Przygotowane jako część projektu finansowanego ze środków Komisji Europejskiej poprzez Służbę ds. Wspierania Reform Strukturalnych

USŁUGI CHMUROWE W SEKTORZE USŁUG PUBLICZNYCH

Wytyczne dla administracji publicznej

KPRM

gt

European Bank for Reconstruction and Development

ashurst MARUTA r3

Wspólna Infrastruktura Informatyczna Państwa („WIIP“)

Wytyczne dla administracji publicznej

KPRM
KANCELARIA PREZESA
RADY MINISTRÓW

SPIS TREŚCI

01. WSTĘP

Niniejszy przewodnik został opracowany w ramach projektu asysty technicznej finansowanej przez Komisję Europejską za pośrednictwem Serwisu Wsparcia Reformy Strukturalnej oraz wdrożony przez Europejski Bank Odbudowy i Rozwoju (EBOR) za pośrednictwem jego Zespołu ds. Transformacji Prawnej. Nadrzędnym celem projektu jest udzielenie wsparcia Kancelarii Prezesa Rady Ministrów RP przy wdrażaniu rozwiązań informatycznych, w tym technologii chmury obliczeniowej, w usługach publicznych oferowanych przez rząd.

1. Jaki jest cel przewodnika?

Przewodnik powstał w ramach realizacji Programu Wspólna Infrastruktura Informatyczna Państwa (dalej: „WIIP") w celu udzielenia wsparcia przy identyfikacji możliwych zastosowań usług chmury obliczeniowej podczas procesu zamawiania nowych bądź aktualizowania istniejących usług informatycznych.

Niniejszy przewodnik informuje odnośnie funkcjonalności chmury obliczeniowej oraz korzyści przyjęcia opartych na niej rozwiązań. Określa on także ramy pomocne w ocenie, jakie dane nadają się do przechowywania w chmurze.

Przewodnik nie wprowadza obowiązku nabywania chmury obliczeniowej podczas zamawiania nowych lub aktualizowaniu istniejących usług informatycznych. W każdym przypadku, organ Administracji publicznej powinien zamówić rozwiązanie, które najlepiej odpowiada jego potrzebom. Pomimo że nie ma przeszkód, aby wybrać alternatywne rozwiązanie, które nie jest oparte na chmurze, zawsze w pierwszej kolejności warto rozważyć i ocenić możliwe rozwiązania chmurowe. Przy wyborze rozwiązania, które nie jest oparte na chmurze, organ powinien być w stanie wykazać, w jaki sposób wybrane rozwiązanie zapewnia odpowiedni poziom bezpieczeństwa, elastyczności i stosunku jakości do ceny w porównaniu z równoważnymi rozwiązaniami w chmurze.

2. Dla kogo jest ten przewodnik?

Przewodnik skierowany jest do administracji publicznej. Może mieć też znaczenie dla szerokiego grona czytelników zaangażowanych w podejmowanie decyzji dotyczących inwestowania w nowe technologie bądź też aktualizowania istniejących rozwiązań technologicznych.

3. Jakie są założenia tego przewodnika?

Próba uzyskania jednoznacznej odpowiedzi na pytanie, czy rozwiązanie chmurowe jest właściwe dla danej usługi, może być trudna. Aby w tym pomóc:

- rozdział „Przegląd Systemów Klasyfikacji" przedstawia w zarysie, jakie systemy klasyfikacji danych i systemów IT zostały wdrożone w ramach WIIP i dlaczego są one ważne przy rozważaniu zastosowania usług chmurowych, natomiast
- rozdział „Podejmowanie decyzji o chmurze" opisuje prosty, 4-etapowy proces pomagający określić, które z posiadanych danych mogą być przetwarzane w chmurze. Rozdział ten jest pomocny przy podejmowaniu decyzji dotyczących nabywania usług IT.

System ZUCH, opracowany w ramach WIIP, również zawiera wskazówki, które pomogą ocenić przydatność technologii chmurowych do zamówień z zakresu IT. Ogólne informacje na temat systemu ZUCH oraz sposobu jego działania znajdują się w Rozdziale 2.

Korzystanie z chmury każe postawić sobie również kluczowe pytania o bezpieczeństwo, prywatność i odporność. Przewodnik omawia te istotne zagadnienia w Rozdziale 5 i 6. Ostatni Rozdział Przewodnika zawiera z kolei odpowiedzi na niektóre z pytań najczęściej zadawanych podczas zamawiania rozwiązań chmurowych.

Znajdujący się na końcu przewodnika słowniczek wyjaśnia kluczowe używane terminy (pisane wielkimi literami).

4. Czym jest chmura obliczeniowa?

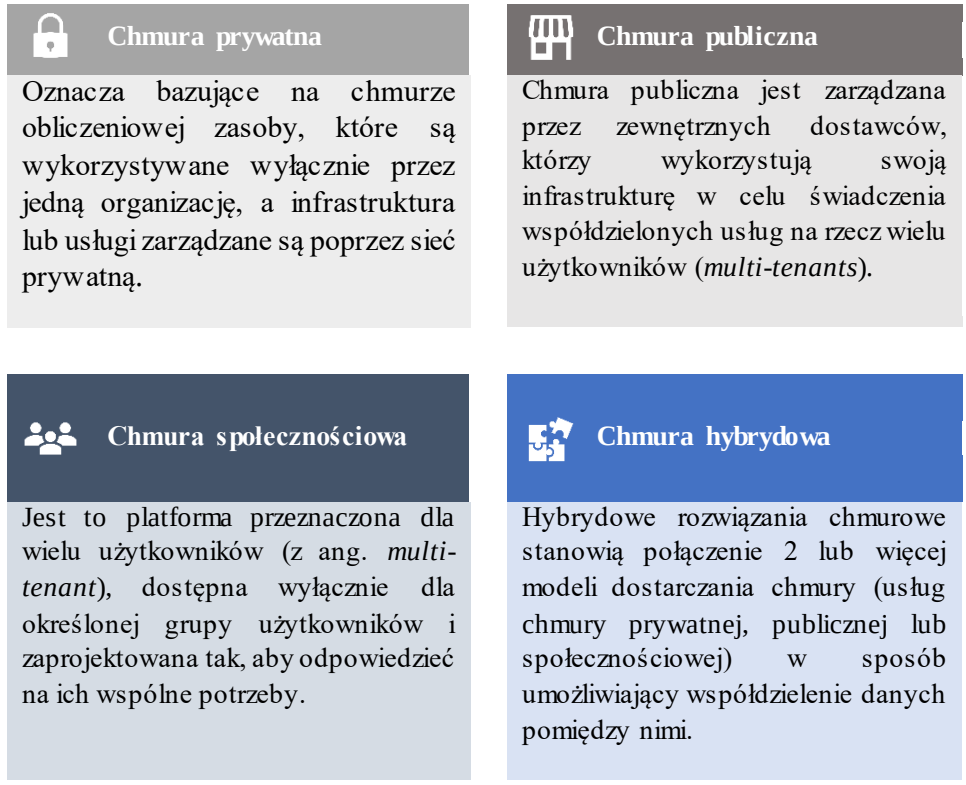
Według Narodowego Instytutu Norm i Technologii (NIST), chmura obliczeniowa jest modelem umożliwiającym powszechny, wygodny dostęp sieciowy na żądanie do wspólnej puli konfigurowalnych zasobów obliczeniowych (np. sieci, serwerów, pamięci masowej, aplikacji i usług), które mogą być szybko dostarczone i uruchomione przy minimalnym wysiłku zarządczym lub interakcją z dostawcą usług. Innymi słowy, chmura obliczeniowa to metoda przechowywania, pobierania i przetwarzania danych oraz uzyskiwania dostępu do oprogramowania przez Internet (lub inne sieci). Zamiast kupować, posiadać i utrzymywać określone aktywa fizyczne – takie jak serwery – lokalnie (z ang. *on-premise*), można uzyskiwać od dostawcy usług chmurowych dostęp do usług technologicznych, takich jak moc obliczeniowa, przechowywanie i aplikacje, w zależności od aktualnych potrzeb. Może to pozwolić na szybsze wprowadzanie innowacji, elastyczne pozyskiwanie zasobów i istotne korzyści skali.

Istnieją trzy główne modele świadczenia usług chmurowych:

- Oprogramowanie jako usługa (z ang. *Software as a Service*, dalej: „SaaS"): umożliwia korzystanie z aplikacji za pomocą Internetu. Przykładami SaaS będą Salesforce i Microsoft Office 365.
- Platforma jako usługa (z ang. *Platform as a Service*, dalej: „PaaS"): dostarcza internetową platformę obliczeniową, na której można rozwijać, testować i wdrażać aplikacje. Przykładami PaaS będą Azure App Service, Heroku, Google App Engine i Openshift.
- Infrastruktura jako usługa (z ang. *Infrastructure as a Service,* dalej: „IaaS"): zapewnia dostęp za pomocą Internetu do zwirtualizowanych zasobów fizycznych, dzięki czemu można rozwijać oprogramowanie bez konieczności zakupu lub konserwacji własnego sprzętu. Przykładami IaaS będą AWS Elastic Compute Cloud, Azure Virtual Machines i Google Compute Engine.

Istnieją również różne modele dostarczania chmury obliczeniowej. Rysunek 1 przedstawia 4 główne modele dostarczania usług chmurowych.

Rysunek 1: *Główne modele dostarczania chmury obliczeniowej*



Jeśli nie wskazano inaczej, zawarte w niniejszym przewodniku odniesienia do chmury oznaczają model dostarczania chmury społecznościowej. Co prawda istnieją okoliczności, w których inne modele dostarczania chmury mogą okazać się właściwsze, ale podstawowe korzyści dla Administracji Publicznej będą realizowane poprzez wykorzystanie chmury publicznej. Ponadto – z uwagi na fakt, że aplikacje SaaS są zazwyczaj łatwiejsze do wdrożenia dla osób niezaznajomionych z chmurą – zaleca się na początku rozważenie usług SaaS, w szczególności przy zamawianiu nowych lub zastępowaniu dotychczasowych rozwiązań IT lub funkcjonalności *back office*.

5. Dlaczego warto używać technologii chmurowych?

Chmura obliczeniowa stanowi inny sposób wdrażania zasobów informatycznych, który oferuje istotne korzyści. Niektóre z ważniejszych z nich to:

5.1 Najlepsze w swojej klasie funkcjonalności

Rozwiązaniom informatycznym typu *on-premise* trudno jest osiągnąć poziom dorównujący temu oferowanemu przez podstawowe produkty chmurowe. Przykładowo przy użyciu rozwiązania *on-premise* nie jest możliwe (a przynajmniej nie jest efektywne kosztowo) zapewnienie nieograniczonej pojemności danych dla wszystkich pracowników Administracji publicznej. Taką możliwość oferują jedynie usługi chmurowe. Rozwiązania chmurowe – w porównaniu do większości alternatywnych rozwiązań typu *on-premise* – mogą umożliwić szerszą współpracę, ułatwiając dzielenie się dokumentami i zdalną pracę and nimi.

5.2 Wsparcie i utrzymanie

Rozwiązania IT typu *on-premise* (zarówno zewnętrzne, jak i wewnętrzne) wymagają odpowiedniego budżetu, wysiłku i planowania w celu zapewnienia wsparcia, utrzymania i aktualizacji. Nadążanie za ciągłym zapotrzebowaniem na aktualizacje i poprawki bezpieczeństwa stanowi wyzwanie. W przypadku Administracji publicznej, które podlegają znacznemu nadzorowi budżetowemu, powstaje ryzyko, że technologia typu *on-premise* stanie się nieaktualna ze względu na koszty i/lub trudności związane z jej wsparciem.

Usługi chmurowe świadczone są zazwyczaj w ramach regularnego programu aktualizacji, poprawek i ulepszeń, przeważnie wliczanych w koszty. Oznacza to, że możliwe jest uniknięcie aktualizacji systemów operacyjnych serwerów, zakupu nowego sprzętu oraz zatrudniania konsultantów w celu utrzymania korzyści związanych z posiadaniem aktualnych technologii.

Rozwiązania nieoparte na chmurze często opierają się na oprogramowaniu „klienckim", zainstalowanym na urządzeniu użytkownika. Oprogramowanie to musi być zarządzane wraz z pozostałymi aplikacjami lokalnymi. W przeciwieństwie do rozwiązań nieopartych na chmurze usługi chmurowe zaprojektowane są w taki sposób, aby umożliwić dostęp do tych usług przez Internet, za pomocą przeglądarki internetowej. W ten sposób ilość aplikacji lokalnych na urządzeniach użytkownika może zostać zminimalizowana. Dla lokalnych organów władzy publicznej, wykorzystujących setki lub nawet tysiące urządzeń takich jak komputery stacjonarne, laptopy i tablety, zmniejszenie ilości oprogramowania zainstalowanego na tych urządzeniach może okazać się korzystne.

5.3 Zapewnienie elastyczności dla przyszłych zastosowań

Rozwijanie rozwiązań typu *on-premise* może w prosty sposób doprowadzić do powstania wysoce zindywidualizowanych, złożonych systemów. To z kolei może utrudnić wspieranie takich rozwiązań, a z czasem doprowadzić do radykalnego zwiększenia kosztów, czasu i ryzyka związanego z realizacją programów rozwoju i zmian w zakresie IT.

Rozwiązania chmurowe są z natury rzeczy ograniczone pod względem liczby dostępnych możliwości indywidualnego dostosowania, ale jednocześnie zapewniają możliwość wyboru konfiguracji. Pozwala to w pewnym stopniu dostosować te rozwiązania do potrzeb klientów, jednakże z pominięciem złożoności infrastruktury. Przykładowo dane z rozwiązań chmurowych są zazwyczaj pobierane za pomocą interfejsów API – co oznacza, że dane te mogą być przenoszone w standardowym, rozpoznawanym formacie w celu łatwiejszej archiwizacji lub migracji do alternatywnych rozwiązań.

5.4 Elastyczność

Nawet najbardziej wydajne rozwiązania typu *on-premise* posiadają ograniczenia w zakresie pojemności zasobów dostępnych dla użytkowników. W miarę jak zapotrzebowanie na usługi będzie rosnąć (przykładowo na skutek zmian w prawie wymagane mogą być dodatkowe zasoby), potrzebne będą regularne inwestycje i nakłady w zakresie zarządzania projektami, aby zapewnić utrzymanie wystarczającej pojemności zasobów. Zarządzanie wysoce zmiennym lub sezonowym zapotrzebowaniem na usługi – takie jak np. składanie deklaracji podatkowych, których szczyt przypada na koniec roku fiskalnego– wymaga zazwyczaj zakupu nadwyżki przepustowości, która poza okresami szczytowymi pozostaje niewykorzystana.

Usługi chmurowe mogą pozwolić na uniknięcie tych wyzwań. Określone zasoby mogą być dostarczane w razie potrzeby i zwalniane wówczas, gdy nie są już potrzebne. To z kolei oznacza, że możliwe jest zapewnienie elastycznej skalowalności w celu zaspokojenia zapotrzebowania na wydajność nawet największych organów Administracji publicznej – bez ponoszenia kosztów utrzymania nadmiarowych zasobów. Zwiększanie skali zazwyczaj nie wiąże się również z żadnymi (lub też wiąże się z marginalnymi) opóźnieniami, nie pociąga za sobą kosztów inwestycji kapitałowych w nowy sprzęt ani też skomplikowanego planowania zasobów lub zarządzania projektami/zmianami.

6. Przegląd korzyści związanych z wykorzystaniem chmury

Podsumowując, korzystanie z chmury oferuje korzyści wykraczające poza te zapewniane przez tradycyjne rozwiązania IT typu *on-premise*. Te potencjalne korzyści zostały podsumowane na Rysunku 2 poniżej.

***Rysunek 2**: Kluczowe korzyści płynące z wykorzystania chmury*

Koszty: Chmura obliczeniowa zmniejsza nakłady kapitałowe w zakresie inwestycji w sprzęt i oprogramowanie, a także koszty zakładania i utrzymania lokalnych centrów danych.

Skala: Chmura obliczeniowa jest elastycznym modelem dostarczania zasobów, co oznacza, że możliwe jest dynamiczne dostosowywanie (zwiększanie i zmniejszanie) jej zasobów w zależności od zapotrzebowania.

Szybkość: Większość produktów chmury obliczeniowej jest oferowana jako usługi samoobsługowe, dostępne na żądanie. Oznacza to, że zasoby chmurowe mogą być dostarczane szybko i elastycznie.

Transparentność: Usługi chmurowe zazwyczaj podlegają pomiarom, dzięki czemu użytkownik ma stały wgląd w poziom zużycia danej usługi. Pomaga to w zarządzaniu budżetem IT.

Wydajność: Usługi chmurowe są regularnie ulepszane w celu zapewnienia szybkiej i wydajnej pracy. Osiągnięcie równoważnego poziomu wydajności usług w przypadku rozwiązań typu *on-premise* może być niezwykle kosztowne.

Produktywność: Centra danych typu *on-premise* wymagają znacznych nakładów wstępnych oraz bieżącego utrzymania. Chmura obliczeniowa przenosi to zadanie na dostawcę, dzięki czemu wewnętrzne zespoły IT mogą skoncentrować się na bardziej strategicznych celach.

02. JAKIE SYSTEMY CHMUROWE SĄ DOSTĘPNE?

1. **Zarys rozdziału**

Niniejszy rozdział opisuje system Zapewniania Usług Chmurowych (ZUCH), stanowiący narzędzie przeznaczone dla organów Administracji publicznej (Administracji rządowej i Lokalnych organów władzy publicznej), służące do przeszukiwania, porównywania i nabywania usług chmurowych.

W dalszej części rozdziału przedstawione zostaną katalog Rządowej Chmury Obliczeniowej (dalej: „**Katalog RChO**”) i katalog Publicznej Chmury Obliczeniowej (dalej: **„Katalog PChO”**) udostępnione w ramach systemu ZUCH, wraz z wyjaśnieniem, w jaki sposób można je wykorzystać do zakupu usług chmurowych przez organ Administracji publicznej.

2. **Wstęp**

Zamawianie usług chmurowych przez organy administracji publicznej nie powinno być procesem złożonym. Niektóre kraje, takie jak Wielka Brytania, Stany Zjednoczone czy Estonia, wdrożyły dedykowaną administracji publicznej politykę *cloud first*, która zachęca, a w niektórych przypadkach nawet nakazuje stosowanie rozwiązań chmurowych jako preferowanego modelu zamówieniowego w zakresie usług informatycznych.

W Wielkiej Brytanii zamówienia na usługi informatyczne realizowane są za pośrednictwem *Digital Marketplace* (tj. portalu służącego do zamawiania usług, w tym usług chmurowych), a usługi chmurowe są nabywane na podstawie z góry określonych umów ramowych z uprzednio zweryfikowanymi dostawcami usług, w ramach modelu G-Cloud.[1]

1.1 Brytyjski model G-Cloud był punktem odniesienia przy powstawaniu programu WIIP. W dniu 24 września 2019 r. przyjęta została uchwała Rady Ministrów w sprawie programu Wspólna Infrastruktura Informatyczna Państwa (WIIP). Program WIIP zakłada zwiększenie bezpieczeństwa danych przetwarzanych w systemach teleinformatycznych Administracji publicznej oraz optymalizację kosztów utrzymania tych systemów, uproszczenie procesów wdrażania e-usług, a także poprawę dostępności obecnie oferowanych usług. Konsolidacja ram organizacyjnych i prawnych oraz opracowanie najlepszych praktyk w zakresie wykorzystania chmury obliczeniowej przyczyni się do zapewnienia wysokiego poziomu usług dostarczanych społeczeństwu przez Administrację publiczną. WIIP promuje polską politykę *cloud first* z uwagi na korzyści, jakie oferują rozwiązania chmurowe przy rozbudowie nowych rozwiązań informatycznych w administracji publicznej. Nie nakazuje w żaden sposób Administracji publicznej stosowanie tych rozwiązań.

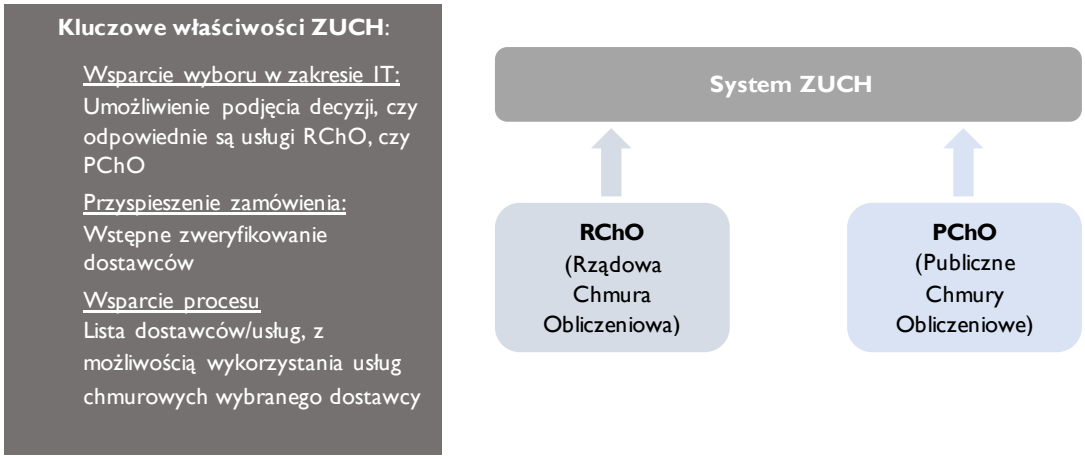
3. **Czym jest system ZUCH i do czego jest wykorzystywany?**

System ZUCH stanowi kluczowy element WIIP. Jest to platforma informatyczna, za pośrednictwem której organy administracji publicznej mogą wyszukiwać i pozyskiwać zweryfikowane pod względem bezpieczeństwa usługi chmurowe, zawarte w katalogach RChO lub

[1] Więcej informacji na ten temat można znaleźć w badaniu: *„Analiza brytyjskiego systemu G-Cloud pod kątem możliwości wdrożenia brytyjskich rozwiązań do polskiego systemu prawnego, w tym ewentualnych ograniczeń w zakresie takiego wdrożenia”*: Analiza brytyjskiego G-Cloud (dostęp na dzień 21 stycznia 2020).

PChO. System ZUCH zapewnia również organom Administracji publicznej dostęp do informacji oraz wsparcie przy zamawianiu usług chmurowych. Rysunek 3 poniżej przedstawia ogólny zarys systemu ZUCH i jego kluczowych charakterystyk:

Rysunek 3: *Zarys systemu ZUCH*



3.1 Katalog RChO

Katalog RChO jest wykorzystywany przede wszystkim do świadczenia usług IaaS, PaaS, DRaaS i SaaS, ale w przyszłości zostanie także rozszerzony o inne usługi chmurowe (takie jak XaaS). Wyznaczonym dostawcą usług chmurowych wymienionych w katalogu RChO jest Minister Cyfryzacji.

Każda z usług wymienionych w katalogu RChO jest indywidualnie oceniana pod kątem zgodności architektonicznej, integralności danych oraz bezpieczeństwa.

3.2 Katalog PChO

Usługi chmurowe wymienione w katalogu PChO są oferowane przez komercyjnych dostawców usług chmurowych, którzy zostali uprzednio zweryfikowani pod względem bezpieczeństwa w następstwie procesu aplikacji.

Oferowanie i zamawianie usług chmurowych z katalogu PChO składa się na dwuetapowy proces. Najpierw, aby usługa została wymieniona w katalogu PChO, dostawca usług chmurowych musi zostać zweryfikowany pod względem bezpieczeństwa Proces weryfikacji składa się z następujących etapów:

(a) Dostawca usług chmurowych składa aplikację wraz z zapewnieniami oraz (jeżeli zostanie do tego wezwany) dokumentację, która wykazuje spełnienie wymagań procesu zamówień formułowanych przez Administrację publiczną, w tym SCCO – Cyberbezpieczeństwo w Chmurze Obliczeniowej (C3) Poziomy wpływu – C3IL (por. Rozdział 3 poniżej);

(b) Usługi dostawcy usług chmurowych są następnie weryfikowane pod kątem spełnienia wymogów bezpieczeństwa zgodnie z SCCO.

Organ Administracji publicznej chcący nabyć daną usługę chmurową – po opublikowaniu zapytania ofertowego – wybierze jednego ze zweryfikowanych zgodnie z powyższymi kryteriami dostawców usług chmurowych i uzgodni z nim umowę wdrożeniową oraz umowę ramową na konkretną usługę będącą przedmiotem zamówienia. Proces

zamówieniowy zostaje przeprowadzony przez Administrację publiczną poza systemem ZUCH, zgodnie z prawem zamówień publicznych (por. pkt 5 niniejszego Rozdziału).

Lista dostawców usług chmurowych wymienionych w katalogu PChO jest okresowo uaktualniana. Katalog PChO obejmuje usługi odnoszące się do elementów zamieszczonych na rysunku 4 poniżej.

Rysunek 4: *Przegląd systemu ZUCH*

	Maszyna wirtualna	DNS	System Nazw Domen (z ang. *Domain Name System*, DNS)
	Przestrzeń dyskowa		Firewall Aplikacji Sieciowej (z ang. *WEB Application Firewall*, WAF)
	Brama Sieciowa VPN		Firewall
	Sieć prywatna		Sieć Dostarczania Treści (z ang. *Content Delivery Network*, CRN)
	Dodatkowe IP		System Zarządzania Kluczami (z ang. *Key Management System*, KMS)
	Równoważnik obciążeń (z ang. *Load Balancer*)		System operacyjny
	Środowisko kontenerowe (z ang. *Container environment)*		Baza danych

4. Kto może korzystać z systemu ZUCH?

System ZUCH, łącznie z usługami wymienionymi w katalogach RChO i PChO, jest dostępny dla wymienionych poniżej kategorii podmiotów:

a) podmioty sektora finansów publicznych, o których mowa w art. 9 ust. 1-13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2019 r., poz. 869)[2];

b) inne państwowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, banków i spółek prawa handlowego;

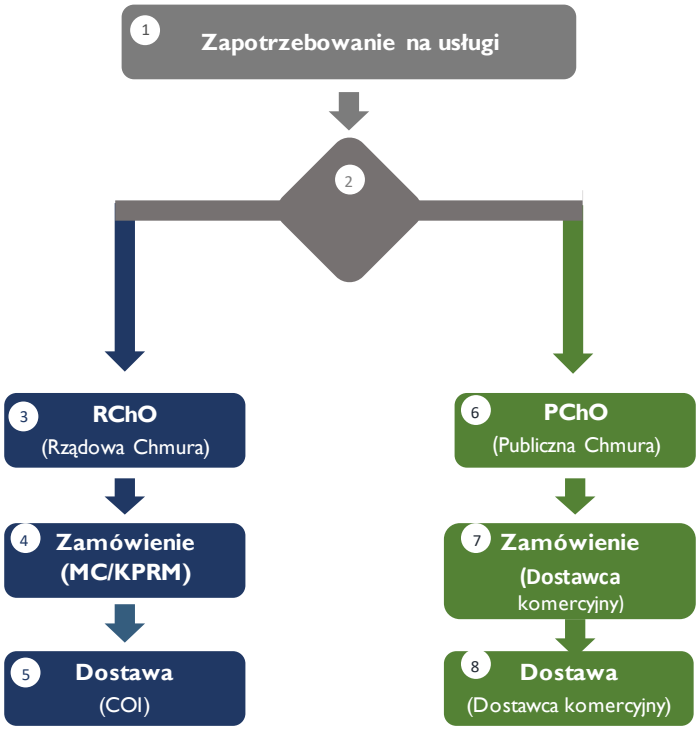
c) nieposiadające osobowości prawnej państwowe jednostki organizacyjne inne niż określone w ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych, np. Państwowe Gospodarstwo Leśne „Lasy Państwowe".

[2] Podmiotami sektora finansów publicznych, o których mowa w art. 9 ust. 1 - 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, są następujące podmioty: organy władzy publicznej, w tym organy rządowe, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały; jednostki samorządu terytorialnego i ich związki; związki metropolitalne; jednostki budżetowe; jednostki budżetowe samorządów terytorialnych; agencje wykonawcze; instytucje gospodarki budżetowej; fundusze państwowe; Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze, Kasa Rolniczego Ubezpieczenia Społecznego oraz fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego; Narodowy Fundusz Zdrowia; samodzielne publiczne jednostki ochrony zdrowia; uczelnie publiczne; Polska Akademia Nauk i jej jednostki organizacyjne; państwowe i samorządowe instytucje kultury.

5. **Jak mogę skorzystać z systemu ZUCH w celu nabycia usług chmurowych?**

Kluczową częścią funkcjonalności systemu ZUCH jest zapewnienie centralnego wsparcia przy zamawianiu usług chmurowych. Administracja publiczna może wykorzystać system ZUCH, jako pomoc przy ocenie, czy chmura obliczeniowa jest odpowiednia dla tworzonego (lub aktualizowanego) przez ten organ rozwiązania informatycznego. Jeżeli chmura obliczeniowa jest odpowiednia, wówczas proces kwalifikacji systemu (SCCO) wskaże, katalog usług (tj. Katalog RChO lub Katalog PChO) z którego powinien skorzystać organ do pozyskania odpowiedniej usługi od dostawcy chmurowego. Po zidentyfikowaniu odpowiedniego katalogu usług, system ZUCH przeprowadzi użytkownika przez proces zamówienia. Proces ten został przedstawiony na Rysunku 5.

Rysunek 5:
Proces zamówienia w systemie ZUCH



Każdy z etapów powyższego procesu został wyjaśniony poniżej:

1. **Zapotrzebowanie na usługi:** odnosi się do sytuacji, gdy w danej organizacji pojawia się biznesowa potrzeba rozważenia, czy rozwiązanie chmurowe jest odpowiednie – tj. albo jako nowa usługa informatyczna albo jako aktualizacja już istniejącej usługi informatycznej.

2. **Kwalifikacja systemu**: w tym kroku w systemie ZUCH należy określić podstawowe informacje dotyczące zamawianej usługi informatycznej. Na podstawie tych informacji oraz klasyfikacji danych WIIIP, proces kwalifikacji SCCO zidentyfikuje, czy usługa chmurowa jest w danym przypadku odpowiednim rozwiązaniem, a jeśli tak, to czy powinna zostać pozyskana z katalogu RChO, czy z katalogu PChO.

3. **Rządowa Chmura Obliczeniowa – RChO**: w tym kroku należy określić bardziej szczegółowe wymagania wobec zamawianej infrastruktury IT, w tym konkretne

wymagania niezbędne do zaspokojenia potrzeb biznesowych organizacji (przykładowo oczekiwane maszyny wirtualne i ich parametry, wielkość wymaganej przestrzeni dyskowej itp.).

4. **Zamawianie usług (MC/KPRM)**: po określeniu wymagań usługi są zamawiane. Na tym etapie operator RChO potwierdza swoją gotowość do świadczenia usług w określonym zakresie.

5. **Dostawa usług (Centralny Ośrodek Informatyki – COI)**: zamówione usługi są dostarczane do organu Administracji publicznej, która następnie może przejąć kontrolę nad konfiguracją udostępnionej jej infrastruktury chmurowej. Konfiguracja infrastruktury chmurowej odbywa się za pomocą narzędzi udostępnionych użytkownikowi przez operatora RChO.

6. **Publiczna Chmura Obliczeniowa – PChO**: ten etap wymaga szczegółowego określenia wszystkich wymagań wobec zamawianego systemu informatycznego, w tym wskazanie konkretnych usług chmurowych, które są konieczne do zaspokojenia potrzeb biznesowych organu. Na tym etapie organ Administracji publicznej powinien:

   - posiadać informacje odnośnie dostępności systemu informatycznego lub usługi chmurowej w katalogu PChO i możliwości ich ewentualnego nabycia oraz określić szczegółowe oczekiwania dotyczące usługi informatycznej, która będzie świadczona i utrzymywana przez jednego z uprzednio zweryfikowanych pod względem bezpieczeństwa dostawców chmury PChO;

   - ustalić szacunkowy budżet na usługi, które mają być pozyskane. W związku z tym, oprócz konkretnych wymagań technicznych, należy określić również kryteria, które będą brane pod uwagę przy wyborze najlepszej oferty.

7. **Zamawianie usług (dostawca komercyjny):** po określeniu wymogów następuje proces zamawiania usługi. Na tym etapie, wymagania użytkownika wraz z prośbą o wycenę są przekazywane potencjalnym dostawcom usług chmurowych, zarejestrowanym w systemie ZUCH. Dostawcy usług chmurowych mogą odpowiedzieć na zapytanie ofertowe, podając konkretną wycenę dla wszystkich wybranych i skonfigurowanych usług. System ZUCH automatycznie wskaże najlepszą ofertę od dostawców usług chmurowych w oparciu o podane przez organ Administracji publicznej wymagania. Końcowym elementem tego etapu jest podpisanie umowy wdrożeniowej dotyczącej danej usługi lub usług chmurowych pomiędzy wybranym dostawcą organem Administracji publicznej. Zawarcie umowy następuje poza systemem ZUCH, zgodnie z prawem zamówień publicznych.

8. **Dostawa usług (dostawca komercyjny)**: na tym etapie zamówiona usługa lub usługi chmurowe są dostarczane do użytkownika, który w ramach dostępnych zasobów może przejąć kontrolę nad konfiguracją udostępnionych mu usług. Konfiguracja usług chmurowych odbywa się za pomocą narzędzi udostępnionych użytkownikowi przez dostawcę.

6. **Jakie są zalety korzystania z systemu ZUCH?**

System ZUCH oferuje szereg korzyści:

(a) Podstawową zaletą systemu ZUCH jest umożliwienie organom Administracji publicznej **łatwego i szybkiego wyszukiwania usług chmurowych**, przy jednoczesnym umożliwieniu monitorowania i kontroli parametrów świadczenia usług – takich jak koszty, wymogi techniczne (w tym dotyczące bezpieczeństwa) oraz wymogi prawne.

i. Szybkość i prostota procesu zakupu redukują koszty oraz skracają czas potrzebny na zamówienie usług chmurowych –zarówno po stronie Administracji publicznej, jak i po stronie dostawców usług.

ii. Proces weryfikacji pod względem bezpieczeństwa dostawców oferujących usługi chmurowe na systemie ZUCH, gwarantuje najwyższy poziom bezpieczeństwa i przejrzystości oraz **zmniejsza ryzyko oszustw i korupcji.**

iii. System ZUCH **promuje również konkurencję** między dostawcami usług chmurowych, umożliwiając większej liczbie dostawców ubieganie się o prekwalifikację oraz – po jej przejściu – udział w procesie zamówień.

iv. Korzystanie z systemu ZUCH **gwarantuje zgodność z obowiązującymi przepisami prawa**.

7. **Czy jest obowiązek korzystania z ZUCH?**

Nie. System ZUCH oferuje liczne korzyści, jednak korzystanie z niego nie jest obowiązkowe dla organów Administracji publicznej. Nadal możliwe jest nabywanie przez nie usług chmurowych poza system ZUCH, w ramach obowiązujących regulacji prawa zamówień publicznych.

8. **Jak dołączyć do systemu ZUCH?**

Dostęp do systemu ZUCH można uzyskać za pośrednictwem oficjalnej strony internetowej: https://chmura.gov.pl

Na stronie znajdują się również dalsze informacje oraz wskazówki dotyczące platformy i korzystania z niej.

03. PRZEGLĄD KLASYFIKACJI SYSTEMÓW TELEINFORMATYCZNEGO I INFORMACJI

1. **Jaki jest cel klasyfikacji systemów teleinformatycznych i informacji?**

Klasyfikacja obejmuje identyfikację rodzajów poszczególnych zbiorów danych, które organ Administracji publicznej gromadzi, generuje, przyjmuje, przechowuje, przetwarza lub przekazuje (dalej łącznie: **„przetwarzanie”**), oraz przypisanie każdego zbioru danych do konkretnej kategorii potencjalnego wpływu na bezpieczeństwo w oparciu kryteria, wymagania oraz cele bezpieczeństwa informacji określone w SCCO.

Podstawowym celem sklasyfikowania informacji do konkretnej kategorii po jest umożliwienie zarządzania i kontrolowania danych przetwarzanych z wykorzystaniem usług chmur obliczeniowych, zgodnie z wcześniej określonymi zasadami i standardami mającymi zastosowanie do danej kategorii. Głównym celem stosowania tych zasad i standardów jest zapewnienie odpowiedniego poziomu bezpieczeństwa informacji. Tym niemniej, klasyfikacja danych może być również przydatna do zapewnienia zgodności z obowiązującymi wymogami prawnymi, do których przestrzegania zobowiązany jest organ Administracji publicznej lub przy wdrażaniu szerszej strategii zarządzania danymi.

W kontekście wdrażania chmury, zaproponowana klasyfikacja systemów teleinformatycznych i informacji zapewnia istotne ramy do oceny, które zbiory danych wykorzystywane przez organ Administracji publicznej mogą być przetwarzane w chmurze oraz z którego katalogu usług w ramach systemu ZUCH należy zamówić odpowiednią usługę chmurową (zob. Rozdział 2: „Jakie systemy chmurowe są dostępne?").

2. **Dlaczego klasyfikacja systemów teleinformatycznych i informacji jest ważna?**

2.1 <u>Zarządzanie ryzykiem</u>

Klasyfikacja systemów teleinformatycznych i informacji, które mają być przetwarzane z wykorzystaniem usług chmur obliczeniowych, ustanawia ramy do oceny ryzyka i potencjalnego wpływu, jakie miałoby nieuprawnione ujawnienie, zniszczenie lub zakłócenie, na bezpieczeństwo danych przetwarzanych w chmurze obliczeniowej.

Identyfikacja tego ryzyka i potencjalnego wpływu na bezpieczeństwo danych, może umożliwić zapewnienie proporcjonalnego, podstawowego poziomu zabezpieczeń w odniesieniu do wszystkich danych przetwarzanych przez organ Administracji publicznej. Klasyfikacja zwiększa spójność sposobu przetwarzania i ochrony danych pomiędzy organami Administracji publicznej, a także umożliwia zewnętrznym doradcom lepsze zrozumienie szerszego kontekstu przetwarzania danych, co może pomóc w zarządzaniu ryzykiem.

2.2 <u>Zarządzanie łańcuchem dostaw</u>

Istotną korzyścią klasyfikacji systemów teleinformatycznych i informacji, które mają być przetwarzane z wykorzystaniem usług chmur obliczeniowych jest możliwość kontroli nad minimalnymi wymogami i standardami bezpieczeństwa dotyczącymi każdej kategorii informacji w ramach klasyfikacji.

2.3 Efektywność

Klasyfikacja pozwala na bardziej efektywne przetwarzanie danych. Tylko te, które w ramach klasyfikacji zostaną uznane za generujące największe ryzyko, powinny zostać objęte najwyższymi zabezpieczeniami. W przypadkach, w których informacje zakwalifikowane będą jako związane z najniższym ryzykiem, będzie można polegać na podstawowej warstwie bezpieczeństwa.

Nadmierna kontrola bezpieczeństwa powoduje zwiększenie złożoności przetwarzania danych, a tym samym powoduje wzrost kosztów. Zastosowanie kontroli bezpieczeństwa proporcjonalnej do rzeczywistego ryzyka oraz wprowadzenie minimalnych wymogów i standardów bezpieczeństwa pozwala na redukcję kosztów i istotne oszczędności.

2.4 Dostępność

Dane które określone zostaną zgodnie z klasyfikacją, jako należące do kategorii niskiego ryzyka, mogą być przeznaczone do publicznego udostępnienia e bez prawnych wymagań dotyczących zachowania poufności lub z minimalną kontrolą dostępu.

Umożliwienie szerszego dostępu do informacji o niskim poziomie potencjalnego wpływ na bezpieczeństwo może pomóc w promowaniu szerszych celów, takich jak wspieranie inicjatyw z zakresu otwartych danych, wspieranie konkurencji rynkowej i innowacji lub stymulowanie handlu i możliwości badawczych poprzez wykorzystanie danych przez strony trzecie.

2.5 Możliwość wyszukiwania

Zastosowanie klasyfikacji może sprawić, że dane staną się bardziej czytelne, łatwiejsze do oceny i śledzenia. Usprawnienie całościowej kontroli może pozwolić na zaoszczędzenie czasu i optymalizację pozyskiwania danych, co jest szczególnie ważne przy zapewnianiu zgodności prawnej regulacji obowiązujących u organu Administracji publicznej, np. w zakresie wniosków zawierających dane osobowe lub wniosków o udostępnienie informacji publicznej.

3. Klasyfikacja systemów teleinformatycznych i informacji

3.1 Struktura klasyfikacji

Klasyfikacja systemów teleinformatycznych i informacji została szczegółowo opisana w SCCO – Standardy Cyberbezpieczeństwa Chmur Obliczeniowych[3] *Poziomy wpływu* – C3IL. Istnieją 4 poziomy wymogów bezpieczeństwa SCCO:

- SCCO1: Poziom wpływu 1 – Niekontrolowane informacje nieklasyfikowane;
- SCCO2: Poziom wpływu 2 – Kontrolowane informacje urzędowe;
- SCCO3: Poziom wpływu 3 – Kontrolowane wrażliwe informacje urzędowe;
- SCCO4: Poziom wpływu 4 – Informacje niejawne (zastrzeżone, poufne, tajne i wyższe) – niezawarte w WIIP.

[3] Ang. *Cloud Computing Cybersecurity Standards (C3)*

W niniejszym rozdziale omówione zostaną szczegóły 1, 2 i 3 poziomu bezpieczeństwa SCCO. 4 poziom bezpieczeństwa SCCO nie jest częścią klasyfikacji systemów teleinformatycznych i informacji[4] i nie został szerzej opisany w niniejszych wytycznych.

3.2 SCOO1: Poziom wpływu 1 – Niekontrolowane informacje nieklasyfikowane

- Dozwolone przetwarzanie w Chmurze publicznej[5]
- Obejmuje wszystkie dane przeznaczone do publicznego udostępnienia, o niskim poziomie poufności
- Dozwolony dostęp do usług przez Internet
- Zawiera informacje publiczne, które:
  - nie zawierają danych osobowych chronionych przez RODO
  - nie stanowią informacji prawnie chronionych
  - mogą być związane z ograniczeniami w zakresie prawa autorskiego
- Konsekwencje ujawnienia:
  - brak negatywnych konsekwencji dostępu osób nieupoważnionych lub skutków prawnych związanych z prawem autorskim.

3.3 SCCO2: Poziom wpływu 2 – Kontrolowane informacje urzędowe

- Przetwarzanie w Chmurze publicznej dozwolone jest przy zachowaniu polskiej jurysdykcji (zarówno miejsca przetwarzania, jak i same dane)
- Zawiera dane istotne dla ustawowego funkcjonowania Administracji publicznej, dostępne bez ograniczeń dla pracowników instytucji lub na podstawie umów o zachowaniu poufności
- Zawiera informacje publiczne, które:
  - zawierają dane osobowe podlegające ochronie ustawowej (RODO)
  - zawierają tajemnicę przedsiębiorców, w tym chronione tajemnice handlowe / tajemnicę przedsiębiorstwa
- Konsekwencje ujawnienia informacji:
  - negatywne konsekwencje nieautoryzowanego dostępu mogą obejmować naruszenie RODO, nieuprawnione ujawnienie tajemnic handlowych (np. tajemnicy przedsiębiorstwa), a w konsekwencji pociągnąć za sobą sankcje ustawowe (np. art. 23 Ustawy o dostępie do informacji publicznej).

3.4 SCCO3: Poziom wpływu 3 – Kontrolowane wrażliwe informacje urzędowe

- Wyłącznie Rządowa Chmura Obliczeniowa
- Poziom 3 obejmuje wrażliwe, prawnie chronione informacje oraz dane referencyjne z rejestrów krajowych, określone w odrębnych przepisach (w tym dane o kluczowym znaczeniu dla bezpieczeństwa publicznego).

3.5 Klasyfikacja systemów teleinformatycznych

Przetwarzanie informacji w modelach chmury obliczeniowej wymaga dostosowania procesów zarządzania ryzykiem, zwykle obejmujących lokalne zasoby fizyczne, systemy i aplikacje.

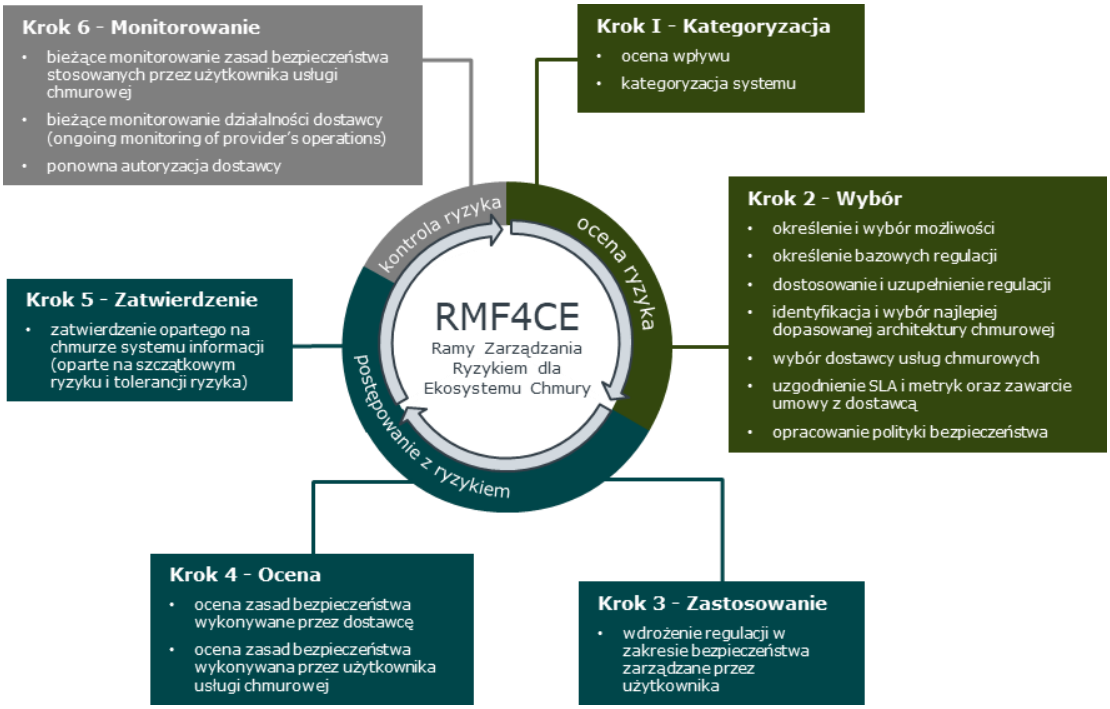
[4] Przetwarzanie takich informacji regulują odrębne przepisy (Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych), które zakazują przetwarzania tych informacji w środowiskach nieakredytowanych przez właściwe organy bezpieczeństwa.

[5] Przetwarzanie w Chmurze Publicznej jest dozwolone na terenie UE.

Proces oceny ryzyka w zakresie migracji informacji w celu ich przetwarzania w modelach przetwarzania w chmurze obliczeniowej koncentruje się na ocenie wymogów dla poziomów potencjalnego wpływu na bezpieczeństwo informacji. Przy wyborze oferty dostawcy usług chmury obliczeniowej, potencjalni odbiorcy usług kierują się potrzebami operacyjnymi i funkcjonalnymi oraz weryfikują ich zgodność z wymogami SCCO na poziomie odpowiadającym klasyfikacji systemu i informacji, które mają być przetwarzane z wykorzystaniem usług chmury obliczeniowej.

Proces zarządzania ryzykiem związany z przetwarzaniem informacji w modelach chmury opisany jest w poniższym cyklu Ram Zarządzania Ryzykiem (z ang. *Risk Management Framework*, dalej: RMF).

Rysunek 6: *NIST: Ramy zarzadzania ryzykiem dla ekosystemu chmury*



Opisany powyżej proces RMF (schemat 6-stopniowy) umożliwia administracji publicznej usystematyzowane stosowanie i monitorowanie wspólnych, hybrydowych i właściwych dla bezpieczeństwa informatycznego systemów oraz formułowanie wymogów bezpieczeństwa na potrzeby zamówień publicznych dotyczących świadczenia usług w modelach chmury obliczeniowej.

04. PODEJMOWANIE DECYZJI O PRZETWARZANIU W CHMURZE

1. Praktyczne kroki przy zastosowaniu klasyfikacji

Rysunek 7 poniżej przedstawia najważniejsze zalecane kroki, które powinno się rozważyć przy zastosowaniu klasyfikacji danych przetwarzanych przez Administrację publiczną (zob. Rozdział 8 – Słownik definicji pojęć pisanych wielkimi literami na Rysunku 7). Poniższa procedura ma za zadanie wesprzeć Administrację publiczną w zarządzaniu ryzykiem podczas klasyfikowania danych przeznaczonych do przetwarzania w rozwiązaniach opartych na chmurze.

Rysunek 7: *Praktyczne kroki przy klasyfikacji*

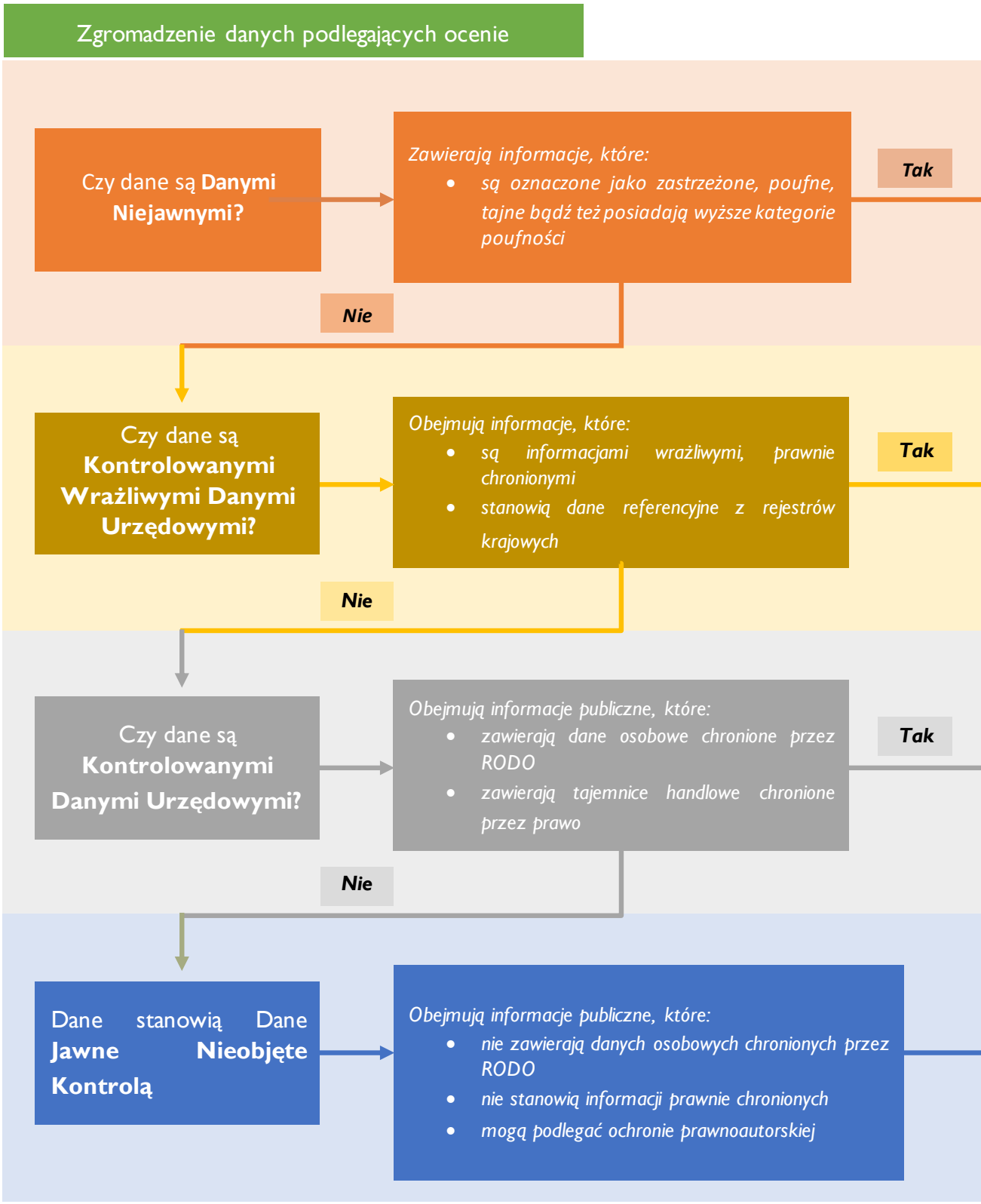
Zalecany krok	Zarys działań
1 Określenie danych objęte zakresem Przetwarzania	• Zidentyfikowanie wszystkich danych, które będą Przetwarzane przez proponowane rozwiązanie chmurowe (z ang. *in-scope data*, dalej: „dane objęte zakresem”). • Określenie, która metodyka klasyfikacji jest najodpowiedniejsza do zastosowania w odniesieniu do danych objętych zakresem. Wielkość zidentyfikowanych danych objętych zakresem oraz ich charakter (np. czy są to dane ustrukturyzowane, czy nieustrukturyzowane) pomoże określić, czy odpowiednia jest Klasyfikacja oparta na użytkowniku, Klasyfikacja oparta na atrybutach czy też Metodyka klasyfikacji hybrydowej. • Po dokonaniu klasyfikacji, należy użyć właściwych kategorii danych do określenia skutków prawnych i regulacyjnych, które będą miały zastosowanie wobec danych objętych zakresem.
2 Określenie przypadku wykorzystania chmury	• Określenie wymagań dotyczących proponowanego rozwiązania chmurowego. • Zweryfikowanie wymagań z perspektywy zidentyfikowanych kategorii danych dla danych objętych zakresem (wraz z wszelkimi innymi potencjalnymi czynnikami, które nie są objęte klasyfikacją, takimi jak np. dostępność lub integralność danych). • Określenie podejścia do ryzyka (gotowość na akceptację ryzyka) zidentyfikowanie ryzyka, które będzie nie do przyjęcia w sytuacji, gdy określone wymagania nie zostaną spełnione.
3 Wyznaczenie kluczowych standardów bezpieczeństwa i środki kontroli	• Zastosowanie właściwej kategorii danych dla danych objętych zakresem, w celu określenia, jakie standardy bezpieczeństwa i środki kontroli są wymagane od dostawcy usług chmurowych w danym przypadku korzystania z chmury. • Należy zwrócić uwagę na wymagania użytkownika i ocenę gotowości do akceptacji ryzyka.

4 Potwierdź, w jaki sposób wymagania bezpieczeństwa zostaną wdrożone i udokumentowane	• Organ powinien poprosić potencjalnego dostawcę (potencjalnych dostawców) usług chmurowych o potwierdzenie:
	  ○ w jaki sposób zostaną wdrożone standardy bezpieczeństwa i środki kontroli odpowiednie dla każdej z kategorii danych oraz
	  ○ w jaki sposób dostawca usług chmurowych wykaże, że te standardy/kontrole zostały prawidłowo wdrożone.
	• Organ powinien zrozumieć wszelkie ryzyka, które wynikają z odpowiedzi dostawcy.

5	Zidentyfikuj dodatkowe środki mitygujące ryzyko, które możesz zastosować	• Rozważenie wprowadzenia dodatkowych środki mitygujące ryzyko, które organ (jako użytkownik usług chmurowych) może zastosować, aby pomóc w zminimalizowaniu zidentyfikowanego ryzyka w odniesieniu do każdej z kategorii danych.
6	Oceń wszystkie pozostałe ryzyka	• Ocena czy ewentualne inne ryzyka (których nie można wyeliminować przy zastosowaniu innych środków) są akceptowalne w odniesieniu do konkretnych danych, przy uwzględnieniu kategorii danych, do której dane ryzyko się odnosi.

Zastosowanie klasyfikacji względem danych Schemat przedstawiony na Rysunku 8 poniżej ma za zadanie ułatwić poruszanie się po zagadnieniach kluczowych do określenia, które z kategorii danych powinny znaleźć zastosowanie wobec danego zbioru danych objętych zakresem.

Rysunek 8: *Zastosowanie klasyfikacji względem danych*



Danych niejawnych nie można umieszczać **w jakiejkolwiek chmurze.**

Dane te muszą być przechowywane w bezpiecznej lokalizacji fizycznej z zastosowaniem wszystkich wymaganych środków bezpieczeństwa.

Można umieścić w chmurze Kontrolowane Wrażliwe Dane Urzędowe, **ale tylko**:

- w **rządowej chmurze społecznościowej oraz**
- jeżeli infrastruktura chmurowa należy do administracji publicznej.

Zatwierdzone usługi chmurowe dla Kontrolowanych Wrażliwych Danych Urzędowych można znaleźć w katalogu **RChO** w systemie ZUCH.

Można umieścić Kontrolowane Dane Urzędowe w chmurze **publicznej lub prywatnej**, ale:

- dane muszą pozostać na terenie Polski (tj. chmura musi być hostowana w Polsce, a transfery danych nie mogą być dokonywane poza Polskę) oraz
- każdy z dostawców chmury publicznej musi zapewnić, że jego **serwery pozostaną w Polsce.**

Zatwierdzone usługi chmurowe dla Kontrolowanych Danych Urzędowych można znaleźć w katalogu **RChO** oraz **PChO** w systemie ZUCH.

Można umieścić Dane Jawne Nieobjęte Kontrolą w **chmurze publicznej.**

Nie obowiązują żadne restrykcje dotyczące lokalizacji, w których chmura może być utrzymywana.

Zatwierdzone usługi chmurowe dla Danych Jawnych Nieobjętych Kontrolą można znaleźć w katalogu **PChO** w systemie ZUCH.

05. WZGLĘDY BEZPIECZEŃSTWA I PRYWATNOŚCI

1. **Zarys rozdziału**

Ta część przewodnika zawiera wskazówki dotyczące ochrony danych i środków cyberbezpieczeństwa związanych z wdrożeniem i wykorzystaniem technologii chmury obliczeniowej. Opisuje ona również niektóre problemy dotyczące Przetwarzania Danych Osobowych w chmurze oraz zawiera proponowane rozwiązania tych problemów.

2. **W jaki sposób regulacje dotyczące ochrony Danych Osobowych odnoszą się do usług chmurowych?**

RODO stosuje się we wszystkich przypadkach Przetwarzania Danych Osobowych. Jeżeli organ Administracji publicznej jest Administratorem Danych Osobowych, obowiązywać go będą regulacje RODO dotyczące Przetwarzania Danych Osobowych niezależnie od tego, czy Dane Osobowe są Przetwarzane poza chmurą, czy też zostały do niej przeniesione.

3. **Identyfikacja Administratorów i Podmiotów Przetwarzających dane w chmurze**

Jedną z powszechnie wyrażanych obaw jest to, czy autonomia dostawcy usług chmurowych oznacza, że dana instytucja zamawiająca usługę nie będzie zakresu kontroli nad operacjami Przetwarzania, pozwalającego jej działać jako Administrator Danych Osobowych Przetwarzanych w chmurze. Jednakże tak długo, jak długo to dana organizacja będzie określać *środki* i *cele* Przetwarzania, tak długo to ona będzie Administratorem z punktu widzenia RODO – a dostawca usług chmurowych będzie działał jako Podmiot Przetwarzający (tzn. będzie Przetwarzał Dane Osobowe w imieniu organizacji).

Administracja publiczna musi określić *środki i cele* Przetwarzania w każdym przypadku, w którym będzie decydowała o jednym lub kilku z działań przedstawionych na Rysunku 9 poniżej. Instytucja nie musi być prawnie zobowiązania do wykonywania tych czynności, a im więcej takich czynności będzie wykonywać, tym większe jest prawdopodobieństwo, że będzie Administratorem tych Danych Osobowych, których dotyczy Przetwarzanie.

Rysunek 9: *Wskaźniki Administrowania*

	Podejmowanie decyzji o zbieraniu Danych Osobowych
	Podejmowanie decyzji o podstawie prawnej Przetwarzania
	Podejmowanie decyzji o rodzajach Danych Osobowych, które są zbierane
	Podejmowanie decyzji o celach, do których Dane Osobowe są wykorzystywane
	Podejmowanie decyzji, od jakich Podmiotów Danych uzyskiwać Dane Osobowe
	Podejmowanie decyzji o ujawnieniu Danych Osobowych oraz o tym, komu zostaną one ujawnione
	Podejmowanie decyzji o sposobie odpowiedzi na Wnioski Osób, których dane dotyczą
	Podejmowanie decyzji o tym, jak długo przechowywać Dane Osobowe i kiedy je zmieniać
	Podejmowanie decyzji o tym, jakie informacje o Przetwarzaniu Danych należy przekazać Osobom, których Dane dotyczą

Oprócz Przetwarzania Danych Osobowych w celu świadczenia usług chmurowych niektórzy dostawcy usług chmurowych mogą Przetwarzać Dane Osobowe w celu wykonywania czynności pomocniczych. Typowe czynności pomocnicze obejmują zarządzanie kontami, badania i analizy lub wykrywanie oszustw. Zazwyczaj to dostawca usług chmurowych określa *środki i cele* Przetwarzania Danych Osobowych na potrzeby dodatkowych czynności (pomocniczych) – wówczas, to dostawca usług chmurowych stanie się Administratorem Danych Osobowych na potrzeby tych dodatkowych działań. W takich okolicznościach dostawca usług chmurowych będzie:

(a) Podmiotem Przetwarzającym w instytucji Administracji publicznej w odniesieniu do Przetwarzania, które dostawca usługi chmurowej prowadzi w celu świadczenia usługi chmurowej, oraz

(b) Administratorem, na własny rachunek, w odniesieniu do Danych Osobowych, które Przetwarza w związku z czynnościami pomocniczymi, i jako Administrator będzie odpowiedzialny na podstawie RODO za przestrzeganie RODO w odniesieniu do tych czynności pomocniczych.

Biorąc powyższe pod uwagę, ważne jest, aby zarówno role i obowiązki organu Administracji publicznej, jak i role i obowiązki dostawcy usługi chmurowej były jasno określone w odpowiedniej umowie chmurowej.

4. Wybór dostawców usług chmurowych: kluczowe kwestie w zakresie ochrony Danych Osobowych

4.1 Środowiska wielu użytkowników

Środowisko wielu użytkowników występuje w sytuacji, gdy dostawca usług chmurowych kształtuje swój produkt w taki sposób, że wielu klientów (dalej: „**Użytkowników**") ma dostęp do tego samego środowiska w chmurze i dzieli je w tym samym czasie, ale są oni odpowiednio oddzieleni poprzez własny interfejs użytkownika, własne zasoby i usługi.

Powszechna obawa związana z wykorzystaniem chmury dotyczy tego, w jaki sposób Dane Osobowe są chronione w środowiskach wielu użytkowników. Istnieje przekonanie, że potencjalne podatności polityki dostępu dostawcy usługi chmurowych lub też środków kontroli bezpieczeństwa mogłyby doprowadzić do tego, że Użytkownik uzyska dostęp do Danych Osobowych innego Użytkownika.

Aby ograniczyć to ryzyko, przy wyborze dostawcy usług chmurowych należy zweryfikować:

(a) czy i w jaki sposób dostawca usług chmurowych oddzieli środowisko chmury organu Administracji publicznej od innych Użytkowników. Można tego dokonać przykładowo poprzez wdrożenie fizycznego rozdzielenia różnych Użytkowników bądź poprzez wykorzystanie różnych maszyn wirtualnych dla danych każdego z Użytkowników w ramach tego samego serwera;

(b) jakie szyfrowanie jest stosowane w odniesieniu do Danych nieaktywnych / w spoczynku (ang. *data at rest*) i Danych w trakcie przesyłu w chmurze. Jeżeli kluczami do szyfrowania zarządza dostawca usług chmurowych, organ Administracji publicznej powinien sprawdzić, czy zostaną wprowadzone odpowiednie środki bezpieczeństwa w celu ochrony tych kluczy w czasie, gdy znajdują się one w posiadaniu dostawcy, oraz

(c) czy dostawca usług chmurowych posiada zaświadczenie pochodzące z jednego lub większej liczby uznanych chmurowych systemów certyfikacji, potwierdzające, że odpowiednio poradzi sobie z tym ryzykiem.

Niektórzy dostawcy usług chmurowych w środowiskach wielu użytkowników mogą być niechętni do przyznania daleko idących uprawnień w zakresie audytu swoim Użytkownikom, powołując się na trudności praktyczne oraz ryzyko dla bezpieczeństwa i integralności danych innych Użytkowników. W celu uzyskania dalszych szczegółów – zob. pkt 6.3 poniżej.

4.2 Kwestie związane z niezawodnością i odpornością

Biorąc pod uwagę specjalistyczny charakter usług chmurowych, większość głównych dostawców chmury zapewnia wysoki poziom odporności i niezawodności, będący zazwyczaj powyżej poziomu oferowanego przez większość tradycyjnych rozwiązań typu *on-premise*. Z tego względu usługa chmurowa może zaoferować Administracji publicznej wyższy poziom dostępności i odporności.

Tym niemniej, zgodnie z RODO, instytucja nadal będzie musiała wykazać i udokumentować, że dokonała oceny, w jaki sposób integralność i dostępność jej Danych Osobowych będzie chroniona w środowisku chmurowym. W związku z tym należy dokonać przeglądu polityki dostawcy usług chmurowych pod kątem ciągłości działania i usuwania skutków awarii oraz przeprowadzić dodatkową techniczną analizę *due diligence* w zakresie stosowanych przez dostawcę środków zapewnienia ciągłości działania i usuwania skutków awarii (w celu zapewnienia zdolności dostawcy do zaspokojenia potrzeb instytucji dotyczących niezawodności i odporności). Może to obejmować żądanie od dostawcy usług chmurowych informacji o wszelkich wcześniejszych doznanych awariach oraz o tym, w jaki sposób zarządza on zmiennością zapotrzebowania na wydajność zgłaszaną przez swoich klientów.

Większość dostawców usług chmurowych będzie tworzyć kopie zapasowe danych przekazywanych do chmury (w tym Danych Osobowych) w częstych, regularnych odstępach czasu (nierzadko w czasie rzeczywistym lub zbliżonym do rzeczywistego), korzystając ze zmiennych awaryjnych centrów danych (dalej: „**Obiekt Rezerwowy**"). Takie działanie stanowi jeden ze środków zapewniania ciągłości działania i usuwania skutków awarii przez dostawców usług chmurowych. Należy sprawdzić zapewnienia dostawcy usług chmurowych w zakresie procesu tworzenia kopii zapasowych oraz zabezpieczeń na wypadek awarii, w tym zapewnienia dotyczące wskaźników docelowego czasu odzyskiwania (z ang. *Recovery Time Objective*, dalej: „RTO") i akceptowalnego poziomu utraty danych (z ang. *Recovery Point Objective*), w celu upewnienia się, że odpowiadają one potrzebom instytucji. Należy również potwierdzić lokalizację każdego Obiektu Rezerwowego – zarówno w celu zapewnienia, że jest ona dostatecznie oddalona od głównego centrum danych obsługującego usługę chmurową, jak i w celu zapewnienia, że jeśli Obiekt Rezerwowy znajduje się poza Polską i/lub EOG, w celu zapewnienia zgodności z ograniczeniami transferowymi i wymogami lokalizacyjnymi RODO (zob. pkt 4.3 poniżej) umowa chmurowa obejmuje odpowiednie postanowienia w tym zakresie. Korzyścią z pozyskiwania usług chmurowych za pośrednictwem systemu ZUCH (zob. Rozdział 2) jest to, że wspomniana powyżej weryfikacja jest dokonywana przez centralny organ zamawiający, a niezbędne wymogi dotyczące ciągłości działania zawarte są w umowie ramowej z zatwierdzonymi dostawcami usług chmurowych.

Oprócz zapewnienia niezawodności i odporności oferowanych przez dostawcę usług chmurowych, organ Administracji publicznej powinien rozważyć wprowadzenie środków mających na celu zminimalizowanie potencjalnych skutków poważnej awarii.

4.3 Rozwiązania chmurowe utrzymywane poza Polską/EOG

Uchwała WIIP (tj. Uchwała dotycząca Wspólnej Infrastruktury Informatycznej Państwa) przewiduje klasyfikację systemów w zależności od przetwarzanych w nich informacji oraz dopasowuje te systemy do modeli chmurowych, które mogą znaleźć zastosowanie w odniesieniu do danego systemu. Określa ona również terytorium, na którym dane powinny być przetwarzane. W celu uzyskania większej ilości szczegółów dotyczących klasyfikacji systemów informatycznych w ramach Uchwały WIIP zob. Rozdział 4 przewodnika. Niezależnie od powyższego zastosowanie znajdą ogólne przepisy RODO dotyczące transferu danych poza EOG, chyba że Uchwała przewiduje bardziej rygorystyczny system.

W 2013 r. poprzedni organ nadzorczy (tj. Generalny Inspektor Ochrony Danych Osobowych) przedstawił wytyczne dotyczące korzystania z chmury obliczeniowej przez urzędy administracji publicznej („**Wytyczne dotyczące chmury obliczeniowej z 2013 r.**"). Zgodnie z tymi wytycznymi organ powinien dysponować wiedzą w zakresie wszystkich lokalizacji, w których Dane Osobowe są przechowywane przez dostawcę usług chmurowych (niezależnie od tego, czy taka lokalizacja znajduje się w Polsce, w EOG, czy gdziekolwiek indziej). Wytyczne dotyczące chmury obliczeniowej z 2013 r. nie są dokumentem wiążącym. Administracja publiczna powinna przy każdej okazji zweryfikować czy – biorąc pod uwagę szacowany poziom ryzyka – istnieje potrzeba potwierdzenia lokalizacji fizycznych serwerów dostawcy usługi chmurowej. Lokalizacja nie musi być określona za pomocą dokładnego adresu i zazwyczaj jest określana ogólnie, według regionu (np. Europa) lub kraju.

5. Kluczowe obowiązki

Poniższy punkt wyjaśnia niektóre z głównych obowiązków Administracji publicznej przy rozważaniu umieszczenia Danych Osobowych w chmurze. Więcej informacji w tym zakresie dostępnych jest w dokumencie „Wytyczne w zakresie wykorzystania usług chmury obliczeniowej przez instytucje i organy europejskie".

5.1 Ocena i udokumentowanie ryzyka w zakresie ochrony danych

Przed przeniesieniem Danych Osobowych do chmury instytucja Administracji publicznej musi ocenić ryzyko związane z ochroną Danych w ramach proponowanego rozwiązania chmurowego. W szczególności musi ocenić, jakie ryzyko (ryzyka) dane rozwiązanie może tworzyć dla praw i wolności Osób, których dane dotyczą. Ocena ta powinna obejmować:

(a) charakter Danych Osobowych, które mają być Przetwarzane w chmurze;

(b) rodzaj Przetwarzania, które ma być wykonywane w chmurze, wraz ze wskazaniem, czy stwarza ono szczególnie wysokie ryzyko, takie jak w przypadku zautomatyzowanego podejmowanie decyzji i profilowania;

(c) zakres Przetwarzania, czyli na przykład liczbę rekordów zawierających Dane Osobowe lub liczbę Osób, których dane dotyczą, oraz

(d) środki bezpieczeństwa stosowane przez planowanego dostawcę usług chmurowych, a także jego reputację rynkową oraz weryfikację rękojmi zastosowania odpowiednich środków w całym okresie obowiązywania umowy.

Należy również ocenić, jakie środki mogą zostać podjęte w celu zmitygowania zidentyfikowanych obszarów ryzyka. W przypadku stwierdzenia, że nie można zmitygować jednego lub większej ilości obszarów ryzyka, należy zdecydować, czy dana usługa chmurowa będzie właściwa, biorąc pod uwagę istnienie tego ryzyka.

W celu wykazania zgodności z określoną w RODO zasadą rozliczalności, rekomenduje się, aby przy przeprowadzaniu oceny skutków dla ochrony danych (z ang. *Data Protection Impact Assessment*, dalej: „**DPIA**"), Administracja publiczna udokumentowała przeprowadzoną ocenę ryzyka, wszelkie działania mitygujące, które należy podjąć, oraz ostateczną decyzję w tym przedmiocie. Czynności te powinny zostać dokonane, jako część projektu wdrożenia usług chmurowych.

Należy zauważyć, że zgodnie z RODO przeprowadzenie DPIA jest obowiązkowe w sytuacjach, kiedy Przetwarzanie Danych może wiązać się z wysokim ryzykiem dla praw i wolności Osób, których dane dotyczą, w szczególności w przypadku zastosowania nowych technologii. Biorąc pod uwagę powyższe, przeprowadzenie DPIA prawdopodobnie okaże się obowiązkowe przy większości projektów obejmujących duże ilości Danych Osobowych znajdujących się w środowisku chmurowym (w szczególności, kiedy dotyczyć będzie którejkolwiek ze Szczególnych Kategorii Danych Osobowych). Zespół do spraw ochrony danych osobowych / prywatności w organie Administracji publicznej może udzielić dalszych porad w zakresie sposobu, w jaki DPIA będzie przeprowadzane.

Tak jak w przypadku każdego obowiązkowego DPIA, Administracja publiczna powinna zapewnić, że DPIA w odniesieniu do każdego planowanego projektu chmurowego zawiera, co najmniej:

(a) ocenę konieczności i proporcjonalności Przetwarzania w stosunku do jego celów;

(b) ocenę ryzyka dla praw i wolności Osób, których dane dotyczą, oraz

(c) środki przewidziane w celu przeciwdziałania tym ryzykom, w tym zabezpieczenia i środki bezpieczeństwa (w szczególności zabezpieczenia i środki bezpieczeństwa stosowane przez planowanego dostawcę usług chmurowych).

Należy również mieć świadomość, że organy nadzorcze w państwach członkowskich UE opublikowały wykaz rodzajów operacji Przetwarzania Danych, do których wymagane jest DPIA w poszczególnych jurysdykcjach. Wykaz opublikowany przez polski organ nadzoru, tj. Prezesa Urzędu Ochrony Danych Osobowych, nie odnosi się bezpośrednio do kwestii operacji Przetwarzania w chmurze w zakresie odnoszącym się do Administracji publicznej. Tym niemniej należy pamiętać, że Prezes Urzędu Ochrony Danych Osobowych wymaga przeprowadzenia DPIA w różnych okolicznościach, w tym w odniesieniu do:

(a) systemów monitorujących przeznaczonych do kontrolowania ruchu;

(b) komunalnych systemów wypożyczania rowerów/samochodów;

(c) monitoringu miejskiego;

(d) operacji Przetwarzania Danych związanych z przynależnością polityczną;

(e) różnego rodzaju rejestrów centralnych (m.in. rejestrów uprawnień dla poszczególnych zawodów);

(f) systemów informatycznych informujących o nieprawidłowościach (tzw. *whistleblowing*);

(g) Przetwarzania Danych mającego zastosowanie do Internetu rzeczy (z ang. *Internet of things*, IoT), w celu świadczenia usług komunalnych.

Pełna lista zdarzeń, w przypadku których należy przeprowadzić DPIA, jest dostępna pod adresem: http://monitorpolski.gov.pl/MP/2019/666. W odniesieniu do wymienionych powyżej operacji Przetwarzania Danych istnieje duże prawdopodobieństwo, że organ Administracji publicznej będzie zobowiązany do przeprowadzenia DPIA bez względu na to, czy przy tych operacjach korzysta z usługi chmurowej, czy też nie.

Należy również przeprowadzić dodatkowe DPIA w szczególności w przypadku, w którym po przeniesieniu Danych Osobowych do chmury charakter, zakres, kontekst lub cel Przetwarzania w chmurze ulegną zmianie mogącej stwarzać ryzyka dla praw i wolności Osób, których dane dotyczą.

5.2 Informowanie Osób, których dane dotyczą, o Przetwarzaniu w chmurze

Po przekazaniu Danych Osobowych do chmury, organ Administracji publicznej powinien rozważyć aktualizację treści klauzul informacyjnych w zakresie Przetwarzania Danych Osobowych. Przykładowo, może zaistnieć potrzeba aktualizacji odbiorców bądź też kategorii odbiorców Danych Osobowych wymienionych w klauzulach informacyjnych w zakresie Przetwarzania Danych Osobowych, w celu uwzględnienia w nich również dostawcy usług chmurowych. Osoby, których dane dotyczą, musiałyby zostać poinformowane również wtedy, kiedy ich Dane Osobowe zostałyby przeniesione do lokalizacji znajdującej się poza EOG (zob. pkt 4.3 powyżej).

5.3 Monitorowanie dostawcy usług chmurowych oraz działań Dalszego Podmiotu Przetwarzającego

Po wdrożeniu wybranego rozwiązania chmurowego nadal należy monitorować sposób wykonywania przez dostawcę usług chmurowych (oraz wszystkich Dalszych Podmiotów Przetwarzających zaangażowanych przez dostawcę usług chmurowych) jego obowiązków wynikających z umowy chmurowej. Obejmuje to monitorowanie środków technicznych i organizacyjnych oraz innych zabezpieczeń określonych w umowie chmurowej w celu zapewnienia, że Dane Osobowe w dalszym ciągu są odpowiednio chronione.

Audyty stanowią kluczową część procesu monitorowania. Bardziej szczegółowe omówienie audytów Danych Osobowych w kontekście rozwiązań chmurowych znajduje się w pkt 6.3 poniżej.

5.4 Szkolenie pracowników

Organ Administracji publicznej musi zapewnić swoim pracownikom odpowiednie szkolenia w następującym zakresie:

(a) w jaki sposób właściwie korzystać z wybranej usługi chmurowej, w tym jak korzystać z wszelkich jej narzędzi lub funkcji, które mają związek z obowiązkami nałożonymi na Administrację publiczną na podstawie RODO w zakresie ochrony lub przechowywania Danych Osobowych, a także rozpatrywania wniosków od Osób, których dane dotyczą, oraz

(b) w jaki sposób monitorować działanie wybranego dostawcy usług chmurowych (zob. pkt 5.4 powyżej).

Szkolenie powinno być przeprowadzone dla wszystkich właściwych pracowników. Zwykle będzie oznaczało to osoby mające regularny dostęp do Danych Osobowych w chmurze, kierownika(ów) umowy chmurowej, osobę(y) decyzyjną(e) oraz zespoły ds. informatyki i bezpieczeństwa.

5.5 Usługi chmurowe a wnioski od Osób, których dane dotyczą

Przenoszenie Danych Osobowych do chmury nie powinno uniemożliwiać Osobom, których dane dotyczą, składania Wniosków dotyczących tych Danych, jak również wpływać na wynikającą z RODO odpowiedzialność w zakresie udzielania odpowiedzi na te Wnioski. Dlatego też należy

zapewnić możliwość obsługiwania Wniosków osób, których dotyczą dane przetwarzane w chmurze.

Jeżeli dostawca usług chmurowych działa, jako Podmiot Przetwarzający instytucji będącej Administratorem (zob. pkt 3), to zgodnie z RODO jest on zobowiązany do udzielenia pomocy w obsłudze Wniosków osób, których dane dotyczą. Niezależnie od tego ważne jest też, aby określić w umowie chmurowej zakres pomocy udzielanej przez dostawcę usług chmurowych. W szczególności organ Administracji publicznej powinien potwierdzić, czy za pomocą narzędzi lub funkcji chmury będzie miała wystarczająco dużo kontroli, aby bezpośrednio obsługiwać Wnioski osób, których dane dotyczą (np. poprzez możliwość skorygowania Danych Osobowych przechowywanych w chmurze za pomocą interfejsu webowego), oraz czy istnieją okoliczności, w których instytucja będzie musiała poinstruować dostawcę, aby w jej imieniu obsługiwał niektóre Wnioski osób, których dane dotyczą.

Jeżeli organ Administracji publicznej będzie musiał zlecić dostawcy usług chmurowych, aby w jego imieniu obsłużył niektóre Wnioski osób, których dane dotyczą, umowa chmurowa powinna nakładać na dostawcę określone ramy czasowe wykonania takich działań oraz wyraźnie określać, że nie może on odpowiadać bezpośrednio na te Wnioski, chyba że zostanie odmiennie poinstruowany.

Jeśli wybrane rozwiązanie chmurowe oferuje narzędzia lub funkcje, które umożliwiają bezpośrednią obsługę Wniosków osób, których dane dotyczą, organ Administracji publicznej będzie musiał zapewnić, że:

(a) rozumie sposób działania tych narzędzi i funkcji;

(b) wszyscy właściwi pracownicy zostali odpowiednio przeszkoleni w zakresie tych narzędzi (zob. pkt 5.5) oraz

(c) aktualizuje swoją obecną politykę lub procedury w zakresie odpowiedzi na Wnioski osób, których dane dotyczą, w celu uwzględnienia:

(i) tych narzędzi lub funkcji oraz

(ii) sposobu, w jaki może odpowiedzieć na Wniosek osoby, której dane dotyczą, jeżeli te narzędzia lub funkcje nie działają lub stały się niedostępne (w tym wsparcia udzielanego w takiej sytuacji przez dostawcę usług chmurowych).

6. Zawieranie umów w chmurze – względy praktyczne

6.1 Postanowienia obligatoryjne

Jeżeli dostawca usług chmurowych działa jako Podmiot Przetwarzający (zob. pkt 3), należy zawrzeć w umowie chmurowej odpowiednie postanowienia, aby spełnić wymogi określone w art. 28 ust. 3 RODO. Artykuł ten wymaga wprowadzenia określonych obligatoryjnych postanowień umownych pomiędzy Administratorami a Podmiotami Przetwarzającymi w celu zapewnienia, że na Podmioty Przetwarzające zostały nałożone minimalne obowiązki w odniesieniu do Przetwarzanych przez nich Danych Osobowych (dalej: „**Postanowienia obligatoryjne**").

Powszechnym wyzwaniem w tym zakresie jest fakt, że niektórzy z największych dostawców usług chmurowych bywają wyraźnie niechętni do odstępowania od swoich standardowych warunków umownych. Chociaż przyjmowane przez nich standardowe warunki kontraktowe w większości przypadków są zgodne z Postanowieniami obligatoryjnymi, niektórzy z dostawców mogą

przyjmować wąską interpretację niektórych Postanowień obligatoryjnych lub zapewniać jedynie

minimalny standard wymaganych obowiązków. Postanowienia obligatoryjne zazwyczaj obejmują postanowienia dotyczące bezpieczeństwa, audytu, usuwania i przechowywania Danych Osobowych, jak również obowiązki związane z Naruszeniami Danych Osobowych. Zostaną one omówione poniżej.

Uchwała WIIP wymaga, aby niektóre Dane Przetwarzane w chmurze podlegały polskiej jurysdykcji lub jurysdykcji innego kraju członkowskiego UE (więcej informacji znajduje się w Rozdziale 3 przewodnika – „Przegląd systemów klasyfikacji").

6.2 Odpowiednie techniczne i organizacyjne środki bezpieczeństwa w chmurze

RODO wymaga, aby:

v. Administracja publiczna zapewniała stosowanie technicznych i organizacyjnych środków bezpieczeństwa w celu ochrony Danych Osobowych, aby środki te były odpowiednie do ryzyka związanego z Przetwarzaniem tych Danych Osobowych, oraz

vi. aby Administracja publiczna korzystała wyłącznie z tych Podmiotów Przetwarzających, którzy stosują odpowiednie środki techniczne i organizacyjne w celu Przetwarzania Danych Osobowych.

Oznacza to, że jeżeli Dane Osobowe mają być Przetwarzane w chmurze, Administracja publiczna będzie musiała zapewnić, że techniczne i organizacyjne środki bezpieczeństwa dostawcy usług chmurowych są odpowiednie i będą stosowane w celu ochrony Danych Osobowych.

Rysunek 10 przedstawia niektóre z powszechnie występujących obszarów ryzyka w zakresie bezpieczeństwa, które mogą pojawić się w kontekście rozwiązań chmurowych. Jeżeli takie ryzyka bezpieczeństwa wystąpią, organ Administracji publicznej będzie musiał dopilnować, aby odpowiednie środki techniczne i organizacyjne – zarówno własne, jak i zapewniane przez dostawcę usług chmurowych – odpowiednio te ryzyka uwzględniały.

Rysunek 10: *Powszechnie występujące ryzyka w zakresie bezpieczeństwa*

Ryzyko	Powszechnie stosowane środki techniczne i organizacyjne
Ryzyko związane z **poufnością** i **integralnością** Danych Osobowych podczas przesyłania (ang. *data in transit*) przez Internet.	• Wdrażanie wirtualnych sieci prywatnych (z ang. *Virtual Private Network*, VPN). • Silne protokoły szyfrujące, takie jak HTTPS.
Awarie Internetu prowadzące do problemów z **dostępnością.**	• Korzystanie z wielu dostawców usług internetowych. • Posiadanie dodatkowych łączy od tego samego dostawcy usług internetowych. • Zakupienie dedykowanego łącza danych w celu zapewnienia niezakłóconej, trwałej łączności z rozwiązaniem chmurowym zamiast korzystania z Internetu.
Możliwe **uzależnienie od jednego dostawcy** chmury i **ograniczona możliwość** przejścia do innego dostawcy.	• Testowanie rozwiązania (rozwiązań) alternatywnych. • Okresowe tworzenie kopii zapasowych Danych Osobowych poza rozwiązaniem chmurowym. • Opracowanie planu migracji w celu umożliwienia zmiany dostawców usług chmurowych w razie pilnej konieczności rezygnacji z usługi.
Potencjalne podatności w polityce dostępu lub środkach kontroli bezpieczeństwa powodujące **nieuprawniony dostęp** do Danych Osobowych w organizacji.	• Zapewnienie, że dostawca usług chmurowych odizoluje środowisko chmury organu Administracji publicznej od innych Użytkowników (np. poprzez fizyczną segregację lub korzystanie z różnych maszyn wirtualnych pomiędzy Użytkownikami). • Zapewnienie odpowiedniego szyfrowania w chmurze danych nieaktywnych (ang. *data at rest*) i przesyłanych (ang. *data in transit*). • Korzystanie z usług dostawcy chmury posiadającego wydany przez niezależny podmiot certyfikat potwierdzający, że stosuje on właściwe środki kontroli tożsamości i zarządzania dostępem.

Ze względu na ustandaryzowany charakter usług chmurowych ich dostawcy zazwyczaj korzystają ze znacznej autonomii w zakresie środków technicznych i organizacyjnych, które wdrażają w celu ochrony Danych Osobowych. W rezultacie przed przeniesieniem jakichkolwiek Danych Osobowych do wybranego rozwiązania chmurowego instytucja powinna upewnić się, że standardy bezpieczeństwa dostawcy usług chmurowych są zarówno odpowiednie, jak i wystarczające dla Danych Osobowych, które zamierza Przetwarzać w chmurze. Organ Administracji publicznej może to uczynić poprzez:

(a) wymaganie, aby dostawca usług chmurowych udostępniał swoje certyfikaty i standardy dotyczące bezpieczeństwa – powszechnie stosowane certyfikaty to ISO 27001 (standard dotyczący systemów zarządzania bezpieczeństwem informacji), ISO 27017 (kodeks praktyk w zakresie kontroli bezpieczeństwa informacji dla usług chmurowych) oraz ISO 27018 (kodeks praktyk w zakresie ochrony informacji umożliwiających identyfikację osób w chmurach publicznych) – oraz

(b) wgląd w raporty z przeprowadzonych audytów dostawcy usług chmurowych, oceniających skuteczność przyjętych środków technicznych i organizacyjnych w świetle wskazanych powyżej standardów/norm, w celu zapewnienia bezpieczeństwa Przetwarzania (zob. pkt 6.3 poniżej dot. audytów).

Oprócz przeprowadzenia opisanego powyżej badania *due diligence* w zakresie środków technicznych i organizacyjnych zapewnianych przez dostawcę usług chmurowych organ powinien dokonać również przeglądu własnych wewnętrznych procedur kontroli tożsamości i zarządzania dostępem – w celu zapewnienia, że będą one odpowiednie w odniesieniu do proponowanego rozwiązania chmurowego. Co do zasady przejście na rozwiązanie chmurowe zapewni pracownikom Administracji publicznej większą elastyczność w dostępie do Danych Osobowych przechowywanych w chmurze z różnych lokalizacji i urządzeń. Przykładowo pracownicy będą mogli uzyskać dostęp do danych na urządzeniu mobilnym za pośrednictwem bezpiecznego portalu VPN podczas pracy zdalnej, spoza głównego biura, co może ułatwić wprowadzenie elastycznych zasad pracy, takich jak praca z domu. Często to właśnie ta elastyczność nie znajduje pełnego odzwierciedlenia w przypadku środków kontroli tożsamości i zarządzania dostępem przeprowadzanych poza chmurą. Jest to zatem kluczowy obszar, który organ powinien sprawdzić w celu zrozumienia, jakie protokoły uwierzytelniania są wykorzystywane przez rozwiązanie chmurowe oraz w jaki sposób konta użytkowników/środki uwierzytelnienia mogą być tworzone, aktualizowane i usuwane.

6.3 Audyt

Postanowienia Obligatoryjne (zob. pkt 6.1) mają zastosowanie w stosunku do Podmiotów Przetwarzających w równym stopniu, niezależnie od tego, czy świadczą oni usługi w środowisku chmurowym, czy też poza chmurą. W związku z tym Postanowienia Obligatoryjne w zakresie audytu powinny zobowiązywać dostawcę usług chmurowych do:

(a) dostarczenia organowi wszystkich informacji niezbędnych do wykazania, że obowiązki dostawcy usług chmurowych przewidziane przez RODO zostały wypełnione, oraz

(b) zezwolenia na przeprowadzanie audytów i inspekcji przez organ (lub audytora wyznaczonego przez organ) oraz współdziałania w przeprowadzeniu tych audytów i inspekcji.

Oczywistym celem wspomnianych powyżej Postanowień Obligatoryjnych jest zapewnienie, aby organ Administracji publicznej (jako Administrator) miał praktyczne możliwości skutecznego monitorowania wykonywania obowiązków umownych / zgodności dostawcy usług chmurowych zarówno z umową chmurową, jak i z RODO. Dostawcy usług chmurowych często jednak starają się ograniczyć bądź też zawęzić swoje obowiązki w zakresie audytu, szczególnie w środowiskach wielu użytkowników (zob. pkt 4.1). Dostawcy argumentują, że przyznanie wielu Użytkownikom prawa do fizycznej kontroli ich lokali lub systemów tworzyłoby niedopuszczalne ryzyko operacyjne i w zakresie bezpieczeństwa. Ryzyko to może być kontrolowane, jeżeli zamiast audytu na miejscu klienci będą mogli skorzystać z informacji dostarczonych przez dostawcę usług chmurowych w celu sprawdzenia, czy przestrzega on określonych w umowie chmurowej obowiązków w zakresie bezpieczeństwa.

Jest to rozwiązanie pragmatyczne, niepokrywające się z literalnym brzmieniem Postanowień Obligatoryjnych RODO. Przyjęty pogląd zakłada, że postanowienia tego rodzaju mogą być wystarczające pod warunkiem, że:

(a) audytorzy dostawców usług chmurowych są niezależni i odpowiednio akredytowani;

(b) raporty z audytu obejmują wszystkie aspekty zgodności z ochroną danych istotne dla konkretnego przypadku Przetwarzania, w tym środki techniczne i organizacyjne wdrożone przez dostawcę usług chmurowych, oraz

(c) jeżeli dostawca usług chmurowych zaangażował Dalsze Podmioty Przetwarzające, raporty z audytu obejmują również zgodność tych Dalszych Podmiotów Przetwarzających.

6.4 Retencja i usuwanie Danych

Administracja publiczna zobowiązana jest do Przetwarzania Danych Osobowych tylko tak długo, jak długo są one potrzebne do celów, do których są gromadzone. Oznacza to, że Dane Osobowe muszą zostać usunięte, gdy nie są już potrzebne. Ponadto w szczególnych okolicznościach Osoby, których dane dotyczą, mają prawo do żądania usunięcia tych Danych Osobowych, a organ będzie odpowiedzialny na podstawie RODO za zapewnienie, że żądania te zostaną wykonane. Wymogi te powinny zostać zaadresowane w polityce przechowywania danych organu Administracji publicznej.

Dostawcy usług chmurowych zazwyczaj przechowują kopie Danych Osobowych w różnych lokalizacjach w ramach swojego środowiska, w celu optymalizacji procesów operacyjnych, takich jak zwiększenie odporności lub zmniejszenie opóźnień występujących w rozwiązaniu chmurowym. Może to jednak stwarzać wyzwanie w zakresie zapewnienia, że wszystkie kopie Danych Osobowych przechowywane w całym środowisku usługi chmurowej zostaną trwale usunięte, gdy nie będą już potrzebne lub w odpowiedzi na Wniosek Osoby, której dane dotyczą, o usunięcie tych Danych.

Organ Administracji publicznej powinien sprawdzić, czy wybrane rozwiązanie chmurowe zapewnia narzędzia lub funkcje umożliwiające realizację polityki przechowywania Danych, a także zapewnić, że wszyscy pracownicy zaangażowani w zarządzanie Danymi Osobowymi są odpowiednio przeszkoleni w zakresie rozwiązania chmurowego.

Aby zapewnić zgodność z Postanowieniami obligatoryjnymi, umowa chmurowa musi zobowiązywać dostawcę usług chmurowych do bezpiecznego usunięcia lub zwrotu Danych

Osobowych na żądanie organu Administracji publicznej lub po zakończeniu świadczenia usług. Niektórzy dostawcy usług chmurowych mogą dążyć do spełnienia tego wymogu poprzez umożliwienie instytucji bezpośrednio doprowadzenia do takiego usunięcia lub uzyskania Danych Osobowych za pomocą narzędzi lub funkcji rozwiązania chmurowego. Jest to dopuszczalne z punktu widzenia zgodności z RODO pod warunkiem, że umowa chmurowa potwierdza, że wszystkie kopie Danych Osobowych przechowywane w rozwiązaniu chmurowym mogą zostać usunięte lub możliwe jest uzyskanie ich za pomocą udostępnionych narzędzi lub funkcji.

Jeśli to tylko możliwe, należy dążyć do uwzględnienia w umowie chmurowej:

(a) konkretnych terminów, w których dostawca będzie zobowiązany do zwrotu lub usunięcia Danych Osobowych;

(b) obowiązku zapewnienia, że wszelkie Dane Osobowe, które są zwracane lub możliwe do uzyskania, będą miały określony format, w celu umożliwienia przeniesienia Przetwarzania z powrotem do własnych zasobów lub do innego dostawcy usług chmurowych, oraz

(c) obowiązku, aby dostawca usług chmurowych po skutecznym dokonaniu zwrotu bądź usunięcia Danych Osobowych oświadczył pisemnie, że zwrócił lub bezpiecznie usunął te Dane Osobowe.

6.5 Raportowanie naruszeń Danych Osobowych a chmura

Organy Administracji publicznej odpowiadają na podstawie RODO za zgłaszanie organowi regulacyjnemu ds. ochrony danych osobowych (a w niektórych okolicznościach także Osobom, których dane dotyczą) wszelkich Naruszeń Danych Osobowych. Te obowiązki sprawozdawcze muszą być wypełnione w określonych terminach (co do zasady w ciągu 72 godziny od chwili, w której Administrator Danych Osobowych dowie się o naruszeniu) i mają zastosowanie w równym stopniu do wszystkich Naruszeń Ochrony Danych Osobowych, niezależnie od tego, czy dane Naruszenie odnosi się do Przetwarzania Danych przez dany organ, czy też przez dostawcę usług chmurowych. Dlatego też, jeżeli Naruszenie Ochrony Danych Osobowych wystąpi w rozwiązaniu chmurowym, organ będzie musiał polegać na tym, że dostawca usług chmurowych powiadomi o jego zaistnieniu. Jest mało prawdopodobne, aby to instytucja samodzielnie zidentyfikowała wystąpienie incydentu z zakresu Naruszenia Ochrony Danych Osobowych. Postanowienia Obligatoryjne wymagają, aby dostawca usług chmurowych udzielił organowi pomocy przy wypełnianiu obowiązku notyfikacji.

Dostawca usług chmurowych powinien być zobowiązany do zawiadomienia instytucji o zaistniałym Naruszeniu Ochrony Danych Osobowych jak najszybciej po powzięciu informacji w tym zakresie, aby pomóc jej w wypełnieniu obowiązku notyfikacji. Organ Administracji publicznej może również potrzebować uzyskać konkretne informacje od dostawcy usług chmurowych, aby móc odpowiednio ocenić Naruszenie Ochrony Danych Osobowych. W konsekwencji umowa chmurowa powinna zapewnić, że organ otrzyma od dostawcy usług chmurowych dostęp do wszystkich niezbędnych informacji.

Oprócz samej umowy chmurowej organ powinien samodzielnie upewnić się, że wybrany dostawca usług chmurowych wdrożył odpowiednie procedury w celu reagowania na Naruszenia Ochrony Danych Osobowych. W praktyce oznacza to, że organ powinien sprawdzić plan reagowania dostawcy na Naruszenia Ochrony Danych Osobowych. Dobrze przygotowane plany reagowania będą zawierać: (i) dane kluczowych pracowników w zespole ds. naruszeń (takich jak specjaliści ds. IT, HR, kwestii prawnych, zarządczych, PR i ciągłości działania) wraz ze wskazaniem ich

konkretnej roli / zakresu odpowiedzialności; (ii) dane kontaktowe odpowiednich osób trzecich / doradców (takich jak firmy PR, zewnętrzne kancelarie prawne, agencje ochrony) oraz (iii) określenie kanałów komunikacyjnych, protokołów i terminów w celu zapewnienia przejrzystości i szybkości komunikacji.

6.6 Postanowienia nieobligatoryjne

Zgodnie z Wytycznymi dotyczącymi usług chmury obliczeniowej z 2013 r. Administracja publiczna powinna – jeśli to możliwe – uwzględnić w umowie chmurowej zobowiązanie dostawcy usług chmurowych do notyfikowania o wezwaniach skierowanych do dostawcy przez zagraniczne publiczne instytucje lub instytucje nadzorcze w zakresie dostępu do danych Administracji publicznej. Dostawca usług chmurowych powinien być również zobowiązany do notyfikowania wynikających z prawa, któremu podlega, zobowiązań prawnych dotyczących udzielenia dostępu do danych.

6.7 Środki naprawcze przysługujące w razie niewypełnienia przez dostawcę usług chmurowych obowiązków w zakresie ochrony danych

Standardowe warunki umowne dostawców usług chmurowych zazwyczaj zmierzają do ograniczenia ich odpowiedzialności za naruszenie obowiązków związanych z Przetwarzaniem Danych, przede wszystkim poprzez dążenie do ograniczenia odpowiedzialności odszkodowawczej (często do wysokości opłat należnych za usługę chmurową) w przypadku, gdy spowodowane przez nich naruszenie sprawia, że Administrator nie spełnia wymogów przewidzianych przez RODO. Biorąc pod uwagę wystandaryzowany charakter usług chmurowych oraz ich warunków kontraktowych, postanowienia w tym zakresie mogą być trudne do renegocjowania.

7. Regulacje w zakresie cyberbezpieczeństwa i inne ważne regulacje krajowe

Rysunek 11 przedstawia kluczowe regulacje oraz inne istotne regulacje krajowe, z którymi należy się zapoznać, rozważając rozwiązanie chmurowe:

Rysunek 11: *Kluczowe regulacje w zakresie cyberbezpieczeństwa inne ważne regulacje krajowe (na dzień 1 stycznia 2020 r.)*

Regulacje krajowe	Link do regulacji
Uchwała Rady Ministrów z dnia 11 września 2019 r. w sprawie Wspólnej Infrastruktury Informatycznej Państwa	Uchwała WIIP z 2019 r.
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa	Ustawa o krajowym systemie cyberbezpieczeństwa z 2018 r. [tekst ujednolicony]
Ustawa z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne	Ustawa o informatyzacji z 2005 r. [tekst ujednolicony]
Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.	Ustawa w sprawie Krajowych Ram Interoperacyjności z 2012 r. [tekst ujednolicony]

Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych	Ustawa o ochronie informacji niejawnych z 2010 r. [tekst ujednolicony]
Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego	Rozporządzenie w sprawie podstawowych wymagań bezpieczeństwa IT z 2011 r.

06. MIGRACJA I CIĄGŁOŚĆ DZIAŁANIA

1. Migracja do chmury

Ogólna strategia planowania migracji do chmury nie różni się znacząco od planowania jakiegokolwiek innego dużego projektu informatycznego. W obu przypadkach kluczowe znaczenie ma odpowiednie przygotowanie. Rysunek 12 przedstawia niektóre z kluczowych praktycznych kroków, które należy uwzględnić, planując migrację do rozwiązania chmurowego – czy to w formie uruchomienia nowego rozwiązania, czy też przejścia z już istniejącego systemu typu *on-premise*.

Rysunek 12: *Podstawowe kroki migracji do chmury*

Krok		Procedura migracji
1	Uruchomienie środowiska chmurowego	Krok ten powinien obejmować zapewnienie, instalację oraz przetestowanie niezbędnych zasobów pamięci, obliczeniowe, sieciowe i bezpieczeństwa tworzące środowisko chmurowe, w którym będzie działać oprogramowanie/usługa po migracji.
2	Wdrożenie zasobów w zakresie monitorowania i zarządzania	Krok ten powinien obejmować stworzenie zespołu organizacyjnego, opracowanie procesów, procedur i narzędzi, których będą używane do zarządzania i monitorowania usługą chmurową, aby osiągnąć uzgodnione poziomy usługi. Może to być zespół mieszany, w który zaangażowane będą osoby zarówno z organu Administracji publicznej, jak i z organizacji dostawcy usług chmurowych.
3	Instalacja i konfiguracja aplikacji i oprogramowania pośredniego	Dostawcy usług chmurowych zazwyczaj dokonują instalacji i konfiguracji za pomocą zautomatyzowanych metod wdrażania, jednakże należy zweryfikować, jak dokładnie przebiega ten proces u wybranego dostawcy usług chmurowych.
4	Gwarancja odporności środowiska produkcyjnego	Krok ten może obejmować instalację dodatkowych narzędzi zapewniających ciągłość działania (zob. poniżej), takich jak funkcje automatycznego tworzenia kopii zapasowych czy też oprogramowanie antywirusowe. Niektóre z tych usług mogą zostać zapewnione przez dostawcę usług chmurowych. W takim przypadku, organ nie będzie musiał ich instalować, ale nadal będzie musiał je przetestować.
5	Migracja testową	Organ Administracji publicznej na tym etapie powinien wykonać testowy plan migracji, aby wykryć wszelkie nieprzewidziane wyniki lub problemy, które nie zostały uwzględnione w fazie planowania migracji. Data migracji testowej nie powinna znajdować się zbyt blisko planowanej końcowej daty zakończenia projektu, tak aby pozostało jeszcze wystarczająco dużo czasu na rozwiązanie ewentualnych problemów.
6	Test gotowości operacyjnej	Krok ten powinien obejmować testowanie procesów operacyjnych, takich jak proces odzyskiwania danych po awarii czy testowanie zespołów ds. zarządzania incydentami/problemami (oraz przekazywanie ich do helpdesku dostawcy usług chmurowych). Pozwoli to upewnić się, że zespół operacyjny, procesy i narzędzia są gotowe do wsparcia usługi chmurowej.

7	Uruchomienie usługi chmurowej	Krok ten powinien dotyczyć aktualizacji planu migracji (który obejmuje wszystkie kroki przed, w trakcie i po migracji), biorąc pod uwagę doświadczenia zdobyte podczas migracji testowej (zob. pkt 5 powyżej). Plan migracji powinien zawierać nazwiska i dane kontaktowe kluczowego personelu, a także instrukcje dotyczące eskalacji w przypadku wystąpienia problemów. Należy upewnić się, że zespół migracyjny dostawcy usług chmurowych jest zaangażowany (oraz wszelkie inne osoby trzecie, takie jak wszyscy właściwi dostawcy oprogramowania). Uwaga: mogą to być inne osoby/zespoły niż te, które były zaangażowane w proces migracji testowej.

2. Zarządzanie ciągłością działania

2.1 Czym jest zarządzanie ciągłością działania?

Wdrożenie planu zarządzania ciągłością działania jest najbardziej kompleksowym sposobem zapewnienia jak największej odporności organu Administracji publicznej w przypadku wystąpienia zdarzenia zakłócającego (czasami określanego, jako siła wyższa, taka jak na przykład klęska żywiołowa w postaci trzęsienia ziemi, powodzi lub pożaru).

Zarządzanie ciągłością działania nie jest istotne wyłącznie w zakresie rozwiązań chmurowych – organ powinien dysponować taki planem w odniesieniu do kluczowych systemów, aplikacji i procesów.

2.2 Ciągłość działania nie jest tym samym, co odzyskiwanie danych po awarii

Odzyskiwanie danych po awarii jest podobne do ciągłości działania, jednak nie są to pojęcia tożsame.

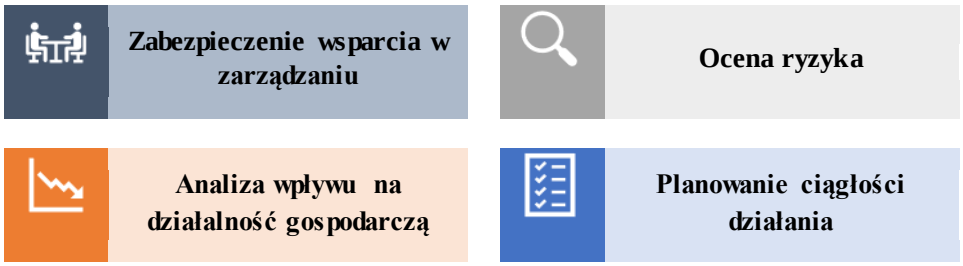
Odzyskiwanie danych po awarii odnosi się do udokumentowanej serii kroków niezbędnych do odzyskania funkcjonalności IT po wystąpieniu zdarzenia zakłócającego w danej organizacji. Odzyskiwanie danych po awarii jest zatem środkiem naprawczym, którego celem jest jak najszybsze przywrócenie normalnego funkcjonowania wszystkich dotkniętych awarią systemów informatycznych i systemów pokrewnych.

Dla odmiany ciągłość działania koncentruje się na utrzymaniu zdolności do działania w przypadku wystąpienia zdarzenia zakłócającego. Następuje to poprzez zapewnienie, że najważniejsze funkcje biznesowe/administracyjne będą mogły w dalszym ciągu działać – nawet jeśli ze zmniejszoną wydajnością – podczas gdy organ będzie starał się poradzić sobie ze zdarzeniem zakłócającym. W odróżnieniu od odzyskiwania danych po awarii, planowanie ciągłości działania będzie wymagało wdrożenia środków niezbędnych do utrzymania przynajmniej minimalnego poziomu funkcjonalności, które są konieczne do nieprzerwanego działania organu Administracji publicznej.

2.3 Zasady zarządzania ciągłością działania

2.4 Międzynarodowa norma ISO 22301:2012 zawiera specyfikację najlepszych praktyk w zakresie zarządzania ciągłością działania. Norma ISO opiera się na kilku podstawowych zasadach i działaniach, które przedstawiono na Rysunku 13 poniżej.

Rysunek 13: *Podstawowe zasady najlepszych praktyk ISO22301*



Pozostała część niniejszego punktu zawiera krótkie omówienie każdej z tych podstawowych zasad.

(a) Wsparcie w zarządzaniu

Jak w przypadku wszystkich dużych projektów, aby system zarządzania ciągłością działania odniósł sukces, musi być wspierany przez zarząd lub kierownictwo wyższego szczebla. Wsparcie ze strony kierownictwa pomoże zapewnić, że:

- niezbędne zasoby (w tym finansowanie) będą dostępne;
- system zarządzania ciągłością działania będzie odpowiadał szerszym celom strategicznym organizacji i ją wspierał;
- system będzie ciągle ulepszany;
- system zarządzania będzie wspierany na wszystkich poziomach.

Jeżeli kierownictwo wyższego szczebla zapewni wsparcie przez cały czas trwania projektu, istnieje też większe prawdopodobieństwo, że pracownicy będą spełniać wymogi dotyczące zasad zarządzania ciągłością działania, dzięki czemu system będzie bardziej efektywny.

Warto pamiętać, że mało prawdopodobnym jest, aby zarząd lub kadra kierownicza wyższego szczebla zaangażowały się w realizację planu, który nie jest jasno zdefiniowany. Z tego względu, jednym z priorytetowych działań powinno być ustalenie zakresu i celów systemu zarządzania.

(b) Ocena ryzyka

Pierwszym krokiem w podejmowaniu decyzji o tym, jak i kiedy utrzymać kluczowe funkcje biznesowe, jest jasne określenie, jakie zdarzenia lub okoliczności mogą je zakłócić. Ustalenie tych okoliczności jest kluczowym wynikiem etapu oceny ryzyka. Ocena ta powinna również określać, jak prawdopodobne jest wystąpienie zdarzeń zakłócających oraz jak poważne mogą być ich skutki.

Zrozumienie ekspozycji na ryzyko polega na mapowaniu kombinacji wpływu (tj. tego, jak poważne byłoby zdarzenie, gdyby do niego doszło) i prawdopodobieństwa (tj. jak prawdopodobne jest, że może dojść do danego zdarzenia). Kombinacja ta daje „ocenę ryzyka", którą można następnie porównać z tolerancją na ryzyko wyznaczającą poziom ryzyka akceptowalny dla organu. Tolerancja na ryzyko w danej instytucji będzie prawdopodobnie silnie uzależniona od jej charakteru i wielkości.

Jeżeli wynik oceny ryzyka związanego z określonym wydarzeniem – np. awarią dostawcy mediów – wykracza poza poziom tolerancji ryzyka, należy podjąć dodatkowe działania. Może to być np. podwyższenie wysokości ubezpieczenia bądź też zainstalowanie odpowiednich urządzeń, np. zapasowego generatora prądu.

(c) Analiza wpływu na działalność gospodarczą

Analiza wpływu na działalność gospodarczą stanowi, wraz z oceną ryzyka, podstawowy element zarządzania ciągłością działania. Analiza wpływu na działalność definiuje krytyczne dla organu działania i zasoby oraz określa, jak poważne byłyby skutki biznesowe, gdyby te działania zostały przerwane lub gdyby te zasoby zawiodły (tym różni się od oceny ryzyka – nie ma tu znaczenia samo zdarzenie zakłócające).

Wyniki analizy wpływu na działalność są wykorzystywane do ustalenia priorytetów w zakresie odzyskiwania po wystąpieniu zakłócenia. Kluczowym czynnikiem przy ustalaniu priorytetów jest fakt, że wpływ danego zdarzenia zakłócającego zazwyczaj wzrasta wraz z upływem czasu. Ocena wpływu na działalność powinna zatem określać, w jakim momencie taki rosnący wpływ staje się nie do przyjęcia. To z kolei umożliwi ustalenie, jak szybko każde działanie lub zasób muszą zostać wznowione po wystąpieniu danego zdarzenia.

Podstawowym produktem analizy wpływu na działalność gospodarczą jest czas odzyskiwania po awarii (RTO) określany dla każdego działania lub zasobu. Informacje te następnie bezpośrednio kształtują wskaźniki RTO, które z kolei stanowić będą podstawę planu ciągłości działania.

(d) Plany ciągłości działania

Ocena ryzyka i ocena wpływu na działalność stanowią podstawę do opracowania planu ciągłości działania. Pozwalają one na zapewnienie, że plan ciągłości działania dokładnie odzwierciedli wymagania , strukturę i konkretne okoliczności.

Plan ciągłości działania zazwyczaj obejmuje:

- dane kontaktowe organów regulacyjnych, dostawców i innych kluczowych udziałowców;
- dane kontaktowe kluczowych pracowników w celu zapewnienia dostępności odpowiednich osób; oraz
- listy kontrolne lub kroki, które należy podjąć w przypadku określonych zdarzeń.

W przypadku wystąpienia zdarzenia zakłócającego podstawowym celem planu ciągłości działania jest ustabilizowanie sytuacji, a tym samym umożliwienie organowi kontynuowania działalności pomimo wystąpienia zdarzenia zakłócającego.

Plan ciągłości działania stanowi centralny element każdego systemu zarządzania ciągłością działania. Plan zawiera priorytetowe działania, które będzie należało podjąć w odpowiedzi na wszelkie zdarzenia zagrażające kluczowym działaniom lub zasobom danego organu.

Chociaż wiele instytucji tworzy plan ciągłości działania, nierzadko zdarza się, że nie wprowadzają one szerszych systemów zarządzania ciągłością działania. Jednocześnie bez zasadniczego systemu zarządzania ciągłością działania plany ciągłości działania (nawet te

dobrze przygotowane) mogą szybko stać się nieaktualne. To z kolei może skutkować nieoptymalnym zastosowaniem planów w momencie, kiedy rzeczywiście dojdzie do zdarzenia zakłócającego.

Systemy zarządzania ciągłością działania oparte na najlepszych praktykach zapewniają, że wszystkie elementy dotyczące ciągłości działania, w tym plany ciągłości działania, są opracowywane, testowane, weryfikowane i aktualizowane regularnie i konsekwentnie, przy wykorzystaniu coraz bardziej rygorystycznego procesu. Oznacza to, że plan reagowania jest udoskonalany w sposób iteracyjny w miarę upływu czasu. Ponadto posiadanie systemu zarządzania ciągłością działania oznacza, że wszyscy właściwi pracownicy / osoby zainteresowane są informowani o planie reagowania poprzez centralny, sformalizowany proces oraz rozumieją przydzielone im role i obowiązki, jeśli zaistnieje potrzeba zastosowania planu.

2.5 Najlepsza praktyka – nieustanne doskonalenie

Najlepsza praktyka w ramach ISO 22301:2012 oznacza opracowywanie i podążanie za procesem ciągłego ulepszania, ponieważ podejście takie gwarantuje, że system zarządzania ciągłością działania będzie w stanie dostosować się do nowych zagrożeń i zmian w środowisku operacyjnym organizacji. Co ważne, ustanawia ona również mechanizm monitorowania skuteczności systemu zarządzania ciągłością działania.

W szczególności w stosunku do systemów zarządzania ciągłością działania norma ISO 22301:2012 zaleca zastosowanie modelu PDCA (z ang. *Plan-Do-Check-Act*). Jak pokazano na Rysunku 14 poniżej, pierwszym krokiem ciągłego doskonalenia opartego na modelu PDCA jest zaplanowanie jaką zmianę zamierza się wprowadzić, a następnie wykonanie tego planu. W kolejnym kroku efekt zmiany powinien zostać porównany z przyjętym planem w celu podjęcia decyzji, czy coś wymaga poprawy. Na koniec wszelkie zidentyfikowane ulepszenia powinny zostać wdrożone.

Rysunek 14: *Zarys modelu PDCA*

Najlepszą praktyką jest regularne przeprowadzanie procesu monitorowania wyników i ciągłego doskonalenia. Zazwyczaj powinno to następować co 2 lata, ale również po przeprowadzeniu jakiegokolwiek audytu wewnętrznego lub po wywołaniu planu ciągłości działania.

07. CZĘSTO ZADAWANE PYTANIA

Niniejszy rozdział zapewnia pomoc w zakresie najczęściej zadawanych pytań podczas rozważania zastosowania rozwiązań chmurowych.

Jeśli macie Państwo jakiekolwiek inne pytania lub chcielibyście Państwo uzyskać więcej informacji, prosimy o kontakt z ● pod adresem ●.

+ Prawo konsumenckie

Czy Ustawa o prawach konsumenta będzie miała zastosowanie, jeżeli moja organizacja zdecyduje się na korzystanie z chmury?

Status konsumenta może być brany pod uwagę tylko w przypadku stosunków cywilnoprawnych. Nie ma on zastosowania w stosunkach pomiędzy władzą publiczną a obywatelem bądź inną osobą fizyczną.

W związku z tym przy migracji do chmury nie ma zastosowania Ustawa o prawach konsumenta. W zakresie, w jakim organizacja wykonuje swoje uprawnienia, działając jako organ publiczny, osoby fizyczne korzystające z usług organizacji nie są uważane za konsumentów.

Z drugiej strony, jeżeli organizacja nawiązuje stosunki prawne we własnym imieniu (np. w przypadku umów handlowych), prawa konsumenta mogą znaleźć zastosowanie. Może to mieć miejsce przykładowo w sytuacji świadczenia usług komunalnych na rzecz obywateli przez przedsiębiorstwo komunalne. Stosunki z udziałem osób fizycznych, w szczególności stosunki między przedsiębiorcami a konsumentami, wymagają wypełnienia obowiązków informacyjnych, w tym dostarczenia konsumentowi informacji na temat kompatybilnego oprogramowania i sprzętu, a także funkcjonalności i odpowiednich technicznych środków ochrony treści cyfrowych. Ponadto w takich przypadkach zastosowanie mogą znaleźć regulacje Kodeksu Cywilnego nakładające ograniczenia w stosowaniu niedozwolonych klauzul umownych.

Kwestia, czy regulacje dot. praw konsumenta znajdą bądź nie zastosowanie w danym przypadku, nie będzie zależała wyłącznie od kwestii korzystania z chmury przez Państwa organizację i musi być analizowana indywidualnie dla każdego przypadku.

+ Odpowiedzialność

Kto jest odpowiedzialny za dane Przetwarzane w chmurze lub za wady rozwiązań chmurowych?

Korzystanie z usług chmurowych nie modyfikuje ogólnych zasad odpowiedzialności władzy publicznej – ani w dziedzinie prawa prywatnego i stosunków z osobami fizycznymi, ani w odniesieniu do wykonywania władzy publicznej. W konsekwencji wszelkie szkody spowodowane wadami rozwiązań chmurowych podlegają ogólnym zasadom prawa.

Niezależnie od tego, czy Państwa organizacja korzysta z usług chmurowych, odpowiedzialność Państwa organizacji za wyrządzone szkody opiera się na tych samych zasadach ogólnych Kodeksu Cywilnego, a mianowicie:

(a) Organizacja ponosi odpowiedzialność umowną lub deliktową za szkody wyrządzone osobom trzecim w stosunkach wynikających z zasad prawa prywatnego; odpowiedzialność ta zależy od okoliczności konkretnej sprawy.

Należy wziąć pod uwagę w szczególności przewidzianą w przepisach RODO odpowiedzialność cywilną za szkody wynikające z Naruszenia Danych Osobowych bądź też bezprawnego Przetwarzania.

Ogólna zasada regulująca ten rodzaj odpowiedzialności opiera się na zasadzie winy podmiotu odpowiedzialnego.

(b) Odpowiedzialność za bezprawne działania lub zaniechania przy wykonywaniu władzy publicznej (prawo publiczne).

Niezależnie od odpowiedzialności umownej lub deliktowej w stosunkach prywatnoprawnych władze publiczne są zobowiązane do wypełniania zobowiązań prawnych poprzez wykonywanie władzy publicznej, na przykład poprzez prowadzenie rejestrów publicznych. W kontekście technologii chmury obliczeniowej szczególne znaczenie ma zapewnienie zgodności z minimalnymi wymogami przewidzianymi dla systemów teleinformatycznych oraz wymiany informacji w formie elektronicznej, określonych w Ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne.

Nienależyte wykonywanie obowiązków publicznoprawnych, wyrządzające szkodę jakiejkolwiek osobie (fizycznej lub prawnej), może skutkować odpowiedzialnością odszkodowawczą Skarbu Państwa lub jednostki samorządu terytorialnego albo innej osoby prawnej wykonującej władzę publiczną na podstawie przepisów prawa. Odpowiedzialność za szkodę wyrządzoną przy wykonywaniu władzy publicznej nie jest zależna od winy organu władzy publicznej. To bezprawność działań będzie skutkowała powstaniem odpowiedzialności, o której mowa.

Administracja rządowa oraz Lokalne organy władzy publicznej podlegają również odpowiedzialności administracyjnej, w szczególności w zakresie Przetwarzania Danych Osobowych w sposób określony w RODO. Na większość organów Administracji rządowej oraz Lokalnych organów władzy publicznej może zostać nałożona grzywna w wysokości do 100 000 PLN w przypadku Przetwarzania Danych bez podstawy prawnej lub innego naruszenia RODO (np. wycieku lub utraty Danych). Z drugiej strony spółki będące własnością Skarbu Państwa lub jednostek samorządu terytorialnego podlegają zasadom ogólnym, co oznacza, że w przypadku dokonania naruszenia mogą zostać ukarane grzywną w wysokości do 4 % całkowitego rocznego obrotu lub do 20 000 000 EUR (w zależności od tego, która kwota jest wyższa).

Czy dostawca usług chmurowych będzie odpowiedzialny za szkody wyrządzone mojej organizacji?

Jeżeli dostawca usług chmurowych wyrządzi jakąkolwiek szkodę Państwa organizacji, zastosowanie znajdą ogólne zasady prawa cywilnego.

Oznacza to, że Państwa organizacja będzie zasadniczo uprawniona do dochodzenia odszkodowania odpowiadającego wysokości szkody wyrządzonej przez dostawcę usług chmurowych. Na przykład w sytuacji, gdy organizacja będzie musiała zaspokoić roszczenia powstałe w związku z wyciekiem danych spowodowanym nienależytym wykonaniem usług przez dostawcę usług chmurowych. Jednakże zakres odszkodowania, jakie Państwa

organizacja będzie mogła uzyskać od dostawcy usług chmurowych, będzie podlegał regulacjom umownym określonym w umowie chmurowej.

Czy dostawca usług chmurowych może ograniczyć swoją odpowiedzialność za utratę danych lub inne szkody?

Ogólne zasady prawa cywilnego co do zasady pozwalają wykonawcom na ograniczenie odpowiedzialności w stosunku do większości rodzajów szkody. Kodeks Cywilny przewiduje wyjątek od tej zasady tylko w odniesieniu do szkód spowodowanych umyślnym działaniem wykonawcy. W przypadku, gdy umowa chmurowa podlegać będzie prawu obcemu, jest prawdopodobne, że zasada ograniczenia odpowiedzialności również znajdzie zastosowanie i umowne ograniczenia odpowiedzialności pozostaną skuteczne.

Dostawcy usług chmurowych mają na ogół tendencję do wprowadzania istotnych ograniczeń swojej odpowiedzialności w przyjętych przez nich warunkach świadczenia usług. W większości przypadków tego rodzaju ograniczenia stosowane są zarówno w zakresie maksymalnej kwoty należnej w przypadku wyrządzenia szkody, jak i do określenia różnych zdarzeń i okoliczności, za które dostawca usługi chmurowej nie ponosi odpowiedzialności. Dostawcy usług chmurowych zazwyczaj dążą w szczególności do wyłączenia swojej odpowiedzialności za utratę danych.

Na gruncie prawa polskiego tego rodzaju ograniczenia odpowiedzialności są zasadniczo ważne i wiążące, a w większości przypadków okażą się skuteczne również w świetle prawa obcego.

Czy dostawca usług chmurowych ponosi odpowiedzialność za niezgodne z prawem lub niewłaściwe Przetwarzanie Danych Osobowych?

W zakresie, w jakim dostawca usług chmurowych działa w imieniu organizacji, będzie on Podmiotem Przetwarzającym w rozumieniu RODO. Oznacza to, że będzie on nie tylko ponosił umowną i deliktową odpowiedzialność za wyrządzone szkody, ale będzie również ponosił odpowiedzialność administracyjną za naruszenie swoich obowiązków wynikających z RODO. W szczególności dostawca usług chmurowych może być odpowiedzialny za stosowanie nieadekwatnych środków bezpieczeństwa, w zależności od konkretnego przypadku.

W przypadku szkody wyrządzonej przez dostawcę usług chmurowych osobie fizycznej (na przykład na skutek utraty danych) zarówno Państwa organizacja, jak i dostawca usług chmurowych będą ponosić solidarną odpowiedzialność wobec Osoby, której dotyczą dane, przy zachowaniu prawa do zwrotnego dochodzenia od osoby, która zawiniła, części odszkodowania odpowiadającej rozmiarowi odpowiedzialności danej strony.

Należy jednak wziąć pod uwagę, że powyższe nie wyklucza odpowiedzialności administracyjnej organizacji jako Administratora Danych.

Co, jeżeli dostawca usług chmurowych okaże się niewypłacalny?

Ogólnie rzecz biorąc, sytuacja ta nie różni się od niewypłacalności dostawcy usług informatycznych, które nie są świadczone w chmurze. Jeżeli w umowie chmurowej nie zawarto szczególnych ustaleń w tym zakresie, Państwa organizacja będzie niezabezpieczonym wierzycielem wszelkich należnych jej z tego tytułu środków

pieniężnych (w tym wszelkich odszkodowań zasądzonych w wyniku podjętych działań prawnych).

Pod względem operacyjnym niewypłacalność dostawcy usług chmurowych może spowodować przerwanie świadczenia danej usługi, jak również wypowiedzenie umowy przez syndyka masy upadłościowej. Umowa chmurowa powinna zatem zawierać szczegółowe warunki postępowania w przypadku niewypłacalności, w tym przewidywać odpowiednie zabezpieczenia dla organizacji – takie jak skuteczne prawo do odzyskania danych oraz wsparcie w przejściu na usługę alternatywną.

Czy istnieją jakieś standardowe warunki kontraktowe, powszechnie stosowane przez dostawców usług chmurowych?

Każdy dostawca usług chmurowych opracował swoje własne standardowe warunki umowne i poziomy usług, uwzględniające świadczone przez niego usługi i podejście do ryzyka.

+ Własność intelektualna (z ang. *Intellectual Property*, dalej: „IP")

Czy mojej organizacji będą przysługiwać prawa autorskie do rozwiązania w chmurze?

Usługi chmurowe są zazwyczaj wysoce wystandaryzowane i dlatego nie wymagają wytworzenia nowych przedmiotów praw własności intelektualnej bądź też wymagają ich wytworzenia jedynie w bardzo niewielkim zakresie. W związku z powyższym mało prawdopodobne jest, aby w trakcie zamawiania usługi chmurowej potrzebne było wytworzenie nowych przedmiotów praw własności intelektualnej.

Szczególne utwory mogą zostać wytworzone w trakcie rozwijania chmury prywatnej lub hybrydowej albo gdyby Państwa organizacja potrzebowała, aby dostawca chmury opracował konkretne interfejsy dające dostęp do usługi chmurowej. W takich sytuacjach Państwa organizacja może oczekiwać przeniesienia powstałych majątkowych praw autorskich do utworów, aby zapobiec ich ponownemu wykorzystaniu przez dostawcę usług chmurowych.

O ile umowa z dostawcą usług chmurowych nie stanowi inaczej, właścicielem autorskich praw majątkowych staje się podmiot, który je wytworzył. Z tego względu powinni Państwo sprawdzić warunki świadczenia usług zapewniane przez dostawcę usług chmurowych, aby upewnić się, że majątkowe prawa autorskie do wszelkich utworów, które mają zostać wytworzone, zostaną przeniesione na Państwa organizację.

Czy mogę umieścić w chmurze dane zawierające przedmioty praw własności intelektualnej, należące do mojej organizacji?

Tak. Umieszczenie takich danych w chmurze może być jednak uzależnione od ich klasyfikacji w ramach systemu klasyfikacji danych WIIP. Jeśli własność intelektualna ma dla Państwa organizacji charakter poufny, należy zapewnić odpowiednie zabezpieczenia i środki kontroli dostępu do usługi chmurowej.

Więcej szczegółów znajduje się w Rozdziale 3 oraz 4 niniejszego przewodnika.

Czy istnieją jakiekolwiek sankcje cywilne/karne za umieszczenie w chmurze materiałów naruszających prawa własności intelektualnej?

Nie ma żadnych szczególnych przepisów z zakresu praw własności intelektualnej, które odnosiłyby się wyłącznie do usług chmurowych.

Oznacza to, że ogólne zasady prawa w zakresie ochrony utworów (w tym sankcje cywilne i karne) będą miały zastosowanie w równym stopniu do usług informatycznych świadczonych w chmurze, jak i poza nią.

Kto jest właścicielem danych, które moja organizacja umieszcza w chmurze?

W polskim prawie nie istnieje koncepcja własności danych.

Zamiast tego dane są chronione przez różne uprawnienia, takie jak prawo do zachowania poufności informacji oraz pewne prawa własności intelektualnej (takie jak prawo autorskie lub prawa dotyczące baz danych).

Uprawnienie do korzystania z danych jest przedmiotem umów chmurowych. Zazwyczaj dostawca usług chmurowych nie dąży do nabycia własności danych umieszczonych w chmurze, ale raczej jest zainteresowany uzyskaniem licencji na korzystanie z tych danych (w celu ich kopiowania, przechowywania i przekazywania) w zakresie niezbędnym do świadczenia usługi chmurowej.

Czy usługi chmurowe zawierają oprogramowanie o otwartym kodzie źródłowym (z ang. *open source*)?

Tak, oprogramowanie *open source* jest powszechnie stosowane w infrastrukturze usług chmurowych.

Jeżeli usługa chmurowa pozyskiwana jest z ZUCH (zob. Rozdział 2 w celu uzyskania dalszych szczegółów), oprogramowanie *open source* zostanie sprawdzone podczas zatwierdzania dostawców usług chmurowych do katalogu PChO.

Jeżeli zdecydują się Państwo na samodzielne pozyskanie usługi chmurowej, to w ramach procedury *due diligence* wobec dostawcy usług chmurowych należy poznać zakres oprogramowania *open source* wykorzystywanego w wybranej usłudze chmurowej.

Czy dostawcy usług chmurowych mogą zostać pociągnięci do odpowiedzialności za jakiekolwiek materiały naruszające prawa własności intelektualnej, które umieszczamy w chmurze?

Tak, możliwe jest, że dostawca usług chmurowych będzie ponosił odpowiedzialność za naruszenia praw własności intelektualnej wynikające z materiałów umieszczonych w chmurze przez Państwa organizację.

W związku z powyższym dostawcy usług chmurowych zazwyczaj starają się przenieść tę odpowiedzialność na swoich klientów za pomocą swoich standardowych warunków umownych. Należy zatem dokładnie zweryfikować warunki świadczenia usług wybranego dostawcy w celu upewnienia się, że alokacja ryzyka w tym zakresie jest odpowiednia i racjonalna.

08. SŁOWNIK POJĘĆ

Klasyfikacja oparta na cechach danych	oznacza metodę klasyfikacji wykorzystującą zautomatyzowane narzędzia do przypisywania danych do wybranych kategorii, w oparciu o zdefiniowane reguły. Reguły te zazwyczaj odnoszą się do kontekstu lub zawartości danych objętych zakresem i dotyczą podstawowych cech danych, odnoszących się do wszystkich zbiorów danych (takich jak geolokalizacja, znacznik czasu lub autor). Dane są następnie analizowane elektronicznie według danej cechy, a zasady są stosowane automatycznie w celu określenia odpowiedniej kategorii danych. Klasyfikacja oparta na cechach umożliwia szybką klasyfikację danych, zazwyczaj na znacznie większą skalę niż Klasyfikacja oparta na użytkowniku.
jako Usługa (z ang. *as a Service*, „aaS")	„jako Usługa [chmurowa]". Jest to to przyrostek opisujący zdolność obliczeniową, wspierającą wszystkie pięć podstawowych cech charakterystycznych chmury obliczeniowej. Termin „jako Usługa (aaS)" oznacza, że SaaS, PaaS i IaaS są dostarczane za pomocą oprogramowania.
Chmura społecznościowa	oznacza infrastrukturę chmurową dostarczaną do wyłącznego użytku konkretnej społeczności klientów z organizacji mających te same potrzeby (np. cel, projekt, wymogi bezpieczeństwa, politykę lub aspekty zgodności). Może ona stanowić własność, być zarządzana i eksploatowana przez jedną lub więcej organizacji w danej społeczności, osobę trzecią lub określoną kombinację powyższych podmiotów, a także może być umiejscowiona lokalnie lub nie (NIST SP 800-145).
Administrator	ma znaczenie określone w art. 4 pkt 7 RODO. Jest to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby Przetwarzania Danych Osobowych; jeżeli cele i sposoby takiego Przetwarzania są określone w prawie Unii Europejskiej lub w prawie państwa członkowskiego, to również w prawie Unii Europejskiej lub w prawie państwa członkowskiego może zostać wyznaczony Administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.
Osoba, której dane dotyczą	ma znaczenie określone w art. 4 pkt 1 RODO. Jest to możliwa do zidentyfikowania osoba fizyczna, a zatem osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Wnioski osób, których dotyczą dane	wnioski pochodzące od osób, których dane dotyczą, o skorzystanie z praw przysługujących im na podstawie rozdziału III RODO, w tym wnioski o usunięcie, poprawienie lub przeniesienie ich danych osobowych, jak również wnioski o dostęp do Danych Osobowych i ograniczenie Przetwarzania Danych Osobowych.
Odzyskiwanie po awarii jako Usługa (z ang. *Disaster Recovery as a Service*, DRaaS)	zdolność, oferowana klientowi usługi chmurowej, do ochrony aplikacji i danych przed skutkami jakiejkolwiek katastrofy naturalnej lub niedostępności usług IT w pojedynczej lokalizacji poprzez stworzenie dodatkowego punktu odzyskiwania w chmurze.
EOG	Europejski Obszar Gospodarczy.
RODO	Rozporządzenie o Ochronie Danych Osobowych 2016/679.
Klasyfikacja hybrydowa	oznacza metodę klasyfikacji łączącą w sobie zarówno Klasyfikację opartą na użytkowniku, jak i Klasyfikację opartą na cechach danych podczas stosowania systemu klasyfikacji danych. Przykładowo „sugerowana klasyfikacja" polega na zastosowaniu Klasyfikacji opartej na cechach, aby najpierw określić cechy każdego zbioru danych i wygenerować sugerowaną klasyfikację. Każda sugerowana klasyfikacja jest następnie przedstawiana interesariuszom do zatwierdzenia zgodnie z zasadami Klasyfikacji opartej na użytkowniku.
Postanowienia obligatoryjne	obowiązkowe klauzule, które muszą być zawarte w umowach pomiędzy Administratorami a Podmiotami Przetwarzającymi, zgodnie z wymogami art. 28 ust. 3 RODO.
Infrastruktura jako Usługa (z ang. *Infrastructure as a Service*, IaaS)	zdolność, oferowana klientowi usługi chmurowej, do zapewnienia przetwarzania, przechowywania, sieci i innych podstawowych zasobów obliczeniowych w taki sposób, że klient jest w stanie wdrożyć i uruchomić dowolne oprogramowanie, które może obejmować systemy operacyjne i aplikacje. Klient usługi chmurowej nie zarządza podstawową infrastrukturą chmury ani jej nie kontroluje, ale ma kontrolę nad systemami operacyjnymi, pamięcią i wdrożonymi aplikacjami, a także ewentualnie ograniczoną kontrolę nad wybranymi komponentami sieciowymi (takimi jak firewall hostów).
Dane Osobowe	mają znaczenie określone w art. 4 pkt 1 RODO. Są to wszelkie informacje odnoszące się do Osoby, której dane dotyczą.
Naruszenie Ochrony Danych Osobowych	ma znaczenie określone w art. 4 pkt 12 RODO. Jest to naruszenie bezpieczeństwa prowadzące do przypadkowego lub bezprawnego zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych Osobowych przesyłanych, przechowywanych lub w inny sposób Przetwarzanych.
Platforma jako Usługa (z ang. *Platform as a Service*, PaaS)	zdolność, oferowana klientowi usługi chmurowej, do wdrożenia na infrastrukturze chmury aplikacji wytworzonych przez tego klienta bądź też przez niego nabytych, stworzonych przy użyciu języków programowania, bibliotek, usług i narzędzi wspieranych przez dostawcę usługi chmurowej. Klient usługi chmurowej nie zarządza podstawową

	infrastrukturą chmury ani jej nie kontroluje, ma natomiast kontrolę nad wdrożonymi aplikacjami i ewentualnie ustawieniami konfiguracyjnymi dla środowiska hostingowego aplikacji.
Podmiot Przetwarzający	ma znaczenie określone w art. 4 pkt 8 RODO. Jest to osoba fizyczna lub prawna, władza publiczna, agencja lub inny organ Przetwarzający Dane Osobowe w imieniu Administratora.
Przetwarzanie	ma znaczenie określone w art. 4 pkt 2 RODO. Jest to każda operacja lub zestaw operacji wykonywanych na Danych Osobowych lub zbiorach Danych Osobowych, w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
Administracja publiczna	oznacza Administrację rządową i Lokalne organy władzy publicznej.
Szczególne Kategorie Danych Osobowych	mają znaczenie określone w art. 9 ust. 1 RODO. Są to Dane Osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne w razie ich Przetwarzania w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczących zdrowia, seksualności lub orientacji seksualnej danej osoby.
Oprogramowanie jako usługa (z ang. *Software as a Service*, SaaS)	możliwość korzystania z aplikacji dostawcy usług chmurowych w ramach infrastruktury chmury. Aplikacje te są dostępne za pomocą różnych urządzeń klienckich poprzez interfejs cienkiego klienta (ang. *thin client*), taki jak przeglądarka internetowa (np. internetowa poczta elektroniczna) lub interfejs programu. Klient usługi chmurowej nie zarządza ani nie kontroluje podstawowej infrastruktury chmury, w tym możliwości aplikacji, z wyjątkiem sytuacji, gdy dostarczone są mu pewne ustawienia konfiguracyjne.
Dalszy Podmiot Przetwarzający	każdy Podmiot Przetwarzający wyznaczony przez lub w imieniu Podmiotu Przetwarzającego do Przetwarzania Danych Osobowych.
Klasyfikacja oparta na użytkowniku	oznacza metodę klasyfikacji, zgodnie z którą kluczowym zainteresowanym stronom powierza się ręczne przypisanie wszystkich danych objętych zakresemdo konkretnej kategorii w oparciu o wcześniej ustalone kryteria w ramach odpowiedniego systemu klasyfikacji. Klasyfikacja oparta na użytkowniku ma tę zaletę, że zainteresowane strony wykorzystują swoją wiedzę i ocenę danych przy rozważaniu, kryteria których kategorii znajdą zastosowanie. Klasyfikacja oparta na użytkowniku może jednak pochłaniać dużą ilość zasobów i być czasochłonna. Istnieje również ryzyko, że poszczególne zainteresowane strony nieprawidłowo sklasyfikują dane bądź też zastosują kryteria w sposób niespójny. W związku z powyższym rekomendowane są skrupulatne procesy kontroli jakości.