Bezpieczne finanse w chmurze

Pomoc w zapewnieniu zgodności z postanowieniami Komunikatu UKNF z dnia 23 stycznia 2020 r. 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 przepisami prawa oraz 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:

KPMG oferuje **kompleksową usługę** wsparcia świadczoną przez **interdyscyplinarny zespół ekspertów** z różnych dziedzin. W ramach jednej, dedykowanej usługi, nasi Klienci otrzymają wsparcie w zakresie:

- **cyberbezpieczeństwa** i zarządzania ryzykiem przy przetwarzaniu w chmurze,
- **kwestii prawnych**, w tym dotyczących weryfikacji umów z dostawcami oraz związanych z przetwarzaniem danych osobowych i ich międzynarodowym przepływem,
- tworzenia i wdrażania procedur **dla instytucji finansowych** (Financial Services Advisory).

W celu zapewnienia zgodności z postanowieniami Komunikatu, Eksperci KPMG, w tym radcowie prawni, pomogą w przeprowadzeniu prac związanych z poniższymi zagadnieniami:

Klasyfikacja i ocena informacji

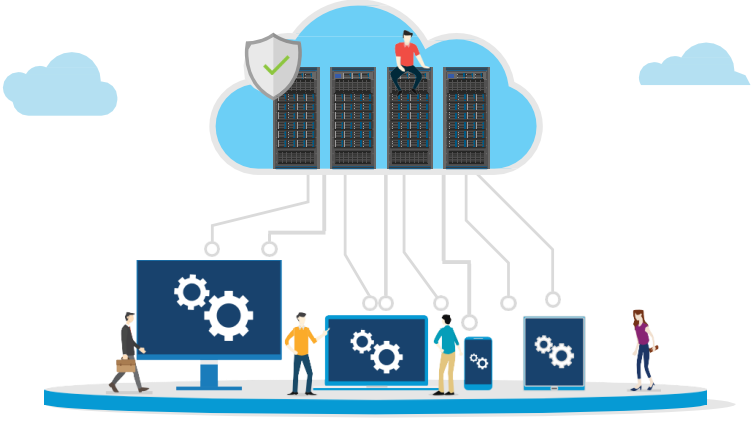
- Weryfikacja obecnie posiadanych polityk i procedur związanych z procesem klasyfikacji informacji.
- W przypadku braku wymaganej dokumentacji lub jej niekompletności, pomoc w przeprowadzeniu zgodnego z Komunikatem udokumentowanego procesu klasyfikacji informacji. Wsparcie prawne przy klasyfikacji informacji jako różnych kategorii informacji prawnie chronionych.
- Weryfikacja obecnej inwentaryzacji danych zawierających informacje prawnie chronione lub wsparcie w jej przygotowaniu.
- Pomoc w ocenie informacji pod kątem dopuszczalności jej przetwarzania w chmurze obliczeniowej.
  Pomoc w ocenie informacji pod kątem zgodności z wymaganiami prawa oraz specyficznymi dla danego sektora lub podmiotu nadzorowanego postanowieniami oraz zobowiązaniami umownymi
- 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 dla 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.
- weryfikacja formalnoprawna umowy z dostawcą usług chmury obliczeniowej pod kątem spełniania wymogów opisanych w treści Komunikatu.
- 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 z obowiązującym prawem** oraz z postanowieniami Komunikatu co umożliwi poinformowanie UKNF o zamiarze przetwarzania lub przetwarzaniu informacji w chmurze obliczeniowej i wykazanie spełnienia wymogów określonych w Komunikacie
- potwierdzenie dla regulatora oraz organów nadzorczych **dochowania należytej staranności** poprzez przeprowadzoną zgodnie z wymogami weryfikację, wykonaną przez niezależny i uznany w branży zespół konsultantów
- **oszczędność zasobów**, dzięki odciążeniu pracowników w tworzeniu dokumentacji związanej z wymaganymi przez Kominikat mechanizmami kontrolnymi

Dlaczego KPMG?

Nasz **interdyscyplinarny zespół** pozwoli dostarczyć **kompleksową usługę** łączącą wiedzę ekspercką z obszaru bezpieczeństwa rozwiązań chmurowych, prawnych aspektów przetwarzania danych w chmurze oraz znajomość specyfiki branży finansowej

Nasi polscy eksperci zrealizowali **kilkaset projektów** dla polskich i zagranicznych przedsiębiorstw z **branży finansowej**

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

Dobrze **rozumiemy technologię chmurową** - nasz zespół składa się z **kilkunastu certyfikowanych inżynierów** bezpieczeństwa środowisk chmurowych

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

Rozumiemy procesy biznesowe, przez co nasze rekomendacje są dostosowane do rzeczywistych potrzeb i wnoszą realnąwartość

Zespół prawny tworzą **radcowie prawni** posiadających doświadczenie w zakresie realizacji projektów dotyczących cyberbezpieczeństwa systemów informatycznych oraz outsourcingu bankowego

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

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**)

Jesteśmy **elastyczni** i dostosowujemy się do zmieniających się dynamicznie potrzebklientów

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 zograniczoną 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

Michał Kurek
Partner
Cyberbezpieczeństwo
T: +48 22 528 13 69
K: +48 660 440 041
E: michalkurek@kpmg.pl

Przemysław Rosiak
Partner Associate
Doradztwo prawne
T: +48 22 528 1331
K: +48 601 826 090
E: pkrosiak@kpmg.pl

Łukasz Staniak
Senior Manager
Cyberbezpieczeństwo
T: +48 22 528 34 52
K: +48 605 511 286
E: lstaniak@kpmg.pl

Michał Sieroń
Associate
Doradztwo prawne
T: +48 22 528 1795
K: +48 605 511 539
E: msieron@kpmg.pl

KPMG Poland

kpmg.pl