Jak przestrzegać RODO **w placówce medycznej**

Fot. istockphoto.com

Raport Najwyższej Izby Kontroli „Wdrożenie przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych" wykazał, że ochrona danych osobowych w szpitalach pozostawia wiele do życzenia. Zasadne jest założenie, że w innych placówkach medycznych sytuacja wygląda podobnie. Jak powinny postępować podmioty lecznicze, by z jednej strony należycie chronić dane osobowe pacjentów, a z drugiej nie wprowadzać „absurdów RODO"?

Bezpieczeństwo informacji w placówkach medycznych to wyzwanie, które istniało na długo przed 25 maja 2018 r. Wejście w życie ogólnego rozporządzenia o ochronie danych sprawiło, że wiele niejasnych kwestii zwróciło uwagę opinii publicznej, ale wygenerowało też nowe problemy. Sprawy te zostały wypunktowane w jednym z ostatnich raportów NIK – w niniejszym artykule przyjrzymy się kluczowym obszarom wskazanym w trakcie kontroli i odpowiemy, jak powinny się z nimi mierzyć podmioty lecznicze.

Dokumentacja ochrony danych osobowych

Zgodnie z RODO każda placówka medyczna (administrator danych) powinna nie tylko przestrzegać przepisów o ochronie danych, ale także być w stanie to udowodnić. Tak rozumiana zasada rozliczalności może być realizowana w szczególności przez prowadzenie dokumentacji ochrony danych osobowych zawierającej procedury, wytyczne, instrukcje itp. uregulowania związane z bezpieczeństwem informacji.

Z raportu NIK wynika, że większość szpitali utrzymała model obowiązujący przed 25 maja 2018 r., tj. gros reguł pozostało ujętych w polityce bezpieczeństwa. Zastrzeżenia NIK budzi jednak treść tych polityk.

W jedenastu skontrolowanych podmiotach leczniczych (45,8 proc.) nie zaktualizowano wraz z wejściem w życie RODO podstawowych dokumentów opisujących bezpieczeństwo danych osobowych oraz sposoby ich przetwarzania. Chociaż posiadana dokumentacja nie zawierała niezbędnych uregulowań (…) jej aktualizację w siedmiu szpitalach przeprowadzono dopiero po upływie od 37 do 263 dni od wejścia w życie nowych uregulowań[1].

Jedną z przyczyn takiej sytuacji jest zmiana modelu prawa o ochronie danych osobowych. W przeciwieństwie do wcześniejszych przepisów RODO nie daje zbyt wielu konkretnych zaleceń dotyczących bezpieczeństwa

informacji. W treści ogólnego rozporządzenia o ochronie danych wprost mówi się jedynie o trzech dokumentach:
- rejestrze czynności przetwarzania (zastępującym ewidencję zbiorów danych osobowych),
- rejestrze kategorii czynności przetwarzania (prowadzonym, jeśli placówka medyczna jest tzw. podmiotem przetwarzającym dane osobowe),
- ewidencji naruszeń ochrony danych osobowych.

Z treści zaleceń NIK, ale także przepisów obowiązującego prawa można jednak wywnioskować konieczność posiadania przez placówkę medyczną innych dokumentów związanych z ochroną danych osobowych.

Na dokumentację ochrony danych osobowych w placówce medycznej powinny się składać następujące elementy:

- rejestr czynności przetwarzania,
- rejestr kategorii czynności przetwarzania,
- ewidencja naruszeń ochrony danych osobowych,
- sposób postępowania z naruszeniami ochrony danych osobowych (procedura alarmowa),
- procedura rozpatrywania „wniosków z RODO" (w sprawie dostępu do danych, kopii danych, prawa do bycia zapomnianym itp.),
- procedura udostępniania dokumentacji lub informacji medycznych,
- zasady pracy w systemach informatycznych.

Umowy związane z wykorzystaniem danych osobowych

Podmioty lecznicze były obowiązane do zawierania pisemnych umów powierzenia przetwarzania danych, gdy udostępniają takie dane podmiotom zewnętrznym. W pięciu ze skontrolowanych szpitali (21 proc.) stwierdzono błędy w tym zakresie[2].

Raport NIK zwraca uwagę przede wszystkim na umowy powierzenia przetwarzania danych osobowych. W takich porozumieniach mamy dwie strony: administratora danych (podmiot dominujący, który określa cele wykorzystania danych osobowych) i podmiot przetwarzający (podmiot podległy, który wykorzystuje dane dla celów wskazanych przez administratora). Istnieją jednak także sytuacje, w których przekazywanie danych między placówką medyczną a podmiotem zewnętrznym jest relacją dwóch równorzędnych partnerów udostępniających dane osobowe, np. przy świadczeniu usług z zakresu medycyny pracy.

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[3] – wskazał jeszcze w październiku 2018 r. prezes Urzędu Ochrony Danych Osobowych.

Niezawieranie umów związanych z wykorzystaniem danych w sytuacji, gdy wymagają tego przepisy RODO, może mieć poważne konsekwencje. Prezes Urzędu Ochrony Danych Osobowych 30 października 2019 r. nałożył administracyjną karę pieniężną (40 000 zł) na burmistrza Aleksandrowa Kujawskiego m.in. za niezawarcie umowy powierzenia z podmiotem zewnętrznym[4].

Zalecenia dotyczące umów związanych z wykorzystaniem danych osobowych:

- informowanie inspektora ochrony danych (lub innej osoby odpowiedzialnej za ochronę danych osobowych) o każdej zawieranej umowie, w ramach której będzie dochodziło do przekazywania danych osobowych (w celu weryfikacji, czy wymagane jest zawarcie umowy powierzenia, udostępnienia, współadministrowania lub innej),
- dokonanie przeglądu obecnie obowiązujących umów z podmiotami zewnętrznymi w celu sprawdzenia, czy we wszystkich wymagających tego przypadkach zawarto umowę powierzenia (lub inną dotyczącą przekazywania danych),
- w razie stwierdzenia, że odpowiednie umowy związane z przekazaniem danych nie zostały zawarte, skontaktowanie się z właściwymi kontrahentami i wskazanie na konieczność podpisania porozumienia (nie ma znaczenia, która ze stron zaproponuje zawarcie umowy – jej podpisanie leży w interesie obu podmiotów).

Klauzule informacyjne

Klauzule zawierające informacje o wykorzystaniu danych osobowych to dla wielu pacjentów lub członków ich rodzin pierwsze zetknięcie się z RODO w przestrzeni placówki medycznej. Najwyższa Izba Kontroli zwróciła uwagę na to, że w kilku sytuacjach problemem była nie sama treść klauzuli, ale jej fizyczne udostępnienie pacjentom: *W Powiatowym Centrum Zdrowia sp. z o.o. w Drezdenku – z powodu niedopatrzenia – przy żadnej z rejestracji ani w ogólnodostępnym dla pacjentów miejscu nie umieszczono klauzul informacyjnych RODO. W trakcie kontroli NIK w budynku Szpitala klauzule informacyjne RODO zamieszczono na tablicach informacyjnych, w głównej rejestracji i w Izbie Przyjęć*[5].

Na drugim biegunie problemów związanych z klauzulami informacyjnymi znajduje się kwestia podpisywania klauzul przez osoby, dla których są przeznaczone. Wiele placówek jest przekonanych, że nie będzie w stanie wykazać spełnienia zasady rozliczalności, jeżeli pacjenci nie podpiszą obowiązku informacyjnego. Tymczasem z uważnej lektury art. 12 ust. 1 RODO wynika, że podmiot medyczny – jako administrator danych – jest zobowiązany do dania osobom, których dane dotyczą, realnej szansy zapoznania się z treścią obowiązku informacyjnego.

Prywatność pacjentów

Poszanowanie intymności i godności osób korzystających z usług placówki medycznej nie zaczyna się dopiero za drzwiami gabinetu lekarskiego. Już na etapie rejestracji i oczekiwania na przyjęcie obsługa pacjentów powinna odbywać się w sposób, który gwarantuje, że

Spełnienie powyższego postulatu wymaga wzięcia pod uwagę potrzeb różnych odbiorców: regularnie odwiedzających placówkę medyczną, przychodzących do lekarza sporadycznie, posiadających dostęp do Internetu lub nie. Optymalne będzie publikowanie klauzuli informacyjnej na kilka sposobów:

- przez umieszczenie na tablicy informacyjnej lub tablicy ogłoszeń (jak w przykładzie przywołanym w raporcie NIK),
- przez wydrukowanie kilku egzemplarzy i umieszczenie na rejestracji w taki sposób, by pacjent (lub inna osoba) mógł zabrać ze sobą egzemplarz,
- przez umieszczenie na stronie internetowej placówki medycznej lub w Biuletynie Informacji Publicznej (jeżeli podmiot jest zobowiązany do prowadzenia BIP-u).

osoby postronne nie będą w stanie wejść w posiadanie informacji, które nie są dla nich przeznaczone (np. który konkretnie pacjent leczy się u lekarza danej specjalności).

Szczególną uwagę w tym zakresie raport NIK poświęca stanowiskom rejestracji: *Dziewięć szpitali (37,5 proc.) nie zapewniło odpowiednich odległości między oknami rejestracji lub przesłon między nimi, a sześć nie wyznaczyło stref oddzielających pacjentów obsługiwanych przy okienkach od reszty osób w kolejce. W trzech kolejnych podmiotach mimo zapewnienia odpowiedniego usytuowania okien rejestracji nie wprowadzono środków gwarantujących zachowanie odległości pomiędzy osobami rejestrującymi się i oczekującymi w kolejce*[6].

Z satysfakcją należy natomiast odnotować, że praktycznie we wszystkich kontrolowanych jednostkach zrezygnowano z wyczytywania pacjentów po nazwiskach (zamiast tego stosuje się takie rozwiązania, jak systemy numerkowe, wyczytywanie pacjentów po imieniu lub wyczytywanie po umówionej godzinie wizyty).

Zalecenia związane z poszanowaniem prywatności pacjentów:

- umieszczenie przy rejestracji informacji: Przy stanowisku rejestracji może przebywać tylko jedna osoba,
- umieszczenie na podłodze przed rejestracją linii określającej strefę, poza którą czekają na swoją kolej inni pacjenci,
- ustawienie krzeseł przy rejestracji w taki sposób, by nie było możliwe przypadkowe usłyszenie rozmowy pracownika rejestracji z pacjentem przez inne osoby,
- ustawienie przepierzeń między poszczególnymi stanowiskami (jeżeli w rejestracji jest więcej niż jedno „okienko"),
- unikanie wyczytywania pacjentów po nazwisku (w zamian możliwe jest wyczytywanie pacjenta po numerze nadanym w rejestracji, po imieniu lub po godzinie wizyty). Wywoływanie po nazwisku jest dopuszczalne w wyjątkowych sytuacjach (np. na Szpitalnych Oddziałach Ratunkowych, w jednostkach ratownictwa medycznego, a także wtedy, gdy ze względu na zagrożenie życia lub zdrowia pacjenta nie jest możliwe posłużenie się inną metodą).

Przechowywanie papierowej dokumentacji medycznej

Przechowywanie dokumentacji w placówkach medycznych jest problemem konsekwentnie podnoszonym przez NIK. W raporcie z 2019 r. wskazano:

W dziewięciu szpitalach (37,5 proc.) nie zapewniono właściwego przechowywania papierowej dokumentacji medycznej pacjentów. Podręczna papierowa dokumentacja pielęgniarska, zawierająca dane osobowe pacjentów, znajdowała się w niezamykanych szafkach usytuowanych w otwartych pomieszczeniach. (…) Najczęstszymi przyczynami niezapewnienia właściwych warunków do przechowywania dokumentacji medycznej było przeświadczenie personelu, że wystarczą pokoje lekarskie i dyżurki pielęgniarskie zamykane na klucz, lub oczekiwanie na remont pomieszczeń, który obejmie również meble na oddziałach, niedostosowane do przechowywania dokumentacji pacjentów w zamknięciu.

Z kolei w raporcie z 2015 r. zwracano uwagę np. na następujące niedociągnięcia w przechowywaniu dokumentacji w monitorowanych placówkach:

- brak zabezpieczeń okien w pomieszczeniach, w których przechowywano dokumentację,
- obecność zacieków wodnych w sytuacji, w której dokumentacja była jedynie częściowo nakryta folią lub w ogóle nie była zabezpieczona,
- przechowywanie dokumentacji luzem, bezpośrednio na podłodze[7].

Nie istnieje jedno, uniwersalne rozwiązanie tego problemu, można jednak wskazać oczekiwane kierunki działań.

W celu właściwego przechowywania dokumentacji medycznej placówka medyczna powinna w szczególności:

- w miarę możliwości przechowywać ją w jednym pomieszczeniu, które można dodatkowo zabezpieczyć (np. przez wykorzystanie krat, rolet antywłamaniowych, czujek ruchu) i do którego nie mają dostępu osoby nieupoważnione,
- przechowywać ją w szufladach, szafkach lub szafach zamykanych na klucz; samo zamknięcie na klucz pomieszczenia, gdzie jest dokumentacja, nie pomoże, ponieważ dostęp do pomieszczenia mogą mieć osoby spoza personelu medycznego (np. personel sprzątający) lub włamywacze,
- zwracać uwagę na wspomniane wyżej klucze – powinny być one przechowywane w bezpiecznym miejscu (kryterium tego nie spełnia pozostawianie kluczy w zamkach po godzinach pracy lub ich chowanie w „wiadomym miejscu", jak szuflada lub puszka po herbacie); zalecane jest używanie np. szyfrowanych kluczników.

Przechowywanie dokumentacji archiwalnej wymaga dodatkowo zapewnienia takich warunków, w których dokumenty będą mogły być przetrzymywane przez okres przewidziany przepisami (co do zasady 20 lat od ostatniego wpisu):

- dokumentacja powinna być przechowywana w pomieszczeniach o odpowiedniej wilgotności (ok. 45–60 proc.), temperaturze (ok. 14–20°C) i należycie wentylowanych;
- w razie przechowywania dokumentacji w pomieszczeniach piwnicznych należy uwzględnić ryzyko zalania (np. przez pęknięcie rury, podtopienia lub powodzie). Dokumentacja powinna być umieszczona w zamykanych kartonach, nieustawianych bezpośrednio na podłodze. Najniższa półka z dokumentacją powinna być umieszczona kilka centymetrów nad podłogą;
- w razie przechowywania dokumentacji na strychu należy ją zabezpieczyć przed skutkami zjawisk atmosferycznych (deszcze, śniegi, burze itp.), np. przez obłożenie kartonów folią.

Upoważnienia i uprawnienia osób zatrudnionych

Każda osoba zatrudniona w placówce medycznej powinna mieć określony zakres dostępu do danych osobowych i innych uprawnień, uwzględniający jej obowiązki. Zakres ten będzie inny w przypadku pracownika odpowiedzialnego za sprawy kadrowe, lekarza i osoby sprzątającej. Tymczasem i tutaj NIK miała zastrzeżenia do sposobu postępowania, zwracając w szczególności uwagę na:

- nieodpowiednie uprawnienia pielęgniarek dotyczące dostępu do danych osobowych pacjentów w szpitalnym systemie informatycznym (HIS),
- brak odpowiednich upoważnień do przetwarzania danych osobowych pacjentów,
- nadawanie upoważnień osobom, które nie powinny przetwarzać danych osobowych.

Niekontrolowany dostęp do danych osobowych w placówce medycznej może być źródłem problemów finansowych. Większość podmiotów medycznych karanych w Unii Europejskiej za naruszenia przepisów o ochronie danych osobowych ma na sumieniu właśnie nieodpowiednie uregulowanie zasad dostępu do informacji medycznych lub danych osobowych[8].

Inaczej będzie się mierzyć z problemem upoważnień niewielki ośrodek zdrowia, a inaczej szpital wojewódzki, jednak wszyscy administratorzy danych powinni przestrzegać pewnych wspólnych zasad.

Właściwe nadawanie upoważnień do dostępu do danych osobowych, baz danych lub systemów informatycznych wymaga:

- sporządzenia zbiorczej listy wszystkich zasobów, do których mogą mieć dostęp osoby zatrudnione w placówce medycznej (dane osobowe pacjentów, dane osobowe osób zatrudnionych, konto w systemie IT, kod PIN do alarmu, nagrania z monitoringu itp.),
- powiązania określonych stanowisk w hierarchii służbowej z dostępem do danych lub systemów (w razie potrzeby decyzję o zmianie powinien podejmować, po konsultacji z IOD, bezpośredni przełożony),
- określenia, kto nadaje osobie zatrudnionej upoważnienia lub dostępy i kto je w razie potrzeby odbiera.

Nadawanie i odbieranie upoważnień może być w szczególności uregulowane w ramach „obiegówki" (lub włączone do już istniejącego u administratora systemu wydawania sprzętu służbowego).

Udostępnianie dokumentacji medycznej

Podczas kontroli NIK nie stwierdzono zbyt wielu naruszeń przepisów związanych z wydawaniem dokumentacji medycznej. Przyczyną takich incydentów (dotyczących 16,7 proc. badanych szpitali) było przede wszystkim:

- niewłaściwe zweryfikowanie (lub brak weryfikacji) tożsamości lub uprawnień wnioskodawcy,
- nieuwzględnianie upoważnień do dostępu do dokumentacji lub informacji medycznej,
- niewłaściwe zabezpieczenie miejsca przechowywanie dokumentacji (NIK przywołuje m.in. sytuację, w której niezrównoważony psychicznie mężczyzna ukradł z pomieszczenia rejestracji dokumentację kilku pacjentów[9]).

Zalecenia związane z udostępnianiem dokumentacji medycznej:

- przed wydaniem dokumentacji medycznej komukolwiek (pacjentowi, osobie upoważnionej, przedstawicielowi podmiotu zewnętrznego) należy dokonać weryfikacji uprawnień (czy wnioskodawca ma prawo otrzymać dokumentację lub informację?) i weryfikacji tożsamości (czy wnioskodawca rzeczywiście jest osobą, za którą się podaje?),
- w razie wątpliwości co do tożsamości pacjenta, przedstawiciela ustawowego lub innej osoby upoważnionej placówka medyczna ma prawo zażądać okazania dokumentu potwierdzającego tożsamość (dowodu osobistego),
- każde wydanie dokumentacji medycznej powinno być odnotowywane w wykazie prowadzonym zgodnie z art. 27 ust. 4 ustawy o prawach pacjenta,
- miejsce przechowywania papierowej dokumentacji medycznej powinno być zabezpieczone przed dostępem osób nieupoważnionych.

Zabezpieczenie danych przechowywanych w formie elektronicznej

Bardzo poważnym problemem w placówkach kontrolowanych przez NIK jest zabezpieczenie danych przechowywanych w formie elektronicznej:

W 18 skontrolowanych szpitalach (75 proc.) nie zastosowano odpowiednich środków technicznych do zabezpieczenia danych osobowych przechowywanych w postaci elektronicznej. Poszczególne elementy wpływające na bezpieczeństwo zostały niewłaściwie zaplanowane bądź były w nieodpowiedni sposób użytkowane. Stanowiło to naruszenie art. 5 ust. 1 lit. f RODO, zobowiązującego do przetwarzania danych osobowych w sposób zapewniający ich bezpieczeństwo (w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem), za pomocą odpowiednich środków technicznych lub organizacyjnych[10].

Takie zabezpieczenia powinny przede wszystkim gwarantować, że osoba nieupoważniona nie będzie mogła uzyskać dostępu do systemu lub komputera, na którym pracuje system. Część środków bezpieczeństwa jest uzależniona od konkretnego systemu informatycznego, istnieją jednak ogólne zalecenia, które powinny być przestrzegane wszędzie.

Zalecenia związane z zabezpieczeniem danych przechowywanych w formie elektronicznej:

- zagwarantowanie, aby każda osoba mająca dostęp do systemu informatycznego posiadała swój login i swoje hasło (w ocenie NIK wykorzystywanie zbiorczych kont nie powinno mieć miejsca, ponieważ utrudnia przypisanie odpowiedzialności konkretnej osobie, a także narusza rozporządzenie w sprawie Krajowych Ram Interoperacyjności[11]),
- system powinien wymuszać stosowanie przez pracowników odpowiednio skomplikowanych haseł (minimum 8 znaków, w tym małe i wielkie litery, cyfry lub znaki specjalne),

- pracownicy powinni zostać pouczeni o konieczności zachowania haseł w tajemnicy (obejmuje to zarówno zakaz udostępniania haseł między pracownikami, jak i zapisywanie haseł na karteczkach, pod klawiaturą lub w innych miejscach, do których mogą uzyskać dostęp osoby nieupoważnione),
- pracownicy powinni mieć dostęp do kont z uprawnieniami na poziomie administratora w sytuacji, gdy rzeczywiście jest to niezbędne do wykonywania ich obowiązków,
- komputer pracownika placówki medycznej powinien automatycznie blokować się w przypadku dłuższej nieobecności pracownika (np. przez włączenie wygaszacza ekranu); pracownicy powinni być nauczeni blokowania komputera przy każdym odejściu od stanowiska pracy (np. przez wybranie na klawiaturze kombinacji WINDOWS + L),
- na wszystkich komputerach wykorzystywanych w placówce medycznej (nawet niepodłączonych do Internetu) powinno być zainstalowane oprogramowanie antywirusowe, które jest na bieżąco aktualizowane.

Dostęp do systemów informatycznych

Kwestia nadawania odpowiednich uprawnień w systemach IT została omówiona wcześniej, w tym miejscu natomiast zwracamy uwagę na bardzo niepokojące zjawisko, jakim jest brak dbałości o cofnięcie uprawnień w systemach po zakończeniu współpracy.

W 15 skontrolowanych podmiotach leczniczych (62,5 proc.) nie wywiązano się z obowiązku niezwłocznego odbierania byłym pracownikom uprawnień do systemów informatycznych tych jednostek (…)[12]. W skrajnym przypadku opisanym przez NIK zablokowanie dostępu nastąpiło dopiero 227 dni (ponad 7 miesięcy!) po zakończeniu współpracy[13].

Niezachowywanie przez placówkę medyczną kontroli nad osobami mającymi dostęp do systemów IT może powodować ryzyko zarówno dla pacjentów (bezprawne edytowanie lub usuwanie informacji), jak i dla samej placówki medycznej. Portugalski Centro Hospitalar Barreiro Montijo otrzymał w zeszłym roku 150 tys. euro kary za naruszenie RODO przez niewłaściwe uregulowanie dostępu do danych pacjentów (w momencie kontroli ustalono istnienie 985 kont dla lekarzy w szpitalnym systemie IT, choć w rzeczywistości pracowało tam jedynie 296 lekarzy)[14].

W celu uniknięcia sytuacji, w których w ewidencji upoważnień, systemie IT lub bazie danych placówki medycznej figurują „martwe dusze", należy przede wszystkim przestrzegać procedury nadawania i odbierania upoważnień (opisanej wcześniej). Zasadne jest też wykonywanie z określoną częstotliwością (np. raz do roku) przeglądu listy osób mających dostęp do systemów IT (dostarczonej przez informatyka) oraz listy osób zatrudnionych w placówce medycznej (dostarczonej przez osobę odpowiedzialną za sprawy kadrowe) w celu ustalenia, czy nie występują w nich jakieś rozbieżności wymagające interwencji.

Szkolenia osób zatrudnionych

Światowej klasy zabezpieczenia informatyczne, szyfrowane kluczniki, procedury udostępniania dokumentacji medycznej – wszystkie te środki techniczne i organizacyjne zawiodą, jeżeli osoby na co dzień pracujące z danymi osobowymi nie będą świadome tego, w jaki sposób mają postępować i jakie będą ewentualne konsekwencje naruszenia zasad bezpieczeństwa (dla nich lub dla placówki medycznej). Niezastąpionym elementem systemu bezpieczeństwa są zatem szkolenia.

W raporcie NIK zwrócono uwagę, że w podmiotach medycznych, w których przeszkolono z RODO co najmniej 95 proc. personelu, było najmniej istotnych nieprawidłowości dotyczących ochrony danych osobowych pacjentów[15]. Celem administratora powinno być zatem przeszkolenie jak największej liczby osób (oraz bieżące szkolenie nowych pracowników).

Przepisy prawa nie wskazują, jaką formę mają mieć szkolenia z ochrony danych osobowych. Najbardziej wartościowe są szkolenia prowadzone na żywo przez osobę, której można zadawać dodatkowe pytania, ale dopuszczalne jest także wykorzystywanie innych sposobów, np. e-learningu, webinariów, prezentacji lub materiałów szkoleniowych. Z uwagi na zmieniający się stan prawny (zarówno w zakresie przepisów medycznych, jak i związanych z ochroną danych) szkolenia takie powinny być organizowane minimum raz do roku.

Adam Klimowski
główny specjalista ds. ochrony danych osobowych, prawnik, JAMANO sp. z o.o.

Przypisy

[1] 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. 26.11.2019 r.), s. 10.
[2] *Ibidem*, s. 10.
[3] Urząd Ochrony Danych Osobowych, *Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców* (https://uodo.gov.pl/pl/file/1469, dostęp 02.12.2019 r.)
[4] 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. 02.12.2019 r.)
[5] Najwyższa Izba Kontroli, *op.cit.*, s. 31.
[6] *Ibidem*, s. 30.
[7] 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. 02.12.2019 r.), s. 27.
[8] A. Klimowski, *Które podmioty ukarano za naruszenie RODO?* (https://www.termedia.pl/mz/Ktore-podmioty-ukarano-za-naruszenie-RODO-,35513.html, dostęp dn. 02.12.2019 r.)
[9] 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. 02.12.2019 r.), s. 43.
[10] *Ibidem*, s. 13.
[11] *Ibidem*, s. 46.
[12] *Ibidem*, s. 12.
[13] *Ibidem*, s. 40.
[14] A. M. Monteiro, *First GDPR fine in Portugal issued against hospital for three violations* (https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/, dostęp dn. 02.12.2019 r.).
[15] Najwyższa Izba Kontroli, *op.cit.*, s. 8.