Kompendium wiedzy dla placówek w zakresie RODO

Projekt „Zdrowe Firmy Zdrowi Ludzie podniesienie jakości w POZ” jest realizowany w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014–2020 i współfinansowany ze środków Europejskiego Funduszu Społecznego.

Fundusze Europejskie Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Unia Europejska Europejski Fundusz Społeczny

Spis treści

Rozdział I.	Rola administratora danych w świetle przepisów o ochronie danych osobowych	3
Rozdział II.	Inspektor Ochrony Danych – doradca w zakresie ochrony danych osobowych	17
Rozdział III.	Pracownik jako element systemu ochrony danych osobowych	29
Rozdział IV.	Dokumentacja ochrony danych osobowych w placówce medycznej	36
Rozdział V.	Wiedza oraz świadomość pracowników odnośnie ochrony danych osobowych	46
Rozdział VI.	Konieczność ochrony prawnej placówek medycznych, zgodność z prawem regulacji wewnętrznych, wzorów dokumentów i formularzy, konieczność oceny prawnej projektów umów	57
Rozdział VII.	Konsekwencje funkcjonowania RODO dla praw pracowników (Kodeks pracy) i pacjentów (Ustawa o prawach pacjentów i Rzeczniku Praw Pacjenta)	69
Rozdział VIII.	Zasady wydawania i ewidencjonowania wydawania dokumentacji medycznej; konieczność wdrożenia właściwych procedur zgodnych z RODO i ustawami regulującymi funkcjonowanie służby zdrowia	77
Rozdział IX.	Współpraca placówki medycznej z podmiotami zewnętrznymi przy przekazywaniu danych osobowych	92
Rozdział X.	Organizacja pracy placówki medycznej a bezpieczeństwo administratora	102
Rozdział XI.	Archiwizacja danych osobowych	115

Rozdział I. Rola administratora danych w świetle przepisów o ochronie danych osobowych

Obecne przepisy o ochronie danych osobowych (obowiązujące od maja 2018 r.) różnią się od wcześniejszych. Kiedyś więcej było konkretnych obowiązków. Przepisy jasno wskazywały, jak ma wyglądać polityka bezpieczeństwa czy instrukcja zarządzania systemem informatycznym. Nawet minimalna długość haseł była konkretnie uregulowana.

Wejście w życie RODO oznaczało zmianę o 180 stopni. Ogólne rozporządzenie o ochronie danych ma bardzo niewiele konkretnych zaleceń. Jego główne przesłanie brzmi: „Administratorze, oceń ryzyko związane z ochroną danych osobowych. Potem zrób tak, żeby te dane były bezpieczne i żebyś mógł to udowodnić w razie kontroli".

Przyczyna takiej sytuacji jest jasna. Postęp technologiczny nie ustaje. To, co kiedyś było ostatnim krzykiem mody i zabezpieczeniem nie do sforsowania, teraz budzi jedynie uśmiech politowania. Nowe przepisy o ochronie danych osobowych pisano tak, by mogły być wykorzystywane przez około 20 lat. Nie mogą zatem dawać zbyt konkretnych zaleceń. Zamiast tego nacisk kładzie się na analizę ryzyka i przestrzeganie zasad ogólnych.

Ogólne zasady

RODO wskazuje siedem ogólnych zasad ochrony danych osobowych. Są to:

- zgodność z prawem, rzetelność i przejrzystość
- ograniczenie celu
- minimalizacja danych
- prawidłowość
- ograniczenie przechowywania
- integralność i poufność
- rozliczalność.

Zasady te omówimy w dalszej części tekstu.

Zgodność z prawem, rzetelność i przejrzystość

Za każdym razem, kiedy placówka medyczna wykorzystuje czyjeś dane osobowe (pacjenta, pracownika, przedstawiciela kontrahenta), musi to robić:

- **zgodnie z prawem** – przede wszystkim zgodnie z RODO, ale także polskimi przepisami medycznymi, np. ustawą o prawach pacjenta
- **rzetelnie i przejrzyście** – w sposób zrozumiały dla pacjenta, pracownika lub innej osoby.

Zgodnie z przepisami w dokumentacji dorosłego pacjenta mają się znaleźć następujące dane osobowe na jego temat: imię, nazwisko, data urodzenia, płeć, adres miejsca zamieszkania, numer PESEL.

Zbieranie tych danych na podstawie zgody pacjenta jest niezgodne z prawem (podstawą będzie tu nie zgoda, ale przepis prawa) i nierzetelne (pacjent został wprowadzony w błąd).

Ograniczenie celu

Wykorzystanie danych osobowych zawsze musi mieć swój cel. Przykładowo placówka medyczna zbiera dane pacjentów po to, by:

- udzielać świadczeń zdrowotnych
- prowadzić dokumentację medyczną
- realizować obowiązki wobec NFZ.

Wykorzystanie adresów zamieszkania pacjentów, np. do wysłania im reklam zaprzyjaźnionego z placówką medyczną biura rachunkowego byłoby **poważnym naruszeniem zasady ograniczenia celu (i wielu innych przepisów prawnych).**

Dokumenty, zawierające informacje o osobach przebywających w [holenderskim] szpitalu (imiona, nazwiska, daty urodzenia, dolegliwości oraz historie choroby i przyjmowanych leków) były wykorzystywane przez pracowników jako… listy zakupów. Pracownicy używali dokumentacji medycznej jako miejsca do zapisywania prywatnych notatek i wynosili to poza teren ośrodka. Zdarzenie wyszło na jaw, gdy jeden z klientów supermarketu znalazł pozostawione „listy" w wózku na zakupy. Było to kilka stron A4 dokumentacji osób, które korzystały ze świadczenia usług zdrowotnych wyżej wspomnianego szpitala.

- Naruszenie RODO w szpitalu. Użyli dokumentacji medycznej jako list zakupowych[1].

Minimalizacja danych

Placówka medyczna powinna używać tylu kategorii danych osobowych, ile jest niezbędne do wykonania konkretnego zadania – ale nie więcej. Nie można zbierać informacji „na zaś", „na wszelki wypadek", „bo mogą się kiedyś przydać".

Zgodnie z przepisami w dokumentacji dorosłego pacjenta mają się znaleźć następujące dane osobowe na jego temat: imię, nazwisko, data urodzenia, płeć, adres miejsca zamieszkania, numer PESEL.

Dodatkowe zbieranie np. informacji o numerze buta lub o poglądach politycznych pacjenta będzie naruszeniem zasady minimalizacji danych.

[1] *Naruszenie RODO w szpitalu. Użyli dokumentacji medycznej jako list zakupowych*, https://www.politykazdrowotna.com/49336,naruszenie-rodo-w-szpitalu-uzyli-dokumentacji-medycznej-jako-list-zakupowych (dostęp 28.11.2019 r.).

Prawidłowość

Zasada prawidłowości oznacza, że dane używane przez administratora muszą być prawidłowe, a w razie potrzeby – uaktualniane.

W przypadku gdy pracownica wychodzi za mąż i zmienia nazwisko, konieczne jest uwzględnienie tego faktu w dokumentacji kadrowej, prowadzonej przez administratora danych.

Ograniczenie przechowywania

Danych osobowych nie można trzymać w nieskończoność. Są one zbierane w konkretnym celu. Gdy cel jest zrealizowany, dane powinny być usunięte.

Podmiot udzielający świadczeń zdrowotnych przechowuje dokumentację medyczną przez okres 20 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu, z wyjątkiem:

1) dokumentacji medycznej w przypadku zgonu pacjenta na skutek uszkodzenia ciała lub zatrucia, która jest przechowywana przez okres 30 lat, licząc od końca roku kalendarzowego, w którym nastąpił zgon;

1a) dokumentacji medycznej zawierającej dane niezbędne do monitorowania losów krwi i jej składników, która jest przechowywana przez okres 30 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu;

2) zdjęć rentgenowskich przechowywanych poza dokumentacją medyczną pacjenta, które są przechowywane przez okres 10 lat, licząc od końca roku kalendarzowego, w którym wykonano zdjęcie;

3) skierowań na badania lub zleceń lekarza, które są przechowywane przez okres:

a) 5 lat, licząc od końca roku kalendarzowego, w którym udzielono świadczenia zdrowotnego będącego przedmiotem skierowania lub zlecenia lekarza,

b) 2 lat, licząc od końca roku kalendarzowego, w którym wystawiono skierowanie - w przypadku gdy świadczenie zdrowotne nie zostało udzielone z powodu niezgłoszenia się pacjenta w ustalonym terminie, chyba że pacjent odebrał skierowanie;

4) dokumentacji medycznej dotyczącej dzieci do ukończenia 2. roku życia, która jest przechowywana przez okres 22 lat.

2. Po upływie okresów wymienionych w ust. 1 podmiot udzielający świadczeń zdrowotnych niszczy dokumentację medyczną w sposób uniemożliwiający identyfikację pacjenta, którego dotyczyła. Dokumentacja medyczna przeznaczona do zniszczenia może być wydana pacjentowi, jego przedstawicielowi ustawowemu lub osobie upoważnionej przez pacjenta.

- art. 29 ust. 1-2 ustawy o prawach pacjenta[2]

Integralność i poufność

Dane osobowe muszą być (...) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

- art. 5 ust. 1 lit. f RODO

To jedna z ważniejszych w RODO zasad i przyczyna licznych nieporozumień, związanych z tym aktem prawnym. Tak jak wspominaliśmy na wstępie, postęp technologiczny, zmiany prawa i inne okoliczności sprawiają, że w przepisach o ochronie danych osobowych nie może być konkretnych zaleceń, bo szybko tracą na aktualności.

Druga istotna kwestia to konieczność dostosowania ochrony danych do branży administratora i jego możliwości. Inaczej będzie wdrażać RODO salon fryzjerski, inaczej praktyka lekarza rodzinnego, a jeszcze inaczej uczelnia wyższa.

Wdrażanie RODO ułatwia stosowanie **kodeksu postępowania**. Taki kodeks doprecyzowuje zawiłe przepisy, uwzględnia specyfikę sektora, dla którego jest przygotowywany i daje konkretniejsze odpowiedzi na pytania związane z ochroną danych osobowych. W sektorze medycznym toczą się obecnie prace nad dwoma kodeksami:

- dla małych placówek medycznych, należących do Federacji Porozumienie Zielonogórskie (firmowany przez FPZ)
- dla placówek medycznych (firmowany przez Polską Federację Szpitali).

Obecnie (listopad 2019 r.) żaden z dwóch projektów kodeksu nie został jeszcze zatwierdzony przez Prezesa Urzędu Ochrony Danych Osobowych.

Postępy prac nad kodeksem dla małych placówek medycznych, należących do Federacji Porozumienie Zielonogórskie, można śledzić na stronie internetowej:

kodeksfpz.jamano.pl

[2] Ustawa z dnia 06.11.2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2019 r. poz. 1127 ze zm.).

Rozliczalność

Administrator danych musi nie tylko przestrzegać zasad wskazanych powyżej, ale też być w stanie wykazać ich przestrzeganie. Oznacza to, że w ramach dbania o zgodność działań placówki medycznej z RODO konieczne jest prowadzenie określonej dokumentacji (instrukcji, procedur, wytycznych itp.).

Podstawy dla wykorzystania danych

Za każdym razem, gdy placówka medyczna wykorzystuje czyjeś dane osobowe, musi mieć ku temu podstawę prawną.

W przypadku danych zwykłych (takich jak imiona, nazwiska, adresy czy PESEL-e) RODO wskazuje następujące podstawy prawne:

> *a) **osoba, której dane dotyczą wyraziła zgodę** na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;*
> *b) przetwarzanie jest niezbędne do wykonania **umowy, której stroną jest osoba, której dane dotyczą**, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;*
> *c) przetwarzanie jest niezbędne do wypełnienia **obowiązku prawnego** ciążącego na administratorze;*
> *d) przetwarzanie jest niezbędne do ochrony **żywotnych interesów osoby, której dane dotyczą** lub innej osoby fizycznej;*
> *e) przetwarzanie jest niezbędne do wykonania **zadania realizowanego w interesie publicznym** lub w ramach sprawowania władzy publicznej powierzonej administratorowi;*
> *f) przetwarzanie jest niezbędne do celów wynikających z **prawnie uzasadnionych interesów realizowanych przez administratora** lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.*
>
> - art. 6 ust. 1 RODO

Z kolei przetwarzanie szczególnych kategorii danych (danych osobowych wrażliwych) obwarowane jest dodatkowymi zastrzeżeniami. Np. wykorzystanie danych o stanie zdrowia powinno mieć miejsce wtedy, gdy jest „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" (art. 9 ust. 2 lit. h RODO).

Wskazanie właściwej podstawy prawnej dla wykorzystania danych osobowych wymaga zaangażowania inspektora ochrony danych. Wykorzystanie niewłaściwej przesłanki może oznaczać naruszenie zasady zgodności z prawem, rzetelności i przejrzystości. Szczególnie dotyczy to przypadków, gdy niepotrzebnie żąda się podpisania zgody na wyc korzystanie danych osobowych.

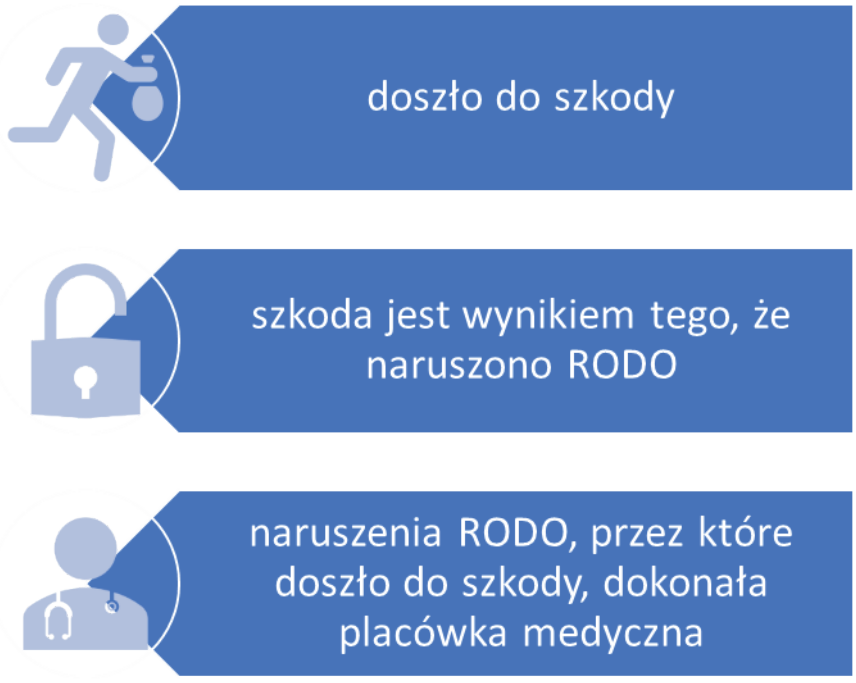
Odpowiedzialność administratora za zgodność z przepisami o ochronie danych osobowych

Jeżeli administrator danych nie przestrzega zasad wykorzystania danych osobowych, naraża się na odpowiedzialność za swoje zachowanie. Wiele podmiotów zwraca uwagę głównie na odpowiedzialność wobec organów państwowych, np. Prezesa Urzędu Ochrony Danych Osobowych lub Rzecznika Praw Pacjenta.

RODO podkreśla także wagę dbałości o odpowiedzialność wobec konkretnych osób: przedstawicieli kontrahentów, pracowników lub pacjentów. Nieprzestrzeganie ogólnego rozporządzenia o ochronie danych przez placówkę medyczną może doprowadzić do powstania szkody.

> *Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.*
>
> - art. 82 ust. 1 RODO

Oczywiście nie każda szkoda związana z naruszeniem ochrony danych osobowych automatycznie prowadzi do przyznania „odszkodowania za RODO". Aby tak się stało muszą być spełnione jednocześnie trzy warunki:



Szkoda

Przepisy RODO mówią o szkodzie majątkowej lub niemajątkowej. **Szkoda majątkowa** występuje wtedy, kiedy konkretna osoba straciła pieniądze lub część swojego majątku. Przykładem szkody majątkowej mogą być koszty kredytu zaciągniętego na pracownika (w sytuacji, gdy wyciek danych dotknął akta pracownicze, gdzie niezgodnie z przepisami przechowywano kserokopie dowodu osobistego pracownika).

Szkoda niemajątkowa jest wtedy, kiedy doszło do psychicznego cierpienia lub krzywdy moralnej. Przykładem szkody niemajątkowej może być rozpad małżeństwa pacjenta (w sytuacji, gdy pacjent cierpiał na chorobę weneryczną,

a pracownik placówki medycznej poinformował o tym żonę pacjenta, mimo tego że nie była upoważniona do sięgania po jego dane medyczne).

Szkoda jako wynik naruszenia RODO

Aby wystąpiła odpowiedzialność cywilna z art. 82 RODO, szkoda musi być wynikiem naruszenia przepisów RODO.

Szkoda, która jest wynikiem naruszenia RODO, to na przykład koszty kredytu zaciągniętego na pracownika (w sytuacji, gdy wyciek danych dotknął akta pracownicze, gdzie niezgodnie z przepisami przechowywano kserokopie dowodu osobistego pracownika).

Szkoda, która nie jest wynikiem naruszenia RODO, to na przykład opublikowanie skanu dokumentacji pacjenta na Facebooku (w sytuacji, gdy placówka medyczna wydała dokumentację pacjentowi zgodnie z przepisami, ten ją zgubił, a przypadkowy znalazca opublikował ją na Facebooku).

Placówka medyczna jako sprawca naruszenia

Aby wystąpiła odpowiedzialność cywilna z art. 82 RODO, szkoda musi być wynikiem naruszenia przepisów RODO przez placówkę medyczną. Jeżeli podmiot leczniczy nie dopuścił się takiego naruszenia, istotny warunek szkody nie zaistnieje i odszkodowanie od placówki wówczas się nie należy.

Koordynowanie procesów przetwarzania danych w organizacji

Zdjęcie: Jake Hills, Unsplash (https://unsplash.com/photos/bt-Sc22W-BE).

Właściwa koordynacja procesów przetwarzania danych osobowych w organizacji obejmuje:

1. Audyt ochrony danych osobowych
2. Analizę ryzyka
3. Ustalenie zaleceń związanych z ryzykami
4. Wykonanie zaleceń
5. Powtórzenie pkt. 1-4.

Audyt ochrony danych osobowych

W ramach audytu należy ustalić w szczególności:

- jakie mamy kategorie danych osobowych (imiona, nazwiska, adresy, telefony, e-maile, dane o stanie zdrowia…)
- czyje dane osobowe posiadamy (kandydatów do pracy, pracowników, pacjentów, przedstawicieli kontrahentów…)
- skąd mamy dane osobowe (bezpośrednio od osób, których dane dotyczą, z innych placówek medycznych…)
- do jakich celów używamy danych osobowych (udzielanie świadczeń zdrowotnych, prowadzenie dokumentacji kadrowej…)
- na jakiej podstawie wykorzystujemy dane (przepis prawa, umowa, zgoda…)
- kto oprócz nas wykorzystuje te dane osobowe (inne placówki medyczne, laboratoria, firmy księgowe, przedsiębiorstwa IT…).

W ten sposób ustalamy stan faktyczny – wiemy, jak jest. Potem sprawdzamy, czy stan faktyczny jest zgodny z przepisami o ochronie danych osobowych i zasadami bezpieczeństwa, tj. w szczególności:

- czy jakichś danych nie zbiera się niepotrzebnie
- czy jakich danych nie wykorzystuje się zbyt długo
- czy dane są zbierane zgodnie z przepisami prawa
- czy dane są używane we właściwych celach
- czy w związku z wykorzystaniem danych prowadzona jest odpowiednia dokumentacja
- czy przy przekazywaniu danych na zewnątrz podpisane są odpowiednie umowy związane z ochroną danych osobowych.

Jeżeli wychodzą nam tutaj odstępstwa, oznacza to, że występuje ryzyko. Trzeba je przeanalizować.

Analiza ryzyka

W analizie ryzyka związanego z ochroną danych osobowych chodzi o ustalenie:

- co może pójść nie tak (**skutek**)
- **jak bardzo prawdopodobne jest, że coś pójdzie nie tak (prawdopodobieństwo).**

Po wymnożeniu skutku przez prawdopodobieństwo otrzymujemy **ryzyko. Dla potrzeb audytu najlepiej przyjąć następujące poziomy skutku, prawdopodobieństwa i ryzyka:**

- bardzo niskie
- niskie
- średnie
- wysokie.

Zależność między poszczególnymi poziomami ryzyka przedstawia poniższa tabela.

Prawdopodobieństwo / Skutek	Bardzo niskie (1)	Niskie (2)	Średnie (3)	Wysokie (4)
Niski (1)	1	3	3	4
Średni (2)	2	4	6	8
Wysoki (3)	3	6	9	12
Bardzo wysoki (4)	4	8	12	16

Skutek x prawdopodobieństwo	**Ryzyko**
1-3	bardzo niskie
4-7	niskie
8-11	średnie
12-16	wysokie

Poniżej przykład oceny ryzyka dla konkretnego stanu faktycznego.

Dokumentacja medyczna jest (z braku miejsca) przechowywana w niezamykanych szafach, stojących na publicznie dostępnym korytarzu.

Prawdopodobieństwo, że ktoś nieupoważniony zabierze tę dokumentację, jest co najmniej średnie. Skutek wyniesienia dokumentacji przez osobę nieupoważnioną jest bardzo wysoki. Zatem ryzyko utraty kontroli nad dokumentacją z szafy na korytarzu jest **bardzo wysokie i wymaga natychmiastowej reakcji ze strony placówki medycznej**.

Ustalenie zaleceń związanych z ryzykami

Gdy ustalimy ryzyko, należy podjąć decyzję, czy wymaga ono działania i czy ma to być działanie pilne. Im „cięższy" skutek i większe prawdopodobieństwo, tym pilniejsze musi być działanie placówki medycznej. Zalecenia muszą brać pod uwagę możliwości techniczne, logistyczne i finansowe administratora.

Przykład:

Ryzyku utraty kontroli nad dokumentacją z niezamkniętej szafy na publicznie dostępnym korytarzu można zapobiec np. poprzez:

- zastąpienie szaf niezamykanych zamykanymi
- przeniesienie dokumentacji do innego, lepiej zabezpieczonego pomieszczenia
- fizyczne oddzielenie szafy od pozostałej części placówki medycznej (np. przez zamontowanie folii antywłamaniowej).

Wykonanie zaleceń

Powyższe kroki związane z audytem najczęściej są wykonywane w ścisłej współpracy z inspektorem ochrony danych. Należy jednak pamiętać o tym, że ostateczną decyzję w sprawie konkretnych działań podejmuje administrator, tj. najwyższe kierownictwo placówki medycznej.

To kierownik lub dyrektor decyduje, czy należy wprowadzić nową procedurę, kupić szafy zamykane na klucz lub przeszkolić pracowników, i to on będzie – w razie ewentualnej kontroli – rozliczany z tej decyzji. Inspektor ochrony danych czy audytor ma tutaj jedynie rolę doradczą: wskazuje zagrożenia, sposoby ich naprawy i konsekwencje sytuacji, gdy zagrożenia nie zostaną zaadresowane.

Powtórzenie pkt. 1-4

Ten punkt jest bardzo istotny, ponieważ wiele podmiotów medycznych o nim zapomina uważając, że skoro X lat temu (lub 24 maja 2018 r.) miały audyt, wydrukowały dokumenty i przeszkoliły pracowników, to są gotowe na RODO i nie muszą robić nic więcej.

– Z RODO jest trochę jak z kotem – głaskanie to proces, a nie jednorazowa czynność – mówi żartobliwie dr Łukasz Olejnik, badacz i konsultant cyberbezpieczeństwa i prywatności. – Trzeba pamiętać, że prywatność nie jest produktem, a procesem, który nie ma końca. Nie jest tak, że kupi się oprogramowanie wdrażające RODO, firewalle, antywirusy, zamówi audyt i szkolenia – i to rozwiąże problem. Kluczowa jest ciągłość. Trzeba nieustannie analizować zmiany planów i celów organizacyjnych w firmie, ale także otoczenie – zmiany technologiczne, nowe zagrożenia oraz wpływ jednego na drugie, i płynnie odpowiadać na te wyzwania – wylicza ekspert.

- Małe firmy nie są gotowe na RODO. O czym powinni pamiętać przedsiębiorcy przed 25 maja?[3]

Zdjęcie: Yerlin Matu, Unsplash (https://unsplash.com/photos/GtwiBmtJvaU)

[3] S. Wikariak, *Małe firmy nie są gotowe na RODO. O czym powinni pamiętać przedsiębiorcy przed 25 maja?* https://prawo.gazetaprawna.pl/artykuly/1125264,rodo-w-malych-firmach-co-trzeba-wiedziec.html, (dostęp 28.11.2019 r.).

Przepisy prawa nie stawiają tu żadnych konkretnych wymagań. Jednak rozsądnie jest przeprowadzać audyt (i związane z nim działania) co roku.

Upoważnienia do przetwarzania danych osobowych

Przez 20 lat, aż do wejścia w życie w Polsce RODO, administratorzy danych mieli obowiązek prawny nadawania upoważnień do przetwarzania danych osobowych. Po 25 maja 2018 r. wiele podmiotów utrzymało tę praktykę – mimo że nie wynika ona wprost ani z RODO, ani z polskiej ustawy o ochronie danych osobowych.

Placówka medyczna, która chce nadawać upoważnienia do przetwarzania danych osobowych, musi pamiętać o kilku zasadach.

Komu nadawać upoważnienie, a komu nie?

Upoważnienie powinna mieć każda osoba, która pracuje w placówce medycznej i ma dostęp do danych osobowych – niezależnie od tego, jakie ma stanowisko, jak długo pracuje albo na jakiej podstawie jest zatrudniona.

Upoważnienie do przetwarzania danych osobowych powinni otrzymać zatrudnieni w placówce medycznej: lekarze, pielęgniarki, fizjoterapeuci, pracownicy rejestracji.

Upoważnienia nie potrzebują osoby, które w ramach obowiązków służbowych nie muszą sięgać do danych osobowych. Takie osoby powinny jednak podpisać oświadczenie o zachowaniu poufności.

Upoważnienia do przetwarzania danych osobowych nie powinna otrzymać osoba z personelu sprzątającego, ponieważ do wykonywania jej obowiązków nie jest jej potrzebny dostęp do dokumentów lub baz danych zawierających dane osobowe.

Upoważnienia nie należy także nadawać osobie, która ma dostęp do danych osobowych na podstawie zawartej umowy powierzenia.

Przykład:
Pani Kowalska prowadzi biuro rachunkowe. Placówka medyczna zawarła umowę z biurem rachunkowym na usługi księgowe oraz – zgodnie z przepisami RODO – umowę powierzenia. Pani Kowalska może zatem uzyskiwać dostęp do danych osobowych pracowników, kontrahentów, itp. w związku z realizacją umowy. Nie potrzebuje już dodatkowego upoważnienia do przetwarzania danych osobowych.

Upoważnienia specjalne

W razie ewentualnej kontroli upoważnienia nadane każdemu, kto ma dostęp do danych osobowych pacjentów, pracowników itp. osób w celach służbowych ułatwią udowodnienie, że administrator danych dba o to, kto ma do czego dostęp. Istnieją jednak także przypadki, gdy nadanie upoważnienia jest obowiązkiem, wynikającym z przepisów prawa.

Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO[4] w kilku przypadkach wskazała, że konieczne jest nadawanie upoważnień do przetwarzania danych osobowych, m.in. gdy dotyczą:

- szczególnych kategorii danych, gromadzonych przez pracodawcę na podstawie zgody pracownika (takie upoważnienie musi otrzymać pracownik odpowiedzialny za sprawy kadrowe)
- danych o zdrowiu, przekazywanych przez osoby korzystające z zakładowego funduszu świadczeń socjalnych (takie upoważnienie musi otrzymać członek komisji socjalnej).

Z punktu widzenia przepisów o ochronie danych osobowych nie ma przeszkód, aby do każdego z tych celów było nadane oddzielne upoważnienie. Poprawne będzie także nadanie jednego, zbiorczego upoważnienia.

Kto ma nadawać, odbierać, podpisywać oświadczenia?

Działania związane z upoważnieniami powinny być wykonywane przez osobę reprezentującą administratora danych (w przypadku placówki medycznej jest to najczęściej jej kierownik). Jeżeli kierownik chce, aby inna osoba zamiast niego (np. kadrowa, księgowy) nadawała i odbierała upoważnienia, musi wystawić takiej osobie pełnomocnictwo do nadawania upoważnień.

Co ma zawierać upoważnienie? Wzór upoważnienia

Upoważnienie do przetwarzania danych osobowych powinno zawierać te elementy:

- określenie administratora danych
- imię, nazwisko i stanowisko osoby, która jest upoważniona
- wskazanie zakresu upoważnienia
- okres, na jaki jest nadawane upoważnienie.

Dodatkowo do upoważnienia można dodać:

- odwołanie do dokumentacji ochrony danych osobowych
- zobowiązanie do zachowania poufności lub upoważnienia specjalne.

Poniżej znajduje się przykładowy wzór upoważnienia do przetwarzania danych osobowych:

---

[4] Ustawa z dnia 21.02.2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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. z 2019 r. poz. 730).

Upoważnienie do przetwarzania danych osobowych

JAMANOWSKI PRAKTYKA LEKARZA RODZINNEGO (ul. Piekarska 221B, 57-540 Lądek-Zdrój) (**Administrator**) niniejszym upoważnia:

Imię	Paweł
Nazwisko	Klimkowski
Stanowisko	lekarz

do przetwarzania danych osobowych w zakresie zbierania, utrwalania, przechowywania, opracowywania, zmieniania, udostępniania, archiwizowania oraz usuwania danych osobowych w związku z zajmowanym stanowiskiem.

Niniejsze upoważnienie obejmuje także (proszę zaznaczyć odpowiednie pola):

☐ szczególne kategorie danych, gromadzonych przez pracodawcę na podstawie zgody pracownika (art. 22[1b] Kodeksu pracy)

☐ dane o zdrowiu, przekazywane przez osoby korzystające z zakładowego funduszu świadczeń socjalnych (art. 8 ust. 1b ustawy z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych).

Upoważnienie zostaje udzielone na okres od dnia __.__.20__ r. do odwołania lub zakończenia świadczenia pracy bądź usług na rzecz Administratora.

_____ (data i podpis Administratora)

Niniejszym potwierdzam zapoznanie się z treścią obowiązującej u Administratora dokumentacji ochrony danych osobowych i zobowiązuję się jej przestrzegać. Zobowiązuję się także zachować w tajemnicy wszelkie informacje, w tym dane osobowe, do których będę mieć dostęp, jak również sposoby ich zabezpieczenia, także po wygaśnięciu tego upoważnienia.

Przyjmuję do wiadomości, że udostępnienie danych osobowych lub umożliwienie dostępu do tych danych osobom nieupoważnionym może podlegać odpowiedzialności, szczególnie odpowiedzialności karnej, zgodnie z powszechnie obowiązującymi przepisami.

_____ (data i podpis osoby upoważnionej)

Zobowiązanie osób zatrudnionych do zachowania informacji w tajemnicy

Każda osoba zatrudniona powinna podpisać oświadczenie o zachowaniu danych w poufności. Dotyczy to zarówno tych osób, które mają dostęp do danych w celach służbowych (np. lekarze lub pielęgniarki), jak i innych osób (np. personel sprzątający).

Oświadczenie może być oddzielnym drukiem. Oświadczenie można także połączyć z upoważnieniem do przetwarzania danych osobowych (tak jak we wzorze powyżej).

Poniżej znajduje się przykładowy wzór oświadczenia o poufności:

Oświadczenie o poufności

W związku z wykonywaniem zadań na rzecz JAMANOWSKI PRAKTYKA LEKARZA RODZINNEGO (**Administratora**) i pracą w pomieszczeniach, gdzie wykorzystywane są dane osobowe, którymi zarządza Administratora, ja, niżej podpisana/podpisany, (*proszę podać imię i nazwisko*):

_____ oświadczam, co następuje:

- mam świadomość, że nie mam prawa przetwarzania danych osobowych administrowanych przez Administratora, zwłaszcza prawa wglądu do dokumentów papierowych lub systemów IT Administratora
- nie będę dokonywać przetwarzania danych osobowych
- będę niezwłocznie informować Administratora o stwierdzonych naruszeniach bezpieczeństwa danych
- w razie wejścia w posiadanie danych osobowych lub sposobów ich zabezpieczeń (np. w związku z incydentem bezpieczeństwa) zachowam je w tajemnicy – zarówno w toku współpracy z Administratorem, jak i po jej zakończeniu.

Oświadczam także, że znane mi są przepisy prawa dotyczące ochrony danych osobowych oraz mam świadomość odpowiedzialności prawnej (w tym karnej) związanej z naruszeniem tych przepisów.
Przyjmuję ponadto do wiadomości, że naruszenie tych przepisów może stanowić ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę lub natychmiastowego rozwiązania umowy będącej podstawą zatrudnienia.

_____ (data i podpis osoby upoważnionej)

Rozdział II. Inspektor Ochrony Danych – doradca w zakresie ochrony danych osobowych

Ogólne rozporządzenie o ochronie danych (RODO) przewiduje możliwość wyznaczenia przez placówkę medyczną fachowego doradcy, który wspierałby ją we wszystkich działaniach związanych z przetwarzaniem danych osobowych. RODO nazywa go inspektorem ochrony danych (IOD).

Motyw 97 preambuły RODO

(...) w monitorowaniu wewnętrznego przestrzegania niniejszego rozporządzenia administrator lub podmiot przetwarzający powinni być wspomagani przez osobę dysponującą wiedzą fachową na temat prawa i praktyk w dziedzinie ochrony danych (...)

Idea funkcjonowania w organizacjach ekspertów wspierających administratora danych w zarządzaniu procesami przetwarzania danych osobowych nie jest pomysłem nowym. Już w 1995 r., na mocy Dyrektywy 95/46/WE (RODO zastąpiło właśnie tę dyrektywę), możliwe było wyznaczenie tzw. urzędnika ds. ochrony danych (data protection official, DPO). Dyrektywa nie opisywała jednak szczegółowo zadań takiego DPO, wiązała jedynie tę instytucję z możliwością wprowadzenia zwolnień z obowiązku zgłaszania do organów nadzorczych operacji przetwarzania danych osobowych – czego przykładem była rejestracja zbiorów danych osobowych w Polsce.

Na przestrzeni ponad 20 lat obowiązywania dyrektywy, wiele państw Unii Europejskiej przewidziało obowiązek lub możliwość powołania takiego inspektora ochrony danych. Podobnie było również w Polsce. Od 1 maja 2004 r., zgodnie z obowiązującą przed RODO ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, placówki medyczne mogły wyznaczać administratora bezpieczeństwa informacji (ABI).

Na przestrzeni ostatnich kilkunastu lat powołanie ABI było źródłem wielu korzyści dla administratorów danych. Przede wszystkim, ABI prowadził lokalnie rejestr zbiorów danych przetwarzanych przez administratora danych osobowych. ABI był również uprawniony do sprawdzenia zgodności przetwarzania danych, czyli przeprowadzenia swojego rodzaju „wewnętrznego audytu", którego wyniki były przekazywane organowi nadzorczemu, dzięki czemu administrator w wielu przypadkach unikał kontroli. Wreszcie, ABI nadzorował opracowanie i aktualizowanie dokumentacji przetwarzania danych osobowych, a także uczestniczył w procesach szkoleniowych dla pracowników administratora.

Zadania ABI bardzo przypominały te, które RODO stawia przed IOD. Podobnie jak obecnie IOD, ABI był doradcą, który miał za zadanie wspierać administratora danych osobowych w zapewnianiu zgodności przetwarzania danych z przepisami o ochronie danych osobowych. W starej ustawie o ochronie danych osobowych z 1997 r. bardzo podobnie uregulowano także kwestie niezależności ABI, czy też wymogów w zakresie posiadania odpowiedniej wiedzy i umiejętności. Zasadniczą różnicą pomiędzy obecnym stanem prawnym, a systemem wprowadzonym starą ustawą o ochronie danych osobowych, było to, że powołanie ABI było jedynie możliwością, natomiast wyznaczenie IOD jest w określonych sytuacjach obowiązkowe, o czym w dalszej części niniejszego rozdziału.

Jak podobne są te funkcje najlepiej świadczy fakt, że w przepisach przejściowych do nowej ustawy o ochronie danych osobowych z 2018 r. przewidziano, że dotychczas powołani ABI stają się z mocy prawa IOD, o ile administrator przekazał do organu nadzorczego dane kontaktowe takiej osoby w wyznaczonych przez przepisy terminach. Dzięki temu wielu ABI pełniących swoją rolę w placówkach medycznych stało się IOD z mocy prawa – bez konieczności wyznaczania takiej osoby raz jeszcze na funkcję IOD.

IOD pełni jedną z głównych ról w zarządzaniu procesami przetwarzania danych osobowych w każdej organizacji – także w placówce medycznej. To on, obok administratora danych, osoby odpowiedzialnej za bezpieczeństwo teleinformatyczne (np. ASI) oraz osób upoważnionych do przetwarzania danych osobowych, ma kluczowy wpływ na zgodne z prawem i bezpieczne wykorzystanie danych osobowych.

ADO

administrator danych osobowych

Decyduje o celach i środkach przetwarzania danych osobowych.

IOD

inspektor ochrony danych

Osoba fizyczna, wspierająca ADO w realizacji obowiązków dotyczących ochrony danych osobowych: prowadzenia dokumentacji, okresowych audytów, szkoleń dla osób wykorzystujących dane osobowe, zgłaszania naruszeń itp..

ASI

administrator systemów informatycznych

Informatyk (lub firma informatyczna), odpowiadająca za zabezpieczenie programów komputerowych, komputerów, sieci, serwerów itp. przed zagrożeniami IT.

osoby upoważnione

Osoby mające **dostęp do danych osobowych w celach służbowych**, niezależnie od zajmowanego stanowiska, stażu pracy lub umowy będącej podstawą zatrudnienia.

Wyznaczanie Inspektora Ochrony Danych

Zgodnie z RODO, wyznaczenie IOD jest obowiązkowe w kilku przypadkach. Jak czytamy w art. 37 RODO, administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:

- przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości
- główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę

lub

- główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10.

Pierwsza w wymienionych powyżej sytuacji nie budzi większych wątpliwości – wszystkie podmioty sektora publicznego mają obowiązek wyznaczenia IOD. Co to są za podmioty? Zgodnie z art. 9 nowej ustawy o ochronie danych osobowych z 2018 r., przez organy i podmioty publiczne rozumie się:

- jednostki sektora finansów publicznych
- instytuty badawcze
- Narodowy Bank Polski.

Do jednostek sektora finansów publicznych zaliczają się Samodzielne Publiczne Zakłady Opieki Zdrowotnej.

Zatem na wszystkich publicznych podmiotach leczniczych spoczywa obowiązek wyznaczenia IOD. Polski organ nadzorczy (Prezes Urzędu Ochrony Danych Osobowych, PUODO) zachęca jednak, żeby IOD powoływały również prywatne jednostki, realizujące zadania w interesie publicznym. PUODO zachęca tym samym, aby inspektora wyznaczyły wszystkie prywatne placówki medyczne udzielające świadczeń opieki zdrowotnej, które są finansowane ze środków publicznych przez Narodowy Fundusz Zdrowia.

Mogłoby się zatem wydawać, że prywatne podmioty lecznicze nie są zobowiązane wyznaczać IOD. Zaprzecza temu kolejna przesłanka wspomnianego art. 37 RODO. Zgodnie z tym przepisem IOD musi bowiem posiadać administrator, którego główną działalnością jest przetwarzanie na dużą skalę szczególnych kategorii danych osobowych (zalicza się do nich przede wszystkim dane o stanie zdrowia). RODO nie przynosi niestety definicji „głównej działalności" ani też „dużej skali". Jak to zatem rozumieć?

Jak czytamy w Wytycznych WP 243 Grupy Roboczej Art. 29[5] dotyczących inspektorów ochrony danych, główna działalność oznacza zasadnicze, nie poboczne działanie.

Dla przykładu działalnością główną szpitali będzie zapewnianie opieki medycznej. Natomiast prowadzenie efektywnej opieki medycznej nie byłoby możliwe bez przetwarzania danych medycznych, jak np. historii choroby pacjenta. W związku z tym działalność polegająca na przetwarzaniu historii choroby pacjenta również powinna zostać zaklasyfikowana jako działalność główna.

Przetwarzanie danych osobowych przez placówkę medyczną jest nierozerwalnie związane z realizowaniem świadczeń opieki zdrowotnej, dlatego też należy je uznać za główną działalność placówki medycznej w rozumieniu RODO.

Pojęcie dużej skali jest jeszcze bardziej nieostre. Pomocne w jej zdefiniowaniu znowu są wspomniane Wytyczne WP 243, zgodnie z którymi zaleca się uwzględnienie następujących czynników podczas określania czy placówka medyczna przetwarza dane osobowe na dużą skalę:

- liczba osób, których dane dotyczą – konkretna liczba osób albo procent określonej grupy społeczeństwa, np. kiedy dana placówka medyczna przetwarza dane osobowe niemal wszystkich mieszkańców małej gminy
- zakres przetwarzanych danych osobowych – ten w przypadku placówek medycznych będzie zawsze szeroki i będzie uwzględniał dane wrażliwe

[5] Niezależny organ doradczy Komisji Europejskiej w zakresie ochrony danych osobowych i prywatności, obecnie Europejska Rada Ochrony Danych.

- okres, przez który dane są przetwarzane – istotną kwestią będzie zgodny z przepisami, maksymalny czas przechowywania dokumentacji medycznej, tj. 30 lat
- zakres geograficzny przetwarzania danych osobowych.

Mając to wszystko na uwadze, wydaje się, że małe placówki medyczne powinny wyznaczyć inspektora ochrony danych osobowych. Nie będzie to jednak dotyczyć sytuacji, kiedy przetwarzanie danych pacjentów – klientów, dokonywane będzie przez pojedynczego lekarza.

W trakcie prac nad **Kodeksem postępowania dotyczącym ochrony danych osobowych przetwarzanych w małych placówkach medycznych**, przekazanym do PUODO przez Federację PZ jeszcze we wrześniu 2018 r. (jako pierwszy kodeks w Polsce) próbowano określić liczbowo pojęcie dużej skali dla placówek medycznych.
Przyjęto, że IOD powinna wyznaczyć placówką medyczna, która ma przypisanych 6000 unikalnych pacjentów, którym udziela świadczeń POZ lub 600 unikalnych pacjentów, którym w miesiącu udziela świadczeń w ramach AOS.
W momencie publikacji niniejszego tekstu powyższe stanowisko nie zyskało jednak akceptacji PUODO.

W takich sytuacjach decyzję o wyznaczeniu IOD musi podjąć placówka medyczna. W imię zasady rozliczalności wyrażonej w RODO, zalecane jest również, aby udokumentować decyzję w zakresie wyznaczenia IOD. W praktyce można np. sporządzić notatkę ze spotkania kierownictwa placówki medycznej, zawierającą argumenty z dyskusji dotyczącej wyznaczenia IOD lub też przygotować analizę w zakresie obowiązku wyznaczenia IOD przez daną placówkę medyczną.

Wyznaczenie IOD powinno odbyć się na mocy uchwały, zarządzenia lub decyzji kierownictwa placówki medycznej, która w formalny sposób wskazuje konkretną osobę, którą wyznacza się do pełnienia funkcji IOD oraz datę wyznaczenia.

……., dnia …….. 2018 r.

Uchwała Zarządu Spółki

……, ……,
KRS …… NIP ……, REGON …… (zwana dalej „Spółką")

1. Na podstawie art. 37 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, zwanego dalej „RODO") wyznacza się Pana/Panią ……, data urodzenia: …… na Inspektora Ochrony Danych (zwany dalej „IOD").
2. IOD podlega bezpośrednio Prezesowi Zarządu Spółki.
3. Uchwała wchodzi w życie w dniu podjęcia.

…… …… ……

Jeden IOD dla kilku placówek medycznych

RODO dopuszcza wyznaczenie IOD dla grupy przedsiębiorstw. Zgodnie z art. 4 pkt 19 RODO grupa przedsiębiorstw oznacza przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane. Załóżmy więc, że mamy do analizy sytuację przedsiębiorcy prowadzącego różne działalności, np. właściciela, który tworzy w ramach grupy powiązanej ze sobą osobowo czy kapitałowo sieć klinik, aptekę i firmę zajmującą się badaniami klinicznymi. Tak rozumiana grupa może wyznaczyć dla wszystkich tych podmiotów jednego IOD. Nic jednak nie stoi na przeszkodzie, by IOD wyznaczyła również grupa przedsiębiorców ze sobą niepowiązanych kapitałowo – przepisy RODO nie zawierają takiego zakazu.

Ile podmiotów może obsługiwać taki pojedynczy IOD? Ani przepisy RODO, ani ich interpretacje wydawane przez PUODO, nie dają odpowiedzi na takie pytanie. Takie rozwiązanie będzie mogło być stosowane w racjonalnych granicach, przy uwzględnieniu przede wszystkim łatwej dostępności takiego IOD dla każdej obsługiwanej placówki medycznej.

Należy jednak pamiętać, że w sytuacji wyznaczania jednego IOD dla kilku podmiotów, każdy z tych podmiotów powinien samodzielnie podjąć uchwałę, zarządzenie lub decyzję wyznaczającą IOD oraz zgłosić ten fakt do PUODO.

Więcej na temat zawiadamiania PUODO o wyznaczeniu IOD w dalszej części rozdziału.

Wiedza i umiejętności IOD

Kogo zatem wybrać do pełnienia funkcji IOD? Przede wszystkim należy pamiętać, że wyznaczenie IOD musi odbywać się na podstawie kwalifikacji takiej osoby, w szczególności jego wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań IOD, określonych w RODO. Taka osoba powinna posiadać:

- odpowiednią wiedzę z zakresu krajowych oraz europejskich przepisów dot. ochrony danych osobowych
- dogłębną wiedzę z zakresu przepisów branżowych regulujących funkcjonowanie placówki medycznej (w szczególności przepisy ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, ustawy o podmiotach leczniczych, etc.)
- wiedzę o procesach przetwarzania, systemach informatycznych oraz zabezpieczeniach stosowanych w placówce medycznej
- wiedzę o procedurach administracyjnych i funkcjonowaniu placówki medycznej.

Priorytetem dla IOD powinno być zapewnienie przestrzegania RODO. Wspieranie „kultury ochrony danych" polegać będzie w głównej mierze na pomocy we wdrażaniu w placówce medycznej elementów RODO, tj.:

- zasad przetwarzania danych osobowych
- praw osób, których dane dotyczą
- ochrony danych w fazie projektowania oraz domyślnej ochrony danych
- rejestru czynności przetwarzania
- wymogów bezpieczeństwa przetwarzania
- zgłaszania naruszeń.

Wiedza i doświadczenie w tym zakresie powinny być kluczowymi kompetencjami kandydata na IOD.

Często niedoceniane w procesie wyboru odpowiedniego IOD są również umiejętności miękkie takiej osoby, do których zalicza się umiejętności komunikacyjne, negocjacyjne czy umiejętność rozwiązywania konfliktów. Cenną umiejętnością IOD będzie na przykład doświadczenie w prowadzeniu wystąpień publicznych – z uwagi na fakt, że IOD bardzo często prowadzi szkolenia dla personelu z zakresu ochrony danych osobowych.

Kierownicy placówek medycznych często pytają, jak w praktyce powinni sprawdzać potrzebną wiedzę i umiejętności kandydata na IOD, bowiem RODO nie reguluje zasad czy trybu weryfikacji spełnienia tego wymogu. Ważnym kryterium weryfikacji będą wobec tego różnego rodzaju certyfikaty, dyplomy oraz inne dokumenty poświadczające wiedzę i doświadczenie inspektora (np. ukończenie podyplomowych studiów z zakresu ochrony danych). Należy jednak pamiętać, że w Polsce nie ma jeszcze systemu certyfikacji wiedzy umiejętności IOD, nie można zatem jednoznacznie stwierdzić, że okazanie określonego certyfikatu czy dyplomu w zupełności potwierdza odpowiednie kompetencje.

Nie można również zapominać o aspekcie etycznym wyznaczenia IOD. Jak wskazuje również PUODO, *jeśli chodzi o osobiste cechy IOD kwalifikujące go do wykonywania funkcji, to są to: rzetelne podejście i wysoki poziom etyki zawodowej. Przydatne będą również: dyskrecja, umiejętność radzenia sobie w trudnych sytuacjach oraz umiejętności interpersonalne.*

Żyjemy w czasach dynamicznie zmieniających się przepisów prawa i rozwijających się technologii. IOD powinien zatem również stale podnosić swoją wiedzę i umiejętności – powinien się kształcić, rozwijać swoje doświadczenia i umiejętności w różnych formach edukacyjnych. Kierownictwo placówki medycznej powinno natomiast inspektorowi w tym pomagać, zapewniając mu m.in. niezbędne środki finansowe. Zgodnie bowiem z art. 38 ust. 2 RODO, placówka medyczna ma obowiązek zapewnienia IOD zasobów niezbędnych do utrzymania wysokiego i aktualnego poziomu wiedzy.

Kto może być IOD?

Zgodnie z art. 37 RODO, IOD może być:

- ktoś z personelu placówki medycznej

lub

- osoba wskazana przez wykonawcę takiego zadania na podstawie umowy o świadczenie usług.
- Placówka medyczna może zatem powierzyć funkcję IOD swojemu pracownikowi, albo też skorzystać z profesjonalnej firmy doradczej, która przejmie na siebie obowiązki IOD (outsourcing IOD).

Decydując się na wewnętrznego IOD, wyłonionego spośród kadry podmiotu leczniczego, należy pamiętać o konieczności zapewnienia takiej osobie realnej możliwości wypełniania obowiązków IOD poprzez właściwe określenie wymiarów czasu pracy na obydwu stanowiskach w sposób umożliwiający IOD wykonywanie swoich zadań. Niedopuszczalna będzie na przykład sytuacja, kiedy pracownik placówki medycznej wyznaczony na IOD będzie miał tak dużo obowiązków związanych z udzielaniem świadczeń opieki zdrowotnej, że nie będzie miał czasu na wykonywanie obowiązków IOD. Wyznaczenie wewnętrznego IOD musi również uwzględniać konflikt interesów – IOD nie może bowiem zajmować w placówce medycznej stanowiska związanego z określaniem sposobów i celów przetwarzania danych.

Kluczowe jest określenie w placówce medycznej listy tzw. niekompatybilnych stanowisk, których połączenie z funkcją IOD będzie niemożliwe. Będą to m.in.:

- stanowiska kierownicze (członek zarządu, dyrektor generalny, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu HR, kierownik działu IT)
- niższe stanowiska, jeśli sprawujące je osoby biorą udział w określaniu celów i sposobów przetwarzania danych, np. koordynator rejestracji, pełnomocnik ds. informacji niejawnych.

Mając powyższe ograniczenia na względzie, skutecznym rozwiązaniem może być korzystanie ze wsparcia zewnętrznej firmy specjalizującej się w ochronie danych osobowych w sektorze medycznym (np. firmy doradczej lub kancelarii prawnej). Należy jednak pamiętać, że eksperci takiej firmy powinni wykazywać się niezbędnymi kwalifikacjami i wiedzą, o których mowa powyżej. Co więcej – w uchwale, zarządzeniu lub decyzji kierownictwa w sprawie wyznaczenia IOD należy określić konkretną osobę fizyczną wskazaną przez taką firmę – nie wystarczy tu odniesienie się jedynie do nazwy firmy.

Zgłoszenie IOD do PUODO

Każda placówka medyczna, która wyznaczyła IOD ma obowiązek zawiadomić o tym fakcie organ nadzorczy. Jednym z kluczowych zadań IOD jest pełnienie roli punktu kontaktowego pomiędzy placówką medyczną a tym organem, dlatego też RODO wymaga, by dostarczyć informacje o tym, że administrator wyznaczył IOD, dając organowi nadzorczemu możliwość skontaktowania się z osobą pełniącą funkcję IOD w placówce medycznej. *Wskazuje to na szczególną rolę IOD jako głównego – i w oczywisty sposób preferowanego – partnera PUODO.*

Przepisy ustawy o ochronie danych osobowych wskazują, jakie konkretnie dane należy przekazać do PUODO.

Art. 10 ust. 1. ustawy o ochronie danych osobowych z 2018 r.

Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o jego wyznaczeniu w terminie 14 dni od dnia wyznaczenia, wskazując ***imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora****.*

Polskie przepisy wskazują również na formę zawiadamiania o danych kontaktowych IOD, przesądzając, że zawiadomienia sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP. W praktyce oznacza to, że jedyną dopuszczalną formą zgłoszenia IOD jest forma elektroniczna. Zawiadomienie należy przesłać, wykorzystując w tym celu jedną z dostępnych usług znajdujących się na stronie portalu biznes.gov.pl. Alternatywną formą zawiadomienia PUODO o danych kontaktowych IOD jest zawiadomienie, które można wysłać przez platformę epuap.gov.pl (użytkownik po zalogowaniu i wybraniu formularza przekierowywany jest na portal obywatel.gov.pl), załączając właściwy formularz spośród dostępnych na stronie PUODO.

Wymóg zachowania formy elektronicznej zawiadomienia może nastręczać pewnych praktycznych problemów, bowiem nie wszystkie osoby reprezentujące placówki medyczne dysponują takim podpisem kwalifikowanym czy też profilem zaufanym ePUAP. Rozwiązaniem dla takich placówek może być zawiadomienie o danych kontaktowych swojego IOD przez pełnomocnika (np. pracownika firmy świadczącej usługę outsourcingu IOD). Wówczas upoważnienie wydane przez kierownika placówki może zostać uwierzytelnione przez notariusza, który nada temu dokumentowi wymaganą formę elektroniczną, odpowiednią do przekazania PUODO.

Czy notariusz może uwierzytelnić elektronicznie pełnomocnictwo upoważniające do zawiadomienia?
Tak, osoba działająca w imieniu administratora/podmiotu przetwarzającego, może do zawiadomienia o wyznaczeniu inspektora ochrony danych załączyć pełnomocnictwo, które będzie uwierzytelnione elektronicznie przez notariusza. W takim przypadku do zawiadomienia należy załączyć pełnomocnictwo poświadczone za zgodność przez notariusza i opatrzone jego kwalifikowanym podpisem elektronicznym (art. 97 § 2 ustawy z dnia 14 lutego 1991 r. Prawo o notariacie, Dz. U. z 2017 r. poz. 2291 z późn. zm.). *
* Wytyczne PUODO, https://uodo.gov.pl/pl/224/632

Należy pamiętać, że na zgłoszenie IOD placówka medyczna ma jedynie 14 dni – liczone od dnia wyznaczenia IOD (czyli od dnia podjęcia uchwały/zarządzenia/decyzji kierownictwa wyznaczającego konkretną osobę fizyczną na funkcję IOD).

Zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych w ciągu 14 dni wymaga także:

- zmiana imienia, nazwiska, e-maila lub telefonu IOD
- zmiana nazwy, adresu siedziby lub REGON-u
- odwołanie inspektora ochrony danych.

Odpowiednie formularze dostępne są na stronie www.uodo.gov.pl oraz www.biznes.gov.pl

Wyznaczanie IOD

https://www.biznes.gov.pl/pl/firma/obowiazki-przedsiebiorcy/chce-chronic-dane-osobowe/proc_871-zawiadomienie-o-wyznaczeniu-nowego-iod

Zmiana danych IOD

https://www.biznes.gov.pl/pl/firma/obowiazki-przedsiebiorcy/chce-chronic-dane-osobowe/proc_872-zawiadomienie-o-zmianie-danych-inspektora-ochrony-danych

Zmiana danych ADO

https://www.biznes.gov.pl/pl/firma/obowiazki-przedsiebiorcy/chce-chronic-dane-osobowe/proc_877-zmiana-danych-administratora-lub-podmiotu-przetwarzajacego-dane

Odwołanie IOD

https://www.biznes.gov.pl/pl/firma/obowiazki-przedsiebiorcy/chce-chronic-dane-osobowe/proc_873-zawiadomienie-o-odwolaniu-inspektora-ochrony-danych

Publikacja danych kontaktowych IOD

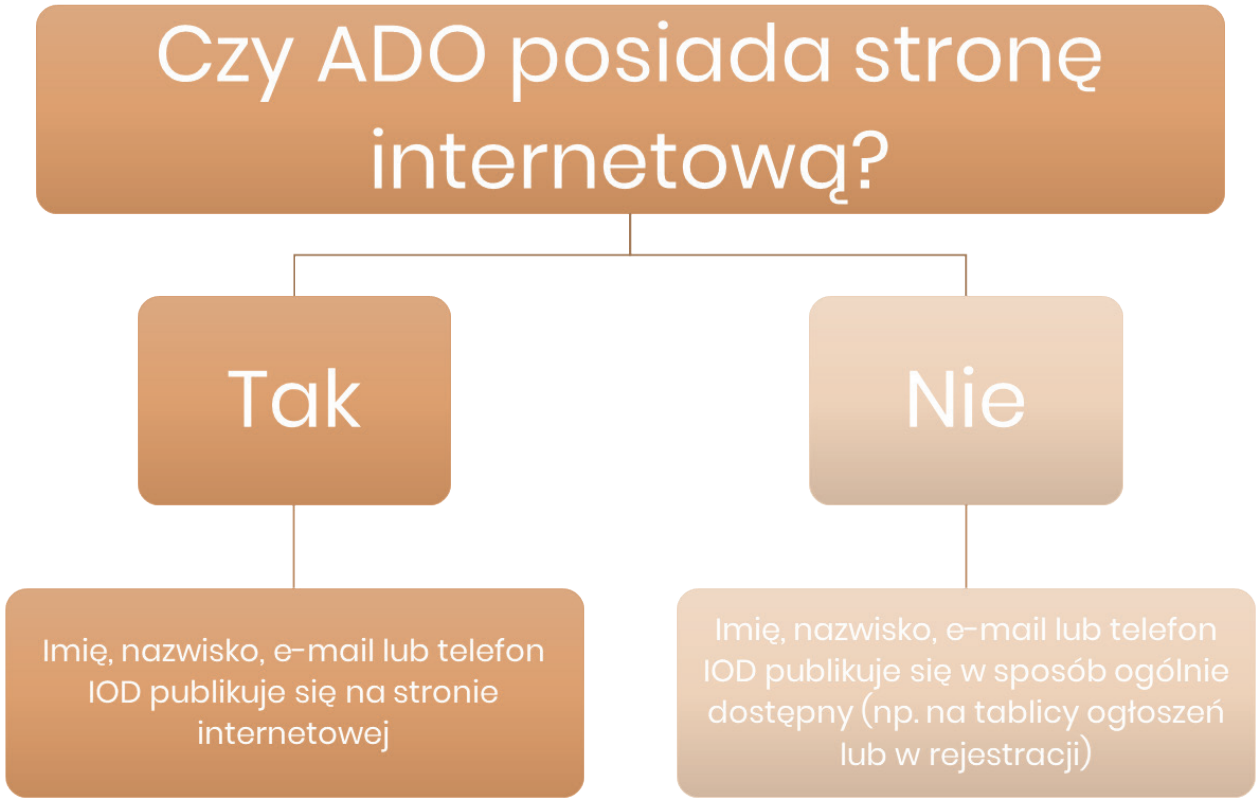
Niezależnie od poinformowania PUODO o danych kontaktowych IOD, każda placówka medyczna posiadająca inspektora jest zobowiązana również do niezwłocznego opublikowania danych kontaktowych IOD. Tylko dzięki temu można zapewnić pacjentom łatwy i bezpośredni kontakt z IOD, bez konieczności kontaktowania się z innymi jednostkami podmiotu. W ten oto sposób IOD staje się punktem kontaktowym zarówno dla PUODO (o czym wcześniej), ale również dla wszystkich osób, których dane dotyczą.

Imię i nazwisko, adres poczty elektronicznej lub nr telefonu IOD należy opublikować na stronie internetowej placówki medycznej. Najczęściej stosowanym na rynku rozwiązaniem jest umieszczenie tych informacji w zakładce KONTAKT lub też dedykowanej zakładce poświęconej ochronie danych osobowych (najczęściej nazywanej RODO lub OCHRONDA DANYCH).

Złą praktyką będzie publikowanie danych kontaktowych IOD w sposób utrudniający pacjentowi dotarcie do tych informacji, np. jedynie w klauzuli informacyjnej, czy też polityce prywatności dostępnej na stronie internetowej placówki.

Zgodnie z wymogiem łatwej dostępności tych informacji, placówka medyczna powinna dać realną możliwość łatwego znalezienia kontaktu do IOD na jej stronie internetowej.

Jeśli natomiast placówka medyczna nie prowadzi własnej strony internetowej, dane kontaktowe swojego IOD publikuje w sposób ogólnie dostępny w miejscu prowadzenia działalności, np. poprzez podanie tej informacji na tablicy ogłoszeń.



Niezależność IOD

W motywie 97 preambuły RODO czytamy, że IOD – bez względu na to, czy jest pracownikiem placówki medycznej – powinien być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny. Z tego powodu w RODO znalazło się wiele gwarancji tej niezależności.

Przede wszystkim IOD musi podlegać bezpośrednio najwyższemu kierownictwu. Bezpośrednia podległość oznacza, że w ramach wykonywanych zadań IOD nie może podlegać jakimkolwiek innym osobom lub jednostkom organizacyjnym wchodzącym w skład struktury administratora danych.

IOD powinien być zatem tak umieszczony w strukturze organizacyjnej, żeby odpowiadać jedynie przed kierownictwem placówki medycznej. Należy pamiętać, żeby takie umiejscowienie IOD znalazło swoje odzwierciedlenie w postanowieniach regulaminu organizacyjnego oraz wykresach struktury organizacyjnej placówki medycznej.

Od placówki medycznej oczekuje się również, że będzie wspierać IOD w wypełnianiu jego zadań. W przytoczonych już wcześniej Wytycznych WP 243 czytamy, że pomoc ta może polegać m.in. na:

- zapewnieniu odpowiedniego wsparcia finansowego, infrastrukturalnego (np. przekazanie IOD pomieszczenia, sprzętu, wyposażenia) i kadrowego
- oficjalnym zakomunikowaniu wszystkim pracownikom faktu wyznaczenia IOD i wskazaniu na jego rolę i zadania
- umożliwieniu dostępu do innych działów organizacji, np. HR, działu prawnego, IT.

Aby IOD mógł należycie wykonywać swoje zadania, niezbędne jest zapewnienie mu udziału we wszystkich zagadnieniach związanych z ochroną danych osobowych. Zgodnie z RODO, IOD powinien być włączany we wszystkie sprawy placówki medycznej dotyczące danych osobowych – i to od najwcześniejszego etapu. IOD powinien mieć również możliwość prezentowania swoich stanowisk i brać udział w spotkaniach kierownictwa – tak, aby ułatwiać w placówce medycznej zapewnianie zgodności w podejmowanych decyzjach w zakresie ochrony danych osobowych pacjentów.

W praktyce należy zatem zachęcać personel placówki medycznej do konsultowania wszelkich wewnętrznych regulaminów, procedur czy nawet wątpliwości związanych z wykonywaniem bieżących zadań – zawsze kiedy to działanie dotyczy danych osobowych.

W przypadku wątpliwości w zakresie ustalenia, czy osoba wnioskująca o kopię dokumentacji medycznej zmarłego pacjenta jest faktycznie osobą bliską, za którą się podaje, pracownik rejestracji powinien taką sytuację skonsultować z IOD. Od IOD oczekiwane będzie w tym zakresie przedstawienie opinii (ew. po zasięgnięciu opinii prawnika) co do zasadności udostępnienia dokumentacji i wskazania ryzyk związanych z przekazaniem tej dokumentacji osobie nieupoważnionej.

IOD powinien być również każdorazowo informowany o naruszeniach ochrony danych w placówce medycznej, tak by pomóc we właściwej ocenie ryzyka, jakie wiąże się z danym incydentem i w podjęciu decyzji o ewentualnym zawiadomieniu PUODO, czy nawet pacjentów, o naruszeniu.

W ramach wypełniania swoich obowiązków IOD nie powinien otrzymywać poleceń kierownictwa odnośnie sposobów załatwienia danej sprawy, czy też przyjęcia oczekiwanej przez kierownictwo wykładni przepisów RODO albo ustaw branżowych. W praktyce wydawanie instrukcji określonego działania dla IOD może mieć bardzo negatywne konsekwencje dla placówki medycznej. Wiedza i umiejętności IOD powinny być wykorzystywane bowiem do właściwej oceny ryzyk i konsekwencji prawnych określonego działania placówki medycznej, dzięki czemu kierownik tej placówki, przed podjęciem decyzji dotyczących np. udostępnienia danych osobowych, będzie miał pełniejszy ogląd sytuacji.

IOD nie może być również odwołany, ani karany, w związku z wykonywaniem swoich zadań. Nie może zatem zostać odwołany, ani ukarany, za zajęcie określonego stanowiska i przekazanie zalecenia, nawet jeśli jest ono niezgodne ze stanowiskiem reprezentowanym przez kierownictwo placówki medycznej. Chodzi tu o kary w różnych formach, np. brak albo opóźnienie awansu, utrudnienie rozwoju zawodowego, ograniczenie dostępu do korzyści oferowanych pozostałym pracownikom. Nie oznacza to jednak, że IOD nie może zostać odwołany w uzasadnionych sytuacjach z przyczyn innych niż wykonywanie swoich obowiązków wynikających z RODO – mowa tu np. o odpowiedzialności dyscyplinarnej w związku z kradzieżą sprzętu służbowego.

Zadania IOD

Podstawowym celem działalności IOD w placówce medycznej jest wspieranie placówki w „monitorowaniu wewnętrznego przestrzegania RODO", jak czytamy w motywie 97 preambuły RODO. IOD ma zatem, w gruncie rzeczy, funkcję doradczą. Niedopuszczalną praktyką będzie uznanie IOD jako osoby odpowiedzialnej za właściwą realizację obowiązków wynikających z RODO. Jest to już wyłączną odpowiedzialnością administratora danych, czyli placówki medycznej reprezentowanej przez jej kierownictwo.

Zgodnie z RODO, zadania IOD można podzielić na 4 zasadnicze grupy:

- zadania informacyjne i doradcze
- zadania monitorujące i nadzorcze
- zadania w zakresie współpracy z organem nadzorczym
- inne zadania niewskazane w komentowanym przepisie.

IOD będzie zatem odpowiedzialny za informowanie kierownictwa oraz pracowników placówki medycznej, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz przepisów branżowych.

W praktyce oznaczać to będzie przypisanie IOD zadania przygotowania odpowiedniej dokumentacji RODO dla placówki medycznej oraz jej pracowników. Mowa tu m.in. o: polityce bezpieczeństwa, procedurze nadawania upoważnień czy też zasadach wykrywania i postępowania z naruszeniami ochrony danych.

Więcej na temat dokumentacji RODO w placówce medycznej znajduje się w rozdziale VII.

Od IOD oczekiwane jest również prowadzenie rejestru przetwarzania danych zgodnie z art. 30 RODO. Co prawda – jak wskazano wcześniej – odpowiedzialność za realizację obowiązków wynikających z RODO spoczywa na administratorze danych, jednak w zgodnej opinii unijnych organów ochrony danych, to właśnie IOD będzie w praktyce realizował zadanie prowadzenia i aktualizacji rejestru czynności przetwarzania danych.

Wprawdzie z art. 30 rozporządzenia ogólnego bezsprzecznie wynika, że obowiązek prowadzenia rejestrów należy do administratorów i podmiotów przetwarzających, nie zaś do inspektora ochrony danych, niemniej trudno sobie wyobrazić, że inspektor ochrony danych – jako osoba dysponująca odpowiednią wiedzą i umiejętnościami w dziedzinie ochrony danych osobowych –– nie będzie angażował się w tworzenie i prowadzenie rejestrów, a następnie wykorzystywał ich w swojej pracy.
Inspektor ochrony danych jako fachowiec może wspomagać administratora w tworzeniu i prowadzeniu rejestrów na przykład poprzez zbieranie informacji w celu identyfikacji procesów przetwarzania.
Wytyczne PUODO, https://uodo.gov.pl/pl/225/659

IOD w dalszej kolejności będzie monitorować przestrzeganie RODO analizując procesy przetwarzania danych odbywające się w placówce medycznej. Oznacza to potrzebę włączania IOD w proces opiniowania zawieranych przez placówkę medyczną umów czy też uwzględnianie rekomendacji IOD w zakresie organizacji udzielania świadczeń opieki zdrowotnej (np. regulaminów i innych procedur funkcjonowania rejestracji zapewniających poszanowanie prawa do prywatności pacjenta).

IOD powinien być konsultowany w przypadku zawierania umowy z laboratorium diagnostycznym oraz każdym innym podmiotem, któremu przekazywane są dane osobowe pacjentów placówki medycznej.
Zasadne jest również konsultowanie najróżniejszych wniosków o dostęp do dokumentacji medycznej kierowanych przez podmioty czy instytucje (takie jak sądy, ZUS czy zakłady ubezpieczeń). IOD powinien pomóc ocenić czy wniosek został złożony przez uprawniony podmiot, czy żądanie danych osobowych jest zasadne, etc.

IOD będzie również odpowiedzialny za prowadzenie cyklicznych audytów ochrony danych, sprawdzających stosowanie procedur związanych z ochroną danych osobowych. Taki audyt powinien obejmować wszystkie istotne obszary działalności podmiotu leczniczego, mianowicie obszar prawny, fizyczny oraz informatyczny.

Audyt obszaru prawnego obejmuje m.in. sprawdzenie, przygotowanie lub aktualizację takich dokumentów jak: dokumentacja RODO, upoważnienia do danych osobowych, umowy z firmami/podmiotami zewnętrznymi, wnioski/formularze/dokumenty (pod kątem podstaw prawnych zbierania danych, zasadnego zakresu danych oraz okresów przechowywania) czy też klauzule informacyjne.
Audyt obszaru fizycznego obejmuje przegląd wprowadzonych środków organizacyjnych, np. stosowanie zasady czystego biurka, czy szuflady/szafki/szafy zamykane są na klucz, sprawność działania systemu alarmowego, monitoring wizyjny, sprzątanie pomieszczeń, prowadzenie dokumentacji archiwalnej, ustawienie monitorów, procesy niszczenia dokumentacji medycznej.
Audyt obszaru informatycznego obejmuje przegląd wprowadzonych środków technicznych, np. statusy w zakresie stosowania indywidulanych loginów i haseł, aktualność programów antywirusowych, firewalli itp., bezpieczeństwo wysyłania wiadomości e-mail, zasady używania nośników danych jak również zasady wykonywania kopii zapasowych.

Po przeprowadzonym audycie, IOD powinien przygotować i przekazać kierownikowi placówki medycznej raport poaudytowy. W raporcie należy opisać stan faktyczny, jaki stwierdzono przy sprawdzaniu oraz zalecenia, jakie w związku z tym należy wprowadzić. W ramach zaleceń może powstać potrzeba kupienia nowych sprzętów lub urządzeń, nowa procedura postępowania (np. weryfikacji tożsamości pacjentów), nowe dokumenty czy też nowe wersje dokumentów już istniejących.

Rolą IOD będzie również prowadzenie działań zwiększających wiedzę i świadomość personelu z zakresu ochrony danych osobowych, w tym szkoleń wszystkich osób uczestniczących w operacjach przetwarzania danych.

IOD będzie w końcu pierwszym wyborem każdego pacjenta w zakresie pytań związanych z przetwarzaniem ich danych osobowych oraz realizacji praw, jakie pacjentom przyznaje RODO (np. prawo dostępu do danych czy też prawo sprzeciwu). To IOD powinien również wyznaczać standardy w zakresie udzielania odpowiedzi na te pytania – zasady potwierdzania tożsamości wnioskodawcy, czas na załatwienie sprawy czy też ocenę zasadności wniosków.

Pełnienie funkcji punktu kontaktowego przez IOD najlepiej widać podczas lektury klauzul informacyjnych stosowanych na rynku. Zgodnie z wymogami art. 13-14 RODO, przekazując pacjentowi informacje o zasadach przetwarzania danych, placówka medyczna ma obowiązek poinformować o danych kontaktowych właśnie IOD. Podając nr telefonu lub adres e-mail IOD wskazujemy pacjentom, że to właśnie inspektor ochrony danych będzie dla nich punktem kontaktowym we wszystkich sprawach związanych z RODO.

Rozdział III. Pracownik jako element systemu ochrony danych osobowych

Podstawowe zasady bezpieczeństwa danych osobowych

Zapewnienie bezpieczeństwa danych osobowych jest jednym z kluczowych wyzwań stojących przed administratorem danych, chcącym zachować zgodność z przepisami o ochronie danych osobowych. Zgodnie z art. 32 RODO podmiot leczniczy, działając jako administrator danych, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania a także ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, ma obowiązek wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

Bezpieczeństwo danych może zostać zapewnione poprzez stosowanie:

- środków ochrony fizycznej (drzwi ognioodporne, korzystanie z usług firmy ochroniarskiej, monitoringu wizyjnego)
- środków technicznych (np. szyfrowania danych, pseudonimizacji, stosowania kopii zapasowych, ochrony antywirusowej)
- środków organizacyjnych (np. utworzenie polityki bezpieczeństwa, prowadzenie szkoleń podnoszących wiedzę personelu).

Należy jednak pamiętać, że wdrożenie w podmiocie leczniczym jedynie środków organizacyjnych, np. poprzez stosowanie polityki bezpieczeństwa, procedur, standardów, norm, certyfikatów, lub zabezpieczeń fizycznych, bez wdrażania jakichkolwiek środków technicznego zabezpieczenia systemów informatycznych w praktyce spowoduje podniesienie poziomu ryzyka dla ochrony danych znajdujących się w tych systemach.

Przykład:
Wdrożenie w podmiocie leczniczym odpowiedniej polityki i procedur z zakresu ochrony danych osobowych, a także zamontowanie wysokiej klasy systemów antywłamaniowych czy krat w oknach może nie stanowić wystarczających środków ochrony danych osobowych, jeśli komputery pracowników nie zostaną właściwie zabezpieczone, np. pracownicy będą pracować na systemach operacyjnych, które zostały pozbawione wsparcia – Windows XP oraz Windows Vista lub nie będą posiadać zainstalowanych na komputerach programów antywirusowych, a podmiot leczniczy nie będzie wykonywał kopii bezpieczeństwa posiadanych danych.

W powyższej sytuacji będzie istniało wysokie ryzyko zainfekowania komputera wirusem i kradzieżą danych przechowywanych na komputerach, czy też zaszyfrowania dysku twardego komputera przez hackera, co w praktyce będzie oznaczało utratę dostępności danych osobowych, a tym samym istotne naruszenie ochrony danych osobowych. Dlatego powyższy przykład jasno pokazuje, że wdrożenie jednego rodzaju środków zabezpieczenia danych osobowych w praktyce nie będzie skuteczne i w konsekwencji może doprowadzić do poważnego naruszenia ochrony danych osobowych, w wyniku którego podmiot leczniczy może nawet stracić dostęp do większości przetwarzanych przez siebie danych osobowych. Współcześnie skala zagrożeń dla systemów informatycznych jest tak duża, że nawet małe podmioty lecznicze mogą stać się celem ataku hackerskiego, dlatego tak ważne jest wdrażanie odpowiednich zabezpieczeń technicznych.

Należy jednak wskazać, że nawet w przypadku posiadania najlepszych zabezpieczeń organizacyjnych, technicznych czy fizycznych zawsze będzie istniał jeden niezwykle wrażliwy element systemu ochrony danych osobowych, którym będzie człowiek. Dlatego projektując system ochrony danych osobowych w podmiocie leczniczym, zawsze trzeba pamiętać o pracowniku, jako jego najbardziej wrażliwym elemencie, któremu należy poświęcić odpowiednią uwagę.

Jeden z najważniejszych obowiązków podmiotu leczniczego w kontekście pracownika został wskazany w art. 29 RODO, zgodnie z nim podmiot leczniczy, działając jako administrator danych, zobowiązany jest upoważnić do przetwarzania danych osobowych swoich pracowników, którzy mają dostęp do danych osobowych i je przetwarzają. Należy jednak w tym miejscu wskazać, że upoważnienia do przetwarzania danych osobowych powinny zostać nadane jedynie pracownikom, których zadania służbowe wymagają przetwarzania danych osobowych, dlatego błędem będzie udzielanie upoważnień do przetwarzania danych osobowych personelowi sprzątającemu.

Niezwykle ważnym zadaniem podmiotu leczniczego, które ma kluczowe znaczenie dla bezpieczeństwa danych osobowych przetwarzanych przez niego, jest zapoznanie swoich pracowników z obowiązującymi zasadami przetwarzania danych. W tym celu podmiot leczniczy powinien:

- prowadzić szkolenia dla nowych pracowników, obejmujące zagadnienia z zakresu ochrony danych osobowych
- prowadzić szkolenia okresowe, uwzględniające specyfikę funkcjonowania podmiotu leczniczego
- udostępniać i wymagać zapoznania się z dokumentacją przetwarzania danych, np. z polityką, procedurami oraz instrukcjami określającymi zasady działania obowiązujące w podmiocie leczniczym, a w razie aktualizacji tych dokumentów – informować o stosowanych zmianach
- uświadamiać czym są naruszenia i wskazywać na konieczność zgłaszania naruszeń, w tym w jaki sposób można dokonać takiego zgłoszenia
- uwzględniając sposoby komunikacji z pracownikami przyjęte w podmiocie leczniczym, wskazywać na najczęstsze przypadki, w których dochodzi do naruszenia przepisów o ochronie danych osobowych
- wskazywać w jaki sposób należy się zachować, jeśli pracownik, który nie jest wyznaczony w podmiocie leczniczym do odpowiadania na wnioski podmiotów danych, otrzyma taki wniosek
- wskazywać zasady przetwarzania danych osobowych przy współpracy z zewnętrznymi podmiotami, w tym informować, kiedy zachodzi konieczność zawarcia umowy powierzenia przetwarzania danych osobowych i jakie konsekwencje wynikają z jej zawarcia, np. konieczność uzupełnienia rejestru czynności przetwarzania
- udostępniać sprzęt zapewniający bezpieczne przetwarzanie danych i określić przejrzyste zasady postępowania z tym sprzętem
- określać jasne zasady przechowywania danych, w tym postępowania z danymi w przypadku opuszczania miejsca pracy lub zakończenia dnia pracy
- przypisać rolę wybranym pracownikom, którzy będą odpowiedzialni za operacyjne procesy realizowania obowiązków wynikających z RODO, np. odpowiadanie na wnioski podmiotów danych, zbieranie informacji o naruszeniu, przeprowadzanie analiz ryzyka czy oceny skutków dla ochrony danych, zwłaszcza gdy u pracodawcy nie powołano inspektora ochrony danych lub specjalnej komórki, która wspiera pracodawcę w realizowaniu obowiązków wynikających z RODO
- cyklicznie sprawdzać realizację obowiązków przez pracowników w zakresie ochrony danych osobowych i w razie potrzeby podejmować działania zmierzające do zapewnienia zgodności postępowania pracowników z zasadami ustalonymi w podmiocie leczniczym.

Należy wskazać, że środki bezpieczeństwa stosowane przez podmiot leczniczy powinny być adekwatne do istniejącego ryzyka. Jednak analizując ryzyko związanie z naruszeniem bezpieczeństwa danych osobowych, należy brać pod uwagę nie tylko ryzyko związane z naruszeniem praw i wolności osób, których dane dotyczą, ale także ewentualne negatywne konsekwencje naruszenia ochrony danych osobowych dla podmiotu leczniczego.

Przykład:
Prywatna klinika leczenia niepłodności w ramach przeprowadzonej analizy ryzyka nie uwzględniła w sposób wystarczający podatności systemu, w którym były przetwarzane dane pacjentów. Na skutek braku odpowiednich zabezpieczeń doszło do wycieku danych z systemu. Poza koniecznością zgłoszenia naruszenia do organu nadzorczego i poinformowania osób, których dane dotyczą, klinika poniosła straty wizerunkowe, tj. utratę dotychczasowych i przyszłych (potencjalnych) klientów i materialne, z uwagi na konieczność zapłaty administracyjnej kary pieniężnej nałożonej przez organ nadzorczy.

Konsekwencje nieprzestrzegania zasad bezpieczeństwa danych osobowych przez pracownika

Nieprzestrzeganie zasad bezpieczeństwa danych osobowych zawartych w RODO może spowodować negatywne konsekwencje dla podmiotu danych w postaci:

- kradzieży tożsamości lub oszustwa dotyczącego tożsamości
- straty finansowej
- naruszenia dobrego imienia
- naruszenia poufności danych osobowych chronionych tajemnicą zawodową
- nieuprawnionego odwrócenia pseudonimizacji
- wszelkiej innej znacznej szkody gospodarczej lub społecznej.

Ochrona danych osobowych w podmiocie leczniczym nie ogranicza się jedynie do kwestii związanych z ochroną prywatności podmiotu danych (pacjenta). Nieprawidłowe przetwarzanie danych osobowych przez podmiot leczniczy może mieć bezpośredni wpływ na stan zdrowia pacjentów, co obrazują poniższe przykłady.

Przykład:
Błędne oznaczenie próbek z materiałem biologicznym pacjenta może spowodować postawienie błędnej diagnozy dolegliwości pacjenta.

W powyższym przykładzie mamy do czynienia z pomyłką pracownika, która polegała na błędnym oznaczeniu próbki materiału biologicznego pobranego od pacjenta, tym samym doszło do naruszenia ochrony danych osobowych w zakresie integralności danych.

Przykład:
Zagubienie dokumentacji medycznej lub jej części przez pracownika podmiotu leczniczego może mocno opóźnić (w skrajnych przypadkach uniemożliwić) udzielenie doraźnej pomocy pacjentowi, który zgłosi się do podmiotu leczniczego.

W powyższym przykładzie mamy do czynienia ze zgubieniem przez pracownika dokumentacji medycznej pacjenta, na skutek czego podmiot leczniczy utracił czasowo dostęp do dokumentacji , tym samym doszło do naruszenia ochrony danych osobowych w zakresie dostępności danych.

Przykład:
W wyniku pomylenia dokumentacji zabiegowej przez pracownika podmiotu leczniczego pacjent może przejść zabieg, który nie był dla niego zaplanowany, np. może zostać mylnie zacewnikowany.

W powyższym przykładzie mamy do czynienia z pomyłką pracownika podmiotu leczniczego, która polegała na pomyleniu dokumentacji zabiegowej dwóch pacjentów, w konsekwencji doszło do naruszenia ochrony danych osobowych w zakresie integralności danych.

Przykład:
Przeglądanie przez pracownika podmiotu leczniczego niezaufanych stron internetowych na służbowym komputerze może doprowadzić do zainfekowania urządzenia złośliwym oprogramowaniem, które może uniemożliwić dostęp (zaszyfrować dysk twardy komputera) do danych przechowywanych na komputerze lub doprowadzić do pobrania danych z komputera przez nieuprawnioną do tego osobę. W pierwszym przypadku nie będziemy w stanie pomóc pacjentowi, w razie nagłego zagrożenia dla jego życia i w konieczności szybkiego uzyskania informacji o dotychczasowym przebiegu choroby pacjenta. Natomiast w drugim przypadku może dojść do naruszenia dobrego imienia lub innych dóbr osobistych pacjenta, na skutek wykorzystania wrażliwej informacji o stanie jego zdrowia, np. informacji o licznych chorobach wenerycznych osoby pozostającej w trwałym związku.

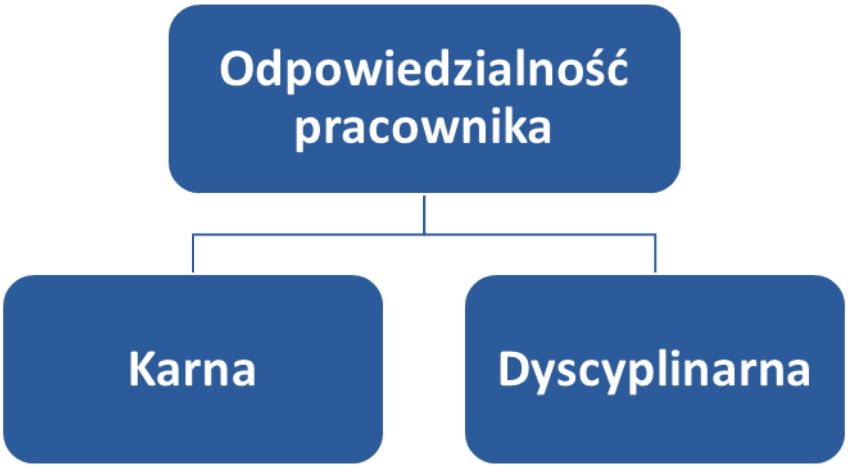
W powyższym przykładzie mamy do czynienia z nierozważnym działaniem pracownika podmiotu leczniczego, które może doprowadzić do poważnych konsekwencji dla podmiotu leczniczego, gdyż w przypadku zdalnego zaszyfrowania dysku twardego podmiot leczniczy traci dostęp do danych przechowywanych na dysku twardym takiego komputera, a tym samym dochodzi do naruszenia ochrony danych osobowych w zakresie dostępności danych. Natomiast w przypadku pobrania danych przechowywanych na komputerze przez nieuprawnioną do tego osobę dochodzi do naruszenia ochrony danych osobowych w zakresie poufności danych.

Przykład:
Wyrzucenie przez pracownika podmiotu leczniczego na śmietnik dokumentów zawierających dane osobowe, zamiast ich zniszczenia, może spowodować naruszenie dobrego imienia pacjenta lub innych jego dóbr osobistych, na skutek upublicznienia wrażliwej informacji o stanie jego zdrowia.

W powyższym przykładzie mamy do czynienia z lekkomyślnym działaniem pracownika podmiotu leczniczego, które może doprowadzić do nielegalnego ujawnienia danych osobowych, a tym samym do naruszenia ochrony danych osobowych w zakresie poufności danych.

Odpowiedzialność pracownika w zakresie przetwarzania danych osobowych

Mimo że administrator i podmiot przetwarzający są odpowiedzialni za naruszenie przepisów RODO pracownik przetwarzający dane w imieniu tych podmiotów również może odpowiadać za naruszenie przepisów o ochronie danych. W zakresie naruszenia przepisów o ochronie danych osobowych możemy rozpatrywać karną lub dyscyplinarną odpowiedzialność pracownika.



Rodzaje odpowiedzialności pracownika

W związku z powyższym każdy pracownik przetwarzający dane osobowe powinien:

- zapoznać się z dokumentacją obowiązującą w podmiocie leczniczym i podpisać oświadczenie, w który zobowiązuje się do przestrzegania przyjętych w organizacji rozwiązań w przedmiocie ochrony danych osobowych
- otrzymać upoważnienie do przetwarzania danych osobowych określające zakres danych, które ma prawo przetwarzać w ramach pełnionych przez niego obowiązków służbowych.

§ 1. Za nieprzestrzeganie przez pracownika ustalonej organizacji i porządku w procesie pracy, przepisów bezpieczeństwa i higieny pracy, przepisów przeciwpożarowych, a także przyjętego sposobu potwierdzania przybycia i obecności w pracy oraz usprawiedliwiania nieobecności w pracy, pracodawca może stosować:
1) karę upomnienia
2) karę nagany.
§ 2. Za nieprzestrzeganie przez pracownika przepisów bezpieczeństwa i higieny pracy lub przepisów przeciwpożarowych, opuszczenie pracy bez usprawiedliwienia, stawienie się do pracy w stanie nietrzeźwości lub spożywanie alkoholu w czasie pracy – pracodawca może również stosować karę pieniężną.

§

- art. 108 Kodeksu pracy

Jako naruszenia ustalonej organizacji i porządku w procesie pracy należy traktować wszelkie uchybienia w stosunku do aktów wewnątrzzakładowych, które ten porządek określają, takich jak układ zbiorowy pracy czy regulamin pracy. Każde uchybienie w stosunku do szczegółowo skonkretyzowanych powinności pracownika zaliczyć należy do zachowań rodzących odpowiedzialność porządkową[6].

Odpowiedzialność porządkowa charakteryzuje się winą w działaniu i bezprawnością zachowania pracownika. Wina z reguły będzie występowała w formie winy umyślnej. Istotne jest, że rodzaj naruszonych przepisów i stopień winy powinny być uwzględniane przy wyborze rodzaju kary porządkowej. Za bezprawne uważa się także zachowania sprzeczne z obowiązującymi przepisami, zarówno tymi z Kodeksu pracy, jak i regulaminu pracy, a także z poleceniami służbowymi pracodawcy. Jednak polecenia pracodawcy muszą być zgodne z prawem i muszą dotyczyć pracy. Do poleceń pracodawcy, jako podstawy działania pracownika, odnosi się także samo RODO.

[6] Zob. W. Muszalski, *Kodeks pracy. Komentarz, Warszawa 2019.*

Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarza je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

§

- art. 29 RODO

Poza odpowiedzialnością porządkową pracownik może także odpowiadać karnie za bezprawne przetwarzanie danych osobowych. Choć RODO nie przewiduje odpowiedzialności karnej za przetwarzanie danych osobowych niezgodnie z jego przepisami, to jednak zgodnie z motywem 149 RODO państwa członkowskie mają możliwość ustanawiania przepisów przewidujących sankcje karne za naruszenie RODO, w tym za naruszenie krajowych przepisów przyjętych na jego mocy.

Powyższe uprawnienie pozwala państwom członkowskim wprowadzić odpowiedzialność karną za nielegalne przetwarzanie danych osobowych. Polski ustawodawca zdecydował się skorzystać z tego uprawnienia i wprowadził przepisy karne za bezprawne przetwarzanie danych osobowych w poniżej przytoczonych przepisach ustawy o ochronie danych osobowych.

1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.
2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

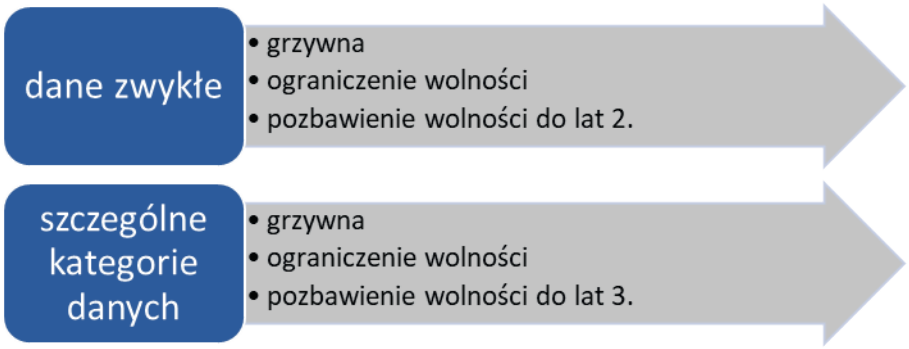
§

- art. 107 Ustawy o ochronie danych osobowych[7]

Odpowiedzialność, o której mowa w przywołanym powyżej przepisie ma charakter powszechny i dotyczy każdej osoby, która przetwarza dane osobowe, choć nie posiada ważnej podstawy prawnej do ich przetwarzania, przetwarzanie danych jest wprost zakazane albo gdy dane przetwarzane są przez osobę nieposiadającą do tego upoważnienia, lub osobę, która przekroczy jego zakres.

Ponadto przytoczony przepis przewiduje różne kary za bezpodstawne przetwarzanie danych zwykłych oraz szczególnych kategorii danych. W razie przetwarzania danych zwykłych przepis przewiduje karę grzywny, ograniczenia wolności lub pozbawienia wolności do 2 lat. Natomiast w przypadku przetwarzania szczególnych kategorii danych, maksymalny wymiar kary zwiększony został do 3 lat pozbawienia wolności.

[7] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).



Kary za naruszenie art. 107 ustawy o ochronie danych osobowych.

Należy tutaj podkreślić, że podleganie odpowiedzialności karnej z tytułu naruszenia art. 107 ustawy o ochronie danych osobowych nie jest uzależnione od winy czy umyślności działania sprawcy.

Przykład:
Pracownik, który nie posiadał upoważnienia do przetwarzania danych i nieumyślnie usunął dokumentację medyczną pacjentów podmiotu leczniczego będzie mógł zostać pociągnięty do odpowiedzialności z tytułu art. 107 ustawy o ochronie danych osobowych, ponieważ przetwarzał dane dotyczące zdrowia, mimo że nie był uprawniony do ich przetwarzania.

Rozdział IV. Dokumentacja ochrony danych osobowych w placówce medycznej

Jednym ze sposobów spełnienia warunku rozliczalności jest dokumentowanie procesów przetwarzania danych osobowych. Oznacza to, że procedury lub instrukcje związane z ochroną danych osobowych powinny być spisane. Jest to bardzo dobre rozwiązanie, zwłaszcza na wypadek ewentualnej kontroli.

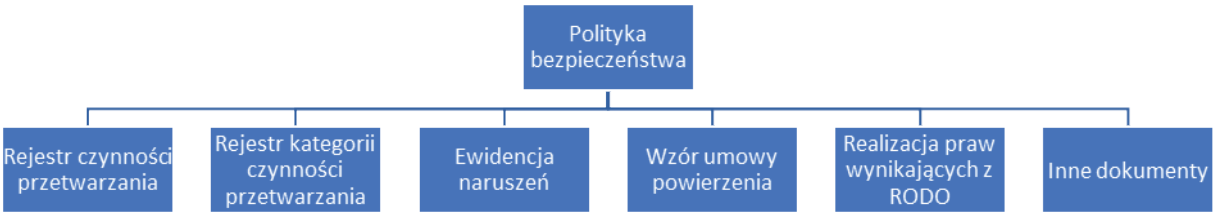
W treści tego rozdziału opiszemy najważniejsze dokumenty, które powinny być wykorzystywane przez placówkę medyczną w związku ze stosowaniem RODO.

Polityka bezpieczeństwa

Do maja 2018 r. każdy administrator danych miał mieć politykę bezpieczeństwa. Powinny się tam znajdować m.in. miejsca przetwarzania danych osobowych, zbiory danych i wykorzystywane środki bezpieczeństwa.

Po rozpoczęciu stosowania RODO prowadzenie polityki nie jest już obowiązkiem. Tego przyzwyczajenia nie trzeba jednak zmieniać. Trzeba pamiętać tylko o tym, że przepisy już nie wskazują jasno, co ma być w polityce a co musi znaleźć swoje odbicie w treści dokumentu.

W naszej ocenie polityka bezpieczeństwa ma być podstawową częścią dokumentacji RODO. Ma się tam znaleźć zbiór najważniejszych informacji. Pozostałe, bardziej szczegółowe instrukcje czy procedury powinny być załącznikami do polityki.



Co ma się znaleźć w polityce bezpieczeństwa placówki medycznej?

- nazwa i dane kontaktowe administratora danych
- wskazanie sposobu wykorzystania danych osobowych
- określenie podstawowych zasad bezpieczeństwa danych w placówce medycznej
- wskazanie, czy wyznaczono inspektora ochrony danych i, w razie potrzeby, określenie jego obowiązków
- wskazanie, czy wyznaczono administratora systemów informatycznych (ASI) i, w razie potrzeby, określenie jego obowiązków.

W załącznikach należy uregulować w szczególności:

- rejestr czynności przetwarzania
- rejestr kategorii czynności przetwarzania
- ewidencję naruszeń ochrony danych
- sposób realizacji praw wynikających z RODO (dostęp do danych, kopia danych, prawo do bycia zapomnianym)
- procedurę udzielania informacji lub wydawania dokumentacji medycznej

- sposób postępowania w razie stwierdzenia naruszeń ochrony danych (procedura alarmowa)
- sposób pracy w systemach informatycznych
- wzór upoważnienia do przetwarzania danych osobowych
- wzór umowy powierzenia.

Rejestr czynności przetwarzania

Rejestr czynności przetwarzania to najważniejszy z dokumentów, jakie wprost wskazano w RODO.

Każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się wszystkie następujące informacje:
a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
b) cele przetwarzania;
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.
- art. 30 ust. 1 RODO

Co ma się znaleźć w rejestrze?

W rejestrze czynności przetwarzania należy przede wszystkim wskazać:

- nazwę i dane kontaktowe administratora danych – placówki medycznej (np. JAMANOWSKI PRAKTYKA LEKARZA RODZINNEGO (ul. Piekarska 221B, 57-540 Lądek-Zdrój))
- dane kontaktowe inspektora ochrony danych (np. iod@jamanowski.pl).

Potem w rejestrze należy wypisać wszystkie czynności przetwarzania, jakie mają miejsce w placówce medycznej z uwzględnieniem informacji, o których mowa w art. 30 ust. 1 lit. b-g RODO, tj.:

- cele przetwarzania – do czego używamy danych osobowych? Co się z nimi dzieje? Po co są przetwarzane?
- opis kategorii danych osób, których dane dotyczą – kim są osoby, których dane osobowe wykorzystujemy? Pracownikami, pacjentami, przedstawicielami kontrahentów?
- opis kategorii danych osobowych – jakie konkretnie rodzaje danych osobowych wykorzystujemy? Imiona, nazwiska, adresy zamieszkania, numery telefonów, informacje o stanie zdrowia?
- kategorie odbiorców – kto oprócz nas będzie wykorzystywał te dane osobowe? Dostawca programu do obsługi pacjentów, księgowa, informatyk, firma zajmująca się archiwizacją dokumentów? UWAGA: ze względu na definicję odbiorcy w RODO nie umieszczamy tu instytucji, które dostęp do danych mają na mocy przepisów prawa (np. NFZ wobec danych o pacjentach lub ZUS w stosunku do danych o pracownikach)

- przekazanie danych osobowych do państwa trzeciego – w zdecydowanej większości przypadków w placówkach medycznych do takiego przekazywania nie dochodzi. „Państwo trzecie" w rozumieniu RODO to kraj, który nie należy do Europejskiej Organizacji Gospodarczej
- planowane terminy usunięcia poszczególnych kategorii danych – kiedy planujemy usunąć te dane osobowe? Im dokładniej podamy ten termin, tym lepiej
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa – podkreślenia wymaga tu słowo „ogólny". Wystarczające będzie np. wskazanie, że używamy czujek ruchu, stosujemy monitoring wizyjny lub mamy zainstalowane programy antywirusowe – bez doprecyzowania, jaka firma zakładała czujki, gdzie są rozmieszczone kamery albo jak nazywa się producent antywirusa.

Najprościej prowadzić rejestr czynności przetwarzania w formie tabeli:

Administrator danych			
Inspektor ochrony danych			
	Czynność przetwarzania #1	Czynność przetwarzania #2	Czynność przetwarzania …
Cel przetwarzania			
Kategorie osób			
Kategorie danych osobowych			
Kategorie odbiorców			
Przekazanie danych do państwa trzeciego			
Planowane terminy usunięcia danych			
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa			

Jak szczegółowo powinien być prowadzony rejestr czynności przetwarzania? Ile czynności przetwarzania należy w nim wyróżnić? Nie ma jednej odpowiedzi. Pod uwagę powinno się brać między innymi wielkość placówki medycznej (według specjalizacji, według liczby pacjentów, według liczby pracowników) – co do zasady im większa placówka, tym więcej procesów przetwarzania.

Poniżej przykładowy sposób wypełnienia rejestru czynności przetwarzania dla czynności PROWADZENIE DOKUMENTACJI MEDYCZNEJ

	Prowadzenie dokumentacji medycznej
Cel przetwarzania	realizacja obowiązków prawnych związanych z prowadzeniem dokumentacji placówki medycznej
Kategorie osób	pacjenci, przedstawiciele ustawowi pacjentów, osoby upoważnione
Kategorie danych osobowych	pacjenci: imię, nazwisko, data urodzenia, płeć, adres, PESEL przedstawiciele ustawowi: imię, nazwisko, adres osoby upoważnione: imię, nazwisko, data urodzenia, dane kontaktowe

Kategorie odbiorców	dostawca systemu informatycznego do obsługi przychodni laboratoria diagnostyczne
Przekazanie danych do państwa trzeciego	nie dotyczy
Planowane terminy usunięcia danych	zgodnie z przepisami prawa, w szczególności art. 29 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	Nadawanie upoważnień osobom zatrudnionym, mającym dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Zapewnienie, by osoby nieupoważnione miały dostęp do pomieszczeń Administratora jedynie pod nadzorem osób zatrudnionych u Administratora. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenie wykorzystywanych u Administratora systemów informatycznych i baz danych przed wyciekiem danych. Inne zabezpieczenia, wskazane w treści Polityki bezpieczeństwa i załącznikach do niej.

W jakiej formie prowadzić rejestr?

Rejestr czynności przetwarzania może być prowadzony w formie:

- papierowej
- elektronicznej (np. z wykorzystaniem arkusza kalkulacyjnego MS Excel lub OpenOffice Calc)
- z wykorzystaniem specjalnego oprogramowania.

Forma, w jakiej jest prowadzony rejestr czynności przetwarzania, ma znaczenie drugorzędne. Kluczowa jest jego treść.

Kto prowadzi rejestr?

Tak jak wskazano w RODO, prowadzenie rejestru czynności przetwarzania jest obowiązkiem administratora danych. Kierownictwo placówki może jednak przekazać to zadanie innej osobie (np. księgowemu lub kadrowej).

Prowadzenie rejestru czynności przetwarzania jest jednym z zadań, które wymaga pomocy inspektora ochrony danych.

Rejestr kategorii czynności przetwarzania

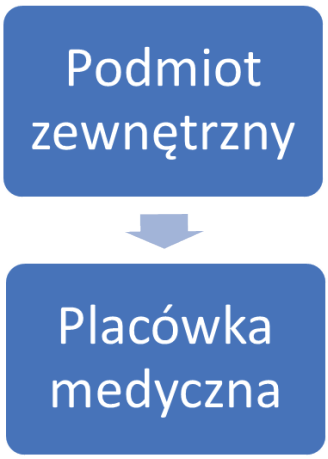
Rejestr kategorii czynności przetwarzania to kolejny z dokumentów, jakie wprost wskazano w RODO.

Każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:
a) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
c) gdy ma to zastosowanie – przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

§

- art. 30 ust. 2 RODO

Dokument ten będzie używany tylko wtedy, gdy placówka medyczna będzie – na podstawie umowy powierzenia – wykorzystywać dane osobowe w imieniu i na rzecz podmiotu zewnętrznego. Takie sytuacje występują w placówkach medycznych stosunkowo rzadko.



Co ma się znaleźć w rejestrze?

W rejestrze kategorii czynności przetwarzania należy przede wszystkim wskazać nazwę i dane kontaktowe podmiotu przetwarzającego – placówki medycznej (np. JAMANOWSKI PRAKTYKA LEKARZA RODZINNEGO (ul. Piekarska 221B, 57-540 Lądek-Zdrój)).

Potem należy wymienić wszystkich administratorów danych, którzy przekazują nam dane osobowe z uwzględnieniem informacji, o których mowa w art. 30 ust. 2 lit. b-d RODO, tj.:

- kategorie przetwarzań – co robimy z danymi osobowymi, które otrzymaliśmy od administratora danych? Pomocne może tu być odniesienie się do umowy powierzenia, gdzie zapisano, jak placówka medyczna może wykorzystywać dane
- przekazanie danych osobowych do państwa trzeciego – tak jak wskazywaliśmy przy rejestrze czynności przetwarzania, w zdecydowanej większości przypadków w placówkach medycznych nie dochodzi do przekazywania danych do państw trzecich
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa – analogicznie jak przy rejestrze czynności przetwarzania, wystarczy ogólny opis (może to być w szczególności odwołanie się do środków wymienionych w dokumentacji ochrony danych).

Najprościej prowadzić rejestr kategorii czynności przetwarzania w formie tabeli:

Podmiot przetwarzający			
Inspektor ochrony danych			
	Administrator #1	Administrator #2	Administrator …
Kategorie przetwarzań			

Przekazanie danych do państwa trzeciego			
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa			

W jakiej formie prowadzić rejestr?

Rejestr kategorii czynności przetwarzania, tak jak rejestr czynności przetwarzania, może być prowadzony w formie:

- papierowej
- elektronicznej (np. z wykorzystaniem arkusza kalkulacyjnego MS Excel lub OpenOffice Calc)
- z wykorzystaniem specjalnego oprogramowania.

Forma, w jakiej jest prowadzony rejestr kategorii czynności przetwarzania, ma znaczenie drugorzędne. Kluczowa jest jego treść.

Kto prowadzi rejestr?

Podobnie jak przy rejestrze czynności przetwarzania, prowadzenie rejestru kategorii czynności przetwarzania jest obowiązkiem podmiotu przetwarzającego. Kierownictwo placówki może jednak przekazać to zadanie innej osobie (np. księgowemu lub kadrowej).

Prowadzenie rejestru kategorii czynności przetwarzania jest jednym z zadań, które wymaga pomocy inspektora ochrony danych.

Ewidencja naruszeń ochrony danych osobowych

Ewidencja naruszeń ochrony danych osobowych to jeden z nielicznych, konkretnie wskazanych dokumentów w RODO

> *Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikować przestrzeganie niniejszego artykułu.*
>
> - art. 33 ust. 5 RODO

Co ma się znaleźć w ewidencji naruszeń?

Przy ewidencji nie mamy konkretnie, punkt po punkcie wyliczonych elementów (tak jak przy rejestrze czynności lub kategorii czynności przetwarzania). Jeśli weźmie się jednak pod uwagę cały tekst art. 33 RODO, powstanie lista potrzebnych elementów:

- **krótki opis naruszenia – co się stało?**
- **kiedy stwierdzono naruszenie – kiedy administrator uznał, że zdarzenie jest incydentem bezpieczeństwa w rozumieniu RODO?**
- **kategoria osób poszkodowanych – czyje dane padły ofiarą incydentu?**
- **przybliżona liczba osób, których dane dotyczą – dane ilu osób padły ofiarą incydentu?**
- **kategorie danych związanych z naruszeniem – jakich danych osobowych dotyczyło naruszenie?**

- **możliwe konsekwencje naruszenia** – w jaki sposób osoby, których dane dotyczą, mogą być zagrożone w związku z incydentem bezpieczeństwa?
- **środki dla zaradzenia naruszeniu** – co administrator danych zrobił albo planuje zrobić, by podobne zdarzenie już się nie wydarzyło?
- **środki dla zminimalizowania naruszenia** – co administrator danych może zrobić dla zmniejszenia negatywnych skutków?
- **informacja dla organu nadzorczego** – czy naruszenie było na tyle poważne, że wymagało zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych?
- **informacja dla osób, których dane dotyczą** – czy naruszenie wymagało powiadomienia osób, których dane padły ofiarą incydentu?

Tabela przedstawia wzór ewidencji.

	Incydent #1	Incydent #2	Incydent ...
Krótki opis naruszenia			
Kiedy stwierdzono naruszenie?			
Kategorie osób			
Liczba osób			
Kategorie danych			
Możliwe konsekwencje			
Środki zaradcze			
Środki minimalizujące			
Czy zawiadomiono PUODO?			
Czy zawiadomiono osoby, których dane dotyczą?			

W jakiej formie prowadzić ewidencję naruszeń?

Ewidencja naruszeń może być prowadzona w formie:

- papierowej
- elektronicznej (np. z wykorzystaniem arkusza kalkulacyjnego MS Excel lub OpenOffice Calc)
- z wykorzystaniem specjalnego oprogramowania.

Kto prowadzi ewidencję naruszeń?

Z RODO wynika bezpośrednio, że to administrator danych ma prowadzić ewidencję. Kierownictwo placówki może jednak zlecić to zadanie innej osobie (np. księgowemu lub kadrowej).
W prowadzenie ewidencji należy także angażować inspektora ochrony danych.

Jak udowodnić realizację obowiązków z RODO?

Wspomnianej na wstępie tego rozdziału zasady rozliczalności nie należy wykorzystywać jedynie w stosunku do prowadzenia dokumentacji. Polityka bezpieczeństwa, rejestry i ewidencje są dokumentami wewnętrznymi. Równie

istotna jest natomiast realizacja tych obowiązków wynikających z RODO, które mają charakter „zewnętrzny". Takimi obowiązkami są w szczególności:

- realizacja obowiązku informacyjnego
- zbieranie zgód na wykorzystanie danych osobowych.

Obowiązki informacyjne

Realizacja obowiązku informacyjnego oznacza spełnienie kilku warunków:

1) przygotowanie treści wg kryteriów z RODO
2) przygotowanie procedury realizacji obowiązku informacyjnego
3) realizowanie obowiązku informacyjnego.

Co ma się znaleźć w treści obowiązku informacyjnego? Następujące elementy, wskazane w art. 13 RODO:

- nazwa i dane kontaktowe administratora danych (np. JAMANOWSKI PRAKTYKA LEKARZA RODZINNEGO (ul. Piekarska 221B, 57-540 Lądek-Zdrój))
- dane kontaktowe inspektora ochrony danych (np. iod@jamanowski.pl)
- cel i podstawa prawna przetwarzania danych (np. prowadzenie procesu rekrutacji pracowników zgodnie z przepisami kodeksu pracy; podstawą jest wówczas art. 6 ust. 1 lit. c RODO)
- informacja o odbiorcach danych (np. firma zajmująca się obsługą kadrową placówki medycznej)
- informacje o zamiarze przekazania danych osobowych do państwa trzeciego, gdy ma to zastosowanie (w placówkach medycznych taka sytuacja najczęściej nie ma miejsca)
- okres, przez który dane osobowe będą przechowywane (np. 20 lat na przechowywanie dokumentacji medycznej pacjentów, z wyjątkami wynikającymi z ustawy o prawach pacjenta)
- informacje o prawach wynikających z RODO (takich jak dostęp do danych osobowych, ich sprostowanie, usunięcie itp.)
- informacje o prawie wniesienia skargi do organu nadzorczego (Prezesa Urzędu Ochrony Danych Osobowych)
- informacje, czy podanie danych osobowych jest wymagane i jakie są ewentualne konsekwencje niepodania danych (np. brak możliwości udziału w rekrutacji pracowników)
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 RODO (w placówkach medycznych taka sytuacja najczęściej nie ma miejsca).

W zależności od tego, dla kogo obowiązek informacyjny jest przeznaczony (uczestnika rekrutacji, pracownika, pacjenta itd.) treść będzie się oczywiście nieco różnić – konkretne kryteria są wskazane w art. 13-14 RODO.

Po przygotowaniu treści obowiązku informacyjnego należy ustalić, jak będzie realizowany. Dla celów rozliczalności procedura spełniania obowiązku powinna być utrwalona, np.:

- w formie załącznika do polityki bezpieczeństwa
- pisma kierownictwa placówki medycznej do pracowników
- e-maila inspektora ochrony danych do kierownika placówki medycznej.

Możliwe sposoby realizacji obowiązku informacyjnego opisano w rozdziale X niniejszej publikacji.

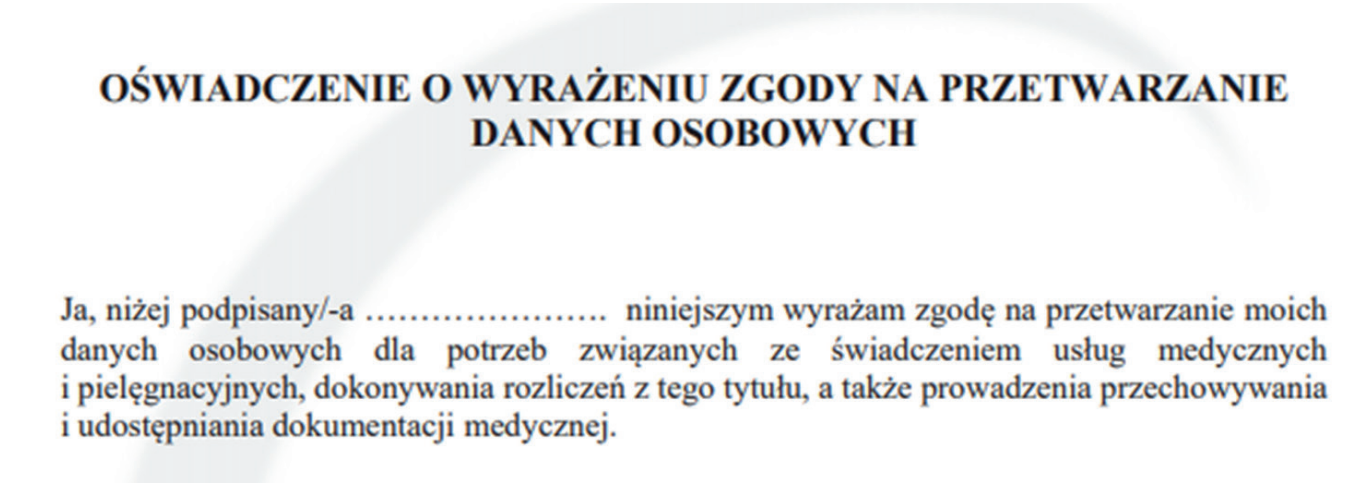
Zgoda na wykorzystanie danych osobowych

Prawidłowe uzyskanie zgody na wykorzystanie danych osobowych wymaga spełnienia kilku wymagań:

1) ustalenia, czy dla wskazanego celu konieczne jest uzyskanie zgody
2) przygotowanie treści zgody wg kryteriów z RODO
3) przygotowanie procedury zbierania zgód
4) zbieranie zgód.

Proces zbierania zgody należy zacząć od ustalenia, czy taka zgoda w ogóle jest potrzebna lub zasadna.

Przez ostatnich kilkanaście lat utarło się w Polsce błędne przekonanie, że każde wykorzystanie danych osobowych musi opierać się na zgodzie. Tymczasem zgoda powinna być wykorzystywana dopiero wtedy, gdy nie ma innej, bardziej zasadnej przesłanki. Taką przesłanką dla placówki medycznej jest przede wszystkim przepis prawa.



OŚWIADCZENIE O WYRAŻENIU ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH

Ja, niżej podpisany/-a ..... niniejszym wyrażam zgodę na przetwarzanie moich danych osobowych dla potrzeb związanych ze świadczeniem usług medycznych i pielęgnacyjnych, dokonywania rozliczeń z tego tytułu, a także prowadzenia przechowywania i udostępniania dokumentacji medycznej.

Przykład zbędnego zbierania zgody na wykorzystanie danych pacjenta w związku ze świadczeniem usług medycznych.

Sytuacją, w której zbieranie zgody przez placówkę medyczną będzie uzasadnione, jest na przykład zbieranie zgody na wykorzystanie wizerunku. Jeżeli placówka medyczna chce umieścić zdjęcia swojego personelu na stronie internetowej, musi mieć na to ich zgodę – nie będzie tu innej przesłanki.

Jakie warunki musi – w świetle RODO – spełniać zgoda?

1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.

2. Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.

3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

4. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

§

- art. 7 RODO

Zgoda musi być zatem:

- dobrowolna (nie można jej na nikim wymuszać)
- konkretna (osoba wie konkretnie, co wiąże się z wyrażeniem przez nią zgody)
- świadoma (osoba wie o tym, że wyraża zgodę)
- jednoznaczna (nie może być wątpliwości co do tego, że zgoda została wyrażona).

W świetle przepisów polskiego prawa forma wyrażenia zgody (ustna, pisemna, elektroniczna) nie ma kluczowego znaczenia. Jednak dla celów dowodowych powinna być utrwalona, np. w formie pisemnego oświadczenia.

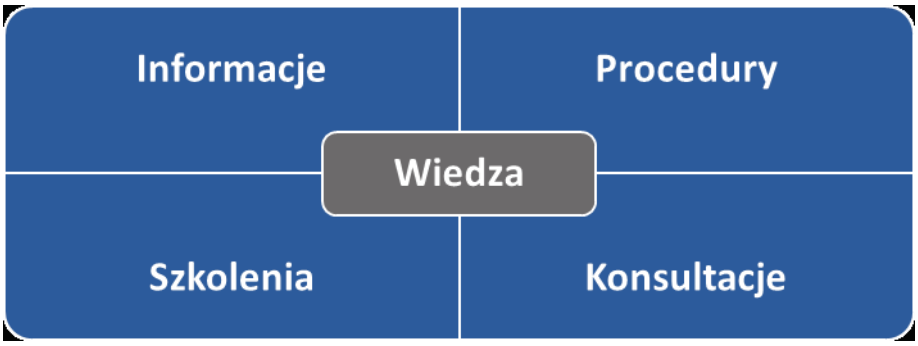
Tak jak przy spełnianiu obowiązku informacyjnego, procedura zbierania zgody na użycie danych osobowych powinna być spisana, np.:

- w formie załącznika do polityki bezpieczeństwa
- pisma kierownictwa placówki medycznej do pracowników
- e-maila inspektora ochrony danych do kierownika placówki medycznej.

Rozdział V. Wiedza oraz świadomość pracowników odnośnie ochrony danych osobowych

Obowiązek zapewnienia pracownikom odpowiedniej wiedzy z zakresu ochrony danych

Budowanie świadomości pracowników jest jednym z najważniejszych, ale też najtrudniejszych wyzwań związanych z zapewnieniem zgodności podmiotu leczniczego z przepisami RODO. To pracownicy dysponują największą wiedzą w zakresie procesów przetwarzania danych. Dlatego tak ważne jest przekazanie pracownikom wszystkich koniecznych informacji oraz ustalenie jasnych i przejrzystych zasad (procedur) postępowania z danymi osobowymi. W budowaniu świadomości pracowników istotne znaczenie ma organizowanie cyklicznych szkoleń mających na celu podniesienie wiedzy pracowników z zakresu ochrony danych osobowych, a także zapewnienie pracownikom możliwości konsultowania wątpliwości w zakresie zgodności z prawem dokonywanych przez nich działań, np. z powołanym w podmiocie leczniczym inspektorem ochrony danych.



Budowanie wiedzy pracownika

Podmiot leczniczy ma obowiązek przekazania wszystkim osobom, których dane przetwarza jako Administrator danych, informacji, w jaki sposób przetwarza ich dane osobowe. Należy tutaj wskazać, że taki obowiązek informacyjny powinien zostać zrealizowany m.in. wobec pracowników podmiotu leczniczego. Wspomniany obowiązek wynika wprost z art. 13 RODO, zgodnie z nim podmiot leczniczy powinien poinformować o tym, że jest administratorem danych oraz podać swoje dane kontaktowe, a także przekazać pozostałe informacje wskazane w treści art. 13 RODO.

Treść obowiązku informacyjnego realizowanego przez podmiot leczniczy została szczegółowo opisana w rozdziale IV niniejszej publikacji.

Poza przekazaniem informacji odnośnie sposobu przetwarzania danych osobowych, które podmiot leczniczy musi przekazać jako administrator danych, bardzo ważne jest podjęcie działań, mających na celu ustalenie jasnych i przejrzystych zasad (procedur) postępowania z danymi osobowymi (zostaną one omówione w dalszej części niniejszego rozdziału), a następnie uświadomienie (poprzez przeprowadzanie szkoleń) pracownikom ich roli w procesie przetwarzania danych osobowych, w toku wykonywania przez nich codziennych czynności służbowych.

RODO nie zawiera literalnie obowiązku przeprowadzania szkoleń pracowniczych zakresu ochrony danych osobowych. Wskazuje jedynie, że ich przeprowadzanie jest zadaniem inspektora ochrony danych (IOD). Należy jednak wskazać, że w praktyce przeprowadzanie szkoleń z zakresu ochrony danych osobowych jest niezbędne dla właściwego funkcjonowania systemu ochronnych danych osobowych w podmiocie leczniczym. Powyższe wynika z faktu, że pracownicy nie są w stanie odpowiednio chronić danych osobowych, jeśli nie wiedzą, czym one są, albo jakie obowiązki spoczywają na nich, jako pracownikach podmiotu leczniczego, będącego administratorem danych.

IOD ma bardzo duże znaczenie w kontekście budowania wiedzy oraz świadomości pracowników w zakresie ochrony danych osobowych, dlatego powinien on być właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Zgodnie z przepisami RODO na inspektorze ochrony danych spoczywają obowiązki wprost odnoszące się do pracowników podmiotu leczniczego, będącego administratorem danych.

Obowiązki IOD względem pracowników:

- informowanie pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisach Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie
- prowadzenie działań zwiększających świadomość
- prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania.

Należy wskazać, że wymiar zadań IOD dotyczący pracowników administratora ma dwojaki charakter, z jednej strony IOD informuje pracowników o prawach im przysługujących, a z drugiej wskazuje na obowiązki i zakres ich odpowiedzialności wobec administratora (podmiotu leczniczego) i osób, których dane dotyczą.

Ponadto, jak wskazuje Europejski Inspektor Danych Osobowych, zapewnienie zgodności z zasadami ochrony danych osobowych zaczyna się przede wszystkim od podniesienia świadomości pracowników, a rola IOD jest w tym zakresie kluczowa. Podnoszenie świadomości pracowników jest przejawem proaktywnego podejścia administratora (podmiotu leczniczego) do ochrony danych oraz środkiem zapobiegającym przyszłym naruszeniom.

Środki mające na celu podniesienie świadomości pracowników:

- publikowanie notatek/komunikatów informacyjnych dla pracowników
- wysyłanie newslettera
- organizowanie szkoleń dla pracowników w zakresie ochrony danych.

Inspektor ochrony danych planując swoje zadania powinien uwzględnić w planie szkoleń:

- szkolenia dla nowych pracowników
- szkolenia dla dotychczasowych pracowników
- szkolenia dodatkowe, np. na skutek złamania zasad ochrony danych osobowych obowiązujących u administratora
- szkolenia dedykowane pracownikom określonego działu
- szkolenia osób z zespołu IOD
- szkolenia podnoszące kwalifikacje IOD.

Drugim podstawowym zadaniem inspektora ochrony danych jest stanowienie punktu kontaktowego dla osób, których dane dotyczą. W razie jakichkolwiek pytań czy wątpliwości, administrator (podmiot leczniczy) i jego pracownicy powinni mieć możliwość łatwego kontaktu z IOD w celu skonsultowania z nim wszelkich zagadnień związanych

z ochroną danych osobowych. Administrator powinien zadbać o właściwie zakomunikowanie roli IOD w podmiocie leczniczym oraz poinformować w sposób przyjęty w organizacji, jak można skontaktować się z inspektorem.

Przykład:
U administratora funkcjonuje wewnętrzna platforma dla pracowników, na której umieszczane są wszystkie informacje dotyczące pracowników, wydarzeń ogólnofirmowych czy zmian organizacyjnych. Administrator umieścił tam dane inspektora ochrony danych oraz krótko opisał zakres jego zadań i spraw, z którymi można się do niego zwracać.

W przypadku większych podmiotów leczniczych możliwe jest również delegowanie części zadań IOD na członków jego zespołu. Takie rozwiązanie powinno być stosowane zwłaszcza wtedy, gdy skala działania podmiotu wskazuje, że samodzielne wykonywanie zadań przez IOD mogłoby być utrudnione lub wręcz niemożliwe.

Procedury z zakresu ochrony danych osobowych

Jak zostało wskazane wcześniej, wiedzę i kompetencje pracowników odnośnie ochrony danych osobowych możemy budować poprzez wdrożenie i stosowanie w podmiocie leczniczym odpowiednich procedur. **Wspomniane procedury powinny być napisane w jasny i przejrzysty sposób, ze wskazaniem prawidłowego sposobu postępowania z danymi osobowymi.**

Procedury obowiązujące w podmiocie leczniczym powinny regulować:

- nadawanie i odwoływanie upoważnień do przetwarzania danych osobowych

Procedura nadawania upoważnień do przetwarzania danych osobowych została szerzej opisana w rozdziale I niniejszej publikacji.

- przeprowadzanie analizy ryzyka oraz oceny skutków dla ochrony danych osobowych

Procedura dokonywania analizy ryzyka została szerzej opisana w rozdziale I niniejszej publikacji.

- pozyskiwanie danych osobowych oraz realizacji obowiązków informacyjnych

Procedura realizacji obowiązków informacyjnych została szerzej opisana w rozdziale X niniejszej publikacji.

- dołączanie do dokumentacji prowadzonej w formie elektronicznej dokumentów utworzonych w postaci papierowej

W wypadku dołączania do dokumentacji prowadzonej w formie elektronicznej dokumentów utworzonych w postaci papierowej należy stworzyć procedurę, która krok po kroku opisywałaby, w jaki sposób – z zachowaniem wiarygodności danych – powinny być wprowadzane.
Powyższa procedura powinna wskazywać osobę odpowiedzialną za wykonanie czytelnego odwzorowania cyfrowego dokumentacji papierowej i zdjęć radiologicznych oraz umieszczenie go w systemie informatycznym. Ponadto system powinien odnotowywać datę wprowadzenia dokumentu oraz dane osoby, która wprowadziła materiał do systemu. Dodatkowo administrator musi wybrać odpowiedni sposób digitalizacji dokumentacji medycznej, który zapewni dostęp i spójność posiadanej przez niego dokumentacji.
Omawiana procedura powinna także opisywać, co zrobić z oryginałem dokumentu, utworzonym w wersji papierowej po wprowadzeniu jego odwzorowania do systemu informatycznego, uwzględniając przy tym ust. 2 §81 Rozporządzenia Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania, który wyraźnie wskazuje, że dołączenie do dokumentacji elektronicznej dokumentów utworzonych w innej postaci powinno być dokonane przez osobę upoważnioną przez podmiot leczniczy w sposób zapewniający czytelność, dostęp i spójność dokumentacji. Po wykonaniu digitalizacji danych oryginał powinien być wydany pacjentowi lub trwale zniszczony, w sposób uniemożliwiający identyfikację pacjenta. Zdigitalizowany dokument nadal jest ważnym nośnikiem informacji w rozumieniu Kodeksu cywilnego, dlatego nie ma potrzeby przetrzymywania papierowej wersji dokumentu.

- weryfikację tożsamości pacjenta

Procedura weryfikacji tożsamości pacjenta została szerzej opisana w rozdziale VIII niniejszej publikacji.

- udostępnianie dokumentacji medycznej

Procedura udostępniania dokumentacji medycznej została szerzej opisana w rozdziale VI niniejszej publikacji.

- realizację praw podmiotu danych (pacjenta)

Procedura realizacji praw podmiotu danych została szerzej opisana w rozdziale VII niniejszej publikacji.

- reagowanie na incydenty z zakresu ochrony danych osobowych

Procedura reagowania na incydenty z zakresu ochrony danych osobowych została szerzej opisana w rozdziale X niniejszej publikacji.

- okresy przechowywania dokumentacji w formie elektronicznej oraz papierowej

Procedura (instrukcja) zawierająca okresy przechowywania dokumentacji medycznej powinna uwzględniać wszystkie rodzaje dokumentów, zawierające dane osobowe, które są przechowywane przez podmiot leczniczy.
Ponadto dokument zawierający okresy przechowywania dokumentacji medycznej może być częścią lub załącznikiem procedury niszczenia dokumentów.

- archiwizacji dokumentacji medycznej

Procedura archiwizacji dokumentacji medycznej została szerzej opisana w rozdziale XI niniejszej publikacji.

- niszczenie dokumentacji medycznej.

Procedura niszczenia dokumentacji medycznej została szerzej opisana w rozdziale XI niniejszej publikacji.

Opracowanie i wdrożenie w podmiocie leczniczym procedur z zakresu ochrony danych osobowych stanowi element realizacji zasady rozliczalności, która wymaga od administratora danych, aby był w stanie wykazać, w jaki sposób chroni dane osobowe oraz wypełnia zasady i obowiązki wskazane w RODO.

Powyższe stanowisko zostało potwierdzone przez Grupę Roboczą Art. 29, która w swojej opinii[8] wskazała, że zasada rozliczalności oznacza:

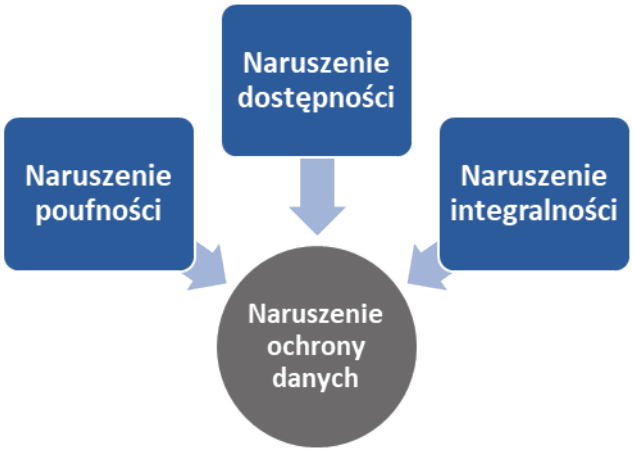
- wdrożenie środków (w tym wewnętrznych procedur) gwarantujących przestrzeganie przepisów o ochronie danych w związku z operacjami ich przetwarzania
- sporządzenie dokumentacji, która wskazuje osobom, których dane dotyczą, oraz organom nadzorczym, jakie środki podjęto, aby zapewnić przestrzeganie przepisów o ochronie danych osobowych.

[8] Opinia 3/2010 w sprawie zasady rozliczalności (WP 173), s. 9.

Naruszenia ochrony danych osobowych

Naruszenie ochrony danych osobowych to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem:

- zniszczenia
- utracenia
- zmodyfikowania
- nieuprawnionego ujawnienia
- nieuprawnionego dostępu danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez administratora danych, którym może być podmiot leczniczy.



Rodzaje naruszeń ochrony danych

Rodzaje naruszeń ochrony danych osobowych:

- naruszenie poufności – niedozwolone lub przypadkowe ujawnienie lub udostępnienie danych osobowych, np.:
  - wydanie dokumentacji medycznej osobie nieupoważnionej przez pacjenta
  - wyciek bazy danych pacjentów podmiotu leczniczego do internetu.
- naruszenie dostępności – niedozwolona lub przypadkowa utrata dostępu do danych osobowych lub zniszczenie ich, np.:
  - zgubienie pendrive'a ze zdjęciami medycznymi pacjenta
  - zablokowanie dostępu lekarza do bazy danych pacjentów w wyniku ataku ransomware na komputer tego lekarza.
- naruszenie integralności – niedozwolona lub przypadkowa zmiana danych osobowych, np.:
  - zmiana nazwiska osoby fizycznej w systemie elektronicznej dokumentacji medycznej
  - zmiana danych w systemie rezerwacji na wizytę i wykonanie niewłaściwego badania/zabiegu pacjentowi.

Fundamentem systemu ochrony danych osobowych w podmiocie leczniczym jest to, że każda osoba zatrudniona w podmiocie leczniczym jest odpowiedzialna za bezpieczeństwo danych osobowych. Dlatego pracownik, który podejrzewa lub stwierdza zdarzenie mogące doprowadzić do naruszenia bezpieczeństwa danych osobowych, zobowiązany jest do natychmiastowego poinformowania o tym odpowiedniej osoby (inspektora ochrony danych oraz swojego przełożonego).

Sposób przekazywania informacji o incydencie z zakresu ochrony danych osobowych powinien zostać ściśle uregulowany przez podmiot leczniczy w obowiązujących u niego procedurach. Powyższa kwestia ma bardzo duże znaczenie dla podmiotu leczniczego, jako administratora danych, ponieważ zgodnie z poniżej przytoczonym przepisem RODO, ma on jedynie 72 godziny na formalne zgłoszenie naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych (PUODO), który jest polskim organem nadzorczym w zakresie ochrony danych osobowych.

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

§

- art. 33 ust. 1 RODO

Dla podmiotu leczniczego, jako administratora danych osobowych, w przypadku wystąpienia naruszenia ochrony danych osobowych, bardzo ważne jest urzędowe zawiadomienie o zaistnieniu takiego naruszenia, w ciągu 72 godzin od stwierdzenia takiego naruszenia. Bardzo ważne jest to, że wspomniane 72 godziny nie zaczynają się dopiero w momencie, kiedy to właściciel podmiotu leczniczego lub powołany przez niego inspektor ochrony danych otrzyma informację o naruszeniu. Powyższe wynika z faktu, że wspomniane 72 godziny zaczynają się od momentu, kiedy to podmiot leczniczy (administrator danych) lub jeden z jego pracowników pozyska informację, która będzie wskazywała z dużym prawdopodobieństwem, że doszło do naruszenia ochrony danych osobowych w podmiocie leczniczym.

Przykład:
W podmiocie leczniczym nie obowiązuje procedura reagowania na incydenty z zakresu ochrony danych osobowych. Pacjent **o godzinie 10:00 w piątek** wysłał do podmiotu leczniczego mail z informacją, że przesłano do niego pocztą kopię dokumentacji medycznej innego pacjenta. Pracownik podmiotu leczniczego odczytał mail **o godzinie 12:00 w piątek**. Ze względu na nadmiar obowiązków pracownik zapomniał poinformować o otrzymanej wiadomości przełożonego oraz inspektora ochrony danych powołanego w podmiocie leczniczym. O mailu otrzymanym od pacjenta przypomniał sobie w poniedziałek z rana i w związku z tym przekazał informację o nim swojemu przełożonemu **o godzinie 8:00 w poniedziałek**. Wspomniany pracownik zapomniał jednak poinformować inspektora ochrony danych, który został powołany w podmiocie leczniczym. Inspektor ochrony danych został poinformowany o błędnym przesłaniu kopii dokumentacji medycznej dopiero przez właściciela podmiotu leczniczego **o godzinie 9:00 w poniedziałek**. W powyższej sytuacji pracownik podmiotu leczniczego pozyskał pewną informację o naruszeniu ochrony danych **o godzinie 12:00 w piątek** i to od tego momentu biegną 72 godziny. Dlatego podmiot leczniczy ma czas na zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego (PUODO) **do godziny 12:00 w poniedziałek**.

Powyższy przykład jasno pokazuje, jak ważne jest opracowanie i wdrożenie procedury reagowania na incydenty (naruszenia) z zakresu ochrony danych osobowych. W przedstawionej sytuacji pracownik podmiotu leczniczego nie miał jasnych wytycznych odnośnie sposobu postępowania w razie otrzymania informacji o naruszeniu ochrony danych osobowych, dlatego zbagatelizował otrzymany mail i nie przekazał odpowiednim osobom informacji o naruszeniu. Dodatkowo później przekazał informację o naruszeniu jedynie swojemu przełożonemu, w wyniku czego inspektor ochrony danych został poinformowany o wystąpieniu naruszenia ochrony danych z kolejnym opóźnieniem. W analizowanym przypadku administrator (podmiot leczniczy) i powołany przez niego inspektor ochrony danych mieli jedynie 3 godziny na przygotowanie formalnego zawiadomienia o naruszeniu ochrony danych, które należy przesłać do organu nadzorczego.

Działania, jakie powinien podjąć podmiot leczniczy w przypadku wystąpienia naruszenia ochrony danych szerzej opisano w rozdziale X niniejszej publikacji.

Polskie sądy i organy publiczne wobec naruszeń ochrony danych osobowych

Kwestie związane z przetwarzaniem danych osobowych przez podmioty lecznicze od wielu lat pozostają w sferze zainteresowania polskich sądów, urzędów oraz organów publicznych. Wspomniane podmioty wielokrotnie wskazywały na nieprawidłowości w przechowywaniu i przetwarzaniu dokumentacji medycznej przez podmioty lecznicze. Sposób przetwarzania przez podmioty lecznicze danych osobowych oraz wdrożenie przez te podmioty regulacji z zakresu ochrony danych osobowych były ostatnimi czasy przedmiotem kontroli przeprowadzonej przez Najwyższą Izbę Kontroli (NIK). Wspomniane kontrole objęły 24 podmioty lecznicze z sześciu województw i trwały od 25 maja 2018 r. do 23 kwietnia 2019 r.

W ramach Informacji o wynikach kontroli[9] NIK zwrócił uwagę na poniższe nieprawidłowości:

- niestosowanie odpowiednich środków organizacyjnych i technicznych
- niezamieszczenie na stronach internetowych podmiotów leczniczych danych IOD oraz sposobu i formy kontaktu z nim
- nieprzeprowadzenie analizy ryzyka dla procesów związanych z przetwarzaniem i ochroną danych osobowych
- nieprzeprowadzenie oceny skutków dla ochrony danych
- nieaktualizowanie dokumentacji (procedur) z zakresu ochrony danych osobowych
- nierzetelne prowadzenie rejestrów czynności przetwarzania
- brak odpowiednich umów powierzenia w sytuacji przekazywania do danych osobowych do podmiotów trzecich w ramach powierzenia
- nierealizowanie obowiązku informacyjnego podmiotu leczniczego wobec pacjentów,
- nieprzeprowadzanie szkoleń pracowniczych z zakresu ochrony danych osobowych
- brakrozwiązań gwarantujących pacjentom prywatność w procesie rejestracji
- umieszczanie nadmiarowych danych (imię i nazwisko, numer PESEL) na opaskach identyfikacyjnych i kartach przyłóżkowych
- błędy w sposobie przechowywania dokumentacji medycznej pacjentów
- zbyt szerokie uprawnienia dostępowe pracowników podmiotów leczniczych
- nieposiadanie odpowiednich upoważnień do przetwarzania danych osobowych przez pracowników podmiotu leczniczego, którzy w ramach swoich obowiązków przetwarzali dane osobowe
- nadawanie upoważnień do przetwarzania danych osobowych pracownikom podmiotu leczniczego, którzy w ramach swoich obowiązków nie przetwarzają danych osobowych,
- nieodbieranie byłym pracownikom uprawnień w systemach informatycznych wykorzystywanych przez podmiot leczniczy
- błędy w sposobie udostępniania dokumentacji medycznej
- niewłaściwe zabezpieczenie danych osobowych przetwarzanych w formie elektronicznej
- posiadanie przez pracowników podmiotów leczniczych nieodpowiednich (zbyt szerokich) uprawnień w systemach operacyjnych
- brak ochrony antywirusowej na komputerach wykorzystywanych przez podmioty lecznicz,
- wykorzystywanie systemów operacyjnych nieposiadających wsparcia producenta
- niewłaściwe zabezpieczenie serwerowni
- niewłaściwe przechowywanie kopii bezpieczeństwa.

[9] Informacje o wynikach kontroli, zob. *Wdrożenie przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych, NIK, Warszawa 2019.*

Na podstawie przeprowadzonych kontroli NIK zalecił kierownikom podmiotów leczniczych:

- analizowanie ryzyka dotyczącego ochrony danych osobowych, uwzględniającego aktualny stan wiedzy technicznej, a następnie stosowanie rozwiązań adekwatnych do ustalonych zagrożeń
- nadawanie pracownikom upoważnień do przetwarzania danych osobowych oraz uprawnień w systemach informatycznych w stopniu adekwatnym do realizowanych przez nich zadań
- przeprowadzanie regularnych szkoleń osób uczestniczących w procesach przetwarzania informacji, ze szczególnym uwzględnieniem zagrożeń bezpieczeństwa informacji, skutków naruszenia zasad bezpieczeństwa informacji, odpowiedzialności prawnej oraz stosowania środków zapewniających bezpieczeństwo informacji
- przechowywanie kopii bezpieczeństwa posiadanych zasobów informacyjnych w innym miejscu niż dane na bieżąco wykorzystywane.

W przedmiocie ochrony danych osobowych oraz przechowywania dokumentacji medycznej pacjentów swoje stanowisko przedstawił też Rzecznik Praw Pacjenta wydając objaśnienia prawne[10]. W ich treści wskazano na problem przechowywania dokumentacji medycznej w nieodpowiednich i nieprzystosowanych do tego pomieszczeniach, takich jak piwnice budynków, w których działają podmioty lecznicze. Rzecznik Praw Pacjenta wskazał na występowanie przypadków zniszczenia dokumentacji medycznej przechowywanej przez podmioty lecznicze na skutek zalania piwnicy, co oczywiście stanowi naruszenie ochrony danych osobowych w zakresie poufności.

„Przechowywanie dokumentacji medycznej w pomieszczeniu z dojściem do maszynowni windy, do obsługi urządzeń wentylacyjnych i do skrzynki alarmowej (...) nie stanowi o zapewnieniu odpowiednich warunków zabezpieczających dokumentację przed zniszczeniem, uszkodzeniem lub utratą i dostępem osób nieupoważnionych. Konieczność konserwacji ww. urządzeń może spowodować, że dostęp do tej dokumentacji medycznej będą miały osoby wykonujące ww. czynności, a więc osoby nieupoważnione. W dodatku dokumentacja ta nadal jest narażona na zniszczenie, utratę lub uszkodzenie."

- wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie[11]

Jak zostało wyżej wskazane problematyka właściwego przechowywania dokumentacji medycznej była też przedmiotem zainteresowania polskich sądów. W przytoczonym fragmencie uzasadnienia wyroku wskazano na problem przechowywania dokumentacji medycznej w miejscach, które dostępne były osobom, które nie były upoważnione do przetwarzania danych osobowych, np. serwisantom wind, czy klimatyzacji, a także pracownikom ochrony. Ponadto sąd zwrócił uwagę, że w przypadku przechowywania dokumentacji medycznej w pomieszczeniach wskazanych powyżej istnieje duże ryzyko jej zniszczenia.

[10] Objaśnienia prawne z dnia 20.02.2019 r. wydane przez Rzecznika Praw Pacjenta, zob. *Udostępnianie, prowadzenie i przechowywanie dokumentacji medycznej – zagadnienia praktyczne, Warszawa 2019.*

[11] Wyrok WSA w Warszawie z dnia 10.05.2017 r., VII SA/Wa 361/17.

„Odbierając część historii choroby (...) zdawał sobie sprawę, że 3 kartony, które zabrał, nie zawierają całej dokumentacji medycznej jego pacjentów – prowadził przecież działalność leczniczą 7 lat (...) w dwóch lokalizacjach. Miał więc świadomość, że w lokalu znajdującym się w (...) pozostawia część dokumentacji medycznej swoich pacjentów. Dodatkowo miał świadomość, że jego działanie spowoduje brak możliwości dostępu do części dokumentacji medycznej pacjentów jego przychodni oraz że nie będzie miał możliwości jej zabezpieczenia a dostęp do niej będą mogły mieć osoby nieupoważnione. Brak odebrania całej dokumentacji, brak informacji, gdzie przedmiotowa dokumentacja się znajduje oraz w jaki sposób można uzyskać do niej dostęp, spowodował niemożność realizacji przez pacjentów ich prawa do dokumentacji medycznej."
- wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie [12]

W przytoczonym powyżej fragmencie uzasadnienia wyroku wskazano na bardzo ważny aspekt, a mianowicie, że obowiązek przechowywania i zabezpieczenia dokumentacji medycznej pacjentów nie kończy się w momencie zaprzestania prowadzenia działalności leczniczej. Dlatego właściciel podmiotu leczniczego kończąc działalność leczniczą powinien zadbać o dalsze przechowywanie i zabezpieczenie dokumentacji medycznej przez okresy wskazane przepisami prawa.

Działania, jakie powinien podjąć podmiot leczniczy w przypadku zaprzestania przez niego działalności szczegółowo opisano w rozdziale X niniejszej publikacji.

Należy wskazać, że w przedmiocie przetwarzania danych przez podmioty lecznicze swoje stanowisko przedstawił także Generalny Inspektor Ochrony Danych Osobowych (GIODO, czyli poprzednik obecnego organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych). Przedmiotem zainteresowania GIODO była sprawa[13], w której skarżąca zarzuciła podmiotowi leczniczemu nieuprawnione udostępnienie jej danych osobowych i danych osobowych jej małoletniej córki utrwalonych w dokumentacji medycznej osobom nieuprawnionym – na potrzeby sporządzenia przez lekarzy opinii dotyczących opieki okołoporodowej skarżącej i jej córki, dla celów związanych z prowadzonym postępowaniem sądowym z powództwa skarżącej przeciwko podmiotowi leczniczemu o odszkodowanie i zadośćuczynienie.

W przytoczonej sprawie skarżąca zwróciła uwagę, że wspomniane udostępnienie danych nastąpiło na rzecz osób nie będących biegłymi sądowymi (określonych przez nią mianem „prywatnych ekspertów"). Ponadto w skardze zaakcentowano, że w celu uzyskania opinii ww. lekarzy na temat opieki okołoporodowej skarżącej i jej córki oraz ewentualnego jej wpływu na obecny stan zdrowia tej ostatniej, zbędne było ujawnienie informacji identyfikujących skarżącą i jej córkę, gdyż w ocenie skarżącej wystarczające byłoby przekazanie zanonimizowanej informacji medycznej. Ponadto w skardze zarzucono również, że na skutek kwestionowanego udostępnienia danych osobowych doszło do naruszenia art. 26 ustawy o prawach pacjenta[14]. Należy tutaj wskazać, że powołany przepis przewiduje zamknięty katalog podmiotów, na rzecz których podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną pacjenta – natomiast w ocenie skarżącej osoby, którym udostępniono kwestionowane dane nie były uwzględnione we wspomnianym katalogu.

[12] Wyrok WSA w Warszawie z dnia 10.05.2017 r., VII SA/Wa 361/17.
[13] Decyzja GIODO z dnia 21.05.2013 r., DOLiS/DEC-564/13.
[14] Ustawa z dnia 6.11.2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2019 r. poz. 1127 ze zm.).

W analizowanej sprawie GIODO nie przyznał racji skarżącej wskazując, że złożyła ona do akt sprawy szereg dokumentów, w tym kopie dokumentacji medycznej dotyczącej jej i jej córki. W konsekwencji podmiot leczniczy uzyskał dostęp do rzeczonych danych i prawo ich dalszego przetwarzania już nie jako podmiot udzielający świadczeń medycznych i w celach związanych z udzielaniem tych świadczeń, lecz jako strona przedstawionego postępowania sądowego, w celach związanych z jego przebiegiem. Należy tutaj wskazać, że pozyskanie przez podmiot leczniczy z akt sprawy sądowej kwestionowanych danych osobowych skarżącej i jej córki zostało zrealizowane na warunkach określonych w obowiązującym w tamtym czasie art. 27 ust. 2 pkt 2 ustawy o ochronie danych osobowych[15]. Przytoczony przepis zezwalał na takie pozyskanie danych, bowiem przepisy Kodeksu postępowania cywilnego stwarzają gwarancje właściwej ochrony danych przetwarzanych, w ramach postępowania regulowanego tymi przepisami.

[15] Ustawy z dnia 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 1997 Nr 133, poz. 883 ze zm.).

Rozdział VI. Konieczność ochrony prawnej placówek medycznych, zgodność z prawem regulacji wewnętrznych, wzorów dokumentów i formularzy, konieczność oceny prawnej projektów umów

Aspekty prawa ochrony danych w regulaminie organizacyjnym placówki medycznej

W dniu 1 lipca 2011 roku obowiązującą przez blisko dwie dekady ustawę o zakładach opieki zdrowotnej[16] zastąpiła ustawa z dnia 15 kwietnia 2011 roku o działalności leczniczej[17]. Jednym z nowych rozwiązań wprowadzonych w nowym akcie prawnym było zastąpienie dotychczasowych regulaminów porządkowych przez zupełnie nowe regulacje wewnętrzne – regulaminy organizacyjne. Podmioty wykonujące działalność leczniczą miały czas na dostosowanie się do nowych regulacji do 31 grudnia 2012 roku. Po upływie wyznaczonego terminu posiadanie regulaminu organizacyjnego jest obowiązkowe dla wszystkich podmiotów z wyjątkiem:

1) lekarzy lub lekarzy dentystów wykonujących indywidualną praktykę lekarską lub indywidualną specjalistyczną praktykę lekarską wyłącznie w zakładzie leczniczym na podstawie umowy z podmiotem leczniczym prowadzącym ten zakład
2) pielęgniarek lub położnych wykonujących indywidualną praktykę pielęgniarki lub położnej albo indywidualną specjalistyczną praktykę pielęgniarki lub położnej wyłącznie w zakładzie leczniczym na podstawie umowy z podmiotem leczniczym prowadzącym ten zakład
3) fizjoterapeutów wykonujących indywidualną praktykę fizjoterapeutyczną wyłącznie w zakładzie leczniczym na podstawie umowy z podmiotem leczniczym prowadzącym ten zakład jeżeli nie prowadzą monitoringu pomieszczeń.

Regulamin organizacyjny ma rozstrzygać w sprawach dotyczących sposobu i warunków udzielania świadczeń zdrowotnych przez podmiot wykonujący działalność leczniczą, nieuregulowanych w ustawie o działalności leczniczej lub statucie. Ma charakter aktu wewnętrznego, mimo że część regulacji w nim zawartych dotyczy relacji z pacjentem[18] i stanowi zbior najważniejszych informacji na temat funkcjonowania danego podmiotu. Nie ma potrzeby by w regulaminie przepisywać treści, które znajdziemy w ustawie o działalności leczniczej. Podobnie nie jest rekomendowanym rozwiązaniem wpisywanie do regulaminu organizacyjnego innych treści, które można odnaleźć w powszechnie obowiązujących przepisach prawa, takich jak w szczególności ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta czy ustawa o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. Każda zmiana prawa będzie bowiem powodowała, że zapisy regulaminu staną się nieaktualne i niezbędne będzie wprowadzanie kolejnych zmian.

Regulamin organizacyjny ustala kierownik, czyli w zależności od formy w jakiej jest prowadzona działalność lecznicza może to być osoba uprawniona do kierowania podmiotem i reprezentowania go na zewnątrz (np. dyrektor SP ZOZ-u), ale również zarząd spółki kapitałowej. Regulamin organizacyjny będzie zatem wprowadzany odpowiednio uchwałą lub zarządzeniem.

---

16 Ustawa z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej (Dz.U. 2007 Nr 14 poz. 89 ze zm.).
17 Dz.U. 2018 poz. 2190 ze zm.
18 F. Grzegorczyk (red.), *Ustawa o działalności leczniczej*. Komentarz, Warszawa 2013.

Przepisy mówią o regulaminie organizacyjnym jako wewnętrznej regulacji opisującej to, czego nie znajdziemy w ustawie ani w statucie. Posiadanie statutu jest obowiązkowe w przypadku podmiotów leczniczych niebędących przedsiębiorcami. Statut jest nadawany przez podmiot tworzący, regulamin organizacyjny przez kierownika, z uwzględnieniem wniosków i opinii rady społecznej. Co istotne, regulamin organizacyjny ma uzupełniać a nie korygować statut. Postanowienia regulaminu nie mogą być zatem sprzeczne z ustaleniami ze statutu. Mimo że statut jest obligatoryjny tylko dla podmiotów niebędących przedsiębiorcami, zdarzają się sytuacje, w których akt ten funkcjonuje np. w spółce z ograniczoną odpowiedzialnością. Nie jest to błędem, natomiast należy zadbać, by statut był odpowiednio aktualizowany, a jeżeli występowanie dwóch aktów, tj. statutu i regulaminu organizacyjnego jest problematyczne, można rozważyć uchylenie go i posługiwanie się jedynie regulaminem organizacyjnym.

Spośród wielu informacji, które muszą co do zasady znaleźć się w regulaminie organizacyjnym, z perspektywy ochrony danych osobowych istotna jest analiza kilku obszarów, takich jak:

1) miejsce udzielania świadczeń
2) opis stosowanego monitoringu
3) status prawny IOD w strukturach podmiotu leczniczego i jego zakres zadań
4) sposób przepływu informacji o pacjencie
5) wysokość opłat za udostępnienie dokumentacji medycznej
6) proces udostępniania dokumentacji medycznej
7) identyfikacja personelu.

Jako jedna z pierwszych informacji wymaganych w regulaminie organizacyjnym pojawia się miejsce udzielania świadczeń. To pozornie proste pytanie często przysparza trudności z udzieleniem prawidłowej odpowiedzi. Nie bierze się bowiem pod uwagę, że świadczenia są udzielane nie tylko w przychodni, ale i w miejscu, w którym przebywa pacjent.

Miejsce udzielania świadczeń POZ	**Gabinet lekarza**	**Gabinet zabiegowy**	**Gabinet szczepień**	**Miejsce pobytu pacjenta**	**Transport sanitarny**	**Gabinet pielęgniarki szkolnej**
Personel zaangażowany w proces	lekarz asystent medyczny rejestratorka medyczna	pielęgniarka rejestratorka medyczna	pielęgniarka rejestratorka medyczna	pielęgniarka Położna lekarz kierowca rejestratorka medyczna	kierowca ratownik medyczny rejestratorka medyczna lub osoba przyjmująca zlecenia na transport sanitarny	pielęgniarka szkolna lub higienistka szkolna
Przykładowe kwestie związane z zabezpieczeniem danych	właściwa organizacja przestrzeni w gabinecie uniemożliwiająca zapoznanie się przez pacjenta z danymi innych osób, np. poprzez właściwe ustawienie monitorów czy właściwy interwał zadziałania wygaszacza ekranu			przewożenie dokumentacji medycznej w samochodzie		dostęp do gabinetu osób zatrudnionych w szkole, nieuprawnionych do wglądu w prowadzoną dokumentację medyczną
	zakres uprawnień -rejestratorka nie powinna mieć dostępu do szczegółowych danych z przebiegu leczenia	udzielanie świadczeń kilku pacjentom równolegle	przekazywanie kart uodpornienia – musi odbywać się za pokwitowaniem przez osobę, która kontynuuje realizację obowiązku szczepień, nie zaś np. sekretarkę lub rejestratorkę medyczną	zabezpieczenie sieci internetowej w przypadku korzystania z urządzeń bezprzewodowych podczas wizyty		warunki przechowywania dokumentacji medycznej (w tym adekwatne i skuteczne zabezpieczenia przed dostępem osób nieuprawnionych)

Miejsce udzielania świadczeń POZ	Gabinet lekarza	Gabinet zabiegowy	Gabinet szczepień	Miejsce pobytu pacjenta	Transport sanitarny	Gabinet pielęgniarki szkolnej
	odpowiednie zabezpieczenia fizyczne pomieszczeń z zewnątrz -zarówno te mające na celu zapewnienie pacjentowi prywatności podczas realizacji świadczenia jak i te związane z zabezpieczeniem urządzeń, na których przetwarzane są dane.			przechowywanie dokumentacji medycznej do następnego dnia roboczego, jeżeli nie wraca się do siedziby świadczeniodawcy		brak danych na temat aktualnej deklaracji wyboru w POZ ucznia i wynikające z tego trudności z dotarciem do osoby, której należałoby przekazać zakończoną dokumentację medyczną ucznia
	miejsce asystenta medycznego – gabinet lub rejestracja pod warunkiem zapewnienia w niej odpowiednich warunków poufności danych			ryzyko zagubienia dokumentacji medycznej w domu pacjenta lub jej utraty poprzez zdarzenia losowe, np. kradzież samochodu z pozostawionymi w nim dokumentami		
				przewożenie materiału do badań pobranego w miejscu pobytu pacjenta, w oznakowanych jego danymi opakowaniach/ probówkach		
				nieodnotowany w wykazie udostępnionej dokumentacji medycznej wgląd w dokumentację medyczną		

Na przykładzie powyższej tabeli widoczne staje się zarówno zróżnicowane ryzyko w obszarze naruszeń danych osobowych, jak i konieczność zapewnienia różnych poziomów uprawnień do pracy na danych osobowych, stosownie do różnych czynności wykonywanych na danym stanowisku.

Kwestie dotyczące przestrzeni wykorzystywanej do prowadzenia działalności leczniczej pojawiają się w regulaminie organizacyjnym również w kontekście monitoringu wykorzystywanego do obserwacji pomieszczeń. Kierownik podmiotu, w którym jest wykorzystywany monitoring wizyjny jest zobligowany do określenia w regulaminie organizacyjnym sposobu oraz potrzeby zastosowania środka obserwacji pomieszczeń:

1) ogólnodostępnych, jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pacjentów lub pracowników pomieszczeń
2) w których są udzielane świadczenia zdrowotne oraz pobytu pacjentów, w szczególności pokoi łóżkowych, pomieszczeń higieniczno-sanitarnych, przebieralni, szatni, jeżeli wynika to z przepisów odrębnych.

W praktyce POZ nie występują pokoje łóżkowe, nie ma również przepisów szczególnych usprawiedliwiających montaż monitoringu, np. w gabinetach, w których są udzielane świadczenia. Uregulowania wymaga zatem przede wszystkim kwestia monitoringu obejmującego swoim zasięgiem przestrzeń przy rejestracji czy ciągi komunikacyjne w podmiocie. Należy przy tym zaznaczyć, że o monitoringu możemy mówić, jeżeli obraz jest rejestrowany a nie jedynie służy do obserwacji w czasie rzeczywistym, bez możliwości zapisu. Monitoring ma także spełniać określone wymogi co do charakteru nagrań, mogą one bowiem obejmować jedynie obraz, ale nie dźwięk. Mówimy o monitoringu wizyjnym, który pozwoli np. ustalić przebieg zdarzenia, gdy pacjent straci przytomność na korytarzu, ale nie może zbierać danych w postaci zapisu dźwięku, np. z rozmów pacjentów na korytarzu przed gabinetem. Monitoring ma – jak wskazano w przepisie – służyć bezpieczeństwu, nie może być natomiast wykorzystywany do innych celów, a w szczególności nie może stanowić podstawy oceny pracy personelu.

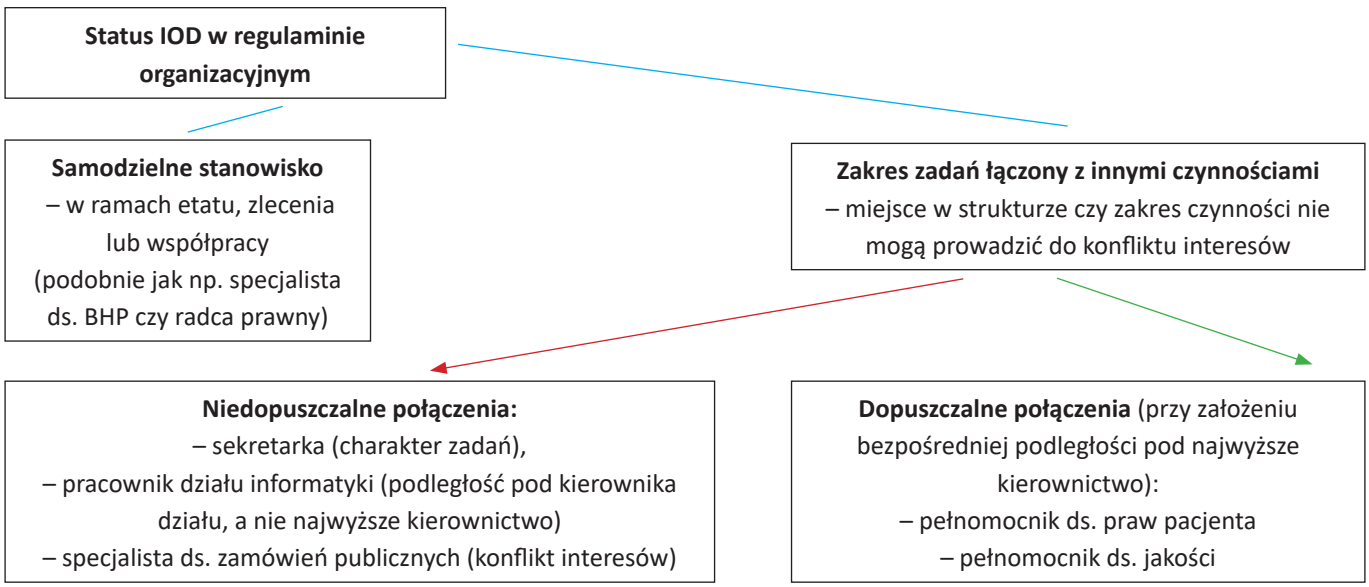
Kamery w podmiocie leczniczym muszą być odpowiednio oznaczone:

1) jeżeli zapisują obraz – należy umieścić informację o monitoringu wizyjnym
2) jeżeli obraz z kamer nie jest zapisywany a służy tylko obserwacji w czasie, np. przez personel ochrony – należy umieścić informację o bieżącym nadzorze kamer bez możliwości zapisu
3) kamera, która uległa czasowej awarii i nie zapisuje obrazu lub ma usterki techniczne musi zostać opatrzona stosowną informacją o czasowej niesprawności.

Jeżeli natomiast kamera w ogóle nie działa a jest tylko atrapą – musi zostać zdemontowana. Stwarza ona złudne poczucie bezpieczeństwa – pacjenci są przekonani, że w razie wypadku czy kradzieży będą mogli ustalić przebieg zdarzenia, podczas gdy zapis obrazu nigdy nie powstał.

Nagrania z monitoringu mogą być przechowywane przez określony czas nieprzekraczający trzech miesięcy. Najczęściej przyjętym rozwiązaniem jest zapisywanie nowych danych w miejsce najstarszych zapisów na nośniku przeznaczonym do utrwalania z monitoringu. W związku z tym warto wprowadzić cykliczną ocenę tego, czy z perspektywy potrzeb podmiotu okres przechowywania obrazu jest wystarczający i czy zapisane dane są prawidłowe i możliwe do odtworzenia. Po upływie okresu przewidzianego w ustawie o działalności leczniczej, dane osobowe podlegają zniszczeniu, o ile przepisy odrębne nie stanowią inaczej.

Regulamin organizacyjny to również dokument zawierający kluczowe informacje na temat struktury wewnętrznej podmiotu leczniczego. Miejsce poświęca się opisowi zarówno komórek organizacyjnych udzielających świadczeń medycznych, jak i strukturom administracyjnym wspierającym ich pracę. W tym miejscu warto zwrócić uwagę na rozstrzygnięcia dotyczące statusu Inspektora Ochrony Danych w podmiocie. Jego miejsce musi być bowiem prawidłowo określone, zarówno na schemacie w formie graficznej czy opisowej, jak i pod względem ewentualnych zadań powierzonych mu dodatkowo, poza sferą obowiązków związanych z zapewnieniem bezpieczeństwa danych osobowych.



Szerzej na temat statusu prawnego IOD w podmiocie leczniczym w rozdziale II.

IOD jest osobą współpracującą w zakresie zabezpieczenia danych w podmiocie leczniczym ze wszystkimi osobami zatrudnionymi w podmiocie leczniczym, zarówno w poszczególnych komórkach organizacyjnych, jak i na samodzielnych stanowiskach. Istotną rolę w procesie zabezpieczenia danych odgrywa również właściwa współpraca pomiędzy realizatorami poszczególnych etapów diagnostyki i leczenia, a także z personelem pomocniczym pracującym na danych, np. w związku z rejestracją pacjenta. Równie ważne są relacje z zewnętrznymi podmiotami, z którymi placówka współdziała na rzecz pacjenta i w związku z tym przekazywane są dane o pacjencie. Informacje dotyczące tego procesu mogą się znaleźć w części przeznaczonej na opisanie:

1) przebiegu procesu udzielania świadczeń zdrowotnych, z zapewnieniem właściwej dostępności i jakości tych świadczeń w jednostkach lub komórkach organizacyjnych zakładu leczniczego;
2) organizacji i zadań poszczególnych jednostek lub komórek organizacyjnych zakładu leczniczego oraz warunków współdziałania tych jednostek lub komórek dla zapewnienia sprawnego i efektywnego funkcjonowania podmiotu pod względem diagnostyczno-leczniczym, pielęgnacyjnym, rehabilitacyjnym i administracyjno-gospodarczym;
3) warunków współdziałania z innymi podmiotami wykonującymi działalność leczniczą w zakresie zapewnienia prawidłowości diagnostyki, leczenia, pielęgnacji i rehabilitacji pacjentów oraz ciągłości przebiegu procesu udzielania świadczeń zdrowotnych.

W związku ze współpracą z podmiotami zewnętrznymi, przekazywane są nierzadko informacje o pacjencie. Przekazywane dokumenty mogą występować w formie wyników badań laboratoryjnych, kopii i wydruków dokumentacji czy też zleceń lub skierowań. Pewne kluczowe kwestie dotyczące tej współpracy mogą być zapisane w regulaminie organizacyjnym. W dokumencie tym pojawić się mogą pewne rozstrzygnięcia dotyczące udostępniania dokumentacji medycznej. Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta nakazuje m.in. rozstrzygnięcie w regulaminie organizacyjnym, czy podmiot będzie udostępniał dokumentację medyczną w formie skanu. Przyjęto, że nie wszystkie podmioty są technicznie gotowe na skanowanie dokumentacji, mogą zatem postanowić, że nie będą wykonywać skanów. Warto natomiast pamiętać, by opisując w regulaminie sposób udostępniania dokumentacji medycznej nie zamieszczać informacji sprzecznych z prawem.

Przykład:

W regulaminie organizacyjnym poradni zapisano, że podmiot nie wykonuje odpisów dokumentacji medycznej. Chodziło o ograniczenie sytuacji, w których personel byłby angażowany w czasochłonne wykonanie odpisu.

Takie rozwiązanie nie jest prawidłowe, w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta wskazano, w jakich formach jest udostępniana dokumentacja medyczna i odpis został wymieniony jako jedna z form. Dowolność w zakresie decyzji, co do formy udostępnienia, pozostawiono podmiotom leczniczym tylko w przedmiocie skanu. Można zdecydować, że skany nie będą wykonywane. W przypadku odpisu takiej możliwości nie ma.

Przykład:

Kierownik przychodni przygotowując regulamin chciał doprecyzować niejasny jego zdaniem zapis o udostępnianiu dokumentacji medycznej „bez zbędnej zwłoki". W regulaminie organizacyjnym zapisano, że dokumentację udostępnia się w terminie 7 dni od daty złożenia wniosku. Rzecznik Praw Pacjenta, do którego złożono skargę wskazał na naruszenie zbiorowych praw pacjenta w przychodni.

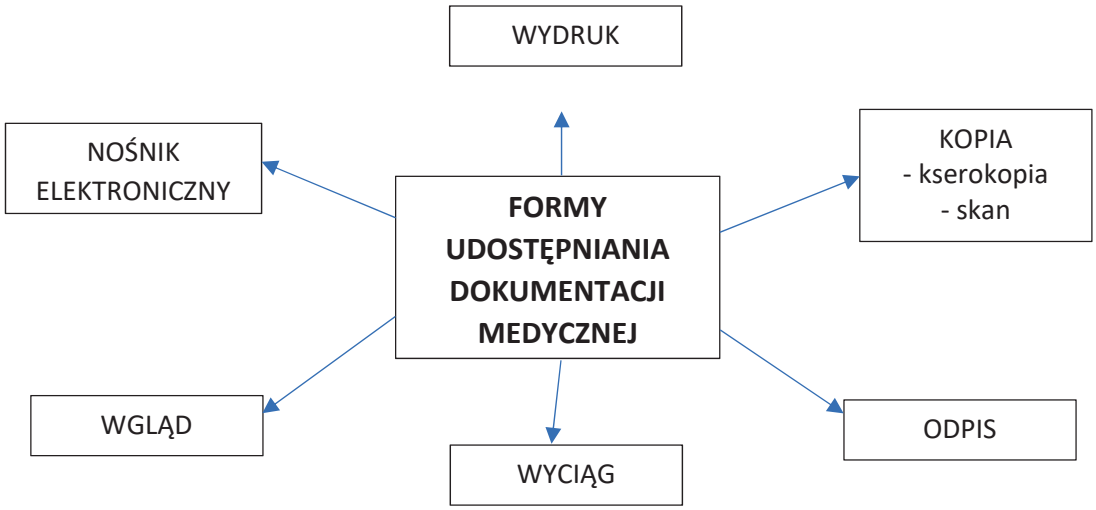
Wskazanie konkretnego terminu udostępniania w tym przypadku można uznać za naruszenie praw pacjentów. Jeżeli pacjent poprosi o jedną stronę kserokopii dokumentacji medycznej znajdującej się na miejscu w rejestracji, 7-dniowy czas oczekiwania uznać należy za nazbyt długi i mogący naruszać interesy pacjenta.

Z drugiej strony zastrzeżenie 7-dniowego terminu może być niekorzystne dla podmiotu. Jeżeli pacjent poprosi o wykonanie odpisu całej historii zdrowia i choroby, termin może okazać się niemożliwy do dotrzymania.

Z procesem udostępniania dokumentacji medycznej wiąże się także kwestia odpłatności. Szczegółowe rozwiązania dotyczące pobierania opłat zostały opisane w rozdziale VIII. Z perspektywy zapisów w regulaminie organizacyjnym, istotne natomiast jest by konkretna, kwotowa wysokość opłat za udostępnienie dokumentacji medycznej została określona bezpośrednio w regulaminie organizacyjnym, a nie poprzez osobne zarządzenie. Zapisy dotyczące opłat za poszczególne formy udostępnienia dokumentacji medycznej mogą znaleźć się zarówno w treści regulaminu, jak i w załączniku do tego dokumentu.

Ogólne zasady udostępniania dokumentacji medycznej

Prowadzenie dokumentacji medycznej ma na celu zobrazowanie przebiegu poszczególnych etapów diagnostyki i leczenia u pacjenta. Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta kładzie jednak szczególny akcent na kwestie dostępu do dokumentacji medycznej. Opisane zostały zatem nie tylko kwestie odpłatności za udostępnienie dokumentacji medycznej, ale i poszczególne formy jej udostępnienia, natomiast szczegóły techniczne dotyczące rozwiązań przyjętych w konkretnym podmiocie opisywane są bezpośrednio w regulaminie organizacyjnym bądź w instrukcjach lub procedurach.



Uprawnionym podmiotom należy zapewnić wgląd do dokumentacji medycznej polegający na możliwości przejrzenia i zapoznania się z treścią wpisów i poszczególnymi załącznikami. Należy zwrócić uwagę na trzy kluczowe problemy techniczne związane z prawidłową realizacją prawa do wglądu do dokumentacji medycznej:

1. wgląd do dokumentacji medycznej musi odbywać się pod nadzorem uprawnionego personelu podmiotu leczniczego;
2. podczas wglądu należy zagwarantować dochowanie prywatności osobie przeglądającej dokumenty;
3. w trakcie przeglądania dokumentacji uprawniona osoba może wykonywać zdjęcia lub sporządzać notatki;
4. wgląd do dokumentacji łącznie z uwagami dotyczącymi zakresu zdjęć wykonanych przez pacjenta musi zostać odnotowany w wykazie udostępnionej dokumentacji medycznej;
5. wgląd jest zawsze bezpłatny.

Przykład:

Pacjent poprosił o wgląd do dokumentacji medycznej. Dokumentację chciał przejrzeć na miejscu, możliwie szybko. W rejestracji został poinformowany, że obecnie rejestruje się dużo pacjentów i nie ma pracownika, który mógłby towarzyszyć mu podczas przeglądania dokumentacji w gabinecie, natomiast dokumentacja może zostać mu pokazana przy okienku rejestracyjnym, tak aby rejestratorka nie musiała opuszczać stanowiska pracy.

Dokumentacja medyczna musi być udostępniona bez zbędnej zwłoki, jednak faktycznie względy organizacyjne mogą przesądzać o tym, że nie będzie to możliwe w chwili zgłoszenia pacjenta. Pacjentowi podczas przeglądania dokumentacji musi towarzyszyć uprawniona do przetwarzania danych osoba, ponieważ istnieje ryzyko, że pacjent będzie chciał w nią ingerować poprzez jej zniszczenie lub zabranie całości lub jej części. Niezbędne jest również odnotowanie, jakie zdjęcia wykonywał pacjent, ponieważ w razie ujawnienia danych z dokumentacji medycznej, podmiot będzie mógł wskazać, że źródłem wycieku danych nie jest działanie personelu placówki a np. samego pacjenta, który upublicznił informacje o swoim stanie zdrowia.

O tym, czy propozycja wglądu do dokumentacji medycznej przy stanowisku rejestracji będzie zapewniała poufność danych decydują kwestie organizacyjno-techniczne. Jeżeli punkty obsługi są odpowiednio wydzielone, tak by pacjenci nie mogli śledzić wzrokowo przebiegu czynności przy sąsiednim stanowisku pracy, ryzyko jest znacznie zmniejszone. Musi być jednak spełniony dodatkowy warunek w postaci odpowiedniego odstępu pomiędzy kolejnymi pacjentami. Należy zdawać sobie sprawę, że przypadkowo może dojść do ujawnienia danych o pacjencie, np. na podstawie zauważonych przez innych pacjentów wyników badań czy dokumentów o charakterystycznym układzie graficznym, jak np. karta diagnostyki i leczenia onkologicznego.

Przykład:

Mama dziecka, które leczy się w poradni specjalistycznej, poprosiła lekarza podczas swojej wizyty o wgląd do dokumentacji medycznej dziecka. Lekarz nie zgodził się, argumentując, że takie sprawy załatwia się w rejestracji a nie podczas wizyty.

Jeżeli sposób realizacji wniosku nie utrudnia dostępu do danych, np. poprzez ograniczone godziny otwarcia rejestracji, wskazanie konkretnej komórki organizacyjnej zajmującej się udostępnianiem dokumentacji medycznej nie będzie błędem. W tym przypadku może być niezbędne zweryfikowanie, czy nie ma w dokumentacji pacjenta żadnej informacji o ograniczeniu możliwości zapoznania się z jej treścią.

Istotne jest natomiast, by zapewnić pacjentowi możliwość wykonywania zdjęć i notatek oraz wpisać dane dotyczące udostępnienia do właściwego wykazu.

Przez wiele lat pojawiały się wątpliwości wokół sposobu przygotowania wyciągu lub odpisu dokumentacji medycznej w odpowiedzi na żądanie ich sporządzenia przez uprawnione podmioty. Ostatecznie w 2017 roku rozstrzygnięto o sposobie przygotowania wyciągu i odpisu, dodając dwie nowe definicje, zgodnie z którymi:

1) odpis to dokument wytworzony przez przepisanie tekstu z oryginału dokumentacji medycznej z wiernym zachowaniem zgodności treści z oryginałem;
2) wyciąg to skrótowy dokument zawierający wybrane informacje lub dane z całej dokumentacji medycznej.

Odpis to zatem nie kserokopia z pieczątką „ODPIS" a dokument, którego wytworzenie będzie wymagało znacznie większego zaangażowania. Oryginalna dokumentacja pacjenta musi zostać przepisana. Wyciąg z kolei będzie zawierał część danych, np. dotyczących leczenia określonego problemu zdrowotnego. Pacjent nie potrzebuje danych z całej dokumentacji a jedynie określonego zakresu, np. dla celów dochodzenia roszczeń po wypadku.

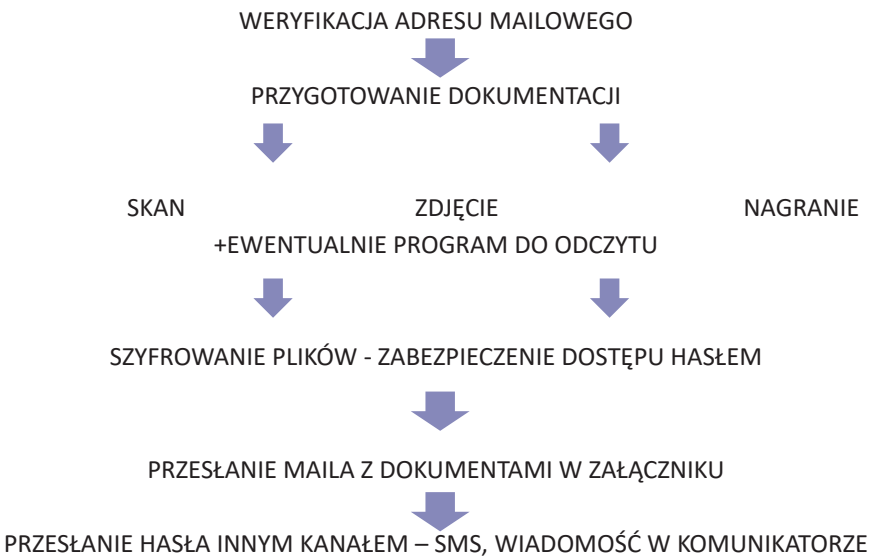
Oczywiście nie ma przeszkód, by zamiast odręcznego przepisywania posiłkować się edytorem tekstu w komputerze. Jeżeli dokumentacja jest prowadzona przy użyciu programu informatycznego można również skorzystać z opcji wydruku. Ważne by odpowiednio poświadczyć, że treść jest zgodna z oryginałem, jak również opisać elementy takie jak widoczne w oryginale załączniki, pieczątki czy podpisy[19]. Nie ma bowiem potrzeby szukać używanych przed laty wzorów pieczątek czy zabiegać

[19] Szerzej na temat zasad sporządzania odpisów: I.M. Aleksandrowicz, *Odpis dokumentacji medycznej, Otwarty System Ochrony Zdrowia nr 6/2019, s. 31-32.*

o podpisy osób, które udzielały świadczeń. W wielu sytuacjach okazałoby się to niemożliwe. Poniżej tabela zawierająca elementy, których nie będziemy mogli zawrzeć w tekście oraz ich przykładowe opisy.

Pieczątka podmiotu lub komórki organizacyjnej	**Pieczątka imienna i podpis osoby udzielającej świadczenia**	**Wyniki badań obrazowych (wydruk z badania USG, zdjęcie RTG)**	**Płyta CD z wynikiem badań**	**Rysunek (np. zaznaczenie zmian reumatoidalnych na schemacie, rysunek obrazujący pole widzenia pacjenta)**	**Podpis pod oświadczeniem pacjenta**
w tym miejscu na oryginale pieczątka o treści……	w tym miejscu na oryginale pieczątka o treści …….. oraz właściwy podpis	w tym miejscu załączono wydruk badania USG	płytę w miarę możliwości należy skopiować i załączyć, podobnie jak ma to miejsce w oryginale dokumentacji medycznej	jeżeli rysunek nie ma podpisu, należy potwierdzić u personelu medycznego właściwe oznaczenie i odpowiednio oznaczyć np.: w tym miejscu w oryginale dokumentacji medycznej zawarto schematyczny rysunek obrazujący pole widzenia pacjenta	w tym miejscu na oryginale oświadczenia znajduje się podpis pacjenta

Wydanie kopii dokumentacji medycznej może nastąpić poprzez wykonanie kserokopii lub jeżeli tak postanowiono w regulaminie organizacyjnym, również skanu. Skany oraz dokumenty wytworzone w systemach informatycznych mogą być przekazywane na nośnikach informatycznych lub za pośrednictwem maila. Nośniki, czyli płyta CD, DVD lub pendrive, powinny być przekazane przez podmiot leczniczy, a nie dostarczone przez wnioskodawcę; dostarczony nośnik mógłby stanowić zagrożenie dla systemu. Poniżej schemat postępowania przy zabezpieczaniu danych wysyłanych mailowo:



Wydanie oryginału dokumentacji medycznej ma być sytuacją o wyjątkowym charakterze, należy bowiem zadbać o to, by znajdowała się ona w zasobach podmiotu leczniczego, jako że jest to niezbędne, by pacjent miał do niej dostęp. Oryginał jest zatem udostępniany tylko z zastrzeżeniem zwrotu po wykorzystaniu, czyli pożyczany, a nie przekazywany na zawsze. Podmiotami uprawnionymi do takiej formy udostępnienia są jedynie organa władzy publicznej oraz sądy powszechne. W trosce o prawidłowy przebieg postępowania dokumentacja ta jest udostępniana również w przypadku gdy zwłoka w wydaniu dokumentacji mogłaby spowodować zagrożenie życia lub zdrowia pacjenta.

Umowy powierzenia – zgodność ze standardami RODO

Narzędziami, które zapewniają bezpieczeństwo prawne podmiotu są nie tylko rozstrzygnięcia zawarte w regulaminie organizacyjnym i w instrukcjach, bądź procedurach nadających praktyczny wymiar udostępnianiu dokumentacji medycznej w podmiocie leczniczym. Równie istotne dla bezpieczeństwa danych są opisane w odpowiednich umowach relacje z podmiotami zewnętrznymi. Czynniki otoczenia zewnętrznego mają bowiem bardzo duży wpływ na prawidłowe funkcjonowanie podmiotu wykonującego działalność leczniczą.

Szczegółowo kwestie związane z zawieraniem umów powierzenia zostały opisane w rozdziale IX.

Administracyjne kary pieniężne za naruszenie przepisów prawa

Z perspektywy podmiotu leczniczego zapewnienie bezpieczeństwa prawnego na poziomie wewnętrznych regulacji i umów z kontrahentami jest kluczowe dla przestrzegania zasady rozliczalności. Jeżeli podmiot nie będzie w stanie wykazać należytej staranności w postępowaniu w tej materii naraża się na ryzyko nałożenia na niego kary administracyjnej.

Wprowadzenie kar administracyjnych stanowiło największą zmianę w podejściu do ochrony danych osobowych wynikającą z wprowadzenia RODO. W obowiązującej wcześniej ustawie o ochronie danych osobowych system sankcji oparty był na przepisach określających czyny karalne[20]. Nowe przepisy wprowadziły możliwość nakładania kar pieniężnych, zasadniczo jednolitych na terenie wszystkich krajów, w których obowiązuje RODO. Maksymalna wysokość kary może sięgać nawet 20 mln euro, bądź 4% obrotu, przy czym to czy nałożona zostanie kara kwotowa, czy obliczana procentowo od wartości obrotu, zależy od oceny, która z przyjętych wartości jest wyższa. Taka perspektywa ma skłonić, zwłaszcza największe korporacje, do zwrócenia szczególnej uwagi na problematykę ochrony danych osobowych.

Każdy przypadek, w którym organ nadzorczy podejmie decyzję o zastosowaniu kary administracyjnej, musi być rozpatrywany indywidualnie, z uwzględnieniem m.in. charakteru naruszenia, rodzaju ujawnionych danych, liczby osób, których dotyczy naruszenie, okoliczności ujawnienia informacji o naruszeniu i powiadomienia organu nadzorczego, ale również stopień współpracy z organem nadzorczym. Nakładane kary mają przede wszystkim być skuteczne, proporcjonalne i odstraszające.

Dotychczasowa praktyka nakładania kar na podmioty ochrony zdrowia przez organy nadzorcze w krajach Unii Europejskiej pokazuje że w tym obszarze nie można liczyć na pobłażliwość. Biorąc pod uwagę zakres danych i ewentualne następstwa, należy liczyć się z dotkliwymi karami finansowymi, które mogą być nałożone zarówno na duże szpitale, jak i niewielkie podmioty ambulatoryjne.

---

[20] D. Lubasz, *RODO. Zmiany w zakresie ochrony danych osobowych. Porównanie przepisów. Praktyczne uwagi, Warszawa 2018, s.113.*

Kraj, w którym nałożono karę	Wysokość kary	Ukarany podmiot	Istota naruszenia	Możliwości przeciwdziałania
Portugalia	€150.000 – za niewłaściwe uregulowanie dostępu do danych pacjentów €150.000 – za niewłaściwe nadawanie uprawnień w systemie €100.000 – za błędy w systemie IT Łącznie €400.000 za naruszenie przepisów RODO	szpital Centro Hospitalar Barreiro Montijo	Brak kontroli nad nadawanymi uprawnieniami do pracy w systemie: niewłaściwe uregulowanie dostępu do danych pacjentów - 296 lekarzy udzielało świadczeń, a w systemie funkcjonowało 985 kont niewłaściwe nadawanie uprawnień w systemie -wszyscy lekarze mieli dostęp do danych wszystkich pacjentów błędy w systemie IT -dane bieżące nie zostały oddzielone od archiwalnych, mechanizmy uwierzytelnienia były nieskuteczne.	różnicowanie poziomów dostępu dla różnych członków personelu, np. rejestratorka, pielęgniarka, lekarz blokowanie dostępu osobom, z którymi zakończono współpracę - np. blokada w przypadku braku aktywności konta przez 30 dni sprawdzanie prawidłowości danych w systemie
Holandia	€460.000	szpital w Hadze (Haga Ziekenhuis)	Holenderska celebrytka Samantha de Jong trafiła do szpitala po przedawkowaniu narkotyków. Tego samego roku podjęła na terenie placówki próbę samobójczą. Po tym zdarzeniu wielu pracowników szpitala (w żaden sposób niezaangażowanych w leczenie), zapoznało się z dokumentacją medyczną pacjentki. Według ustaleń holenderskiego organu nadzorczego z dokumentami zapoznało się aż 85 osób. Okazało się również, że dane innych pacjentów (szpital przyjmuje ich rocznie ok. 250.000) również są w łatwy sposób dostępne dla osób nieuprawnionych.	dostęp personelu do danych tylko tych pacjentów, którymi się zajmuje sprawdzenie zabezpieczeń informatycznych

Kraj, w którym nałożono karę	Wysokość kary	Ukarany podmiot	Istota naruszenia	Możliwości przeciwdziałania
Cypr	€5.000	Szpital Makariosa w Nikozji	Pacjentka zgłosiła, że odmówiono wydania jej dokumentacji medycznej. Szpital nie był w stanie znaleźć dokumentacji medycznej.	właściwe zabezpieczenie szaf kartotekowych prawidłowe oznaczenie dokumentacji w archiwum, tak by była ona łatwa do odszukania
Niemcy	€80.000	nazwa nie została podana do publicznej wiadomości w trosce o dobro pacjentów	przypadkowa publikacja wielu danych medycznych w internecie	aktualne programy antywirusowe wysyłanie danych w mailach zabezpieczonych hasłem przesyłanym innym kanałem (np. sms lub za pośrednictwem komunikatorów)
Bułgaria	€510	niewymienione z nazwy centrum medyczne	Przychodnia przekazała w sposób nieuprawniony dane medyczne pacjenta w związku ze zmianą lekarza podstawowej opieki zdrowotnej. Użyto oprogramowania, żeby wygenerować nową deklarację wyboru, co zostało zgłoszone do płatnika publicznego. Dane medyczne do nowej przychodni zostały jednak przekazane bez zgody pacjenta.	przestrzeganie prawa pacjenta do tajemnicy informacji o jego stanie zdrowia i udzielonych świadczeniach weryfikacja podstaw prawnych i stanu faktycznego przy wnioskach o udostępnianie danych.

Odpowiedzialność cywilna za naruszenie przepisów prawa

Podmiot wykonujący działalność leczniczą, który nie wywiązuje się ze swoich obowiązków jako Administrator danych, naraża się na interwencję ze strony UODO, tak jak każdy Administrator z innej branży. Specyfiką podmiotów leczniczych jest natomiast czuwanie nad przebiegiem wewnętrznych procesów przez szereg wyspecjalizowanych instytucji. Z tego względu działanie lub zaniechanie może być rozpatrywane nie tylko w kontekście kar nakładanych przez PUODO, ale również jako naruszenie zbiorowych praw pacjentów, czy złamanie warunków umowy z NFZ.

Należyte prowadzenie, udostępnianie i niszczenie dokumentacji medycznej stanowi realizację zapisanego w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta prawa pacjenta do dokumentacji medycznej. Do nieuprawnionego ujawnienia danych nie zawsze dochodzi jednak w formie pisemnej, w związku z nieprawidłowościami przy udostępnianiu dokumentacji medycznej, ale również na skutek naruszenia prawa pacjenta do tajemnicy informacji z nim związanych i przekazania danych w formie ustnej.

Rzecznik Praw Pacjenta bada sprawy, w których istnieje podejrzenie naruszenia zbiorowych praw pacjentów. Poprzez naruszenie zbiorowych praw pacjentów rozumiemy taką praktykę, której stosowanie nie jest sumą naruszeń praw indywidualnych pacjentów, a nieokreślonej zbiorowości, która mogłaby chcieć z danego prawa skorzystać. Kluczowe znaczenie zatem mają przyjęte rozwiązania wewnętrzne oraz procedury i zasady postępowania wypracowane w podmiocie leczniczym. Przez praktykę naruszającą zbiorowe prawa pacjentów rozumie się przede wszystkim bezprawne

zorganizowane działania lub zaniechania podmiotów udzielających świadczeń zdrowotnych, mające na celu pozbawienie pacjentów przysługujących im praw lub ograniczenie tych praw, w szczególności podejmowane celem osiągnięcia korzyści majątkowej. Stosowanie praktyk naruszających zbiorowe prawa pacjentów jest zakazane, a w postępowaniu w sprawie naruszeń zastrzeżono dwie sankcje karne:

1) rzecznik w przypadku nieprzekazania przez podmiot udzielający świadczeń zdrowotnych dokumentów oraz wszelkich informacji dotyczących okoliczności stosowania praktyk, co do których istnieje uzasadnione podejrzenie, iż mają charakter praktyk naruszających zbiorowe prawa pacjentów, w drodze decyzji nakłada karę pieniężną do wysokości 50.000 złotych;
2) rzecznik nakłada na podmiot karę pieniężną do wysokości 500.000 złotych w przypadku niepodjęcia działań określonych w decyzji o uznaniu praktyki za naruszającą zbiorowe prawa pacjenta, w terminie w niej wskazanym. Należy przy tym zaznaczyć, że jeżeli podmiot zaprzestał stosowania praktyki naruszającej zbiorowe prawa pacjenta, to na nim spoczywa ciężar udowodnienia, że już niestosuje zabronionych praktyk.

Podmioty, które realizują świadczenia w oparciu o umowę z NFZ muszą dodatkowo liczyć się z możliwością nałożenia na nie kary umownej przez płatnika publicznego. Wynika to z zapisów rozporządzenia z dnia 8 września 2015 roku w sprawie ogólnych warunków umów o udzielanie świadczeń opieki zdrowotnej. W przypadku kar nakładanych przez Rzecznika Praw Pacjenta maksymalną wartość określono kwotowo w ustawie, PUODO może nakładać kary do maksymalnej wartości określonej kwotowo lub jako odsetek obrotów, natomiast kary nakładane w wyniku kontroli prowadzonej przez NFZ są obliczane procentowo od wartości umowy, z którą związane jest stwierdzone naruszenie. Z szerokiego katalogu kar zawartych w przywołanym rozporządzeniu, wybrać można te, które będą mogły zostać nałożone w związku z nieprawidłowościami w przetwarzaniu danych osobowych. Przewidziano zatem kary umowne w razie niewykonania lub wykonania umowy niezgodnie z jej postanowieniami, z przyczyn leżących po stronie świadczeniodawcy, w wysokości:

1) do 2% kwoty zobowiązania wynikającego z umowy za każde stwierdzone naruszenie w przypadku udzielania świadczeń w sposób rażąco nieodpowiadający wymogom określonym w obowiązujących przepisach lub umowie;
2) do 1% kwoty zobowiązania określonej w umowie, za każde stwierdzone naruszenie, w przypadku:
   a) przedstawienia przez świadczeniodawcę danych niezgodnych ze stanem faktycznym, na podstawie których NFZ dokonał płatności nienależnych środków finansowych
   b) przedstawienia przez świadczeniodawcę danych niezgodnych ze stanem faktycznym, na podstawie których NFZ ustala stawkę ryczałtu systemu zabezpieczenia
3) do 1% kwoty zobowiązania określonej w umowie, za każdy rodzaj stwierdzonego naruszenia, w przypadku:
   a) nieprowadzenia list oczekujących na udzielenie świadczenia lub prowadzenia tych list w sposób naruszający przepisy prawa
   b) nieprzekazywania w terminie oraz niezgodnie ze stanem faktycznym:
      – danych dotyczących list oczekujących
      – informacji o pierwszym wolnym terminie udzielenia świadczenia
   c) gromadzenia informacji lub prowadzenia dokumentacji, w tym dokumentacji medycznej, w sposób naruszający przepisy prawa
   d) udzielania świadczeń w sposób lub w warunkach nieodpowiadających wymogom określonym w obowiązujących przepisach lub umowie.

Rozdział VII. Konsekwencje funkcjonowania RODO dla praw pracowników (Kodeks pracy) i pacjentów (Ustawa o prawach pacjentów i Rzeczniku Praw Pacjenta)

Uprawnienia pracowników

Zmiany wprowadzone przez RODO wymagają w sektorze ochrony zdrowia refleksji nie tylko nad należytym zabezpieczeniem danych pacjentów, ale również personelu. Często bowiem zapomina się, że pracodawca ma zapewnić nie tylko bezpieczne i higieniczne warunki pracy, ale i szanować dobra osobiste, w tym również poprzez staranne zabezpieczenie danych.

Jakkolwiek Kodeks pracy nadal jest kluczowym aktem prawnym regulującym relacje pomiędzy pracownikiem a pracodawcą, po zmianach wprowadzonych nowymi ustawami wdrażającymi rozwiązania zawarte w RODO znacząco zmieniły się zakres i podejście do pozyskiwania i przetwarzania danych pracowników. Obecnie katalog danych, które mogą być pozyskiwane od pracownika obejmuje:

1) imię (imiona) i nazwisko
2) datę urodzenia
3) dane kontaktowe wskazane przez taką osobę
4) adres zamieszkania
5) wykształcenie
6) kwalifikacje zawodowe – jeżeli jest to niezbędne
7) przebieg dotychczasowego zatrudnienia
8) numer PESEL, a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość
9) numer rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych
10) inne dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy
11) inne dane osobowe, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

Niedozwolone jest gromadzenie przez pracodawcę kopii dokumentów, które nie są potrzebne do wykonywania przez pracownika określonych zadań na jego stanowisku pracy, takich jak dowód osobisty, wyroki sądu czy akta własności. Należy również dążyć do ograniczenia ingerencji w życie prywatne pracownika. Powszechnie stosowaną praktyką jest zobowiązanie pracownika do podawania w kwestionariuszu osobowym danych swoich dzieci. Jeżeli jednak pracownik nie ma zamiaru korzystać z przywilejów związanych z rodzicielstwem, nie ma potrzeby podawania informacji o swoich dzieciach. Wskaże je tylko, jeżeli zamierza skorzystać z uprawnień pracowniczych z tym związanych. Podobnie w przypadku urlopu okolicznościowego – jest on udzielany po wskazaniu przez pracownika okoliczności, które go uzasadniają i ewentualnie w razie potrzeby okazanie odpowiednich dokumentów (np. zaświadczeń czy aktów stanu cywilnego). Dokumenty te nie mogą być jednak kopiowane i włączane do dokumentacji pracowniczej. Kolejnym nagannym przykładem stosowanym przez polskich pracodawców jest niewłaściwe prowadzenie list obecności. Błędne jest oznaczanie na nich powodu nieobecności pracownika, np. że korzysta on z urlopu okolicznościowego. Na listach obecności powinno się podawać jedynie fakt nieobecności bez omawiania jego przyczyn.

Najważniejsze informacje dotyczące zatrudnienia są gromadzone w aktach osobowych prowadzonych osobno dla każdego pracownika. Prowadzenie i właściwe przechowywanie dokumentacji pracowniczej, w tym również po zakończeniu stosunku pracy jest jednym z podstawowych obowiązków pracodawcy . Od 1 stycznia 2019 roku obowiązuje nowe rozporządzenie określające zasady prowadzenia akt osobowych . Rozstrzygnięto w nim istotne kwestie związane z przetwarzaniem danych pracownika, w tym w szczególności jego prawo do dostępu do swojej dokumentacji. W przypadku gdy dokumentacja pracownicza jest przechowywana przez pracodawcę w postaci papierowej, pracodawca wydaje kopię jej całości lub części w zależności od żądanej i możliwej do zrealizowania formy:

1) w postaci papierowej, opatrzoną podpisem pracodawcy, lub osoby upoważnionej przez pracodawcę, potwierdzającym zgodność kopii z dokumentacją pracowniczą

albo

2) w postaci elektronicznej, jako odwzorowanie cyfrowe sporządzone zgodnie z wymaganiami określonymi w załączniku do rozporządzenia, zapisane w formacie PDF i opatrzone kwalifikowaną pieczęcią elektroniczną lub kwalifikowanym podpisem elektronicznym, pracodawcy lub osoby upoważnionej przez pracodawcę, potwierdzającym zgodność kopii z dokumentacją pracowniczą.

W przypadku gdy dokumentacja pracownicza jest przechowywana przez pracodawcę w postaci elektronicznej, pracodawca wydaje kopię jej całości lub części w postaci elektronicznej lub jako wydruk opatrzony odpowiednimi danymi oraz podpisem pracodawcy, lub osoby upoważnionej przez pracodawcę, potwierdzającym zgodność kopii z dokumentacją pracowniczą znajdującą się w jego zasobach.

Pracodawca wydaje kopię całości lub części dokumentacji pracowniczej na podstawie wniosku, nie później niż w terminie 30 dni od dnia jego otrzymania. Wniosek musi zostać włączony do akt osobowych pracownika.

Akta osobowe pracownika składają się z 4 części – dwie pierwsze dotyczą zatrudnienia i przebiegu stosunku pracy, część C – zakończenia umowy o pracę a część D kar porządkowych. W zakresie związanym z przetwarzaniem danych osobowych akta obejmują:

1) w części A – oświadczenia lub dokumenty dotyczące danych osobowych, zgromadzone w związku z ubieganiem się o zatrudnienie
2) w części B – oświadczenia lub dokumenty dotyczące nawiązania stosunku pracy oraz przebiegu zatrudnienia pracownika, w tym:
   a) oświadczenia lub dokumenty dotyczące danych osobowych, gromadzone w związku z nawiązaniem stosunku pracy
   b) potwierdzenie zapoznania się przez pracownika z zakresem informacji objętych tajemnicą określoną w odrębnych przepisach dla danego rodzaju pracy, zajmowanego stanowiska lub pełnionej funkcji
   c) potwierdzenie poinformowania pracownika o celu, zakresie oraz sposobie zastosowania monitoringu.

W dokumentacji pracowniczej również może znaleźć się rozstrzygnięcie dotyczące identyfikatora. Jego noszenie nie jest wymagane w przepisach dotyczących ambulatoriów. Niemniej jednak w standardach akredytacyjnych dla POZ znaleźć można zalecenie, by pacjent mógł zidentyfikować poszczególnych członków personelu na podstawie identyfikatora zawierającego co najmniej imię i nazwisko oraz funkcję sprawowaną w podmiocie . Możliwe jest zatem uzyskanie zgód wszystkich zatrudnionych na wprowadzenie identyfikatorów, co jednak może okazać się problematyczne z uwagi na możliwość niewyrażenia zgody lub jej odwołania przez poszczególne osoby. Lepszym rozwiązaniem jest wprowadzenie zapisu w regulaminie pracy, a jeżeli nie wszystkie osoby są zatrudniane w oparciu o umowę o pracę i nie obejmuje ich regulamin pracy – w regulaminie organizacyjnym. Umieszczanie informacji o osobach udzielających świadczeń przy gabinecie jest natomiast wymagane, ponieważ wg przepisów prawa świadczeniodawca ma taki obowiązek.

Przykład:

Zatrudniony w przychodni wielospecjalistycznej lekarz poprosił pracodawcę o usunięcie jego danych z tablicy informacyjnej przy gabinecie, powołując się na obowiązywanie RODO. Pracodawca odmówił, wskazując, że pacjenci muszą wiedzieć, kto przyjmuje w danym gabinecie.

Wyjaśnienie

Pracodawca miał rację odmawiając lekarzowi. Niezależnie od rozwiązań prawnych zapisanych w RODO, istnieją jeszcze przepisy szczegółowe dla danego rodzaju działalności. W ogólnych warunkach umów zapisano, że świadczeniodawca jest obowiązany umieścić wewnątrz budynków siedziby i jednostek organizacyjnych informacje dotyczące m.in. imion i nazwisk osób kierujących pracą komórki organizacyjnej, a w przypadku ambulatoryjnych świadczeń – także imion i nazwisk osób udzielających świadczeń oraz godzin i miejsca ich udzielania. Co więcej, brak takiej informacji może skutkować nałożeniem kary umownej. Informacją nieobligatoryjną jest wypisanie specjalizacji uzyskanych przez lekarza i w tym zakresie może on poprosić o usunięcie danych.

Przykład:

Pielęgniarka zatrudniona w przychodni POZ poprosiła pracodawcę o wyjaśnienie, czy musi nosić identyfikator, na którym jest jej imię i nazwisko oraz tytuł zawodowy i wskazanie specjalizacji.

Wyjaśnienie

Nie ma przepisów, które wskazywałyby na taki obowiązek w przychodni. Jedynie w odniesieniu do osób zatrudnionych w szpitalu oraz pozostających w stosunku cywilnoprawnym z podmiotem leczniczym, którego zakładem leczniczym jest szpital artykuł 36 ustawy o działalności leczniczej wprowadza obowiązek noszenia w widocznym miejscu identyfikatora zawierającego imię i nazwisko oraz funkcję tej osoby. Być może jednak kwestia identyfikatorów w tej przychodni została rozstrzygnięta w regulaminie organizacyjnym lub regulaminie pracy.

Pracodawca, który zamierza wykorzystać wizerunek konkretnego pracownika, musi w myśl zasady rozliczalności wykazać, że ma na to jego zgodę, w której wskazano konkretne sposoby wykorzystania wizerunku, np. na stronie internetowej, w mediach społecznościowych, broszurach, na tablicach informacyjnych. Należy zwrócić uwagę, aby w przypadku gotowej zgody przedkładanej pracownikowi przez pracodawcę nie występowały blokowe zestawienia sposobów wykorzystania wizerunku. Pracownik może zgodzić się np. jedynie na wykorzystanie jego wizerunku na broszurach informacyjnych a jednocześnie być niechętnym w stosunku do np. portali społecznościowych.

Z wizerunkiem pracownika wiąże się również kwestia monitoringu wizyjnego. Z perspektywy podmiotów leczniczych bardzo długo brakowało odpowiednich regulacji, a luka w prawie wynikająca z rozwoju techniki i upowszechnienia obserwacji przy pomocy kamer prowadziła do nadużyć i zakładania kamer z wykorzystywaną możliwością rejestracji głosu, np. w gabinetach czy przebieralniach. Pacjenci mogli przez to nie czuć się w pełni swobodnie i przemilczeć pewne problemy, z którymi zgłaszali się do lekarza, czy nawet rezygnować ze świadczeń. Szczegółowe regulacje dotyczące monitoringu w podmiotach leczniczych zaczęły obowiązywać dopiero od 4 maja 2019 roku, jednak już 25 maja 2018 roku nowa ustawa o ochronie danych osobowych wprowadziła zmiany do Kodeksu pracy dotyczące zastosowania kamer we wszystkich zakładach pracy. Pracownik nie ma co prawda możliwości niezgodzenia się na objęcie monitoringiem wizyjnym, ale musi być poinformowany o tym, że ten jest stosowany, a odpowiednie zapisy dodane zostały do regulaminu pracy. Co istotne, zapisy z monitoringu nie mogą być wykorzystywane do oceny pracy, czy badania efektywności pracowników. Instalacja monitoringu ma na celu zapewnienie bezpieczeństwa pracowników, ochronę mienia lub też zachowanie w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Zastosowane rozwiązania techniczne nie mogą naruszać prywatności pracowników. Wykluczono zatem możliwość zamontowania kamer w pomieszczeniach sanitarnych, szatniach, stołówkach, palarniach lub w pomieszczeniach udostępnianych zakładowej organizacji związkowej, chyba że stosowanie urządzeń rejestrujących obraz w tych

pomieszczeniach jest niezbędne do realizacji dopuszczalnych prawem celów monitoringu i nie naruszy to godności oraz innych dóbr osobistych pracownika, a także zasady wolności i niezależności związków zawodowych, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób. Dodatkowo maksymalny czas na przechowywanie zapisu obrazu z kamer określono na trzy miesiące. Teren objęty monitoringiem musi być oznaczony w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem.

Uprawnienia pacjentów

Wprowadzenie RODO wiązało się ze zwróceniem szczególnej uwagi na ochronę danych osobowych pacjentów, nie mniej już wcześniej istniały rozwiązania prawne, które miały zapewnić im bezpieczeństwo w tym zakresie. Obowiązującą od 5 czerwca 2009 roku ustawą o prawach pacjenta i Rzeczniku Praw Pacjenta ustanowiono dwa istotne uprawnienia w tym zakresie:

1. prawo pacjenta do tajemnicy informacji
2. prawo pacjenta do dokumentacji medycznej.

Na gruncie RODO przyznano osobom, których dane są przetwarzane przez Administratorów, niezależnie od profilu działalności, następujące uprawnienia:

1. prawo do informacji (obowiązek informacyjny) – obligatoryjne przekazanie szczegółowych informacji o Administratorze, podstawach prawnych, celu i sposobie przetwarzania danych dokonane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – „udzielić osobie, której dane dotyczą, wszelkich informacji"
2. prawo dostępu do danych – zapewnienie, by każdy pacjent oraz inne osoby, których dane osobowe mogą być przetwarzane przez podmiot, uzyskały potwierdzenie, czy rzeczywiście dane są przetwarzane, w jakim celu oraz jakie dane znajdują się w zasobach
3. prawo do sprostowania danych – każdy pacjent lub inna osoba, której dane przetwarza podmiot, ma prawo żądać sprostowania danych, które są nieprawidłowe lub nieaktualne jak również prosić o uzupełnienie danych, które są niekompletne
4. prawo do usunięcia danych (prawo bycia zapomnianym) – możliwość zgłoszenia żądania całkowitego usunięcia wszystkich danych dotyczących danej osoby przetwarzanych przez określony podmiot
5. prawo do ograniczenia przetwarzania – zapewnienie możliwości wniesienia żądania, by na danych nie można było przeprowadzać innych operacji niż przechowywanie. RODO upoważnia do dalszego przetwarzania danych, mimo zgłoszonego wniosku o ograniczenie, jeśli uzasadnia to interes publiczny nadrzędny wobec uprawnienia osoby. Ograniczenie przetwarzania danych zawartych w dokumentacji medycznej mogłoby nieść duże ryzyko dla zdrowia i życia pacjenta, z tego powodu, wobec danych medycznych prawo do ograniczenia przetwarzania co do zasady nie będzie miało zastosowania
6. prawo do przenoszenia danych – osoba, której dane dotyczą, ma prawo otrzymać (w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego) dane osobowe jej dotyczące, które dostarczyła administratorowi oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy oraz gdy przetwarzanie odbywa się w sposób zautomatyzowany
7. prawo do sprzeciwu – nadające pacjentowi lub innej osobie uprawnienie do wprowadzenia wobec Administratora ograniczeń w przetwarzaniu danych. W takiej sytuacji nie wolno już przetwarzać danych osobowych, chyba że Administrator wykaże istnienie ważnych, prawnie uzasadnionych, podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą lub podstaw do ustalenia, dochodzenia albo obrony roszczeń
8. prawo do wycofania zgody w dowolnym momencie – przyzwolenie na zmianę decyzji dotyczącej zgody na wykorzystanie danych osobowych w przypadku danych przetwarzanych zgodnie z dobrowolną zgodą danej osoby.

Po wprowadzonych zmianach, obowiązujących od 25 maja 2018 roku bardziej rozbudowaną strukturę i zakres danych otrzymała klauzula informacyjna przekazywana pacjentom. Powinna się ona znaleźć na tablicy informacyjnej w miejscu rejestracji, bądź udzielania świadczeń, na stronie internetowej oraz w zapowiedzi telefonicznej przed połączeniem z Administratorem, a także w stopce maila – choćby w skróconej formie i wraz z odesłaniem do pełnej treści na stronie internetowej. Często bowiem kontakt mailowy jest pierwszą możliwością przekazania informacji o Administratorze.

Nowa ustawa o ochronie danych osobowych wprowadziła również obowiązek ujawnienia przez Administratora wyznaczonego przez niego Inspektora Ochrony Danych. W ustawie z 10 maja 2018 roku o ochronie danych osobowych (Dz.U. 2018 poz. 1000) zapisano obowiązek umieszczenia informacji o IOD na stronie internetowej, a jeżeli Administrator nie prowadzi strony internetowej – udostępnienia takiej informacji w miejscu udzielania świadczeń, np. na tablicy informacyjnej.

Podstawa prawna:

Art. 11.

Podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa w art. 10 ust. 1, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.

Art. 10.

1. Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o jego wyznaczeniu w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora.

Pacjent ma zatem nie tylko, tak jak dotychczas, prawo do informacji na temat zasad składania skarg i wniosków do kierownictwa podmiotu, komórki organizacyjnej właściwej ds. skarg i wniosków w oddziale wojewódzkim NFZ oraz Rzecznika Praw Pacjenta, ale również możliwość skontaktowania się w razie wątpliwości z Inspektorem Ochrony Danych lub zgłoszenia podejrzenia incydentu bezpieczeństwa do PUODO.

Prawo do bycia zapomnianym i jego ograniczenia

Wprowadzenie RODO zapewniło osobom, których dane są przetwarzane m.in. gwarancję bezpieczeństwa danych w postaci możliwości wystosowania do Administratora żądania usunięcia danych osobowych. Wiele podmiotów wskazuje na przeszkody natury technicznej przy realizacji tego uprawnienia. W stosunku do osoby, której dane są przetwarzane jednak prawo to nie będzie miało zastosowania przede wszystkim jeśli przetwarzanie tych danych jest niezbędne do realizacji obowiązku prawnego. Biorąc pod uwagę fakt, że dane medyczne pacjentów przetwarzane są na podstawie stosownych przepisów prawa, dane pacjenta oraz jego dokumentacja medyczna nie będą mogły zostać usunięte na wniosek pacjenta. Sposób ich pozyskiwania, zakres obligatoryjnie przekazywanych danych oraz czas ich przechowywania zostały uregulowane w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta oraz w odpowiednich aktach wykonawczych. Ponadto podmioty realizujące umowę z Narodowym Funduszem Zdrowia muszą realizować obowiązki sprawozdawcze. Dane o udzielonych świadczeniach znajdujące się w dokumentacji medycznej stanowią podstawę do ewentualnej weryfikacji prawidłowości rozliczeń.

Z prawa do bycia zapomnianym można natomiast skorzystać, jeżeli brakuje podstawy prawnej do przetwarzania danych, czyli w szczególności gdy upłynął już ustawowo określony czas przechowywania dokumentacji medycznej. W przypadku historii zdrowia i choroby prowadzonej w podmiocie leczniczym, okres przechowywania dokumentacji medycznej zgodnie z ustawą o prawach pacjenta i Rzeczniku Praw Pacjenta wynosi co do zasady 20 lat licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu. Jeżeli pomimo upływu tych terminów podmiot nadal przechowuje dokumentację, żądanie ich usunięcia jest w pełni uzasadnione.

Przykład:

Pacjent zdecydował się na zmianę lekarza POZ. Po złożeniu deklaracji wyboru w nowej przychodni pacjent zwrócił się do dyrektora centrum medycznego, w którym leczył się dotychczas, z żądaniem usunięcia jego danych. Dyrektor postanowił skonsultować się z powołanym w centrum medycznym Inspektorem Ochrony Danych, który wykluczył możliwość spełnienia żądania pacjenta.

Wyjaśnienie

Konsekwencją zmiany lekarza POZ jest konieczność założenia przez lekarza w przychodni, którą wybrał pacjent, nowej historii zdrowia i choroby opatrzonej danymi identyfikacyjnymi, w tym kodami resortowymi odpowiednimi dla tego podmiotu. Dane dotychczasowego leczenia muszą pozostać w przychodni, która wytworzyła tę dokumentację medyczną. Podmiot ten odpowiada za właściwe zabezpieczenie danych pacjenta i ich przechowywanie przez kolejnych 20 lat od końca roku kalendarzowego, w którym dokonano ostatniego wpisu. Przez ten czas dostęp do danym ma zapewniony zarówno pacjent, jak i osoba przez niego uprawniona oraz ustawowo upoważnione instytucje.

Inspektor ochrony danych udzielił dyrektorowi trafnej porady, którą warto zawrzeć w odpowiedniej procedurze reagowania na wnioski związane z ochroną danych osobowych.

Przykład:

Pacjentka jako dziecko była leczona w przychodni. Ostatnia porada u lekarza pediatry miała miejsce w 1993 roku. Pacjentka zwróciła się do przychodni z pytaniem, czy jej dokumentacja medyczna znajduje się w archiwum. Po uzyskaniu informacji, że dokumentacja znajduje się nadal w przychodni, pacjentka napisała wniosek, w którym prosi o zniszczenie dokumentacji powołując się na prawo do zapomnienia zapisane w RODO.

Wyjaśnienie

Przychodnia już kilka lat wcześniej powinna zniszczyć dokumentację pacjentki. Jeśli tak się nie stało dokumentację należy zniszczyć niezwłocznie, pacjentce przekazać stosowną informację o podjętych działaniach oraz dokonać weryfikacji w archiwum pod kątem terminu przechowywania znajdującej się tam dokumentacji innych pacjentów.

Terminy przechowywania zapisane w ustawie nie mogą być wydłużane zarządzeniem kierownika czy innymi aktami wewnętrznymi. Organizacja pracy w podmiocie i sposób postępowania z dokumentacją archiwalną nie może stać w sprzeczności z obowiązującym prawem.

Opłata za realizację praw związanych z RODO

W myśl artykułu 15 RODO, osoba, której dane są przetwarzane, może uzyskiwać od Administratora informacje na temat zasad przetwarzania danych, a także występować o potwierdzenie czy jej dane są w ogóle przetwarzane przez dany podmiot. Pacjent, ale również osoba zatrudniona w podmiocie leczniczym, może zatem zwrócić się o informacje obejmujące:

1) cele przetwarzania
2) kategorie odnośnych danych osobowych
3) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych, w przypadku

których niezbędne jest także wskazanie informacji o wdrożonych zabezpieczeniach (należy zwrócić uwagę zwłaszcza gdzie trafiają dane z serwerów czy nagrania rozmów telefonicznych)
4) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu (w przypadku przychodni trudno powiedzieć jak długo dane będą znajdowały się w zasobach podmiotu leczniczego, ale można wskazać, że okres przechowywania trwa np. 20 lat i rozpocznie się od końca roku kalendarzowego, w którym dokonywany jest ostatni wpis w dokumentacji)
5) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania
6) informacje o prawie wniesienia skargi do organu nadzorczego
7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle (np. w przypadku rejestracji przez osoby trzecie)
8) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Co do zasady, komunikacja w sprawach wynikających z RODO, związanych z realizowaniem uprawnień osoby, której dane są przetwarzane, powinna być prowadzona bez opłat. Można jednak wyobrazić sobie pacjenta, który ustawicznie wnosząc o przygotowanie informacji w różnych zakresach praktycznie paraliżuje pracę osoby odpowiedzialnej za udzielanie takich informacji. Gdy żądania są nieuzasadnione lub nadmierne, podmiot leczniczy ma możliwość ustalenia wynagrodzenia, które RODO określa jako rozsądną opłatę. Koszty związane ze sporządzeniem kopii dokumentacji, o ile będą na poziomie odpowiadającym realnie poniesionym nakładom czyli kosztom administracyjnym, opłatom za wysyłkę czy przesłanie kurierem, uznać można za prawidłowo ustalone. To istotne narzędzie ochrony personelu przed wielokrotnym odpowiadaniem na to samo pytanie kierowane przez jednego pacjenta.

Prawo do kopii danych pacjenta a prawo do dokumentacji medycznej pacjenta

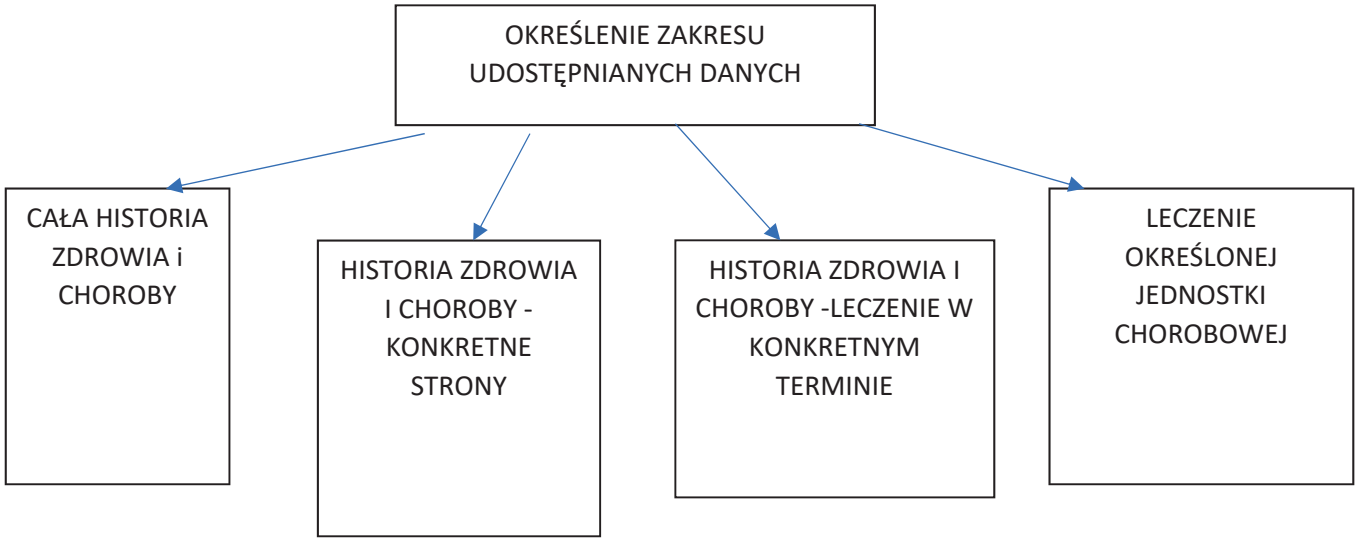
Pacjent przed wejściem w życie RODO miał zapewniony dostęp do danych zawartych w dokumentacji medycznej na mocy regulacji zawartych w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta. W wymienionej ustawie zapisano, że dostęp do danych ma pacjent, jego przedstawiciel ustawowy oraz osoba upoważniona przez pacjenta. Odpłatność za udostępnienie dokumentacji medycznej warunkowana była wewnętrznymi regulacjami podmiotu leczniczego, z którego usług korzystał pacjent. Ustawodawca określił jedynie sposób obliczania wartości maksymalnej opłaty ustalając jej wysokość na podstawie przeciętnego wynagrodzenia, tak by nie dochodziło do prób zawyżenia kwot i ograniczania w ten sposób dostępu do danych.

W RODO zapisano prawo do nieodpłatnego dostępu do danych osobowych przetwarzanych przez Administratora, tak by móc zapoznać się z zakresem informacji posiadanych na temat osoby zainteresowanej przez dany podmiot. Początkowo pojawiały się wątpliwości dotyczące zakresu pojęciowego i kwestii tożsamości kopii danych z kopią dokumentacji medycznej. Ostatecznie, celem rozwiązania pojawiających się trudności interpretacyjnych, rozstrzygnięto w ustawie implementującej RODO sposób postępowania w przypadku wydania pierwszej kopii dokumentacji medycznej.

Występujące w RODO pojęcie kopii zinterpretowano rozszerzająco, wskazując, że chodzi nie tylko o kserokopię, ale również odpis, wyciąg lub wydruk, a także o przekazanie danych na nośniku informatycznym (nie pobiera się wówczas opłat za płytę CD, DVD czy inny nośnik pamięci). Zapewnienie wglądu do dokumentacji medycznej nie jest natomiast wystarczające – pacjent musi uzyskać fizyczne potwierdzenie informacji, jakie znajdują się w zasobie określonego podmiotu.

Od dnia wejścia w życie ustawy pacjent oraz jego przedstawiciel ustawowy mogą uzyskać za darmo pierwszy dostęp do dokumentacji medycznej w danym zakresie w wybranej przez siebie formie. Według stanowiska prezentowanego przez Ministra Zdrowia, uprawnienie do pierwszego bezpłatnego dostępu przysługuje również osobie upoważnionej przez pacjenta. Uargumentowano to faktem, że osoba upoważniona może być osobą działającą na rzecz pacjenta niepełnosprawnego, który sam nie jest w stanie zgłosić się do podmiotu leczniczego w celu realizacji przysługującego mu prawa.

Co istotne, udostępnienie, pomimo że jest bezpłatne, podlega obowiązkowi odnotowania w wykazie udostępnionej dokumentacji medycznej, o której szerzej w rozdziale VIII. To szczególnie ważne, jako że mowa jest o dostępie pierwszorazowym do danych w danym zakresie jako dostępie nieodpłatnym. Każde powtórne udostępnienie danych w konkretnym zakresie może już wiązać się z odpłatnością. Z tego też względu prowadzenie ewidencji pozwala na ustalenie, czy z danego uprawnienia już skorzystano, czy też nie. Sam zakres można interpretować różnie, w zależności od tego, jakie będzie żądanie pacjenta, nie można natomiast w żadnym przypadku pytać o cel, w jakim pacjent chce pozyskać dokumentację, czy próbować ograniczać formę udostępnienia, zwłaszcza w przypadku odpisu, którego sporządzenie jest czasochłonne, a w nowym stanie prawnym jest on możliwy do uzyskania bez ponoszenia opłat. Szczegóły powinny zostać odpowiednio opisane właśnie w wykazie udostępnianej dokumentacji medycznej.



Rozdział VIII. Zasady wydawania i ewidencjonowania wydawania dokumentacji medycznej; konieczność wdrożenia właściwych procedur zgodnych z RODO i ustawami regulującymi funkcjonowanie służby zdrowia

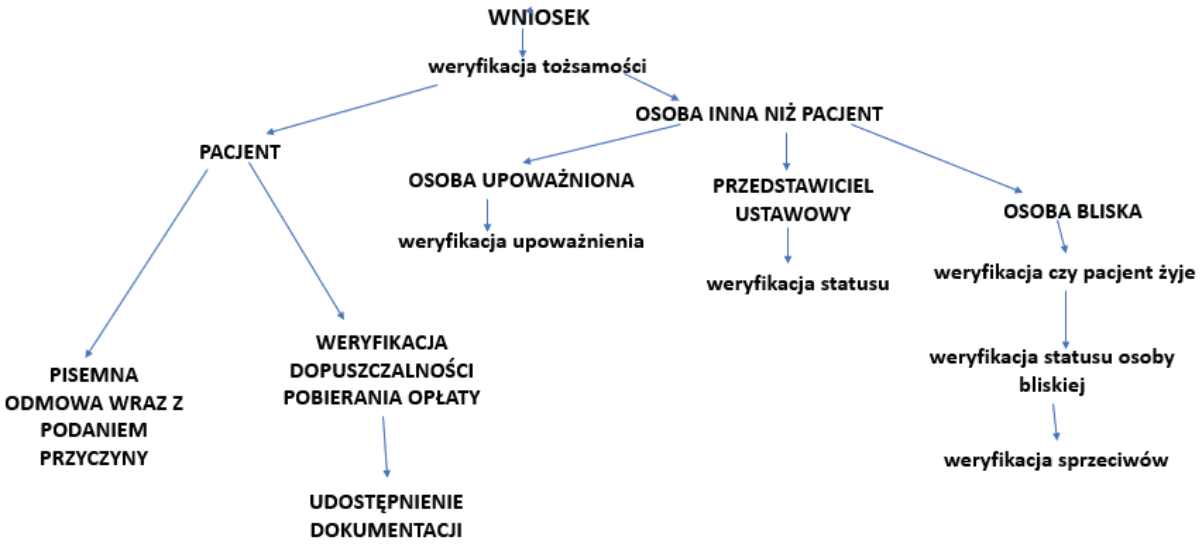
Identyfikacja tożsamości i uprawnień osób fizycznych zwracających się o dokumentację medyczną

Na gruncie RODO wskazano, że dane dotyczące zdrowia muszą podlegać szczególnej ochronie. Należy zatem wdrożyć odpowiednie środki organizacyjne i techniczne, które mają zminimalizować ryzyko związane z przypadkowym ujawnieniem danych osobom nieuprawnionym.

Podstawowym mechanizmem zabezpieczającym przed ujawnieniem danych niewłaściwej osobie jest weryfikacja tożsamości. Jej podstawą jest okazanie aktualnego dokumentu potwierdzającego tożsamość. Art. 26 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta jasno wskazuje, że podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną pacjentowi lub jego przedstawicielowi ustawowemu, bądź osobie upoważnionej przez pacjenta. Nie ma zatem możliwości, by wydać dokumentację każdej osobie, która się po nią zgłosi, a ściśle określonej w ustawie. W przypadku braku możliwości potwierdzenia tożsamości w pełni uzasadniona jest odmowa zarówno realizacji świadczeń jak i wydawania dokumentacji medycznej czy przekazywania informacji o stanie zdrowia i udzielonych świadczeniach. Jakkolwiek identyfikacja jest niezbędna nie ma podstaw dla wykonywania kopii dokumentów, na podstawie których potwierdzono tożsamość, czy nawet odnotowywania numerów dokumentów, takich jak dowód osobisty czy paszport.

Wnioski osób fizycznych o udostępnienie dokumentacji medycznej powinny być weryfikowane wg następującego schematu:

Wnioski osób fizycznych o udostępnienie dokumentacji medycznej powinny być weryfikowane wg następującego schematu:



Brak właściwej identyfikacji pacjenta może sprzyjać incydentom bezpieczeństwa, takim jak np.:

- przekazanie danych pacjenta innemu pacjentowi (omyłkowe wydanie krzyżowo np. wyników badań)
- przekazanie danych osobie upoważnionej przez innego pacjenta
- wydanie recept niewłaściwej osobie.

Jeżeli w wyniku nieprawidłowej identyfikacji dojdzie do przekazania danych, nawet jeżeli dane te obejmują jedynie imię, nazwisko i PESEL, innej niż pacjent osobie, która nie powinna mieć dostępu do tych danych, musimy brać pod uwagę różne następstwa tego zdarzenia. Żeby w możliwie najlepszy sposób pomóc osobie, której dane dotyczą, należy przekazać jej informację wg poniższego wzoru:

Szanowny Panie,

Informujemy, że w dniu ……..…. doszło w naszej przychodni ……...…. do incydentu naruszenia bezpieczeństwa, polegającego na przekazaniu Pana/Pani danych innej, nieuprawnionej osobie. W wyniku zaistniałej sytuacji może dojść do naruszenia Pana/Pani praw lub wolności. Zwracamy uwagę, że Pana dane mogą zostać wykorzystane do:

- naruszenia Pana/Pani dobrego imienia (np. przez uzyskanie dostępu do danych osobowych i wykorzystanie tej wiedzy przeciwko Panu/Pani)
- pozbawienia lub ograniczenia Pana/Pani praw (np. przez głosowanie w Pana/Pani imieniu w sprawach budżetu obywatelskiego przy wykorzystaniu Pana/Pani danych)
- działań równoznacznych z utratą kontroli nad Pana/Pani danymi osobowymi (np. uzyskania dostępu do świadczeń opieki zdrowotnej na podstawie karty informacyjnej z leczenia szpitalnego przy podaniu danych przez telefon lub rejestracji bez prawidłowej weryfikacji tożsamości)
- zarejestrowania na Pana/Panią dane osobowe przedpłaconej karty telefonicznej (pre-paid), która może posłużyć do celów przestępczych
- uzyskania przez osoby trzecie dostępu do Pana/Pani środków, zgromadzonych na prywatnych kontach bankowych, wyłudzonych przez wcześniej wymienione osoby podszywające się pod instytucje finansowe za pomocą SMS-ów
- zawarcia w Pana/Pani imieniu umowy o świadczenie usług (np. telewizji kablowej, telefonu, energii elektrycznej, usług dostępu do materiałów audio lub wideo poprzez media strumieniowane, np. aplikacje streamingowe itp.), która to umowa nie będzie opłacana i może spowodować dla Pana/Pani znaczne zadłużenie

- działań równoznacznych z utratą kontroli nad Pana/Pani danymi osobowymi (np. podszywania się pod Pana/Panią celem wzięcia kredytu lub pożyczki na Pana/Pani dane, w szczególności w przypadku usług, do których dostęp uzyskuje się przez internet, wyłudzenia ubezpieczenia lub środków z ubezpieczenia, co może spowodować negatywne konsekwencje w postaci problemów związanych z próbą przypisania Panu/Pani odpowiedzialności za takie oszustwa – kradzież tożsamości)
- przetwarzania danych osobowych w celach marketingowych, bez uprzedniego uzyskania Pańskiej/Pani zgody.

Rozpatrywanie wniosków firm, instytucji lub urzędów ws. udostępnienia dokumentacji medycznej

Dokumentacja medyczna zawiera dane, które są istotne nie tylko dla osoby, której dotyczą, ale mogą również mieć znaczenie dla realizacji zadań nałożonych na niektóre instytucje. Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta wymienia kategorie podmiotów uprawnionych do występowania o udostępnienie dokumentacji medycznej. Zastrzega ona również okoliczności uprawniające do złożenia odpowiedniego wniosku.

Rozpatrując wnioski należy pamiętać, że instytucje, podobnie jak pacjent czy osoba przez niego upoważniona, mogą uzyskać dostęp w każdej określonej w ustawie formie. Ujawniając dane pacjenta podmiot musi jednak być pewny, którego pacjenta dotyczy wniosek. Jeżeli wniosek zawiera wyłącznie imię i nazwisko, należy poprosić o dodatkowe dane, w szczególności data urodzenia lub PESEL, żeby omyłkowo nie przekazać informacji o innej osobie noszącej to samo lub zbliżone imię i nazwisko.

Lp.	Kategorie uprawnionych podmiotów	Wyjaśnienie	Uwagi
1.	podmioty udzielające świadczeń zdrowotnych, jeżeli dokumentacja ta jest niezbędna do zapewnienia ciągłości świadczeń zdrowotnych	by kontynuować proces leczenia często niezbędne jest przekazania danych dotyczących dotychczasowego leczenia. Generalną zasadą jest przekazanie kopii, ale mogą się zdarzyć sytuacje, w których przekazanie nastąpi w formie skanu czy w przypadku zagrożenia życia lub zdrowia pacjenta – również w formie oryginału z zastrzeżeniem zwrotu po wykorzystaniu	1. nie można wydać oryginału np. historii zdrowia i choroby, by kolejny podmiot kontynuował w niej wpisy 2. jeżeli podmiot zwraca się telefonicznie o przekazanie dokumentacji należy zweryfikować, czy rzeczywiście telefon wykonano z uprawnionego podmiotu – np. weryfikacja numeru w RPWDL i wykonanie połączenia zwrotnego, albo prośba o przesłanie wniosku np. faksem
2.	organa władzy publicznej w zakresie niezbędnym do wykonywania przez te podmioty ich zadań, w szczególności nadzoru i kontroli	w ustawie brak definicji organu władzy publicznej	istotne jest określenie, czy w danej sprawie organ wykonuje swoje zadania i jaką ma podstawę prawną do wnioskowania w tej sprawie o dostęp do dokumentacji medycznej

Lp.	Kategorie uprawnionych podmiotów	Wyjaśnienie	Uwagi
3.	Rzecznik Praw Pacjenta w zakresie niezbędnym do wykonywania swoich zadań, w szczególności nadzoru i kontroli	zgodnie z art. 52 ustawy Rzecznik może w toku postępowania wyjaśniającego żądać złożenia wyjaśnień oraz zapewnienia dostępu do dokumentów przez podmioty udzielające świadczeń zdrowotnych	
4.	Narodowy Fundusz Zdrowia w zakresie niezbędnym do wykonywania swoich zadań, w szczególności nadzoru i kontroli	w § 30 rozporządzenia w sprawie ogólg nych warunków umów zapisano, że istnieje możliwość zastrzeżenia w umowach z płatnikiem publicznym kar umownych, w tym do 1% kwoty zobowiązania określonej w umowie w przypadku gromadzenia informacji lub prowadzenia dokumentacji, w tym dokumentacji medycznej, w sposób naruszający przepisy prawa	od 1 czerwca 2019 roku do ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych włączono nowe przepisy dotyczące kontroli: osoba przeprowadzająca kontrolę ma prawo badać i oceniać wszelkie informacje związane z zakresem kontroli, zawarte w dokumentach, w tym w dokumentacji medycznej i finansowo-księgowej oraz na innych nośnikach informacji kontrolujący może zażądać od kierownika podmiotu kontrolowanego nieodpłatnego sporządzenia, w terminie wyznaczonym przez kontrolera lub tę osobę, niezbędnych dla osiągnięcia celów kontroli odwzorowań cyfrowych, zestawień i obliczeń przygotowanych na podstawie dokumentów lub elektronicznych baz danych, a w przypadku braku możliwości technicznych, sporządzenia dokumentów, zestawień i obliczeń w postaci papierowej 3) na żądanie kontrolującego zgodność odwzorowań cyfrowych oraz kopii, wyciągów, zestawień i obliczeń sporządzonych w postaci papierowej z dokumentami źródłowymi lub danymi z elektronicznych baz danych potwierdza kierownik komórki organizacyjnej, w której dokumenty się znajdują lub osoba do tego upoważniona

Lp.	Kategorie uprawnionych podmiotów	Wyjaśnienie	Uwagi
5.	organa samorządu zawodów medycznych w zakresie niezbędnym do wykonywania swoich zadań, w szczególności nadzoru i kontroli	szczegółowe regulacje znajdują się w: ustawie z dnia 2 grudnia 2009 roku o izbach lekarskich (Dz.U. 2019 poz. 965), ustawie z dnia 1 lipca 2011 roku o samorządzie pielęgniarek i położnych (Dz.U. 2018 poz. 916), ustawie z dnia 25 września 2015 roku o zawodzie fizjoterapeuty (Dz.U. 2019 poz. 952)	
6.	konsultanci w ochronie zdrowia w zakresie niezbędnym do wykonywania swoich zadań, w szczególności nadzoru i kontroli	szczegóły dotyczące zadań wykonywanych przez konsultantów zostały opisane w ustawie z dnia 6 listopada 2008 roku o konsultantach w ochronie zdrowia (Dz.U 2019 poz. 886)	
7.	Rzecznik Praw Pacjenta Szpitala Psychiatrycznego w zakresie niezbędnym do wykonywania swoich zadań, w szczególności nadzoru i kontroli	zadania Rzecznika Praw Pacjenta Szpitala Psychiatrycznego reguluje art. 10a i następne ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego	
8.	podmioty przeprowadzające kontrolę na zlecenie Ministra Zdrowia	zgodnie z art. 119 ustawy o działalności leczniczej: 1. minister właściwy do spraw zdrowia może zlecić przeprowadzenie kontroli: 1) wojewodom 2) konsultantom krajowym 3) jednostkom organizacyjnym podległym lub nadzorowanym przez tego ministra 2. minister właściwy do spraw zdrowia może zlecić, na podstawie umowy, odpłatne przeprowadzenie jednorazowej kontroli: 1) organom samorządów zawodów medycznych 2) medycznym towarzystwom naukowym 3) uczelniom medycznym 4) instytutom badawczym 5) specjalistom z poszczególnych dziedzin medycyny	zlecana kontrola przeprowadzana jest przez osoby wykonujące zawód medyczny

Lp.	Kategorie uprawnionych podmiotów	Wyjaśnienie	Uwagi
9.	upoważnionym przez podmiot tworzący – w przypadku podmiotów leczniczych niebędących przedsiębiorcami – osobom wykonującym zawód medyczny, w zakresie niezbędnym do sprawowania nadzoru nad podmiotem leczniczym niebędącym przedsiębiorcą	zgodnie z art. 121 ustawy o działalności leczniczej, w ramach nadzoru podmiot tworzący może żądać informacji, wyjaśnień oraz dokumentów od organów podmiotu leczniczego niebędącego przedsiębiorcą oraz dokonać kontroli i oceny działalności tego podmiotu. Kontrola i ocena obejmują w szczególności: 1) realizację zadań określonych w regulaminie organizacyjnym i statucie, dostępność i jakość udzielanych świadczeń zdrowotnych 2) prawidłowość gospodarowania mieniem oraz środkami publicznymi 3) gospodarkę finansową	
10.	Agencja Oceny Technologii Medycznych i Taryfikacji, w zakresie niezbędnym do wykonywania przez nią zadań określonych w art. 31n ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych		współpraca z AOTMiT jest jednym z obowiązków świadczeniodawców
11.	Agencja Badań Medycznych w zakresie określonym ustawą z dnia 21 lutego2019 r. o Agencji Badań Medycznych (Dz. U. poz. 447)	zgodnie z art. 15 ustawy o Agencji Badań Medycznych, Do zadań agencji w zakresie działalności określonej w art. 2 należy: 1) tworzenie i zarządzanie programami, na podstawie których będą dofinansowywane projekty, w tym projekty interdyscyplinarne 2) upowszechnianie informacji o planowanych lub ogłaszanych konkursach 3) ocena wniosków i zawieranie umów z beneficjentami 4)nadzór i kontrola realizacji projektów, w tym projektów interdyscyplinarnych 5) prowadzenie własnych badań naukowych i prac rozwojowych 6) dofinansowanie projektów niekomercyjnych badań klinicznych	w zakresie przetwarzanych danych osobowych ABM ma prawo dostępu do: 1) danych gromadzonych przez Narodowy Fundusz Zdrowia oraz do baz danych dotyczących świadczeń opieki zdrowotnej finansowanych ze środków publicznych, prowadzonych przez podmioty inne niż Narodowy Fundusz Zdrowia 2) rejestrów medycznych 3) dokumentacji medycznej

Lp.	Kategorie uprawnionych podmiotów	Wyjaśnienie	Uwagi
12.	minister właściwy do spraw zdrowia w związku z prowadzonym postępowaniem		istotne jest przywołanie danych konkretnego postępowania
13.	sąd właściwy w związku z prowadzonym postępowaniem		
14.	sąd dyscyplinarny w związku z prowadzonym postępowaniem		
15.	prokuratura w związku z prowadzonym postępowaniem		
16.	lekarz sądowy w związku z prowadzonym postępowaniem		
17.	Rzecznik Odpowiedzialności Zawodowej, w związku z prowadzonym postępowaniem		
18.	uprawnione, na mocy odrębnych ustaw, organa i instytucje, jeżeli badanie zostało przeprowadzone na ich wniosek	przykładem tego rodzaju działań jest badanie przeprowadzane na wniosek policji, dotyczące oceny stanu zdrowia osoby zatrzymanej, uregulowane w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 13 września 2012 roku w sprawie badań lekarskich osób zatrzymanych przez policję	
19.	organ rentowy w związku z prowadzonym przez niego postępowaniem	organami rentowymi są w szczególności: Zakład Ubezpieczeń Społecznych Kasa Rolniczego Ubezpieczenia Społecznego Zakład Emerytalno-Rentowy MSWiA	
20.	zespół do spraw orzekania o niepełnosprawności, w związku z prowadzonym przez niego postępowaniem	funkcjonowanie zespołów opisano w art. 6 i następnych ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej osób niepełnosprawnych (Dz.U. 2019 poz. 1172 ze zm.)	
21.	podmiot prowadzący rejestr usług medycznych, w zakresie niezbędnym do prowadzenia rejestru		

Lp.	Kategorie uprawnionych podmiotów	Wyjaśnienie	Uwagi
22.	zakład ubezpieczeń, za zgodą pacjenta	Kwestie związane z uzyskiwaniem dokumentacji medycznej przez zakłady ubezpieczeń reguluje art. 38 ustawy z dnia 11 września 2015 roku o działalności ubezpieczeniowej i asekuracyjnej: 1. zakład ubezpieczeń może uzyskać odpłatnie od podmiotów wykonujących działalność leczniczą, które udzielały świadczeń zdrowotnych ubezpieczonemu lub osobie, na rachunek której ma zostać zawarta umowa ubezpieczenia, informacje o okolicznościach związanych z oceną ryzyka ubezpieczeniowego i weryfikacją podanych przez tę osobę danych o jej stanie zdrowia, ustaleniem prawa tej osoby do świadczenia z zawartej umowy ubezpieczenia i wysokością tego świadczenia 2. zakres informacji o stanie zdrowia ubezpieczonego lub osoby, na rachunek której ma zostać zawarta umowa ubezpieczenia, obejmuje następujące informacje o: 1) przyczynach hospitalizacji, wykonanych w jej trakcie badaniach diagnostycznych i ich wynikach, innych udzielonych świadczeniach zdrowotnych, wynikach leczenia oraz o wynikach sekcji zwłok, jeżeli została przeprowadzona 2) przyczynach leczenia ambulatoryjnego, wykonanych w jego trakcie badaniach diagnostycznych i ich wynikach, innych udzielonych świadczeniach zdrowotnych oraz wynikach leczenia 3) wynikach przeprowadzonych konsultacji 4) przyczynie śmierci ubezpieczonego. 3. Informacje, o których mowa w ust. 2, udzielane są z wyłączeniem wyników badań genetycznych. 4. Informacje o przyczynach hospitalizacji i leczenia zawierają kod jednostki chorobowej zgodnie z Międzynarodową Statystyczną Klasyfikacją Chorób i Problemów Zdrowotnych Rewizja Dziesiąta.	Z żądaniem przekazania informacji występuje lekarz upoważniony przez zakład ubezpieczeń. Wystąpienie zakładu ubezpieczeń o informacje wymaga zgody ubezpieczonego lub osoby, na rachunek której ma zostać zawarta umowa ubezpieczenia, albo jej przedstawiciela ustawowego. Podmiot wykonujący działalność leczniczą przekazuje posiadane informacje o stanie zdrowia ubezpieczonego lub osoby, na rachunek której ma zostać zawarta umowa ubezpieczenia, zakładowi ubezpieczeń, który o te informacje występuje, w terminie nie dłuższym niż 14 dni, licząc od dnia otrzymania wystąpienia o przekazanie informacji.

Lp.	Kategorie uprawnionych podmiotów	Wyjaśnienie	Uwagi
23.	komisje lekarskie podległe ministrowi właściwemu do spraw wewnętrznych, wojskowe komisje lekarskie oraz komisje lekarskie Agencji Bezpieczeństwa Wewnętrznego lub Agencji Wywiadu, podległe szefom właściwych agencji		
24.	osoby wykonujące zawód medyczny, w związku z prowadzeniem procedury oceniającej podmiot udzielający świadczeń zdrowotnych na podstawie przepisów o akredytacji w ochronie zdrowia albo procedury uzyskiwania innych certyfikatów jakości, w zakresie niezbędnym do ich przeprowadzenia	Art. 3 ust. 5 ustawy z dnia 6 listopada 2008 r. o akredytacji w ochronie zdrowia stanowi, że: w ramach przeglądu upoważniona przez ośrodek akredytacyjny osoba jest uprawniona do: 1) wstępu na teren podmiotu udzielającego świadczeń zdrowotnych 2) wglądu do dokumentacji medycznej na zasadach określonych w ustawie z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta w sposób uniemożliwiający identyfikację pacjenta, w zakresie niezbędnym do przeprowadzenia przeglądu 3) wglądu do innej dokumentacji niezbędnej do przeprowadzenia przeglądu, a w szczególności dotyczącej pracowników podmiotu udzielającego świadczeń zdrowotnych oraz struktury organizacyjnej i funkcjonowania tego podmiotu 4) prowadzenia wywiadów z pracownikami podmiotu udzielającego świadczeń zdrowotnych oraz z pacjentami.	
25.	wojewódzka komisja do spraw orzekania o zdarzeniach medycznych w zakresie prowadzonego postępowania		
26.	spadkobiercy w zakresie prowadzonego postępowania przed wojewódzką komisją do spraw orzekania o zdarzeniach medycznych		

Lp.	Kategorie uprawnionych podmiotów	Wyjaśnienie	Uwagi
27.	osoby wykonujące czynności kontrolne na podstawie art. 39 ust. 1ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, w zakresie niezbędnym do ich przeprowadzenia	Zgodnie z przywołanym artykułem minister właściwy do spraw zdrowia może zlecić przeprowadzenie jednorazowej kontroli baz danych w zakresie ochrony zdrowia oraz przekazywania danych w nich zawartych do systemu informacji instytutom badawczym, innym jednostkom organizacyjnym podległym lub nadzorowanym przez ministra właściwego do spraw zdrowia, a także specjalistom z poszczególnych dziedzin medycyny, farmacji oraz dziedzin mających zastosowanie w ochronie zdrowia, za ich zgodą.	Upoważnione osoby zwane dalej „kontrolerami” mają prawo: 1) wstępu do pomieszczeń podmiotu kontrolowanego 2) wglądu do wszelkich baz danych w zakresie ochrony zdrowia oraz dokumentów związanych z działalnością podmiotu kontrolowanego 3) żądania od pracowników podmiotu kontrolowanego udzielenia ustnych lub pisemnych wyjaśnień. W przypadku, gdy czynności podejmowane w trakcie kontroli są związane z dostępem do jednostkowych danych medycznych lub dokumentacji medycznej, mogą być realizowane wyłącznie przez osobę wykonującą zawód medyczny, właściwy ze względu na rodzaj i zakres kontrolowanych danych lub zakres udostępnianej dokumentacji medycznej. Kontrolerzy mają obowiązek zachowania w tajemnicy informacji związanych z pacjentem, w tym jednostkowych danych medycznych, a uzyskanych w związku z wykonywanymi czynnościami kontrolnymi. Ich wykorzystanie na potrzeby czynności kontrolnych może nastąpić wyłącznie w sposób uniemożliwiający identyfikację pacjenta.

Lp.	Kategorie uprawnionych podmiotów	Wyjaśnienie	Uwagi
28.	członkowie zespołów kontroli zakażeń szpitalnych, o których mowa w art. 14 ustawy z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz. U. z 2018r.poz. 151i 1669) w zakresie niezbędnym do wykonywania ich zadań	Przywołany przepis wskazuje, że: 1. kierownicy podmiotów leczniczych wykonujących działalność leczniczą w rodzaju świadczenia szpitalne są obowiązani do wdrożenia i zapewnienia funkcjonowania systemu zapobiegania i zwalczania zakażeń szpitalnych, obejmującego: 1) powołanie i nadzór nad działalnością zespołu i komitetu kontroli zakażeń szpitalnych 2) ocenę ryzyka i monitorowanie występowania zakażeń szpitalnych i czynników alarmowych 3) organizację udzielania świadczeń zdrowotnych, w sposób zapewniający: a) zapobieganie zakażeniom szpitalnym i szerzeniu się czynników alarmowych b) warunki izolacji pacjentów z zakażeniem lub chorobą zakaźną oraz pacjentów szczególnie podatnych na zakażenia szpitalne c) możliwość wykonywania badań laboratoryjnych w ciągu całej doby d) wykonywanie badań laboratoryjnych umożliwiających identyfikację biologicznych czynników chorobotwórczych wywołujących zakażenia i choroby zakaźne oraz ich weryfikację przez uprawnione podmioty e) ograniczenie narastania lekooporności biologicznych czynników chorobotwórczych w wyniku niewłaściwego stosowania profilaktyki i terapii antybiotykowej 4) monitorowanie i rejestrację zakażeń szpitalnych i czynników alarmowych 5) sporządzanie i przekazywanie właściwemu państwowemu inspektorowi sanitarnemu raportów o bieżącej sytuacji epidemiologicznej szpitala 6) zgłaszanie w ciągu 24 godzin potwierdzonego epidemicznego wzrostu liczby zakażeń szpitalnych właściwemu państwowemu inspektorowi sanitarnemu.	

Opłaty za wydawanie dokumentacji medycznej

Za udostępnienie dokumentacji medycznej może być pobierana opłata. O tym, czy takie rozwiązanie zostanie wdrożone decyduje podmiot w regulaminie organizacyjnym. Ustawodawca chcąc zapewnić dostęp do danych zawartych w dokumentacji medycznej wprowadził ograniczenia dla maksymalnej wysokości opłat za udostępnienie dokumentacji medycznej. Podstawę dla obliczenia maksymalnej, modyfikowanej co kwartał opłaty stanowi przeciętne wynagrodzenie w poprzednim kwartale, ogłaszane przez Prezesa Głównego Urzędu Statystycznego w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski" na podstawie art. 20 pkt 2 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, począwszy od pierwszego dnia miesiąca następującego po miesiącu, w którym nastąpiło ogłoszenie.

Na etapie procedowania zmian w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta w 2017 roku pojawiła się propozycja zastąpienia dotychczasowego sposobu obliczania maksymalnej wartości wyrażonej kwotowo. Ostatecznie zaniechano prac nad wdrożeniem tego rozwiązania, uznając że choć byłoby ono prostsze i czytelniejsze, prowadziłoby do konieczności dokonywania zmian maksymalnej kwoty z powodu zmiany ustawy, tj. jej przyjęcia przez Sejm, Senat oraz zatwierdzenia przez Prezydenta.

Maksymalna wysokość opłaty wynosi zatem odpowiednio:

1) za jedną stronę wyciągu albo odpisu dokumentacji medycznej – 0,002 przeciętnego wynagrodzenia
2) za jedną stronę kopii albo wydruku dokumentacji medycznej – 0,00007 przeciętnego wynagrodzenia
3) udostępnienie dokumentacji medycznej na informatycznym nośniku danych – nie może przekraczać 0,0004 przeciętnego wynagrodzenia.

Wysokość opłaty uwzględnia podatek od towarów i usług, jeżeli na podstawie odrębnych przepisów usługa jest opodatkowana tym podatkiem. Opłata za stronę jest obliczana niezależnie od formatu strony (np. A4 lub A5). Niedopuszczalne jest również pobieranie dodatkowych opłat nieprzewidzianych w przepisach, np. za poświadczenie dokumentacji medycznej za zgodność z oryginałem.

Dodatkowo 4 maja 2019 r. zmieniły się zasady pobierania opłat za wydanie dokumentacji medycznej – zgodnie z nowymi przepisami pacjent lub przedstawiciel ustawowy pacjenta otrzymuje dokumentację medyczną za darmo po raz pierwszy w żądanym zakresie. Opłatę za wydanie dokumentacji można pobierać jedynie:

- od pacjenta wnioskującego o dokumentację po raz kolejny w żądanym zakresie
- od przedstawiciela ustawowego wnioskującego o dokumentację po raz kolejny w żądanym zakresie.

Przyjmuje się, że wniosek osoby upoważnionej przez pacjenta może stanowić wypełnienie woli pacjenta, w szczególności pacjenta niepełnosprawnego co do pozyskania dokumentacji celem przekazania mu, a zatem również i w takim przypadku należy odstąpić od pobierania opłaty.

Wydawanie dokumentacji medycznej po śmierci pacjenta

Zarówno w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta, jak i w RODO pojawia się postulat należytego zabezpieczenia danych przed dostępem osób nieuprawnionych, ze szczególnym akcentem na dane medyczne. Z drugiej jednak strony pacjent może chcieć zabezpieczyć swoje interesy lub osób mu bliskich przez wskazanie członków rodziny lub innych osób, które obdarza zaufaniem jako uprawnionych do zapoznawania się z jego dokumentacją medyczną.

Osoby bliskie zostały wskazane w ustawie. Od 9 lutego 2019 roku, po zmianie definicji ustawowej do kręgu osób bliskich zalicza się małżonka, krewnego do drugiego stopnia lub powinowatego do drugiego stopnia w linii prostej, przedstawiciela ustawowego, osobę pozostającą we wspólnym pożyciu lub osobę wskazaną przez pacjenta.

Obecnie dostęp do dokumentacji medycznej jako krewni i powinowaci mają:

1. Krewni – linia prosta

Pierwszy stopień pokrewieństwa: 1) ojciec 2) matka 3) syn 4) córka

Drugi stopień pokrewieństwa: 1) dziadek 2) babka 3) wnuk 4) wnuczka

Krewni – linia boczna

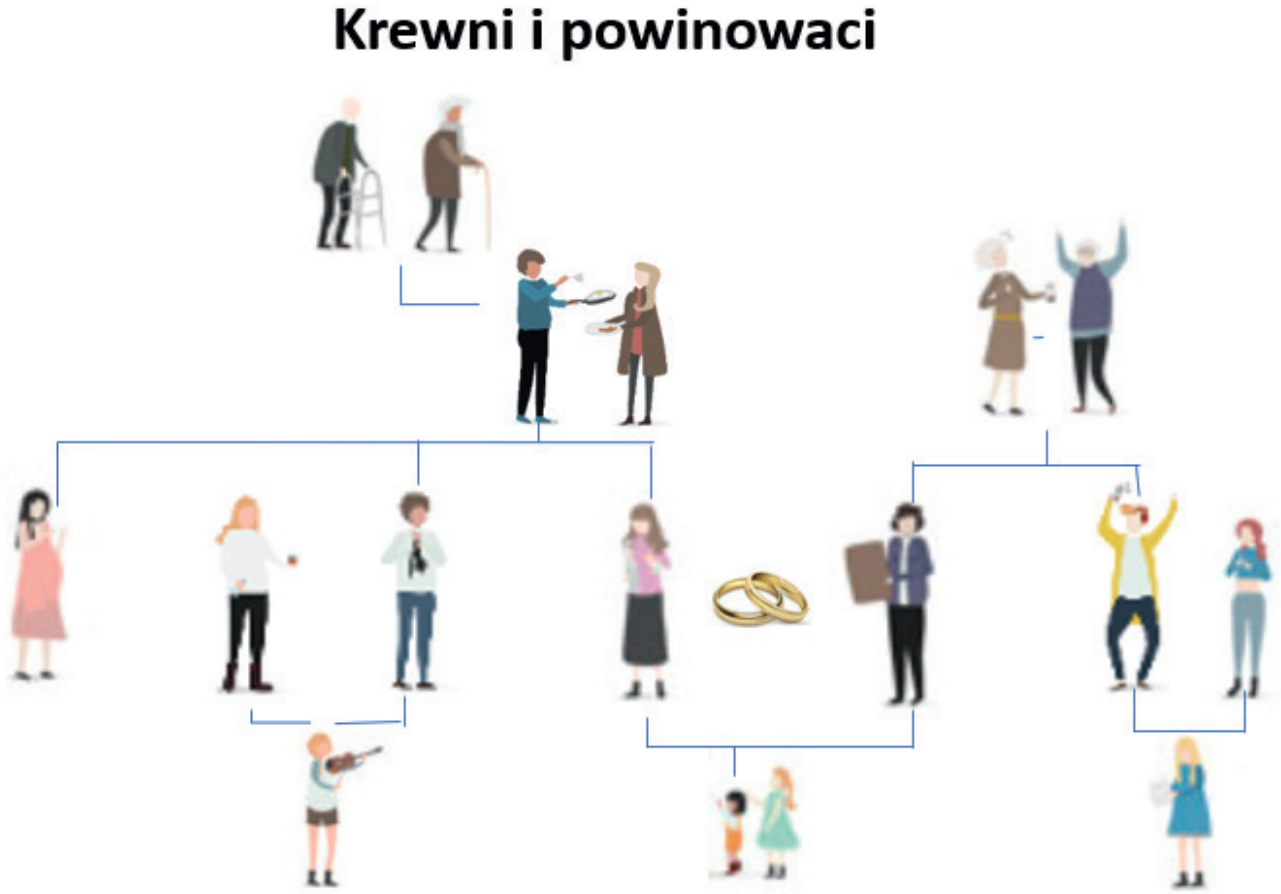
Tu nie ma pierwszego stopnia

Drugi stopień pokrewieństwa w linii bocznej: 1) brat 2) siostra

2. Powinowaci – linia prosta

Pierwszy stopień: 1) ojciec męża/ojciec żony (zwyczajowo teść) 2) matka męża/matka żony (zwyczajowo teściowa) 4) mąż córki (zwyczajowo zięć) 5) żona syna (zwyczajowo synowa)

Drugi stopień: 1) dziadek męża/dziadek żony 2) babka męża/babka żony 3) mąż wnuczki 4) żona wnuka.



Wskutek zmian w ustawie, obowiązujących od 9 lutego 2019 roku, po śmierci pacjenta dokumentacja medyczna jest udostępniana osobie upoważnionej przez pacjenta za życia lub osobie, która w chwili zgonu pacjenta była jego

przedstawicielem ustawowym. Dokumentacja medyczna jest udostępniana także osobie bliskiej, chyba że udostępnieniu sprzeciwi się inna osoba bliska lub sprzeciwił się temu pacjent za życia. Jeżeli jednak doszłoby do sporu między osobami bliskimi o udostępnienie dokumentacji medycznej, zgodę na udostępnienie wyraża sąd w postępowaniu nieprocesowym na wniosek osoby bliskiej lub osoby wykonującej zawód medyczny. Osoba wykonująca zawód medyczny zyskała również uprawnienie do wystąpienia do sądu również w przypadku uzasadnionych wątpliwości, czy osoba występująca o udostępnienie dokumentacji lub sprzeciwiająca się jej udostępnieniu jest osobą bliską.

Sprzeciw pacjenta nie ma charakteru bezwzględnego. W przypadku gdy pacjent za życia sprzeciwił się udostępnieniu dokumentacji medycznej, sąd w postępowaniu nieprocesowym, na wniosek osoby bliskiej, może wyrazić zgodę na udostępnienie dokumentacji medycznej i określić zakres jej udostępnienia, jeżeli jest to niezbędne:

1) w celu dochodzenia odszkodowania lub zadośćuczynienia, z tytułu śmierci pacjenta
2) dla ochrony życia lub zdrowia osoby bliskiej.

W przypadku wystąpienia do sądu z jednym z wniosków, o których mowa powyżej, sąd bada:

1) interes uczestników postępowania
2) rzeczywistą więź osoby bliskiej ze zmarłym pacjentem
3) wolę zmarłego pacjenta
4) okoliczności wyrażenia sprzeciwu.

Niezwykle istotne jest zatem opracowanie prawidłowego formularza sprzeciwu, który pacjent będzie mógł złożyć. Na formularzu powinna znaleźć się przede wszystkim informacja o celu zgłaszania sprzeciwu. Samo niewskazanie osoby upoważnionej do dostępu do dokumentacji medycznej nie jest równoznaczne ze sprzeciwem pacjenta.

Prowadzenie wykazu udostępnianej dokumentacji medycznej

Od 11 maja 2017 roku zaczęły obowiązywać przepisy[21], które wprowadziły do ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta zapis o obowiązku prowadzenia wykazu dokumentującego fakt udostępnienia dokumentacji medycznej. Wprowadzenie obowiązkowego wykazu uzasadniano koniecznością kontroli nad prawidłowością realizowanych wniosków o udostępnienie dokumentacji medycznej. Wskazywano, że potrzebę doprecyzowania przepisów dostrzegła NIK w zaleceniach pokontrolnych po przeprowadzonej kontroli pn. „Tworzenie i udostępnianie dokumentacji medycznej”[22]. Wobec braku dostatecznych rozwiązań na poziomie ogólnym i niesprecyzowania systemowo sposobu udostępniania dokumentacji medycznej, świadczeniodawcy przyjmują w swojej działalności różne rozwiązania organizacyjne, nie zawsze korzystne dla pacjentów. W szczególności brakowało nadzoru nad procesem i jednolitych w całym podmiocie leczniczym rozwiązań, a składanie i rozpatrywanie wniosków często utrudniały przeszkody organizacyjne znacznie wydłużające czas realizacji wniosku. Rzadko wnioski o udostępnienie dokumentacji medycznej były zbierane w usystematyzowanym układzie, częstym błędem było również wpisywanie informacji o udostępnionej dokumentacji bezpośrednio w treści dokumentów.

Po nowelizacji podmiot udzielający świadczeń zdrowotnych prowadzi wykaz zawierający następujące informacje dotyczące udostępnianej dokumentacji medycznej:

1) imię (imiona) i nazwisko pacjenta, którego dotyczy dokumentacja medyczna
2) sposób udostępnienia dokumentacji medycznej
3) zakres udostępnionej dokumentacji medycznej

---

[21] Ustawa z dnia 23 marca 2017 r. o zmianie ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz niektórych innych ustaw (Dz.U. 2017 poz. 836).

[22] .....UZUPEŁNIĆ

4) imię (imiona) i nazwisko osoby innej niż pacjent, której została udostępniona dokumentacja medyczna, a w przypadkach udostępniania dokumentacji wnioskodawcom instytucjonalnym także nazwę uprawnionego organu lub podmiotu
5) imię (imiona) i nazwisko oraz podpis osoby, która udostępniła dokumentację medyczną
6) datę udostępnienia dokumentacji medycznej.

Wzór wykazu musi zostać opracowany według powyższych wskazań – niezależnie od przyjętej formy – tekstu ciągłego czy tabelarycznej. Nie może zawierać innych danych osobowych, takich jak np. nr dowodu osobistego. Nie można również wymagać kwitowania odbioru dokumentacji medycznej poprzez złożenie podpisu, ustawa nie przewidziała bowiem takiej możliwości.

Wykaz musi być należycie zabezpieczony. Ewentualne zniszczenie będzie bowiem skutkowało brakiem możliwości ustalenia, kto i w jakim zakresie uzyskał dokumentację medyczną. Kradzież wykazu może z kolei doprowadzić do niekorzystnego rozporządzenia danymi osobowymi osób wymienionych w tej ewidencji. Co więcej, wobec istnienia pojedynczego egzemplarza wykazu, nie ma możliwości ustalenia nawet przybliżonego kręgu osób, których może dotyczyć naruszenie.

Przykład:

Rejestracja w Ośrodku Zdrowia, żeby usprawnić sobie pracę związaną z prowadzeniem wykazu udostępnionej dokumentacji medycznej, postanowiła zastąpić papierowy wykaz plikiem w arkuszu kalkulacyjnym w komputerze. Podczas audytu prowadzenie wykazu w takiej formie oceniono jako nieprawidłowe.

Wyjaśnienie

Prowadzenie wykazu w systemie informatycznym z pewnością zapewnia większą czytelność i łatwość wyszukiwania danych, jednak przepisy jasno wskazują na podpis osoby wydającej jako jeden z obligatoryjnych elementów. Wobec tego nie ma możliwości, by wykaz funkcjonował bez autoryzacji przez osobę dokonującą udostępnienia. Można natomiast rozważyć umieszczanie danych w pliku, drukowanie i podpisywanie przez właściwą osobę.

Przykład:

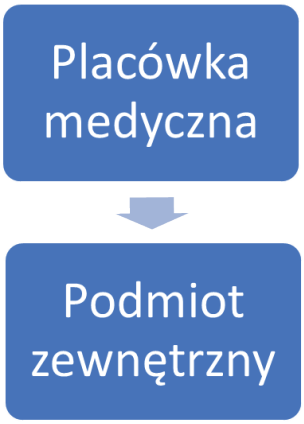
Sekretariat przychodni prowadzi segregator z wnioskami pacjentów i osób trzecich o udostępnienie dokumentacji medycznej. Wnioski są przyjmowane w przypadku wydawania kopii lub wydruku. W przychodni nigdy nie zdarzyło się, by poproszono o odpis, a wgląd jest realizowany podczas wizyty u lekarza. Wnioski przychodzące z instytucji znaleźć można w rejestrze korespondencji przychodzącej.
Przygotowując się do akredytacji i dokonując przeglądu procedur, dyrektor przychodni zaczął się zastanawiać, czy przyjęte rozwiązania są wystarczające.

Wyjaśnienie

Przepisy jasno wskazują, że chodzi o prowadzenie wykazu, a nie zbioru wniosków. Oczywiście same wnioski również stanowią istotną wartość dla celów dowodowych w razie roszczeń pacjentów, czy kontroli uprawnionych organów. Jednak wykaz służy właśnie temu, by zebrać dane dotyczące udostępnień – zarówno tych na rzecz pacjentów i osób przez nich upoważnionych, jak i instytucji. W razie ujawnienia dokumentacji medycznej pacjenta łatwej będzie ustalić, czy istnieje ewentualność, że dokumentację uzyskiwały wcześniej inne podmioty, które mogły ją upublicznić. Należy zauważyć, że wgląd do oryginału dokumentacji również jest formą jej udostępnienia i powinien być odnotowany w wykazie, zwłaszcza że można podczas tej czynności wykonywać zdjęcia dokumentacji. Trzeba być przygotowanym na wniosek o odpis, taki wniosek należy odpowiednio przyjąć i przygotować dokument dla wnioskującego podmiotu.

Rozdział IX. Współpraca placówki medycznej z podmiotami zewnętrznymi przy przekazywaniu danych osobowych

Powierzenie danych osobowych



W ramach działalności placówki medycznej może dochodzić do przekazywania danych osobowych zewnętrznemu podmiotowi. Najczęściej takie przekazywanie następuje od placówki medycznej na zewnątrz, a podmiot zewnętrzny używa danych w celach wskazanych przez placówkę medyczną. Dochodzi wówczas do powierzenia danych osobowych.

Przy każdym powierzeniu danych osobowych mamy dwie strony: administratora danych i podmiot przetwarzający (procesora). Administrator danych decyduje o tym jak i do jakich celów wykorzystywać dane osobowe. Procesor realizuje te cele. Relacja między podmiotami jest pionowa (jak na powyższym schemacie).

Placówka medyczna korzysta z systemu informatycznego do obsługi pacjentów. Firma, która dostarczyła system, zajmuje się też jego aktualizacją, konserwacją itp. działaniami. W związku z tymi działaniami ma dostęp do danych osobowych pacjentów. **Firma nie może używać tych danych w wybrany przez siebie sposób, ponieważ nie jest ich administratorem**.

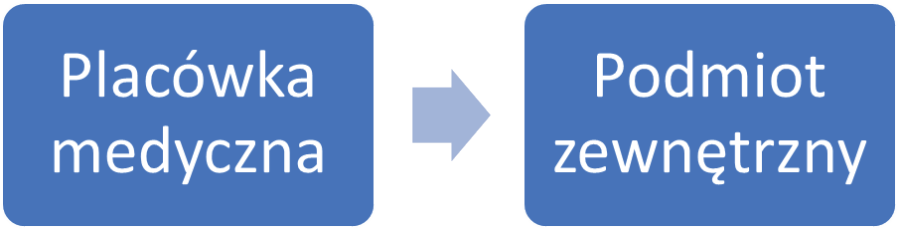
Kiedy należy zawrzeć umowę powierzenia

Poniżej wskazano kategorie podmiotów, z którymi placówka medyczna powinna co do zasady (po konsultacji z IOD) zawrzeć umowę powierzenia:

- firmy informatyczne
- firmy księgowe
- firmy kadrowe
- podmioty zajmujące się archiwizacją dokumentacji
- firmy zajmujące się niszczeniem dokumentów
- firmy prowadzące szkolenia BHP.

Kiedy nie należy zawierać umowy powierzenia

Umowy powierzenia nie zawiera się w sytuacji, gdy nie dochodzi do powierzenia danych osobowych. Tak dzieje się najczęściej wtedy, gdy placówka medyczna i podmiot zewnętrzny wykorzystują dane osobowe – ale jako oddzielni administratorzy. Każdy z nich ma oddzielne prawa i obowiązki związane z danymi. Taki sposób przekazywania danych nazywamy udostępnieniem danych osobowych. Relacja między podmiotami jest wtedy pozioma (równorzędna).



Przykładem udostępnienia danych osobowych jest współpraca w ramach medycyny pracy.

> *Jednym z obowiązków pracodawcy, zgodnie z przepisami prawa pracy, jest kierowanie osób zatrudnionych na badania lekarskie. Artykuł 229 Kodeksu pracy wskazuje w szczególności, że pracodawca może dopuścić do pracy jedynie osobę posiadającą aktualne orzeczenie lekarskie, a wszelkie badania tego typu (wstępne, okresowe, kontrolne) odbywają się na podstawie skierowania wydanego przez pracodawcę. Regulacja ta jednoznacznie przesądza, że to pracodawca – w odniesieniu do danych pracowników kierowanych na badania – jest ich administratorem w rozumieniu przepisów ogólnego rozporządzenia o ochronie danych (RODO).*
>
> *Opisane wyżej badania lekarskie są realizowane przez odrębny podmiot – placówkę medyczną, świadczącą usługi z zakresu medycyny pracy. Ustawa o służbie medycyny pracy określa, że badania wstępne, okresowe i kontrolne pracowników oraz inne świadczenia zdrowotne są wykonywane na podstawie pisemnej umowy między pracodawcą a placówką medyczną – umowa powinna określać w szczególności osoby objęte świadczeniami z tytułu umowy. Obowiązek przekazania danych osobowych pracowników i osób przyjmowanych do pracy wynika zatem z przywołanych przepisów.*
>
> *Jednostka medycyny pracy staje się zatem odrębnym administratorem wobec tych danych osobowych, przetwarza bowiem szerszy zakres informacji na temat tych osób. Artykuł 11 przywołanej ustawy o służbie medycyny pracy zobowiązuje taką jednostkę do prowadzenia dokumentacji medycznej, która zawiera – poza informacjami przekazanymi przez pracodawcę – inne dane, w tym przede wszystkim dotyczące zdrowia pracowników i osób przyjmowanych do pracy.*
>
> *Co więcej, pracodawca nie ma nawet prawa przetwarzania danych w takim zakresie, stałoby to bowiem w sprzeczności z art. 22[1] Kodeksu pracy, który zawiera zamkniętą listę informacji, o pracowniku i osobie przyjmowanej do pracy, jakie pracodawcy wolno przetwarzać. Danych wrażliwych o stanie zdrowia tam nie znajdziemy, nie mogą więc trafić do pracodawcy.*
>
> *- Medycyna pracy – dlaczego to nie powierzenie danych?*[23]

[23] *Medycyna pracy – dlaczego to nie powierzenie danych*, https://jamano.pl/2018/10/25/medycyna-pracy-powierzenie-danych/ (dostęp 28.11.2019 r.).

Identyczne stanowisko zajął 4 października 2018 r. Prezes Urzędu Ochrony Danych Osobowych.

Czy kierując pracowników na badania profilaktyczne pracodawca musi zawrzeć z jednostką służby medycyny pracy umowę powierzenia?

Nie. Pracodawca i podstawowa jednostka służby medycyny pracy zawierając umowę, o której mowa powyżej, działają niezależnie od siebie (każdy z nich samodzielnie ustala cele i środki przetwarzania danych osobowych). A zatem są oddzielnymi administratorami danych.

- Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców[24]

Umowy powierzenia nie podpisuje się także z placówką oświatową, gdzie pielęgniarka lub higienistka opiekuje się dziećmi. Ani szkoła, ani ośrodek zdrowia nie znajdują się tu na pozycji podrzędnej. Także i tu występuje dwóch administratorów.

Obowiązek właściwego przechowywania dokumentacji medycznej ciąży na podmiocie leczniczym świadczącym opiekę zdrowotną w szkole. Zasady obchodzenia się z tego typu dokumentacją określają zwłaszcza przepisy ustawy o prawach pacjenta oraz rozporządzenia wykonawcze. W związku z niezależnością świadczenia opieki zdrowotnej, zarówno szkołę, jak i podmiot leczniczy należy traktować jako odrębnych administratorów danych, którzy sami, każdy w swoim zakresie i celu, określają sposoby przetwarzania danych osobowych.

- Ochrona danych osobowych w szkołach i placówkach oświatowych. Poradnik RODO[25]

Trzecim, często występującym typem współpracy, który nie wymaga powierzenia danych, jest współpraca z laboratoriami diagnostycznymi lub innymi placówkami medycznymi (dla zachowania ciągłości usług medycznych). Także i tu jest dwóch administratorów, a każdy z nich ma swój zbiór obowiązków.

O czym pamiętać w umowie powierzenia?

Art. 28 ust. 3 RODO opisuje, jak ma wyglądać umowa powierzenia.

Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

[24] Urząd Ochrony Danych Osobowych, *Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców*, https://uodo.gov.pl/pl/file/1469 (dostęp 28.11.2019 r.).

[25] Urząd Ochrony Danych Osobowych, *Ochrona danych osobowych w szkołach i placówkach oświatowych. Poradnik RODO*, https://uodo.gov.pl/pl/file/1388 (dostęp 28.11.2019 r.).

a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

c) podejmuje wszelkie środki wymagane na mocy art. 32;

d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4;

e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III;

f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36;

g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;

h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

§

- art. 28 ust. 3 RODO

Tłumacząc to z prawniczego na polski – z umowy powierzenia musi wynikać, że:

- osoby, z pomocą których podmiot przetwarzający będzie realizować umowę, zachowają w tajemnicy dane osobowe
- podmiot przetwarzający będzie stosował odpowiednie środki techniczne i organizacyjne, by zapewnić bezpieczeństwo danych
- podmiot przetwarzający będzie posługiwał się podwykonawcami w takim zakresie, jaki ustalił z administratorem
- podmiot przetwarzający będzie wspierał administratora przy obsłudze wniosków o dostęp do danych, sprostowanie, prawo do bycia zapomnianym itp.
- podmiot przetwarzający wspiera administratora w realizacji obowiązków dotyczących zgłaszania naruszeń – między innymi sam będzie odpowiednio szybko zgłaszał naruszenia
- po zakończeniu umowy powierzenia dane zostaną zniszczone lub zwrócone administratorowi (chyba że przepis prawa mówi coś innego)
- podmiot przetwarzający da administratorowi możliwość sprawdzenia, czy podmiot właściwie dba o dane osobowe.

Najbezpieczniej jest, gdy placówka medyczna ma swój własny wzór umowy powierzenia, którego używa przy zawieraniu umów. Nie zawsze jednak używanie takiego wzoru będzie możliwe. Należy wówczas uważnie przeczytać umowę powierzenia (w to zadanie powinien być zaangażowany IOD) i zwrócić uwagę zwłaszcza na te kwestie:

Zdjęcie: Amanda Jones, Unsplash (https://unsplash.com/photos/CcIIao_-Eow)

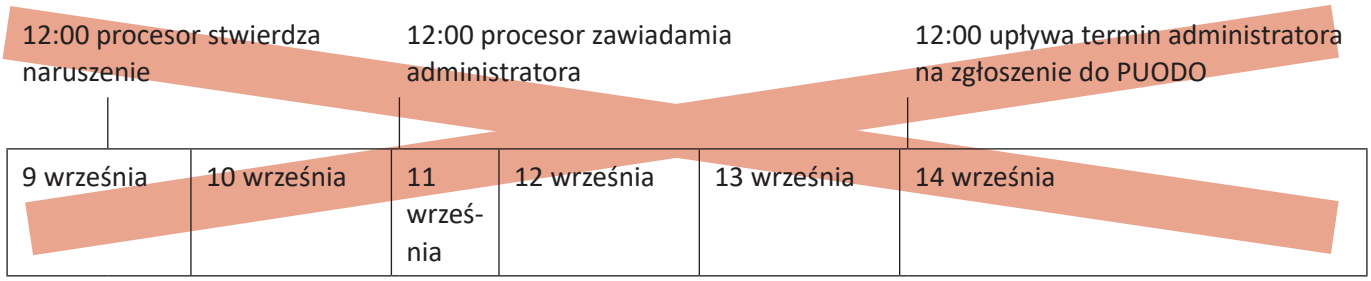
- czas na zgłaszanie naruszeń

Ile czasu – zgodnie z umową – ma procesor na zgłoszenie naruszenia administratorowi? Należy pamiętać, że 72 godziny, jakie administrator ma na zgłoszenie poważnego incydentu do PUODO, liczą się od momentu, gdy naruszenie stwierdził procesor, a nie od momentu, gdy procesor zawiadomił o tym administratora!

Poprawny sposób liczenia terminu na zgłoszenie naruszenia

12:00 procesor stwierdza naruszenie		12:00 procesor zawiadamia administratora	12:00 upływa termin administratora na zgłoszenie do PUODO
9 września	10 września	11 września	12 września

Niepoprawny sposób liczenia terminu na zgłoszenie naruszenia



W związku z tym zasadne jest, aby procesor zgłaszał administratorowi naruszenia niezwłocznie, nie później jednak niż w ciągu 36 godzin zegarowych.

- **zakres odpowiedzialności** – obowiązki procesora, wynikające z umowy, powinny ściśle odpowiadać temu, co zapisano w art. 28 ust. 3 RODO
- **kary umowne** – wiele podmiotów proponuje wprowadzenie kar umownych (w postaci konkretnych sum lub procentu wynagrodzenia) za naruszanie warunków umowy; umowę w tym zakresie warto przekazać prawnikowi lub kancelarii prawnej
- **tabela zgodności** – jeden z sugerowanych przez nas sposobów weryfikacji przestrzegania przez procesora przepisów o ochronie danych; szerzej opisany w dalszej części publikacji
- **możliwość prowadzenia audytu** – jeden z sugerowanych przez nas sposobów weryfikacji przestrzegania przez procesora przepisów o ochronie danych; szerzej opisany w dalszej części publikacji
- **zwrot lub niszczenie danych po zakończeniu współpracy** – z umowy powinno jasno wynikać, co stanie się z danymi osobowymi, które przetwarzał procesor.

Forma umowy powierzenia

Obowiązek z art. 28 ust. 3 RODO najczęściej spełnia się przez zawarcie oddzielnej umowy powierzenia. Nie jest to jednak jedyna dopuszczalna forma. Treść dotyczącą powierzenia można zawrzeć także:

- **bezpośrednio w umowie głównej** (nie jest określone, w której części umowy musi się znaleźć, ani jaki ma mieć numer. Zalecamy jednak, aby nie umieszczać tego paragrafu ani na początku, ani na końcu umowy)
- **w aneksie do umowy głównej**.

Jak zagwarantować właściwe wykorzystanie danych przez podmiot zewnętrzny

Administrator danych co do zasady jeszcze przed zawarciem umowy powierzenia powinien wybrać taki podmiot, który daje gwarancje przestrzegania przepisów o ochronie danych. Nie zawsze jednak takie sprawdzenie jest możliwe. Poniżej omawiamy inne środki, jakie można wtedy wykorzystać.

Tabela zgodności

Tzw. tabelę zgodności można stosować zarówno przed zawarciem umowy powierzenia, jak i w okresie, gdy taka umowa jest podpisana i już obowiązuje. Procesor placówki medycznej odpowiada na szereg pytań (w zależności od rodzaju podmiotu i charakteru współpracy może być ich więcej lub mniej). Z odpowiedzi wynika, czy spełnia kryteria wynikające z RODO.

Poniżej znajduje się przykładowa tabela zgodności, obejmująca następujące obszary: IOD, dokumentacja przetwarzania danych, prawa osób, współpraca z podmiotami zewnętrznymi.

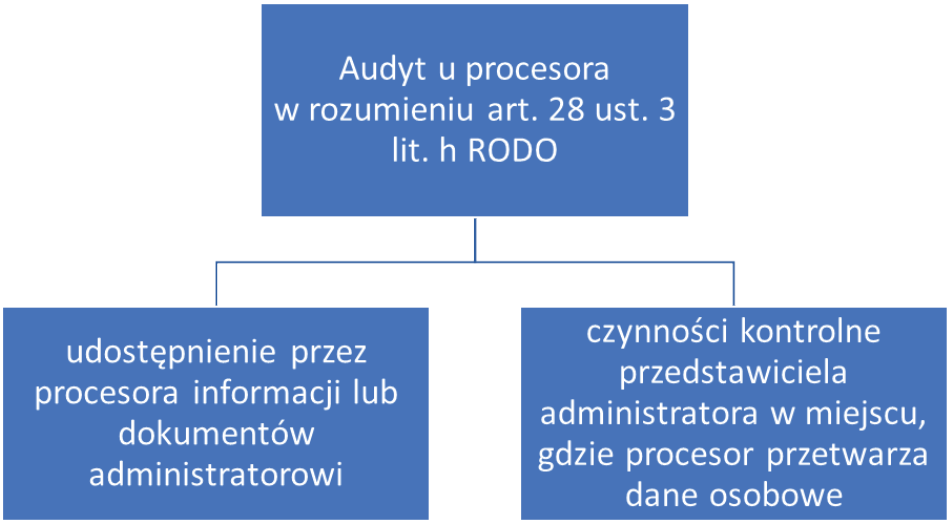
LP.	OBSZAR	INFORMACJE DOTYCZĄCE SPEŁNIENIA WYMAGAŃ		
		TAK	NIE	SZCZEGÓŁY
INSPEKTOR OCHRONY DANYCH (IOD)				
1	Czy Podmiot przetwarzający wyznaczył IOD?	☐	☐	*Jeżeli nie wyznaczono IOD, należy uzasadnić tę decyzję.*
DOKUMENTACJA PRZETWARZANIA DANYCH				
2	Czy Podmiot przetwarzający wdrożył politykę z zakresu ochrony danych osobowych?	☐	☐	*Jeżeli nie wykonano tego obowiązku, należy uzasadnić sytuację i wskazać planowany termin realizacji obowiązku.*
3	Czy Podmiot przetwarzający wdrożył procedurę postępowania w sytuacji naruszenia bezpieczeństwa powierzonych danych osobowych (w tym informowania Administratora o incydentach)?	☐	☐	*Jeżeli nie wykonano tego obowiązku, należy uzasadnić sytuację i wskazać planowany termin realizacji obowiązku.*
4	Czy Podmiot przetwarzający wdrożył procedurę zarządzania ryzykiem naruszenia praw i wolności osób, których dotyczą powierzone dane osobowe?	☐	☐	*Jeżeli nie wykonano tego obowiązku, należy uzasadnić sytuację i wskazać planowany termin realizacji obowiązku.*

5	Czy osoby mające po stronie Podmiotu przetwarzającego dostęp do powierzonych danych osobowych posiadają stosowne upoważnienia do przetwarzania danych osobowych oraz zobowiązały się do zachowania informacji w tajemnicy?	☐	☐	*Jeżeli nie wykonano tego obowiązku, należy uzasadnić sytuację i wskazać planowany termin realizacji obowiązku.*
PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ				
6	Czy Podmiot przetwarzający wdrożył procedury reakcji na żądania, o których mowa w rozdziale III RODO, składane przez osoby, których dotyczą powierzone dane osobowe?	☐	☐	*Jeżeli nie wykonano tego obowiązku, należy uzasadnić sytuację i wskazać planowany termin realizacji obowiązku.*
WSPÓŁPRACA Z PODMIOTAMI ZEWNĘTRZNYMI (PODPROCESORAMI)				
7	Czy Podmiot przetwarzający korzysta z usług podprocesorów?	☐	☐	
8	Czy Podmiot przetwarzający korzysta z usług podprocesorów, którzy przetwarzają dane poza granicami Europejskiego Obszaru Gospodarczego (EOG)?	☐	☐	*Jeżeli taka współpraca ma miejsce, należy wskazać konkretne kraje.*

Audyt u procesora

W trakcie obowiązywania umowy powierzenia administrator może zrealizować u procesora audyt, mający na celu sprawdzenie przestrzegania przez niego przepisów o ochronie danych.

RODO nie określa, jak ma wyglądać taki audyt. W praktyce możliwe są dwa rozwiązania:



W umowie powierzenia warto zapisać, jak może wyglądać taki audyt, co obejmuje i jakie rodzi skutki dla procesora – zwłaszcza gdy formą audytu są czynności kontrolne. Poniżej wymieniamy listę zagadnień, które powinny być ujęte:

- jak wcześnie administrator uprzedza procesora o zamiarze przeprowadzenia czynności kontrolnych – może to być np. 7 dni
- w jakich godzinach mogą odbywać się czynności kontrolne – mogą to być np. godz. 10:00-16:00 w dni powszednie
- jakie działania może realizować przedstawiciel w ramach czynności kontrolnych – przykładowo:
  - sporządzanie notatek z czynności
  - odbieranie wyjaśnień od osób przetwarzających dane osobowe
  - wykonywanie kopii otrzymywanych dokumentów
  - sporządzanie kopii obrazu wyświetlanego na ekranie monitora
  - sporządzanie kopii zapisów rejestru systemu IT, którego procesor używa do przetwarzania danych osobowych
- kto ponosi koszty audytu – administrator czy procesor
- jak ma się zakończyć audyt – np. wskazaniem ewentualnych niedociągnięć, które procesor musi poprawić w określonym czasie.

Konsekwencje braku umowy na wykorzystanie danych osobowych

Jeżeli umowa powierzenia danych osobowych nie będzie podpisana, gdy z przepisów wynika, że trzeba ją zawrzeć, rodzi to problemy i dla administratora, i dla procesora. Administrator przekazuje dane zewnętrznemu podmiotowi bezpodstawnie, podobnie procesor wykorzystuje dane osobowe bez podstawy prawnej.

Podpisanie umowy powierzenia leży zatem w interesie obu stron. Nie ma znaczenia, czy to administrator, czy procesor zaproponuje podpisanie umowy.

Jedną z konsekwencji niepodpisania umowy powierzenia może być administracyjna kara pieniężna. 30 października 2019 r. Prezes UODO ogłosił nałożenie takiej kary – w wysokości 40.000 zł - na Burmistrza Aleksandrowa Kujawskiego. Jedną z przyczyn nałożenia kary było właśnie niezawarcie umowy powierzenia.

W przypadku udostępnienia danych osobowych bez podstawy prawnej (bez uprzednio zawartej umowy powierzenia), następuje naruszenie zasady zgodności z prawem (art. 5 ust. 1 lit. a) ogólnego rozporządzenia o ochronie danych oraz zasady poufności (art. 5 ust. 1 lit. f) ogólnego rozporządzenia o ochronie danych. Burmistrz nie zachował powyższych zasad zlecając prowadzenie BIP ww. podmiotom bez uprzedniego zawarcia umów powierzenia danych. Dopuścił tym samym do braku kontroli nad prawidłowością procesu przetwarzania danych zawartych w BIP i nie wykazał, że następuje on przy spełnieniu wymogów wynikających z przepisów ogólnego rozporządzenia o ochronie danych. W konsekwencji należy również uznać, że Burmistrz w tym zakresie naruszył także zasadę rozliczalności, wynikającą z art. 5 ust. 2 ogólnego rozporządzenia o ochronie danych.

- decyzja Prezesa UODO nr ZSPU.421.3.2019 z dnia 18 października 2019 r.[26]

Niepodpisywanie umów powierzenia (lub braki z nimi związane) było także przedmiotem zastrzeżeń przedstawicieli Najwyższej Izby Kontroli. 14 listopada 2019 r. NIK przedstawiła wyniki sprawdzenia dotyczącego przestrzegania przepisów o ochronie danych osobowych w szpitalach.

Podmioty lecznicze były obowiązane do zawierania pisemnych umów powierzenia przetwarzania danych, gdy udostępniają takie dane podmiotom zewnętrznym. W pięciu ze skontrolowanych szpitali (21%) stwierdzono błędy w tym zakresie. Polegały one głównie na: niepodpisaniu niektórych z umów powierzenia przetwarzania danych, nieprzestrzeganiu uregulowań wewnętrznych podmiotów leczniczych dotyczących wymogów formalnych wobec umów oraz konieczności prowadzenia ich ewidencji, wskazaniu w umowie niewłaściwego zakresu danych osobowych, jakiego powierzenie dotyczyło.

- Informacja o wynikach kontroli WDROŻENIE PRZEZ PODMIOTY LECZNICZE REGULACJI DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH[27]

[26] Decyzja Prezesa UODO nr ZSPU.421.3.2019 z dnia 18 października 2019 r. https://uodo.gov.pl/decyzje/ZSPU.421.3.2019 (dostęp dn. 22.11.2019 r.).

[27] Najwyższa Izba Kontroli, Informacja o wynikach kontroli WDROŻENIE PRZEZ PODMIOTY LECZNICZE REGULACJI DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH LBI.430.004.2019, https://www.nik.gov.pl/plik/id,21467,vp,24109.pdf (dostęp dn. 22.11.2019 r.).

Rozdział X. Organizacja pracy placówki medycznej a bezpieczeństwo administratora

Modele współpracy placówek medycznych

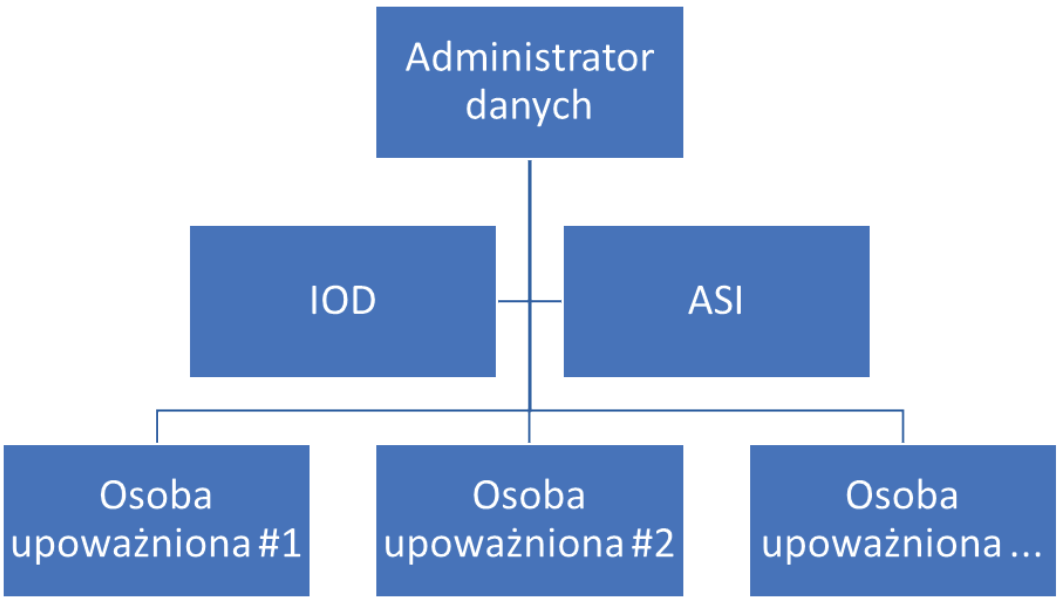
Najczęściej mamy do czynienia z sytuacją, gdy np. w jednym budynku jest jedna placówka medyczna. Jasne jest wtedy, kto odpowiada za rejestrację, sprzęt, dokumentację medyczną itp. kwestie. Problem pojawia się w sytuacji, gdy w jednym budynku mieści się większa liczba takich placówek. Bardzo często (przede wszystkim w mniejszych miejscowościach i ze względu na oszczędności) urządza się wtedy pracę wspólnie: jest jedna rejestracja, w gabinetach przechowuje się dokumentację wielu placówek medycznych, podpisuje się wspólne umowy na niszczenie dokumentacji…

Niezależnie od warunków pracy należy pamiętać o tym, że każdy podmiot leczniczy jest w tej sytuacji oddzielnym administratorem danych. Oznacza to, że pomimo korzystania ze wspólnej przestrzeni, sprzętu lub personelu każda placówka medyczna będzie osobno rozliczana z obowiązków związanych z ochroną danych osobowych. Praktyczne konsekwencje takiego rozróżnienia to np.:

- konieczność wydzielenia szaf, szafek lub szuflad w taki sposób, aby jasne było, gdzie znajduje się dokumentacja konkretnej placówki medycznej
- nadanie pracownikowi rejestracji upoważnień do przetwarzania danych osobowych od wszystkich administratorów danych
- założenie oddzielnych kont użytkowników w aplikacjach, programach lub systemach informatycznych.

Podział obowiązków dotyczących ochrony danych osobowych

Jak wskazano w rozdziałach I, VI i IX, odpowiedzialność za ochronę danych osobowych spoczywa przede wszystkim na placówce medycznej. Nie oznacza to oczywiście, że kierownictwo podmiotu medycznego wykonuje wszystkie operacje przetwarzania i działania ochronne. Tak jak na gruncie służbowym istnieje podział praw, obowiązków i odpowiedzialności, tak samo podobny podział istnieje w zakresie bezpieczeństwa informacji.



Nadrzędną rolę pełni oczywiście **administrator danych** (kierownictwo placówki medycznej). On wdraża dokumentację, zarządza okresowe audyty, zapewnienia szkolenie pracowników i odpowiada przed organami kontrolnymi (na czele z PUODO) za wypełnianie obowiązków wynikających z RODO.

Inspektor ochrony danych (jego wyznaczenie jest obowiązkowe dla większości placówek medycznych) oraz administrator systemów informatycznych (jego wyznaczenie nie jest obowiązkowe, ale zalecane) pełnią role doradcze. Dzięki swojej wiedzy i doświadczeniu są w stanie przedstawiać rozwiązania zmniejszające ryzyka, udzielać odpowiedzi na trudne pytania, przygotowywać odpowiednie dokumenty i procedury czy poprowadzić szkolenie. **Nie podejmują jednak ostatecznych decyzji – te należą do administratora danych.**

Osoby upoważnione mają dostęp do danych osobowych, wynikający z zakresu obowiązków. Ich zadaniem jest przestrzeganie zasad wynikających z dokumentacji, procedur i zaleceń inspektora ochrony danych (popartych autorytetem administratora danych). **Bardzo istotnym obowiązkiem osób upoważnionych jest zwłaszcza zgłaszanie naruszeń (lub podejrzeń naruszeń) ochrony danych osobowych.**

W rozdziale III wskazujemy, jakie konsekwencje dla pracowników może rodzić nieprzestrzeganie zasad ochrony danych osobowych.

Przechowywanie dokumentacji medycznej

Dokumentacja medyczna, ze względu na to, że zawiera dane o stanie zdrowia, jest bardzo istotnym punktem ochrony danych osobowych każdego podmiotu leczniczego. Musi być przechowywana w taki sposób, by:

- osoby nieupoważnione nie miały do niej dostępu
- uchronić ją przed przypadkowym lub celowym uszkodzeniem, zniszczeniem i innymi negatywnymi zdarzeniami.

Badanie Najwyższej Izby Kontroli z 2016 r. wskazuje, że przechowywanie dokumentacji medycznej dla wielu podmiotów jest wyzwaniem.

W przypadku 11, spośród 24 objętych kontrolą podmiotów, nie zapewniono odpowiednich warunków przechowywania dokumentacji medycznej zabezpieczających ją przed zniszczeniem, uszkodzeniem lub utratą, a także przed dostępem osób nieuprawnionych. Na przykład u jednego z kontrolowanych świadczeniodawców dokumentacja składowana była w kartonach na podłodze lub luzem, a u innego – przechowywano ją w drewnianych, niezamykanych szafach ustawionych na korytarzu, do których dostęp miały także osoby postronne (pacjenci, interesanci).

Nie stwierdzono natomiast istotnych nieprawidłowości w zabezpieczeniu i przechowywaniu dokumentacji medycznej w postaci elektronicznej.

- Informacja o wynikach kontroli WDROŻENIE PRZEZ PODMIOTY LECZNICZE REGULACJI DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH[28]

[28] Najwyższa Izba Kontroli, Informacja o wynikach kontroli TWORZENIE I UDOSTĘPNIANIE DOKUMENTACJI MEDYCZNEJ KZD.430.002.2015, https://www.nik.gov.pl/plik/id,10736,vp,13069.pdf (dostęp dn. 22.11.2019 r.).

Zalecane jest, aby dokumentacja medyczna:

- była w miarę możliwości przechowywana na stałe w jednym pomieszczeniu, do którego nie mają dostępu osoby postronne
- była trzymana w szafkach, szufladach lub szafach zamykanych na klucz (do kluczy nie powinny mieć dostępu osoby nieupoważnione, np. członkowie personelu sprzątającego)
- była przenoszona między pomieszczeniami jedynie przez osoby zatrudnione w placówce medycznej.

Dokumentacja archiwalna powinna być przechowywana w warunkach zapewniających jej bezpieczeństwo przez okres wymagany przepisami prawa (co do zasady jest to 20 lat). Najlepszym sposobem jest jej trzymanie w oddzielnym pomieszczeniu, odpowiednio suchym, wentylowanym i nienarażonym na zalanie. Ten ostatni warunek jest bardzo istotny, ponieważ często (ze względu na ograniczenia lokalowe) dokumentację archiwalną przechowuje się w pomieszczeniach piwnicznych, gdzie biegną rury wodno-kanalizacyjne.

Realizacja obowiązku informacyjnego

Poinformowanie pracowników, pacjentów i innych osób o tym, jak są wykorzystywane ich dane osobowe, jest jednym z istotnych obowiązków administratora danych. Częste są jednak przykłady nadgorliwości w tym zakresie. Placówkom medycznym zdarza się np. oczekiwać, by każdy z leczących się u nich pacjentów podpisał zapoznanie się z obowiązkiem informacyjnym. Tymczasem z RODO wcale taki obowiązek nie wynika.

> *Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 (...) Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie.*
>
> - art. 12 ust. 1 RODO

Innymi słowy: każdy uczestnik rekrutacji, pracownik, pacjent, przedstawiciel kontrahenta lub inna osoba musi mieć realną szansę zapoznania się z treścią obowiązku informacyjnego. Administrator powinien tu brać pod uwagę sytuacje, gdy:

- z obowiązkiem będzie chciała się zapoznać osoba odwiedzająca placówkę medyczną
- osoba chce zapoznać się z treścią obowiązku poza godzinami pracy placówki
- osoba pragnąca zapoznać się z treścią obowiązku informacyjnego nie ma dostępu do internetu.

W związku z tym obowiązek informacyjny wobec pacjentów powinien być spełniony następująco:

- wydrukowany i umieszczony na tablicy ogłoszeń
- wydrukowany w kilku egzemplarzach i przechowywany w rejestracji
- umieszczony na stronie internetowej placówki medycznej (jeżeli placówka taką stronę prowadzi).

Odpowiedzialność za naruszenia ochrony danych osobowych

Zdjęcie: Kelli McClintock, Unsplash (https://unsplash.com/photos/sFNn6JyKkfk)

Jeżeli administrator danych nie przestrzega zasad wykorzystania danych osobowych, naraża się na odpowiedzialność za swoje zachowanie.

W rozdziale I wskazujemy, jak wygląda odpowiedzialność cywilna administratora danych względem pacjenta.

W tym rozdziale opiszemy, jak wygląda odpowiedzialność administracyjna (wobec organu nadzorczego).

PUODO jako organ nadzorczy i kontrolny

Prezes Urzędu Ochrony Danych Osobowych jest organem nadzorczym w rozumieniu RODO. Oznacza to, że dba o zgodność przetwarzania danych z przepisami prawa i wydaje opinie na ten temat; może także prowadzić kontrole.

Kontrole mogą być planowane lub prowadzone na wniosek PUODO, gdy dowie się o sytuacji wymagającej jego działania.

Kontrole sektorowe są ogłaszane na dany rok kalendarzowy. Określają ogólnie, jakie firmy lub instytucje z poszczególnych branż mogą spodziewać się kontroli i w jakim zakresie.

Sektor zdrowia, zatrudnienia i szkolnictwa

I. Szkoły i placówki oświatowe - przetwarzanie danych osobowych rejestrowanych za pomocą systemu monitoringu wizyjnego (cd. sektora rozpoczętego w IV kwartale 2018 r.).

II. Pracodawcy - przetwarzanie danych osobowych rejestrowanych za pomocą systemu monitoringu wizyjnego. Przetwarzanie danych w związku z rekrutacją.

III. Podmioty udzielające świadczeń zdrowotnych - przetwarzanie danych osobowych w związku z udostępnianiem dokumentacji medycznej w ramach realizacji praw pacjenta do dostępu do dokumentacji medycznej dotyczącej jego stanu zdrowia oraz udzielonych mu świadczeń zdrowotnych.

- Roczny plan kontroli sektorowych na 2019 rok[29]

Kontrole mogą być także prowadzone na wniosek Prezesa UODO, jeżeli dowie się o niepokojących sygnałach.

Taka kontrola nie w każdym przypadku musi wiązać się z wizytą przedstawiciela urzędu. Bardzo często do administratora danych (lub jego IOD) trafia pismo z urzędu z prośbą o złożenie wyjaśnień w konkretnej sprawie. Dopiero kiedy w toku korespondencji PUODO nabierze przekonania, że sprawa wymaga dokładniejszego sprawdzenia, można spodziewać się kontroli na miejscu.

W zdecydowanej większości przypadków takie kontrole są zapowiedziane z wyprzedzeniem. Przed rozpoczęciem czynności kontroler powinien okazać:

- legitymację służbową

oraz

- imienne upoważnienie do przeprowadzenia kontroli.

Tuż po wejściu w życie RODO miały miejsce przypadki, w których w firmach zjawiali się fałszywi kontrolerzy (podszywający się pod pracowników urzędu), dlatego należy zachować ostrożność. W razie wątpliwości można skontaktować się z UODO pod numerem telefonu 22 531-09-13.

Stary wzór legitymacji służbowej kontrolera urzędu, obowiązujący do 30 kwietnia 2019 r.

[29] Urząd Ochrony Danych Osobowych, *Roczny plan kontroli sektorowych na 2019 rok*, https://uodo.gov.pl/pl/file/1832 (dostęp 28.11.2019 r.).

Aktualny wzór legitymacji służbowej kontrolera (obowiązujący od 30 kwietnia 2019 r.). Zabezpieczenia obejmują hologram godła państwowego oraz nadruk cienkich linii zabezpieczających (w miejscach wpisu nazwiska i imienia).

Kontroler ma, zgodnie z ustawą o ochronie danych osobowych, następuje uprawnienia:

- wstęp (w godz. 6:00-22:00) do budynków lub pomieszczeń placówki medycznej
- wgląd do dokumentów bezpośrednio związanych z kontrolą
- oględziny miejsc, przedmiotów, urządzeń lub systemów IT
- żądanie składania ustnych lub pisemnych wyjaśnień
- przesłuchiwanie pracownika placówki medycznej w charakterze świadka
- wzywanie policji w razie uniemożliwiania lub utrudniania kontroli
- rejestracja obrazu lub dźwięku (w uzasadnionych przypadkach i po uprzednim poinformowaniu kontrolowanego).

Po zakończeniu kontroli powstaje protokół, który opisuje stan faktyczny. Jeśli na jego podstawie okaże się, że dochodzi do poważnych naruszeń ochrony danych, Prezes Urzędu Ochrony Danych Osobowych wszczyna postępowanie, które w skrajnym przypadku może zakończyć się nałożeniem administracyjnej kary pieniężnej.

Maksymalna wysokość administracyjnych kar finansowych wynosi:

- **100.000 zł** – dla jednostki sektora finansów publicznych (np. samodzielnego publicznego zakładu opieki zdrowotnej)
- **€20.000.000 (85.770.000 zł)** lub do **4% rocznego obrotu** (zastosowanie ma kwota wyższa) – dla pozostałych podmiotów.

Jak dotąd w Polsce nie została nałożona żadna „kara za RODO" dla podmiotu medycznego.

Jak postępować z naruszeniami ochrony danych

Mimo najlepszych zabezpieczeń, szkoleń i innych tego typu środków może dojść do naruszenia ochrony danych osobowych. Administrator musi jak najszybciej dowiadywać się o nich, by móc odpowiednio zareagować. Bardzo ważne jest, by wiedzieli o tym także pracownicy. Każda osoba zatrudniona musi wiedzieć:

- czym jest naruszenie
- jak ma je zgłaszać
- komu ma je zgłaszać.

W rozdziale V wskazujemy, jak osoby zatrudnione w placówce medycznej powinny reagować na incydenty bezpieczeństwa.

Kiedy już informacja o naruszeniu trafi do administratora danych, należy ustalić, co z nim zrobić. Zgodnie z przepisami RODO są sytuacje, gdy naruszenie wymaga zgłoszenia do PUODO lub poinformowania osób poszkodowanych w wyniku wycieku. Są też naruszenia mniejszej wagi, które wymagają jedynie odnotowania w ewidencji naruszeń.

Podstawowym czynnikiem, który pozwala na odróżnienie tych rodzajów naruszeń od siebie jest **ryzyko związane z naruszeniem**. Zależności przedstawia poniższa tabela.

	Ewidencja naruszeń	**Zgłoszenie do PUODO**	**Poinformowanie osób dotkniętych zdarzeniem**
Naruszenia ochrony danych, które nie powodują ryzyka naruszenia praw lub wolności osoby, której dane dotyczą	TAK	NIE	NIE
Naruszenia, które mogą skutkować ryzykiem naruszenia praw lub wolności osoby, której dane dotyczą	TAK	TAK	NIE
Naruszenia, które mogą powodować wysokie ryzyko naruszenia praw lub wolności osoby, której dane dotyczą	TAK	TAK	TAK

Oceniając, jak duże ryzyko naruszenia praw lub wolności wiąże się z incydentem bezpieczeństwa, bierzemy pod uwagę:

- charakter naruszenia (poufność, integralność, dostępność…)
- liczbę osób dotkniętych naruszeniem (kilka, kilkanaście, kilkadziesiąt…)
- kategorie osób (pracownicy, pacjenci, stażyści…)
- kategorie danych osobowych (imiona, nazwiska, PESEL-e, numery dokumentów tożsamości, informacje o stanie zdrowia…).

Takiej oceny trzeba dokonać w ciągu 72 godzin zegarowych od momentu stwierdzenia naruszenia. Jeżeli w tym czasie zostanie stwierdzone, że naruszenie może skutkować ryzykiem naruszenia praw lub wolności, trzeba je zgłosić do PUODO. **Ewentualne opóźnienie w zgłoszeniu wymaga uzasadnienia.**

Oceny charakteru naruszenia najczęściej dokonuje inspektor ochrony danych we współpracy z innymi pracownikami administratora (np. informatykiem). Jednak to administrator podejmuje decyzję jak zareagować naruszenie. W szczególności to administrator decyduje, czy naruszenie ma być zgłoszone do PUODO i ponosi za tę decyzję odpowiedzialność.

Poniżej przedstawiamy kilka przykładów sytuacji, jakie mogą mieć miejsce w placówce medycznej. Oceniamy, jakimi są naruszeniami i jak powinna wyglądać reakcja administratora danych.

Zdarzenie	Zgłoszenie do PUODO	Poinformowanie osób dotkniętych zdarzeniem	Uwagi
Administrator przechowywał kopię zapasową archiwum danych osobowych, zaszyfrowaną na płycie CD. Płytę skradziono podczas włamania.	Nie	Nie	Jeżeli dane są zaszyfrowane za pomocą algorytmu zgodnego ze stanem techniki, istnieją kopie zapasowe danych, a unikalny klucz jest bezpieczny, może to być naruszenie niepodlegające obowiązkowi zgłoszenia. Jeżeli jednak w późniejszym czasie coś zagrozi temu bezpieczeństwu, powiadomienie będzie wymagane.
Z powodu krótkotrwałej przerwy w dostawie prądu w placówce medycznej pacjenci nie mogli dodzwonić się do rejestracji.	Nie	Nie	To nie jest naruszenie danych osobowych podlegające obowiązkowi zgłoszenia; niemniej, zdarzenie należy zarejestrować zgodnie z art. 33 ust. 5. RODO.
Na administratora przeprowadzono atak za pomocą oprogramowania typu ransomware, w wyniku którego wszystkie dane zostały zaszyfrowane. Nie istnieją kopie zapasowe i nie można odzyskać danych. W toku dochodzenia staje się jasne, że oprogramowanie jedynie szyfruje dane, a w systemie nie wykryto żadnego innego złośliwego oprogramowania.	Tak, ponieważ doszło do utraty dostępności; należy powiadomić PUODO, jeżeli istnieje możliwość konsekwencji dla osób fizycznych.	Tak, należy powiadomić osoby fizyczne w zależności od charakteru naruszonych danych osobowych i możliwych skutków braku dostępu do danych oraz innych prawdopodobnych konsekwencji.	Jeżeli istniały kopie zapasowe i możliwe jest odzyskanie danych w odpowiednim czasie, o zdarzeniu nie trzeba powiadamiać PUODO ani osób fizycznych, ponieważ nie doszło do trwałej utraty dostępności lub poufności. Niemniej, w przypadku zgłoszenia do organu nadzorczego, organ może rozważyć przeprowadzenie dochodzenia w celu oceny zgodności z szerszymi wymogami bezpieczeństwa wynikającymi z art. 32. RODO.

Zgłoszenie naruszenia do PUODO

Zgłoszenie naruszenia do Prezesa UODO może nastąpić:

- poprzez platformę biznes.gov.pl (wypełnienie dedykowanego formularza elektronicznego dostępnego bezpośrednio na platformie lub za pomocą pisma ogólnego dostępnego na platformie)
- poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP
- tradycyjną pocztą przez wysłanie wypełnionego formularza na adres siedziby PUODO.

Wszystkie rodzaje zgłoszeń są tak samo ważne, ale zalecane jest wykorzystywanie środków komunikacji elektronicznej.

Treść zgłoszenia do Prezesa Urzędu jest określona w przepisach RODO.

Zgłoszenie (...) musi co najmniej:
a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
- art. 33 ust. 3 RODO

Poniżej przykładowa treść zgłoszenia, opisująca naruszenie ochrony danych w postaci laptopów zawierających dane osobowe pacjentów.

Zgłoszenie naruszenia ochrony danych osobowych
1. Charakter naruszenia
Do kradzieży laptopa z siedziby administratora doszło między 8 sierpnia o 19:00 a 9 sierpnia o 8:00 rano. Sprawca kradzieży prawdopodobnie wykorzystał nieobecność pracownika rejestracji na stanowisku pracy i w związku z tym poruszał się niezauważony. Drzwi wejściowe nie noszą śladów przełamania zabezpieczeń.
Laptop skradziono ze stanowiska rejestracji, oddzielnego od korytarza ladą i furtką. Laptop nie miał zaszyfrowanego dysku twardego, był zabezpieczony loginem i hasłem systemu Windows.
Na dysku twardym komputera znajdowały się pliki zawierające dane osobowe pacjentów doktora Judyma (imiona, nazwiska, adresy miejsca zamieszkania, daty urodzenia, PESEL-e, dane o stanie zdrowia) – ok. 40 osób.
2. Dane kontaktowe inspektora ochrony danych
Barbara Zawisza-Czarna, iod@jamanowski.pl
3. Możliwe konsekwencje naruszenia ochrony danych
- utrata kontroli nad własnymi danymi osobowymi
- ograniczenie możliwości realizowania praw
- kradzież lub sfałszowanie tożsamości
- strata finansowa
- naruszenie dobrego imienia.

4. Środki mające na celu zminimalizowanie lub ograniczenie negatywnych skutków

Stosowane

- wdrożenie i stosowanie polityki bezpieczeństwa
- szkolenia dla pracowników dotyczące zasad bezpieczeństwa
- zawiadomienie policji o kradzieży.

Planowane

- zaszyfrowanie dysków twardych wszystkich laptopów
- użytkownicy zostaną pouczeni o tym, by nie zapisywać plików zawierających szczególne kategorie danych na dysku twardym komputera
- dodatkowy audyt bezpieczeństwa informacji
- dodatkowe szkolenie dla pracowników rejestracji
- przypomnienie zasad postępowania z komputerami przenośnymi po godzinach pracy.

Informowanie osób dotkniętych naruszeniem

Naruszenia, które mogą powodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, wymagają także poinformowania o incydencie tych osób. Także i tutaj RODO daje wskazówki.

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d)

[b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.].

- art. 34 ust. 1-2 RODO

Zgłoszenie powinno trafić do osoby dotkniętej naruszeniem:

- bezpośrednio

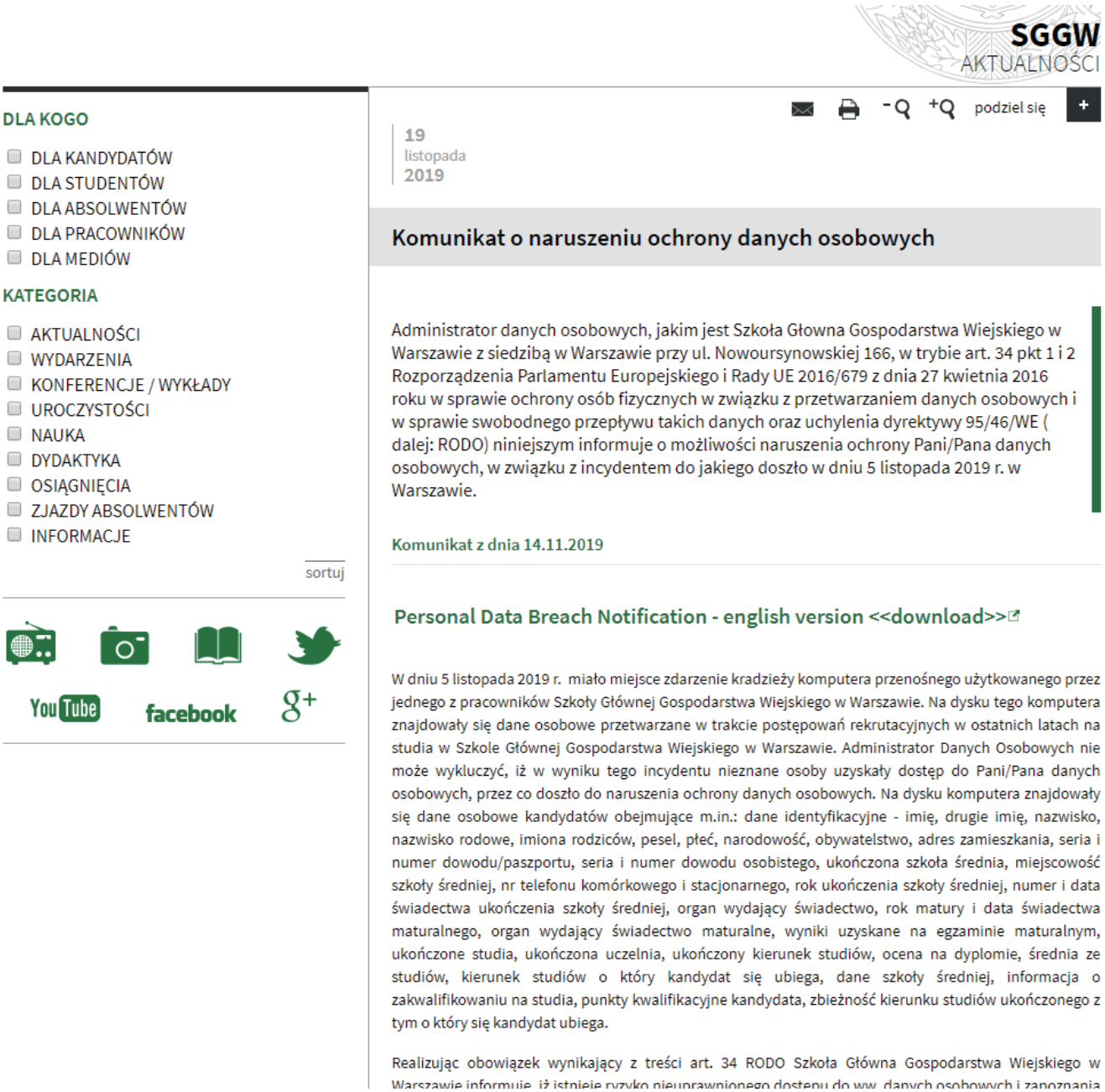
oraz

- bez zbędnej zwłoki.

Jeżeli naruszenie dotyczy większej liczby osób i zawiadomienie każdej z nich osobno wymagałoby niewspółmiernie dużego wysiłku, można zastosować ogłoszenie publiczne. Zalecane jest, aby znalazło się:

- na tablicy ogłoszeń, w rejestracji lub innym miejscu, do którego mają swobodny dostęp osoby dotknięte naruszeniem
- na stronie internetowej placówki, jeżeli taką posiada.

Innym sposobem realizacji takiego ogłoszenia może być powieszenie go w lokalnym urzędzie lub opublikowanie w prasie lokalnej.



SGGW
AKTUALNOŚCI

DLA KOGO

- DLA KANDYDATÓW
- DLA STUDENTÓW
- DLA ABSOLWENTÓW
- DLA PRACOWNIKÓW
- DLA MEDIÓW

KATEGORIA

- AKTUALNOŚCI
- WYDARZENIA
- KONFERENCJE / WYKŁADY
- UROCZYSTOŚCI
- NAUKA
- DYDAKTYKA
- OSIĄGNIĘCIA
- ZJAZDY ABSOLWENTÓW
- INFORMACJE

sortuj

YouTube facebook

podziel się +

19
listopada
2019

Komunikat o naruszeniu ochrony danych osobowych

Administrator danych osobowych, jakim jest Szkoła Głowna Gospodarstwa Wiejskiego w Warszawie z siedzibą w Warszawie przy ul. Nowoursynowskiej 166, w trybie art. 34 pkt 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO) niniejszym informuje o możliwości naruszenia ochrony Pani/Pana danych osobowych, w związku z incydentem do jakiego doszło w dniu 5 listopada 2019 r. w Warszawie.

Komunikat z dnia 14.11.2019

Personal Data Breach Notification - english version <<download>>

W dniu 5 listopada 2019 r. miało miejsce zdarzenie kradzieży komputera przenośnego użytkowanego przez jednego z pracowników Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie. Na dysku tego komputera znajdowały się dane osobowe przetwarzane w trakcie postępowań rekrutacyjnych w ostatnich latach na studia w Szkole Głównej Gospodarstwa Wiejskiego w Warszawie. Administrator Danych Osobowych nie może wykluczyć, iż w wyniku tego incydentu nieznane osoby uzyskały dostęp do Pani/Pana danych osobowych, przez co doszło do naruszenia ochrony danych osobowych. Na dysku komputera znajdowały się dane osobowe kandydatów obejmujące m.in.: dane identyfikacyjne - imię, drugie imię, nazwisko, nazwisko rodowe, imiona rodziców, pesel, płeć, narodowość, obywatelstwo, adres zamieszkania, seria i numer dowodu/paszportu, seria i numer dowodu osobistego, ukończona szkoła średnia, miejscowość szkoły średniej, nr telefonu komórkowego i stacjonarnego, rok ukończenia szkoły średniej, numer i data świadectwa ukończenia szkoły średniej, organ wydający świadectwo, rok matury i data świadectwa maturalnego, organ wydający świadectwo maturalne, wyniki uzyskane na egzaminie maturalnym, ukończone studia, ukończona uczelnia, ukończony kierunek studiów, ocena na dyplomie, średnia ze studiów, kierunek studiów o który kandydat się ubiega, dane szkoły średniej, informacja o zakwalifikowaniu na studia, punkty kwalifikacyjne kandydata, zbieżność kierunku studiów ukończonego z tym o który się kandydat ubiega.

Realizując obowiązek wynikający z treści art. 34 RODO Szkoła Główna Gospodarstwa Wiejskiego w Warszawie informuje, iż istnieje ryzyko nieuprawnionego dostępu do ww. danych osobowych i zapoznania

Przykład komunikatu o naruszeniu ochrony danych osobowych, opublikowany 14 listopada 2019 r. na stronie Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie, https://www.sggw.pl/aktualnosci/komunikat-o-naruszeniu-danych-osobowych (dostęp *22.11.2019 r.).*

Poniżej przykładowa treść informacji dla osób dotkniętych naruszeniem.

Komunikat o naruszeniu ochrony danych osobowych

Szanowni Państwo,

Z przykrością informujemy, że dnia 9 sierpnia 2019 r. doszło do włamania do rejestracji JAMANOWSKI PRAKTYKA LEKARZA RODZINNEGO (ul. Piekarska 221B, 57-540 Lądek-Zdrój) i kradzieży laptopa, na którym znajdowały się dane pacjentów doktora Judyma (imiona, nazwiska, adresy miejsca zamieszkania, daty urodzenia, PESEL-e, dane o stanie zdrowia) – ok. 40 osób.

W związku ze zdarzeniem:

- niezwłocznie zawiadomiliśmy policję
- poinformowaliśmy o sprawie inspektora ochrony danych (IOD)
- zgłosiliśmy sytuację do Prezesa Urzędu Ochrony Danych Osobowych.

Niestety, w wyniku zaistniałej sytuacji może dojść do naruszeń. Sprawcy zdarzenia mogą wykorzystać dane do:

- naruszenia Państwa dobrego imienia
- pozbawienia lub ograniczenia Państwa praw (np. przez głosowanie w Państwa imieniu w projektach budżetu obywatelskiego)
- składania w Państwa imieniu dyspozycji dotyczących wydawania dokumentacji medycznej lub wyrażania sprzeciwu co do udostępniania informacji medycznych czy uzyskiwania kopii Państwa dokumentacji medycznej z innych placówek medycznych, z których usług Państwo korzystali.

W celu zmniejszenia ewentualnych skutków opisanego naruszenia, podajemy poniżej działania rekomendowane przez Prezesa Urzędu Ochrony Danych Osobowych:

- założenie konta w systemie informacji gospodarczej (np. BIK) w celu upewnienia się, że na Państwa dane osobowe nie została wzięta pożyczka lub kredyt
- poinformowanie właściwych organów (np. policji) w sytuacji, gdy dowiedzą się Państwo o szkodzie majątkowej, związanej z kradzieżą tożsamości (np. w sytuacji, gdy ktoś wziął kredyt na Państwa dane osobowe)
- skontaktowanie się – w ciągu najbliższych kilku miesięcy – z innymi placówkami medycznymi, gdzie znajduje się dotycząca Państwa dokumentacja medyczna, w celu upewnienia się, że w Państwa imieniu nie były składane żadne dyspozycje (np. sprzeciw wobec wydania dokumentacji medycznej konkretnej osobie).

W przypadku pytań, do Państwa dyspozycji pozostaje nasz inspektor ochrony danych, Barbara Zawisza-Czarna, pod adresem email iod@jamanowski.pl.

Jednocześnie informujemy, że podjęliśmy szereg działań, które mają zapobiec podobnym incydentom w przyszłości:

- wszystkie obecnie wykorzystywane i nowe laptopy będą miały dyski twarde zaszyfrowane BitLockerem (Windows 10), który uniemożliwia odczyt danych przez osoby niepowołane
- użytkownicy zostaną pouczeni o tym, by nie zapisywać plików zawierających szczególne kategorie danych na dysku twardym komputera
- użytkownicy zostaną pouczeni o konieczności zabezpieczania laptopów po pracy (w szczególności poprzez ich zamykanie na klucz w szafach lub szafkach),
- w planie szkoleń (dla obecnych i przyszłych pracowników) uwzględniono zasady bezpiecznego przechowywania danych i komputerów.

Rozdział XI. Archiwizacja danych osobowych

Okresy przechowywania dokumentów zawierających dane osobowe

Jednym z najważniejszych obowiązków, który spoczywa na podmiocie leczniczym jest obowiązek prowadzenia i przechowywania dokumentacji medycznej przez okresy przewidziane przepisami prawa. Dlatego bardzo ważnym zadaniem dla podmiotów leczniczych jest poprawne określenie okresów przechowywania prowadzonej przez siebie dokumentacji medycznej. Pomocą w określeniu omawianych okresów przechowywania danych jest m.in. przytoczony poniżej przepis.

§

Podmiot udzielający świadczeń zdrowotnych przechowuje dokumentację medyczną przez okres 20 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu, z wyjątkiem:
1) dokumentacji medycznej w przypadku zgonu pacjenta na skutek uszkodzenia ciała lub zatrucia, która jest przechowywana przez okres 30 lat, licząc od końca roku kalendarzowego, w którym nastąpił zgon;
1a) dokumentacji medycznej zawierającej dane niezbędne do monitorowania losów krwi i jej składników, która jest przechowywana przez okres 30 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu;
2) zdjęć rentgenowskich przechowywanych poza dokumentacją medyczną pacjenta, które są przechowywane przez okres 10 lat, licząc od końca roku kalendarzowego, w którym wykonano zdjęcie;
3) skierowań na badania lub zleceń lekarza, które są przechowywane przez okres:
a) 5 lat, licząc od końca roku kalendarzowego, w którym udzielono świadczenia zdrowotnego będącego przedmiotem skierowania lub zlecenia lekarza,
b) 2 lat, licząc od końca roku kalendarzowego, w którym wystawiono skierowanie – w przypadku gdy świadczenie zdrowotne nie zostało udzielone z powodu niezgłoszenia się pacjenta w ustalonym terminie, chyba że pacjent odebrał skierowanie;
4) dokumentacji medycznej dotyczącej dzieci do ukończenia 2. roku życia, która jest przechowywana przez okres 22 lat

- art. 29 ust. 1 ustawy o prawach pacjenta[30]

W przypadku niektórych dokumentów przechowywanych przez podmioty lecznicze okres ich przechowywania nie został wyraźnie wskazany w przepisach prawa. Przykładowo deklaracje wyboru lekarza POZ, będące dokumentami rozliczeniowymi pomiędzy podmiotami leczniczymi i Narodowym Funduszem Zdrowia, powinny być przechowywane przez okres 6 lat – w ich przypadku znajduje zastosowanie ogólny termin przedawnienia roszczeń z art. 118 Kodeksu cywilnego. Należy jednak wskazać, że przed dniem 9 lipca 2018 r. wspomniany okres wynosił 10 lat i zgodnie z przepisami przejściowymi będzie on miał zastosowanie w niektórych przypadkach, co obrazuje poniższy przykład.

[30] Ustawa z dnia 6.11.2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2019 r. poz. 1127 ze zm.).

Przykład:
Deklaracje wyboru lekarza POZ wycofane przed 9 lipca 2014 r. powinny być przechowywana przez **okres 10 lat liczony od dnia wycofania deklaracji**.
Deklaracje wyboru lekarza POZ wycofane od 9 lipca 2014 r. do 8 lipca 2018 r. powinny być przechowywane przez **okres 6 lat liczony od dnia 9 lipca 2018 r.**
Deklaracja wyboru lekarza POZ wycofane od 9 lipca 2018 r. powinny być przechowywane przez okres **6 lat liczony od dnia wycofania deklaracji**.

Przykładowe okresy przechowywania dokumentacji:

<table>
<tr><td colspan="3">Zasadą ogólną jest przechowywanie dokumentacji medycznej przez okres 20 lat,
okresy są liczone od końca roku, w którym dokonano ostatniego wpisu</td></tr>
<tr><td>historia choroby</td><td colspan="2">20 lat</td></tr>
<tr><td>deklaracje wyboru lekarza POZ</td><td colspan="2">6/1031 lat od dnia, kiedy deklaracje przestały być podstawą rozliczeń (tj. wycofania deklaracji)</td></tr>
<tr><td>księgi zabiegowe</td><td colspan="2">20 lat</td></tr>
<tr><td>skierowania zrealizowane</td><td colspan="2">5 lat od końca roku, w którym realizowano skierowanie</td></tr>
<tr><td>skierowania niezrealizowane</td><td colspan="2">2 lata od końca roku, w którym wystawiono skierowanie</td></tr>
<tr><td rowspan="2">kupony RUM</td><td>6/102 lat</td><td>jeśli informacja o świadczeniach zdrowotnych została wprowadzona do indywidualnej lub zbiorowej dokumentacji medycznej</td></tr>
<tr><td>20 lat</td><td>jeśli są jedynym zapisem dotyczącym wykonanych świadczeń zdrowotnych, a tym samym stanowią część dokumentacji medycznej</td></tr>
<tr><td colspan="3">pozostała dokumentacja</td></tr>
<tr><td colspan="3">22 lata – w zakresie dokumentacji medycznej dotyczącej dzieci do ukończenia 2. roku życia</td></tr>
<tr><td colspan="3">30 lat – w przypadku gdy dane są niezbędne do monitorowania losów krwi i jej składników</td></tr>
<tr><td colspan="3">30 lat – w przypadku gdy nastąpił zgon pacjenta na skutek uszkodzenia ciała lub zatrucia</td></tr>
<tr><td colspan="3">10 lat - w przypadku zdjęć rentgenowskich przechowywanych poza dokumentacją medyczną pacjenta, od końca roku kalendarzowego, w którym wykonano zdjęcie</td></tr>
</table>

Archiwizowanie dokumentacji elektronicznej

Archiwizowanie dokumentów zawierających dane osobowe jest na gruncie definicji z art. 4 pkt 2 RODO jednym z rodzajów przetwarzania danych osobowych. Administratorzy danych coraz częściej odchodzą od tradycyjnego, papierowego archiwizowania dokumentów na rzecz przechowywania ich w systemach informatycznych. Elektroniczna archiwizacja dokumentów jest stosowana przez administratorów z jednej strony w celu optymalizacji przestrzeni

[31] Zobacz przykład 1 w rozdziale XI.

w stosunku do danych aktualnie przetwarzanych, np. w celu udzielania świadczeń zdrowotnych, a z drugiej strony, w celu przechowywania danych np. po zakończeniu trwania umowy, wyłącznie na cele związane z ich retencją.

Wybór archiwizacji w formie elektronicznej może stanowić techniczny środek odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych. Rozwiązania takie jak szyfrowanie danych, odzyskanie danych z kopii zapasowych, dostęp do danych z wielu lokalizacji, oszczędność miejsca, czy łatwość i szybkość ich utylizacji to tylko niektóre aspekty wpływające na przewagę archiwizacji elektronicznej nad papierową.

W celu prowadzenia dokumentacji elektronicznej pracodawca może korzystać z własnych narzędzi informatycznych lub współpracować z firmami udostępniającymi zewnętrzne przestrzenie chmurowe dedykowane do takich celów. Jednak w takim przypadku istnieje potrzeba zawarcia odpowiedniej umowy powierzenia ze wspomnianą firmą.

Przykład:
Sieć placówek medycznych postanowiła skorzystać z usług zewnętrznego dostawcy oferującego rozwiązania chmurowe i przechowywać tam dane pacjentów, które do tej pory były przechowywane na serwerach lokalnych.

Jakie czynności powinien podjąć administrator danych osobowych, aby przechowywanie danych w chmurze było zgodne z przepisami RODO?
Korzystając z zewnętrznych narzędzi konieczne jest z jednej strony zweryfikowanie dostawcy takiego narzędzia (np. poprzez ankietę wyboru dostawcy), a z drugiej, zweryfikowanie poziomu bezpieczeństwa, jaki zapewnia oferowane przez niego narzędzie. Często dla administratora, którego główna działalność nie jest związana z przechowywaniem danych, korzystanie z usług chmurowych jest najbardziej optymalnym rozwiązaniem, ponieważ oferują one dużo wyższy poziom bezpieczeństwa danych, niż serwery lokalne. Należy pamiętać także o konieczności zawarcia umowy powierzenia, precyzującej nie tylko zakres danych i sposoby ich zabezpieczenia, ale także zasady współpracy w zakresie notyfikacji naruszeń, czy realizacji wniosków podmiotów danych, przeprowadzania audytów, czy dopuszczalność podpowiedzenia danych osobowych. W przypadku podmiotów medycznych, które często przetwarzają dane dotyczące zdrowia na dużą skalę, konieczne będzie także przeprowadzenie ponownej oceny skutków dla ochrony danych dla tego procesu, z uwagi na zmianę charakteru przetwarzania danych, które dotychczas były przetwarzane lokalnie, a teraz miałyby być przechowywane na zewnętrznych serwerach. W celu ustalenia, czy dochodzi do transferu poza EOG kluczowa jest rzeczywista lokalizacja serwerów, a nie siedziba potencjalnego podmiotu przetwarzającego (procesora).

Zarówno korzystanie z zewnętrznego podmiotu dostarczającego usługę chmurową, z której korzysta administrator, w celu realizacji procesów przetwarzania danych, jak również informacja o tym, że podmiot ten ma siedzibę poza EOG, generuje konieczność uzupełnienia obowiązku informacyjnego o informacje o przekazywaniu danych poza EOG. Konieczne jest również dokonanie stosownego wpisu w rejestrze czynności przetwarzania, w ramach procesu archiwizacji dokumentacji.

Wobec dokumentacji archiwizowanej papierowo i elektronicznie administrator powinien stosować takie same okresy retencji. Wynika to z zasady ograniczenia czasu przetwarzania danych, która nie rozróżnia czasu przetwarzania w zależności od nośnika, na którym znajdują się dane. Wspomniana zasada została potwierdzona w sprawozdaniu Prezesa Urzędu Ochrony Danych Osobowych, w którym wskazano, że określenie odmiennych okresów przechowywania danych osobowych przetwarzanych w tym samym celu, a jedynie za pomocą innego narzędzia (nośnika danych) nie jest spójne i tym samym narusza przepisy RODO.

Należy mieć także na uwadze, że z perspektywy właściwego funkcjonowania takiego archiwum, a także realizacji praw podmiotów danych, konieczne jest takie zaprojektowanie przestrzeni , aby np. na skutek wyszukiwania danych osobowych, dotyczących osoby, która złożyła wniosek o przekazanie kopii jej danych osobowych, nie ujawnić informacji, które mogłyby dotyczyć innych podmiotów danych i tym samym naruszyć ich prawa i wolności. W tym celu

na etapie projektowania takiego archiwum konieczne jest uwzględnienie prywatności osób, których dane dotyczą (privacy by design) i wdrożenie zasady domyślnej ochrony danych (privacy by default),np. poprzez wyświetlanie tylko tych informacji, które są niezbędne z perspektywy uprawnień dostępowych określonego użytkownika. Warto również zaimplementować rozwiązania, które pozwolą na logiczne odseparowanie danych o różnym poziomie wrażliwości z perspektywy RODO w systemie archiwizacyjnym, a także na automatyczne usunięcie danych osobowych po upływie okresu ich przechowywania.

Założenia dla takiego systemu powinny być więc możliwie precyzyjne określone i stanowić podstawę wyboru dostawcy, który zapewni ich spełnienie, a tym samym pozwoli na zapewnienie zgodności z zasadami RODO, a w szczególności pozwoli wykazać rozliczalność działań administratora i jego proaktywne podejście do ochrony prywatności.

Skuteczne niszczenie dokumentów zawierających dane osobowe

Podmiot leczniczy zobowiązany jest do przechowywania dokumentacji medycznej przez okresy wskazane przepisami prawa. Wspomniane okresy zostały przedstawione na początku niniejszego rozdziału. Natomiast po upływie wspomnianych okresów przechowywana dokumentacja medyczna powinna zostać zniszczona przez podmiot leczniczy.

> *Po upływie okresów wymienionych w ust. 1* [przytoczone na początku niniejszego rozdziału] *podmiot udzielający świadczeń zdrowotnych niszczy dokumentację medyczną w sposób uniemożliwiający identyfikację pacjenta, którego dotyczyła. Dokumentacja medyczna przeznaczona do zniszczenia może być wydana pacjentowi, jego przedstawicielowi ustawowemu lub osobie upoważnionej przez pacjenta.*
>
> - art. 29 ust. 2 ustawy o prawach pacjenta[32]

Podmiot leczniczy może rozwiązać kwestię niszczenia dokumentów na dwa sposoby:

- podpisując umowę z firmą zewnętrzną zajmującą się profesjonalnym niszczeniem nośników danych
- samodzielnie niszcząc dokumenty.

W pierwszym przypadku do obowiązków podmiotu leczniczego będzie należało znalezienie podmiotu, który będzie dawał gwarancję należytego wykonywania usługi niszczenia nośników danych (dokumenty papierowe, płyty CD i DVD, pendrive'y, dyski twarde) oraz zawarcie z tym podmiotem odpowiedniej umowy powierzenia.

> Problematykę zawierania umów powierzenia przez podmioty lecznicze szczegółowo opisano w rozdziale IX niniejszej publikacji.

W drugim przypadku podmiot leczniczy powinien określić procedury dotyczące niszczenia papierowej dokumentacji w sposób uniemożliwiający jej późniejsze odczytanie. W praktyce oznacza to, że właściciel podmiotu leczniczego powinien określić osobę odpowiedzialną za niszczenie dokumentów (można też zobowiązać wszystkich pracowników podmiotu leczniczego do bieżącego niszczenia zbędnych dokumentów, które zawierają dane osobowe) oraz sposób w jaki ma się odbywać niszczenie dokumentów (nośników danych), przykładowo z wykorzystaniem niszczarek do papieru powierzonych do dyspozycji pracowników podmiotu leczniczego.

---

[32] Ustawa z dnia 6.11.2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2019 r. poz. 1127 ze zm.).

Cenne wskazówki dla podmiotów leczniczych, co w praktyce oznacza skuteczne niszczenie nośników danych zostały zawarte w poniżej przytoczonym fragmencie komentarza do RODO.

> *Niszczenie sprowadza się natomiast do fizycznej destrukcji nośnika danych, na którym znajdują się dane osobowe. Przez to pojęcie należy także rozumieć zniszczenie części nośnika z danymi osobowymi. Przykładem takiego częściowego zniszczenia będzie wycięcie fragmentu dokumentu i jego wprowadzenie do niszczarki albo zamazanie danych osobowych znajdujących się na części dokumentu w sposób uniemożliwiający ich dalsze przetwarzanie. Zniszczeniem będzie także fizyczne uszkodzenie nośnika, takiego jak twardy dysk lub pamięć przenośna, w taki sposób, że nie będzie można odtworzyć zapisanych na nim danych osobowych.*
> Nie będzie mieściło się w pojęciu niszczenia danych pocięcie dokumentu z danymi, pomimo którego bez większych trudności można go odtworzyć i wyrzucenie tych elementów dokumentu do śmietnika w jednym worku. W takich przypadkach będzie można uznać, że nie doszło do niszczenia danych, lecz w istocie do ich udostępnienia. Podobnie należy zakwalifikować wyrzucenie na śmietnik nośników danych z zapisanymi na nich danymi osobowymi, jeżeli zapoznanie się z nimi jest możliwe po podłączeniu nośnika do innego urządzenia, przykładowo do komputera.
> *- RODO, Ogólne Rozporządzenie o Ochronie Danych, Komentarz* [33]

W sytuacji niszczenia większych ilości dokumentów (nośników danych) obowiązująca w podmiocie leczniczym procedura niszczenia dokumentów powinna zobowiązywać pracowników do sporządzenia protokołu z zniszczenia nośników danych, który powinien zostać stworzony zgodnie z poniższą instrukcją. Po zakończenia niszczenia nośników danych sporządzony przy tej okazji protokół stanowił będzie dowód, że dokumentacja medyczna mogła zostać zniszczona, ponieważ upłynął określony przepisami prawa okres jej przechowywania.

Protokół ze zniszczenia nośników danych

1. Protokół powinien zawierać spis niszczonej/anonimizowanej dokumentacji

- przechowywanej w formie papierowej
- przechowywanej w formie elektronicznej.

2. Zalecane jest wskazanie rodzaju niszczonej/anonimizowanej dokumentacji (z uwzględnieniem formy przechowywania):

- rodzaj danych (dokumentacja medyczna, deklaracje wyboru lekarza POZ, skierowania, wyniki badań, umowy, itd.)
- okres przechowywania (od DD.MM.RRRR do DD.MM.RRRR)
- liczba nośników
- powód niszczenia danych (np. upływ wyznaczonego okresu przetwarzania danych osobowych; utrata przydatności danych osobowych przed upływem wyznaczonego okresu ich przetwarzania; wycofanie z eksploatacji lub przekazanie osobie trzeciej nośnika lub sprzętu wykorzystywanego do przetwarzania danych).

[33] Bielak-Jomaa E., Lubasz D. (red.), *RODO, Ogólne Rozporządzenie o Ochronie Danych, Komentarz*, Warszawa 2017, s. 198-199.

3. Zalecane jest wskazanie sposobu niszczenia dokumentów:

- W przypadku dokumentacji papierowej:
  - za pomocą niszczarki.
- W przypadku dokumentacji elektronicznej:
  - za pomocą specjalistycznego oprogramowania
  - fizyczne zniszczenie nośników danych.

4. Zalecane jest wskazanie sposobu anonimizacji dokumentów:

- W przypadku dokumentacji papierowej:
  - zakreślenie/zamazanie danych.
- W przypadku dokumentacji elektronicznej:
  - wykorzystanie specjalistycznego oprogramowania
  - zakreślenie/zamazanie danych (w plikach graficznych .jpg/.png)
  - usunięcie danyc,
  - zamiana danych na inne znaki np. xxxx lub 0000.

Wydawanie dokumentacji przeznaczonej do zniszczenia osobom, których ona dotyczy

Podmiot leczniczy zobowiązany jest do przechowywania dokumentacji medycznej przez okresy wskazane przepisami prawa, które to zostały przedstawione na początku niniejszego rozdziału. Jak zostało to wcześniej wskazane, po upływie okresów przechowywania dokumentacja medyczna pacjentów powinna zostać zniszczona lub przekazana pacjentom, których dotyczy. Należy tutaj wskazać, że zwrócona pacjentowi może zostać jedynie indywidualna dokumentacja medyczna dotycząca jego osoby. Natomiast zbiorowa dokumentacja medyczna prowadzona przez podmiot leczniczy bezwzględnie podlega zniszczeniu po upływie okresu jej przechowywania.

Powyższe zasady zostały skonkretyzowane w treści przytoczonej poniżej przepisu, który wskazuje, że przekazać pacjentowi możemy tylko dokumentację indywidualną, która jest przeznaczona do zniszczenia. Ponadto do przekazania dokumentacji pacjentowi konieczne jest złożenie przez niego odpowiedniego wniosku. W praktyce oznacza to, że jeśli po upływie okresu przechowywania indywidualnej dokumentacji medycznej będziemy chcieli ją zniszczyć, to wcześniej powinniśmy poinformować pacjenta o tym fakcie i o możliwości złożenia przez niego wniosku o wydanie oryginałów dokumentacji medycznej indywidualnej wewnętrznej przechowywanej przez nas, której zniszczenie planujemy.

Dokumentacja indywidualna wewnętrzna przewidziana do zniszczenia może zostać wydana na wniosek pacjenta, jego przedstawiciela ustawowego albo osoby, o której mowa w § 8 ust. 1 pkt 2 [osoba upoważniona przez pacjenta do dostępu do jego dokumentacji medycznej]*, za pokwitowaniem.*
- § 75 Rozporządzenia w sprawie rodzajów, zakresu i wzorów dokumentacji[34]

[34] Rozporządzenie MZ z dnia 9.11.2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. z 2015 r. poz. 2069).

Przechowywanie dokumentów zawierających dane osobowe po zakończeniu funkcjonowania placówki medycznej

Dla osób prowadzących działalność leczniczą niezwykle problematyczna jest sytuacja, w której zaprzestają oni prowadzenia swojej działalności. Powyższe wynika z tego, że zgodnie z poniżej przytoczonym przepisem podmiot udzielający świadczeń zdrowotnych jest obowiązany prowadzić, przechowywać i udostępniać dokumentację medyczną. Należy tutaj wskazać, że co do zasady powyższy obowiązek spoczywa na podmiocie udzielającym świadczeń zdrowotnych, nawet po zaprzestaniu prowadzenia przez niego działalności.

§

W celu realizacji prawa, o którym mowa w art. 23 ust. 1 [prawo pacjenta do dostępu do dokumentacji medycznej dotyczącej jego stanu zdrowia oraz udzielonych mu świadczeń zdrowotnych]*, podmiot udzielający świadczeń zdrowotnych jest obowiązany prowadzić, przechowywać i udostępniać dokumentację medyczną w sposób określony w niniejszym rozdziale oraz w ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, a także zapewnić ochronę danych zawartych w tej dokumentacji.*
- art. 24 ust. 1 ustawy o prawach pacjenta[35]

Ze względu na zakres wątpliwości zgłaszanych przez podmioty lecznicze, które zaprzestawały swojej działalności, polski ustawodawca wprowadził odpowiednie przepisy w przywoływanej wiele już razy ustawie o prawach pacjenta. Obecnie podmiotom udzielającym świadczeń zdrowotnych, które zamierzają zaprzestać prowadzenia przez siebie działalności, sposób działania wskazuje poniżej przytoczony przepis ustawy o prawach pacjenta.

§

1. W przypadku zaprzestania wykonywania działalności leczniczej podmiot udzielający świadczeń zdrowotnych przekazuje dokumentację medyczną podmiotom, o których mowa w ust. 2–4 i 7, w sposób zapewniający zabezpieczenie przed jej zniszczeniem, uszkodzeniem lub utratą oraz dostępem osób nieuprawnionych.
2. Dokumentację medyczną podmiotu zaprzestającego wykonywania działalności leczniczej przejmuje podmiot, który przejął jego zadania.
3. W przypadku braku podmiotu, o którym mowa w ust. 2, za przechowywanie i udostępnianie dokumentacji medycznej po zaprzestaniu udzielania świadczeń zdrowotnych odpowiada:
1) podmiot tworzący albo sprawujący nadzór – w przypadku podmiotu leczniczego niebędącego przedsiębiorcą w rozumieniu art. 2 ust. 1 pkt 4 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej albo instytutu badawczego, o którym mowa w art. 3 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych;
2) podmiot udzielający świadczeń zdrowotnych, z którym podmiot zaprzestający wykonywania działalności leczniczej zawarł umowę o przechowywanie dokumentacji medycznej – w przypadku podmiotu leczniczego innego niż określony w pkt 1 oraz praktyki zawodowej w rozumieniu art. 5 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej;
3) właściwa Okręgowa Izba Lekarska albo Okręgowa Izba Pielęgniarek i Położnych albo Krajowa Izba Fizjoterapeutów – w przypadku śmierci odpowiednio lekarza albo pielęgniarki lub położnej albo fizjoterapeuty, wykonujących zawód w formie praktyki zawodowej w rozumieniu art. 5 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej.

[35] Ustawa z dnia 6.11.2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2019 r. poz. 1127 ze zm.).

4. W przypadkach, o których mowa w art. 108 ust. 2 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej, organ prowadzący rejestr podmiotów wykonujących działalność leczniczą wzywa podmiot udzielający świadczeń zdrowotnych podlegający wykreśleniu do wskazania, w wyznaczonym terminie, nazwy (firmy) i adresu podmiotu, z którym zawarł umowę o przechowywanie dokumentacji medycznej.
5. W razie bezskutecznego upływu terminu, o którym mowa w ust. 4, organ prowadzący rejestr podmiotów wykonujących działalność leczniczą określa sposób postępowania z dokumentacją medyczną, na koszt podmiotu udzielającego świadczeń zdrowotnych podlegającego wykreśleniu.
6. Do należności z tytułu kosztów, o których mowa w ust. 5, stosuje się przepisy o postępowaniu egzekucyjnym w administracji.
7. W przypadku gdy nie jest możliwe ustalenie podmiotu odpowiedzialnego za przechowywanie dokumentacji medycznej po zaprzestaniu wykonywania działalności leczniczej, za przechowywanie dokumentacji medycznej odpowiada wojewoda.
- art. 30a ustawy o prawach pacjenta[36]

Z punktu widzenia podmiotu zaprzestającego wykonywania działalności leczniczej najmniej problematyczna jest sytuacja, w której inny podmiot leczniczy przejmuje jego zadania, ponieważ w takiej sytuacji dokumentacja medyczna jest przekazywana właśnie temu podmiotowi.

Przykład:
Lekarz A ze względu na podeszły wiek zaprzestaje prowadzenia działalności leczniczej, ale ma znajomego lekarza B, który przejmie jego gabinet i pacjentów. W takiej sytuacji dokumentacja medyczna prowadzona przez lekarza A zostanie przekazana lekarzowi B, który przejmie też obowiązki związane z przechowywaniem i udostępnianiem dokumentacji medycznej prowadzonej dotychczas przez lekarza A.

W sytuacji gdy zadania podmiotu leczniczego zaprzestającego działania nie zostają przejęte przez inny podmiot leczniczy, wspomniany podmiot leczniczy ma obowiązek zawrzeć z innym podmiotem leczniczym umowę o przechowywanie dokumentacji medycznej. Strony wspomnianej umowy mogą w zawieranej umowie zawrzeć także wynagrodzenie, jakie będzie otrzymywał podmiot przyjmujący dokumentację medyczną. Bez względu na to, czy przechowywanie dokumentacji medycznej będzie się odbywało za wynagrodzeniem, czy nie, podmiot przyjmujący dokumentację medyczną podmiotu zaprzestającego działalność leczniczą może w ramach udostępniania dokumentacji medycznej pacjentom pobierać z tego tytułu opłaty przewidziane przepisami prawa. Kwestia pobierania opłat, za udostępnianie dokumentacji medycznej pacjentom, szczegółowo została omówiona w rozdziale VIII.

Przykład:
Działający w miejscowości Z podmiot leczniczy A zaprzestający prowadzenia działalności leczniczej, którego zadania nie zostały przejęte przez inny podmiot leczniczy, powinien zawrzeć umowę o przechowywanie dokumentacji medycznej z podmiotem leczniczym B działającym w miejscowości Y, która leży nieopodal miejscowości Z. Podmioty A i B w umowie o przechowywanie dokumentacji medycznej nie przewidziały wynagrodzenia dla podmiotu B, jednak podmiot B może pobierać opłaty za udostępnianie dokumentacji medycznej pacjentom.

[36] Ustawa z dnia 6.11.2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2019 r. poz. 1127 ze zm.).

Problematykę pobierania przez podmioty lecznicze opłat za udostępnianie dokumentacji medycznej szczegółowo opisano w rozdziale IX niniejszej publikacji.

W razie śmierci lekarza, który prowadził działalność leczniczą w ramach praktyki zawodowej, o której mowa w art. 5 ustawy o działalności leczniczej, obowiązek przyjęcia oraz przechowywania dokumentacji medycznej spoczywa na Okręgowej Izbie Lekarskiej, do której należał lekarz, który umarł.

Przykład:
Umarł lekarz prowadzący działalność leczniczą w Swarzędzu. W takiej sytuacji obowiązek przechowywania dokumentacji medycznej będzie spoczywał na Okręgowej Izbie Lekarskiej w Poznaniu, gdyż to do niej należał lekarz, który umarł.

Polski ustawodawca mając świadomość, że mogą wystąpić sytuacje, gdy nie będzie możliwe ustalenie podmiotu odpowiedzialnego za dalsze przechowywanie dokumentacji medycznej, postanowił, że w takim przypadku odpowiedzialnym za przechowywanie dokumentacji medycznej, prowadzonej przez podmiot zaprzestający wykonywania działalności leczniczej, będzie wojewoda, będący organem rejestrowym dla działalności leczniczej zaprzestającej działalność.

Przykład:
Umarł lekarz A prowadzący jednoosobową działalność gospodarczą w Zakopanem, w ramach której prowadził podmiot leczniczy Z, zatrudniający innych lekarzy. W takiej sytuacji zobowiązanym do prowadzenia i przechowywania dokumentacji medycznej był podmiot leczniczy Z. Z racji, że był to podmiot leczniczy, a nie indywidualna praktyka lekarska to zobowiązanym do przechowywania dokumentacji medycznej nie będzie Okręgowa Izba Lekarska w Krakowie. Ponadto niemożliwe jest zawarcie z innym podmiotem leczniczym umowy o przechowywanie dokumentacji medycznej, gdyż po śmierci lekarza A prowadzona przez niego jednoosobowa działalność gospodarcza podlega wykreśleniu z CEIDG, a tym samym nie może ona realizować umowy o przechowywanie dokumentacji medycznej. Dlatego w powyższej sytuacji odpowiedzialnym za przechowywanie dokumentacji medycznej będzie Wojewoda Małopolski, będący organem rejestrowym dla podmiotu Z.

WYDAWCA
Pracodawcy Zdrowia

NADZÓR MERYTORYCZNY
Zarząd Związku Pracodawców Zdrowia

OPRACOWANIE REDAKCYJNE, KOREKTA, GRAFIKA
JAMANO Sp. z o.o.

PROJEKT GRAFICZNY, SKŁAD I ŁAMANIE
Katarzyna Mróz-Jaskuła, Studio Grafpa, www.grafpa.pl

INFORMACJE O PROJEKCIE
Projekt „Zdrowe Firmy Zdrowi Ludzie podniesienie jakości w POZ" jest realizowany przez Dolnośląski Związek Lekarzy Rodzinnych-Pracodawców w partnerstwie ze związkiem Pracodawców Zdrowia i Fundacją „Promocja Zdrowia-Zdrowie albo tytoń" w ramach umowy WND-POWR.05.02.00-00-0019/17. Projekt jest realizowany w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014–2020 i współfinansowany ze środków Europejskiego Funduszu Społecznego.