Zdrowie Publiczne i Zarządzanie 2022; 20 (2): 54–61
www.ejournals.eu/Zdrowie-Publiczne-i-Zarzadzanie, https://doi.org/10.4467/20842627OZ.22.010.17643

RODO w zdrowiu publicznym – wybrane aspekty praktyczne[1]

Paweł Lipowski[1] https://orcid.org/0000-0002-5056-1848
Iwona Kowalik[2] https://orcid.org/0000-0002-0492-4863

[1] Zakład Polityki Zdrowotnej i Zarządzania, Instytut Zdrowia Publicznego, Wydział Nauk o Zdrowiu, Uniwersytet Jagielloński Collegium Medicum
[2] Clinical Consulting Poland

Adres do korespondencji: Paweł Lipowski, Instytut Zdrowia Publicznego, ul. Skawińska 8, 31-066 Kraków, pawel.lipowski@uj.edu.pl

Abstract

Selected practical aspects of General Data Protection Regulation in public healthph

This article presents the characteristics of selected practical aspects related to the need to apply the provisions of the so-called General Data Protection Regulation (GDPR) in institutions classified as public health. The basic element of the considerations is the presentation of examples of violations of the provisions of the GDPR, and more broadly the provisions relating to the protection of personal data, which, observed in the daily functioning of selected public health institutions, may be an incentive to take preventive measures in all such institutions. At the same time, this paper presents potential remedies that may also take the form of so-called good practices. Being aware of the difficulties in applying the provisions of the GDPR, the authors, by presenting their observations, want to contribute to the discussion on the practical aspects of personal data protection in the area of public health, both in its practical and scientific terms.

Key words: GDPR, personal data protection, public health, data protection breaches

Słowa kluczowe: RODO, ochrona danych osobowych, zdrowie publiczne, naruszenia ochrony danych

Wprowadzenie

Rozumiane *sensu largo* podmioty uczestniczące w realizacji zadań z zakresu zdrowia publicznego generują znaczne ilości danych, dotyczących zarówno do ich przedmiotu działalności (w tym udzielanych świadczeń zdrowotnych), jak i – co wydaje się najistotniejsze —do samych beneficjentów tych działań (w tym pacjentów), przede wszystkim korzystających z udzielanej w tych podmiotach różnego rodzaju opieki medycznej (świadczeń)[2].

Powyższe implikuje konieczność ciągłego rozwoju oraz udoskonalania systemów gromadzenia i przetwarzania w ten sposób pozyskiwanych informacji. Kwestią kluczową jest przy tym dokonywanie permanentnej oceny skuteczności tych systemów ze względu na oczekiwany wysoki poziom ochrony danych dostępnych w podmiotach zdrowia publicznego o różnych rozmiarach prowadzonej działalności (zarówno gmin, jak i ministra właściwego ds. zdrowia). Prawne warunki dla zapewnienia tak rozumianej ochrony danych osobowych beneficjentów działań tych podmiotów (najczęściej obywateli lub osób przebywających nawet czasowo na terenie naszego kraju), zdefiniowane są w przepisach powszechnie obowiązującego prawa.

Celem niniejszego artykułu jest przedstawienie wybranych aspektów praktycznych związanych z koniecznością stosowania w podmiotach zdrowia publicznego przepisów tzw. ogólnego rozporządzenia o ochronie danych (RODO). Podstawowym elementem rozważań jest wskazanie na przykłady naruszeń postanowień RODO, a szerzej naruszeń przepisów odnoszących się do ochrony danych osobowych w obszarze dotąd w niewielkim stopniu „eksplorowanym naukowo", jakim jest działalność podmiotów zdrowia publicznego. Przykłady tego rodzaju deliktów zaobserwowane przez Autorów w codziennym funkcjonowaniu tych

podmiotów, a w szerszym ujęciu: systemu ochrony zdrowia, mogą stanowić asumpt do podjęcia działań o charakterze prewencyjnym także w innych tego typu podmiotach.

Jednocześnie w niniejszej pracy zaproponowano potencjalne środki zaradcze podejmowane w przypadkach naruszeń przepisów o ochronie danych, które mogą również przybierać formę tzw. dobrych praktyk. Autorzy, przedstawiając swoje obserwacje, wynikające z doświadczeń zawodowych i pracy naukowej, chcą tą drogą wpisać się w dyskusję o praktycznych aspektach ochrony danych osobowych w podmiotach zdrowia publicznego.

Prawna ochrona danych osobowych w podmiotach zdrowia publicznego – charakterystyka

Kluczowym aktem prawnym odnoszącym się do ochrony danych osobowych w naszym kraju jako państwie członkowskim Unii Europejskiej jest ogólne rozporządzenie o ochronie danych, tj. RODO[3] [1]. Rozporządzenie to w art. 4 pkt 1 za *dane osobowe* chronione przez przepisy tego aktu prawnego uznaje wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (np. obywatelu, pacjencie). Identyfikacja taka możliwa będzie na podstawie wskazania m.in. imienia i nazwiska, numeru identyfikacyjnego – w systemie informatycznym podmiotu zdrowia publicznego (np. numeru PESEL, numeru w księdze głównej podmiotu leczniczego) oraz jednego (lub kilku) szczególnych czynników określających: fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Czynniki te możemy uznać za opisujące stan zdrowia konkretnie wskazanego członka społeczeństwa (w tym pacjenta).

Przy czym RODO definiuje w art. 4 pkt 15 *dane dotyczące zdrowia* jako dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia (np. na podstawie udzielonych świadczeń zdrowotnych w systemie publicznym lub w ramach leczenia komercyjnego). RODO odnosi się również do *danych genetycznych* – zgodnie z art. 4 pkt 13 tego rozporządzenia są to dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby (np. z badania DNA uczestnika projektu badawczego z zakresu zdrowia publicznego)[4].

I wreszcie, w art. 4 pkt 14 RODO definiuje *dane biometryczne* jako dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne. Jak wskazują przykłady praktyczne, tego rodzaju dane, zwłaszcza te dotyczące cech behawioralnych, mogą być także przetwarzane w podmiotach zdrowia publicznego (np. w przypadkach stosowania kontroli dostępu do pomieszczeń, w przypadku prowadzenia badań naukowych w zdrowiu publicznym opartych na analizach socjologiczno-psychologicznych).

Warto dodać, że dane osobowe mogą znajdować się na dokumentach tworzonych zarówno w formie papierowej, jak i elektronicznej. Coraz powszechniej stosowane w podmiotach zdrowia publicznego pliki cyfrowe z tego rodzaju danymi mogą przy tym różnić się m.in. rodzajem danych oraz ich strukturą (wewnętrzną złożonością danych), *ergo* ich dostępnością. Mogą to być dane: tekstowe (np. opis stanu zdrowia uwzględniający dane genetyczne), obrazy (np. zdjęcie badania RTG), wideo (np. dynamiczny zapis badania diagnostycznego TK, CT, MR, PET), dźwiękowe (np. odczyt badania KTG) – przy czym w związku z rozwojem aparatury medycznej coraz częściej są to sygnały cyfrowe; dane osobowe mogą także znajdować się w nazwach i rozszerzeniach plików (np. identyfikacja imieniem i nazwiskiem pacjenta). Dane o stanie zdrowia mogą mieć również postać sygnałów cyfrowych generowanych przez aparaturę i sprzęt medyczny (np. na salach intensywnej opieki medycznej) i dodatkowo znajdować się w różnych plikach generowanych przez tego rodzaju wyroby medyczne. Wskazane rodzaje danych możemy uznać za dane kliniczne (ich źródłem będzie proces udzielania świadczeń zdrowotnych), a ich wykorzystanie może obejmować nie tylko ww. bezpośrednie korzystanie z usług zdrowotnych przez pacjentów, ale także przygotowanie analiz statystycznych (np. w celu monitorowania i oceny stanu zdrowia społeczeństwa) i opracowań naukowych (np. międzynarodowe projekty badawcze). Inne dane, które mogą być przetwarzane w podmiotach zdrowia publicznego, mogą pochodzić z rejestrów publicznych (np. w ramach tworzonych rejestrów o dostępności kadr medycznych, czy też Elektronicznej Platformy Gromadzenia, Analizy i Udostępnienia Zasobów Cyfrowych o Zdarzeniach Medycznych „P1") i być wykorzystywane do tworzenia dowolnych zestawień statystycznych (np. w ramach systemu obowiązkowej statystyki w ochronie zdrowia). Dotyczyć one mogą zbiorów informacji o zachowaniach jednostkowych i zbiorowych (populacji), uwarunkowaniach społecznych, efektywności udzielanych świadczeń zdrowotnych, zagrożeniach przed wystąpieniem chorób zakaźnych. Odrębny obszar danych osobowych dotyczyć może aspektów finansowych pozwalających na oferowanie komercyjnych usług medycznych. Wszystkie powyższe dane powinny być odpowiednio zabezpieczone (w tym przechowywane) zarówno w formie dokumentów papierowych, jak i w formie cyfrowej w systemach informatycznych czy też systemach składowania danych.

Wskazane wyżej czynniki (fizyczne, fizjologiczne, genetyczne lub psychiczne) składają się na opis stanu zdrowia obywatela (także jako pacjenta) traktowanego jako jego dobro osobiste, którym zgodnie z art. 23 Kodeksu cywilnego[5], jest *zdrowie*. Tak definiowane zdrowie – podobnie jak *nazwisko* (lub *pseudonim*), *wizerunek* (np. zdjęcie), *tajemnica korespondencji* (traktowana także *sensu largo* w procesie przekazywania danych o konkretnej osobie) – jako dobro osobiste, chronione jest przez przepisy Kodeksu (art. 24).

W przypadku osoby fizycznej (nie tylko pacjenta) ochrona jej wizerunku będzie opierała się także na regulacji

art. 81 ustawy o prawie autorskim i prawach pokrewnych[6]. Zgodnie z wyrażoną w tym przepisie zasadą rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej, czyli także pacjenta, którego wizerunek (mogący np. obrazować stan zdrowia) będzie utrwalany w ramach procesu terapii w podmiocie leczniczym oraz wykorzystywany w działalności naukowej podmiotów zdrowia publicznego (np. instytutów naukowo-badawczych, szkół wyższych)[7] [2].

Z kolei w przypadku pacjentów – także w rozumieniu uczestników programów profilaktycznych (niezależnie od źródła ich finansowania) – do ochrony tajemnicy korespondencji, wpisującej się w problematykę praw pacjenta, będzie się odnosiła regulacja ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta[8] [3]. Ten akt prawny, statuujący standard ochrony praw pacjenta w naszym kraju, wskazuje m.in. na prawo pacjenta do: tajemnicy informacji z nim związanych (art. 13–14 ww. ustawy), dokumentacji medycznej (art. 23–30a) oraz do poszanowania życia prywatnego i rodzinnego, w tym kontaktu korespondencyjnego z innymi osobami (art. 33)[9].

Należy przy tym dodać, że na podstawie art. 4 pkt 11 RODO zgoda osoby, której dane dotyczą („obywatela", „pacjenta"), oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli takiej osoby, w formie oświadczenia (np. ustnego) lub wyraźnego działania potwierdzającego (tzw. zgoda dorozumiana), przyzwalającego na przetwarzanie dotyczących jej danych osobowych [4]. Taka definicja wpisuje się w wymóg wyrażenia przez pacjenta zgody na udzielanie mu świadczeń zdrowotnych, wskazany m.in. w art. 16–18 ustawy o prawach pacjenta oraz w art. 32–35 ustawy o zawodzie lekarza i lekarza dentysty[10], a także w Kodeksie cywilnym (art. 60 i nast., normujące także postać elektroniczną oświadczenia woli). Definicja powyższa dotyczyć także będzie wymaganego przez przepisy prawa, w sytuacjach szczególnych, wyrażania zgody w formie pisemnej (np. w przypadku: zabiegów operacyjnych w podmiotach leczniczych, prowadzenia przez podmiot zdrowia publicznego – gminną komisję rozwiązywania problemów alkoholowych, działań związanych z zapobieganiem uzależnieniom oraz skutkom zdrowotnym i społecznym wynikającym z uzależnień u konkretnej osoby).

Warto przy tym podkreślić, że kluczowym pojęciem dla regulacji RODO jest *przetwarzanie danych* (art. 4 pkt 2). Przez przetwarzanie danych należy rozumieć operację lub zestaw operacji wykonywanych na danych osobowych (np. w ramach prowadzenia historii choroby, przygotowania indywidualnego programu edukacji zdrowotnej) lub na zestawach danych osobowych (np. księga raportów pielęgniarskich, oferta badań z zakresu profilaktyki chorób dla danej populacji) w sposób zautomatyzowany (np. w systemie informatycznym) lub niezautomatyzowany (tj. „odręcznie"). Będzie to zarówno zbieranie (np. pozyskanie danych identyfikujących daną osobę), utrwalanie (np. wpis w dokumentacji elektronicznej), organizowanie, porządkowanie, przechowywanie (tj. podejmowanie czynności w przypadku *sensu largo* przygotowania opracowań o wybranych aspektach zdrowia badanej populacji), jak i adaptowanie lub modyfikowanie takich danych (np. w ramach zestawień statystycznych lub finansowych o udzielonych świadczeniach zdrowotnych)[11] [5].

Z dniem wejścia w życie RODO do polskiego systemu prawnego wprowadzono również krajowy akt prawny odnoszący się do ochrony danych osobowych, tj. ustawę o ochronie danych osobowych[12]. Wskazana ustawa reguluje m.in. sprawy związane z wyznaczaniem Inspektora Ochrony Danych (IOD; jako osoby *de facto* odpowiedzialnej za obszar przetwarzania danych osobowych także w podmiotach zdrowia publicznego) oraz z działalnością organu nadzorczego w systemie ochrony danych osobowych w naszym kraju (tj. Prezesa Urzędu Ochrony Danych Osobowych; UODO), którego właściwość merytoryczna będzie odnosiła się także do ww. podmiotów [6].

Dopełniając charakterystyki aktów prawnych dotyczących ochrony danych osobowych, wskazać należy także na ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[13]. Ten akt prawny, odnoszący się do przetwarzania takich danych w systemach informatycznych – także charakteryzowanych podmiotów zdrowia publicznego, jako pierwszy w naszym kraju reguluje bezpośrednio problematykę cyfrowego bezpieczeństwa przetwarzanych danych.

Do tego obszaru ochrony danych osobowych odnosi się także ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[14]. Na podstawie delegacji ustawowej wskazanej w art. 18 tej ustawy Rada Ministrów przyjęła rozporządzenie w sprawie Krajowych Ram Interoperacyjności[15]. W akcie tym określono m.in. minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej (np. służących statystyce publicznej w ochronie zdrowia i rozliczaniu świadczeń zdrowotnych udzielanych w ramach powszechnego ubezpieczenia zdrowotnego) oraz minimalne wymagania dla systemów teleinformatycznych (np. systemów informatycznych stosowanych w podmiotach zdrowia publicznego).

Warto przy tym podkreślić, że art. 9 ust. 1 RODO zakazuje przetwarzania szczególnych kategorii danych osobowych (tzw. danych sensytywnych/wrażliwych), do których przepis ten zalicza dane genetyczne i biometryczne – w celu jednoznacznego zidentyfikowania osoby fizycznej (co dane te zapewniają – przyp. autorów) lub danych dotyczących zdrowia. Warto przy tym dodać, że w tej kategorii znajdują się również dane osobowe ujawniające: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane dotyczące seksualności lub orientacji seksualnej. W przypadku danych ujawniających pochodzenie etniczne, przekonania religijne lub światopoglądowe oraz dotyczących seksualności lub orientacji seksualnej – w podmiotach zdrowia publicznego może dochodzić do przetwarzania tego rodzaju danych (np. w ramach sporządzania oceny jakości życia wybranej populacji).

Zaznaczyć przy tym należy, że wśród 10 kategorii warunków dopuszczających takie przetwarzanie RODO (art. 9 ust. 2 lit. h) wskazuje w pierwszej kolejności na możliwość przetwarzania ww. danych, jeżeli jest to niezbędne do celów profilaktyki zdrowotnej (np. programów

zdrowotnych) lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej (np. w ramach udzielania świadczeń zdrowotnych), zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego (np. orzekanie w sprawach świadczeń z ubezpieczenia społecznego), leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego – np. w ramach kompetencji ministra właściwego ds. zdrowia[16]. Powyższe dotyczy także (art. 9 ust. 2 lit. i) – w drugiej kolejności – przetwarzania danych ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi (np. zagrożenie COVID-19), zapewnienia wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej (np. w ramach działań podejmowanych przez jednostki samorządu terytorialnego realizujących zadania własne z obszaru ochrony zdrowia) oraz produktów leczniczych lub wyrobów medycznych (np. działania Państwowej Inspekcji Farmaceutycznej i Prezesa Urzędu Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych).

Reasumując, charakteryzowany powyżej poziom prawnej ochrony danych osobowych w podmiotach zdrowia publicznego gwarantowany przez przepisy prawa powszechnie obowiązującego należy uznać za wysoki. Dotyczy to ustawodawstwa zarówno unijnego, jak i krajowego, przy czym zwraca uwagę wysoki stopień rozproszenia regulacji prawnych w systemie prawnym. Powyższe można wiązać *par excellence* z multidyscyplinarnością zdrowia publicznego jako obszaru poszukiwań naukowych. Ważnym przy tym zagadnieniem jest zwiększający się zakres przetwarzania danych obywateli w sposób częściowo i/lub całkowicie zautomatyzowany oraz w zbiorach danych, a więc w systemach informatycznych. Także w takim ujęciu celem działania podmiotów zdrowia publicznego powinno być zapewnienie adekwatnego poziomu ochrony obywateli (*in concreto* członków danej populacji), w związku z przetwarzaniem ich danych osobowych (uwzględniając ochronę zdrowia i życia jako dóbr nadrzędnych). Oznacza to jednak, że podnoszenie poziomu ochrony osób fizycznych w związku z przetwarzaniem danych osobowych zwiększa zakres obowiązków pracowników podmiotów zdrowia publicznego.

Praktyczne aspekty ochrony danych osobowych w podmiotach zdrowia publicznego

Odnosząc obserwacje do sfery praktycznej funkcjonowania podmiotów zdrowia publicznego, wskazać należy w pierwszej kolejności na główne („milowe") obszary wdrażania RODO. Będą to:

- spełnienie obowiązku informacyjnego (tzw. klauzula informacyjna dla osób korzystających z działań podejmowanych przez ww. podmioty), także w przypadku stosowania monitoringu wizyjnego, który jest szczególnym rodzajem przetwarzania danych osobowych[17];
- powołanie IOD;
- prowadzenie rejestru czynności przetwarzania (danych osobowych);
- dostosowanie infrastruktury IT (do właściwego przetwarzania danych osobowych)[18];
- usunięcie danych (realizacja prawa do tzw. bycia zapomnianym), sprzeciwu co do przetwarzania danych oraz przenoszenia danych, a także ewentualnego profilowania (pacjenta)[19];
- zawarcie umowy powierzenia przetwarzania danych (np. w przypadku korzystania z usług dostawcy systemu informatycznego);
- prowadzenie analizy ryzyka oraz oceny skutków przetwarzania dla ochrony danych;
- prowadzenie rejestru naruszeń bezpieczeństwa danych.

W ramach powyższych obszarów wdrażania RODO istotna wydaje się eliminacja głównych problemów determinujących stopień ochrony danych osobowych osób korzystających z usług podmiotów zdrowia publicznego (w szerokim i prezentowanym w niniejszej pracy rozumieniu tych podmiotów). Zaliczyć do nich możemy: nieznajomość zagadnień bezpieczeństwa danych osobowych przez personel uczestniczący w ich przetwarzaniu; nadawanie nieadekwatnych do obowiązków uprawnień do obsługi, a także administrowania systemami informatycznymi; niewystarczający poziom ochrony kopii bezpieczeństwa posiadanych zasobów informacyjnych oraz możliwość dostępu do danych osobowych również przez osoby do tego nieupoważnione.

Na tej podstawie, odnosząc także obserwacje do sfery praktycznej, wskazać należy na naruszenia bezpieczeństwa danych osobowych obywateli (korzystających z usług), które możemy zaobserwować w podmiotach zdrowia publicznego. Są to:

- wpisanie niepełnych danych osobowych pacjenta zakwalifikowanego do danej procedury medycznej (świadczenia zdrowotnego) i w konsekwencji otrzymanie dokumentacji medycznej innego pacjenta przez personel medyczny;
- ujawnienie pełnego numeru PESEL pacjenta podczas realizacji recepty na lek w aptece ogólnodostępnej;
- wpisanie w indywidualnej dokumentacji medycznej (historia choroby pacjenta) numeru PESEL lekarza/pielęgniarki/fizjoterapeuty w miejsce numeru prawa wykonywania zawodu (PWZ);
- zabranie przez pacjenta dokumentacji medycznej innego pacjenta wcześniej korzystającego z udzielanych w podmiocie leczniczym świadczeń zdrowotnych w ramach badania klinicznego leku[20];
- pozwolenie na skorzystanie (bez bezpośredniego nadzoru) przez pacjenta z telefonu komórkowego personelu urzędu administracji publicznej, zawierającego (prywatne) dane osobowe;
- przekazanie zwrotu środków za udzielone komercyjnie świadczenie zdrowotne na konto bankowe innej osoby (ze wskazaniem danych osobowych tej osoby);
- wysłanie przez personel urzędu administracji publicznej niezabezpieczoną pocztą elektroniczną tzw. zrzutów z ekranu komputerowego, zawierających dane o obywatelu (dane osobowe, takie jak imię i nazwisko, adres zamieszkania, numer telefonu), a także każde inne wysłanie takich danych, np. poprzez MMS (*Multimedia Messaging Service*) lub komunikator społeczny;

- przekazanie zaproszenia do udziału w lokalnym programie profilaktyki zdrowia (realizowanym przez jednostkę samorządu terytorialnego) z niezmienionymi danymi innej osoby;
- stosowanie jako kartki na notatki brudnopisów z danymi osobowymi (wydruki części dokumentacji medycznej prowadzonej w formie elektronicznej);
- pozostawianie otwartych pomieszczeń, w których przetwarza się dane osobowe obywateli (np. przechowuje się dokumentację medyczną), tj. pomieszczeń personelu medycznego i personelu urzędu administracji publicznej[21];
- wykonywanie kopii dokumentów potwierdzających tożsamość obywatela (np. legitymacja emeryta, karta osoby z niepełnosprawnością)[22];
- udostępnianie danych zawartych w dokumentacji medycznej osobom (zwłaszcza firmom ubezpieczeniowym) nieposiadającym stosownego (pisemnego i wyraźnego) upoważnienia ze strony pacjenta, bez weryfikacji tożsamości podmiotu (osoby) pobierającego takie dane pacjenta;
- dostęp do danych o stanie zdrowia konkretnego obywatela, przetwarzanych w systemie informatycznym, osób nieuprawnionych nieposiadających imiennego i ważnego upoważnienia do przetwarzania danych osobowych (np. pracowników działów kadrowych i finansowo-księgowych, osób wykonujących czynności pomocnicze przy udzielaniu świadczeń zdrowotnych)[23];
- dostęp do danych pacjentów w systemach informatycznych niezgodnie z zasadą odpowiednich (stopniowanych) uprawnień personelu medycznego[24];
- nieodpowiednia złożoność hasła w systemie informatycznym przetwarzającym dane osobowe (np. hasło niezawierające co najmniej ośmiu znaków, w tym liter: dużych, małych, znaków specjalnych i/lub cyfr)[25];
- dostęp do danych rejestrowanych przez kamery monitoringu wizyjnego przez nieuprawniony personel podmiotu zdrowia publicznego z możliwością przeglądania wcześniej zarejestrowanych danych i wykonywania ich kopii;
- korzystanie z oprogramowania antywirusowego bez aktualnych baz sygnatur wirusów i/lub korzystanie z oprogramowania systemu operacyjnego, dla którego wsparcie techniczne producenta się zakończyło[26];
- zgubienie, kradzież nośnika danych w dokumentacji medycznej (np. pendrive, płyta CD) oraz uszkodzenie dysku (także na serwerze) z bazami danych osobowych.

Naruszenia powyższe mogą być kwalifikowane jako tzw. incydenty bezpieczeństwa danych osobowych. Każdorazowo wymagać będą dokonania oceny stopnia zagrożenia dla danych osobowych i w konsekwencji potencjalnego zgłoszenia naruszenia ochrony danych osobowych do Prezesa UODO. Ocena taka powinna być dokonywana z punktu widzenia charakteru naruszenia i oparta na wymaganych przez RODO kluczowych kryteriach: poufności, integralności i dostępności danych. Z jednej strony ich wystąpienie może prowadzić do poważnych konsekwencji prawnych, a z drugiej – odnotowanie takich właśnie zachowań może przyczyniać się do wdrożenia odpowiednich środków zaradczych. Należy przy tym podkreślić, że utrata poufności danych, opisujących *sensu largo* stan zdrowia, jako danych szczególnej kategorii, może wiązać się z poważnymi konsekwencjami z uwagi na ochronę danych osobowych, której *sui generis* gwarantem są rozwiązania prawne statuujące idee tajemnicy zawodowej (osób wykonujących zawody medyczne, ale także pracowników urzędów administracji publicznej i uczelni wyższych).

Wskazać przy tym należy przykłady pozytywnych działań ponadstandardowych, które mogą być kwalifikowane jako tzw. dobre praktyki. Dotyczyć one mogą przede wszystkim tego rodzaju kontaktów obywateli z podmiotem zdrowia publicznego, które mają istotną doniosłość praktyczną z racji powszechności występowania i które możemy uznać za wymagające szczególnej uważności ze strony personelu tych podmiotów. Dotyczy to m.in. procesów pozyskiwania danych osobowych przez personel z zachowaniem maksymalnej poufności (np. samodzielny odczyt z przekazanych dokumentów tożsamości, bez konieczności podawania wszystkich danych ustnie przez daną osobę) oraz weryfikacji tożsamości danej osoby (gwarantującej pełną anonimowość)[27], a także pełnego ograniczenia dostępu obywatela do danych innych osób korzystających z usług danego podmiotu (np. przez „podglądnięcie danych" na ekranie komputera czy usłyszenie danych podczas rozmowy telefonicznej). Powyższe odnosi się w szczególności do całego procesu korzystania z opieki zdrowotnej, w tak szerokim ujęciu, jaki wskazuje ustawa o zdrowiu publicznym (np. edukacja zdrowotna, promocja zdrowia oraz ujmowane w ramach zdrowia publicznego: aktywność fizyczna i prowadzenie badań naukowych), w szczególności w czasie udzielania świadczeń zdrowotnych [7].

Anonimowość w tym względzie będzie zachowana w sytuacji, w której personel nie będzie posługiwać się imionami i nazwiskami. Należy przy tym podkreślić, że anonimizacja jako proces może być także sposobem zabezpieczenia danych, a ochrona danych nie obejmuje danych zanonimizowanych, ponieważ tych informacji nie można powiązać z określonymi osobami. Proces ten jest trwały i nieodwracalny, a takimi danymi mogą posługiwać się np. osoby prowadzące badania statystyczne/naukowe działające w obszarze zdrowia publicznego. Tak rozumiana anonimizacja nie będzie miała zastosowania w pełnym zakresie w podmiocie zdrowia publicznego (leczniczym).

We wszystkich tych przypadkach szczególnego znaczenia nabiera kwestia świadomości personelu podmiotów zdrowia publicznego, która może być podnoszona poprzez system systematycznych szkoleń. Jest to obowiązek IOD określony w art. 39 ust. 1 lit. b RODO, a jego wypełnienie zdefiniowane jest jako stałe odnawianie i uzupełnianie wiadomości związanych z przetwarzaniem danych osobowych. Ma on szczególne znaczenie w obecnych realiach funkcjonowania podmiotów zdrowia publicznego ze względu na specyfikę działalności medycznej (np. rotację pracowników).

Reasumując, istotne wydaje się podkreślenie, że wskazane powyżej w sposób przykładowy praktyczne aspekty ochrony danych osobowych w podmiotach zdrowia publicznego można uznać także za pewną egzemplifikację dysfunkcji w działalności tych podmiotów. Odniesienie

poczynionych obserwacji do funkcjonowania danego podmiotu może sprzyjać zmianie tych przejawów, które kwalifikować możemy jako obszary ryzyka w przetwarzaniu *in concreto* danych osobowych. Wydaje się przy tym istotne, że dotyczy to nie tylko korzystania ze świadczeń zdrowotnych, ale także wyżej wskazanej działalności w dziedzinie zdrowia publicznego definiowanej prawnie [8].

Podsumowanie

Podsumowując, należy przyjąć, że kluczową rolę we właściwym stosowaniu przepisów odnoszących się ochrony danych osobowych w podmiotach zdrowia publicznego, których prawny standard obowiązuje w polskim ustawodawstwie od maja 2018 r., odgrywa personel tych podmiotów. Wydaje się, że konieczne zmiany dotychczasowych, często rutynowych zachowań personelu tego rodzaju podmiotów, o różnej złożoności zarówno struktury organizacyjnej, jak i realizowanych zadań w dziedzinie zdrowia publicznego, mogą być pozytywnie implikowane przeprowadzaniem systematycznych szkoleń – także wymaganych przez przepisy RODO. Tego rodzaju działania mogą, poza funkcją edukacyjną, odgrywać istotną rolę prewencyjną dla podmiotów prowadzących działalność w obszarze zdrowia publicznego, niezależnie od systemowego umiejscowienia tych podmiotów, ich struktury własnościowej oraz zakresu przypisanych im zadań, realizowanych *de facto* i *de iure*.

Kolejnym czynnikiem mogącym bezpośrednio wpływać na stan przestrzegania zarysowanego w niniejszej pracy prawnego standardu ochrony danych osobowych są niezbędne zmiany w infrastrukturze technicznej podmiotów zdrowia publicznego. Dotyczy to przede wszystkim stosowanych systemów informatycznych, w tym operacyjnych a także oprogramowania komputerowego (służącego do gromadzenia danych o stanie zdrowia społeczeństwa).

W zagadnienie to wpisuje się również standard zapewnienia cyberbezpieczeństwa, określony w przepisach prawa, który powinien zapewniać poszanowanie prywatności i intymności każdej osoby w procesie udzielania jej świadczeń zdrowotnych, a więc w wymiarze najczęściej utożsamianym ze zdrowiem publicznym. Odpowiednie rozwiązania techniczne (infrastruktura techniczna) i organizacyjne (organizacja pracy personelu) mogą minimalizować ryzyko naruszenia praw w tym zakresie.

Należy mieć na uwadze, że RODO wprowadza jedynie ogólne zasady zarządzania bezpieczeństwem danych osobowych. Konieczne wydaje się zatem przestrzeganie szczególnych wymagań, które zapewnią bezpieczeństwo tych danych, a także – co najistotniejsze – przyjmowanej na podstawie RODO pragmatyki jego stosowania (także opartej na tzw. dobrych praktykach i interpretacji – ogólnych jednak – postanowień). Przetwarzanie danych osobowych powinno odbywać się rzetelnie, zgodnie z prawem oraz w sposób przejrzysty dla osoby, której dane są przetwarzane. Konieczna jest ocena stopnia ryzyka i skutków dla ochrony danych. Dotyczy to także stosowanej zwłaszcza w mniejszych podmiotach (instytucjach) zdrowia publicznego praktyki przekazywania przetwarzania danych osobowych zewnętrznym podmiotom przetwarzającym.

Trudność w (praktycznym) stosowaniu przepisów RODO może także wynikać z faktu, że ta sama informacja dla jednego podmiotu zdrowia publicznego może być jedną z danych osobowych, natomiast dla innego nią nie jest, ponieważ identyfikacja konkretnej osoby wymagałaby zwiększonego nakładu: finansowego, czasowego i technicznego. Ważne jest, aby osoba pracująca z danymi w analizowanym podmiocie umiała odróżnić informacje dotyczące osoby od danych osobowych. Warto także zaznaczyć, że dane osobowe bez rozszerzonych, a tym bardziej bez podstawowych, zabezpieczeń niosą ryzyko zagrożenia życia prywatnego, które są wypadkową rozwoju informatycznego i postępu gospodarczego. Naruszenie dobrego imienia, szkoda gospodarcza i społeczna, utrata reputacji (zaufania), a także wymierna strata finansowa (kara administracyjna nakładanana przez Prezesa UODO) mogą być poważnymi skutkami incydentu z zakresu ochrony danych dla konkretnego podmiotu zdrowia publicznego.

Przestrzeganie scharakteryzowanych powyżej przepisów jest istotne z punktu widzenia ochrony prywatności obywateli, zwłaszcza wtedy, kiedy ujawnienie danych może istotnie naruszyć prywatność obywatela jako pacjenta, a nawet stać się przyczyną stygmatyzacji. Podmioty działające w obszarze zdrowia publicznego obejmują swym działaniem większość społeczeństwa, co sprowadza się do pozyskiwania, gromadzenia oraz przetwarzania danych osobowych niemalże wszystkich obywateli w kraju. I właśnie dlatego gromadzone przez nie dane, które dotyczą przeszłego, teraźniejszego i przyszłego stanu zdrowia konkretnych osób, powinny być chronione w szczególny sposób.

Przypisy

1. Praca powstała w ramach działalności Studenckiego Koła Naukowego „Prawo w zdrowiu" działającego przy Instytucie Zdrowia Publicznego Collegium Medicum Uniwersytetu Jagiellońskiego w Krakowie.
2. Podmioty realizujące zadania z zakresu zdrowia publicznego wskazuje art. 3 ustawy z dnia 11 września 2015 r. o zdrowiu publicznym (Dz.U. z 2022 r. poz. 1608); zwanej dalej ustawą o zdrowiu publicznym. Ustawa ta jest pierwszym aktem prawnym w dziedzinie zdrowia publicznego w naszym kraju i w swojej zasadniczej części obowiązuje od dnia 3 grudnia 2015 r. Warto dodać, że zadania z zakresu zdrowia publicznego definiuje art. 2 ww. ustawy. Dla jasności dalszego wywodu autorzy będą się posługiwać pojęciem „podmiot zdrowia publicznego".
3. Rozporządzenie 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. UE L z 2016 r. Nr 119, s. 1 ze zm.); zwane dalej w skrócie: RODO. Rozporządzenie to weszło w życie z dniem 24 maja 2016 r., ma zastosowanie w krajach UE od dnia 25 maja 2018 r.

4. Na marginesie można dodać, że do badań klinicznych prowadzonych w obszarze zdrowia publicznego będą odnosiły się, znowelizowane w 2022 r., m.in. przepisy art. 37–37al (w rozdziale 2a) ustawy z dnia 6 września 2001 r. Prawo farmaceutyczne (Dz.U. z 2022 r. poz. 2301).
5. Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. z 2022 r. poz. 1360 ze zm.); zwana dalej Kodeksem cywilnym.
6. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2022 r. poz. 2509).
7. Termin *podmiot leczniczy* w sposób legalny definiuje art. 4 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz.U. z 2022 r., poz. 633 ze zm.). W art. 2 pkt 5 ww. ustawy wprowadzono legalną definicję *podmiotu wykonującego działalność leczniczą* i zgodnie z tą definicją jest to pojęcie o znaczeniu szerszym od pomiotu leczniczego. Podmiotem wykonującym działalność leczniczą jest zarówno podmiot leczniczy, o którym mowa w ww. art. 4 ustawy (m.in. przedsiębiorca oraz samodzielny publiczny zakład opieki zdrowotnej), jak i lekarz (lekarz dentysta), pielęgniarka (położna) lub fizjoterapeuta – wykonujący zawód w ramach działalności leczniczej jako praktykę zawodową..
8. Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2022 r. poz. 1876 ze zm.), zwana dalej ustawą o prawach pacjenta. Zgodnie z tą ustawą (art. 3 ust. 1 pkt 4) pacjentem jest osoba zwracająca się o udzielenie świadczeń zdrowotnych (np. podczas procesu rejestracji) lub korzystająca ze świadczeń zdrowotnych udzielanych przez podmiot udzielający świadczeń zdrowotnych (czyli podmiot leczniczy w powyższym rozumieniu – przyp. autorów) lub osobę wykonującą zawód medyczny (np. technika farmaceutycznego wydającego lek na receptę).
9. Do zagadnienia dokumentacji medycznej odnosi się z kolei wydane na podstawie ustawy o prawach pacjenta rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. z 2022 r. poz. 1304 ze zm.). Innym aktem prawnym z tego zakresu jest rozporządzenie Ministra Zdrowia z dnia 8 maja 2018 r. w sprawie rodzajów elektronicznej dokumentacji medycznej (Dz.U. z 2021 r. poz. 1153 ze zm.), wydane na podstawie ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2022 r., poz. 1555 ze zm.). Zagadnienie to pozostanie jednak poza głównym nurtem rozważań w niniejszej pracy.
10. Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz.U. z 2022 r. poz. 1731 ze zm.).
11. Zgodnie z ww. przepisem dotyczyć to będzie także pobierania, przeglądania, wykorzystywania, ujawniania poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie – danych osobowych.
12. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781). Ustawa ta uchyliła pierwszy akt prawny obowiązujący w polskim ustawodawstwie, odnoszący się do poruszanej problematyki, jakim była ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst pierwotny Dz.U. z 1997 r. Nr 133, poz. 883), obowiązująca od 30 kwietnia 1998 r. Ustawa ta została przyjęta przed akcesją Polski do Unii Europejskiej i wdrażała dyrektywę Nr 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. WE L Nr 281 z dnia 23 listopada 1995 r., s. 31). Dyrektywa ta w ustawodawstwie UE poprzedzała RODO.
13. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2022 r. poz. 1863 ze zm.). Ustawa ta weszła w życie z dniem 28 sierpnia 2018 r. jako pierwszy akt prawny w tym zakresie.
14. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r. poz. 2070 ze zm.). Ustawa weszła w życie z dniem 21 lipca 2005 r. i była również pierwszym aktem prawnym w tej dziedzinie w naszym kraju.
15. Rozporządzenie z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247). Rozporządzenie obowiązuje od dnia 31 maja 2012 r., utraci swoją moc obowiązującą z dniem 23 maja 2024 r.
16. Dane te mogą być przetwarzane (art. 9 ust. 3 RODO), jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej, tj. osoby wykonującej zawód medyczny podlegającej potencjalnie odpowiedzialności prawnej (w tym cywilnej i karnej).
17. Warto dodać, że obowiązek poinformowania pacjenta (uczestnika programu profilaktycznego) o rejestracji obrazu (i dźwięku) podczas udzielania mu świadczeń zdrowotnych dotyczy całego procesu ich świadczenia (także wskutek podjęcia takiej decyzji w trakcie tak rozumianego korzystania ze świadczeń).
18. Tytułem przykładu można wskazać na korzystne z punktu widzenia ochrony danych obywatela oprogramowanie przetwarzające jego dane osobowe na numer (np. recepty, skierowania) i/lub zapis kodu paskowego.
19. Wspomnieć należy, co jest szczególnie istotne w przypadku placówek prowadzących działalność komercyjną, że pacjent ma prawo sprzeciwu wobec przetwarzania danych dla celów marketingu bezpośredniego oraz profilowania w celu podjęcia w przyszłości względem niego bezpośrednich działań marketingowych (np. podczas przyszłych rozmów telefonicznych lub informacji przekazywanych drogą e-mailową o oferowanych usługach medycznych). Warto także dodać, że w przypadku prowadzenia dokumentacji medycznej, także w ramach badań naukowych, prawo do usunięcia danych i sprzeciwu co do przetwarzania danych oraz przenoszenia danych będzie podlegało znacznym ograniczeniom, wskazanym w ww. regulacjach prawnych (odnoszących się do prowadzenia dokumentacji medycznej i eksperymentów medycznych w formule np. badań klinicznych).
20. W tej grupie naruszeń będą się również mieścić: pozostawienie dokumentacji medycznej w miejscu nieograniczonego dostępu do niej dla osób trzecich (np. w toalecie, na kserokopiarce zlokalizowanej na korytarzu placówki), czy też odebranie wyników badań innego pacjenta (np. w wyniku umieszczenia w kopercie z dokumentacją medyczną wyników badań innej osoby).
21. W tej grupie naruszeń mogą mieścić się także sytuacje pozostawienia klucza w zamkach drzwi do tych pomieszczeń, otwartych szafek, nieprzestrzeganie zasad tzw. czystego ekranu i czystego biurka oraz kontrowersyjne ww. stosowanie zamków opartych na danych biometrycznychnaychych personelu. Wyżej wymienione zasady polegają na usuwaniu z niezabezpieczonego miejsca pracy danych osobowych w wersji papierowej oraz znajdujących się na elektronicznych nośnikach, a także na stosowaniu wygaszaczy ekranu w przypadku korzystania z urządzeń wyświetlających dane osobowe.

22. Podobnie może to dotyczyć zbędnego przechowywania (przetrzymywania) dokumentu tożsamości jako tzw. zastawu w miejscu i w sposób niezabezpieczony (np. zatrzymanie przez portiera dowodu osobistego w zamian za wpuszczenie do konkretnego urzędu administracji publicznej).
23. Szczególna odpowiedzialność w tym względzie będzie ciążyła na osobie pełniącej funkcję administratora systemów informatycznych (ASI) w podmiocie zdrowia publicznego oraz osobie przeprowadzającej szkolenie z zakresu ochrony danych osobowych przed rozpoczęciem wykonywania obowiązków pracowniczych (i przed wydaniem upoważnienia do przetwarzania danych). Wprowadzenie takiego rozwiązania ma za zadanie zwiększenie nadzoru, a w konsekwencji weryfikację zasadności dostępu do ww. danych sensytywnych. Na marginesie można wskazać, że administratorem danych osobowych (ADO) będzie najczęściej właściciel lub osoba zarządzająca (w imieniu „właściciela") – decydująca o celach i sposobach przetwarzania, a funkcję IOD będzie pełnił najczęściej wyznaczony pracownik tego podmiotu. Odnotować także należy szczególną odpowiedzialność za stworzenie właściwych warunków do przetwarzania danych osobowych dla osób wyłącznie czasowo dopuszczonych do ich przetwarzania (czasowo zatrudnionych), takich jak praktykanci i wolontariusze. Istotne przy tym będzie dokładane odnotowanie daty przyznania dostępu (np. w systemach informatycznych) i daty jego zakończenia. W tym kontekście należy również wskazać na konieczność (właśnie) niezwłocznego odbierania osobom, które przestały świadczyć pracę na rzecz danego podmiotu, uprawnień w systemach informatycznych tego podmiotu, tak aby uniemożliwić im jakikolwiek do nich dostęp.
24. Wyrazem zapewnienia takiej ochrony będzie przyznawanie uprawnień dostępu dla pracowników medycznych komórek organizacyjnych konkretnego podmiotu leczniczego (gabinetów, poradni, oddziałów) tylko takich danych pacjentów, które są konieczne do świadczenia przez nich pracy.
25. Należy wskazać na zapewnienie właściwego procesu autoryzacji użytkowników w systemie operacyjnym, usługach sieciowych (świadczonych przez internet) i stosowanych aplikacjach informatycznych (służących np. prowadzeniu zestawień statystycznych w zakresie oceny stanu zdrowia społeczeństwa, zagrożeń zdrowia oraz jakości życia związanej ze zdrowiem społeczeństwa). Zgodnie z wykształconym standardem w tym względzie każdy użytkownik systemu operacyjnego powinien posiadać indywidualny login i hasło, tak aby tymi samymi danymi do autoryzacji w systemach operacyjnych nie posługiwała się grupa osób (np. wszyscy pracownicy danej komórki organizacyjnej w podmiocie zdrowia publicznego). Niezbędne jest także każdorazowe wymaganie indywidualnego uwierzytelniania i brak możliwości uruchomienia systemu operacyjnego bez podania loginu i hasła o odpowiedniej złożoności (jego systematyczna, np. comiesięczna, zmiana powinna być wymuszana przez taki system, oczywiście bez zapisywania tych danych przy stanowisku pracy). Po dłuższym braku aktywności właściwym rozwiązaniem jest blokada dostępu i standardowe wygaszanie ekranu przy opuszczaniu stanowiska.
26. W tym kontekście można wskazać także na przypadki zbędnego zgłaszania danych umożliwiających pełną identyfikację danej osoby (ustalenie jego tożsamości) przez personel podmiotów zdrowia publicznego, usterek oprogramowania podmiotom serwisującym. Taka sytuacja daje możliwość implementowania publikowanych aktualizacji zabezpieczeń tych produktów, poprawek opcji asystowanej pomocy technicznej oraz aktualizację zawartości technicznej w trybie on-line. Warto przy tym podkreślić, jak ważne jest nadawanie właściwych uprawnień w systemach operacyjnych (przez pracowników odpowiedzialnych za obszar IT), przejawiające się np. w uniemożliwieniu instalacji dowolnego oprogramowania na użytkowanych komputerach, wyłączenia ochrony antywirusowej, korzystania z dowolnych nośników danych oraz ingerowania w inne ustawienia systemów informatycznych. Niedopuszczalne jest zwłaszcza posiadanie przez personel uprawnień administratora systemów operacyjnych wykorzystywanych komputerów
27. Dotyczyć to może także przypadków złamania tzw. zasady minimum trzech pytań służących do identyfikacji danej osoby (także pacjenta), zwłaszcza podczas rozmowy telefonicznej, której personel danego podmiotu powinien dokonać podstawie posiadanych danych (np. dokumentacji papierowej i/lub elektronicznej).

Piśmiennictwo

1. Fajgielski P., *Komentarz do ustawy o ochronie danych osobowych*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, wyd. II, Wolters Kluwer Polska, Warszawa 2021.
2. *Ustawa o działalności leczniczej. Komentarz*, red. M. Drecz, T. Rek, wyd. III, Wolters Kluwer Polska, Warszawa 2019.
3. Karkowska D., *Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta. Komentarz*, wyd. I, Wolters Kluwer Polska, Warszawa 2021.
4. Litwiński P., *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Wydawnictwo „Beck", Warszawa 2021.
5. *Ustawa o ochronie danych osobowych. Komentarz*, red. D. Lubasz, Wolters Kluwer Polska, Warszawa 2019.
6. Czerniawski M., *Ustawa o ochronie danych osobowych. Komentarz*, Wydawnictwo „Beck", Warszawa 2019.
7. *Ustawa o zdrowiu publicznym. Komentarz*, red. M. Dercz, Wolters Kluwer Polska, Warszawa 2016.
8. Włodarczyk W.C., *Współczesna polityka zdrowotna: wybrane zagadnienia*, Wolters Kluwer business, Warszawa 2014.