

# Trybunał kontra EIOD

## Wyrok w sprawie pseudonimizacji

### W TYM WYDANIU:

TSUE z ważnym wyrokiem ws. pseudonimizacji

1

- Stanowisko TSUE i jego znaczenie

2

- Trybunał zakwestionował stanowisko EIOD — wnioski

3

Zarządzanie ryzykiem – wyjaśniamy cały proces

4

- Wymagania normatywne

5

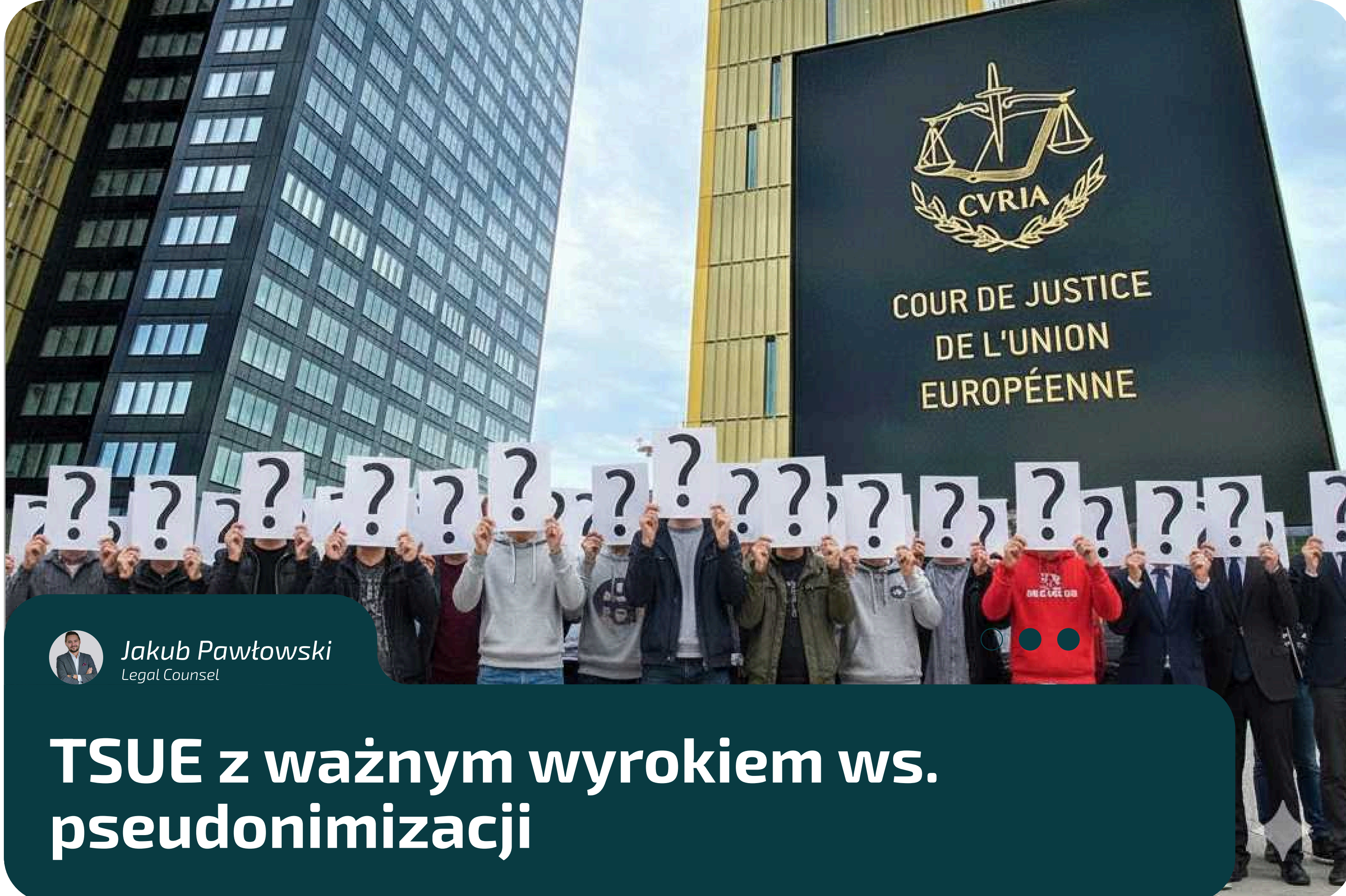
- Kontrola ryzyka - etapy

6

- Metody szacowania ryzyka

10





Jakub Pawłowski  
Legal Counsel

## TSUE z ważnym wyrokiem ws. pseudonimizacji

W jednym z ostatnich artykułów opisywałem zawisłą przed Trybunałem Sprawiedliwości Unii Europejskiej (TSUE) sprawę pod sygnaturą C-413/23 dotyczącą pojęcia pseudonimizacji i anonimizacji danych osobowych. Wówczas można było jedynie spodziewać się rozstrzygnięcia w oparciu motywy wskazane w opinii Rzecznika Generalnego. Teraz mamy już do czynienia z **ostatecznym rozstrzygnięciem**, które znacząco zmienia postrzeganie pseudonimizacji i anonimizacji danych osobowych.

### Czego dotyczyło postępowanie?

Sprawa dotyczyła przetwarzania danych osobowych akcjonariuszy i wierzycieli hiszpańskiego banku, który przeszedł proces restrukturyzacji i uporządkowanej likwidacji. W ramach tego procesu konieczne było oszacowanie, czy akcjonariusze i wierzyciele otrzymaliby lepsze traktowanie w przypadku standardowej procedury niewypłacalności. Do tego celu organ UE, a konkretnie **Jednolita Rada ds. Restrukturyzacji i Uporządkowanej Likwidacji (SRB)**, przekazała dane osobowe firmie audytorskiej, która miała przeprowadzić odpowiednią wycenę.

Głównym punktem sporu było to, czy SRB dopełniła obowiązku informacyjnego wynikającego z rozporządzenia (UE) 2018/1725 względem tych akcjonariuszy i wierzycieli. Europejski Inspektor Ochrony Danych (EIOD), zgodnie z dotychczas mocno ugruntowanym poglądem argumentował, że nawet jeśli dane zostały poddane pseudonimizacji, to nadal podlegają przepisom o ochronie danych osobowych. W związku z tym EIOD twierdził, że SRB miała obowiązek powiadomić osoby, których dane dotyczyły, o przekazaniu ich danych firmie audytorskiej.







**TSUE musiał rozstrzygnąć, czy dane, które są spseudonimizowane dla podmiotu A mogą stracić swój osobowy charakter po przekazaniu ich do podmiotu B. Innymi słowy, problem dotyczył tego, pod jakimi warunkami dane te będą uznawane za dane osobowe lub nieosobowe z perspektywy podmiotu B.**

## Stanowisko TSUE i jego znaczenie

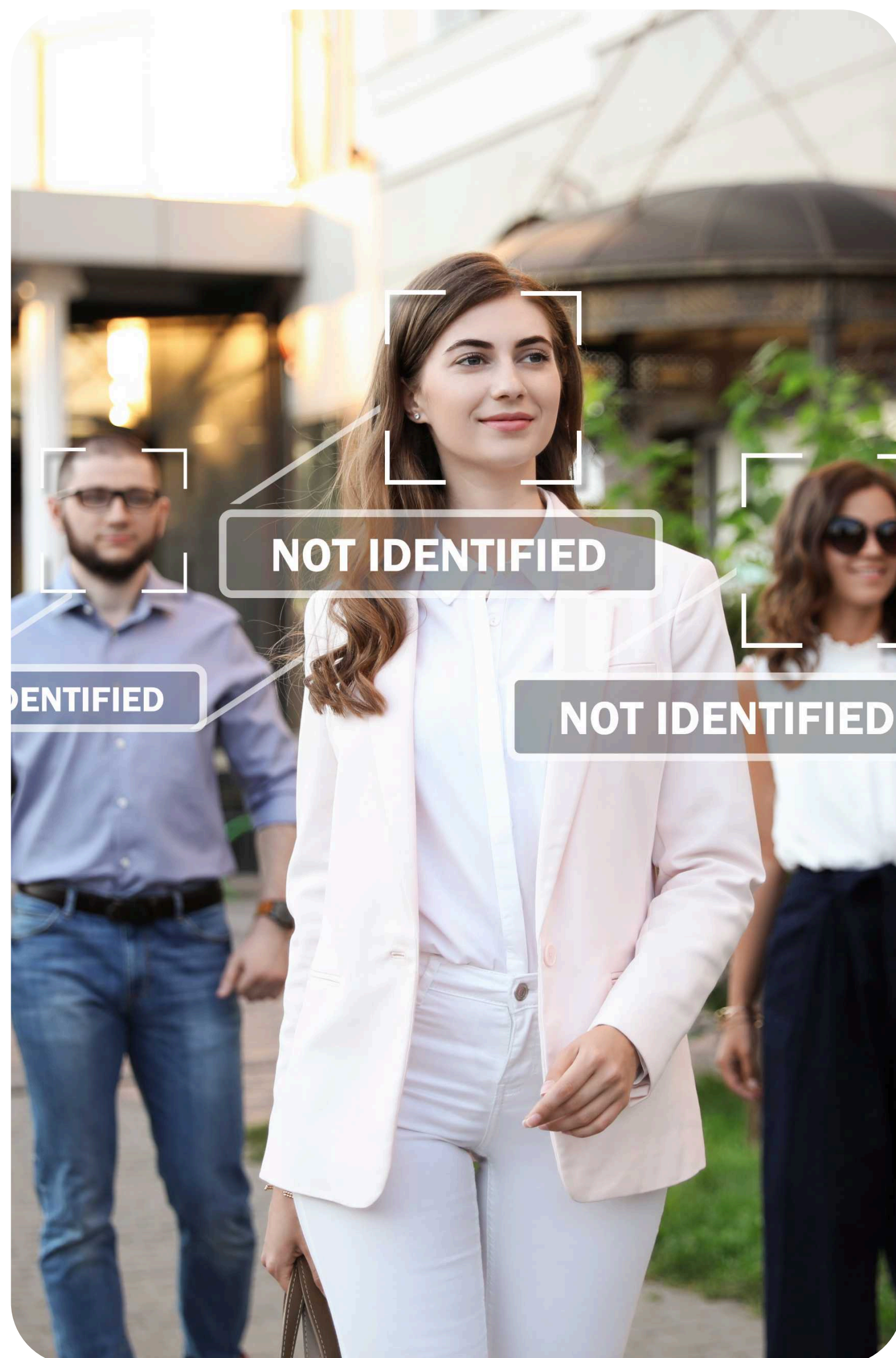
Punktem wyjścia rozważań TSUE było uwaga, że zgodnie z samym brzmieniem art. 3 pkt 1 rozporządzenia 2018/1725, aby informacja mogła zostać zakwalifikowana jako dane osobowe w rozumieniu tego przepisu, musi ona być o „zidentyfikowanej lub możliwej do zidentyfikowania” osobie fizycznej. W związku z tym stosowanie tego rozporządzenia zasadniczo zakłada badanie zidentyfikowanego lub możliwego do zidentyfikowania charakteru osoby, której dotyczą rozpatrywane informacje. Wykładnię tę potwierdzają zdania piąte i szóste motywu 16 rozporządzenia 2018/1725, zgodnie z którymi definicja pojęcia „danych osobowych” nie obejmuje „informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub z możliwą do zidentyfikowania osobą fizyczną”, ani „danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować”.

W dalszej kolejności Trybunał zauważył, że **dane spseudonimizowane nie są wymienione w prawnej definicji pojęcia „danych osobowych”** zawartej w art. 3 pkt 1 rozporządzenia 2018/1725, ale ich charakterystyka wynika z art. 3 pkt 6 tego rozporządzenia. Ten ostatni przepis definiuje pojęcie

„pseudonimizacji” jako „przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej”.

Trybunał wskazał (w ślad za opinią Rzecznika Generalnego), że pseudonimizacja nie stanowi zatem elementu definicji „danych osobowych”, lecz odnosi się do wprowadzenia środków technicznych i organizacyjnych mających na celu zmniejszenie ryzyka powiązania zbioru danych z tożsamością osób, których dane dotyczą.

Zgodnie z motywem 17 wspomnianego rozporządzenia pseudonimizacja „może [tylko] ograniczyć ryzyko dla osób, których dane dotyczą, oraz pomóc administratorom i podmiotom przetwarzającym wywiązać się z obowiązku ochrony danych”.





Ponadto, Trybunał wskazał, że:

1

Z art. 3 pkt 6 rozporządzenia 2018/1725 wynika, że pojęcie „pseudonimizacji” zakłada istnienie informacji pozwalających na zidentyfikowanie osoby, której dane dotyczą. Tymczasem samo istnienie takich informacji stoi na przeszkodzie temu, by dane, które były przedmiotem pseudonimizacji, mogły w każdym wypadku zostać uznane za dane anonimowe, wyłączone z zakresu stosowania tego rozporządzenia.

2

Przewidziany w art. 3 pkt 6 tego rozporządzenia wymóg osobnego przechowywania danych identyfikacyjnych oraz środków technicznych i organizacyjnych uniemożliwiający ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej wskazuje, że pseudonimizacja ma w szczególności na celu uniknięcie sytuacji, w której osoba, której dane dotyczą, mogłaby zostać zidentyfikowana za pomocą samych tylko danych spseudonimizowanych.

3

O ile bowiem takie środki techniczne i organizacyjne są rzeczywiście wprowadzone i mogą zapobiec przypisaniu rozpatrywanych danych osobie, której dane dotyczą, w taki sposób że osoby tej w ogóle nie można zidentyfikować lub już nie można zidentyfikować, o tyle pseudonimizacja może mieć wpływ na osobowy charakter tych danych w rozumieniu art. 3 pkt rozporządzenia 2018/1725.

## Trybunał zakwestionował stanowisko EIOD

Przenosząc powyższe rozważania na przypadek SRB i firmy audytorskiej Trybunał doszedł do wniosku, że

zastosowane przez SRB środki techniczne i organizacyjne (o których mowa w art. 3 pkt 6 rozporządzenia 2018/1725) mogły skutkować tym, że dla tej firmy audytorskiej dane **nie mają** charakteru danych osobowych.

Założeniem takiego wniosku było to, że firma audytorska nie była w stanie znieść tych środków podczas dokonywanego pod jej kontrolą przetwarzania tych danych. Ponadto, jak wskazał TSUE, wspomniane środki muszą w rzeczywistości mieć taki charakter, aby uniemożliwić przypisanie tych danych osobie, której dane dotyczą, również poprzez odwołanie się do innych środków identyfikacji, takich jak porównanie z innymi danymi, w taki sposób, że w ogóle nie można ich zidentyfikować lub już nie można zidentyfikować osoby, której dane dotyczą.

**Trybunał zakwestionował zatem stanowisko EIOD i to w sposób zasadniczy.** Jak bowiem podkreślił TSUE, wbrew temu, co twierdzi EIOD, nie można uznać, by dane spseudonimizowane stanowiły, w każdym wypadku i w odniesieniu do każdej osoby, dane osobowe do celów stosowania rozporządzenia 2018/1725, ponieważ pseudonimizacja może – w zależności od okoliczności danej sprawy – rzeczywiście uniemożliwić osobom innym niż administrator zidentyfikowanie osoby, której dane dotyczą, w taki sposób, że dla tych osób nie jest ona w ogóle możliwa do zidentyfikowania lub już możliwa do zidentyfikowania.

## Jakie wnioski płyną z tego wyroku dla praktyki?

Odpowiednio zaprojektowana i wdrożona pseudonimizacja danych osobowych może pozwolić na bardziej swobodny przepływ danych, pod warunkiem, że administrator i podmiot trzeci będący odbiorcą spseudonimizowanych (z punktu widzenia administratora danych) zagwarantują, że podmiot trzeci nie będzie w żadnym wypadku dysponował danymi lub środkami pozwalającymi na przypisanie tych danych osobie, której dane dotyczą.





**Olga Ograbisz**  
Information Security&Data Protection Expert

# Zarządzanie ryzykiem – wyjaśniamy cały proces!

Czym jest zarządzanie ryzykiem? Odpowiedź wydaje się oczywista, ale diabeł tkwi w szczegółach. Prawidłowe zrozumienie tego procesu pozwoli Ci uniknąć strat finansowych, poprawić bezpieczeństwo firmy i mieć pewność, że Twoja firma nie poniesie kar administracyjnych.

## Zarządzanie ryzykiem w bezpieczeństwie informacji

W pierwszej kolejności wyjaśnijmy pojęcia – minimalizacja ryzyka to jeden z kluczowych elementów Systemu Zarządzania Bezpieczeństwem Informacji (w skrócie SZBI) według międzynarodowego standardu ISO 27001.

### System bezpieczeństwa informacji zbudowany jest z:



polityk



procedur



wytycznych



zasobów (kadrowych, finansowych, technicznych)

oraz działań, które wspólnie zarządzane przyczyniają się do zapewnienia wysokiego poziomu ochrony aktywów informacyjnych organizacji. Wyznacznikiem skuteczności bezpieczeństwa informacji jest zasada **podejścia opartego na ryzyku**.

Szacowanie ryzyka powinno być podstawą do wyboru zabezpieczeń, adekwatnych do podatności danego zasobu i całego kontekstu organizacji.





Zabezpieczenia te powinny być następnie odzwierciedlone w tzw. Deklaracji stosowania zabezpieczeń zbudowanej zgodnie ze schematem Załącznika A do normy PN-EN ISO/IEC 27001:2023. Zarządzanie ryzykiem jako proces ciągły pozwala na racjonalne podejmowanie decyzji związanych z zapewnieniem bezpieczeństwa informacji i efektywną alokację środków, którymi dysponuje w danym momencie organizacja.

## Wymagania normatywne

Ocena ryzyka w bezpieczeństwie informacji to proces **identyfikowania, rozwiązywania i zapobiegania problemom bezpieczeństwa**. Ocena często opiera się na aktywach, a ryzyko ocenia się w odniesieniu do posiadanych zasobów informacyjnych. Ocena prowadzona jest w całej organizacji. Co więcej, ISO 27001 wyraźnie wymaga, aby proces zarządzania ryzykiem był stosowany do przeglądu i potwierdzania kontroli bezpieczeństwa w świetle obowiązków prawnych i umownych.



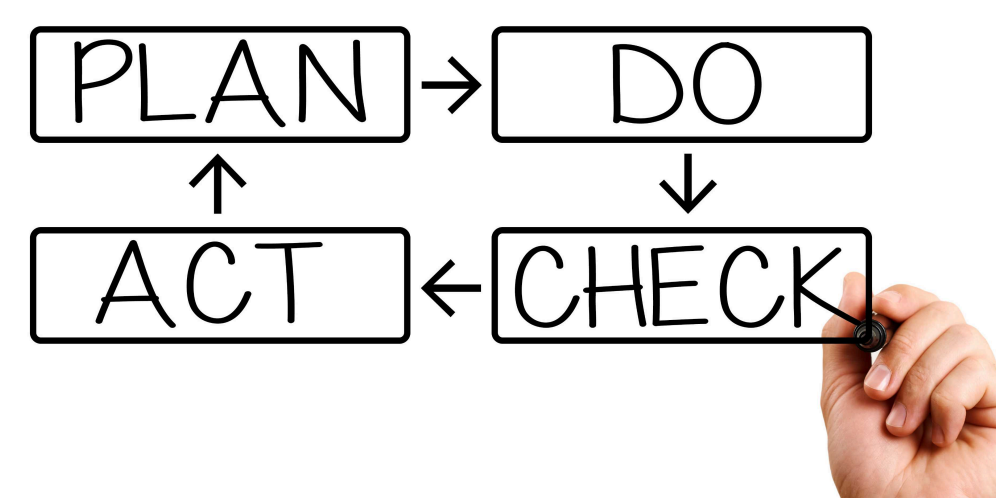
Wymagania w zakresie zarządzania ryzykiem wprowadzają rozdziały 6 i 8 oraz pośrednio 9.3.1.2 PN-EN ISO/IEC 27001:2023 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – System zarządzania bezpieczeństwem informacji. Ww. punkty nie tylko wskazują na potrzebę identyfikowania ryzyka, ale co ważniejsze na postępowanie z ryzykiem, czyli na działania, jakie organizacja podejmuje wobec zdefiniowanych ryzyk czy też szans.

## Zarządzanie ryzykiem w bezpieczeństwie informacji

Ryzyko przez normy z serii ISO definiowane jest jako wpływ niepewności na cele, przy czym następstwem niepewności jest odchylenie od oczekiwań (zarówno pozytywne, jak i negatywne). Rozwijając powyższe – **pod pojęciem ryzyka rozumie się prawdopodobieństwo wystąpienia zdarzenia, które będzie miało określony wpływ (skutki) na realizację założonych celów**. Rolą podejścia opartego na ryzyku jest dostarczenie informacji o potencjalnych zdarzeniach, które mogą oddziaływać na organizację, jej proces czy też zasób, i podejmowanie na tej podstawie działań jeszcze przed zmaterializowaniem się ryzyka. Daje to organizacji rozsądny poziom pewności, pozwalający na skuteczniejsze zarządzanie danym obszarem działalności, co przekłada się na finanse organizacji, osiągnięte cele czy zachowanie bezpieczeństwa aktywów informacyjnych.

**Żaden ze standardów ISO nie mówi wprost, w jaki sposób zarządzanie ryzykiem ma się odbywać, w jaki sposób je identyfikować i mierzyć. Metody szacowania ryzyka i postępowania z ryzykiem powinny być dostosowane do poszczególnych czynników charakteryzujących organizację (czyli „szyte na miarę”), a ich wybór powinien uwzględniać estymację kosztów i korzyści, wymagania prawne czy ten inne priorytety i zmienne właściwe dla danej organizacji.**

Powinny one zapewniać również możliwość porównywania wyników w czasie. Zaleca się, aby proces zarządzania ryzykiem zgodny z ISO 27001 składał się z ośmiu elementów, które mogą odbywać się zgodnie z zasadą PDCA (Plan-Do-Check-Act).





## Etapy kontroli ryzyka

Zarządzanie ryzykiem bezpieczeństwa informacji to systemowe działanie polegające na szacowaniu ryzyka (identyfikowanie ryzyka, jego analiza i ocena) oraz podejmowaniu działań na podstawie stwierdzonego ryzyka w taki sposób, aby miało to

wartość dodaną dla realizacji celów biznesowych. Jego istotą jest także podejmowanie świadomych i odpowiedzialnych decyzji dotyczących ryzyk. Można je podzielić na 8 etapów:

### 1 Ustanowienie kontekstu

Ustanowienie kontekstu jest pierwszym etapem zarządzania ryzykiem. Jest to moment, w którym organizacja powinna określić i zrozumieć czynniki zewnętrzne i wewnętrzne wpływające na jej funkcjonowanie, cele oraz sposoby ich realizacji. **Na kontekst zewnętrzny składają się w szczególności czynniki kulturowe, społeczne, polityczne, ekonomiczne, technologiczne czy finansowe.** Są to także relacje, jakie łączą organizację ze wszystkim interesariuszami i ich oczekiwania. **Przez kontekst wewnętrzny natomiast rozumie się strukturę organizacyjną, strategię, misję, cele organizacji,**

**podział zadań, zasoby, kulturę organizacyjną czy kontrakty biznesowe.** Dokładne zdefiniowanie kontekstu, w jakim działa organizacja pozwala na kolejnych etapach ustalić kryteria oceny ryzyka i jego akceptacji oraz ocenić wpływ zagrożeń na organizację i jej cele.

Określenie zewnętrznych i wewnętrznych kwestii, które są istotne dla celu i które wpływają na zdolność do osiągnięcia zamierzonych wyników systemu zarządzania bezpieczeństwem informacji stanowi wymóg ISO 27001 wskazany w punkcie 4 "Kontekst organizacji".

### 2 Identyfikacja ryzyka

Identyfikacja ryzyka, czyli **proces wyszukiwania, rozpoznawania i opisywania ryzyka polega na określeniu przyczyn i sposobów materializacji niepożądanych zdarzeń.** Obejmuje on ustalenie zasobów (aktywów) informacyjnych, zagrożeń i źródeł ich powstawania. Na tym etapie identyfikuje

się również podatności oraz potencjalne skutki i straty związane z niepożądanymi zdarzeniami. Kluczem do sukcesu na tym etapie jest właściwe i bardzo dokładne zinventaryzowanie **aktywów**, czyli wszystkiego, co posiada dla organizacji wartość i jest nośnikiem informacji.

Najczęściej wyróżnia się następujące kategorie aktywów:

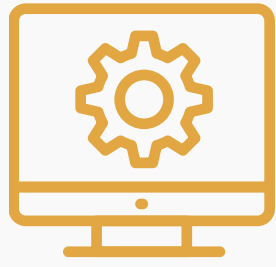


Informacyjne (dokumenty, bazy danych)



Fizyczne (sprzęt komputerowy, budynki, urządzenia komunikacyjne)





**Oprogramowanie (systemy operacyjne, aplikacje)**



**Personel (jego wiedza, doświadczenie i umiejętności)**



**Dobra niematerialne (reputacja, wizerunek)**

Kolejną rzeczą, na którą należy zwrócić uwagę, jest wskazanie dla każdego z aktywów **właściciela**, czyli osoby odpowiedzialnej za jego utrzymanie, korzystanie i bezpieczeństwo. Po określeniu aktywów i przypisaniu im właścicielstwa następuje moment identyfikowania potencjalnych zagrożeń, czyli

zdarzeń (losowych, umyślnych, nieumyślnych), które mogą oddziaływać na bezpieczeństwo aktywa. Dobrze jest także określić podatności aktywa, czyli inaczej mówiąc słabości lub luk w systemie przetwarzania informacji, które umożliwiają zmaterializowanie się danego zagrożenia.

### 3 Analiza ryzyka

Analiza ryzyka to proces dążący do poznania charakteru ryzyka oraz określenia jego poziomu.

Najczęściej sprowadza się on do określenia prawdopodobieństwa oraz skutków zaistnienia zidentyfikowanego ryzyka.

**Zaleca się, aby podczas oceny prawdopodobieństwa zaistnienia określonych zagrożeń rozważyć:**



**Źródło zagrożenia**



**Możliwości dostępne dla potencjalnych atakujących**



**Atrakcyjność i wrażliwość zasobów dla potencjalnych atakujących**



**Lokalizację**



**Możliwość wystąpienia ekstremalnych warunków atmosferycznych**



**Czynniki determinujące powstawanie błędów i pomyłek**

Przy ocenie skutków należy mieć na uwadze zarówno te **bezpośrednie** (koszty odtworzenia utraconych aktywów, konfiguracji, instalacji zasobu czy straty finansowe i wizerunkowe poniesione jako konsekwencja zawieszenia/braku dostępności usługi)

oraz **pośrednie** (naruszenie obowiązków umownych, ustawowych czy kodeksów postępowania). Na tym etapie dokonujemy również oszacowania wielkości ryzyka na podstawie kombinacji prawdopodobieństwa wystąpienia zagrożenia oraz jego skutków.



## 4 Ocena ryzyka

Ocena ryzyka to proces porównania wyników analizy ryzyka z kryteriami ryzyka. Te kryteria to poziomy odniesienia, względem których określa się wysokość

ryzyka. Etap dostarcza informacji, czy dane ryzyko jest dla organizacji akceptowalne. Pozwala on także na uszeregowanie ryzyk zgodnie z ich wartością oraz nadanie priorytetów postępowania z nimi.

## 5 Metody zarządzania ryzykiem

**Proces postępowania z ryzykiem, czyli jego modyfikacji za pomocą różnych strategii, w tym:**



### Redukcja ryzyka

obniżenie ryzyka do poziomu akceptowalnego dla organizacji poprzez dobór i zastosowanie odpowiednich (czy to technicznych, czy organizacyjnych) środków bezpieczeństwa dobranych adekwatnie do skali ryzyka oraz zasobów organizacji



### Unikanie

poprzez podjęcie działań zmierzających do zmodyfikowania lub całkowitego zaprzestania danej aktywności generującej ryzyko



### Przeniesienie

zlecenie czynności tworzącej ryzyko podmiotom zewnętrznym lub wykup polisy ubezpieczeniowej



### Utrzymanie

akceptacja ryzyka na stwierdzonym poziomie, poprzez podjęcie świadomej decyzji o niestosowaniu w danym momencie żadnych działań mających na celu redukcję ryzyka czy jego przeniesienie.

Bez względu na to, na którą z powyższych strategii zdecyduje się organizacja, powinna ona udokumentować swoje stanowisko w tzw. planie postępowania z ryzykiem, o którym mowa w punkcie

6.1.3 standardu ISO 27001. Plan powinien być zaakceptowany przez właściciela ryzyka i weryfikowany w trakcie i po jego zakończeniu w celu oceny skuteczności i efektywności zaplanowanych prac.



## 6 Akceptacja ryzyka

Po wdrożeniu planu postępowania z ryzykiem następuje etap akceptacji tzw. **ryzyka szczątkowego** (rezydualnego), pozostałego po wdrożeniu zabezpieczeń. Ryzyko szczątkowe to takie, którego

nie możemy już wyeliminować, a względem którego kierownictwo ustaliło i przyjęło kryteria akceptacji. Innymi słowy, jest to ryzyko, z którego firma zdaje sobie sprawę i które świadomie podejmuje – oczywiście naszym celem jest doprowadzenie do tego, aby było ono jak najniższe.

## 7 Informowanie o ryzyku

Proces przekazywania wiedzy uczestnikom procesu (pracownikom zaangażowanym w dany proces, korzystającym z danego zasobu) o bieżącym statusie ryzyka. Mechanizmy, zgodnie z którymi te informacje są przekazywane, powinny być zaprojektowane już na etapie budowania systemu zarządzania ryzykiem.

**Powinny one zapewniać dostępność informacji właściwym osobom, w określonym czasie oraz pozwalać na wymianę wiedzy i konsultacje.** Istotą informowania ryzyku jest zapewnienie, że każdy właściciel ryzyka jest świadomy swojej roli oraz zakresu obowiązków i odpowiedzialności.

## 8 Monitorowanie i przegląd ryzyka

Zarządzanie ryzykiem jest procesem ciągłym, więc duże znaczenie ma w nim monitorowanie oraz przegląd ryzyk. Etap ten ma za zadanie:



### Ustalić

czy system zarządzania ryzykiem spełnia założone cele, oraz czy polityki i procedury ustanowione w jego ramach są nadal aktualne, odpowiednie i wydajne.



### Zapewnić

że wszystkie nowe ryzyka zostaną w odpowiednim czasie zidentyfikowane oraz ustanowi się wobec nich priorytety działania. Monitorowanie oraz przegląd ryzyk powinny być prowadzony w kontekście nowych aktywów, zagrożeń i podatności, a także incydentów związanych z naruszeniem bezpieczeństwa informacji. W sytuacji odnotowania jakichkolwiek zmian czynników wpływających na ryzyko należy dokonać ponownego przeglądu ryzyk oraz zaktualizowania ich wartości, jeżeli jest to uzasadnione.



## Metody szacowania ryzyka

Wyróżnia się trzy główne metody szacowania ryzyka:

- ilościową
- jakościową
- mieszaną

**Analiza ilościowa** polega na ocenie prawdopodobieństwa oraz skutków wystąpienia ryzyka poprzez nadanie im konkretnych wartości liczbowych. Zaletami metod ilościowych jest powtarzalność i względna obiektywność wyników, dzięki czemu mogą być one porównywane w czasie. Do metod ilościowych zalicza się między innymi techniki: **drzewo zdarzeń** (Events Tree Analysis), **drzewo błędów** (Faults Tree Analysis) oraz **FMEA**.



**Metoda jakościowa** polega na indywidualnej ocenie ryzyka na podstawie doświadczenia, wiedzy oraz dobrych praktyk. Metoda ta wykorzystuje subiektywne miary i oceny takie jak wartości opisowe poziomów (niski, średni, wysoki). Korzyści metod jakościowych to:

- brak konieczności ilościowego określenia skutków i częstotliwości wystąpienia zagrożeń
- wskazanie ogólnych obszarów ryzyka, na które konieczne jest zwrócenie uwagi

- możliwość uwzględnienia takich czynników jak np. wizerunek organizacji, jej kultura.

**Metoda mieszana** to oczywiście połączenie analizy ilościowej i jakościowej.

## Zalety stosowania podejścia opartego na ryzyku

Podejście oparte na ryzyku coraz częściej wykorzystywane jest w różnych sferach życia organizacji, ponieważ niesie ze sobą wymierne korzyści. Główną zaletą zarządzania ryzykiem jest to, że to organizacja dobiera środki bezpieczeństwa (czy to techniczne, czy organizacyjne) adekwatnie do stwierdzonego w danym czasie ryzyka z uwzględnieniem jej "apetytu na ryzyko" oraz zasobów, którymi w danym momencie dysponuje. Daje to również możliwość optymalizacji kosztów poprzez wczesne reagowanie na anomalie i przyjęcie postawy reaktywnej zamiast zapobiegawczej. Zabezpieczenia są też adekwatne do skali i specyfiki działalności – czego innego potrzebuje bank, a czego innego salon fryzjerski.

### Pozostałe korzyści:



podejmowanie świadomych decyzji przez kierownictwo



zmniejszenie liczby i skali ryzyk



wzrost zaufania klientów i innych stron zainteresowanych



ujednolicenie podejścia od oceny ryzyka i reakcji na nie poprzez wdrożenie jednolitej metody oceny w różnych obszarach organizacji.



## Nie ryzykuj!

Zarządzanie ryzykiem w bezpieczeństwie informacji opiera się na odpowiednim zaplanowaniu, organizacji kierowania oraz kontrolowaniu zasobów. Wymaga zaangażowania oraz współpracy wszystkich stron przetwarzających informacje w celu określenia kryteriów akceptacji, wymagań oraz wyboru opcji postępowania z ryzykiem. Oprócz tego, istotną rolę w obszarze zarządzania ryzykiem przypisuje się kierownictwu organizacji, które jest odpowiedzialne za kształtowanie oraz wzmacnianie wśród pracowników poczucia świadomości występowania zagrożeń, oraz potrzeby przeciwdziałania sytuacjom kryzysowym.

Warto również zauważyć, że podejście oparte na ryzyku i zarządzanie przez ryzyko nie jest cechą

charakterystyczną jedynie dla norm z serii ISO.

**Koncepcja RODO również jest zbudowana jest na tym podejściu, dając administratorom swobodę w wyborze zabezpieczeń i ich racjonalizację w zależności od skali ryzyka, charakteru danych czy specyfiki organizacji.**

Z naszego doświadczenia wynika, że system zarządzania ryzykiem będzie przynosił wymierne efekty tylko wówczas, jeżeli zostanie w odpowiedni sposób zaplanowany i ustanowiony. Ważna jest również komunikacja jego istoty i korzyści wśród personelu. Warto także na koniec podkreślić, że nie ma jednej uniwersalnej metody szacowania ryzyka, a dochodzenie do tej odpowiedniej dla organizacji również jest procesem, który może trwać nawet kilka lat i ewoluować wraz z organizacją.



Unikanie ryzyka to klucz do wiarygodnego biznesu.  
Czy Twoja organizacja na pewno jest chroniona?

**Umów się na bezpłatną konsultację, a  
odpowiemy na wszystkie Twoje pytania.**



Sprawdź cykl

## „Akademia LexDigital”

na [YouTube](#) i [LinkedIn](#), omawiający praktyczne aspekty SZBI wg ISO 27001 i korzyści z wdrożenia.



Newsletter RODO

Październik 2025 nr 10/2025

# Dziękujemy za przeczytanie naszego newslettera!

Masz pytania?

[SKONTAKTUJ SIĘ Z NAMI](#)