Kodeks postępowania dla sektora ochrony zdrowia

uzyskanie członkostwa, dalsze monitorowanie

KPMG Advisory Sp. z o.o. sp. k.

Podmiot Monitorujący

–

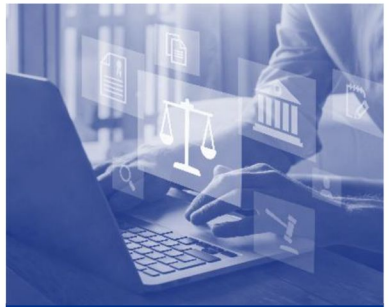
Warszawa, 11 grudnia 2023 r.

Wymagania akredytacyjne – jak je spełniamy

KPMG jako Podmiot Monitorujący

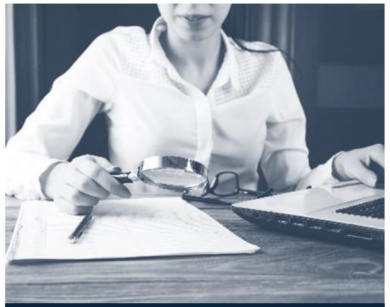
01

Elastyczne dysponowanie personelem oraz środkami organizacyjnymi i technicznymi, dostosowane do skali zainteresowania stosowaniem Kodeksu przez Podmioty Wykonujące Działalność Leczniczą



02

Funkcjonujące zasady zachowania niezależności i unikania konfliktu interesów



03

Procedury oceny kwalifikującej do przystąpienia do stosowania Kodeksu, monitorowania zgodności z Kodeksem, rozpatrywania skarg na naruszenia Kodeksu

04

Wiedza fachowa potwierdzona certyfikatami:

- CIPP/E - Certified Information Privacy Professional/Europe

- CIA - Certified Internal Auditor

- ACO - Approved Compliance Officer

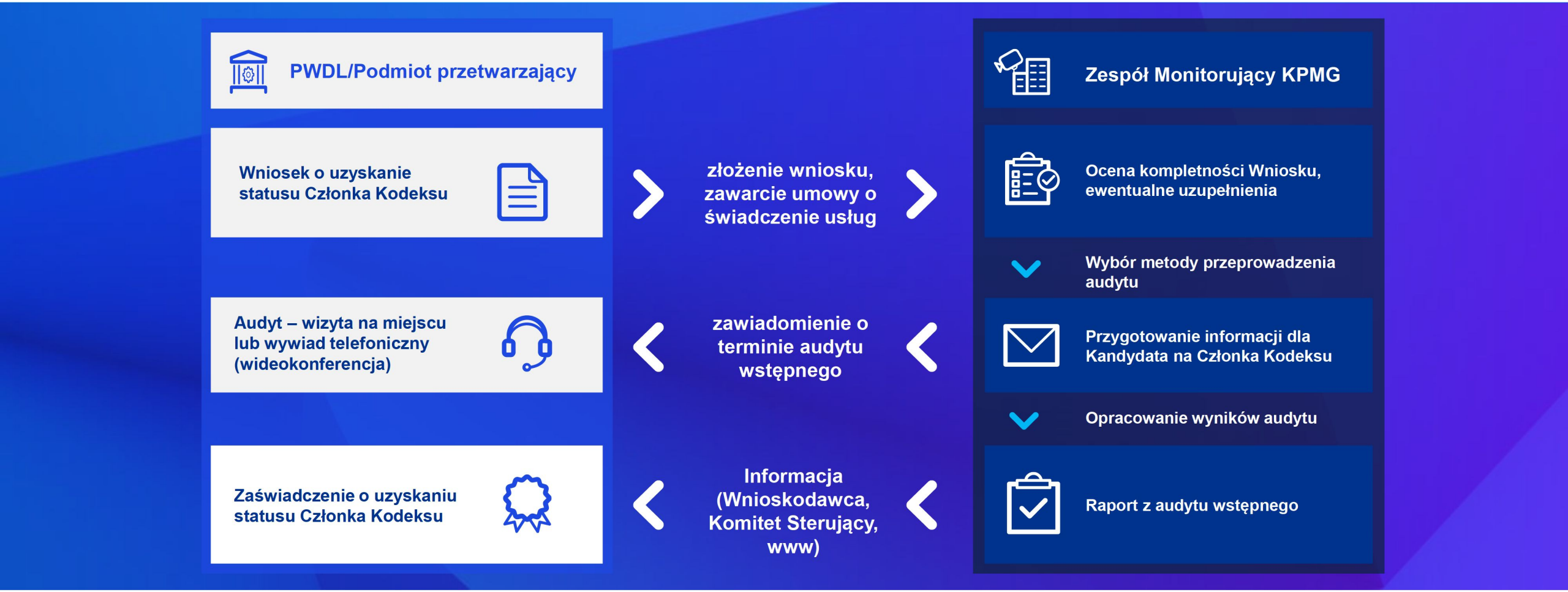
05

Przygotowanie technologiczne – dedykowane skrzynki e-mail, linia telefoniczna, strona www

Realizacja zadań Podmiotu Monitorującego

Jak przystąpić do stosowania kodeksu

Obsługa wniosku i audyt wstępny



Wniosek

Załącznik nr 8

Wzór wniosku o uzyskanie statusu podmiotu przestrzegającego Kodeksu przez Organy i podmioty publiczne

Dane PWDL/ Podmiotu przetwarzającego (dalej: „Podmiot"):

Firma, nazwa albo imię i nazwisko podmiotu leczniczego/ Podmiotu przetwarzającego:

Adres siedziby podmiotu leczniczego/ Podmiotu przetwarzającego, a w przypadku osoby fizycznej – adres do korespondencji:

Numer księgi rejestrowej (rejestr PWDL), jeśli dotyczy:

Numer Krajowego Rejestru Sądowego, jeśli dotyczy:

Numer telefonu kontaktowego:

Adres e-mail:

Adres strony internetowej:

Data złożenia oświadczenia:

Działając na podstawie pkt. 7.3.1. Kodeksu postępowania dla sektora ochrony zdrowia wydanego zgodnie z art. 40 RODO dotyczącego PWDL oraz Podmiotów przetwarzających i zatwierdzonego przez Prezesa Urzędu Ochrony Danych Osobowych w dniu ___ niniejszym w imieniu Podmiotu oświadczam, iż w odniesieniu do:

☐ Całości działalności prowadzonej w charakterze Podmiotu przetwarzającego objętej zakresem Kodeksu

☐ Całości prowadzonej działalności leczniczej objętej zakresem Kodeksu. Działalność prowadzona jest w ramach następujących zakładów leczniczych i jednostek organizacyjnych zakładów leczniczych:

Nazwa zakładu leczniczego	Nazwa jednostki organizacyjnej zakładu leczniczego	Adres	Osoba kontaktowa	Adres e-mail	Nr telefonu	Liczba osób wykonujących zawody medyczne w jednostce organizacyjnej

Załącznik nr 9

Wzór wniosku o uzyskanie statusu podmiotu przestrzegającego Kodeksu przez PWDL oraz Podmioty przetwarzające inne niż Organy i podmioty publiczne

Dane PWDL/ Podmiotu przetwarzającego (dalej: „Wnioskodawca")

Firma, nazwa albo imię i nazwisko podmiotu leczniczego/ Podmiotu przetwarzającego:

Adres siedziby podmiotu leczniczego/ Podmiotu przetwarzającego, a w przypadku osoby fizycznej – adres do korespondencji:

Numer księgi rejestrowej (rejestr PWDL), jeśli dotyczy:

Numer Krajowego Rejestru Sądowego, jeśli dotyczy:

Numer telefonu kontaktowego:

Adres e-mail:

Adres strony internetowej:

Nazwa Podmiotu monitorującego, do którego składany jest wniosek:

Data złożenia wniosku:

Działając na podstawie pkt 7.3.1. Kodeksu postępowania dla sektora ochrony zdrowia wydanego zgodnie z art. 40 RODO dotyczącego PWDL i Podmiotów przetwarzających i zatwierdzonego przez Prezesa Urzędu Ochrony Danych Osobowych w dniu ___ niniejszym w imieniu Wnioskodawcy w odniesieniu do:

☐ Całości działalności prowadzonej w charakterze Podmiotu przetwarzającego objętej zakresem Kodeksu.

Załącznik nr 10

Wzór kwestionariusza, który dołącza się do wniosku, o którym mowa w załączniku nr 8 lub załączniku nr 9

Wymóg wynikający z Kodeksu:	Kogo dotyczy (PWDL/ Podmiot przetwarzający/ oba)	Wyjaśnienia do wymogu	Wskazanie w jaki sposób wymóg został spełniony (wypełnia Podmiot składający oświadczenie lub wniosek)[56]
Prawidłowe określenie celów i podstaw prawnych przetwarzania.	PWDL	Należy ocenić m.in. treści obowiązków informacyjnych, rejestrów czynności przetwarzania, sprawdzić zasadność pobierania zgody	
Prawidłowy zakres przetwarzania danych, dla którego podstawą nie jest zgoda.	PWDL	Należy w szczególności zweryfikować, czy zakres przetwarzanych danych jest adekwatny, stosowny i ograniczony dla celów przetwarzania	
Prawidłowy zakres przetwarzania danych, dla którego podstawą jest zgoda.	PWDL	Należy w szczególności zwrócić uwagę na zasadność wykorzystania zgody jako podstawy prawnej przetwarzania danych w danym procesie, należy ocenić prawidłowość zbieranych zgód w stosunku do procesu przetwarzania, a także procedurę i okoliczności jej gromadzenia (zapewnienie swobody, niewykorzystywanie stosunku zależności) oraz wycofywania (zwłaszcza łatwość wycofania), sposób realizacji zasady rozliczalności w odniesieniu do zgody	
Prawidłowa identyfikacja podmiotów jako Podmioty przetwarzające/ Administratorzy/ osoby przetwarzające dane z upoważnienia.	Oba*	Należy w szczególności zwrócić uwagę czy podmiot odpowiednio identyfikuje w zawartych przez siebie umowach role i obowiązki związane z przetwarzaniem danych, w tym czy zawiera umowy powierzenia przetwarzania danych z właściwymi podmiotami.	

[56] Należy w sposób syntetyczny wskazać sposób wypełnienia obowiązku, jeśli jest to celowe i zasadne należy również odnieść się do dokumentacji wdrożonej przez podmiot, takiej jak posiadane procedury czy wzory.

Kwestionariusz

Należy w sposób syntetyczny wskazać sposób wypełnienia danego wymagania kodeksu, a jeśli jest to celowe i zasadne należy również odnieść się do dokumentacji wdrożonej przez podmiot, takiej jak posiadane procedury czy wzory.

Cele i podstawy przetwarzania

oraz zakres przetwarzania danych w zależności od podstawy.

Udostępnianie dokumentacji medycznej

w szczególności sposób udostępniania dokumentacji medycznej, treść upoważnienia do dostępu do dokumentacji

Prawidłowe określenie ról

procesor/ administrator/ osoby przetwarzające dane z upoważnienia

Zapewnienie odpowiedniego poziomu wiedzy dotyczącej bezpieczeństwa danych osobowych

udokumentowane i cykliczne działania w obszarze zwiększenia wiedzy w zakresie bezpieczeństwa danych osobowych

Zasady dostępu personelu do danych osobowych Pacjentów

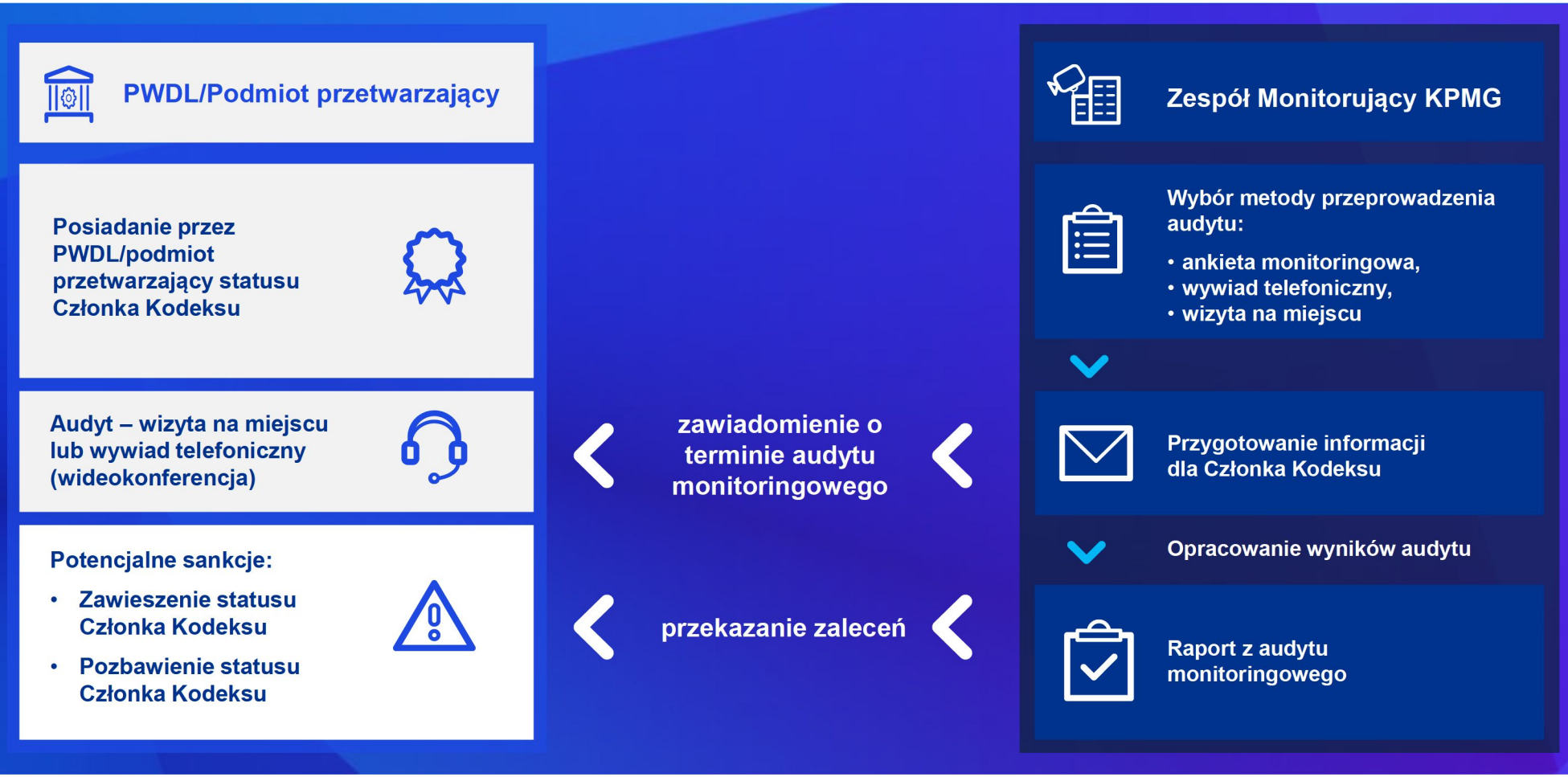
celowość i niezbędność dostępu danych osobowych pacjentów ze względu na zadania personelu.

Zapewnienie właściwej realizacji praw Pacjentów jako podmiotów danych

sposób ustalenia tożsamości Pacjenta, forma przekazywania informacji Pacjentowi, sposób realizacji poszczególnych praw i obowiązków

Dalsze monitorowanie w podmiotach prywatnych

Audyty monitoringowe - planowe i doraźne



Dalsze monitorowanie w podmiotach publicznych

Dalsze monitorowanie jest prowadzone przez **Jednostkę audytującą** w ramach mechanizmów monitorowania i oceny kontroli zarządczej - w szczególności poprzez audyt wewnętrzny albo w ramach nadzoru sprawowanego przez podmiot tworzący lub organ rejestrowy - w szczególności poprzez kontrolę i ocenę działalności podmiotu.

Jednostka audytująca będąca audytorem wewnętrznym lub usługodawcą prowadzącym audyt wewnętrzny, realizuje dalsze monitorowanie w formie zadań zapewniających, na podstawie przepisów ustawy o finansach publicznych oraz przepisów wykonawczych.

Jednostka audytująca będąca podmiotem tworzącym Podmiot przestrzegający Kodeksu realizuje dalsze monitorowanie w formie kontroli i oceny działalności tego podmiotu, na podstawie przepisów ustawy o działalności leczniczej.

Procedury monitorowania

Jednostka audytująca jest zobowiązana do przyjęcia procedury określającej szczegółowe zasady prowadzenia monitorowania przestrzegania przepisów Kodeksu

Niezależność i obiektywizm

Jednostka audytująca jest zobowiązana zapewnić niezależność i obiektywizm w realizacji dalszego monitorowania, wiedzę fachową w dziedzinie będącej przedmiotem kodeksu oraz procedury gwarantujące unikanie konfliktu interesów.

Obsługa skarg

Jednostka audytująca określa szczegółową procedurę zbierania i rozpatrywania skarg i wniosków, przy czym procedura ta powinna uwzględniać funkcjonujące w PWDL zasady przyjmowania skarg

Uwzględnienie monitorowania w planowaniu

Jednostka audytująca określa terminy i sposoby dalszego monitorowania przestrzegania przepisów Kodeksu w corocznych planach audytu lub okresowych planach kontroli

Wsparcie Komitetu sterującego

Komitet sterujący wyda wzory procedur dotyczących unikania konfliktu interesów, zbierania i rozpatrywania skarg oraz szczegółowe rekomendacje i wytyczne w zakresie monitorowania stosowania Kodeksu, w tym wzór skargi oraz wzory list kontrolnych audytów monitoringowych.

,

Dobór metody przeprowadzania audytów

Audyt wstępny

- Metoda dobierana jest odrębnie dla każdej jednostki organizacyjnej zakładu leczniczego
- Uwzględnia wielkość jednostki organizacyjnej zakładu leczniczego, określoną poprzez liczbę osób wykonujących zawody medyczne, udzielających świadczeń zdrowotnych w danej jednostce organizacyjnej,
- Racjonalizacja kosztów,
- Uzależniona od tego, czy Kandydat jest podmiotem publicznym

Audyt monitoringowy - planowy

- Podmioty do przeprowadzenia audytu monitoringowego w formie wizyty na miejscu, wybierane są na podstawie:
  - oceny punktowej Wniosku, prowadzonej na etapie jego obsługi,
  - wyników ankiety monitoringowej i uzyskanych informacji o podmiocie, w tym m.in. dotyczących skali przetwarzania szczególnych danych osobowych, czynników ryzyka zidentyfikowanych na etapie audytu wstępnego, liczby lokalizacji oraz racjonalizacji kosztów badania.
- Do przeprowadzenia planowego audytu monitoringowego w formie wywiadu telefonicznego lub wizyty na miejscu nie są wybierane podmioty, w których w takiej formie (odpowiednio) został przeprowadzony audyt wstępny.

Audyt monitoringowy - doraźny

- Audyt monitoringowy doraźny jest realizowany w szczególności:
  - w procesie rozpatrywania skargi na Członka Kodeksu,
  - w wyniku pozyskania informacji o uzasadnionym podejrzeniu naruszenia przepisów Kodeksu,
  - w przypadku nieprzekazania przez Członka Kodeksu ankiety monitoringowej.
- Przeprowadzany jest w formie wizyty na miejscu lub wywiadu telefonicznego.

Pozostałe zadania podmiotu monitorującego

01

Rozpatrywanie wniosków i skarg, przyjmowanych poprzez: dedykowaną skrzynkę poczty elektronicznej, dedykowany numer telefoniczny, pisemnie na adres KPMG lub ustnie, po uprzednim umówieniu wizyty

02

Informowanie o uzyskaniu lub utracie statusu Członka Kodeksu, podawanie do wiadomości treści wniosku o uzyskanie statusu Członka Kodeksu oraz informacji o możliwości złożenia i zasadach rozpatrywania wniosku lub skargi na naruszenie Kodeksu

03

Współpraca z UODO i Komitetem Sterującym - przekazywanie niezbędnych informacji, udzielanie odpowiedzi na pytania i udzielanie wyjaśnień w zakresie monitorowania stosowania Kodeksu

04

Wsparcie Komitetu Sterującego w prowadzeniu okresowych przeglądów Kodeksu, przekazywanie danych dotyczących stosowania Kodeksu cyklicznie i na żądanie

05

Współpraca z Komitetem Sterującym na rzecz promowania stosowania Kodeksu oraz podejmowania innych działań zwiększających poziom ochrony danych osobowych w sektorze medycznym

Strona internetowa Podmiotu Monitorującego

Uruchomiliśmy dedykowaną podstronę, aby zapewnić niezbędne informacje wszystkim podmiotom zainteresowanym przystąpieniem do stosowania Kodeksu.

Aktualne komunikaty

Wskazanie aktualnych informacji dotyczących monitorowania stosowania Kodeksu.

Informacje dotyczące bezstronności KPMG

Opis spełniania przez KPMG procedur gwarantujących wykonywanie zadań i obowiązków podmiotu monitorującego w sposób niepowodujący konfliktu interesów.

Wykaz Członków Kodeksu

Aktualna lista Członków Kodeksu wraz z datami uzyskania statusu.

Dokumenty do pobrania

Dokumenty dotyczące akredytacji KPMG, jako podmiotu monitorującego, formularz wniosku o uzyskanie statusu Członka Kodeksu oraz informacja o możliwości wniesienia skargi.

Punkt kontaktowy

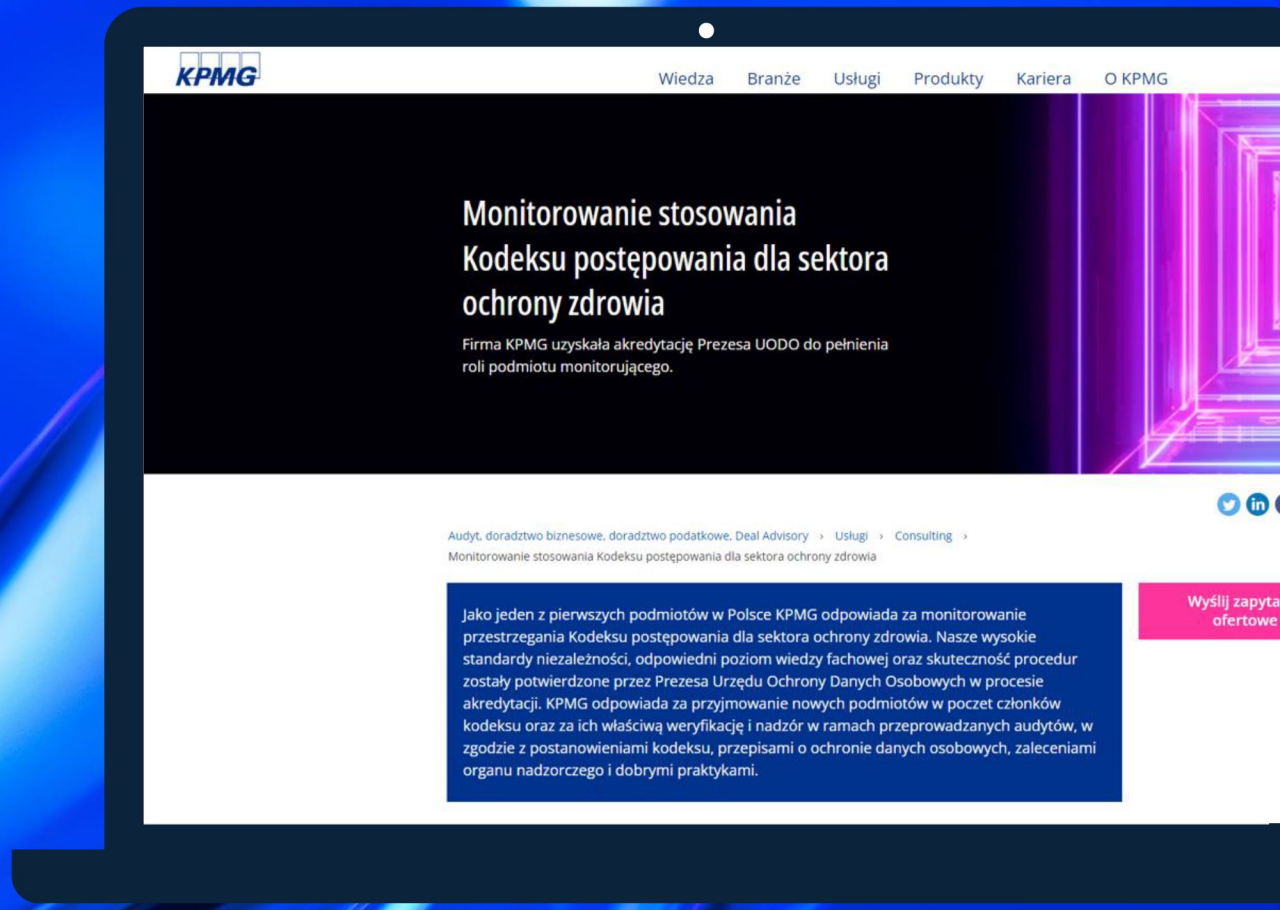
Uruchomiony zostanie Punkt kontaktowy, w którym będzie można uzyskać informacje dotyczące monitorowania stosowania Kodeksu poprzez: dedykowany adres e-mail lub numer telefonu.

Dane kontaktowe

www.kpmg.pl

e-mail:
kodeksRODO_PWDL@kpmg.pl

infolinia:
+48 600 960 201



Kontakt

Michał Kurek
Partner, KPMG Advisory
Cyber Security Consulting

T: + 48 22 528 13 69
M: + 48 660 440 041
E: michalkurek@kpmg.pl

Piotr Burzyk
Starszy Menadżer, KPMG Advisory
Cyber Security Consulting
Data Privacy Team

T: + 48 22 528 18 49
M: + 48 784 079 721
E: pburzyk@kpmg.pl

KPMG Poland