OCHRONA DANYCH OSOBOWYCH

Aktualny stan prawny i kontrole placówek

adwokat Karol Kolankiewicz

Gdańsk, 19 września 2019r.

PODSTAWY PRAWNE

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych […]

USTAWA z dnia 10 maja 2018 r.
o ochronie danych osobowych

USTAWA z dnia 21 lutego 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 [...]

WYPEŁNIENIE OBOWIĄZKU PRAWNEGO

USTAWA z dnia 6 listopada 2008r.
o prawach pacjenta i Rzeczniku Praw Pacjenta

USTAWA z dnia 27 sierpnia 2004r.
o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych

USTAWA z dnia 15 kwietnia 2011 r.
o działalności leczniczej

WYPEŁNIENIE OBOWIĄZKU PRAWNEGO

Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r.
w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania

Rozporządzenie Ministra Zdrowia z dnia 26 czerwca 2019 r.
w sprawie zakresu niezbędnych informacji przetwarzanych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych

DANE O STANIE ZDROWIA

wszelkie informacje, na przykład o chorobie, **niepełnosprawności**, **ryzyku choroby, historii medycznej**, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą **niezależnie od ich źródła**, którym może być na przykład lekarz lub **inny pracownik służby zdrowia**, szpital, **urządzenie medyczne** lub badanie diagnostyczne in vitro

informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej / numer / symbol / oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego jej zidentyfikowania do celów zdrowotnych

informacje o danej osobie fizycznej zebrane podczas świadczenia usług opieki zdrowotnej

DANE W DOKUMENTACJI MEDYCZNEJ

obowiązek prowadzenia dokumentacji medycznej

brak podziału na pacjenta „z NFZ” i pacjenta „komercyjnego”

oznaczenie pacjenta

(art. 25 pkt 1 ustawy o prawach pacjenta)

nazwisko i imię (imiona) / **data urodzenia**
oznaczenie płci / adres miejsca zamieszkania

numer PESEL, jeżeli został nadany, w przypadku noworodka - numer PESEL matki, a w przypadku osób, które nie mają nadanego numeru PESEL - rodzaj i numer dokumentu potwierdzającego tożsamość

gdy pacjent małoletni / całkowicie ubezwłasnowolniony / niezdolny do świadomego wyrażenia zgody - **nazwisko i imię (imiona) przedstawiciela ustawowego oraz adres jego miejsca zamieszkania**

DANE W DOKUMENTACJI MEDYCZNEJ

informacje dotyczące stanu zdrowia
lub udzielonych pacjentowi świadczeń
(art. 25 pkt 1 ustawy o prawach pacjenta)

informacje dotyczące stanu zdrowia i choroby oraz procesu diagnostycznego, leczniczego, pielęgnacyjnego lub rehabilitacji (§ 10 ust 5. rozp. dokum. med.)
w szczególności:

opis udzielonych świadczeń zdrowotnych / rozpoznanie choroby, problemu zdrowotnego, urazu lub rozpoznanie ciąży / zalecenia / informacje o wydanych orzeczeniach, opiniach lekarskich lub zaświadczeniach / informacje o lekach, wraz z dawkowaniem, lub wyrobach medycznych przepisanych pacjentowi na receptach lub zleceniach na zaopatrzenie w wyroby medyczne

DANE W CELACH ROZLICZENIOWYCH

dane charakteryzujące osobę, której udzielono świadczenia

identyfikator osoby (PESEL) oraz kod identyfikatora
identyfikatorem dziecka, któremu nie został nadany numer PESEL, jest identyfikator jednego z rodziców lub identyfikator opiekuna prawnego dziecka

unikalny numer identyfikacyjny karty onkologicznej

imię (imiona) i nazwisko

adres miejsca zamieszkania pacjenta
a jeżeli osoba, której udzielono świadczenia, nie ma miejsca zamieszkania na terytorium RP także adres miejsca pobytu na terytorium RP

numer telefonu kontaktowego lub adres poczty elektronicznej pacjenta - jeżeli został wskazany

data urodzenia pacjenta / płeć pacjenta

DANE W CELACH ROZLICZENIOWYCH

kod tytułu uprawnienia do świadczeń

dane identyfikujące dokument
w przypadku potwierdzenia prawa do świadczeń opieki zdrowotnej kod tytułu uprawnienia dodatkowego

nazwa dokumentu potwierdzającego uprawnienia dodatkowe oraz dane identyfikujące ten dokument

dane przedstawiciela ustawowego albo opiekuna faktycznego imię / imiona i nazwisko / miejsce zamieszkania

ZGODA NA PRZETWARZANIE

konieczność odróżnienia od zgody na leczenie

NUMER TELEFONU / EMAIL
pacjent / osoba upoważniona

osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone **cele przetwarzania ww. danych** osobowych > **organizacja udzielania świadczeń**

w zrozumiałej i łatwo dostępnej formie / jasny i prosty język / może być odwołana w każdym czasie / nie można się zrzec

WYKONANIE UMOWY

gdy przetwarzanie danych jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą > do realizacji praw lub obowiązków wynikających z umowy

także w sytuacji rozwiązywania umowy / zmiany jej treści

gdy niezbędne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy

ŻYWOTNY INTERES

sytuacja, w której zaniechanie przetwarzania danych (np. nieprzekazanie ich innemu podmiotowi) **powodowałoby bezpośrednie zagrożenie dla żywotnych interesów takiej osoby**

+

brak możliwości oparcia przetwarzania na innej przesłance

gdy osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody / konieczność postawienia diagnozy medycznej np. uzyskanie zgody jest niemożliwe gdyż osoba jest nieprzytomna

wygasa z chwilą gdy uzyskanie zgody jest możliwe

OBOWIĄZEK INFORMACYJNY

1. **tożsamość i dane kontaktowe administratora**
2. **dane kontaktowe inspektora ochrony danych**
3. **cele przetwarzania,** do których mają posłużyć dane osobowe **oraz podstawę prawną przetwarzania**
4. **kategorie danych** osobowych
5. **informacje o odbiorcach danych** osobowych lub o kategoriach odbiorców, jeżeli istnieją
6. **informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim**
7. **okres, przez który dane osobowe będą przechowywane**, a gdy nie jest to możliwe, kryteria ustalania tego okresu

OBOWIĄZEK INFORMACYJNY

8. informacje o prawie do żądania od ADO dostępu do danych / *ich sprostowania / usunięcia / ograniczenia przetwarzania / o prawie do wniesienia sprzeciwu wobec przetwarzania / o prawie do przenoszenia danych*

9. informacje o prawie do cofnięcia zgody
w dowolnym momencie

10. informacje o prawie wniesienia skargi do PUODO

11. informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych

12. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu

OBOWIĄZEK INFORMACYJNY

sposoby spełnienia obowiązku

tekst klauzuli informacyjnej na tablicy ogłoszeń / wręczenie kartki / tekst na stronie internetowej / odczytywanie

rozmowa telefoniczna

odczytywanie / odesłanie do pełnego tekstu na stronie i w placówce

korespondencja email

stopka w mailu / odesłanie do pełnego tekstu na stronie / tekst w pdf

PRAWA OSOBY > RODO

Prawo do uzyskania informacji przed wyrażeniem zgody na przetwarzanie

Prawo dostępu do danych

Prawo do sprostowania danych

Prawo do usunięcia danych > „prawo do bycia zapomnianym”

Prawo do ograniczenia przetwarzania / sprzeciw

Prawo do przenoszenia danych

KORZYSTANIE Z PRAW RODO

żądanie przeniesienia danych do innej placówki

obowiązek przechowywania dokumentacji

bezpłatny komplet dokumentacji > prawo dostępu

tylko za pierwszym razem / odpłatne odpisy, kopie

dostęp poprzez email

weryfikacja tożsamości / szyfrowanie / regulacja przetwarzania

dokumentacji papierowej w skan w regulaminie organizacyjnym

WERYFIKACJA TOŻSAMOŚCI

eWUŚ

„świadczeniobiorca **potwierdzi swoją tożsamość poprzez okazanie** dowodu osobistego, paszportu, prawa jazdy albo legitymacji szkolnej; legitymacja szkolna może być okazana jedynie przez osobę, która nie ukończyła 18. roku życia”

inny dokument / oświadczenie

„świadczeniobiorca **po okazaniu dokumentu**, o którym mowa w ust. 2 pkt 1, może przedstawić inny dokument potwierdzający prawo do świadczeń, a jeżeli takiego dokumentu nie posiada, złożyć pisemne oświadczenie o przysługującym mu prawie do świadczeń opieki zdrowotnej”

UDOSTĘPNIANIE DOKUMENTACJI

wyłącznie osobom uprawnionym

na zasadach określonych w ustawie
o prawach pacjenta i Rzeczniku Praw Pacjenta

wydanie dokumentacji medycznej
nie wymaga zwolnienia lekarza (pielęgniarki)
z tajemnicy zawodowej

DOKUMENTACJA RODO

brak obowiązku opracowywania polityki bezpieczeństwa oraz instrukcji systemu informatycznego

administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać

DOKUMENTACJA RODO

rejestr czynności przetwarzania

dokument oceny skutków dla ochrony danych

dokumentacja naruszeń danych

wykaz udostępnień

ewidencja osób upoważnionych do przetwarzania

obowiązek zgłaszania naruszeń do PUODO

obowiązek administratora danych > forma elektroniczna

bez zbędnej zwłoki – w miarę możliwości, **nie później niż w terminie 72 godzin po stwierdzeniu naruszenia**
> do zgłoszenia przekazanego **później dołącza się wyjaśnienie** przyczyn

jeżeli pełnej informacji nie da się udzielić w ww. czasie, można je udzielać sukcesywnie bez zbędnej zwłoki

brak obowiązku zgłoszenia, jeżeli mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych

zawiadomienie osoby o naruszeniu

tylko jeżeli może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych

jasnym i prostym językiem

opis charakteru naruszenia

minimalna zawartość zawiadomienia:

1. **dane kontaktowe IOD**
2. **opis możliwych konsekwencji** naruszenia ochrony danych osobowych
3. **opis środków zastosowanych** / proponowanych przez administratora w celu zaradzenia naruszeniu

Inspektor Ochrony Danych

brak szczególnych wymogów kwalifikacyjnych > wymagana wiedza i praktyka w zakresie zasad przetwarzania danych osobowych + umiejętność wypełnienia zadań

decyzja ADO > obligatoryjnie gdy główna działalność administratora lub podmiotu przetwarzającego **polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych**

brak jednoznacznego określenia „przetwarzanie na dużą skalę”

np. dane 10 000 pacjentów czy też powyżej 50 000 pacjentów

KANDYDAT DO PRACY

Administrator przetwarza następujące dane kandydata:

a. **imię (imiona) i nazwisko**

b. **data urodzenia**

c. **dana kontaktowe wskazane przez taką osobę**

d. **wykształcenie**

e. **kwalifikacje zawodowe**

f. **przebieg dotychczasowego zatrudnienia**

żądanie podania danych z pkt d)-f), gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku

inne niż powyższe dane osobowe
wyłącznie z inicjatywy kandydata do pracy i za jego pisemną zgodą

PRACOWNIK

Administrator przetwarza następujące dane pracownika:

poza danymi uzyskanymi w toku rekrutacji:

a. **adres zamieszkania**

b. **numer PESEL,** a w przypadku jego braku - rodzaj i numer dokumentu potwierdzającego tożsamość

c. **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

d. **wykształcenie i przebieg dotychczasowego zatrudnienia,** jeżeli nie istniała podstawa do ich żądania od kandydata

e. **numer rachunku płatniczego,** jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych

MONITORING WIZYJNY

możliwa rejestracja obrazu > niedopuszczalne rejestrowanie dźwięku

nie może obejmować pomieszczeń nie przeznaczonych do wykonywania pracy
pomieszczenia sanitarne / szatnia / stołówka / palarnia

konieczne zmiany w Regulaminie pracy

informacja dla pracownika przed dopuszczeniem do pracy > piktogramy dla innych osób > informacja o obszarze monitorowanym

WSKAZÓWKI PUODO

Wskazówki Prezesa UODO dotyczące wykorzystywania **monitoringu wizyjnego**
czerwiec 2018

Komunikat Prezesa UODO **w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony**
sierpień 2018 r.

Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców.
październik 2018

WSKAZÓWKI PUODO

Roczny plan kontroli sektorowych na 2019 rok
styczeń 2019 r.

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.

Przychodzi pacjent do lekarza… i na co musi zwrócić uwagę, by chronić swoje dane?
film edukacyjny luty 2019

KONTROLA PUODO

UPRAWNIENIA:

żądanie złożenia pisemnych lub ustnych wyjaśnień

przesłuchiwanie w charakterze świadka osoby
> w zakresie niezbędnym do ustalenia stanu faktycznego
jeżeli świadek nie stawił się / bezzasadnie odmówił złożenia zeznań > kara grzywny

zlecanie sporządzenia ekspertyz i opinii

żądanie wsparcia Policji

KONTROLA PUODO

w obecności administratora / osoby upoważnionej >
jeżeli nie ma przedst. administratora / os. upoważnionej
może być osoba pozostająca w lokalu przedsiębiorcy / przywołany świadek

kontrolowany zapewnia kontrolującemu oraz osobom upoważnionym do udziału w kontroli **warunki i środki** niezbędne do sprawnego przeprowadzenia kontroli

obowiązek sporządzenia we własnym zakresie kopii lub wydruków dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub w systemach

1. niestwierdzenie naruszeń > **brak dalszych czynności**
2. **wszczęcie postępowania przez Prezesa Urzędu**
3. **żądanie wszczęcia postępowania dyscyplinarnego** lub innego przewidzianego prawem postępowania **przeciwko osobom winnym uchybień**
4. **zawiadomienie o popełnieniu przestępstwa**

DECYZJE PUODO

upomnienie w przypadku naruszenia przepisów RODO

ostrzeżenie dot. możliwości naruszenia przepisów przez planowane operacje

nakazanie spełnienia żądania osoby, której dane dotyczą
/ nakazanie sprostowania / usunięcia danych osobowych

nakazanie dostosowania operacji przetwarzania
do przepisów RODO > wskazanie sposobu i terminu

nakazanie zawiadomienia osoby, której dane dotyczą, **o naruszeniu ochrony danych**

wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania,
w tym zakazu przetwarzania

administracyjna kara pieniężna

cofnięcie certyfikacji
/ nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim

kontrole - informacja od PUODO

odpowiedź dla Instytutu – Specjaliści Prawa Ochrony Zdrowia

https://www.ispoz.pl/2019/04/11/najnowsze-statystyki-rodo/

kwiecień 2019 r.

w okresie **od 25 maja 2018r. do dnia 19 marca 2019r**.
z urzędu **3 kontrole** przestrzegania przepisów o ochronie danych osobowych w podmiotach prowadzących działalność leczniczą

wpłynęło **146 zgłoszeń naruszeń** ochrony danych osobowych
od podmiotów wykonujących działalność leczniczą
+ 45 zgłoszeń od innych podmiotów (skargi, wnioski)

nie stwierdzono z urzędu naruszeń ochrony danych osobowych w podmiotach wykonujących działalność lecznic

decyzje PUODO

zgodne z prawem jest udostępnienie danych osobowych rodziców i małoletnich dzieci w zakresie imion, nazwisk, adresu zamieszkania, dat urodzenia, numerów PESEL oraz informacji dotyczących stanu zdrowia dzieci przez Przychodnię na rzecz SANEPID w zakresie dot. obowiązku szczepień obowiązkowych

(ZSZZS.440.50.2019 z dnia 17 czerwca 2019 r.)

dokumentacja medyczna podlega przechowywaniu przez podmiot udzielający świadczeń zdrowotnych przez okres 20 lat od końca roku kalendarzowego, w którym dokonano ostatniego wpisu i przez ten okres żadne dane, nie mogą być z niej usunięte

(ZSZZS.440.659.2018 z dnia 12 kwietnia 2019 r.)

decyzje PUODO

dane osobowe świadczeniobiorcy dotyczące zrealizowanych recept na lekarstwa i zrealizowanych świadczeń medycznych mieszczą się w zakresie danych osobowych przetwarzanych centralnie przez NFZ

(ZSZZS.440.672.2018 z dnia 12 kwietnia 2019 r.)

Przychodnia jest zobowiązana do przygotowania sprawozdania dotyczącego przeprowadzonych szczepień ochronnych i sporządzenia imiennego wykazu osób, które się od szczepień ochronnych uchylają, by umożliwić SANEPID sprawowanie nadzoru nad wypełnianiem tego obowiązku oraz jego efektywną egzekucję. Dane osobowe w postaci numeru telefonu do Skarżącej nie są niezbędne do przekazania w sprawozdaniu

(ZSZZS.440.60.2018 z dnia 27 marca 2019 r.)

ISPOZ

Instytut
Specjaliści Prawa
Ochrony Zdrowia

kontakt:
biuro@ispoz.pl

www.ispoz.pl