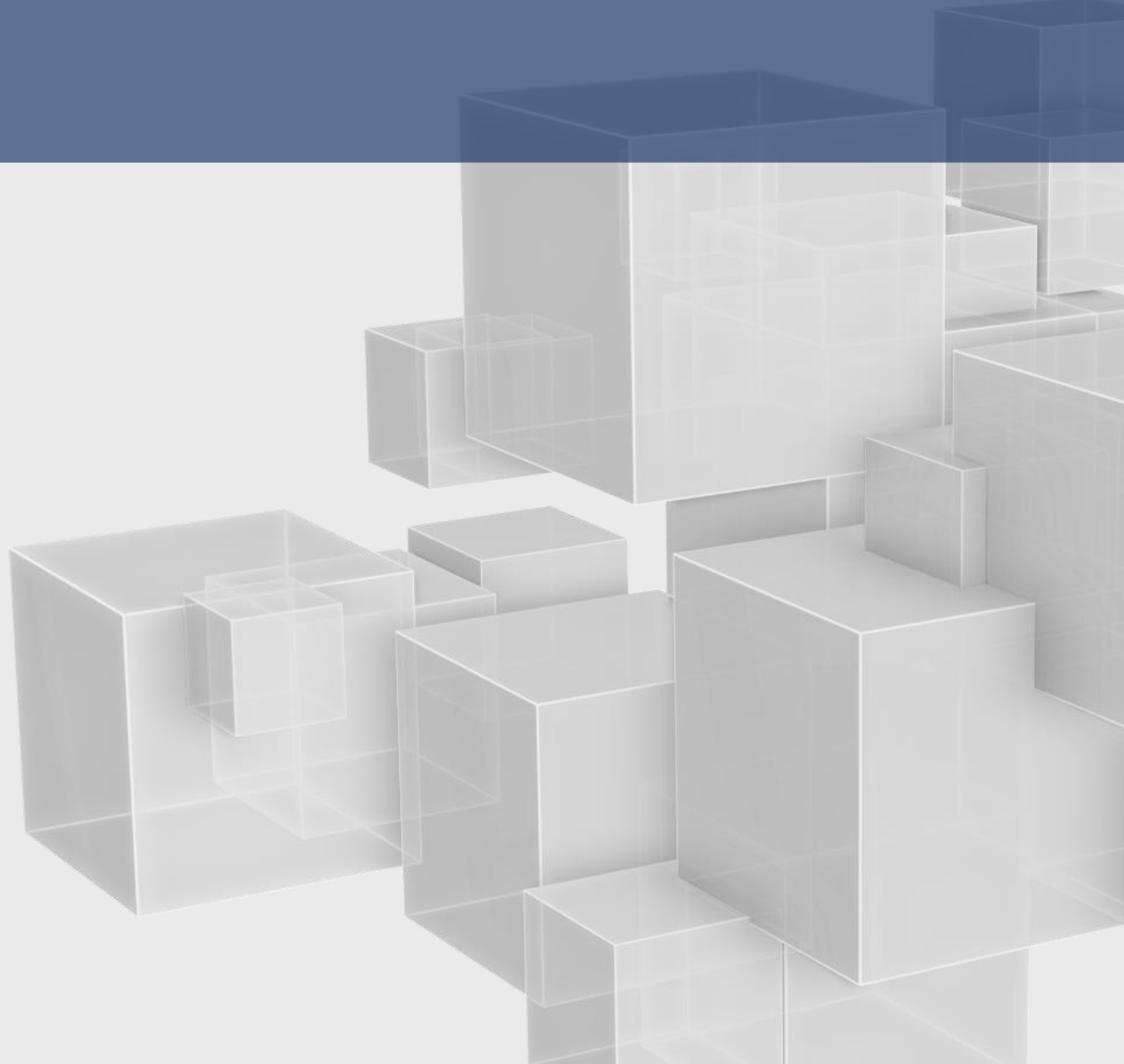
WEBINARIA GRC

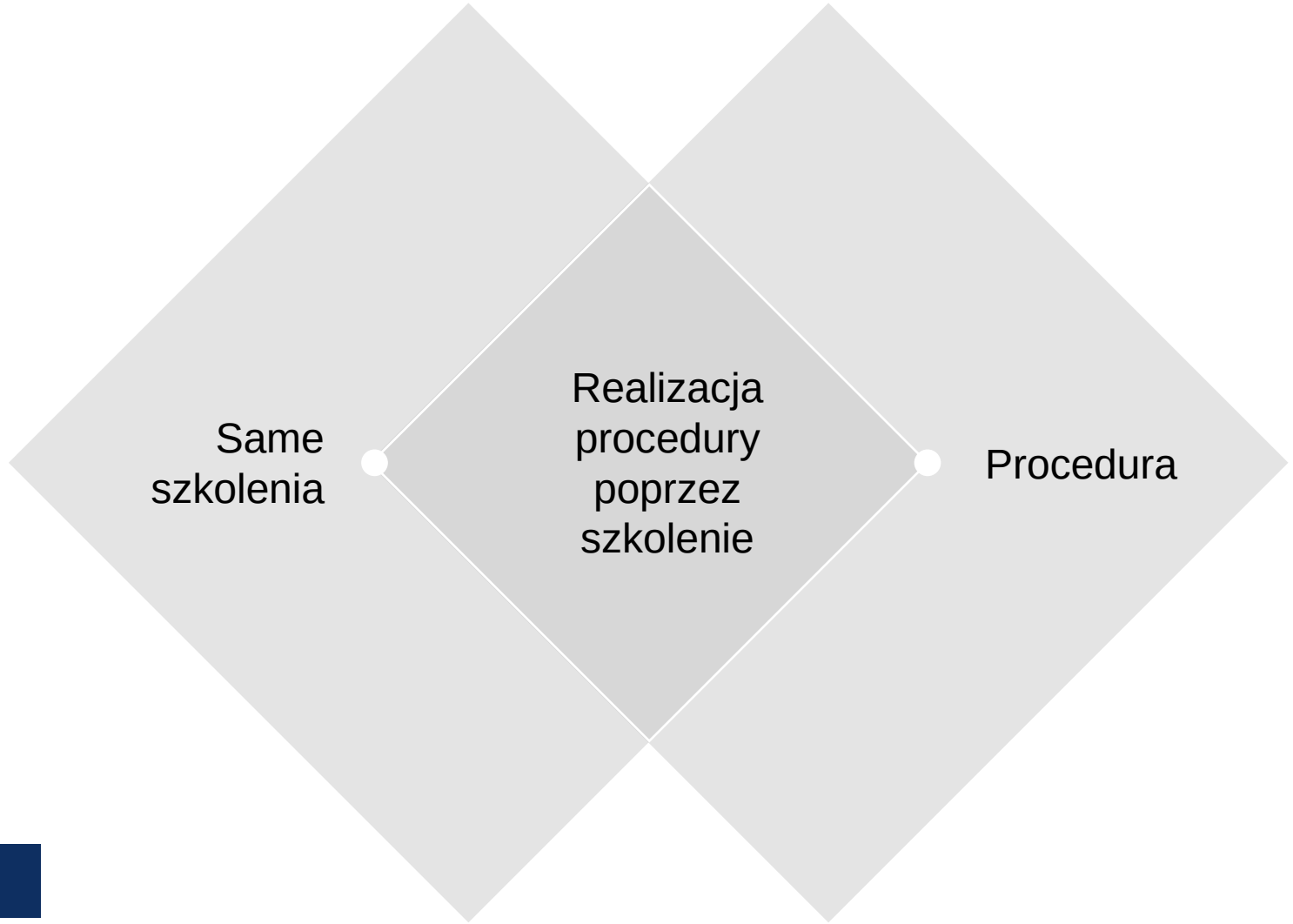
POLITYKA SZKOLENIOWA

Aleksandra Jarkiewicz

GRC LEGAL



Szkolenia – konieczna uciążliwość czy ważniejszy środek bezpieczeństwa?



GRC LEGAL

Źródło obowiązku

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża **odpowiednie środki** techniczne i **organizacyjne**, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. **Środki te są w razie potrzeby poddawane przeglądom i uaktualniane**.

ART. 24 UST. 1 RODO

Źródło obowiązku

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają **odpowiednie środki** techniczne i **organizacyjne**, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

ART. 32 UST. 1 RODO

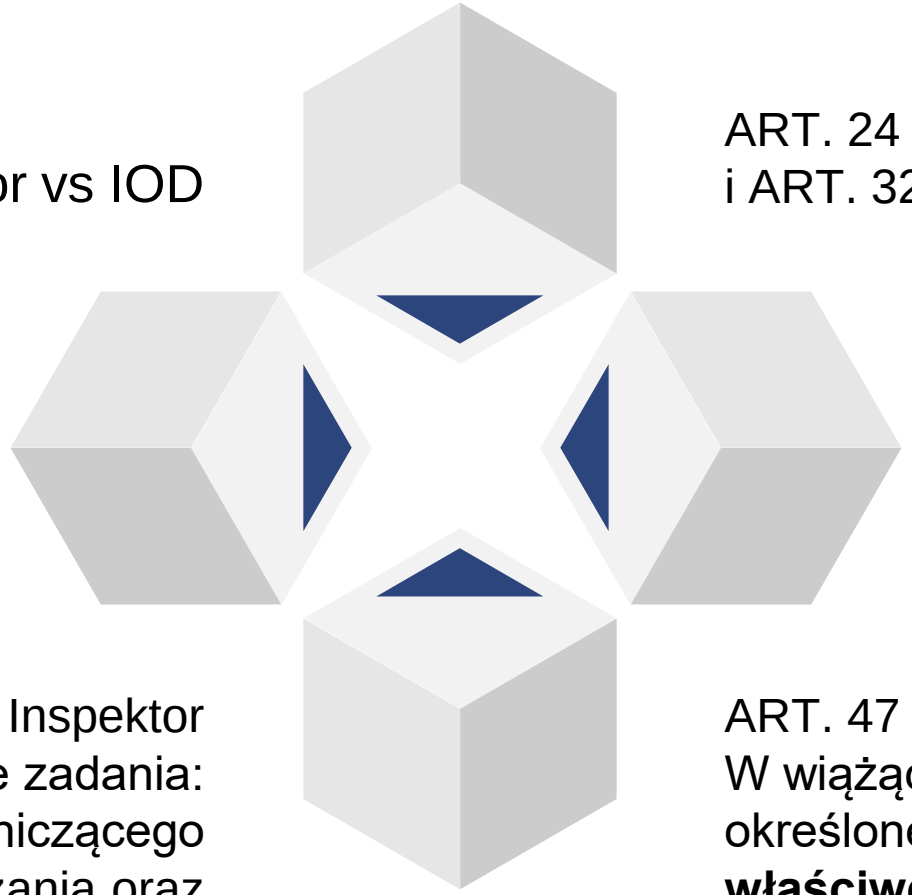
Źródło obowiązku

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.

ART. 32 UST. 4 RODO

Czyj obowiązek?

Administrator vs IOD



ART. 24 UST. 1 RODO
i ART. 32 UST. 1 RODO

ART. 39 UST. 1 LIT. B) RODO: Inspektor ochrony danych ma następujące zadania: (…) **szkolenia personelu** uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty

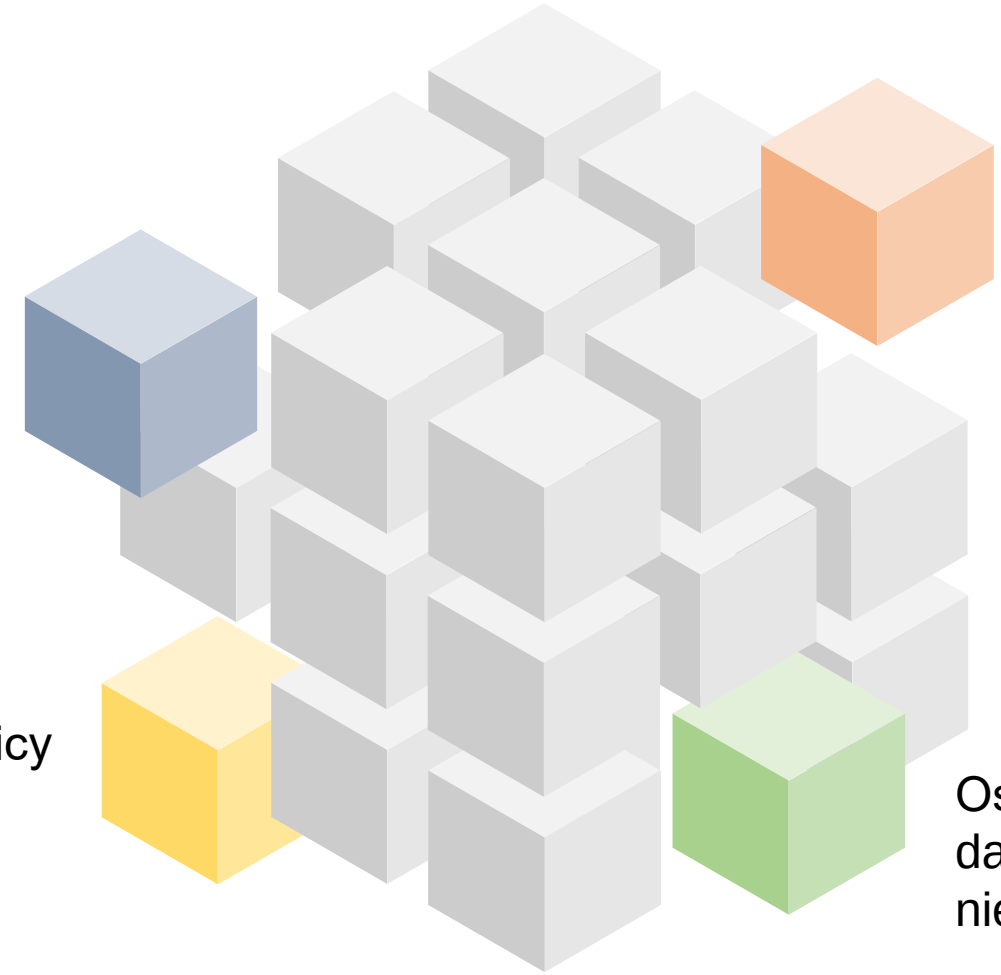
ART. 47 UST. 2 LIT. N) RODO:
W wiążących regułach korporacyjnych, określone zostają co najmniej (…) **właściwe szkolenia z zakresu ochrony danych** dla personelu mającego stały lub regularny dostęp do danych osobowych

Obowiązek IOD

Wytyczne dotyczące inspektorów ochrony danych – wp243rev.01

opisując podejście oparte na analizie ryzyka, wytyczne wskazują, „że selektywne i pragmatyczne podejście powinno ułatwić DPO doradzenie administratorowi, jaką metodologię należy zastosować przy przeprowadzeniu oceny skutków dla ochrony danych, które obszary powinny zostać poddane wewnętrznemu albo zewnętrznemu audytowi, **jakie szkolenia wewnętrzne przeprowadzić dla pracowników lub kierowników odpowiedzialnych za przetwarzanie danych**, i na które operacje przetwarzania przeznaczyć więcej czasu i zasobów.”

Kogo szkolimy



Pracownicy

Współpracownicy

Osoby spoza organizacji (np. pracownicy/ współpracownicy dostawców)

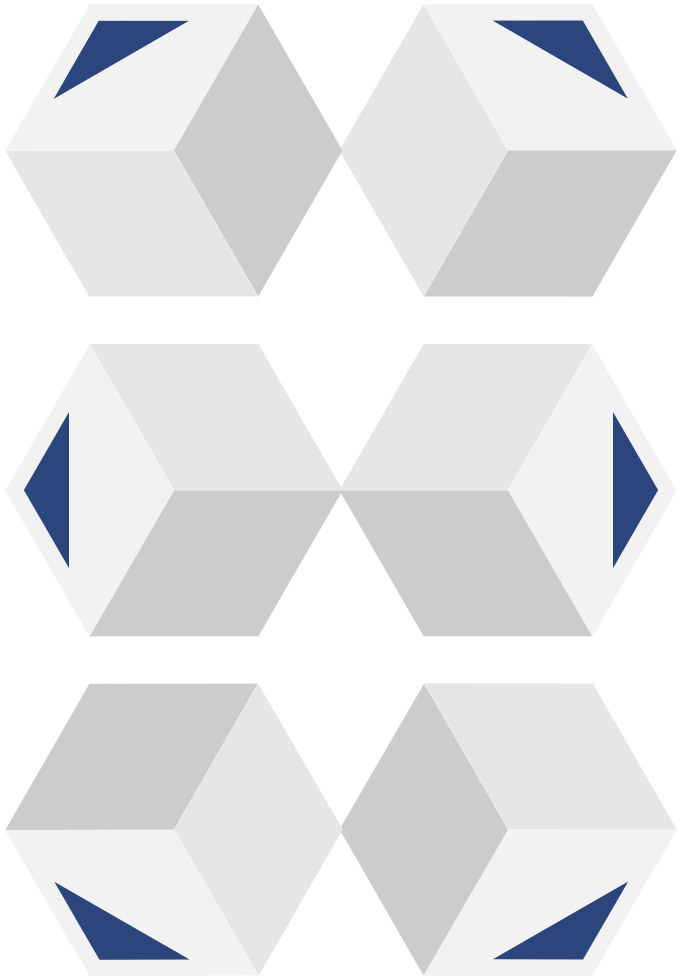
Osoby niemające dostępu do danych osobowych / osoby niemerytoryczne

Rodzaje szkoleń

Szkolenia onboardingowe – ogólne

Szkolenia cykliczne – ogólne

Szkolenia związane z aktualizacją przepisów – ogólne

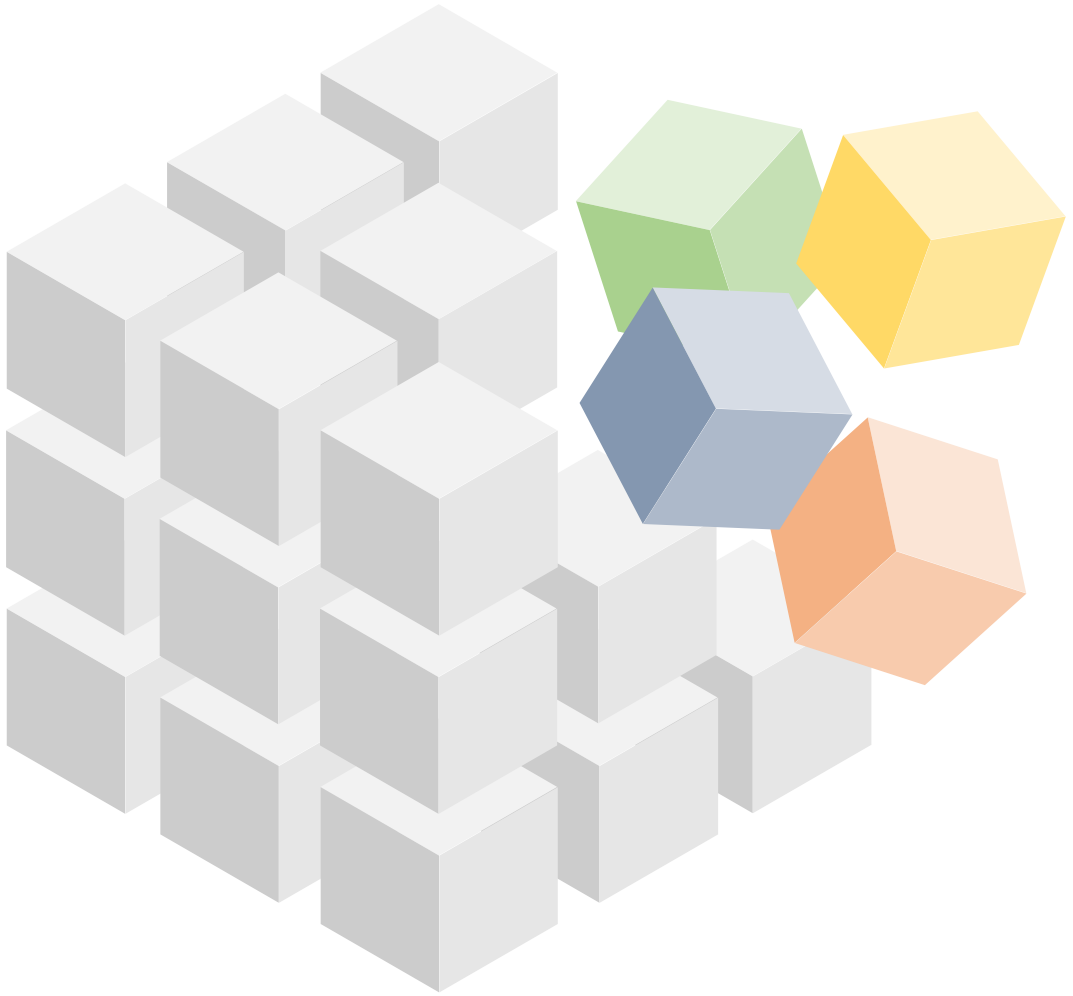


Szkolenia po naruszeniach

Szkolenia warsztatowe (sektorowe) – dedykowane (np. dla działu marketingu / sprzedaży)

Inne…?

Przyczyny szkoleń



- Występowanie dużej liczby incydentów spowodowanych np. błędami pracowników
- Zmiana charakteru pracy pracownika lub rozszerzenie zakresu jego działań
- Istotna zmiana przepisów / stanowiska organów wpływające na działanie organizacji
- Zmiana polityk wewnętrznych lub struktury organizacyjnej firmy

Forma szkolenia – jaka jest skuteczność?

Szkolenie stacjonarne

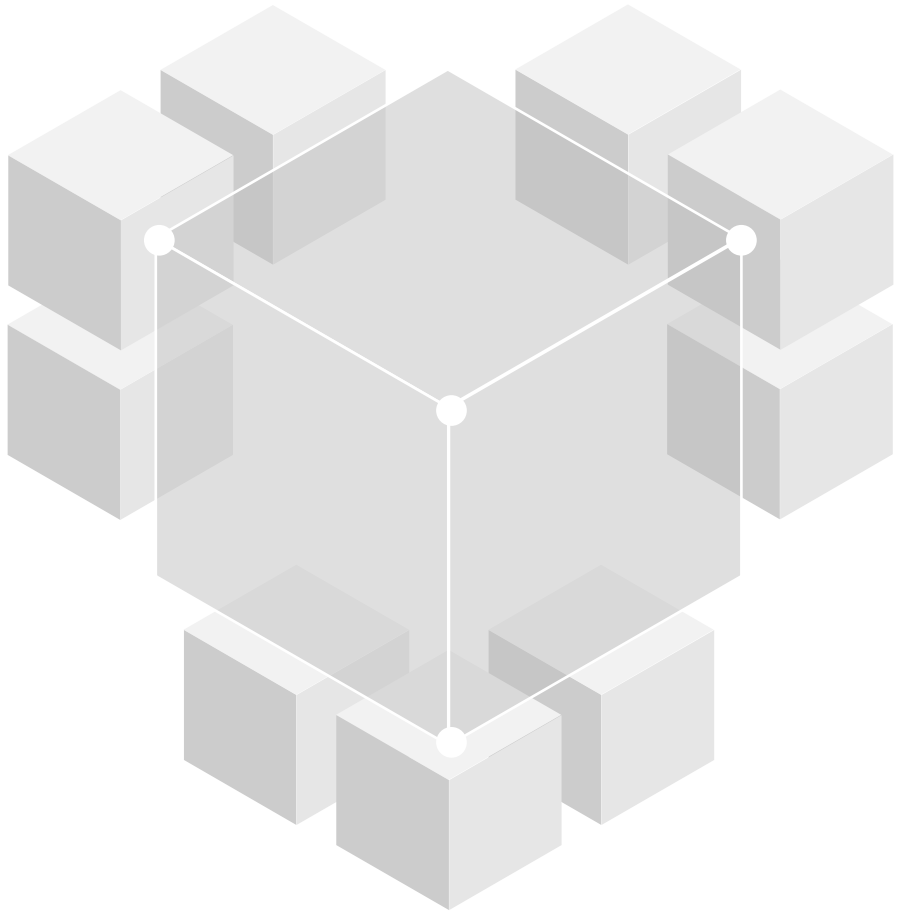
E-learning, kurs

Szkolenie zdalne

Forma hybrydowa:
e-learning połączony
z wykładami

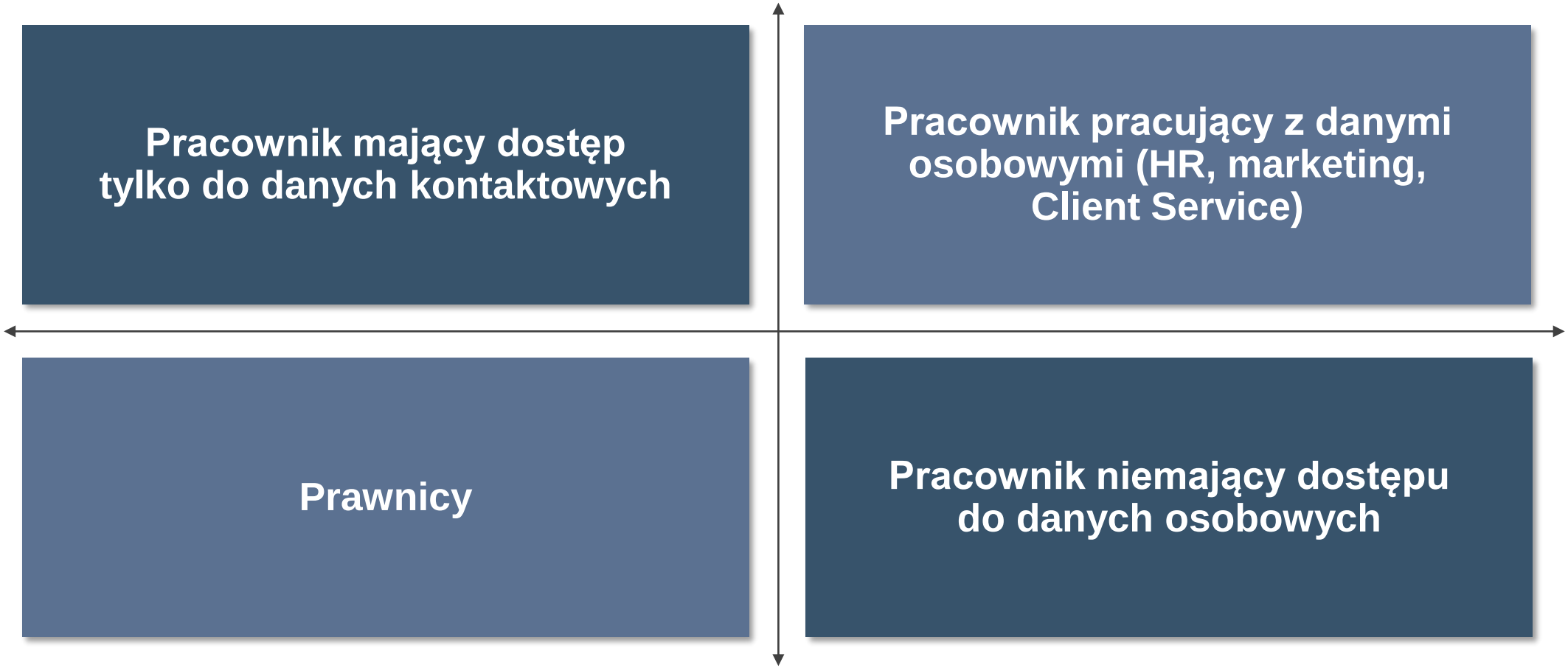
Weryfikacja wiedzy

Aby zapewnić efektywność szkoleń:



- Sprawdzenie wiedzy – test, pytania otwarte, karty pracy, quiz
- Seria pytań i odpowiedzi
- Udostępnienie materiałów szkoleniowych uczestnikom

Różnice w zakresie szkoleń



Zakres przedmiotowy szkolenia ogólnego:

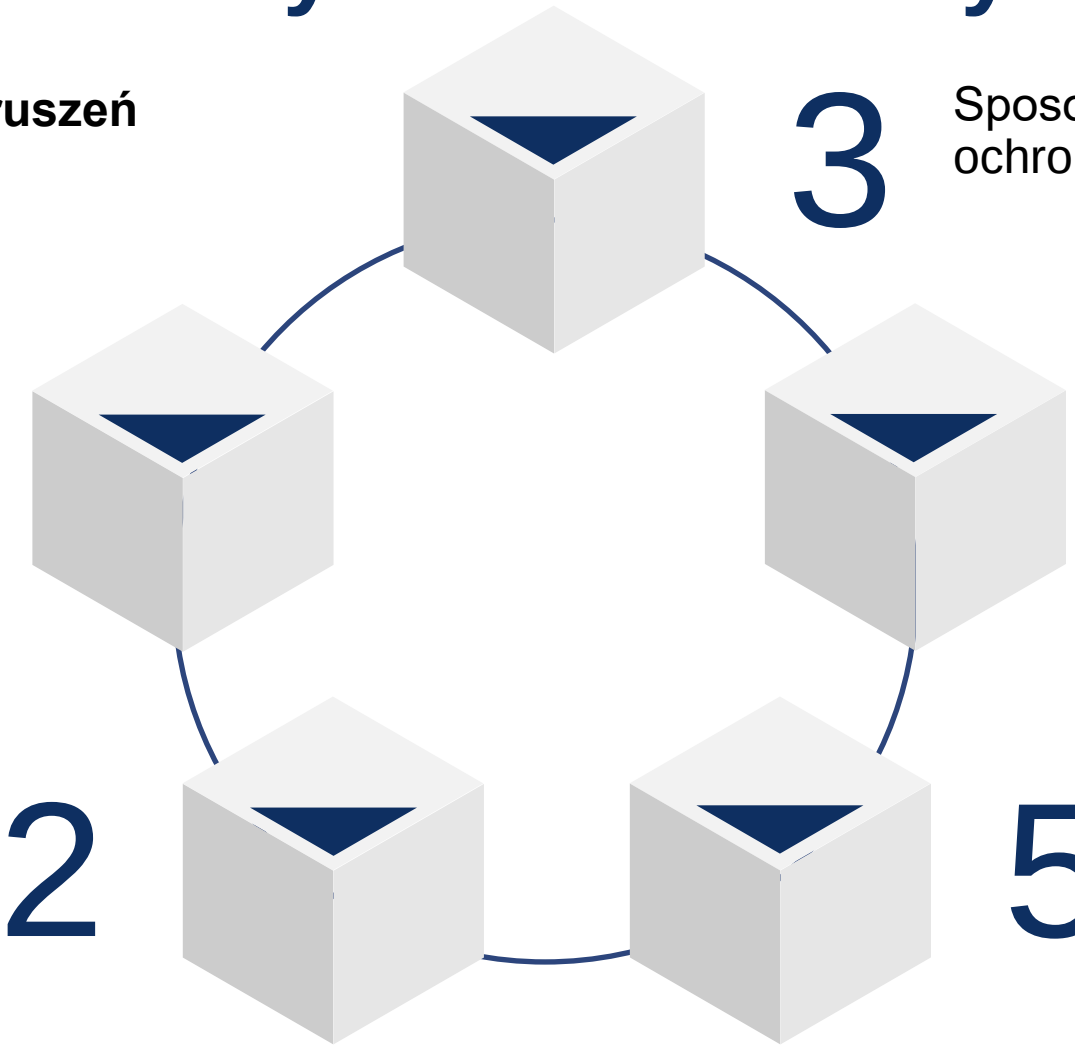
- Najważniejsze pojęcia RODO
- Zasady przetwarzania danych osobowych
- Zadania, odpowiedzialność i pozycja ADO i IOD / KODO (podział kompetencji)
- Dokumentacja ochrony danych osobowych w organizacji – oczekiwania względem personelu
- Naruszenia ochrony danych
- Prawa osób, których dane dotyczą
- Wybór dostawców/ umowy powierzenia
- Analiza ryzyka
- Retencja danych osobowych

Zakres przedmiotowy szkolenia tematycznego (np. HR)

- Przypomnienie podstaw RODO ze szkolenia podstawowego
- Zasady RODO w rekrutacji
- Współpraca z agencjami zatrudnienia / pracy tymczasowej
- Onboarding pracownika (w tym upoważnienia do przetwarzania DO)
- ZFŚS i medycyna pracy
- Benefity pracownicze
- Monitoring i wizerunek pracownika
- Badanie trzeźwości
- Okres przechowywania dokumentacji pracowniczej

Zakres przedmiotowy szkolenia incydentalnego

(np. po zidentyfikowaniu naruszeń dot. błędnej wysyłki maili)



1 Przypomnienie podstaw RODO związanych z tematyką naruszeń

2 Przypomnienie wewnętrznych zasad bezpieczeństwa (np. polityka IT)

3 Sposoby identyfikacji naruszeń ochrony danych osobowych

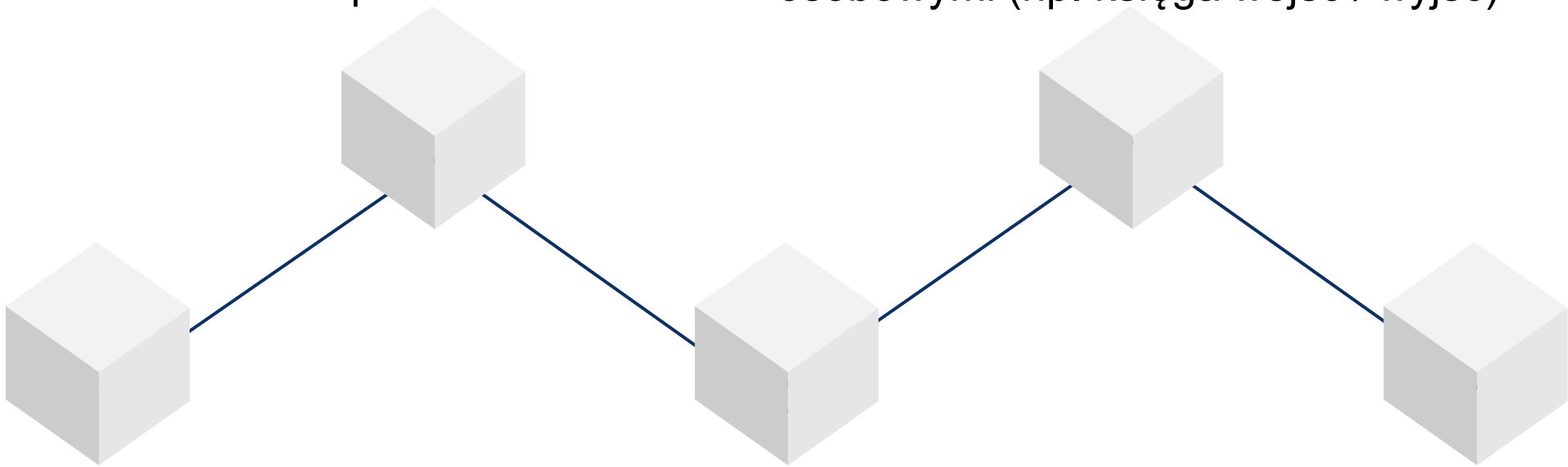
4 Zasady postępowania w razie wystąpienia incydentu – do kogo, kiedy i w jaki sposób się zwrócić?

5 Omówienie wdrożonych dodatkowych środków zabezpieczających

Zakres przedmiotowy szkolenia dla osób niemerytorycznych (np. pracownicy ochrony)

Zasady bezpieczeństwa i poufności

Zasady postępowania z danymi osobowymi (np. księga wejść / wyjść)



Wprowadzenie do podstaw RODO

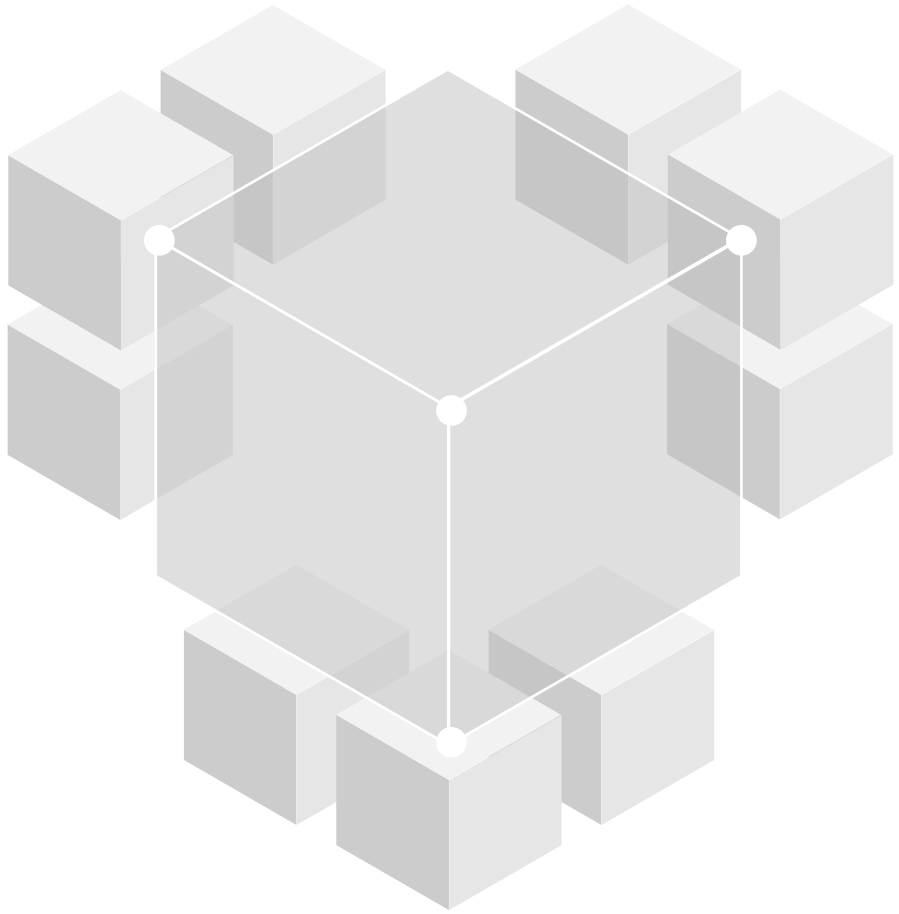
Stosowane środki zabezpieczające

Zasady postępowania w razie wystąpienia incydentu

GRC LEGAL

Weryfikacja wiedzy

Aby zapewnić efektywność szkoleń:



- Sprawdzenie wiedzy – test, pytania otwarte, karty pracy, quiz
- Seria pytań i odpowiedzi
- Udostępnienie materiałów szkoleniowych uczestnikom

Częstotliwość przeprowadzania szkoleń

Szkolenia podstawowe:

- Szkolenia onboardingowe – przed dopuszczeniem do pracy (nowi pracownicy i współpracownicy / osoby niemerytoryczne)
- Szkolenia przypominające – raz na rok (wszyscy)

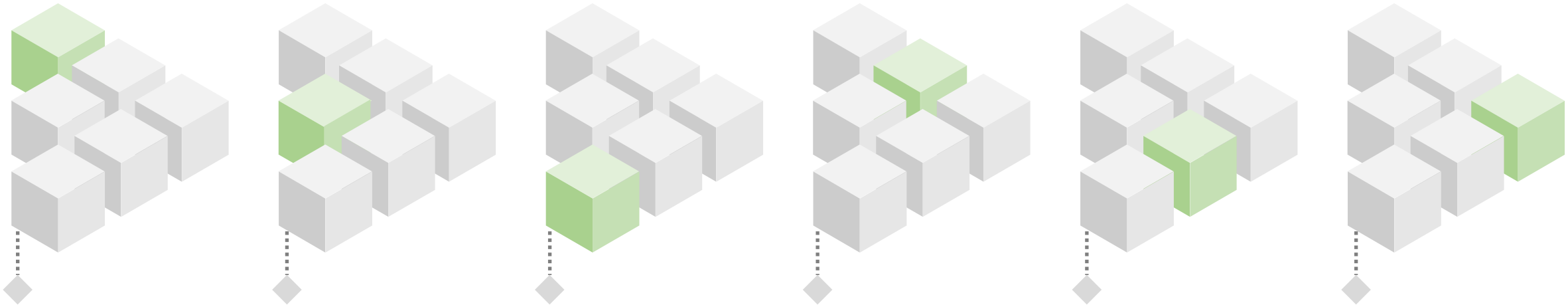
Szkolenia tematyczne (obszarowe):

- Pierwsze + przypominające
- Każdorazowo przy zmianie przepisów (m.in. HR, marketing);
- Każdorazowo przy zmianie kadrowej / personalnej;

Szkolenia incydentalne

- po wystąpieniu naruszenia (średnie / wysokie ryzyko);
- po zidentyfikowaniu wielu naruszeń o podobnym charakterze (niskie ryzyko)
- po zakończeniu zmian organizacyjnych (np. wdrożeniu nowych dokumentów).

Rozliczalność – procedura szkoleniowa



Plan uwzględniający typy szkoleń

Częstotliwość szkoleń

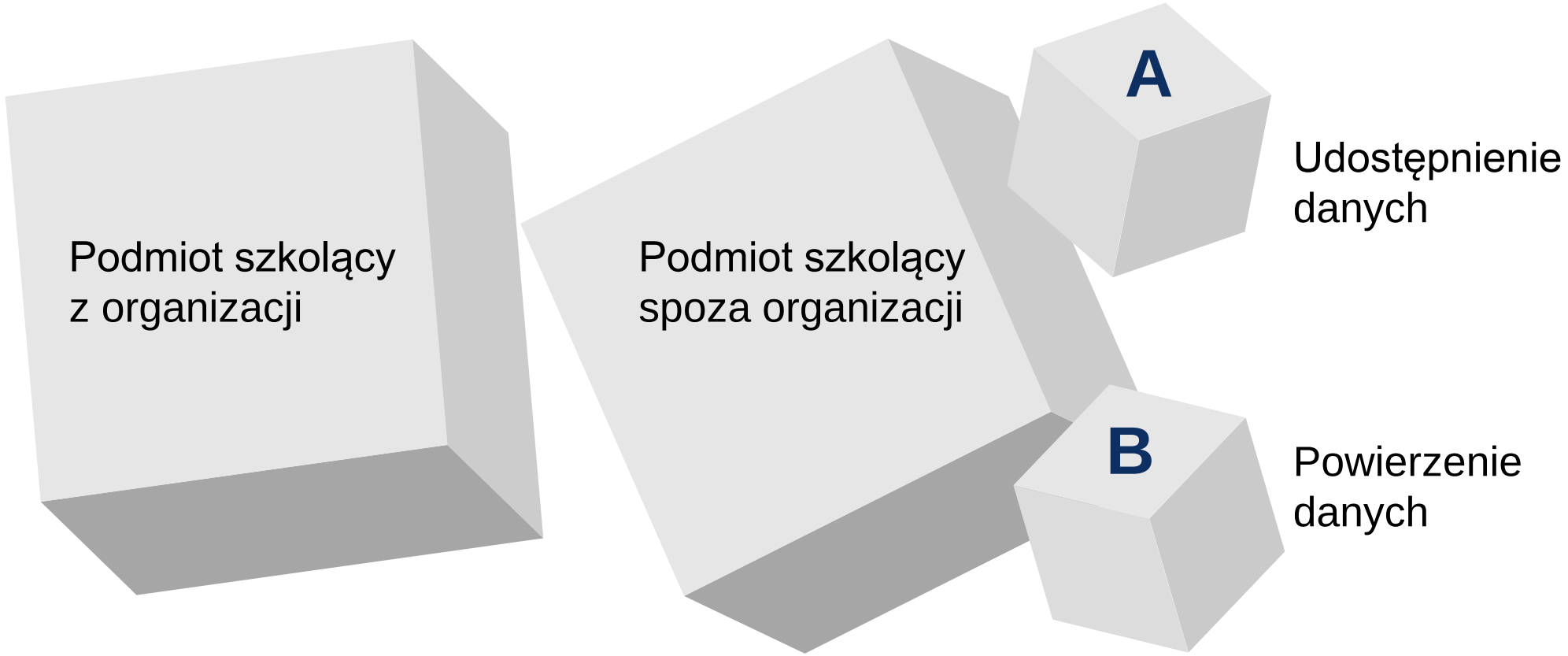
Sposób potwierdzenia odbycia szkolenia (podpisy uczestników, notatka IOD, automatycznie wygenerowana lista)

Zakres szkolenia (np. prezentacje)

Materiały archiwalne (materiały udostępniane po szkoleniu)

Dodatkowe materiały informacyjne

Relacje z podmiotami szkolącymi



Powierzenie czy udostępnienie:

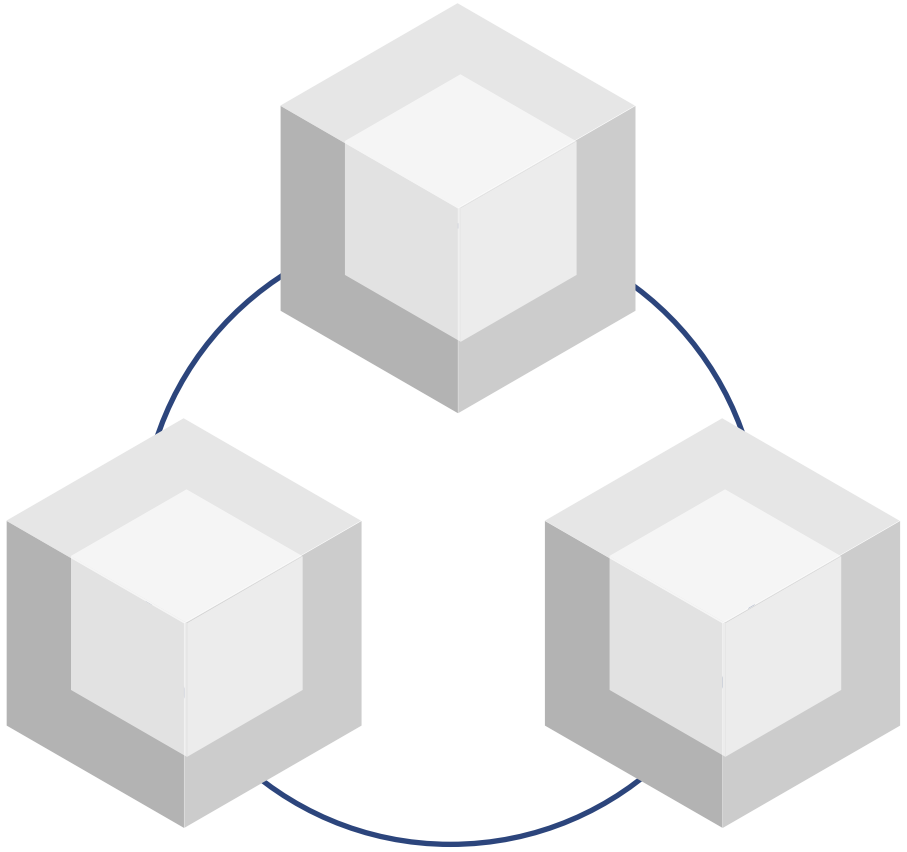
Powierzenie

- podmiot przetwarzający (procesor)
- Umowa powierzenia + obowiązek weryfikacji (art. 28 RODO)
- Kontrola administratora nad przekazanymi danymi
- Przykład: firma specjalizująca się w ochronie danych osobowych

Udostępnienie

- Inny administrator
- Przesłanka legalizująca z art. 6 ust. 1 lub art. 9 ust. 2 ROD
- Podmiot kontrolujący, zarządzający procesem przetwarzania
- Przykład: firma szkoląca z zakresu BHP (listy obecności)

Szkolenie i co dalej?



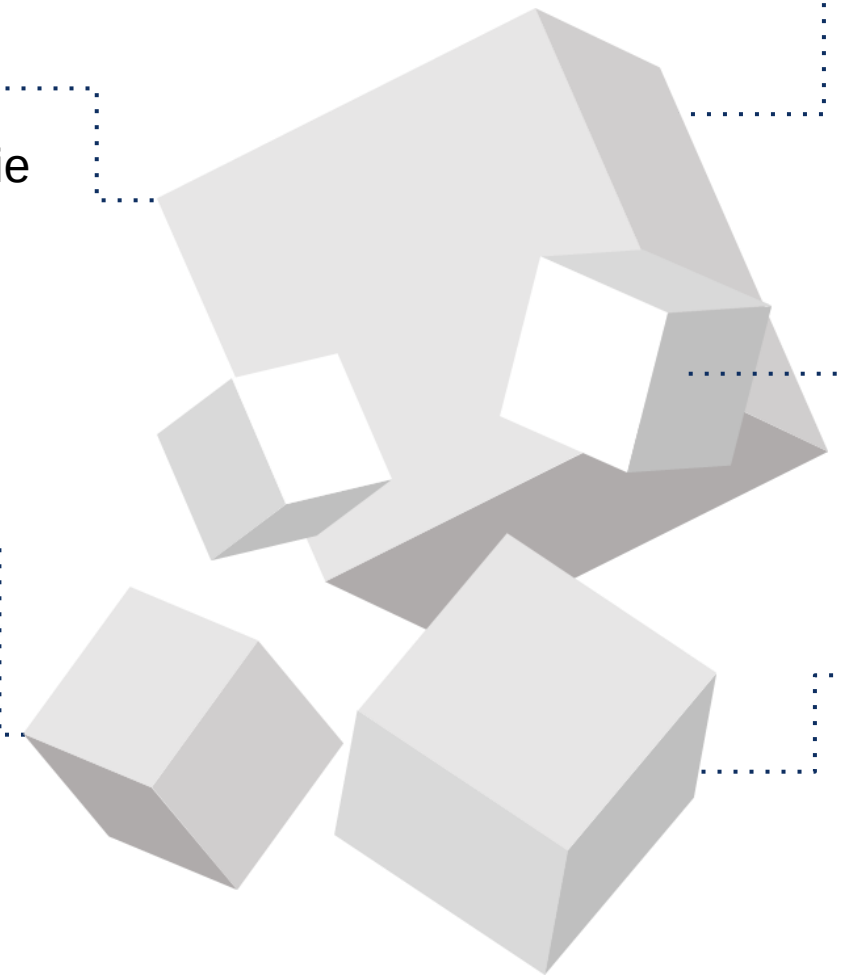
- Nadanie upoważnienia i odebranie oświadczenia o zobowiązaniu do zachowania poufności
- Weryfikacja wiedzy
- Audyt przeprowadzania szkoleń

Szkolenia „po-naruszeniowe”

Weryfikacja wiedzy pracownika objętego szkoleniem

Czy przeprowadzenie szkolenia jest wymagane?

Szkolenie jako środek służący zminimalizowaniu ryzyka ponownego wystąpienia naruszenia wskazany w Rejestrze Naruszeń lub Zawiadomieniu do Prezesa UODO



Jaki powinien być zakres szkolenia?

Przeprowadzenie komunikacji związanej z naruszeniem co do działu objętego incydentem lub do całej spółki

Czy w opinii PUODO zawsze będzie to wystarczający środek zaradczy?

GRC LEGAL

Szkolenia w decyzjach PUODO

„Mając na uwadze powyższe oraz treść art. 24 ust. 1 i art. 32 ust. 1 i 2 rozporządzenia 2016/679, obligujących administratora do wdrożenia odpowiednich środków organizacyjnych i technicznych, Prezes UODO w zawiadomieniu o wszczęciu postępowania administracyjnego stwierdził, że administrator nie wypełnił tego obowiązku należycie **poprzez niedostosowanie formy szkoleń do specyfiki pracy pracowników naukowych oraz zapewnienie wystarczającej rozliczalności w zakresie przeprowadzanych dla pracowników szkoleń**, co niewątpliwie ma wpływ na system bezpieczeństwa i ochrony danych osobowych w organizacji”.

Decyzja PUODO z dnia 21 sierpnia 2020 r., sygn. ZSOŚS.421.25.2019 – kara na SGGW

Szkolenia w decyzjach PUODO

„Ponadto, zgodnie z treścią art. 39 ust. 1 rozporządzenia 2016/679, monitorowanie przestrzegania przepisów, w tym **działania mające na celu zwiększanie świadomości w zakresie ochrony danych osobowych oraz szkolenie pracowników biorących udział w operacjach przetwarzania danych** należy do zadań inspektora ochrony danych, który realizuje je z uwzględnieniem ryzyka dla praw i wolności osób fizycznych.”

Decyzja PUODO z dnia 21 sierpnia 2020 r., sygn. ZSOŚS.421.25.2019 – kara na SGGW

Szkolenia w decyzjach PUODO

„**Prawidłowo przeprowadzone szkolenia pozwolą osobom szkolonym na właściwe zrozumienie zasad przetwarzania danych osobowych określonych przez Administratora, a w konsekwencji przyczyniają się do ograniczenia ryzyka wystąpienia naruszeń w tym obszarze**. Podnieść również należy, że przeprowadzanie szkoleń z zakresu ochrony danych osobowych, aby mogło zostać uznane za adekwatny środek bezpieczeństwa, **musi być realizowane w sposób cykliczny**, co zapewni stałe przypominanie, a w konsekwencji utrwalenie, zasad przetwarzania danych osobowych objętych szkoleniem. Ponadto, w takich szkoleniach **muszą brać udział wszystkie osoby upoważnione do przetwarzania danych osobowych**, a samo szkolenie **musi obejmować swoim programem wszystkie zagadnienia związane z przetwarzaniem danych osobowych w ramach ustalonego tematu szkolenia**.

Decyzja PUODO z dnia 20 kwietnia 2023, sygn. DKN.5131.31.2022
Decyzja PUODO z dnia 21 lipca 2022 r. sygn. DKN.5131.2.2022
Decyzja PUODO z dnia 19 stycznia 2023 r. sygn. DKN.5131.12.2020

Szkolenia w decyzjach PUODO

Pominięcie któregoś z tych elementów spowoduje, że szkolenie nie spełni swojej roli, bowiem część osób nie zostanie w ogóle przeszkolona albo uczestnicy szkolenia nie otrzymają pełnej wiedzy w danym zakresie. Konsekwencją powyższego może być naruszenie ochrony danych osobowych, tak jak w sprawie będącej przedmiotem niniejszego postępowania. Co więcej, brak przeprowadzania szkoleń w opisany wyżej sposób oznacza, że ten środek bezpieczeństwa w praktyce nie obniża ryzyka wystąpienia naruszeń ochrony danych osobowych, co niewątpliwie przyczynia się do osłabienia poziomu ochrony danych osobowych i przesądza o konieczności uznania naruszenia przepisów rozporządzenia 2016/679 odnoszących do obowiązków administratora w zakresie bezpieczeństwa danych.”

Decyzja PUODO z dnia 20 kwietnia 2023, sygn. DKN.5131.31.2022
Decyzja PUODO z dnia 21 lipca 2022 r. sygn. DKN.5131.2.2022
Decyzja PUODO z dnia 19 stycznia 2023 r. sygn. DKN.5131.12.2020

Obowiązki administratorów związane z naruszeniami ochrony danych osobowych

„**Naruszenia polegające na nieprawidłowej wysyłce dokumentów oraz anonimizacji danych osobowych w związku z udostępnianiem informacji publicznej**.

W przypadku podmiotów sektora publicznego, oprócz omyłkowego wysyłania dokumentacji do innego odbiorcy, zdarzają się również sytuacje nieprawidłowej anonimizacji danych. Sytuacje te występowały w przypadku udostępniania danych w trybie dostępu do informacji publicznej, w tym w Biuletynie Informacji Publicznej. Remedium na taki stan rzeczy powinny być **regularne szkolenia pracowników** z zakresu ochrony danych, w tym bezpieczeństwa danych, wprowadzenie szczegółowych instrukcji postępowania z dokumentami zawierającymi dane osobowe, w tym sposobów anonimizacji danych oraz wzmocnienie kontroli nad procesem wysyłki korespondencji (tradycyjnej i e-mail).” s.22

„**Czy RODO wymaga podjęcia innych kroków w związku z naruszeniem**?

Podobnie jak w przypadku każdego incydentu związanego z bezpieczeństwem, administrator powinien ustalić, czy naruszenie było wynikiem błędu ludzkiego lub problemu systemowego i zobaczyć w jaki sposób można zapobiec powtórce incydentu - czy to poprzez lepsze procesy, **dalsze szkolenia** lub inne kroki naprawcze.” s.31

https://archiwum.uodo.gov.pl/pl/134/1029

Inne działania uświadamiające

A

Onepagery

B

Newsletter IOD

C

Komunikacja informacyjna (np. mailowo)

GRC
LEGAL

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