O unijnej reformie ochrony danych osobowych - co zmieniło się w Polsce po 25 maja 2018r.?

Adam Wróblewski
ZdrowePodlasie.pl

Białowieża, 07 czerwca 2018 r.
Wiosenne Podlaskie Spotkania Stomatologiczne

Wstęp

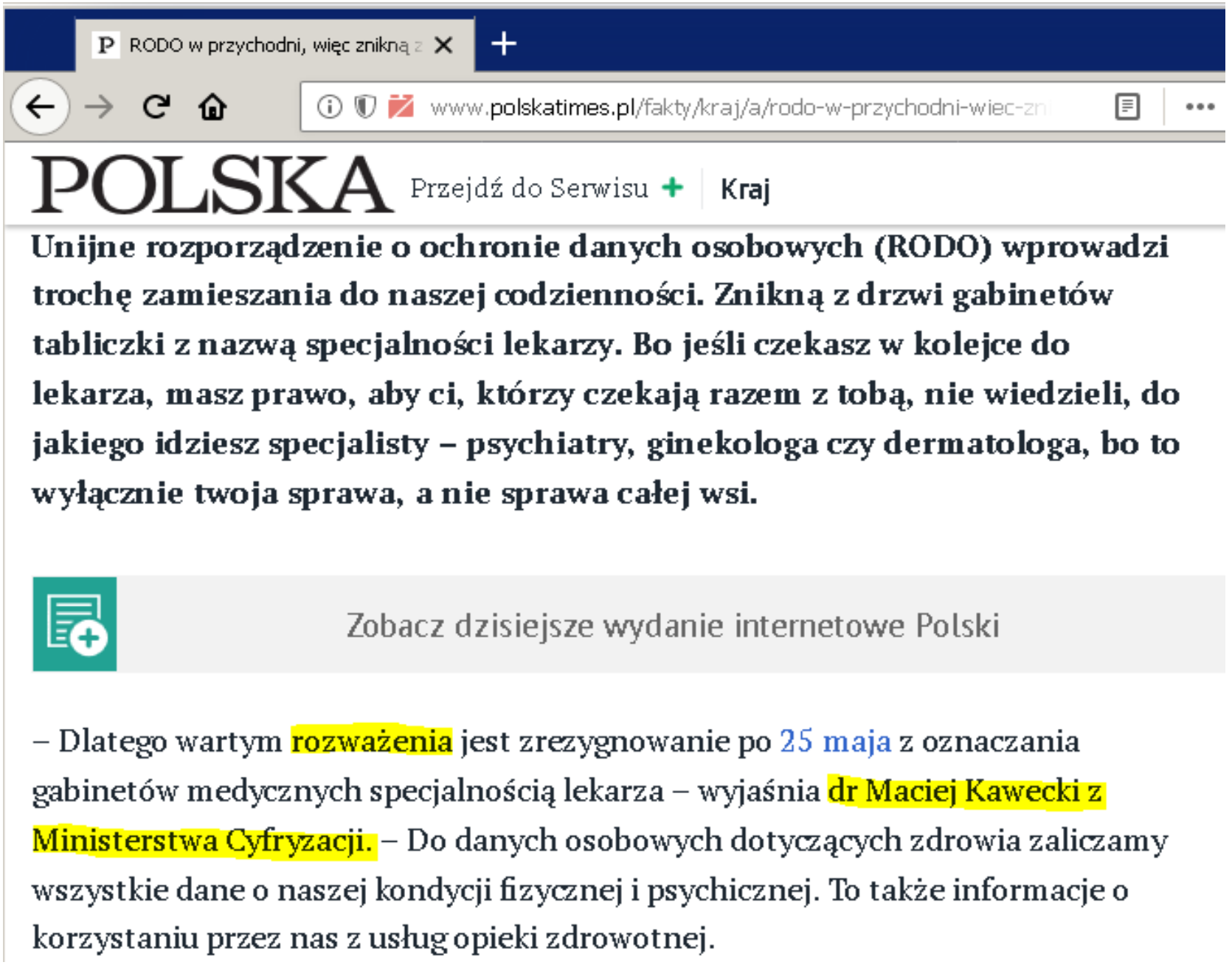
- Organ nadzorczy - po 25.05.2018 miejsce GIODO zajął Urząd Ochrony Danych Osobowych (UODO)
- Na bazie RODO powstała polska Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dziennik Ustaw 2018/1000), która precyzuje pewne rzeczy, wobec których RODO pozostawia dowolność
  - np. maksymalna kara finansowa dla NBP – 100 000 zł
- RODO budzi wiele kontrowersji
  - Ogólność przepisów i jeszcze brak orzecznictwa Sądów
  - Kary finansowe do 20 mln € (wg kursu walut z 28.01)

Kary finansowe

- art. 83 ust. 1 RODO: *„Każdy organ nadzorczy zapewnia, by stosowane na mocy niniejszego artykułu za naruszenia niniejszego rozporządzenia administracyjne kary pieniężne (…) były w każdym* ***indywidualnym*** *przypadku skuteczne, proporcjonalne i odstraszające.”*
- Motyw 148 RODO: "*Jeżeli naruszenie jest niewielkie lub jeżeli grożąca kara pieniężna stanowiłaby dla osoby fizycznej nieproporcjonalne obciążenie, można zamiast tego udzielić upomnienia.*"

Ogólność aktualnych przepisów i daleko idące ich interpretacje

- W Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych znajdował się Art. 36 ust. 1, który nakładał obowiązek ochrony danych osobowych (np. przed utratą, zabraniem, uszkodzeniem, dostępem osób nieupoważnionych)
  - Akt wykonawczy: rozporządzenie MSWiA z 29/04/2004, które nakładało konkretne obowiązki celem ochrony danych osobowych w systemach inf., np. zmiana haseł co 30 dni
- Art. 24 ust. 1 RODO Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz **ryzyko** naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać.



Źródło: http://www.polskatimes.pl/fakty/kraj/a/rodo-w-przychodni-wiec-znikna-z-drzwi-gabinetow-tabliczki-ze-specjalnoscia-lekarzy,13200900/

Inspektor ochrony danych (1/3)

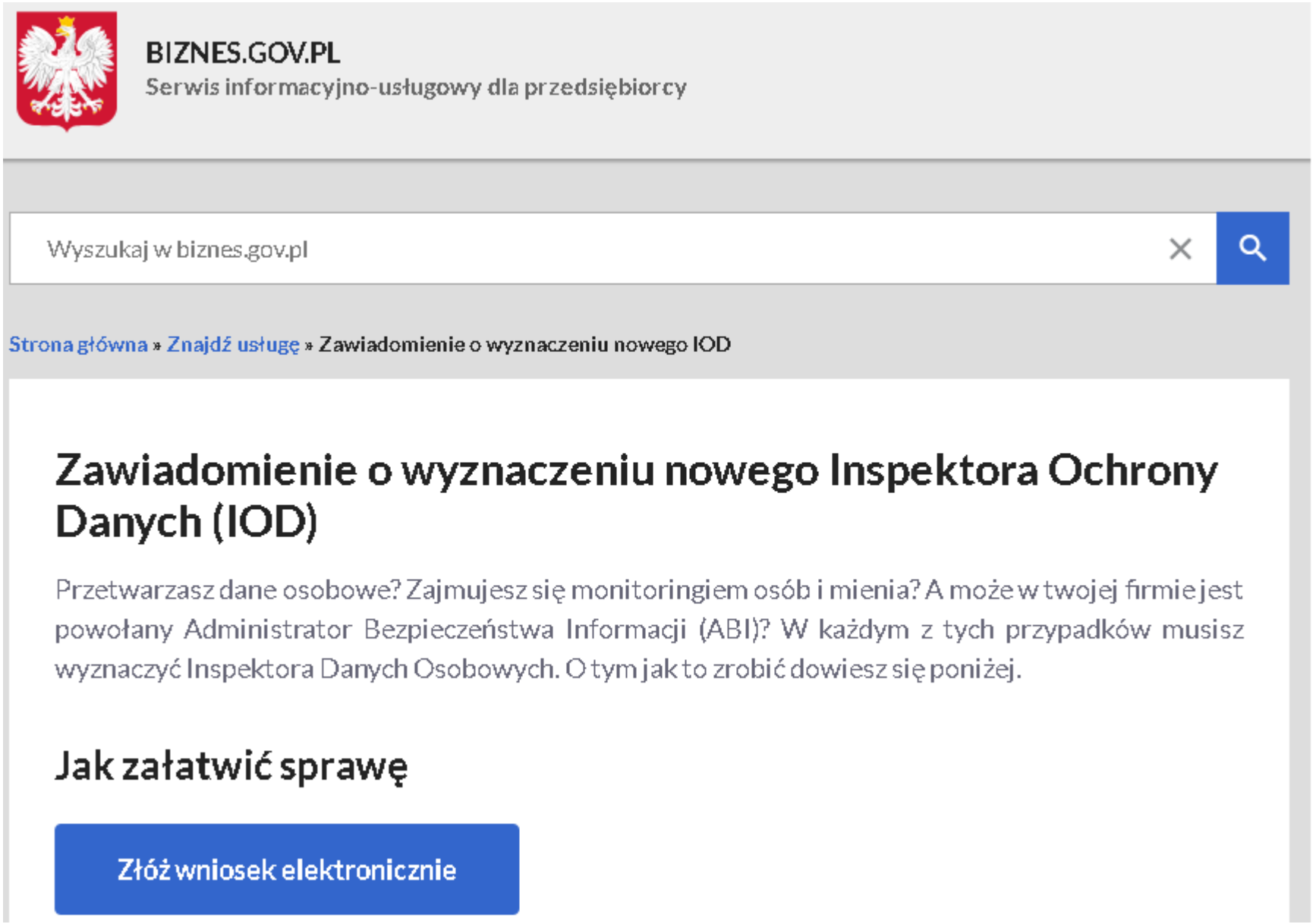
- Inspektor ochrony danych osobowych to taka funkcja, którą można przydzielić konkretnej osobie i do zadań tej osoby będzie należało sprawowanie nadzoru nad bezpieczeństwem danych osobowych
- Inspektor może np.:
  - Przeprowadzać audyty bezpieczeństwa
  - Zastanowić się kiedy ostatnio została wykonana kopia systemu do robienia zdjęć RTG i podjąć działania zmierzające do wykonania takiej kopii
  - Współpracować z organem nadzorczym, gdyż Urząd może zwrócić się do inspektora z jakimś zapytaniem

Inspektor ochrony danych (2/3)

- Poprzednikiem funkcji inspektora był administrator bezpieczeństwa informacji
- Na mocy art. 37 ust. 1 lit. C RODO – każda placówka medyczna, która przetwarza dane osobowe o stanie zdrowia pacjentów na dużą skalę **musi** powołać inspektora ochrony danych osobowych
- Motyw 91 RODO „*Przetwarzanie danych osobowych nie powinno być uznawane za przetwarzanie na dużą skalę, jeżeli dotyczy danych osobowych pacjentów lub klientów i jest dokonywane przez pojedynczego lekarza*”

Inspektor ochrony danych (3/3)

- Jeżeli na właścicielu placówki medycznej w świetle nowych przepisów spoczywa obowiązek wyznaczenia IOD, to powiadomienia należy dokonać (źródło: https://giodo.gov.pl/pl/1520281/10506) :
  - **Do 31/07/2018 r. - gdy administrator nie powołał ABI przed 25/05/2018 r.**
  - do 1 września 2018 r. - gdy administrator wyznaczył ABI przed 25 maja 2018 r. i decyduje, że ta sama osoba będzie pełnić u niego funkcję inspektora ochrony danych
  - w terminie 14 dni – gdy administrator wyznaczył ABI przed 25/05/2018 r., ale IOD będzie inna osoba niż ABI



Adres strony, na której można zgłaszać inspektorów: https://bit.ly/2HatsNb (jest wymagane posiadanie profilu zaufanego ePUAP - https://epuap.gov.pl)

Popularne ryzyka / przykłady naruszeń ochrony danych osobowych

- Awaria komputera (utrata danych) lub pożar
- Pomyłka danych pacjenta podczas wypisywania recepty i wydanie recepty nie temu pacjentowi
- Wirusy komputerowe, które szyfrują dane i wymagają zapłaty za odzyskanie do nich dostępu
- Kradzież danych osobowych papierowych albo kradzież komputera zawierającego dane osobowe
- Udostępnienie dokumentacji medycznej osobie nieupoważnionej (brak weryfikacji tożsamości na podstawie dokumentu tożsamości)

Zgłaszanie naruszeń ochrony danych osobowych

- Na mocy art. 33 RODO, w ciągu 72 godzin od stwierdzenia incydentu, należy zgłosić ten fakt do urzędu ochrony danych osobowych (chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób) oraz – bez zbędnej zwłoki – do osób, których dane dotyczą
- Przykład: jeżeli moje dane zostaną utracone przez placówkę medyczną, to – jeżeli placówka medyczna nie posiada kopii tych danych – wówczas moje prawo do uzyskania kopii dokumentacji medycznej (przy okazji np. przeprowadzki) zostaje naruszone

W jaki sposób powiadomić Prezesa UODO o naruszeniu?

Organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).

1. Zgłoszenia naruszenia dokonuje się elektronicznie **za pomocą odpowiedniego formularza dostępnego poniżej**, który należy wypełnić a następnie...
2. ...załączyć do **pisma ogólnego dostępnego na platformie biznes.gov.pl**

Jeżeli naruszenie dotyczy danych osób w różnych krajach UE, Prezes UODO może być, ale nie musi być wiodącym (czyli właściwym dla administratora lub podmiotu przetwarzającego) organem nadzorczym. W przypadku transgranicznego naruszenia danych administrator powinien dokonać analizy, czy wiodącym organem nadzorczym w odniesieniu do czynności przetwarzania, które zostały objęte naruszeniem jest Prezes UODO, czy też może inny europejski organ nadzorczy (więcej: Wytyczne dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego (WP 244 rew. 01).

2018-05-23

Załączone pliki

Zgłoszenie naruszenia ochrony danych osobowych

Źródło: https://uodo.gov.pl/pl/134/233

Czy warto zgłaszać naruszenia ochrony danych osobowych?

art. 83 ust. 2 (...) **Decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na:** c) działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą; b) umyślny lub nieumyślny charakter naruszenia; h) **sposób, w jaki organ nadzorczy dowiedział się o naruszeniu**, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie;

Aktualnie obowiązują w Polsce dwa sprzeczne przepisy prawa (1/2)

- Art. 15 ust. 3 RODO "*Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych.*"
- Art. 28. ust. 1. Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta *„Za udostępnienie dokumentacji medycznej (...) podmiot udzielający świadczeń zdrowotnych może pobierać opłatę.”*

Aktualnie obowiązują w Polsce dwa sprzeczne przepisy prawa (2/2)

„Pacjenci mają między innymi prawo dostępu do swoich danych osobowych, które mogą zrealizować również poprzez zażądanie ich kopii. Placówki medyczne przetwarzają dane osobowe dotyczące zdrowia pacjentów w szczególności w prowadzonej dokumentacji medycznej. ***Realizując zatem ww. obowiązek będą zobowiązane do bezpłatnego udostępnienia pierwszej kopii dokumentacji medycznej.***”- źródło: strona Rzecznika Praw Pacjenta (https://bit.ly/2sB4KQR)

Zasada prawidłowości danych

- Art. 5 ust. 1 RODO: "Dane osobowe muszą być: d) prawidłowe i w razie potrzeby uaktualniane”
- Jak to zrobić w praktyce?
  - Na początku wizyty, można zapytać pacjenta o imię, nazwisko, datę urodzenia, adres. Jeżeli pacjent poda dane zgodne z tym,które znajdują się na posiadanej przez Państwa karcie historii choroby–unikniemy pomyłki podczas tworzenia dokumentacji, wystawiania recept
  - Można spisywać dane z dokumentu tożsamości (dowód osobisty, prawa jazdy, paszport)

Umowy powierzenia przetwarzania danych osobowych

- Z firmami, dla których przekazują Państwo dane osobowe pacjentów lub pracowników należy podpisać umowę powierzenia przetwarzania danych osobowych, np.: technik dentystyczny, księgowość
- Wzory tego typu umów można znaleźć po wpisaniu „RODO wzór umowy powierzenia” w Google
- Jeśli u Państwa podwykonawcy zdarzy się naruszenie ochrony danych, powinien on poinformować Państwa, a Państwo Urząd i osoby, których dane dotyczą (np. pacjenci, pracownicy)

Rejestr czynności przetwarzania

- Artykuł 30 RODO ust. 1. *„Każdy administrator (…) prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają.”*
- Obowiązek dotyczy także placówek medycznych, w związku z Art. 30 RODO ust. 5 *„Obowiązki, o których mowa w ust. 1 i 2, nie mają zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie (...) obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1”*

Przykład rejestru czynności przetwarzania

Lp	1
Nazwa zbioru danych osobowych	Dokumentacja medyczna pacjentów w postaci papierowej
Lokalizacja	Szafa w pokoju nr 1 w lokalizacji: 15-080 Białystok, ul. Przykładowa 1
art. 30 ust. 1 lit. 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;	NZOZ Stomatologia Jan Kowalski 15-080 Białystok, ul. Przykładowa 1 tel.: 85/000-000-000 Inspektor ochrony danych osobowych: Jan Nowak, tel. 85/000-000-000
art. 30 ust. 1 lit. b) cele przetwarzania;	Organizacja udzielania świadczeń zdrowotnych oraz prowadzenie dokumentacji medycznej pacjentów korzystających z usług medycznych realizowanych w placówce medycznej prowadzonej przez administratora danych osobowych

Przykład rejestru czynności przetwarzania

art. 30 ust. 1 lit. c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;	Dane osobowe pacjentów placówki medycznej. Są to dane osobowe "zwykłe" (np. imię, nazwisko, PESEL) w rozumieniu art. 6 RODO oraz szczególne kategorie danych osobowych w rozumieniu art. 9 ust. 1 RODO, w szczególności dane dotyczące zdrowia.
art. 30 ust. 1 lit. d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;	Dla technika dentystycznego NAZWA I ADRES TECHNIKA jest przekazywane „zlecenie świadczenia protetycznego/ortodontycznego” (zał. nr 3 do zarządzenia 2017/023/DSOZ Prezesa NFZ).
art. 30 ust. 1 lit. 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;	Nie dotyczy ponieważ dane osobowe nie są przekazywane do państw trzecich lub organizacji międzynarodowych .

Przykład rejestru czynności przetwarzania

art. 30 ust. 1 lit. f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;	Zgodnie z art. 29 USTAWY z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta
art. 30 ust. 1 lit. g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.	Szafa z dokumentacją medyczną jest zamykana na klucz. Pokój, w którym znajduje się szafa jest zamykany na klucz. Budynek jest zamykany na klucz. Alarm w budynku. Współpraca z agencją ochrony. Monitoring pokoju z szafą. Dostępność gaśnicy w pokoju, w którym znajduje się szafa. Dostęp do danych posiadają jedynie osoby upoważnione. Klucz do szafy posiadają: XXXX, klucz do pokoju z szafą posiadają: XXXX, klucz do budynku posiadają: XXXXX. Kod do alarmu znają: XXX.

Rozszerzony obowiązek informacyjny

- Art. 13 ust. 1 RODO "*Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:*" - może to być kartka widoczna w sytuacji, gdy pacjent znajduje się w rejestracji
- Przykład:
  - Dane są przetwarzane przez: **[PIECZĄTKA PLACÓWKI MEDYCZNEJ]**
  - W placówce medycznej został powołany inspektor ochrony danych **[IMIĘ NAZWISKO INSPEKTORA TEL. XX]**

Rozszerzony obowiązek informacyjny

- Celem przetwarzania danych osobowych jest: prowadzenie dokumentacji medycznej pacjentów i organizacja udzielania świadczeń zdrowotnych. Podstawa prawna to:
  - Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta
  - Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania
  - Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych
  - Rozporządzenie Ministra Zdrowia z dnia 20 czerwca 2008 r. w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców...
  - Zarządzenia Nr 9/2018/DI, 13/2015/DI, 23/2017/DSOZ Prezesa NFZ
  - Rozporządzenie Ministra Zdrowia z dnia 7/7/2017 r. w sprawie minimalnej funkcjonalności dla systemów teleinformatycznych
  - Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia

Rozszerzony obowiązek informacyjny

- Odbiorcami danych osobowych pacjentów – czyli osobami / firmami, którym dane osobowe mogą być ujawniane, są: 1) informatycy i statystycy; 2) podwykonawcy medyczni; 3) księgowość; 4) płatnicy świadczeń udzielanych pacjentowi; 5) dostawcy usług IT
- Dane osobowe są przechowywane przez okres określony w aktualnie obowiązujących przepisach prawa, w szczególności w Ustawie z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta - tj. przez 20 lat z wyjątkami określonymi w Ustawie

Rozszerzony obowiązek informacyjny

- Pacjent ma prawo do żądania od placówki medycznej dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych. Usunięcie może zostać zrealizowane po upływie terminów ustawowych.
- Pacjent posiada prawo wniesienia skargi do organu nadzorczego – Urzędu ochrony danych osobowych
- Podanie danych osobowych jest wymogiem ustawowym. Brak podania danych osobowych może wiązać się z tym, że placówka medyczna nie będzie mogła wywiązać się z obowiązków ustawowych
- Dane nie są wykorzystywane w celu zautomatyzowanego podejmowania decyzji

Dziękuję za uwagę

Pytania?

biuro@zdrowepodlasie.pl