

RODO w placówkach medycznych

radca prawny Maciej Łokaj



Wolters Kluwer | Szkolenia **online**

Gdańsk, 13.12.2017 r.

www.szkolenia.wolterskluwer.pl

Zasady szkolenia online



Czas trwania szkolenia

60 minut (45 minut + 15 minut pytania lub 50/10)



Pytania techniczne

czat lub e-mail
szkolenia@wolterskluwer.pl



Czat moderowany

Pytania, problemy techniczne
uwagi



Materiały dodatkowe

w publikacji



Prelegent: Maciej Łokaj

Moderator: Alicja Plichta



Prelegent: Maciej Łokaj

Radca prawny. Działalność prawniczą prowadzi od 2010 roku. Zajmuje się obsługą przedsiębiorców, organizacji pozarządowych oraz podmiotów sektora publicznego. Specjalista w dziedzinie prawa ochrony zdrowia. Jego doświadczenie zawodowe obejmuje obsługę prawną licznych podmiotów wykonujących działalność leczniczą (szpitale, przychodnie). Jako ekspert LEX Ochrona Zdrowia od wielu lat współpracuje z Wolters Kluwer Polska S.A. Współpraca obejmuje przygotowanie różnego typu publikacji, w tym komentarzy praktycznych, udzielanie odpowiedzi na pytania zadawane przez użytkowników oraz uczestnictwo w konferencjach i szkoleniach w roli eksperta.

Dlaczego o tym mówimy?

- administracyjne kary pieniężne,
- do 20.000.000 EUR lub
- do 4% całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego,

CZĘŚĆ I

RODO – zakres regulacji i zasady stosowania

Podstawa prawna

- rozporządzenie 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 (ogólne rozporządzenie o ochronie danych), tzw. RODO
- wejście w życie a stosowanie,

Co dalej z przepisami krajowymi?

- uzupełniający charakter regulacji krajowych
- ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych – koniec obowiązywania z dniem 25 maja 2018 roku,
- koniec obowiązywania rozporządzeń wykonawczych w tym:
 - rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
 - rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych,
- nowa ustawa o ochronie danych osobowych (projekt z dnia 12 września 2017 roku)

Co będzie regulować nowa ustawa krajowa?

- inspektor ochrony danych osobowych,
- certyfikacja i akredytacja,
- UODO,
- postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych,
- postępowanie kontrolne,
- odpowiedzialność cywilna,
- administracyjne kary pieniężne,

Zakres stosowania RODO

- zakres przedmiotowy – zautomatyzowane i niezautomatyzowane zbiory danych osobowych,
- zakres podmiotowy – wyznaczany przez zawarte w RODO definicje administratora i podmiotu przetwarzającego,
- zakres terytorialny – jednostki organizacyjne działające na terytorium UE zarówno mające jak i nie mające siedziby na terenie UE,

Przetwarzanie danych osobowych wg. RODO

- dane osobowe - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, gdzie możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
- przetwarzanie - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

Dane osobowe dotyczące zdrowia

- wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą,
- informacje zbierane w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych, podczas rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej,
- informacje pochodzące z badań laboratoryjnych lub lekarskich, części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych,
- wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą,
- informacje pozyskane bez względu na źródło – lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro,

Przetwarzanie danych dotyczących zdrowia

- dane identyfikujące – pozwalające na ustalenie tożsamości pacjenta
- dane wrażliwe (sensytywne) – m. in. informacje dotyczące stanu zdrowia pacjenta
- generalny zakaz przetwarzania danych sensytywnych przy szeregu wyjątków,
- w odniesieniu do danych medycznych przetwarzanie jest dopuszczalne pod warunkiem, że jest to niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego lub jest to niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych,
- bezpośrednia odpowiedzialność za przetwarzanie medycznych danych osobowych pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej

CZĘŚĆ II

RODO a obowiązki placówek medycznych

Obowiązki placówki medycznej jako administratora danych

- obowiązki informacyjne (m. in. dane kontaktowe placówki, dane inspektora ochrony danych osobowych, cel przetwarzania, odbiorcy danych osobowych i kategorie tychże odbiorców),
- prawa pacjenta w związku z danymi osobowymi: prawo dostępu do danych, prawo sprostowania danych (wyłączenie prawa „do bycia zapomnianym”),
- obowiązek reakcji na każde żądanie dostępu czy sprostowania nie dłużej niż w ciągu miesiąca od otrzymania żądania, a w przypadkach szczególnie skomplikowanych nie dłużej niż w ciągu łącznie trzech miesięcy,
- obowiązek wdrożenia wszelkich niezbędnych środków technicznych i organizacyjnych, w celu zapewnienia przetwarzania danych w sposób zgodny z rozporządzeniem (upoważnienia do dostępu, ewidencje osób mających dostęp, polityki ochrony danych)

Powierzenie przetwarzania

- obowiązek zawierania umów powierzenia przetwarzania w formie pisemnej,
- umowa winna stanowić, w szczególności, że podmiot, któremu powierzone zostało przetwarzanie danych:
 - dokonuje tego wyłącznie na udokumentowane polecenie administratora,
 - zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
 - podejmuje wszelkie niezbędne środki bezpieczeństwa dla ochrony przetwarzanych danych,
 - przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o ile dysponuje szczegółową i pisemną zgodą administratora danych na dalsze powierzenie,
 - w miarę możliwości wspiera administratora w zakresie wywiązywania się przez niego z obowiązków związanych z ochroną danych osobowych, nałożonych treścią rozporządzenia, a także udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia powyższych obowiązków,
 - 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 nakazuje przechowywanie danych osobowych,
 - umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji,

Inspektor ochrony danych osobowych

- funkcja obligatoryjna,
- wykonywanie zadań na podstawie umowy o pracę lub umowy cywilnoprawnej,
- główne zadania Inspektora:
 - informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów i doradzanie im w tej sprawie,
 - monitorowanie przestrzegania niniejszego rozporządzenia oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
 - udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
 - współpraca z organem nadzorczym, tj. Urzędem Ochrony Danych Osobowych,

Zgłoszenie naruszenia zasad ochrony danych osobowych

- bezwzględny obowiązek informowania Urzędu Ochrony Danych Osobowych o każdym stwierdzonym naruszeniu zasad ochrony danych osobowych,
- termin - w ciągu 72 godzin od stwierdzenia naruszenia,
- obowiązek zawiadomienia osoby, której dane dotyczą – jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych,
- brak obowiązku – w przypadku jeżeli jest mało prawdopodobne by skutkowało ono naruszeniem praw lub wolności osób fizycznych,

CZĘŚĆ III

Nowe dokumenty wg. RODO

Rejestr czynności przetwarzania

- obowiązek prowadzenia rejestru, zawierającego w szczególności:
 - imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także inspektora ochrony danych,
 - cele przetwarzania,
 - opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
 - kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
 - jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
 - jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,

Ocena skutków dla ochrony danych

- obowiązek dokonania oceny skutków dla ochrony danych osobowych,
- dokument oceny zawierać będzie, w szczególności:
 - systematyczny opis planowanych operacji przetwarzania i celów przetwarzania,
 - ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
 - ocenę ryzyka naruszenia praw lub wolności osób fizycznych (pacjentów), których dane dotyczą,
 - środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie unijnego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy,

CZĘŚĆ IV

RODO – proces przygotowawczy

Etapy przygotowań



⑩ Audyt wewnętrzny



⑩ Przygotowanie dokumentów



⑩ Szkolenie personelu



Dziękujemy za uwagę.

Partnerzy
merytoryczni
szkolenia



KANCELARIA
RADCY PRAWNEGO
MACIEJ ŁOKAJ



Wolters Kluwer

www.szkolenia.wolterskluwer.pl