PORADNIK PRAWNY
DOTYCZĄCY STOSOWANIA W APTECE PRZEPISÓW RODO

1. Od dnia 25 maja 2018 r. aktualizuje się obowiązek 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), zwanego dalej „Ogólnym rozporządzeniem o ochronie danych" lub „RODO".

2. RODO będzie stosowane bezpośrednio, bez potrzeby implementowani go do polskiego porządku prawnego, co oznacza, że nie muszą być wydawane polskie ustawy lub rozporządzenia wykonawcze.

3. Zgodnie z art. 91 ust. 3 Konstytucji RP, przepisy RODO mają pierwszeństwo stosowania w przypadku kolizji z polskimi ustawami.

4. RODO ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych (vide art. 2 ust. 1 RODO).

5. Omawiając znaczenie RODO dla aptek ogólnodostępnych wyjaśnić należy na wstępie podstawowe pojęcia, które zawarte są w tym akcie normatywnym.

1) „*dane osobowe"* to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. „*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;
2) *„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 (art. 4 pkt 2 RODO);

3) „*administrator*” to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (art. 4 pkt 7 RODO);
4) *"podmiot przetwarzający"* to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
5) *„odbiorca"* to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią;
6) *„dane dotyczące zdrowia"* to dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia.

6. Z przytoczonych norm prawnych wynika, że administratorem w rozumieniu RODO jest **podmiot prowadzący aptekę ogólnodostępną a nie kierownik apteki, farmaceuta, czy też technik farmaceutyczny.**

7. Podmiot prowadzący aptekę, w ramach apteki, musi przetwarzać, co najmniej dane zawarte na receptach i zapotrzebowaniach.

8. RODO przewiduje w art. 5 następujące „Zasady dotyczące przetwarzania danych osobowych”:
1) **zasada zgodności z prawem, rzetelności i przejrzystości** - dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
2) **zasada ograniczenia celu** - dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
3) **zasada minimalizacji danych** - dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
4) **zasada prawidłowości** – dane osobowe musza być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
5) **zasada ograniczenia przechowywania** - dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą,

przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;

6) **zasada integralności i poufności** - 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.

9. Podmiot prowadzący aptekę, jako administrator w rozumieniu RODO, jest odpowiedzialny za przestrzeganie ww. zasad i musi być w stanie wykazać ich przestrzeganie (**zasada rozliczalności**).

10. Odnośnie zasady zgodności z prawem wskazać należy, że przetwarzanie danych jest zgodne z prawem, jeżeli odbywa się na podstawie zgody osoby, której dane dotyczą, lub na innej uzasadnionej podstawie przewidzianej prawem, tj. w RODO albo w innym akcie prawnym UE lub w prawie państwa członkowskiego, o których mowa w RODO.

11. Zgodnie z art. 6 ust. 1 lit. c RODO, przetwarzanie jest zgodne z prawem w przypadku, gdy przetwarzanie jest **niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze**. Jeżeli przetwarzanie odbywa się w celu wypełnienia obowiązku prawnego, któremu podlega administrator podstawę przetwarzania powinno stanowić prawo Unii lub prawo państwa członkowskiego. Wystarczające jest, gdy norma prawna stanowi podstawę różnych operacji przetwarzania wynikających z obowiązku prawnego, któremu podlega administrator. W motywach RODO przyjmuje się, że prawo UE lub prawo państwa członkowskiego powinno określać także cel przetwarzania. Ponadto prawo to może doprecyzowywać ogólne warunki określone w RODO dotyczące zgodności przetwarzania z prawem, określać sposoby wskazywania administratora, rodzaj danych osobowych podlegających przetwarzaniu, osoby, których dane dotyczą, podmioty, którym można ujawniać dane osobowe, ograniczenia celu, okres przechowywania oraz inne środki zapewniające zgodność z prawem i rzetelność przetwarzania.

12. Przetwarzanie danych przez podmiot prowadzący aptekę jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze, tzn. obowiązku realizacji podstawowych zadań apteki, w tym wydawania leków na podstawie recept i zapotrzebowań.

13. Dane osobowe przetwarzane przez apteki obejmują „**dane dotyczące zdrowia”.** Zgodnie z art. 9 ust. 1 RODO - co do zasady – zabrania się przetwarzania danych dotyczących zdrowia. Wyjątki, gdy zakaz ten nie ma zastosowania określa art. 9 ust. 2 RODO. W pierwszej kolejności rozważyć należy w pierwszej kolejności normę z art. 9 ust. 2 lit. h RPDO, zgodnie z którą zakaz przetwarzania „*danych dotyczących zdrowia”* nie ma zastosowania, gdy przetwarzanie 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 na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 9 ust. 3 RODO.

14. RODO wprowadza szereg nowych obowiązków informacyjnych dla administratora, przy czym rozróżnia przypadki, gdy:

1) administrator zbiera dane od osoby, której dane dotyczą;
2) administrator pozyskuje dane osobowe w sposób inny niż od osoby, której dane dotyczą.

Podmiot prowadzący aptekę, jako administrator w rozumieniu RODO, ma obowiązek podjąć odpowiednie środki, aby **w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich ww. informacji.** Ponadto, zobowiązany jest w tej samej formie i tym samym językiem prowadzić wszelką komunikację z osobą, której dane dotyczą, w zakresie: prawa do uzyskania dostępu do danych (art. 15), prawa do sprostowania danych (art. 16), prawa do usunięcia danych - prawa do bycia zapomnianym (art. 17), prawa do ograniczenia przetwarzania (art. 18) zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych (art. 34).

W załączeniu wzory dokumentów, które należy wypełnić i powiesić w miejscu widocznym dla pacjentów w aptece wraz z objaśnieniem:

1. **INFORMACJA SKIEROWANA DO OSÓB, KTÓRYCH DANE OSOBOWE SĄ PRZETWARZANE W ZWIĄZKU Z KORZYSTANIEM Z USŁUG APTEKI OGÓLNODSTĘPNEJ, I SĄ ZBIERANE OD TEJ OSOBY.**
2. **INFORMACJA SKIEROWANA DO OSÓB, KTÓRYCH DANE OSOBOWE SĄ PRZETWARZANE W ZWIĄZKU Z KORZYSTANIEM Z USŁUG APTEKI OGÓLNODSTĘPNEJ, A SĄ ZBIERANE OD INNEJ OSOBY.**

3. INFORMACJA SKIEROWANA DO WSZYSTKICH OSÓB KORZYSTAJĄCYCH Z USŁUG APTEKI OGÓLNODSTĘPNEJ.

4. OBJAŚNIENIE.

15. Podmiot prowadzący aptekę, jako administrator w rozumieniu RODO, zobowiązany jest wdrożyć **odpowiednie środki techniczne i organizacyjne,** aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać. Przy ustalaniu odpowiednich środków należy uwzględnić: charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

16. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, ww. środki mogą obejmować **wdrożenie przez administratora odpowiednich polityk ochrony danych**.

WZÓR POLITYKI OCHRONY DANYCH OSOBOWYCH W APTECE JEST PRZYGOTOWYWANY W BIURZE PRAWNYM NIA I ZOSTANIE UDOSTĘPNIONY W NAJBLIŻSZYM CZASIE.

17. Istotne znaczenie ma norma zawarta w art. 29 RODO, zgodnie z którą podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych **przetwarzają je wyłącznie na polecenie administratora,** chyba że wymaga tego prawo UE lub prawo państwa członkowskiego. W myśl art. 32 ust. 4 RODO, administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, **przetwarzała je wyłącznie na polecenie administratora**, chyba że wymaga tego od niej prawo unii lub prawo państwa członkowskiego. Osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego to osoby, które działają w ramach danego podmiotu, tzn. pracownicy i inne osoby przetwarzające dane.

W załączeniu wzory dokumentów, które należy wypełnić i przekazać pracownikom oraz osobom wykonującym czynności na podstawie stosowane upoważnienia.

1. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

2. UPOWAŻNIENIE PRACOWNIKA DO PRZETWARZANIA DANYCH OSOBOWYCH.

18. **Administrator może powierzyć przetwarzanie danych innemu podmiotowi**. Zgodnie z art. 4 pkt 8 RODO, „podmiot przetwarzający" to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, może on korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora.
19. Przetwarzanie danych osobowych przez podmiot przetwarzający **odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu UE** 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 musi zawierać szereg postanowień szczegółowo określonych w art. 28 ust. 3 RODO.**
    W załączeniu wzór umowy o POWIERZENIU PRZETWARZANIA DANYCH OSOBOWYCH.
20. Kolejny obowiązek nałożony przez RODO na administratora polega na rejestrowaniu czynności przetwarzania. Każdy administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada. W rejestrze tym zamieszcza się szczegółowo określone elementy. **Rejestr mają formę pisemną lub formę elektroniczną.** Administrator udostępnia rejestr na żądanie organu nadzorczego. Obowiązek prowadzenia rejestru nie ma zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10. **Apteki są objęte obowiązkiem**

prowadzenia ww. rejestru, ponieważ przetwarzają szczególną kategorię danych osobowych, o której mowa w art. 9 ust. 1 RODO, tj. dane dotyczące zdrowia.
W załączeniu wzór REJESTRU CZYNNOŚCI PRZETWARZANIA.

21. Duże kontrowersje budzi stosowanie do aptek ogólnodostępnych przepisu art. 35 RODO. Norma ta stanowi, że jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania **dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych**.
W załączeniu pismo GIODO.

22. W art. 37 RODO ustanowiono obowiązek wyznaczenia inspektora ochrony danych. Przepis ten stanowi, że administrator i podmiot przetwarzający wyznaczają **inspektora ochrony danych**, zawsze gdy:

a) przetwarzania dokonują organ lub **podmiot publiczny**, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

b) 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

c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO.

Podmiot prowadzący aptekę będzie miał obowiązek wyznaczenia inspektora ochrony danych, gdy ustalone zostanie, że **główna działalność podmiotu prowadzącego aptekę polega na przetwarzaniu na dużą skalę danych dotyczących zdrowia. Zgodnie z motywem 97. RODO,** jeżeli główna działalność administratora polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, to w monitorowaniu wewnętrznego przestrzegania RODO administrator powinien być

wspomagany przez osobę dysponującą wiedzą fachową na temat prawa i praktyk w dziedzinie ochrony danych.

W załączeniu pismo NIA do GIODO

23. **W Rozdziale VIII RODO określono środki ochrony prawnej, odpowiedzialność i sankcje**. Zgodnie z art. 82 ust. 1 RODO, każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora **odszkodowanie za poniesioną szkodę**. Administrator zostanie zwolniony z odpowiedzialności, jeżeli udowodni, że w żaden sposób nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody. Postępowanie sądowe dotyczące odszkodowania jest wszczynane przed sądem właściwym na mocy prawa polskiego.

Ogólne warunki nakładania administracyjnych kar pieniężnych zostały określone w art. 83 RODO. Podstawowa zasada, która ma kierować się organ nadzorczy to obowiązek zapewnienia, aby stosowane administracyjne **kary pieniężne,** w każdym indywidualnym przypadku były:

1) skuteczne;
2) proporcjonalne;
3) odstraszające.