

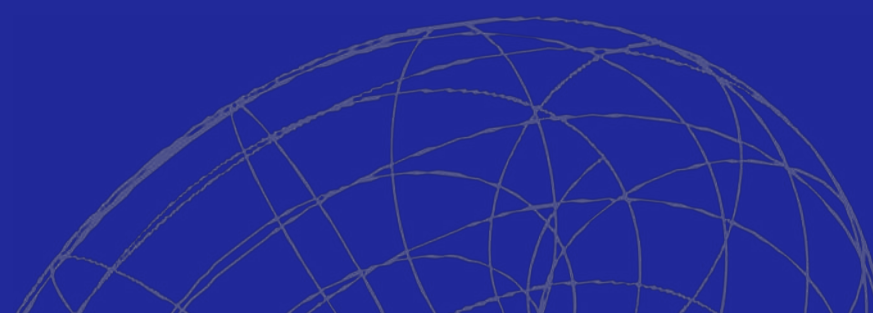
# 3 lata Komunikatu Chmurowego

Monika Maćkowska-Morytz | Kochański & Partners  
Maciej Kuranc | Kochański & Partners

Warszawa, 14 czerwca 2023 r.

# **Komunikat Chmurowy**

## **– aspekty praktyczne**



## Regulacje outsourcingu

### Przepisy prawa

- Prawo bankowe (art. 6a-6d)
- Ustawa o działalności ubezpieczeniowej i reasekuracyjnej
- Rozporządzenie Wyptalność II
- Ustawa o obrocie instrumentami finansowymi (art. 81a i n.)
- Ustawa o usługach płatniczych
- Ustawa o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi
- RODO
- UKSC

### Soft law

#### PL

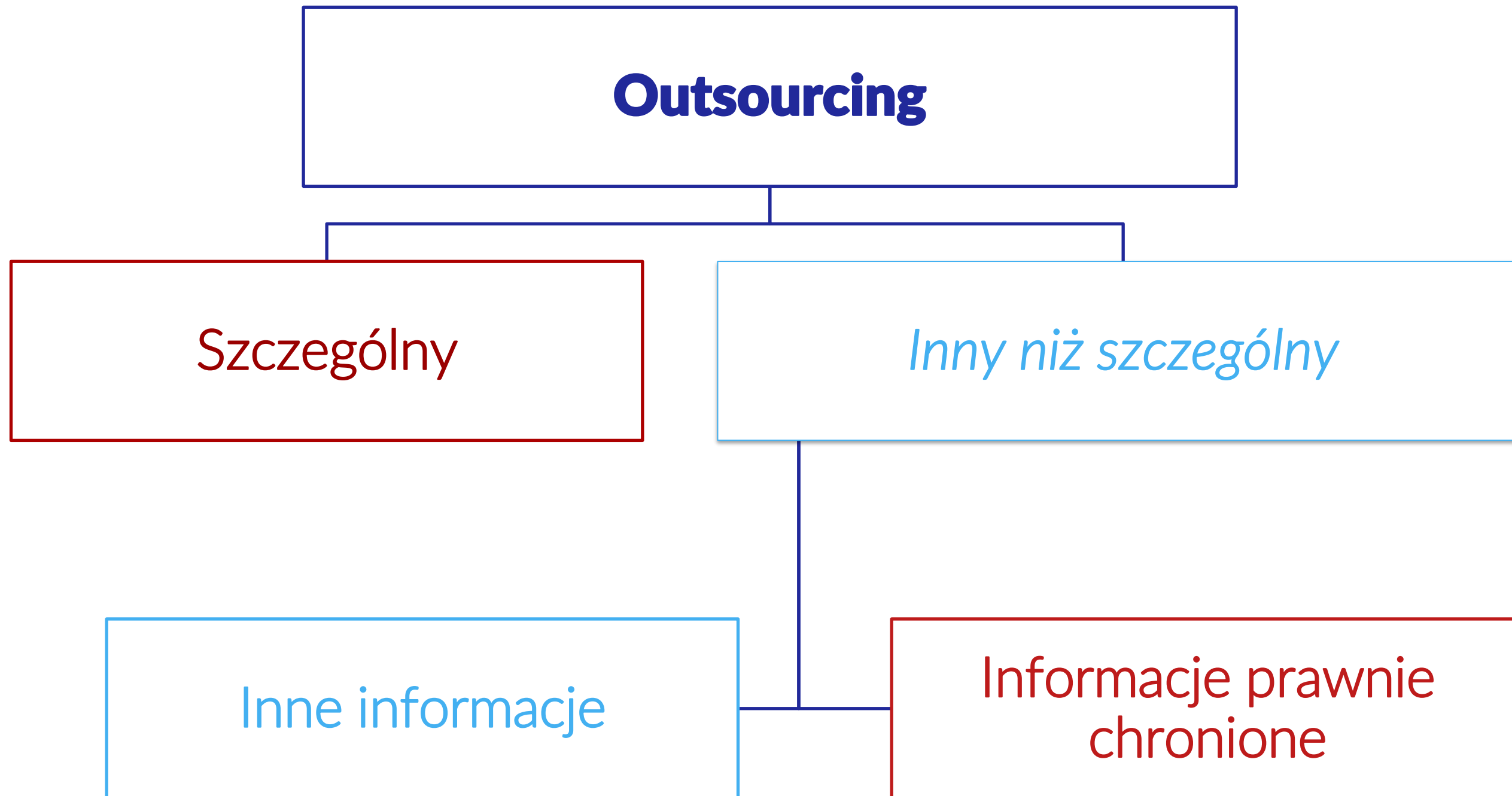
- Rekomendacja D
- Rekomendacja M
- Komunikat Chmurowy UKNF
- Q&A Chmurowe UKNF

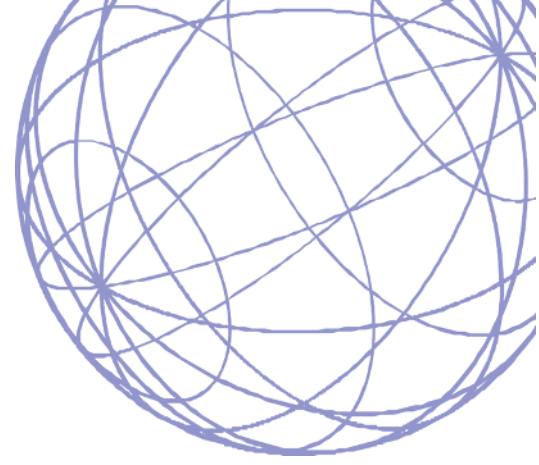
#### UE

- Wytyczne EBA
- Wytyczne ESMA
- Wytyczne EIOPA

# Stosowanie Komunikatu chmurowego

- rodzaje outsourcingu





# Kluczowe problemy projektów wdrożeniowych

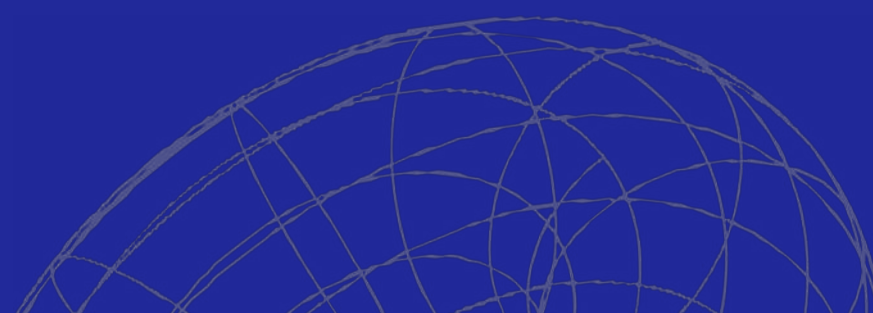
**Outsourcing zagraniczny**

**Łańcuch outsourcingowy  
Podwykonawca a poddostawca**

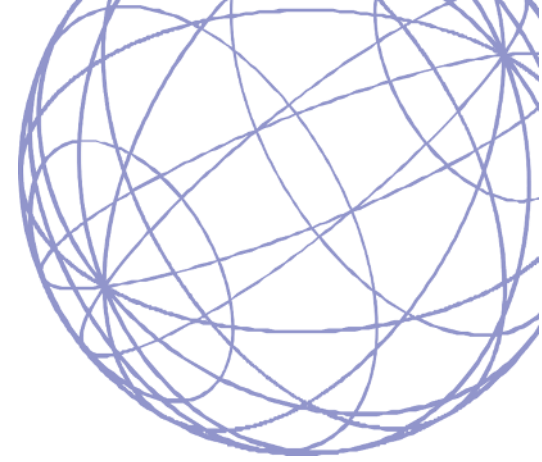
**Partnerzy biznesowi  
wykorzystujący chmurę**

**Odpowiedzialność**

# **Outsourcing zagraniczny / lokalizacja danych**







# Lokalizacja danych

## – regulacje w bankowości

### Art. 6d. ust. 1 prawa bankowego

Zawarcie umowy, o której mowa w art. 6a ust. 1 lub 7, z [1] przedsiębiorcą zagranicznym niemającym miejsca stałego zamieszkania lub nieposiadającym siedziby na terytorium państwa członkowskiego lub [2] umowy przewidującej, że powierzone czynności będą wykonywane poza terytorium państwa członkowskiego, wymaga zezwolenia Komisji Nadzoru Finansowego udzielonego na wniosek banku.

Zwróć uwagę na art. 4 pr. b.!

b) został uznany za taki bank przez Komisję Nadzoru Finansowego;

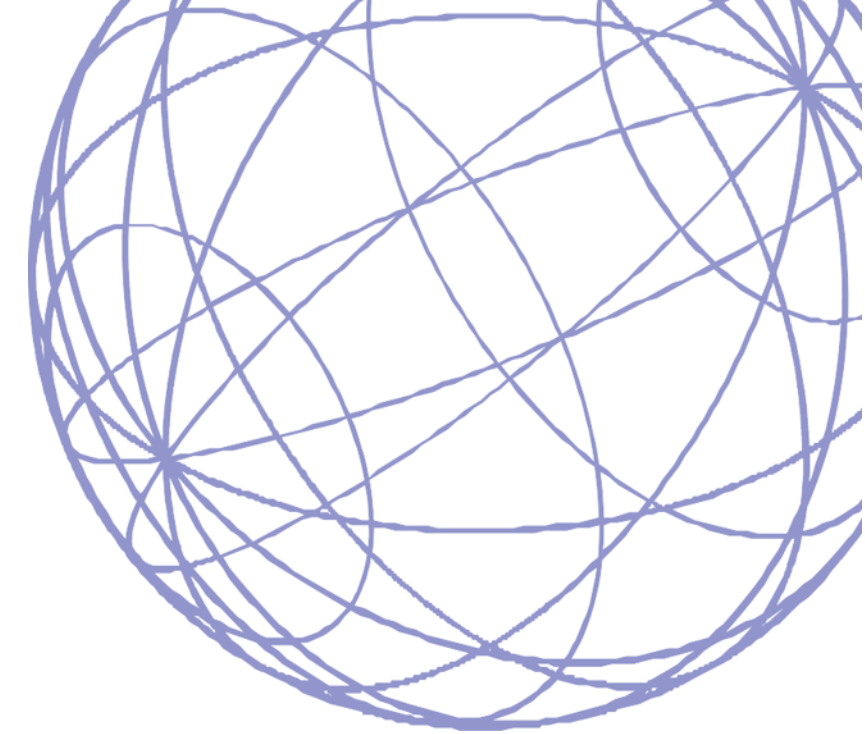
36) państwo członkowskie – państwo członkowskie Unii Europejskiej;

37) ustawa o nadzorze makroostrożnościowym – ustawę z dnia 5 sierpnia 2015 r. o nadzorze makroostrożnościowym nad systemem finansowym i zarządzaniu

z bankiem krajowym, wchodzącym w skład holdingu.

3. Przepisy ustawy dotyczące państw członkowskich stosuje się również do państw trzecich, ale należących do Europejskiego Obszaru Gospodarczego.

4. Bank krajowy i bank zagraniczny są instytucją, o której mowa w art. 4 ust. 1



# Lokalizacja danych – regulacje w bankowości

Czego oczekuje KNF?

## Pkt VII. 6.3. Komunikatu Chmurowego

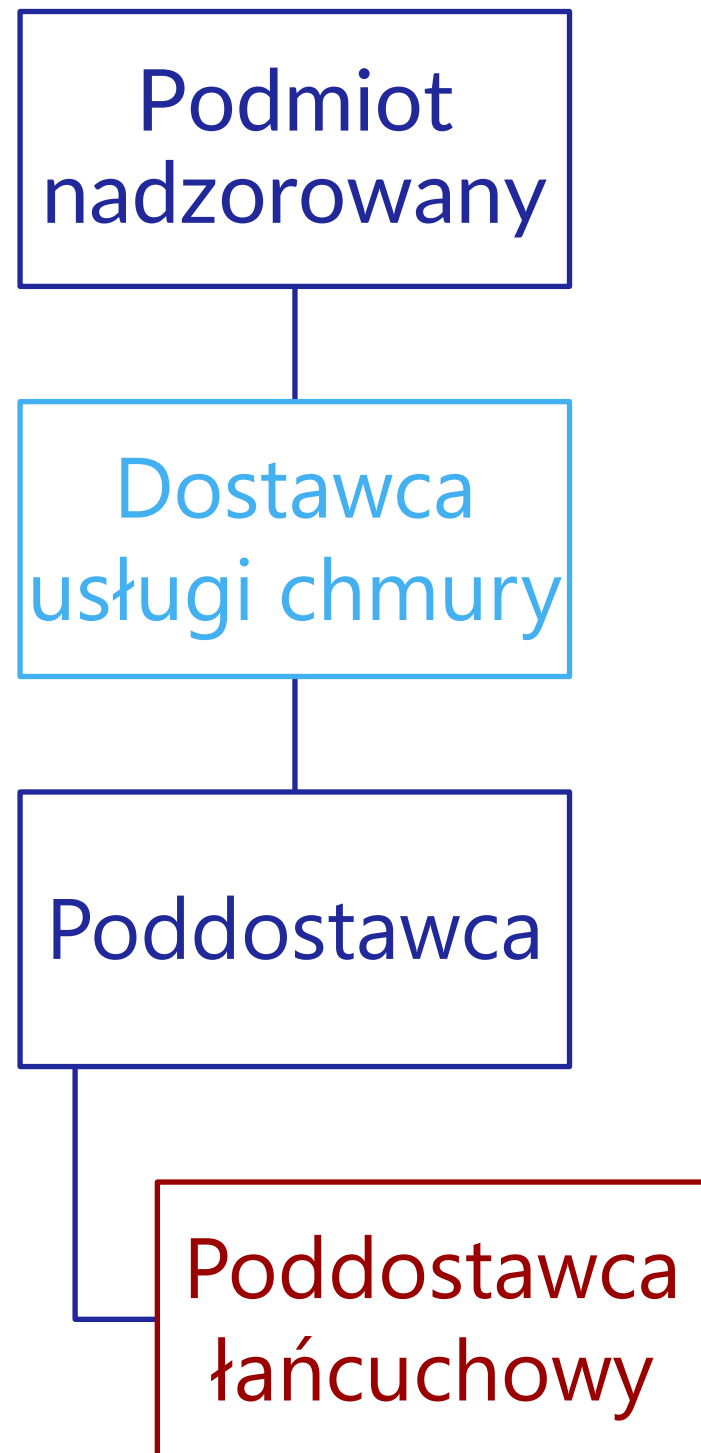
*Nadzór rekomenduje, aby CPD zlokalizowane było na terytorium państwa Europejskiego Obszaru Gospodarczego (EOG). Punkt ten stosuje się z zastrzeżeniem, że podmioty nadzorowane, które:*

- a) zostały uznane stosowną decyzją za operatorów usług kluczowych w rozumieniu art. 5 ust. 2 ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa i którzy wykorzystują usługę chmury obliczeniowej w zakresie realizacji usługi kluczowej lub*
- b) są operatorami infrastruktury krytycznej w rozumieniu ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym i którzy wykorzystują usługę chmury obliczeniowej w zakresie realizacji zadań operowania infrastrukturą krytyczną*

*powinny w pierwszej kolejności wykorzystywać CPD znajdujące się na terenie Rzeczypospolitej Polskiej, o ile – w ocenie podmiotu nadzorowanego – oferowane warunki umowne, ekonomiczne, operacyjne, SLA czy funkcjonalne są nie gorsze od CPD znajdujących się poza terytorium Rzeczypospolitej Polskiej.*



# Szacowanie ryzyka – łańcuch outsourcingowy



## Ograniczenia prawne łańcucha

- ⇒ Zróżnicowanie regulacji:
  - ⇒ **Usługi płatnicze**: brak wyraźnej regulacji
  - ⇒ **Obrót instrumentami finansowymi**: **wyraźny zakaz**
  - ⇒ **Prawo bankowe**: zakaz wynikający ze stanowiska nadzoru\*
  - ⇒ **TFI**: domniemany zakaz
  - ⇒ **Ubezpieczenia**: brak wyraźnej regulacji
- ⇒ Ograniczenia odpowiedzialności poddostawców – przepisy a oczekiwania KNF
- ⇒ Komunikat nie jest źródłem ograniczeń łańcucha

## Poddostawca wg. Komunikatu Chmurowego

*podmiot, który świadczy usługi dla dostawcy usług chmury obliczeniowej, służące dostarczaniu usługi chmury obliczeniowej dla podmiotu nadzorowanego i posiada albo może posiadać identyfikowany dostęp do informacji przetwarzanych przez podmiot nadzorowany;*

## Podoutsourcing - szyfrowanie i dostęp do danych

### Customer Lock Box / Access Approval

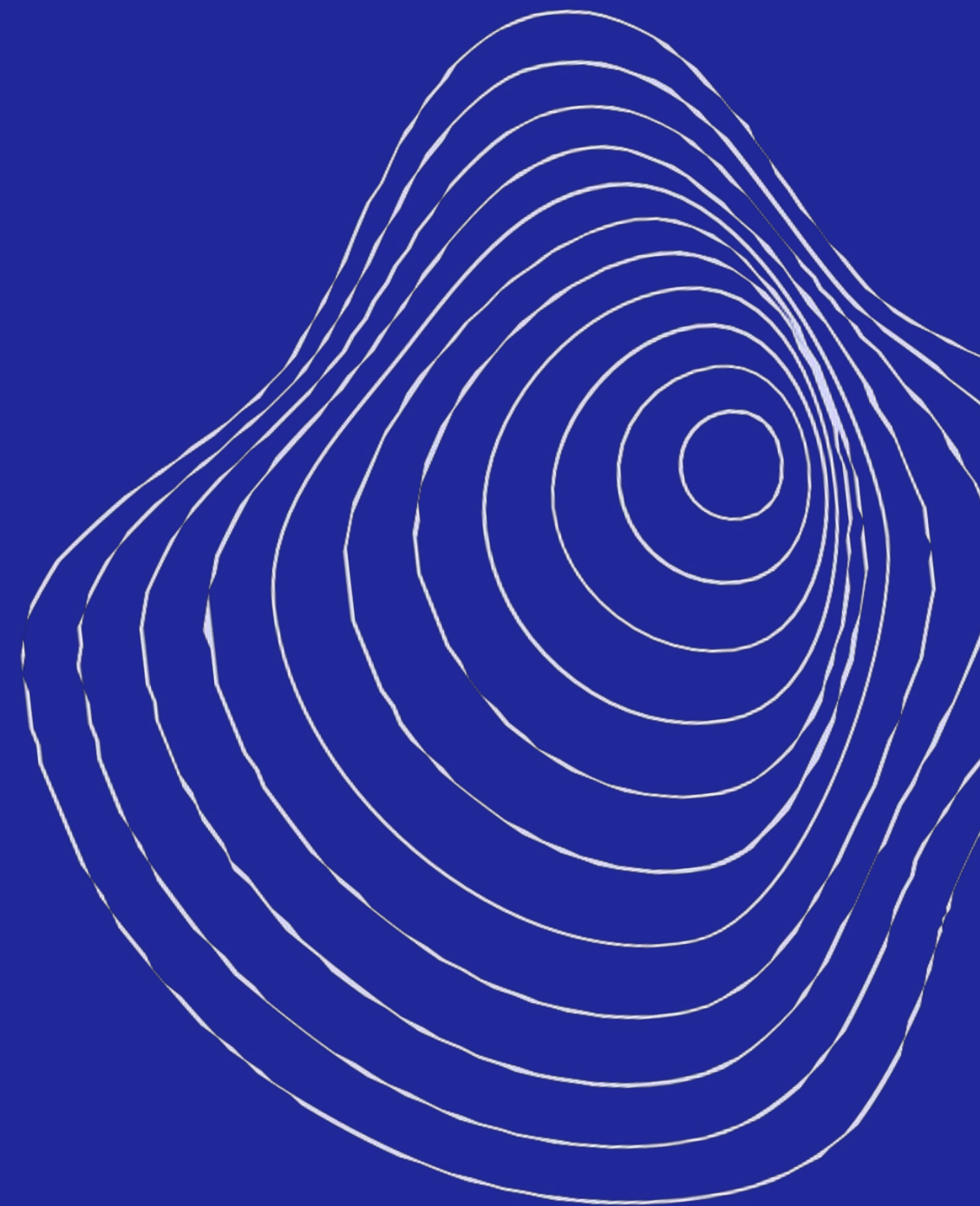
### Customer Key

23) *ujawnienie informacji* – bez uszczerbku dla rozumienia przepisów prawa bezwzględnie obowiązujących, oznacza sytuację, podczas której informacje są przetwarzane w chmurze obliczeniowej:

- a) w sposób *nieszyfrowany* albo
- b) w sposób zaszyfrowany „at rest” lub „in transit”, ale *dostęp do kluczy szyfrujących i szyfrowanej tymi kluczami informacji* posiada albo może posiadać dostawca usług chmury obliczeniowej lub jego poddostawca w łańcuchu outsourcingowym.

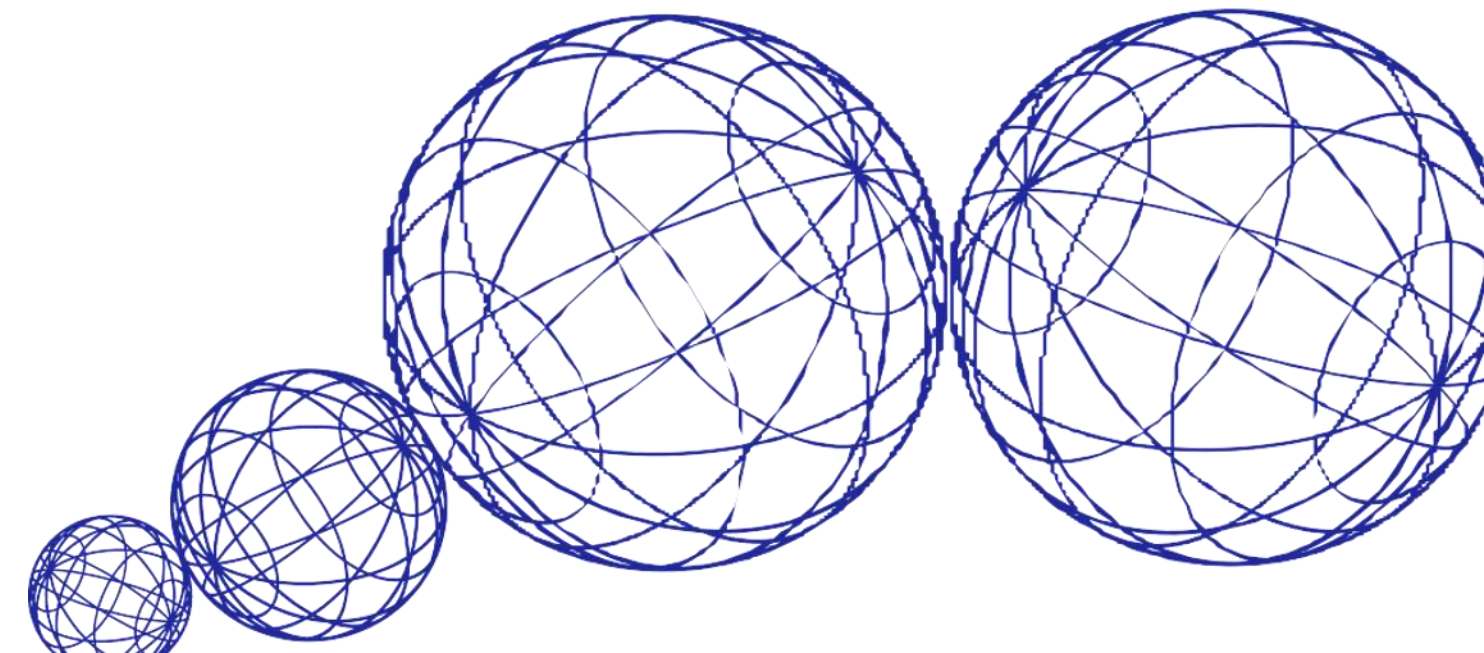
## **Podwykonawcy wykorzystujący chmurę**

**Co gdy partner podmiotu nadzorowanego  
(np. audytor) korzysta z chmury na własne  
potrzeby?**



## Wykorzystanie chmury przez Partnera

- Podstawą dla stosowania wymogów Komunikatu Chmurowego wobec podmiotów nadzorowanych (w tym banków), powinno być **wykorzystanie chmury obliczeniowej w sposób nadający temu korzystaniu charakter outsourcingu chmury obliczeniowej** - związek pomiędzy usługą chmury obliczeniowej a poleceniem wykonywania tej usługi (powierzeniem) na rzecz i w imieniu Banku;
- Samo przetwarzanie informacji prawnie chronionych w chmurze obliczeniowej **nie jest przesłanką do zaistnienia outsourcingu;**
- Test autonomicznego wykorzystania chmury

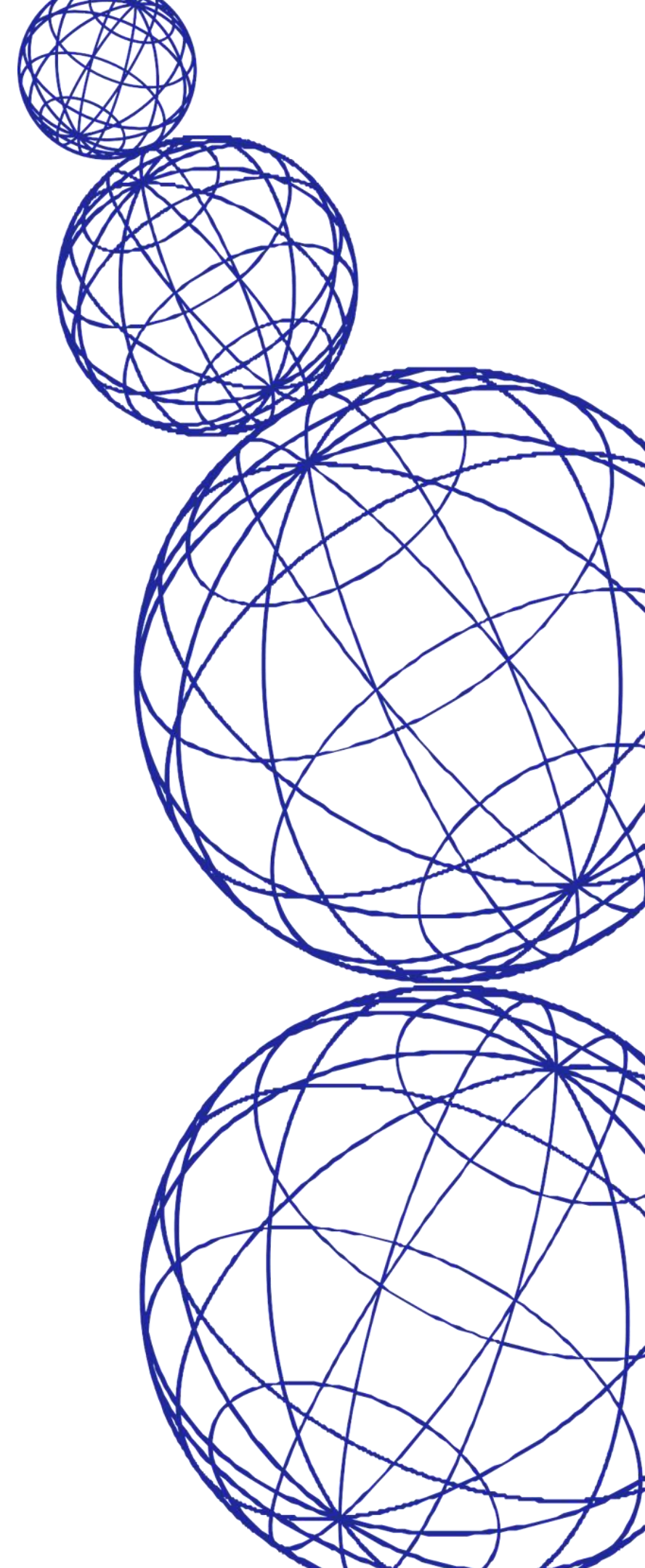




# Wykorzystanie chmury przez Partnera

Wykorzystanie chmury przez Partnera nie będzie się wiązało z zaistnieniem outsourcingu chmury obliczeniowej, gdy spełnione są łącznie następujące warunki:

- usługa chmury obliczeniowej **nie jest niezbędna dla realizacji przedmiotu usługi** świadczonej przez Partnera;
- wykorzystanie usługi chmury obliczeniowej przez Partnera **ma charakter autonomiczny** (tj. usługa chmurowa nie jest elementem charakterystycznym, cechą funkcjonalną);
- usługa chmury obliczeniowej **nie jest udostępniana do bezpośredniego wykorzystania** przez Bank ani nie jest dostępna na jego żądanie.



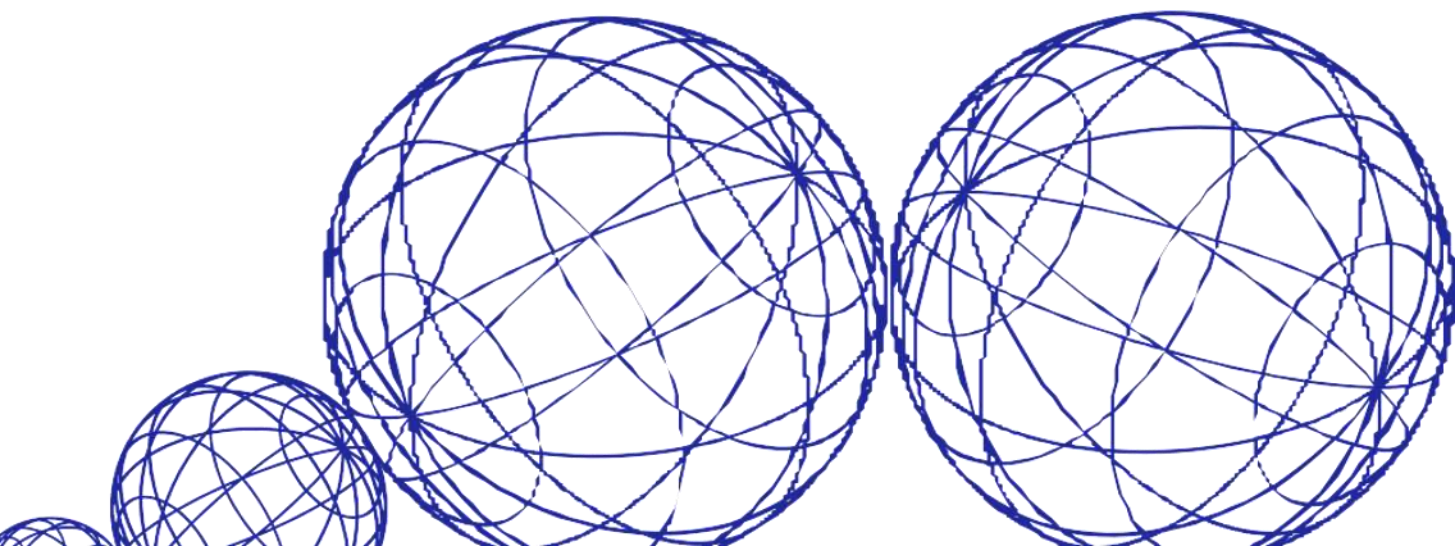


## Przykłady:

### Przykład 1 – Usługa mailingu

*Umowa z dostawcą usługi kampanii marketingowych dedykowanych określonym klientom (tzw. targetowane kampanie). Usługa jest oparta o zewnętrzną pocztę chmurową (np. w formule SaaS), dane objęte tajemnicą są przetwarzane w chmurze obliczeniowej.*

→ **STOSUJEMY KOMUNIKAT**



### Przykład 2 – Usługa tłumaczenia

*Umowa z Partnerem – biurem tłumacza przysięgłego – na tłumaczenia dokumentów (umów z klientami Banku), realizowana w modelu outsourcingu regulowanego<sup>24</sup>. Biuro tłumaczeń korzysta na własne potrzeby z pakietu biurowego w formule chmury obliczeniowej, w modelu SaaS. Poczta oraz przechowywanie dokumentów funkcjonuje w oparciu o serwery i oprogramowanie Dostawcy usługi chmury obliczeniowej, a w ramach tych rozwiązań mogą być przetwarzane dane objęte tajemnicą bankową. Partner nie udostępnia tych rozwiązań na rzecz Banku.*

→ **BRAK OBOWIĄZKU STOSOWANIA  
KOMUNIKATU**

## Nieograniczona odpowiedzialność za szkody wyrządzone klientom wskutek niewykonania lub nienależytego wykonania umowy outsourcingowej

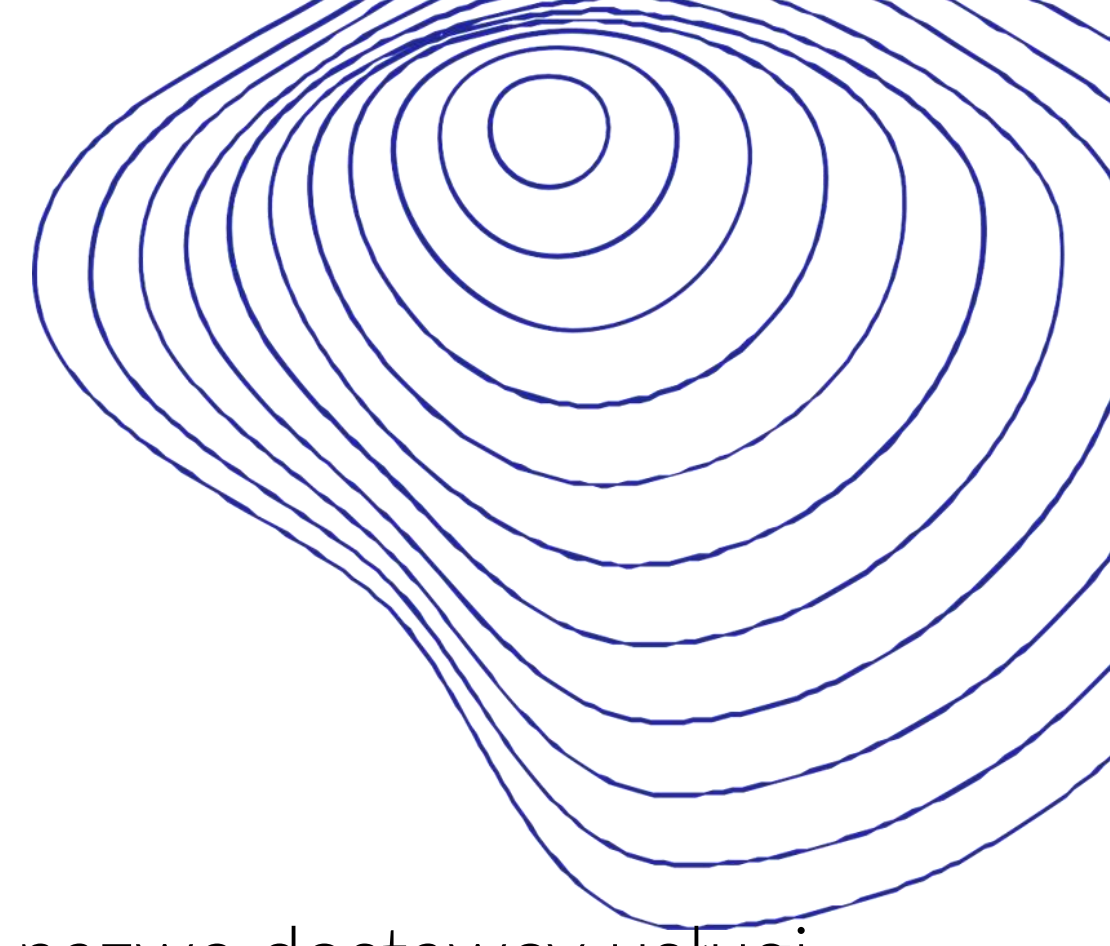
- ✓ Prawo bankowe – art. 6b
- ✓ Ustawa o usługach płatniczych – art. 88 ust. 3
- ✓ Ustawa o obrocie instrumentami finansowymi – art. 81c ust. 2  
(zakaz wyłączenia)

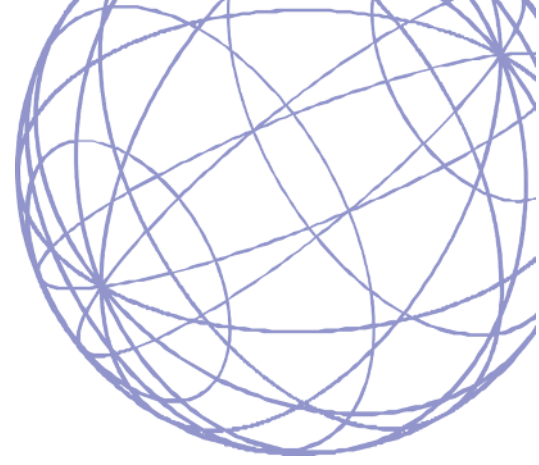
⇒ Ograniczenia odpowiedzialności  
poddostawców – *przepisy a*  
*oczekiwania KNF*

# Notyfikacja do UKNF

## Problematiczne kwestie:

- ✓ **SaaS** – podajemy dostawcę aplikacji czy dostawcę hostingu? – podajemy nazwę dostawcy usługi, warto dodatkowo wskazać dostawcę głównego hostingu (chmury).
- ✓ **Jak szczegółowo opisujemy dane?** – można podawać ogólne kategorie, najważniejsze: czy dane objęte tajemnicą.
- ✓ **Jak wskazywać lokalizację?** - co najmniej „EOG” lub „UE”, wskazane bardziej szczegółowo - **ALE** – uwaga na zmiany lokalizacji.
- ✓ **Data umowy** – pokazujemy datę umowy, której podpisanie wiąże się dla banku z korzystaniem z chmury obliczeniowej. Nie wskazuje się daty podpisania umowy pomiędzy dostawcą aplikacji w modelu SaaS, a jego poddostawcą w zakresie hostingu.





## Nowelizacja prawa bankowego – co nowego?

- Zakres dozwolonego podoutsourcingu → czynności wynikające z umowy, „z zachowaniem tajemnicy prawnie chronionej”.
- Podoutsourcing łańcuchowy dopuszczony → nowy art. 6a. ust. 7a PB
- Outsourcing zagraniczny → zawiadomienie zamiast zezwolenia
  - Zob. nowe wymogi (art. 6d PB, oświadczenie o niekaralności, zawiadomienie o **zmianie** umowy, etc.).
  - Wymogi z UOIF (zakaz podoutsourcingu bez zmian 😊)



# Kochański & Partners współautorem *Polish Cloud Standard*

W ramach Bankowej Grupy Roboczej przy Związku Banków Polskich (ZBP) uczestniczyliśmy – jako jedyny partner prawny – w pracach nad stworzeniem polskiego standardu wdrożeń chmury obliczeniowej w bankach, tzw. **PolishCloud**. Zostaliśmy także ponownie wybrani do pracy nad wersją standardu 2.0, która w najbliższych miesiącach ujrzy światło dzienne.

**PolishCloud** stanowi mapę drogową dla banków w Polsce w zakresie implementacji usług chmurowych.

Unikatowa wiedza zdobyta w trakcie prac nad **PolishCloud** oraz długoletnie doświadczenie płynące z obsługi klientów z sektora finansowego pozwoliły nam stworzyć kompleksowy pakiet usług, które pomogą sprawnie i skutecznie wdrożyć każdą usługę chmurową. Dodatkowo jako jedyny partner prawny wraz z Accenture, Google, Microsoft oraz Operatorem Chmury Krajowej prowadzimy największy w Europie Środkowo-Wschodniej neutralny technologicznie projekt szkoleniowy dla sektora bankowego o nazwie **PolishCloud Academy**.

## Polish Cloud 2.0





## Pozostańmy w kontakcie!

METROPOLITAN  
Plac Piłsudskiego 1  
00-078 Warsaw, Poland

EQUAL BUSINESS PARK  
Wielicka 28B, building C 30-552  
Cracow, Poland

T: +48 22 326 9600  
F: +48 22 326 9601  
E: [biuro@kochanski.pl](mailto:biuro@kochanski.pl)

[www.kochanski.pl](http://www.kochanski.pl)



**Monika Maćkowska-Morytz**  
Adwokat, Partner

M: +48 660 765 918  
E: [m.mackowska-morytz@kochanski.pl](mailto:m.mackowska-morytz@kochanski.pl)



**Maciej Kuranc**  
Associate

M: +48 532 461 055  
E: [m.kuranc@kochanski.pl](mailto:m.kuranc@kochanski.pl)

