WEBINARIA GRC

Granice audytu procesora

czyli jak daleko sięga nadzór i kontrola administratora

Aleksandra Jarkiewicz,
Beata Kąkol-Dembowska

GRC LEGAL

Agenda spotkania

- **Podstawy prawne**
- **Weryfikacja procesora przed zawarciem umowy** – na co zwracać uwagę?
- **Weryfikacja procesora w trakcie trwania umowy** – jak skutecznie zrealizować prawo audytu?
- **Odpowiedzialność administratora i procesora** za naruszenia ochrony danych osobowych

GRC LEGAL

Podstawy prawne

GRC LEGAL

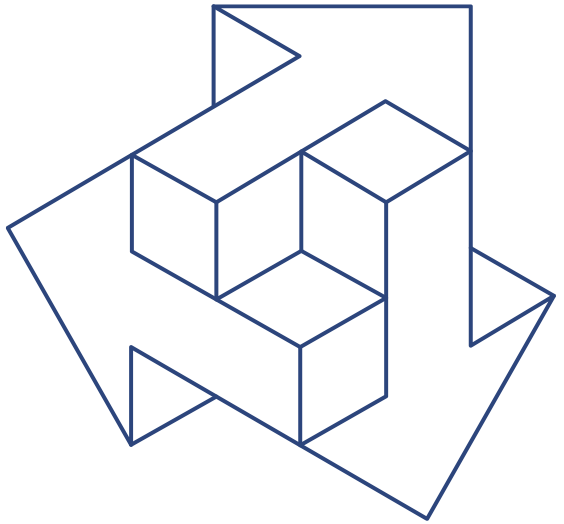
Zasady i obowiązki wynikające z RODO

MOTYW 81 PREAMBUŁY

[należy] korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają **wystarczające gwarancje** – w szczególności jeżeli chodzi o **wiedzę fachową, wiarygodność i zasoby** – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania.

ART. 28 UST. 1

w zw. z motywem 81: **obowiązek uprzedniego zbadania procesora**, tj przed zawarciem umowy powierzenia



Stosowanie Kodeksów i Certyfikatów

MOTYW 81 PREAMBUŁY

Stosowanie przez podmiot przetwarzający **zatwierdzonego kodeksu postępowania** lub **zatwierdzonego mechanizmu certyfikacji** może posłużyć za element wykazujący wywiązywanie się z obowiązków administratora.

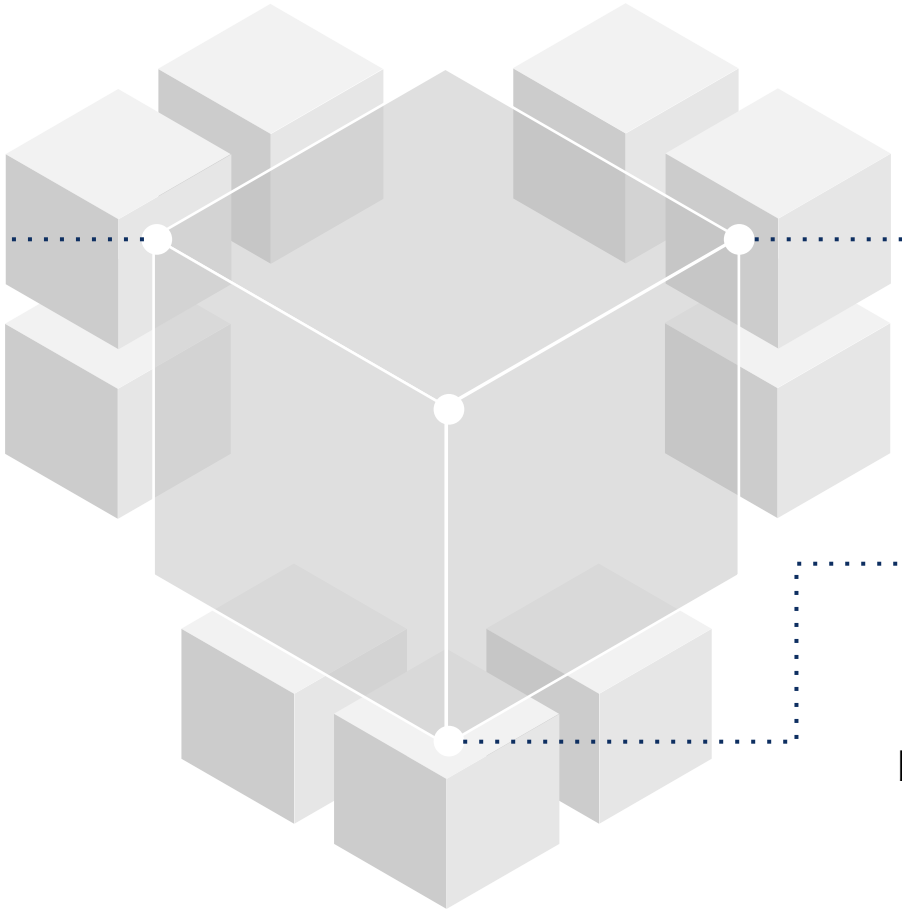
ART. 28 UST 5

Wystarczające gwarancje, o których mowa w ust. 1 i 4 niniejszego artykułu, podmiot przetwarzający może wykazać między innymi poprzez stosowanie **zatwierdzonego kodeksu postępowania**, o którym mowa w art. 40, lub **zatwierdzonego mechanizmu certyfikacji**, o którym mowa w art. 42.

Przepisy szczególne

Szczególne obowiązki w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta

(art. 24 ust. 6, art. 30a ust. 1)



Prawo telekomunikacyjne / Prawo komunikacji elektronicznej

(wykonywanie zadań i obowiązków związanych z bezpieczeństwem – tylko innemu przedsiębiorcy telekomunikacyjnemu, art. 179 ust. 7 PT / art. 50 ust. 1 PKE)

Prawo bankowe

(powierzenie działalności bankowej – umowa agencyjna, art. 6a PB)

Co mówi UODO…

„Administrator musi więc **szczególnie starannie zweryfikować**, czy podmiot, **któremu zamierza on powierzyć przetwarzanie danych osobowych**, dysponuje koniecznymi w tym celu środkami i daje odpowiednie gwarancje przestrzegania obowiązujących przepisów prawa”.

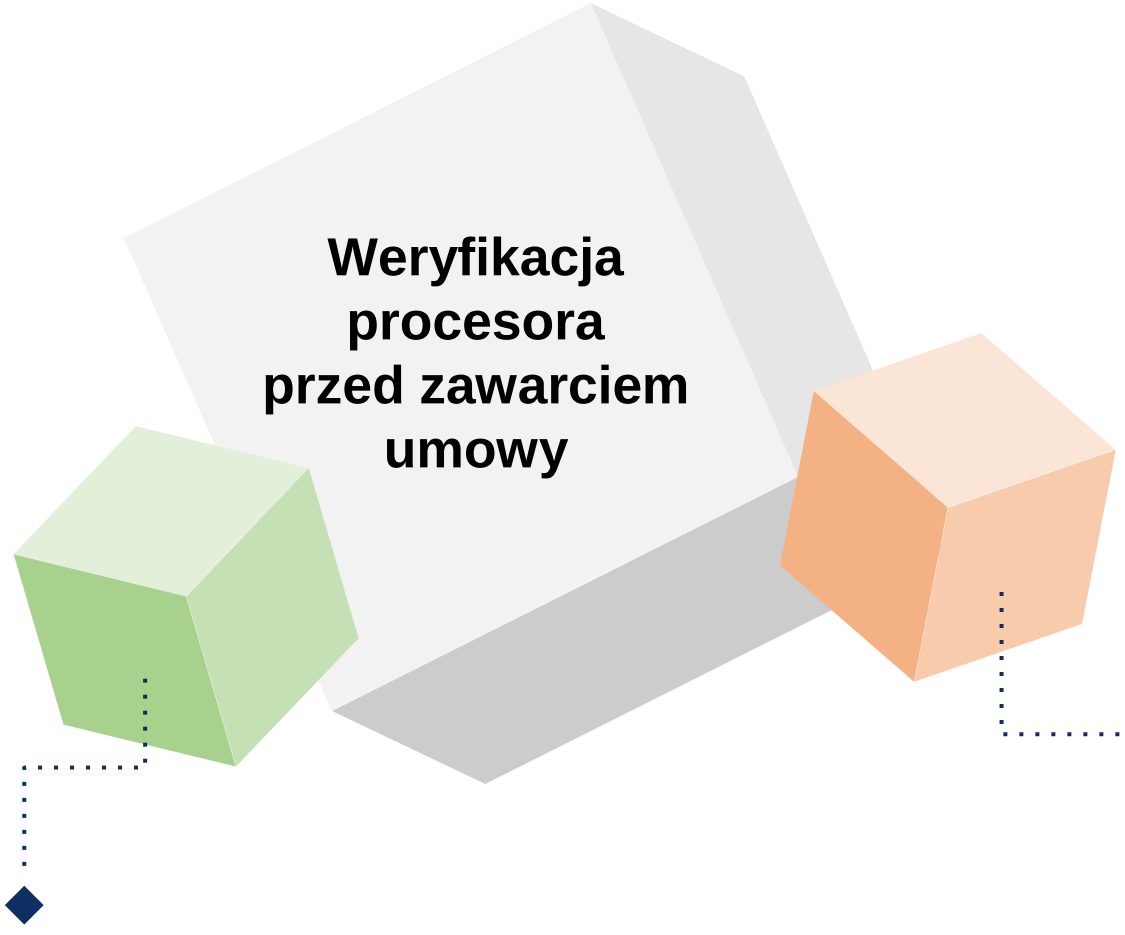
„W związku z tym administrator powinien mieć możliwość sprawdzenia komu powierza dane osobowe oraz w jaki sposób będą one przetwarzane. Prawo dostępu do takich informacji oraz przeprowadzania audytów przysługuje administratorowi **również w trakcie realizacji umowy** powierzenia”.

„Administrator jest bowiem zobowiązany **do stałej kontroli**, czy podmiot przetwarzający przetwarza dane zgodnie z prawem. Kontrole te mogą być przeprowadzane również doraźnie np. w przypadku wystąpienia naruszenia ochrony powierzonych danych osobowych”.

Czy administrator musi kontrolować podmiot przetwarzający?
(https://archiwum.uodo.gov.pl/pl/225/1213)

Weryfikacja procesora przed zawarciem umowy

GRC LEGAL



Bezpieczeństwo administratora

Rozliczalność

Co mówi UODO…

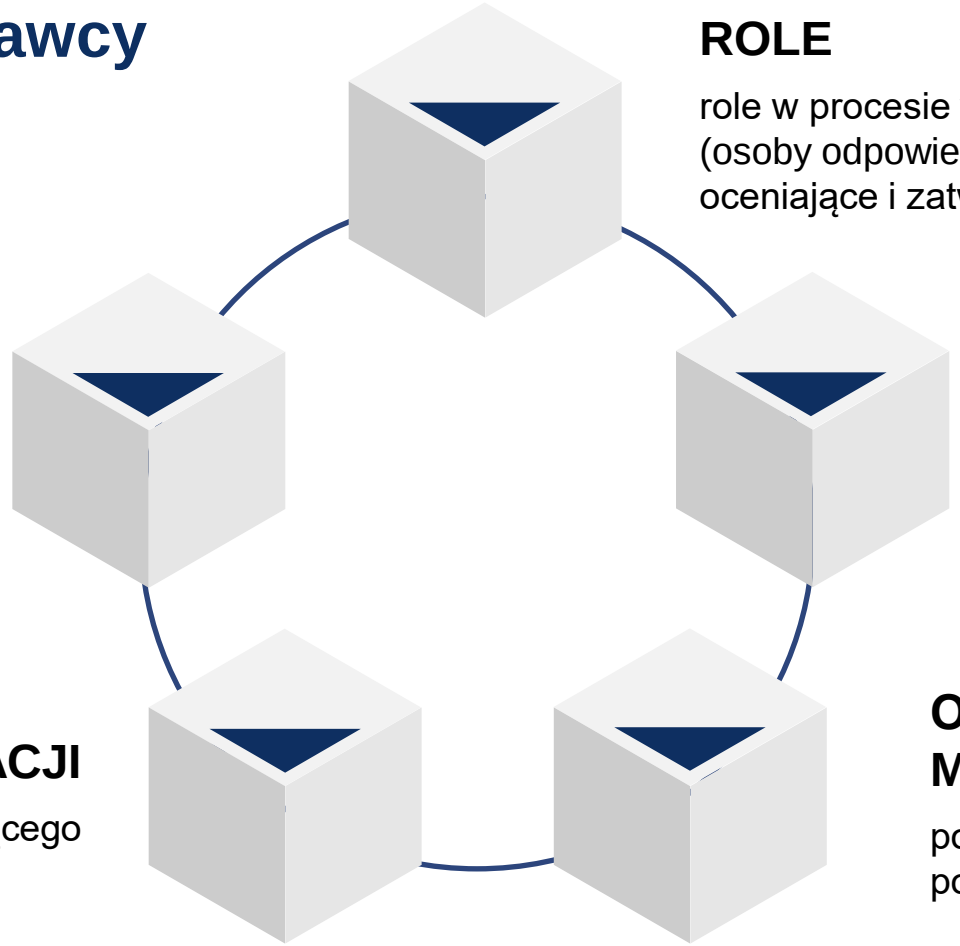
Trzeba ustalić, czy np. inspektor nie został obarczony zadaniem sporządzenia projektu umowy i w związku z tym, **czy to do niego nie należało określenie, w jaki sposób ukształtowana będzie relacja między administratorem i podmiotem przetwarzającym oraz prawa i zobowiązania stron tej umowy.** **Taka sytuacja powodowałaby konflikt interesów**, ponieważ IOD następnie w ramach swoich ustawowych obowiązków zobowiązany byłby ocenić prawidłowość i zgodność z przepisami podjętych w tym zakresie decyzji.

Inspektor nie powinien zatem podejmować zadań, które mogą stać się następnie przedmiotem dokonywania przez niego czynności monitorowania ani podejmować decyzji w zakresie celów i środków dotyczących przetwarzania i zabezpieczania danych. (…)
Ze względu na indywidualny charakter każdej organizacji ten aspekt powinien być analizowany osobno dla każdego podmiotu.

Czy IOD może w imieniu administratora zawierać umowy powierzenia?
(https://archiwum.uodo.gov.pl/pl/225/1804)

Obowiązek weryfikacji w dużej organizacji

– opracowanie i wdrożenie Polityki wyboru dostawcy



ROLE

role w procesie weryfikacji podmiotu przetwarzającego (osoby odpowiedzialne za przeprowadzenie procesu, osoby oceniające i zatwierdzające dany podmiot).

WARUNKI I ZASADY

dopuszczalności współpracy z podmiotem przetwarzającym

SPOSOBY DOKUMENTOWANIA

przeprowadzonej weryfikacji – zasada rozliczalności

SPOSOBY WERYFIKACJI

podmiotu przetwarzającego

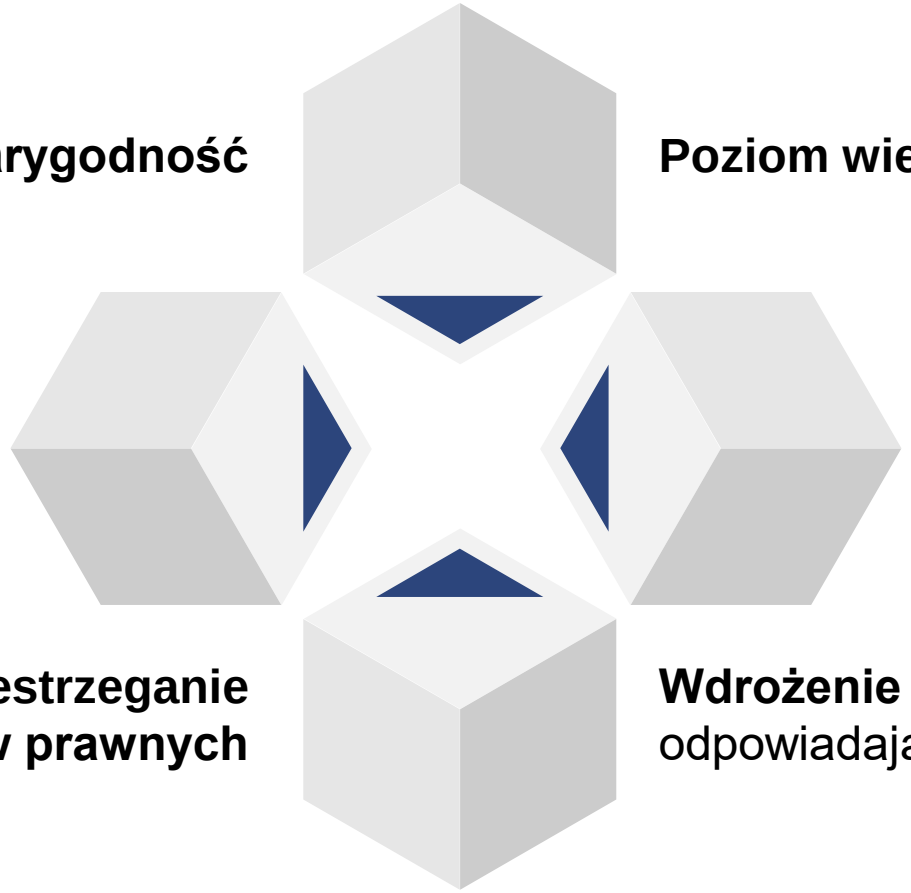
OBOWIĄZEK OKRESOWEGO MONITOROWANIA

podmiotu przetwarzającego co do aktualnego poziomu dawanych wcześniej gwarancji

Co należy zweryfikować?
Czym są właściwe gwarancje?

Wiarygodność

Poziom wiedzy



Przestrzeganie wymogów prawnych

Wdrożenie środków technicznych i organizacyjnych odpowiadających wymogom RODO

Pytania, ich dokładność i zakres powinny zależeć od charakteru powierzenia oraz zakresu powierzonych danych.

!

Wiarygodność

Certyfikaty z zakresu bezpieczeństwa informacji

Kontrole, audyty niezależnych podmiotów

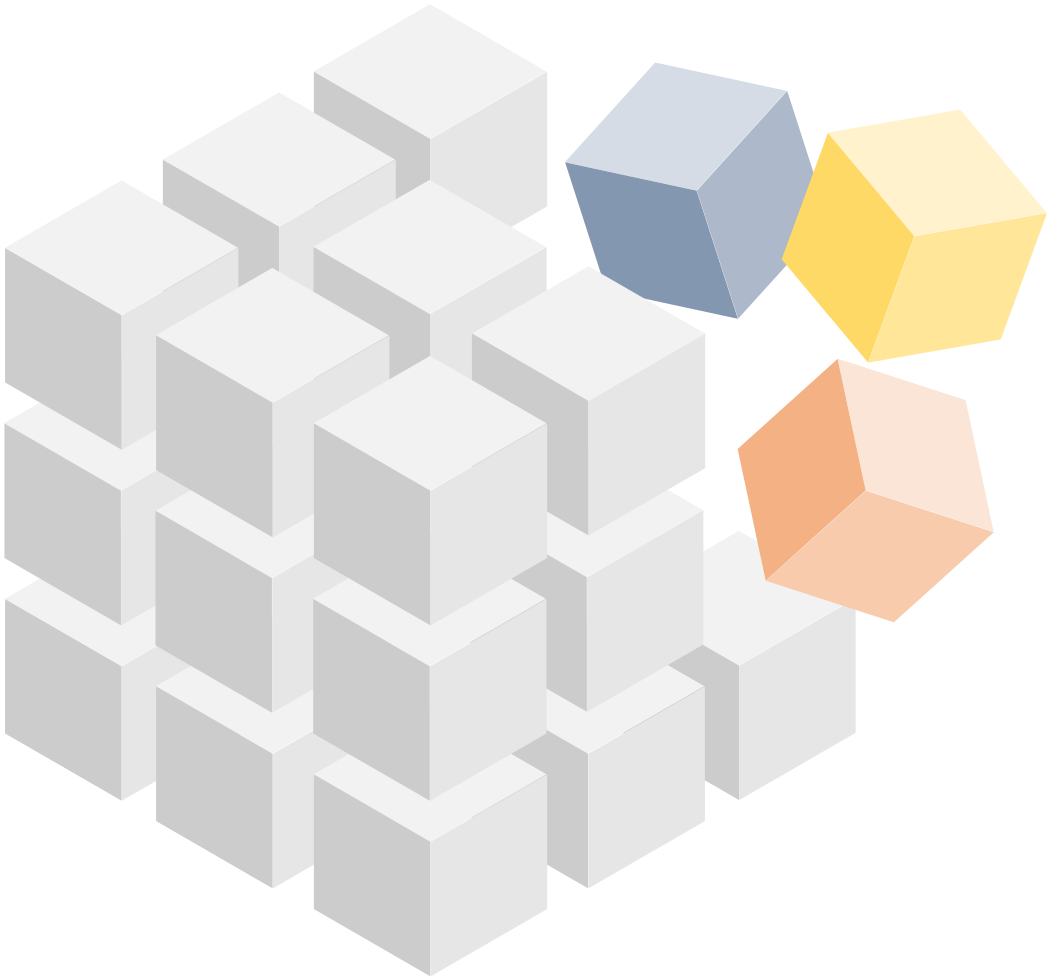
Mechanizm identyfikacji naruszeń ochrony danych

Weryfikacja procesora / podprocesora

Kontrole i postępowania przed PUODO i ich wynik

Stwierdzone naruszenia (liczba) wraz z odpowiednimi mechanizmami oceny i notyfikacji naruszeń

Poziom wiedzy



- **Dokumentacja** ochrony danych osobowych (Polityka ochrony danych; inne polityki i procedury)
- **Świadomość pracowników** co do bezpieczeństwa danych (szkolenia wstępne i okresowe)
- **Kompetencje i kwalifikacje IOD** (jeżeli istniał wymóg jego powołania) lub osoby odpowiadającej w organizacji za obszar ochrony danych osobowych

Przestrzeganie wymogów prawnych

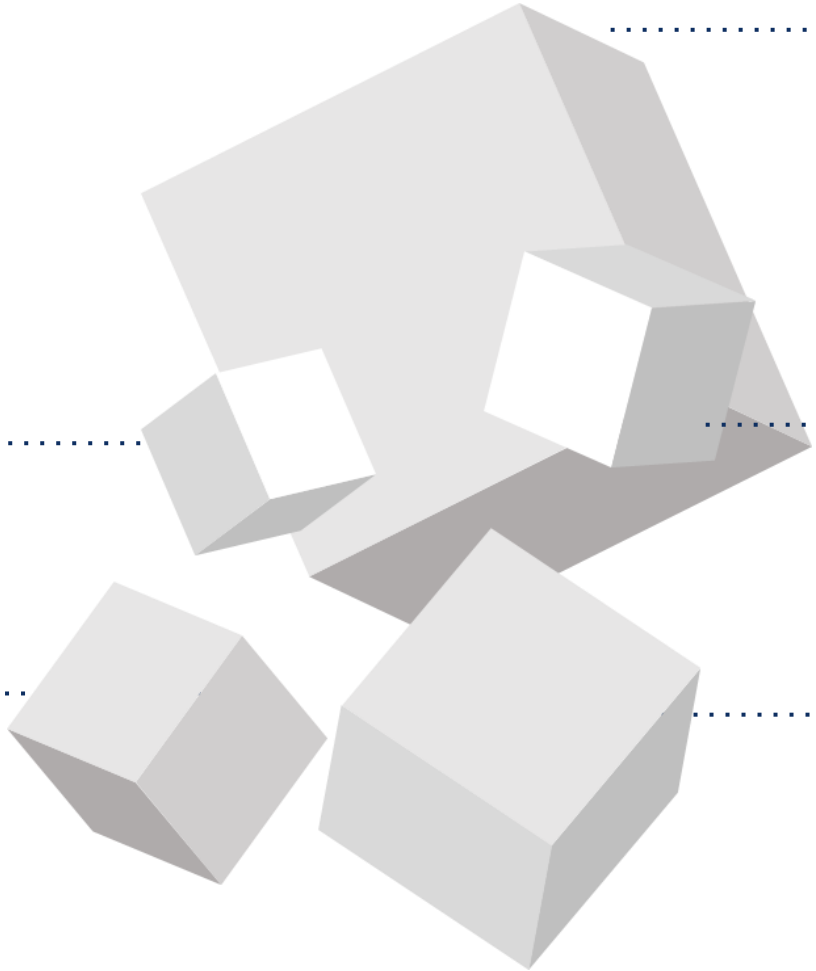
Transfer danych poza EOG i zastosowany mechanizm legalizujący

Rejestry

Zobowiązanie do zachowania tajemnicy

Upoważnienia

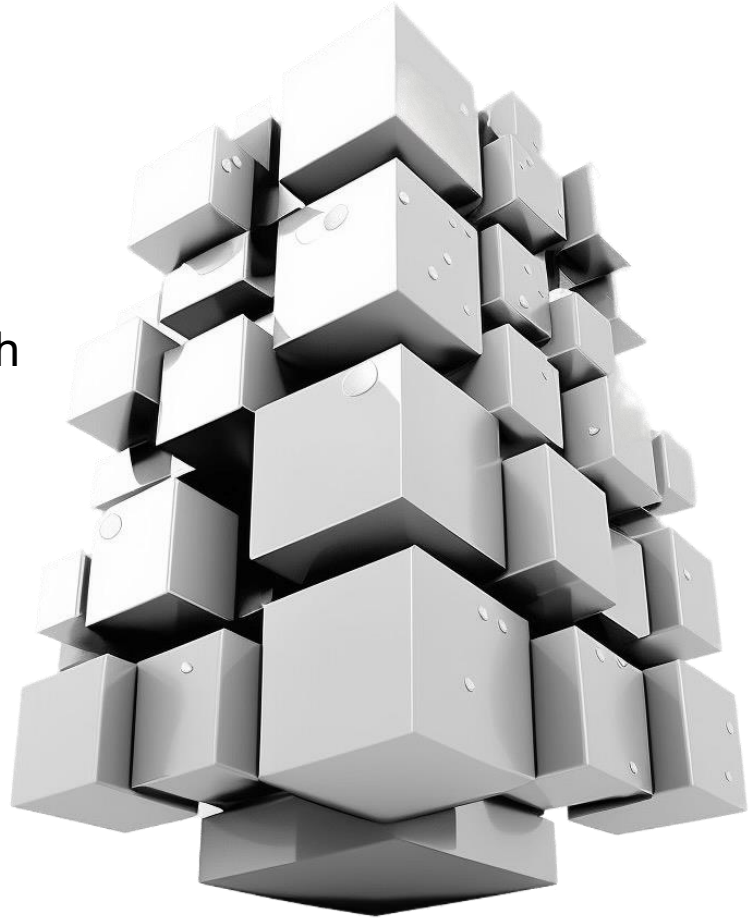
Powołanie Inspektora Ochrony Danych (o ile to konieczne)



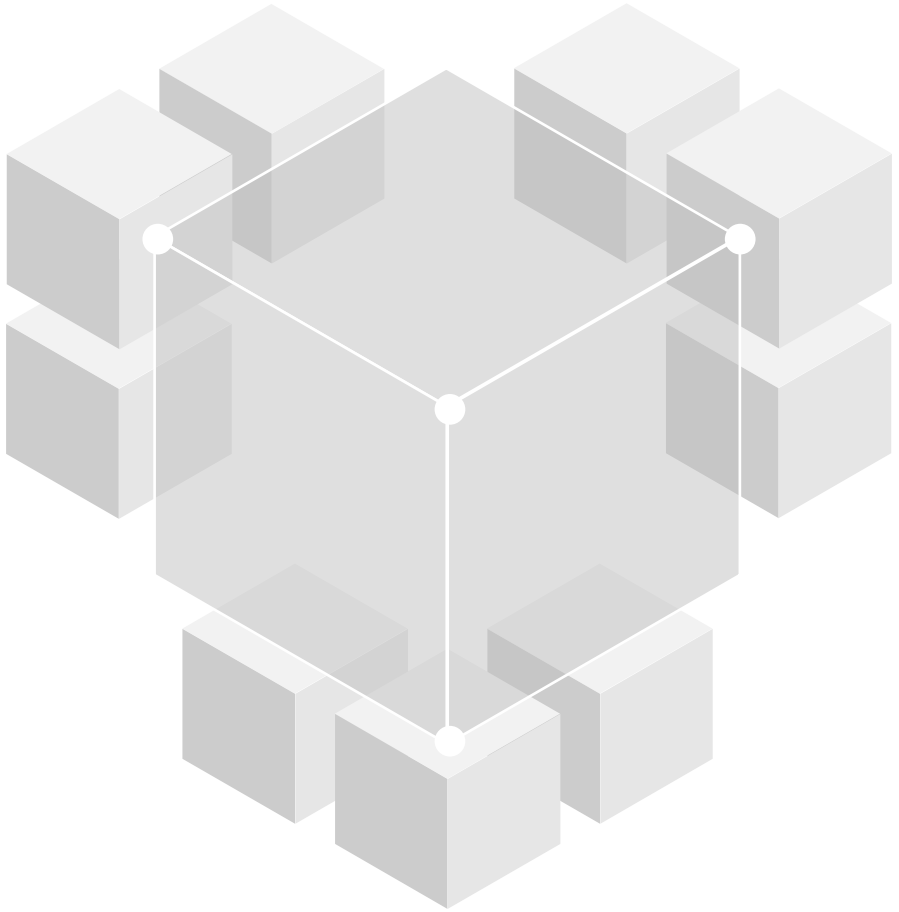
GRC LEGAL

Wdrożone środki techniczne i organizacyjne odpowiadające wymogom RODO

- System kontroli dostępu do obszaru przetwarzania danych
- Sposób przechowywania i zabezpieczania dokumentów papierowych
- Zasady nadawania uprawnień i dostępu do systemów informatycznych
- Polityka haseł (struktura, częstotliwość zmiany)
- Oprogramowanie Antywirusowe;
- Zasady dostępu do sprzętu mobilnego
- Zabezpieczanie sprzętu mobilnego
- Kopie zapasowe
- Zdolność szybkiego przywracania dostępu do danych w sytuacji incydentu fizycznego lub technicznego
- Inne środki gwarantujące poufność, integralność i dostępność danych



Rozliczalność



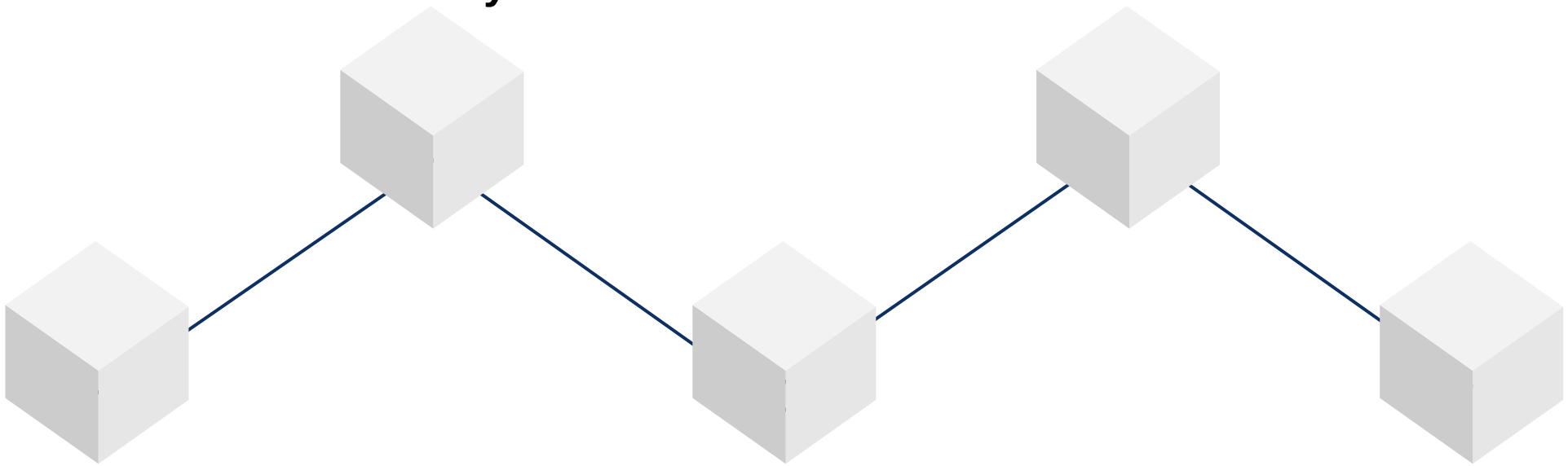
- Weryfikacja pisemna lub elektroniczna
- Rozmowa kwalifikacyjna – niewystarczająca
- Dotychczasowa dobra współpraca – niewystarczająca

Prezes UODO podczas kontroli lub korzystając z uprawnienia, o którym mowa w art. 58 RODO, może żądać potwierdzenia faktu, że Administrator wybiera wyłącznie zaufanych procesorów

Praktyczne rozwiązania wyboru procesorów

Audyt przed zawarciem umowy

Oświadczenie procesora *in spe*



Opracowanie standardowej ankiety procesora badania procesorów

Przedstawione **certyfikaty**

Lista podmiotów zweryfikowanych (długość ważności wpisu)

Weryfikacja procesora w trakcie trwania umowy

GRC LEGAL

Audyt procesora – czynniki niezbędne do ustalenia

KIEDY

- **Cykliczne** – np. raz na rok
- **Incydentalne** – np. po wystąpieniu naruszenia, po zidentyfikowaniu naruszenia umowy, po doniesieniach medialnych dotyczących procesora

JAK

- Administrator **swoimi siłami**
- **Za pośrednictwem** upoważnionego audytora

WAŻNE! Ustalenie harmonogramu audytów i jego terminowe realizowanie pomoże w wykazaniu rozliczalności (art. 5 ust. 2 RODO)

Audyt procesora – czynniki niezbędne do ustalenia

W JAKIEJ FORMIE

- **On site** – np. w miejscu przetwarzania / w lokalu procesora
- **Online** – np. spotkanie przez komunikator internetowy / ankieta weryfikacyjna dostępna na stronie internetowej / checklisty / korespondencja mailowa

W JAKI SPOSÓB

- **Odpowiedzi** na zadane wcześniej pytania
- **Rozmowy** z wyznaczonymi pracownikami
- **Wgląd** do dokumentów lub systemów informatycznych

Audyt procesora – od czego zacząć?

W JAKIM ZAKRESIE

- **Cykliczne** – w zależności od zakresu powierzenia
- **Incydentalne** – w zależności od okoliczności

OPŁATA

- **Czy dopuszczamy odpłatność audytu?**
  Jeśli tak – czy zawsze?
- **Kto ponosi koszty audytu?**
  Administrator / procesor / łącznie

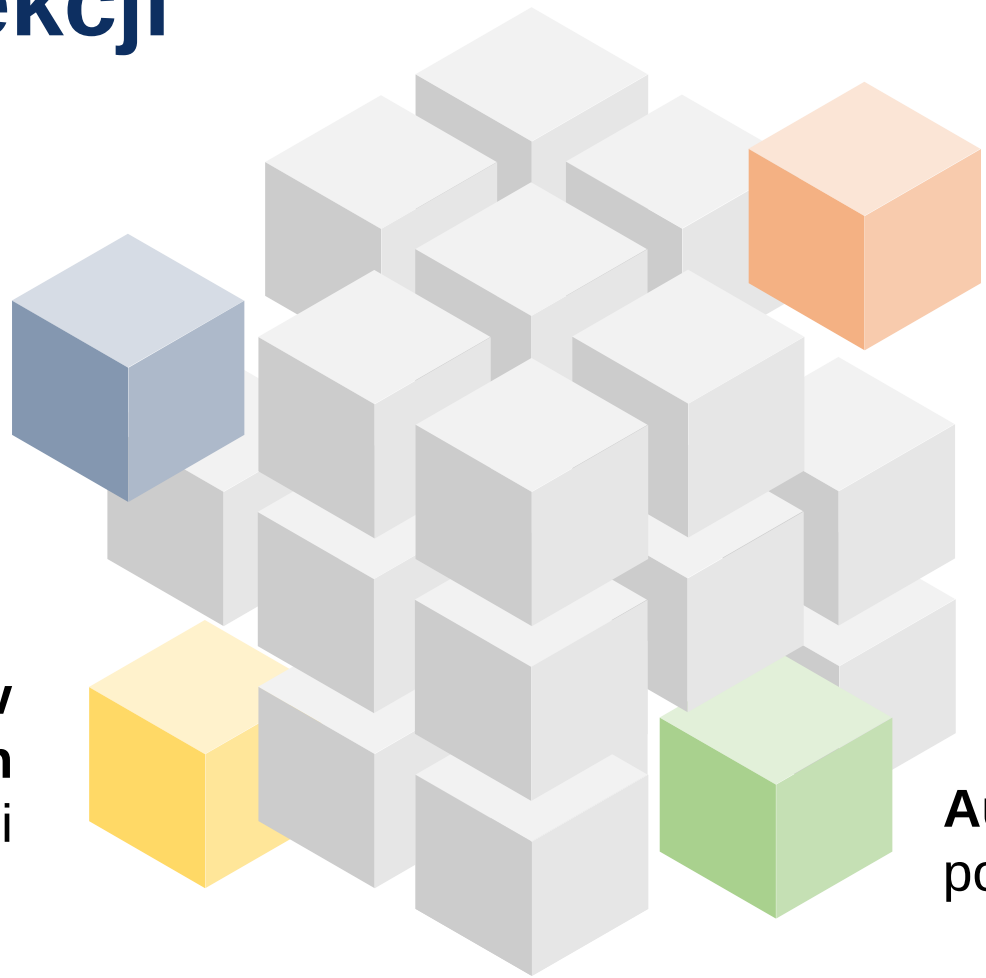
W JAKIM CZASIE

- **Z jakim wyprzedzeniem** administrator informuje procesora o planowanym audycie – np. na 2 tygodnie przed
- **Czas reakcji procesora** – np. potwierdzenie w ciągu 72 h od otrzymania wezwania do przeprowadzenia audytu
- **W jakich godzinach** – np. w czasie pracy procesora / 8:00 -16:00
- **Maksymalny czas trwania audytu** – np. dzień / kilka dni / tydzień

Inne ustalenia dotyczące audytu i inspekcji

Czy dane mogą być **transferowane poza EOG**

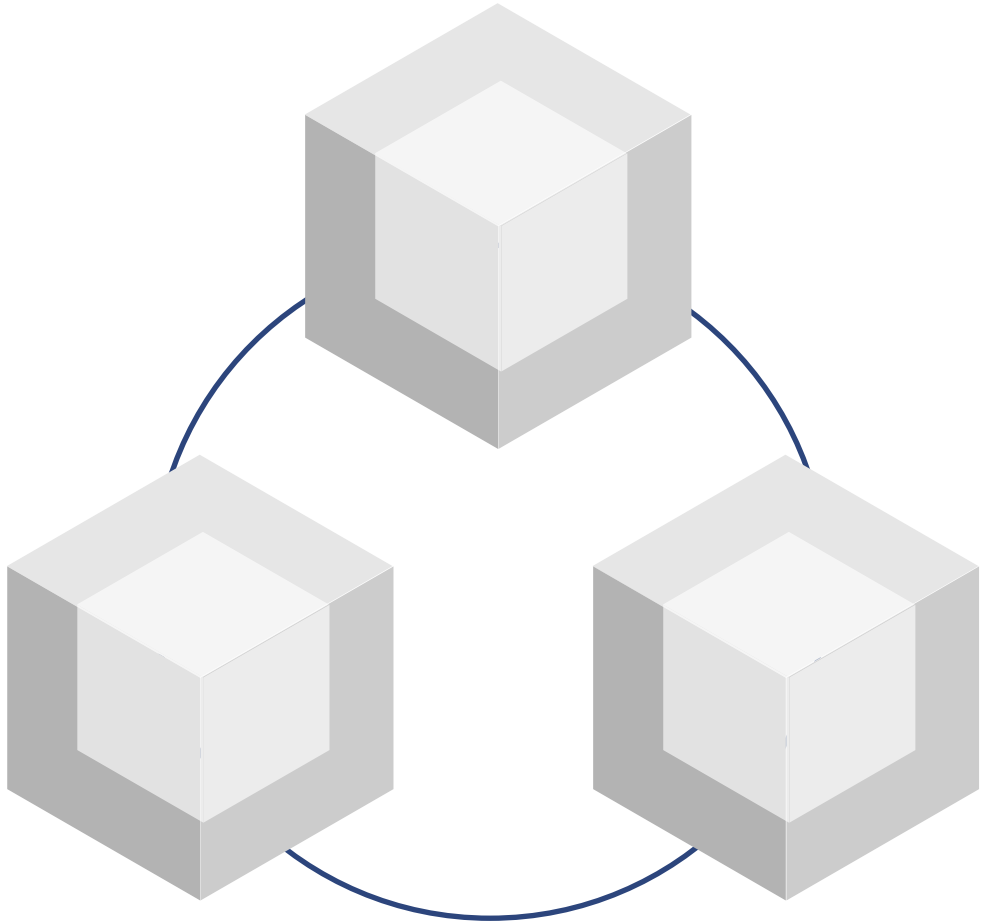
Zakaz udziału podmiotów konkurencyjnych w audycie / inspekcji



Obowiązek zachowania tajemnicy względem informacji zdobytych w ramach audytu / inspekcji

Audyt / inspekcja podprocesora

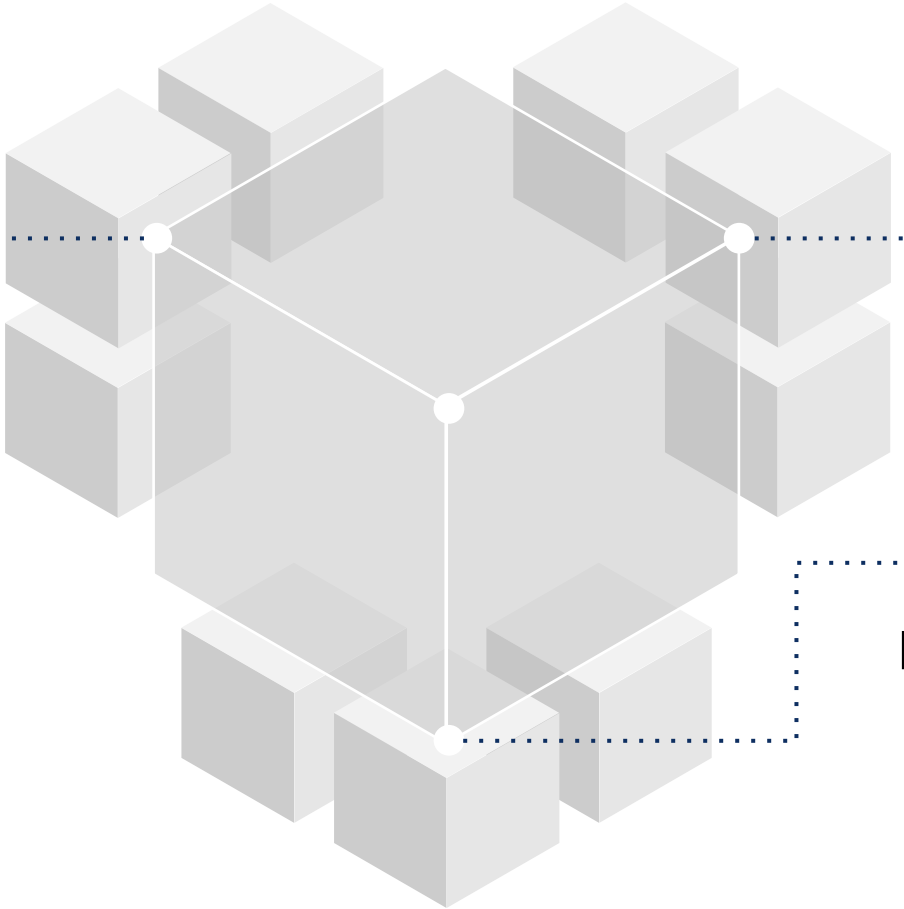
Audyt i inspekcja podprocesora



- **Przepisy wprost nie regulują** – ograniczając obowiązek audytu i inspekcji do pierwszego ogniwa łańcucha powierzenia
- Nie ma przeszkód, aby **uregulować** kwestię audytu dalszych podmiotów przetwarzających **w umowie**
- Jeżeli bowiem dalszy przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, **pełna odpowiedzialność** wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego **spoczywa na pierwotnym podmiocie przetwarzającym**

Problem z monopolistami lub quasi-monopolistami

Trudności z praktyczną realizacją inspekcji



Trudności z otrzymaniem informacji już na etapie przed zawarciem umowy powierzenia

Narzucanie ograniczeń audytów i inspekcji

Udział procesora w kontroli u administratora?

Art. 28 ust. 3 lit. e) i f) RODO

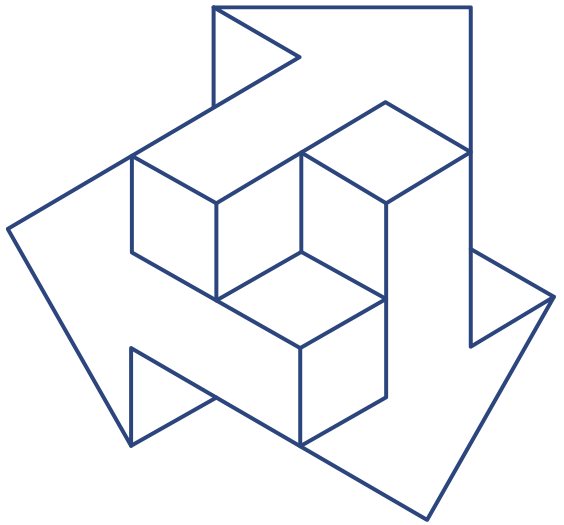
(…) podmiot przetwarzający: (…)

e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III;

f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36

Art. 31 RODO

Administrator i podmiot przetwarzający oraz – gdy ma to zastosowanie – ich przedstawiciele na żądanie współpracują z organem nadzorczym w ramach wykonywania przez niego swoich zadań.



Efekty audytu / kontroli

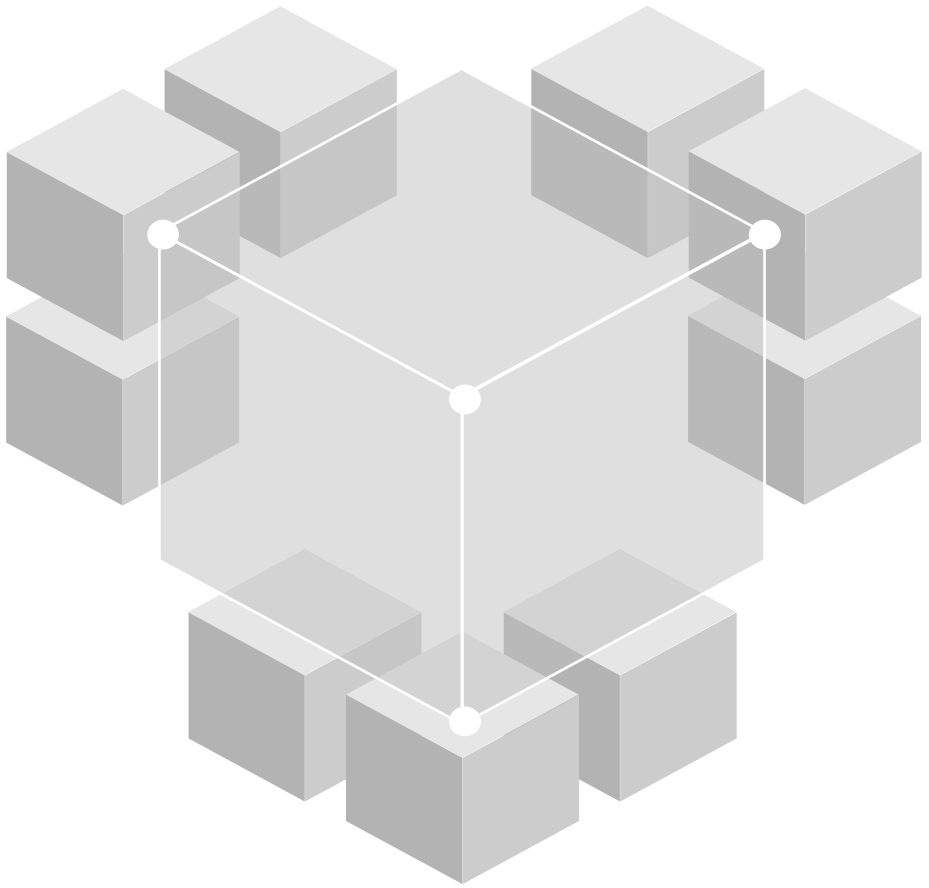
Wyznaczenie **rekomendacji**

Sporządzenie **protokołu pokontrolnego**

Pociągnięcie procesora do odpowiedzialności za uchybienia w realizacji wymogów umowy powierzenia

Ewentualna **zmiana zakresu umowy**

Protokół pokontrolny



- Podpisany przez obie strony
- Treść: zastrzeżenia wraz z rekomendacjami
- Zobowiązanie procesora do dostosowania zaleceń pokontrolnych zawartych w protokole

WAŻNE! Dobrą praktyką będzie ustalenie terminu końcowego na wdrożenie zaleceń pokontrolnych. Po upływie tego terminu należy zweryfikować efekt wdrożenia zaleceń.

Co, gdy procesor w dalszym ciągu nie wdroży zaleceń?

Granice audytu – przykłady z art. 28 RODO

Obowiązek procesora	Co może ADO?	Co przekracza granice audytu? (rekomendacje / odpowiedzialność)
Wdrożenie odpowiednich środków bezpieczeństwa	1. Zweryfikować i ocenić wdrożone przez procesora środki 2. Negocjować wdrożenie dodatkowych środków w zakresie osiągalnym dla procesora	Zobowiązanie procesora do: 1. Przeprowadzenia konkretnej certyfikacji mimo wyraźnego braku przesłanek do jej wdrożenia (np. ISO 27001) 2. Zatrudnienia IOD, mimo przedstawienia uzasadnienia dla braku jego powołania 3. Pociągnięcie procesora do odpowiedzialności za niewdrożenie niewspółmiernych środków zalecanych przez ADO (jak powyżej)
Uzyskanie uprzedniej zgody ADO na korzystanie z usług innych podprocesorów	1. Wyrazić uprzednią szczegółową zgodę 2. Wyrazić uprzednią ogólną zgodę	Pociągnięcie procesora do odpowiedzialności za zaangażowanie nowych podprocesorów bez szczegółowej zgody administratora, podczas gdy w umowie powierzenia udzielona została ogólna zgoda, a administrator nie sprzeciwił się zmianom

Granice audytu – przykłady z art. 28 RODO

Obowiązek procesora	Co może ADO?	Co przekracza granice audytu? (rekomendacje / odpowiedzialność)
Pomoc administratorowi w wywiązaniu się z obowiązku odpowiedzi na żądania podmiotów danych	Zobowiązać procesora do niezwłocznego przekazywania ADO informacji o: 1. otrzymanych żądaniach podmiotów danych 2. zakresie informacji posiadanych o podmiocie danych w związku z prowadzonymi w imieniu ADO czynnościami (np. obsługa call center)	1. Zobowiązanie procesora do przejęcia obsługi żądań podmiotów danych bez kontroli ani wytycznych ze strony ADO 2. Pociągnięcie procesora do odpowiedzialności za brak samodzielnej odpowiedzi na otrzymane żądanie
Pomoc administratorowi w wywiązaniu się z obowiązków związanych ze zgłoszeniem naruszenia	Zobowiązać procesora do niezwłocznego przekazywania ADO informacji o: 1. o stwierdzonych incydentach bezpieczeństwa danych 2. przebiegu naruszenia oraz podjętych środkach zaradczych	1. Zobowiązanie procesora do samodzielnego stwierdzania wystąpienia naruszeń ochrony danych osobowych 2. Pociągnięcie procesora do odpowiedzialności za brak samodzielnego stwierdzenia naruszenia ochrony danych osobowych lub zgłoszenia naruszenia do PUODO

Granice audytu – przykłady z art. 28 RODO

Obowiązek procesora	Co może ADO?	Co przekracza granice audytu? (rekomendacje / odpowiedzialność)
Pomoc administratorowi w wywiązaniu się z obowiązku przeprowadzenia analizy ryzyka	Zobowiązać procesora do dostarczenia informacji niezbędnych do przeprowadzenia przez ADO oceny skutków dla ochrony danych w zakresie prowadzonych procesów przetwarzania	1. Zobowiązanie procesora do samodzielnego przeprowadzenia analizy ryzyka w imieniu ADO 2. Pociągnięcie procesora do odpowiedzialności za brak przeprowadzenia analizy ryzyka w imieniu ADO
Dostarczanie wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w 28	Zobowiązać procesora do przekazania informacji dotyczących przetwarzania danych objętych powierzeniem	1. Domaganie się od procesora informacji, które nie dotyczą przetwarzania danych osobowych objętych powierzeniem

Odpowiedzialność administratora i procesora

GRC LEGAL

O co może pytać UODO…

- **W jaki sposób Administrator zapewnia**, aby podmioty przetwarzające przetwarzały dane osobowe jego klientów zgodnie z przepisami o ochronie danych osobowych?
- **Czy i jakie środki podjął Administrator** w celu zabezpieczenia danych osobowych przetwarzanych w aplikacji funkcjonującej na infrastrukturze podmiotu przetwarzającego oraz jakie przyjęto środki zabezpieczenia technicznego i organizacyjnego?
- **W jaki sposób Administrator zweryfikował** wdrożone środki techniczne oraz organizacyjne przez podmiot przetwarzający dane w imieniu Administratora, u którego wystąpiło naruszenie?
- **Czy, a jeśli tak, to w jaki sposób Administrator dokonywał regularnego testowania**, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych?

Obowiązki ADO i procesora

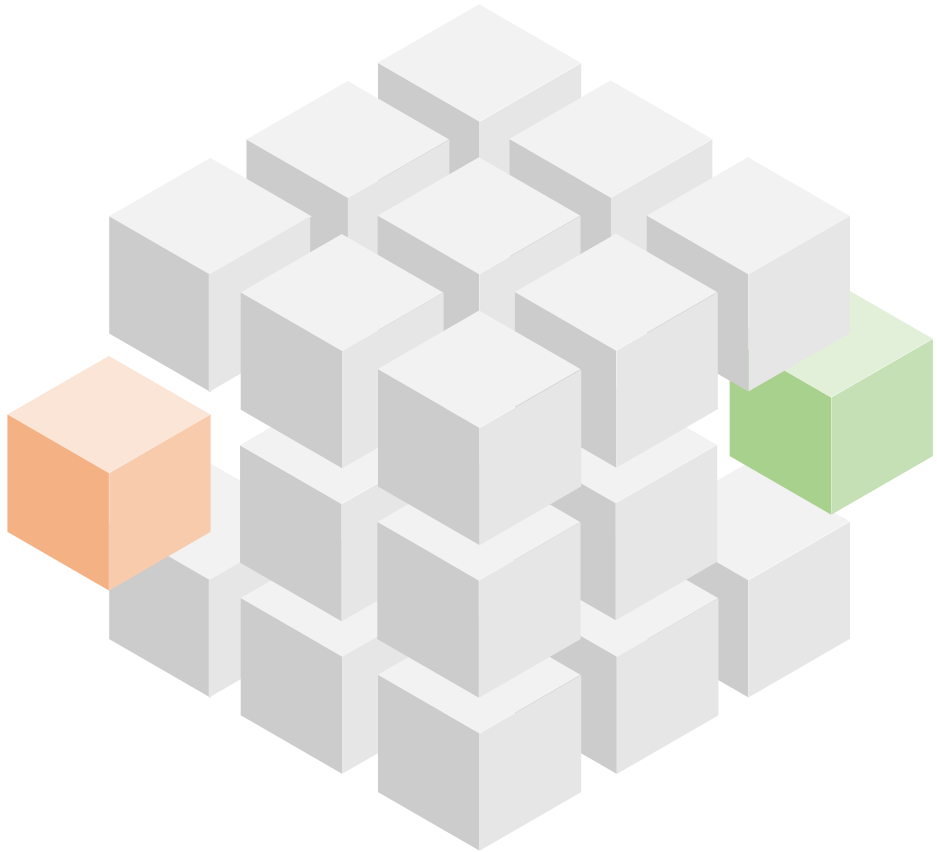
ADO	PROCESOR
Posiadanie podstawy prawnej do przetwarzania danych	Działanie zgodnie z poleceniami ADO
Realizacja i rozpatrywanie żądań podmiotów danych	Wsparcie w realizacji zadań ADO
Analiza skutków dla podmiotów danych	Brak własnego celu przetwarzania
Rozpatrywanie i zgłaszanie naruszeń	Informowanie o naruszeniach

Wspólne obowiązki

Odpowiedzialność za naruszenie bezpieczeństwa powierzonych danych

Prawo do odszkodowania

- zarówno od ADO
- jak i od procesora (wyłącznie, gdy nie dopełnił obowiązków nałożonych na podmioty przetwarzające w RODO lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom)



Solidarna odpowiedzialność

ADO i procesora za odszkodowanie

Najczęstsze powody nałożenia kary z art. 28 RODO

A

Brak weryfikacji procesora przed nawiązaniem współpracy

B

Pozostawienie procesorowi dowolności co do ŚTO

C

Brak cyklicznej weryfikacji

Najpopularniejsze kary – ADO

- **Decyzja DKN.5130.3114.2020** - kara w wysokości 1 136 975 zł nałożona na Cyfrowy Polsat S.A. – współpraca z firmą kurierską

WAŻNE! Wyrok WSA w Warszawie z dnia 15 listopada 2021 r. (sygn. akt II SA/Wa 2465/21) uchylający nałożoną karę

„Organ, w szczególności, nie dokonał w sposób pełny ustaleń co do roli i zakresu odpowiedzialności "podmiotu świadczącego usługi kurierskie'', w tym co do okoliczności pozwalających na "zakwalifikowanie" tego podmiotu jako administratora lub procesora w ramach współpracy z [...] oraz określenia zakresu zadań i obowiązków każdego z nich, w ramach zapewnienia bezpieczeństwa przetwarzania danych klientów [...] przez szybką identyfikację naruszeń.”

- **Decyzja DKN.5131.5.2020** – kara w wysokości 85 588 zł. nałożona na TUiR Warta S.A. m.in. za błędną wysyłkę maila przez agenta ubezpieczeniowego (procesora)
- **Decyzja DKN.5130.2024.2020** – kara w wysokości 100 tys. zł nałożona na KSSiP m.in. za niezastosowanie odpowiednich ŚTO
- **Decyzja DKN.5131.31.2021** – kara w wysokości 1.556,28 nałożona na wspólnotę mieszkaniową za brak umowy powierzenia i niezastosowanie ŚTO

Najpopularniejsze kary – ADO i procesor

- **Decyzja DKN.5131.50.2021** – kara w wysokości 33 012 zł. nałożona na administratora za utracenie poufności danych osobowych oraz w wysokości 427 zł na procesora za niewdrożenie odpowiednich ŚTO

Ważne! PUODO nałożył na administratora nakaz zaprzestania powierzania danych osobowych do podmiotu przetwarzającego

- **Decyzja DKN.5130.2215.2020** – kara w wysokości 4,8 mln nałożona na Fortum Marketing and Sales Polska S.A. oraz w wysokości 250 135 zł na PIKA sp. z o.o. za niewdrożenie odpowiednich ŚTO

- **Wyrok WSA II SA/Wa 310/20**

„Jak już wyżej wskazano, w sytuacji gdy podmiot przetwarzający dane osobowe naruszy ogólne rozporządzenie o ochronie danych przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania (art. 28 ust. 10). Podejmowanie decyzji o celach i sposobach przetwarzania danych należy do sfery uprawnień administratora danych. Jeżeli w tę sferę bezprawnie ingeruje podmiot przetwarzający, wchodząc w zakres zastrzeżony administratorowi, to art. 28 ust. 10 ww. rozporządzenia nakazuje uznać podmiot przetwarzający za administratora w odniesieniu do tego przetwarzania. Oznacza to, że podmiot przetwarzający odpowiada w tym zakresie za naruszenie przepisów rozporządzenia tak jak administrator (Fajgielski P., Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, WKP 2018, art. 28).”

GRC
LEGAL

Aleksandra Jarkiewicz
+ 48 735 200 988
aleksandra.jarkiewicz@grclegal.pl

Beata Kąkol-Dembowska
+ 48 532 691 789
beata.kąkol-dembowska@grclegal.pl