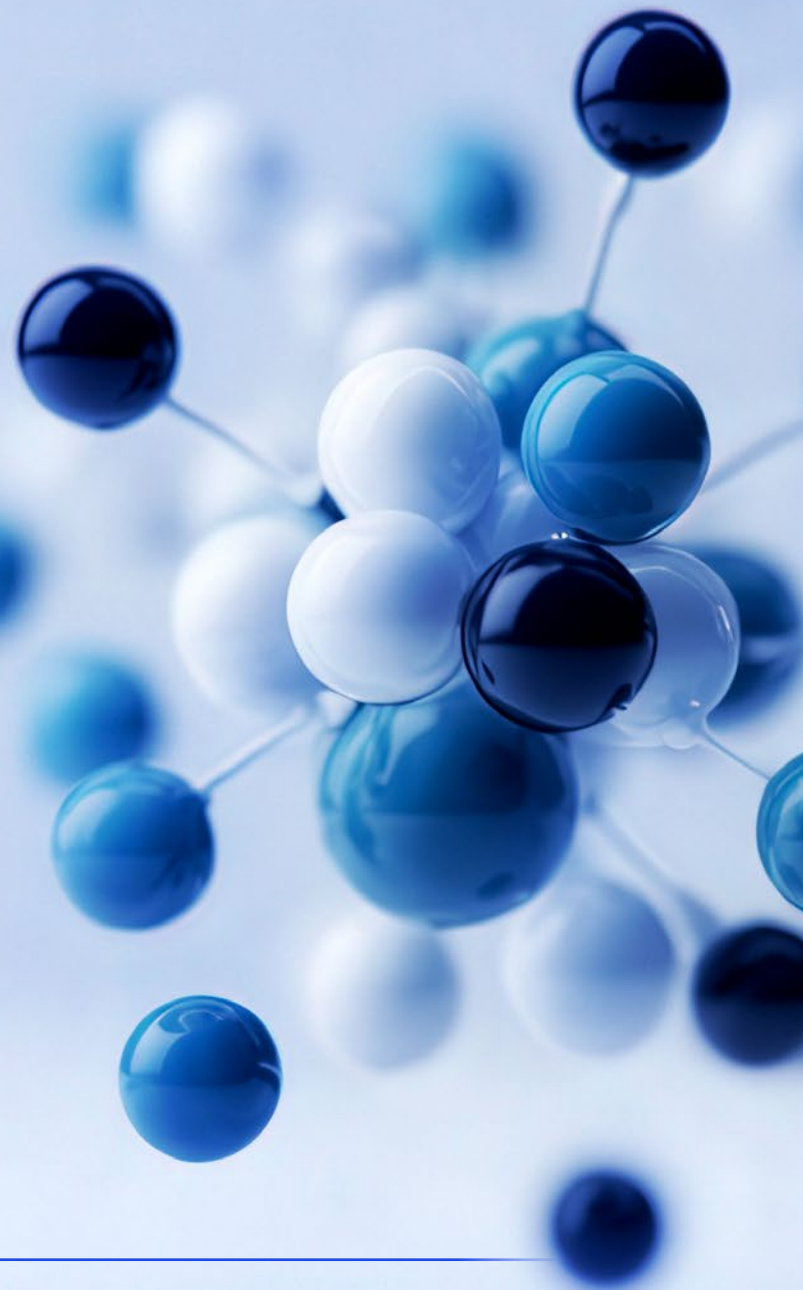


Kodeks postępowania dla sektora ochrony zdrowia

– podmioty publiczne

Zarządzanie zgodnością z RODO w oparciu o sprawdzony standard sektorowy. Kodeks postępowania dla sektora ochrony zdrowia to zatwierdzone przez Prezesa UODO narzędzie, które wspiera podmioty medyczne i ich partnerów w spełnianiu wymogów RODO, ograniczaniu ryzyka regulacyjnego oraz optymalizacji kosztów.



Podmiot monitorujący – KPMG

Niezależna, akredytowana jednostka zapewniająca weryfikację zgodności podmiotu publicznego przed przystąpieniem do stosowania Kodeksu oraz wiarygodne potwierdzenie zgodności wobec organu nadzorczego.



Dla kogo jest Kodeks?

Administratorzy

Do stosowania kodeksu mogą przystąpić wszystkie Podmioty Wykonujące Działalność Leczniczą (PWDL), między innymi:

- szpitale, kliniki, przychodnie,
- niezależnie od formy prawnej

Podmioty przetwarzające

Które na zlecenie PWDL przetwarzają dane osobowe. Mogą to być między innymi:

- dostawcy systemów i usług informatycznych,
- dostawcy sprzętu diagnostycznego.

Kodeks jest dostępny zarówno dla podmiotów publicznych, jak i prywatnych.

Kodeks to praktyczne narzędzie compliance, które łączy zgodność regulacyjną z optymalizacją kosztów i zarządzaniem ryzykiem



Jasne wytyczne stosowania przepisów

- Dopasowane do specyfiki sektora ochrony zdrowia
- Uwzględniają stanowiska EROD i praktykę organów
- Gotowe podejścia i rozwiązania wdrożeniowe



Pozytywny wizerunek i zaufanie pacjentów

- Potwierdzenie wysokich standardów ochrony danych
- Transparentność wobec pacjentów i partnerów
- Wzmocnienie reputacji organizacji



Niezależny audyt

- Weryfikacja przez akredytowany podmiot monitorujący
- Kompleksowa ocena zgodności z RODO
- Możliwość ograniczenia kosztów dodatkowych audytów



Realizacja zasady rozliczalności

- Udokumentowana zgodność z wymogami RODO
- Wsparcie w wykazaniu zgodności (accountability)
- Spójne podejście do zarządzania ochroną danych



Minimalizacja ryzyka prawnego

- Dowód dochowania należytej staranności
- Argument w relacji z organem nadzorczym
- Realne ograniczenie skutków naruszeń



Korzyści dla podmiotów przetwarzających

- Możliwość wykazania odpowiednich środków technicznych i organizacyjnych
- Wzmocnienie pozycji wobec administratorów
- Ustandaryzowane podejście do wymagań RODO

Realne przełożenie na ryzyko regulacyjne – obniżenie kary o 60%

Decyzja Prezesa UODO

Prezes Urzędu Ochrony Danych Osobowych wydał decyzję wobec niepublicznego zakładu opieki zdrowotnej i nałożył karę pieniężną na podmiot, obniżając ją o 60% w wyniku uwzględnienia jako okoliczność łagodzącą przystąpienia do stosowania Kodeksu przez ten podmiot po wystąpieniu naruszenia i wszczęciu postępowania przez organ.



Stosowanie Kodeksu może istotnie ograniczyć ryzyko finansowe w przypadku naruszenia.

Jak przystąpić do kodeksu?

KPMG przeprowadza audyt wstępny zarówno dla podmiotów prywatnych, jak i publicznych. Dalsze monitorowanie zgodności przebiega odmiennie – w sektorze prywatnym jest realizowane przez KPMG, natomiast w sektorze publicznym odbywa się poprzez mechanizmy audytu i kontroli funkcjonujące w danej jednostce.

Wniosek

01

- Są dwa rodzaje wniosków: dla podmiotów prywatnych i dla podmiotów publicznych.
- Stanowią one załączniki do Kodeksu.
- Zawierają podstawowe informacje dotyczące kandydata.

Kwestionariusz

02

- Załączany do wniosku.
- Opisuje podstawowe obszary przetwarzania danych osobowych.

Audyt wstępny

03

- Przeprowadzany po złożeniu wniosku.
- Realizowany zgodnie z metodyką audytową.
- Może być prowadzony zdalnie lub na miejscu.

Monitorowanie

04

- Stosowanie Kodeksu podlega monitorowaniu.
- W podmiotach prywatnych funkcję podmiotu monitorującego pełni KPMG.
- Może przybrać formę ankiety, audytu planowego lub doraźnego.

Model monitorowania Kodeksu w podmiotach publicznych

Jak odbywa się monitorowanie?

Kto monitoruje?

Jednostka audytująca, która prowadzi monitorowanie:

- poprzez audyt wewnętrzny w ramach kontroli zarządczej, albo
- poprzez kontrolę i ocenę działalności prowadzoną przez podmiot tworzący lub organ rejestrowy.

Planowanie

01

- monitorowanie jest uwzględniane w rocznych planach audytu lub okresowych planach kontroli,
- jednostka audytująca sama określa terminy i sposób monitorowania.

Czynności sprawdzające

02

- wykonywane cyklicznie, nie rzadziej niż raz w roku,
- dodatkowo po uzyskaniu informacji o możliwym naruszeniu Kodeksu.

Formy monitorowania

03

- ankieta monitoringowa,
- wywiady telefoniczne,
- wizyta na miejscu.

Minimalna częstotliwość

04

- ankieta monitoringowa – co najmniej raz w roku,
- wywiad lub wizyta na miejscu – co najmniej raz na 5 lat (obejmujące pełny zakres wymagań kodeksu).

Aktualne komunikaty na stronie internetowej



Warunki uzyskania statusu członka kodeksu

Warunkiem przyjęcia jest uzyskanie pozytywnego wyniku audytu wstępnego przeprowadzonego przez podmiot monitorujący.

Dokumenty do pobrania

Formularze wniosków, kwestionariusz, wzór skargi oraz procedura rozpatrywania skarg i odwołań znajdują się na stronie internetowej.

Co jest sprawdzane?

W szczególności:

- zmiany w systemie ochrony danych,
- polityki i procedury,
- zmiany organizacyjne,
- istotne zmiany systemów IT,
- naruszenia ochrony danych,
- nowe przepisy i wytyczne EROD/UODO.

Reakcja na niezgodności

Jednostka audytująca:

- identyfikuje naruszenia,
- wyznacza działania naprawcze,
- może wystąpić o zawieszenie lub pozbawienie statusu podmiotu przestrzegającego Kodeksu,
- raportuje wyniki do Komitetu Sterującego.

Kontakt

KPMG w Polsce
ul. Inflancka 4A
00-189 Warszawa
T: +48 22 528 11 00
E: kpmg@kpmg.pl

Michał Kurek

Partner, Szef Zespołu
Cyberbezpieczeństwa w KPMG w Polsce
i Europie Środkowo-Wschodniej
Advisory
M: +48 660 440 041
E: michalkurek@kpmg.pl



KPMG Poland

kpmg.pl

© 2026 KPMG Advisory Spółka z ograniczoną odpowiedzialnością sp.k., polska spółka komandytowa i członek globalnej organizacji KPMG składającej się z niezależnych spółek członkowskich stowarzyszonych z KPMG International Limited, prywatną spółką angielską z odpowiedzialnością ograniczoną do wysokości gwarancji. Wszelkie prawa zastrzeżone.

Nazwa i logo KPMG są znakami towarowymi używanymi na podstawie licencji przez niezależne firmy członkowskie globalnej organizacji KPMG.

Informacje zawarte w niniejszej publikacji mają charakter ogólny i nie odnoszą się do sytuacji konkretnej osoby lub firmy. Pomimo, iż staramy się dostarczać dokładne i aktualne informacje, nie możemy zagwarantować, że takie informacje będą aktualne na dzień ich otrzymania lub że będą nadal aktualne w przyszłości. Nikt nie powinien podejmować decyzji na podstawie takich informacji bez odpowiedniego profesjonalnego doradztwa po dokładnym zbadaniu konkretnej sytuacji.

Document Classification: KPMG Public