

# Bezpieczne finanse w chmurze

Pomoc w zapewnieniu zgodności z postanowieniami Komunikatu Urzędu Komisji Nadzoru Finansowego z dnia 23 stycznia 2020r. dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej



## Potrzeba biznesowa:

W dzisiejszych czasach coraz więcej firm podejmuje decyzje związane z migracją infrastruktury do środowiska chmurowego. Migracja taka niesie za sobą szereg potencjalnych zalet związanych z obniżeniem kosztów operacyjnych, elastycznością dostępu do danych i zasobów oraz bezpieczeństwem przetwarzanych informacji. Aby jednak było to możliwe, należy przeprowadzić ją w zaplanowany sposób, zgodnie z najlepszymi praktykami i wytycznymi regulatorów. Dzięki wydanemu Komunikatowi, firmy z sektora finansowego uzyskały dostęp do wytycznych pozwalających na zrobienie milowego kroku w kierunku chmury. Opisane wytyczne dotyczą zarówno podmiotów planujących migrację do środowiska chmurowego, jak również tych, które wykonały już migrację i obecnie przetwarzają dane w środowisku chmurowym, bądź hybrydowym.



## Usługa KPMG:

W celu zapewnienia zgodności z postanowieniami Komunikatu, eksperci KPMG pomogą w przeprowadzeniu prac związanych z poniższymi zagadnieniami:

### Klasyfikacja i ocena informacji



Weryfikacja obecnie posiadanych polityk i procedur związanych z procesem klasyfikacji informacji.



W przypadku braku wymaganej dokumentacji lub jej niekompletności, pomoc w przeprowadzeniu zgodnego z Komunikatem udokumentowanego procesu klasyfikacji informacji.



Weryfikacja obecnej inwentaryzacji danych zawierających informacje prawnie chronione lub wsparcie w jej przygotowaniu.



Pomoc w ocenie informacji pod kątem jej dopuszczalności do przetwarzania w chmurze obliczeniowej.



Na podstawie zebranych informacji wskazanie różnicy pomiędzy wymaganiami Komunikatu a stanem obecnym.



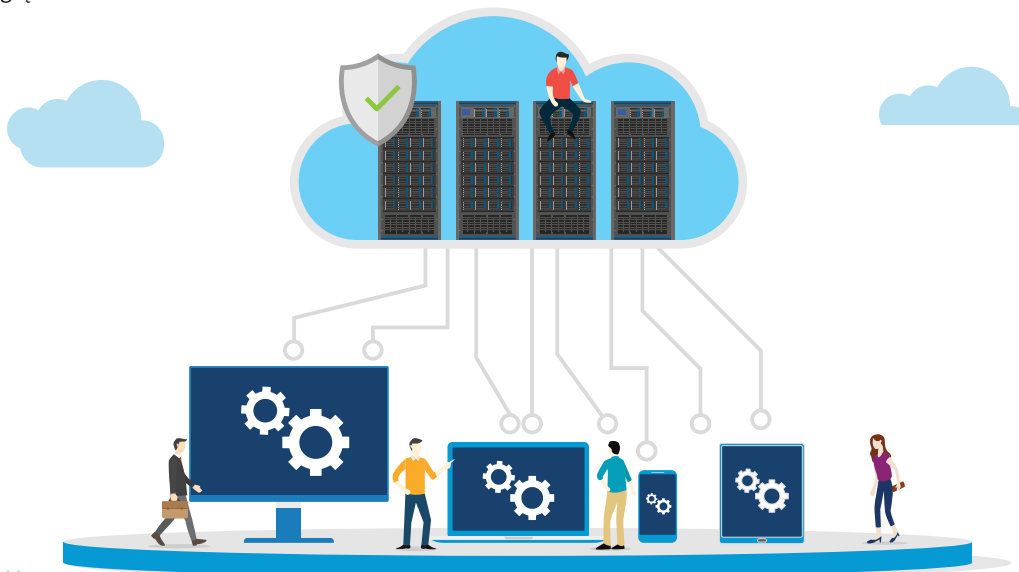
Zaplanowanie dalszych prac niezbędnych do spełnienia wymagań regulatora (w tym ewentualna pomoc w przygotowywaniu niezbędnych procedur/dokumentów) mających na celu udokumentowanie procesu klasyfikacji informacji oraz przeprowadzenie inwentaryzacji danych.

## Szacowanie ryzyka




- Pomoc w przeprowadzeniu szacowania ryzyka na zgodność z poniższymi wymogami wynikającymi z Komunikatu:
  - ogólnych zagrożeń dla stosowania chmury obliczeniowej,
  - specyficznych zagrożeń dla stosowanych konkretnych usług chmury obliczeniowej,
  - specyficznych zagrożeń związanych z zasobami,
  - wartości przetwarzanych informacji oraz skutków bezpośredniej i pośredniej utraty kontroli nad ich przetwarzaniem,
  - w zakresie szyfrowania informacji,
  - w obszarze tworzenia łańcuchów outsourcingowych,
  - w zakresie usług (dostawców chmury obliczeniowej), które są wykorzystywane do świadczenia własnych usług przez bezpośrednich dostawców,
  - w kwestii prawa właściwego umowy pomiędzy dostawcą usług chmury obliczeniowej a podmiotem z sektora finansowego,
  - innych istotnych, zidentyfikowanych zagrożeń, związanych z wykorzystywaniem usług chmury obliczeniowej.
- Zidentyfikowanie słabości wynikających z przeprowadzanego szacowania ryzyka wraz z konkretnymi rekomendacjami pozwalającymi zminimalizować ryzyko.
- Wsparcie w wypracowaniu mechanizmów zabezpieczeń mitygujących kluczowe ryzyka w celu uzyskania zgodności z Komunikatem.

## Pomoc we wdrożeniu minimalnych wymagań dla przetwarzania informacji w chmurze obliczeniowej

- Przegląd techniczny oraz organizacyjny mający na celu potwierdzenie spełnienia minimalnych wymagań w następujących obszarach:
  - zapewnienie kompetencji,
  - umowy z dostawcą usług chmury obliczeniowej,
  - plany przetwarzania informacji w chmurze obliczeniowej,
  - wymagania dla dostawców usług chmury obliczeniowej,
  - metody oraz mechanizmy szyfrujące,
  - monitorowanie środowiska przetwarzania informacji w usługach chmury obliczeniowej,
  - dokumentowanie działań podmiotu finansowego.
- Identyfikacja słabości wynikających z przeglądu oraz wskazanie różnicy między wymogami regulatora a zidentyfikowanym stanem rzeczywistym.
- Wsparcie w spełnieniu minimalnych wymogów dla środków technicznych oraz zasobów organizacyjnych, którym podlegał przegląd.



### Korzyści:

-  Niższe koszty operacyjne, elastyczność i skalowalność zasobów oraz zwiększone bezpieczeństwo danych, które wynikają z migracji do chmury.
-  Zgodność sposobu i zakresu przetwarzania informacji w chmurze obliczeniowej z obowiązującym prawem oraz z postanowieniami Komunikatu co umożliwi poinformowanie UKNF o zamiarze przetwarzania lub przetwarzaniu informacji w chmurze obliczeniowej.
-  Potwierdzenie dla regulatora oraz organów nadzorczych dochowania należytej staranności poprzez przeprowadzoną zgodnie z wymogami weryfikację, wykonaną przez niezależny i uznany w branży zespół konsultantów.



## Dlaczego KPMG?



KPMG to niekwestionowany **światowy lider** w obszarze usług doradczych w zakresie cyberbezpieczeństwa (wg badania Forrester Wave™: Information Security Consulting Services, Q3 2017)



Nasi polscy eksperci zrealizowali **kilkaset projektów** w obszarze cyberbezpieczeństwa dla polskich i zagranicznych przedsiębiorstw z różnych branż



Wiedzę naszych konsultantów potwierdzają **liczne certyfikaty**



W trakcie realizowanych projektów zidentyfikowaliśmy kilkadziesiąt podatności typu **zero-day**



**Rozumiemy procesy biznesowe**, przez co nasze rekomendacje są dostosowane do rzeczywistych potrzeb i wnoszą realną wartość



Obecność w globalnej sieci zespołów cyberbezpieczeństwa KPMG, to **bogate zasoby wiedzy**, narzędzi i nowatorskich rozwiązań



Zespół składający się z **ponad dziesięciu** certyfikowanych konsultantów w **bezpieczeństwie środowisk chmurowych**



**Globalna sieć** to również gwarancja ciągłości współpracy oraz możliwość świadczenia usług w wielu krajach jednocześnie



Aktywnie działamy w organizacjach branżowych (m.in. w zarządzie **OWASP Poland**)



Nasza **wiedza jest doceniana** przez wiodące organizacje edukacyjne – np. wspieramy SANS Institute w roli mentora w zakresie bezpieczeństwa aplikacji



Jesteśmy **niezależni** od producentów rozwiązań bezpieczeństwa, dzięki czemu jesteśmy w stanie optymalnie doradzać



Jesteśmy **elastyczni** i dostosowujemy się do zmieniających się dynamicznie potrzeb klientów



## Nasze wybrane certyfikaty:



- Microsoft Certified: Azure Security Engineer Associate
- Microsoft 365 Certified: Security Administrator Associate
- CISM (Certified Information Security Manager)
- CISSP (Certified Information Systems Security Professional)
- CISA (Certified Information Systems Auditor)
- OSCP (Offensive Security Certified Professional)
- LPT (Licensed Penetration Tester)
- CEH (Certified Ethical Hacker)
- GICSP (Global Industrial Cyber Security Professional)
- GRID (GIAC Response and Industrial Defense)
- GWAPT (GIAC Web Application Penetration Tester)
- GREM (GIAC Reverse Engineering Malware)
- GMOB (GIAC Mobile Device Security Analyst)
- CRISC (Certified in Risk and Information Systems Control)
- CCSP (Cisco Certified Security Professional)
- CCSA (Check Point Security Administrator)
- GCWSA (GIAC Certified Windows Security Administrator)
- MCTS (Microsoft Certified Technology Specialist)
- RHCE (Red Hat Certified Engineer Red Hat Enterprise Linux 6)
- RHCSA (Red Hat Certified System Administrator Red Hat Enterprise Linux 6)
- GCUX (GIAC Certified UNIX Security Administrator)
- LPI LPIC-1 Certified Linux Administrator
- SUSE Certified Administrator
- GSSP-JAVA (GIAC Secure Software Programmer – JAVA)
- ECSA (Certified Security Analyst)
- Information Systems Security (INFOSEC) Professional
- ISO 27001 Information Security Management System Lead Auditor
- GAWN (GIAC Auditing Wireless Networks Certified Professional)
- CCNA (Cisco Certified Network Associate)
- PMP (Project Management Professional)
- CIA (Certified Internal Auditor)

## Kontakt

**KPMG Advisory**  
**Spółka z ograniczoną odpowiedzialnością sp. k.**  
 ul. Inflancka 4A  
 00-189 Warszawa  
**T:** +48 22 528 11 00  
**F:** +48 22 528 10 09  
**E:** [kpmg@kpmg.pl](mailto:kpmg@kpmg.pl)

**Michał Kurek**  
**Partner**  
 Usługi doradcze  
 Cyberbezpieczeństwo  
**T:** +48 22 528 13 69  
**K:** +48 660 440 041  
**E:** [michalkurek@kpmg.pl](mailto:michalkurek@kpmg.pl)

**Łukasz Staniak**  
**Starszy Menedżer**  
 Usługi doradcze  
 Cyberbezpieczeństwo  
**T:** +48 22 528 34 52  
**K:** +48 605 511 286  
**E:** [lstaniak@kpmg.pl](mailto:lstaniak@kpmg.pl)

**Marcin Strzałek**  
**Menedżer**  
 Usługi doradcze  
 Cyberbezpieczeństwo  
**T:** +48 22 528 10 73  
**K:** +48 539 545 789  
**E:** [mstrzalek@kpmg.pl](mailto:mstrzalek@kpmg.pl)