. These are: implementation of adequate technical and organisational security measures, provision of accurate privacy notice to patients as well as introduction of basic personal data documentation, i.e. the records of processing activities and personal data breach notification procedure.

Key words: personal data protection, healthcare, private medical practice, controller, processor, General Data Protection Regulation (GDPR), legal basis

WSTĘP

Ogólne rozporządzenie o ochronie danych (dalej: RODO lub Rozporządzenie 679/2016/UE) ustanawia wiele wymogów, które muszą być spełnione przez każdy podmiot przetwarzający dane osobowe. Wyżej wymieniony akt znajduje zastosowanie również w branży medycznej. W niniejszym artykule przedstawiono najważniejsze elementy, na które należy zwrócić uwagę, organizując system przetwarzania danych osobowych przez lekarzy.

PRZYPORZĄDKOWANIE RÓL W PROCESACH PRZETWARZANIA

Pierwszym elementem, na który trzeba zwrócić uwagę przy przetwarzaniu danych osobowych, jest należyte przyporządkowanie ról w tym procesie. Co do zasady osoby przetwarzające dane mogą występować w 2 podstawowych rolach: administratora albo podmiotu przetwarzającego. Administrator to osoba fizyczna lub prawna, która określa środki i cele przetwarzania [1]. Innymi słowy to ktoś, kto „rządzi" całym procesem przetwarzania danych, jest tym elementem układanki, bez którego nic by się nie wydarzyło, czyli nie byłoby potrzeby przetwarzania danych. To na nim spoczywa podstawowy obowiązek zapewnienia, że przetwarzanie danych osobowych odbywa się zgodnie z prawem. Administrator musi więc m.in. wykazać się istnieniem podstawy prawnej przetwarzania, wprowadzić techniczne oraz organizacyjne środki ochrony danych osobowych, jak również spełnić obowiązek informacyjny wobec osób, których dane dotyczą. Natomiast podmiot przetwarzający dokonuje operacji przetwarzania w imieniu administratora, a jego podstawowym obowiązkiem jest należyte zabezpieczenie danych, które zostały mu powierzone (jest tylko i aż wykonawcą woli „właściciela danych", czyli np. dostawcą usługi przechowywania danych należących do kliniki okulistycznej).
W jaki sposób ww. role wpisują się w działalność lekarzy? Lekarze, w tym okuliści, wykonują działalność leczniczą w 2 podstawowych modelach: prowadzą swoją własną praktykę zawodową lub pracują w podmiocie leczniczym [2]. W przypadku prowadzenia własnej działalności medycznej lekarz okulista jest administratorem danych, co oznacza, że to on ponosi odpowiedzialność za zapewnienie spełnienia wszystkich podstawowych wymogów rozporządzenia. Sytuacja wygląda inaczej w przypadku, gdy lekarz jest zatrudniony w szpitalu. Wówczas to szpital (szerzej: podmiot medyczny) jest administratorem danych osobowych, natomiast lekarz przetwarza dane na podstawie upoważnienia wydanego przez tę instytucję. Tej ostatniej sytuacji nie należy jednakże mylić z powierzeniem przetwarzania danych, gdyż co do zasady lekarz nigdy nie występuje jako podmiot przetwarzający, co wynika m.in. z tego, że podlega on obowiązkowi zachowania tajemnicy lekarskiej [3].

PODSTAWY PRAWNE PRZETWARZANIA

Podstawą prawną przetwarzania danych przez lekarzy oraz szpitale będzie w znakomitej większości przypadków art. 9 ust. 2 lit. h) RODO, zgodnie z którym dopuszcza się przetwarzanie danych dotyczących zdrowia, jeżeli jest to: „niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń". Właściwe określenie podstawy prawnej przetwarzania jest bardzo istotne, ponieważ zależą od niej prawa przysługujące osobie, której dane dotyczą. Jedno z najbardziej popularnych praw na gruncie RODO, tj. prawo do usunięcia danych (zwane również prawem do bycia zapomnianym), nie ma co do zasady zastosowania, jeżeli dane są przetwarzane na podstawie ww. przepisu. Oznacza to, że osoba nie może żądać usunięcia swoich danych medycznych, powołując się na powyższe uprawnienia, chociaż w praktyce lekarze często spotykają się z takim żądaniem. Dodatkowo należy pamiętać, że lekarz nie potrzebuje zgody na przetwarzanie danych osobowych, a nawet nie powinien o nią prosić, ponieważ mogłoby to wprowadzać w błąd co do podstawy prawnej przetwarzania. Zgoda jako przesłanka ma swoje wady i wbrew powszechnej opinii nie jest najlepszą z przesłanek, przynajmniej w zakresie świadczeń medycznych (inaczej w marketingu, ale to osobne zagadnienie).

ORGANIZACJA SYSTEMU PRZETWARZANIA DANYCH PRZEZ LEKARZY

Od czego powinno się zacząć, organizując ochronę danych osobowych we własnej praktyce? Przede wszystkim należy zadbać o należyte zabezpieczenie danych osobowych. W przypadku lekarzy jest to w dużej mierze ułatwione, ponieważ ich działania podlegają tajemnicy, a co za tym idzie grupa ta jest szczególnie świadoma wagi zachowania poufności. Tym niemniej ochrona danych osobowych nie jest tym samym, co tajemnica lekarska [4], gdyż poza obowiązkiem zachowania poufności ustanawia ona również dodatkowe wymagania, takie jak np. konieczność spełnienia obowiązku informacyjnego.

Z uwagi na to, że dokumenty mogą być przechowywane w formie papierowej lub elektronicznej, właściwe wydaje się podzielenie środków ochrony danych osobowych w zależności od formy przechowywania informacji. W przypadku dokumentów papierowych podstawową kwestią jest zapewnienie, że do pomieszczenia, w którym są one przechowywane, nie mają dostępu osoby nieupoważnione. W praktyce oznacza to, że powinno być ono zamykane na klucz. Natomiast w przypadku spełnienia tego warunku nie ma obowiązku, aby dodatkowo zamykać na klucz szuflady z dokumentami. Jeżeli nie da się uniknąć wpuszczenia do pokoju osoby nieupoważnionej, np. z serwisu sprzątającego, należy pamiętać, aby nie pozostawiać jej samej. W odniesieniu do systemów informatycznych trzeba zwrócić uwagę na 2 rodzaje zagrożeń: zewnętrzne oraz wewnętrzne. Zagrożenia zewnętrzne dotyczą przede wszystkim Internetu. W przypadku, gdy systemy informatyczne są podłączone do sieci, należy zapewnić zainstalowanie oprogramowania antywirusowego, które aktualizuje bazę wirusów przynajmniej raz dziennie, a także włączenie zapory internetowej. Ponadto w przypadku przesyłania danych medycznych przez Internet trzeba zapewnić ich zaszyfrowanie oraz przekazanie klucza deszyfrującego w odrębnej wiadomości [5]. W odniesieniu do zagrożeń wewnętrznych należy przede wszystkim utworzyć każdej osobie mającej dostęp do systemu indywidualne konto oraz hasło, którym z nikim nie może się dzielić. Poza tym powinno się zagwarantować działanie mechanizmu pozwalającego na kontrolę tego, kto dokonał zmian w bazie danych pacjentów, jak również trzeba zapewnić istnienie kopii zapasowej danych. Drugim podstawowym elementem jest spełnienie obowiązku informacyjnego wobec osób, których dane dotyczą. Zakres informacji koniecznych do przekazania został określony w art. 13 RODO. Kluczowymi elementami tego obowiązku są właściwe wskazanie administratora danych oraz celu i podstawy prawnej przetwarzania – również dlatego tematom tym poświęcono nieco więcej miejsca na początku niniejszego artykułu. Należycie sformułowany obowiązek informacyjny nie tylko daje administratorowi możliwość wywiązania się ze swoich powinności, ale także pozwala na korzystanie ze swoich praw osobom, których dane dotyczą. W tym kontekście trzeba również zapewnić istnienie efektywnej ścieżki komunikacji z administratorem, np. przez pocztę elektroniczną lub telefon (jej forma jest dowolna). Następnym istotnym obowiązkiem administratora jest sporządzenie rejestru czynności przetwarzania danych osobowych obejmującego elementy, o których mowa w art. 30 Rozporządzenia 679/2016/UE, przy czym dobrą wiadomością jest to, że w przypadku lekarzy liczba tych procesów nie powinna być znaczna. Każdy administrator powinien również posiadać jasno określoną procedurę zgłaszania naruszeń ochrony danych organowi nadzorczemu, ponieważ termin na takie działanie wynosi jedynie 72 h od otrzymania wiadomości o wystąpieniu naruszenia.

PODSUMOWANIE

Celem niniejszego artykułu nie było wymienienie wszystkich obowiązków, jakie spoczywają na lekarzu jako administratorze danych, gdyż taki opis przekroczyłby zamierzoną objętość artykułu. Zamiast tego skupia się on na podkreśleniu najważniejszych, z punktu widzenia lekarza, elementów, które trzeba uwzględnić, organizując ochronę danych w swojej placówce. Należą do nich: zapewnienie bezpieczeństwa danych, należyte opisanie operacji przetwarzania i poinformowanie o tym osób zainteresowanych oraz spełnienie podstawowych wymogów w zakresie dokumentacji, tj. prowadzenie rejestru przetwarzania danych osobowych, a także posiadanie procedury zgłaszania naruszeń do organu nadzorczego. Naturalnie RODO przewiduje również inne wymagania, natomiast na początku warto sprawdzić, czy zapewniono przynajmniej przestrzeganie tych podstawowych, do pozostałych będziemy powracać w kolejnych artykułach.

Na koniec chciałem dodać, że moją ambicją jest także uczulenie na wszechobecne absurdy, jakie narosły wokół tematu, i wskazanie właściwych rozwiązań. Apeluję więc o ostrożność w sięganiu do źródeł, polecam oczywiście strony urzędów odpowiedzialnych za ochronę danych w Polsce, czyli urzędy ochrony danych osobowych oraz ministerstwa cyfryzacji, ale nie są to jedyne źródła. Istnieją też profesjonalne portale, jak chociażby prowadzony przez nas portal www.gdpr.pl, i pozycje książkowe, lecz najważniejszy jest zdrowy rozsądek, o czym przez cały czas będziemy starali się przypominać.

ADRES DO KORESPONDENCJI
mec. Tomasz Osiej
Omni Modo sp. z o.o.
03-910 Warszawa, al. Waszyngtona 40a, I p.
tel.: 505-165-660
e-mail: t.osiej@omnimodo.com.pl

Piśmiennictwo

1. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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 (ogólne rozporządzenie o ochronie danych); Dz.U. L 119 z 4.5.2016: 1-88.
2. Ustawa z dnia 25 kwietnia 2011 r. o działalności leczniczej (Dz.U. z 2018 r. poz. 2190).
3. Wytyczne dotyczące powierzenia przetwarzania danych Niemieckiej Konferencji Ochrony Danych [online: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf].
4. Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz.U. z 2018 r. poz. 617).
5. Pytania i odpowiedzi dotyczące ochrony danych osobowych w sektorze zdrowia, opublikowane przez rzecznika ds. ochrony danych oraz wolności informacji kraju związkowego Badania-Wirtembergia [online: https://www.baden-wuerttemberg.datenschutz.de/faq-datenschutz-in-der-arztpraxis/].