Komisja
LegalTech
Okręgowej Izby
Radców Prawnych
w Warszawie

MARUTA \

STANDARD PRZETWARZANIA INFORMACJI W CHMURZE OBLICZENIOWEJ PRZEZ RADCÓW PRAWNYCH

REKOMENDACJE DLA RADCÓW PRAWNYCH

METRYKA DOKUMENTU	
AUTOR	© Kancelaria Maruta Wachta
WERSJA DOKUMENTU	1.1
DATA DOKUMENTU	15 grudnia 2020 r.
SPIS TREŚCI	

1. WSTĘP

1.1. Korzystanie z chmury obliczeniowej staje się standardem na rynku – także usług prawniczych. Zarówno w przypadku korporacji prawniczych, jak i praktyk indywidualnych korzystanie z Usług chmurowych jest powszechne, nawet jeśli nie zawsze uświadomione.

1.2. Szybko postępujące zmiany związane z rozwojem nowych technologii, ale także z potrzebą dostosowania się do warunków powszechnej obecnie pracy zdalnej, pokazują, że wdrożenie chmury obliczeniowej wiąże się z wieloma wymiernymi korzyściami – takim jak zminimalizowanie kosztów, elastyczność, zwiększenie efektywności pracy.

1.3. Wykorzystanie Usług chmurowych może zapewnić Radcom prawnym ciągłość i płynność funkcjonowania oraz dostateczną ochronę szczególnie chronionych informacji. Jednak korzystanie z takich usług wiąże się także z ryzykami – zarówno o charakterze uniwersalnym, z którymi mierzą się wszyscy użytkownicy Usług chmurowych, jak i zagrożeniami specyficznymi dla zawodu Radcy prawnego (zachowanie tajemnicy radcowskiej, wymogi deontologii prawniczej).

1.4. Naczelnym założeniem niniejszego opracowania jest pomoc w wyborze takiego modelu Usług w chmurze, który najlepiej odpowiada potrzebom i specyfice działalności Radcy prawnego, z uwzględnieniem charakteru przetwarzanych informacji.

2. RAMY PRAWNE PRZETWARZANIA DANYCH PRZEZ RADCÓW PRAWNYCH

2.1. Podejmując decyzję o skorzystaniu z Usług chmury obliczeniowej, Radca prawny powinien wziąć pod uwagę poniższe akty prawne:

Ustawa o radcach prawnych (Urp)

2.2. Urp nie zawiera bezpośrednich regulacji dotyczących zasad korzystania z Usług chmury obliczeniowej. Chmura obliczeniowa jest jednak rozwiązaniem stosowanym w związku z wykonywaniem zawodu Radcy prawnego, a więc zastosowanie znajdują przepisy ogólne Urp, w szczególności regulacje dotyczące tajemnicy zawodowej (art. 3 ust. 3 i 4 Urp) (por. pkt 5) oraz ochrony danych osobowych (por. niżej).

2.3. Zasady te obowiązują niezależnie od formy wykonywania zawodu – ich praktyczna realizacja może jednak różnić się w zależności od tego w jakiej formie Radca prawny wykonuje zawód oraz jaką funkcję pełni w jednostce organizacyjnej.

Rozporządzenie ogólne o ochronie danych (RODO)

ROLE W REŻIMIE PRAWA DANYCH OSOBOWYCH

2.4. Nie omawiając w tym miejscu szczegółowo złożonej problematyki ról w reżimie prawa danych osobowych, należy przyjąć, zgodnie z dominującym w tym zakresie stanowiskiem, że co do zasady Radcowie prawni wykonujący zawód w kancelariach są **administratorami danych osobowych (**podmiotami decydującymi o środkach i celach przetwarzania danych osobowych), przetwarzanych w związku z wykonywaniem zawodu, w szczególności danych swoich klientów oraz danych osobowych przekazanych przez klientów w związku ze

zleceniem pomocy prawnej. Z kolei w przypadku Radców wykonujących zawód spółkach np. komandytowych, partnerskich – administratorami danych są spółki[1].

2.5. W związku z korzystaniem z usług chmurowych, może pojawić się obawa, że z uwagi na szeroką autonomię dostawcy Usług chmurowych, Radca prawny (użytkownik usługi) nie będzie miał takiego zakresu kontroli nad operacjami przetwarzania, który pozwoliłby organizacji działać jako administrator danych osobowych przetwarzanych w chmurze. Stąd też należy podkreślić, że tak długo, jak długo to użytkownik Usług chmurowych będzie określać cel przetwarzania, tak długo będzie on administratorem z punktu widzenia RODO. Dostawca Usług chmurowych, w zakresie świadczenia Usługi chmurowej będzie zaś działał jako podmiot przetwarzający (tzn. będzie przetwarzał dane osobowe w imieniu organizacji).

2.6. Z perspektywy roli Dostawcy w procesie przetwarzania danych osobowych, należy jednak wskazać, że oprócz przetwarzania danych w celu świadczenia usług chmurowych, niektórzy Dostawcy informują o przetwarzaniu danych osobowych w celu wykonywania czynności pomocniczych jak np. zarządzanie kontami, badania i analizy lub wykrywanie oszustw. Dostawcy wykorzystują niekiedy także dane wygenerowane w związku z korzystaniem z usługi czy też dane diagnostyczne, zebrane przy okazji świadczenia usług serwisowych, na potrzeby prowadzenia przez siebie działań analitycznych. W takim przypadku to Dostawca usług chmurowych określi środki i cele przetwarzania danych osobowych na potrzeby tych dodatkowych czynności jako administrator danych osobowych na potrzeby tych dodatkowych działań.

2.7. Radca prawny powinien w tym kontekście, co najmniej:

2.7.1. zweryfikować, czy warunki świadczenia Usług chmurowych spełniają wymogi formalne określone w art. 28 RODO;

2.7.2. przeanalizować ryzyko, związane z Usługą chmurową, w szczególności adekwatność deklarowanych przez dostawcę środków bezpieczeństwa;

2.7.3. zbadać i ocenić ryzyko związane z potencjalnym wykorzystywaniem danych osobowych przez dostawcę Usługi chmurowej dla własnych celów. Radca prawny nie może nie może dopuszczać, by Dostawca Usługi chmurowej wykorzystywał na własne cele dane objęte tajemnicą zawodową.

LOKALIZACJA DANYCH

2.8. Specyfika Usług chmurowych sprawia, że infrastruktura, za pomocą której Usługa chmurowa jest świadczona ma rozproszony charakter. Co więcej, Dostawcy korzystają z serwerów rozłożonych na całym świecie, a użytkownik może nie mieć możliwości uzyskania jednoznacznej informacji odnośnie do państw, w których dane mogą być przetwarzane. Zgodnie z RODO, przekazywanie danych do innego państwa, o ile należy ono do Europejskiego Obszaru Gospodarczego (EOG) jest dozwolone. Gdy natomiast dochodzi do transferu danych poza EOG, każda sytuacja powinna być analizowana indywidualnie w

[1] Por. P. Litwiński, „*Zmiany w przepisach dotyczących przetwarzania danych osobowych przez adwokatów i radców prawnych*” [w:] Monitor Prawniczy 2019, nr 22 str. 47

zależności od miejsca, w którym dane będą przetwarzane. Art. 45 – 49 RODO określają warunki dopuszczalności takiego transferu.

2.9. W przypadku korzystania z Usług chmurowych należy brać pod uwagę przede wszystkim art. 45 ust. 1 RODO, pozwalający na transfer danych do państwa trzeciego, co do którego Komisja wydała decyzję stwierdzającą odpowiedni stopień ochrony (są to np. Japonia, Kanada, Izrael). Drugą, najczęściej stosowaną w praktyce podstawą prawną transferu są tzw. standardowe klauzule umowne, implementowane do warunków świadczenia usług przez Dostawcę. W celu ich stosowania, zgodnie z wyrokiem Trybunału Sprawiedliwości Unii Europejskiej z dnia 16 lipca 2020 r. w sprawie C-311/18 (*Schrems II*), administrator powinien każdorazowo ocenić, czy standardowe klauzule umowne zapewniają w danym przypadku wystarczający poziom ochrony dla danych osobowych, czy też konieczne jest wdrożenie dodatkowych zabezpieczeń. Powyższy wyrok unieważnił równocześnie decyzji Komisji Europejskiej 2016/1250 w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE- USA (*Privacy Schield).*

2.10. Radca prawny powinien zweryfikować, czy wybrany Dostawca Usługi chmurowej umożliwia ograniczenie obszaru przetwarzania danych osobowych do konkretnego regionu (regionów) w granicach Europejskiego Obszaru Gospodarczego. W przypadku większości Dostawców Usług chmurowych takie możliwości istnieją.

2.11. Radca prawny powinien także zbadać, na jakich zasadach Dostawca Usługi chmurowej może uzyskać dostęp do danych z innych lokalizacji, np. w związku ze świadczeniem usług serwisowych, oraz ocenić możliwości konfiguracji Usługi chmurowej ograniczającej taki dostęp do EOG.

2.12. Przed podjęciem decyzji o dokonywaniu transferu danych osobowych do państwa trzeciego w oparciu o standardowe klauzule umowne, Radca prawny powinien, w świetle wyroku *Schrems II*, przeprowadzić analizę i ocenić, w jakim zakresie w związku z korzystaniem z Usługi chmurowej dochodzi do transferu danych osobowych, jaki jest charakter transferowanych informacji, oraz jakie zabezpieczenia stosuje Dostawca Usługi chmurowej.

OCENA RYZYKA

2.13. Jednym z wymogów RODO jest prowadzenie przez administratora oceny ryzyka dla praw i wolności osób fizycznych. Niezależnie zatem od oceny ryzyka biznesowego czy kontraktowego, Radca prawny powinien ocenić ryzyko związane z ochroną danych w ramach proponowanego rozwiązania chmurowego. Ocena ta powinna uwzględnić:

2.13.1. stan wiedzy technicznej,

2.13.2. koszt wdrażania środków bezpieczeństwa

2.13.3. charakter, zakres, kontekst i cele przetwarzania

2.13.4. ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania.

2.14. W razie stwierdzenia, że w odniesieniu do zamierzonego przetwarzania występuje duże prawdopodobieństwo wystąpienia wysokiego ryzyka dla praw lub wolności osób fizycznych,

Radca prawny powinien w udokumentowanym procesie przeprowadzić ocenę skutków przetwarzania danych osobowych.

Kodeks Etyki Radcy Prawnego (KERP)

2.15. KERP powtarza i istotnie rozwija podstawowe zasady wykonywania zawodu Radcy prawnego, określonego w Urp. W tym kontekście szczególnie istotne są:

2.15.1. Ogólny obowiązek wykonywania czynności zawodowych rzetelnie uczciwe i zgodnie z prawem (art. 6) oraz sumiennie i z należytą starannością (art. 12).

2.15.2. Obowiązek dochowania tajemnicy zawodowej (art. 9 oraz art. 15 KERP).

2.15.3. Obowiązek odpowiedniego zabezpieczenia tajemnicy zawodowej (art. 22 i 23 KERP).

2.15.4. Obowiązek traktowania norm określonych w KERP jako nadrzędnych w stosunku do sprzecznych z nimi postanowieniami regulacji wewnętrznych w jednostce organizacyjnej, w której Radca prawny wykonuje zawód (art. 40 KERP).

Regulamin Wykonywania Zawodu Radcy Prawnego (Regulamin)

2.16. Zgodnie z §6 Regulaminu, Radca prawny ma obowiązek podjąć wszelkie niezbędne czynności w celu zapewnienia przestrzegania zakazu ujawniania informacji objętych tajemnicą zawodową Radcy prawnego przez osoby niezwiązane tajemnicą zawodową na mocy ustawy, z pomocą których Radca prawny wykonuje czynności związane ze świadczeniem pomocy prawnej. Radca prawny powinien w tym kontekście wymagać od takich osób pisemnego zobowiązania się do zachowania tajemnicy zawodowej w poufności (§ 6 ust. 2). Zważywszy, że takie zobowiązanie osoby, niebędącej Radcą prawnym ani aplikantem, ma charakter cywilnoprawny, a Regulamin nie określa rygorów dla formy wskazanego oświadczenia, należy uznać, że zobowiązanie to może mieć charakter postanowienia umownego, w tym również w przypadku zawarcia umowy w formie dokumentowej (zaakceptowanie warunków świadczenia usługi drogą elektroniczną).

2.17. Istotne znaczenie ma także §10 ust. 1 w związku z §2 pkt 8) Regulaminu, który zobowiązuje Radcę prawnego do zapewnienia należytych warunków przechowywania dokumentów związanych z wykonywaniem zawodu (czynna ochrona tajemnicy zawodowej – por. pkt 5).

3. CHMURA W DZIAŁALNOŚCI RADCY PRAWNEGO

3.1. Chmura obliczeniowa to dostarczanie usług obliczeniowych — w tym serwerów, magazynu, baz danych, sieci, oprogramowania i analizy - za pośrednictwem Internetu, co umożliwia szybsze wprowadzanie innowacji, elastyczne pozyskiwanie zasobów i znaczne korzyści ekonomii skali. Oznacza to eliminację konieczności zakupu licencji czy instalowania i administracji oprogramowaniem. Zamiast nabywać i utrzymywać obiekty fizyczne (takie jak serwery) w lokalnych centrach danych (z ang. *on-premise*), od Dostawcy Usług chmurowych

można uzyskać dostęp do usług technologicznych, takich jak moc obliczeniowa, przechowywanie i aplikacje, w zależności od konkretnych potrzeb nabywcy.

3.2. Istnieją trzy główne modele świadczenia usług chmurowych:

3.2.1. **Oprogramowanie jako usługa** (z ang. *Software as a Service*, dalej: „SaaS")

Najbardziej popularna warstwa chmury obliczeniowej i najpowszechniej występująca. Polega na udostępnianiu gotowej aplikacji lub funkcjonalności systemu, bez konieczności ingerowania w ich wnętrze przez użytkownika.

Przykładami usług typu SaaS są np. Salesforce, Microsoft Office 365, aplikacje biurowe obejmujące pocztę elektroniczną, kalendarze, programy pozwalające na edycję tekstów, arkusze kalkulacyjne, aplikacje do zarządzania projektami (np. Jira), aplikacje do prowadzenia rozmów lub telekonferencji. Innym przykładem mogą być specjalistyczne aplikacje do wyszukiwania informacji prawnych.

3.2.2. **Platforma jako usługa** (z ang. *Platform as a Service*, dalej: „PaaS")

Usługa obejmuje dostarczenie internetowej platformy obliczeniowej, na której można rozwijać, testować i wdrażać aplikacje. W praktyce oznacza to udostępnienie zasobów sprzętowych wraz z technologiami, które uławiają programistom szybszy rozwój i wdrażanie aplikacji użytkownika. W tym modelu dostawca usługi nie odpowiada za funkcjonowanie i wsparcie rozwiązania, które użytkownik lokalizuje w chmurze. Dostawca odpowiada jedynie za funkcjonowanie platformy; usługi serwisowe i utrzymania systemu czy aplikacji lokalizowanych na platformie mogą być w zależności od potrzeb odrębnie nabywane przez użytkownika.

Przykładem usługi w modelu PaaS są np. Azure App Service, Heroku, Google App Engine i Openhift.

3.2.3. **Infrastruktura jako usługa** (z ang. *Infrastructure as a Service*, dalej: „IaaS")

W ramach usługi zapewniony zostaje dostęp za pomocą Internetu do fizycznej infrastruktury technologicznej, dzięki czemu można rozwijać oprogramowanie bez konieczności zakupu i utrzymania własnego sprzętu. Użytkownik (klient) sam decyduje jaki wolumen takiej infrastruktury jest mu potrzebny. Usługodawca dostarcza mu ją zaś w formie usługi zapewnienia dostępu, a nie jako fizyczny produkt.

Przykładami mogą być wirtualne serwery i dyski w chmurze służące do przechowywania i dzielenia się plikami, np. AWS Elastic Compute Cloud, Azure Virtual Machines czy Google Compute Engine

3.3. W tym kontekście Radca prawny powinien uwzględnić, że często może spotkać się z narzędziami opartymi na chmurze warstwowej (*cloud layering).* W takim przypadku określone rozwiązanie (np. rozwiązanie SaaS) zbudowane jest w środowisku PaaS, które z kolei zostało posadowione w ramach infrastruktury IaaS. Nierzadko też poszczególne warstwy rozwiązania mogą być dostarczane przez różnych Dostawców.

3.4. Radca prawny, decydując się na rozwiązanie chmurowe, powinien w związku z tym ustalić, czy i na jakich zasadach, rozwiązanie to czerpie z innych rozwiązań chmurowych. W takim wypadku, oceniając dopuszczalność korzystania z chmury oraz szacując ryzyko, Radca prawny powinien uwzględnić aspekty związane z każdą z takich technicznych warstw Usługi chmurowej.

3.5. Niezależnie od powyższego rozróżnienia, należy zdawać sobie sprawę również z podziału Usług chmurowych ze względu na kryterium właściwościowe:

3.5.1. **Chmura prywatna** – zasoby oparte na chmurze, wykorzystywane wyłącznie przez jedną organizację, z infrastrukturą lub usługami utrzymywanymi za pośrednictwem prywatnej sieci.

Z uwagi na te założenia, chmura prywatna uważana jest z reguły za rozwiązanie stwarzające najmniejsze ryzyka naruszenia poufności danych (w tym uzyskania dostępu do tajemnicy zawodowej przez osoby nieuprawnione). Warunkiem jest jednak zapewnienie odpowiednio wysokiego poziomu bezpieczeństwa wykorzystywanych rozwiązań technicznych i organizacyjnych.

Chmura prywatna jest rozwiązaniem wykorzystywanym przez wielkie organizacje, a z reguły niespotykanym w przypadku mniejszych podmiotów (takich jak większość Kancelarii prawnych). Może mieć zatem ewentualnie zastosowanie w przypadku gdy Radca prawny wykonuje pracę w przedsiębiorstwie, korzystającym z chmury prywatnej na potrzeby prowadzenia działalności gospodarczej.

3.5.2. **Chmura publiczna** – chmura publiczna jest obsługiwana przez Dostawców (podmioty trzecie), którzy wykorzystują swoją infrastrukturę w celu świadczenia usług współdzielonych (aczkolwiek rozdzielonych) na rzecz wielu użytkowników.

Z uwagi na mnogość podmiotów korzystających z tej samej infrastruktury (*tenantów*), stwarza potencjalnie najistotniejsze ryzyka z perspektywy bezpieczeństwa danych. Jednocześnie, jest to najbardziej rozpowszechniony model korzystania z Usług chmurowych, a ich Dostawcy z reguły deklarują zgodność ze standardami bezpieczeństwa i najlepszymi praktykami.

3.5.3. **Chmura hybrydowa** - hybrydowe rozwiązania chmurowe stanowią połączenie dwóch lub więcej modeli chmury (co do zasady - usług chmury prywatnej i publicznej) w sposób umożliwiający współdzielenie danych pomiędzy nie.

3.5.4. **Chmura społecznościowa** – zasoby obliczeniowe dostępne są wyłącznie dla określonej grupy użytkowników; platforma usługowa zaprojektowana z reguły w ten sposób by zaspokoić specyficzne potrzeby takiej określonej grupy.

4. TECHNOLOGIE INFORMATYCZNE

ŚRODOWISKO *ON PREMISE* A CHMURA OBLICZENIOWA

4.1. W niemal wszystkich porównaniach środowisk *on premise* w stosunku do chmury obliczeniowej wykazuje się wyższość tej ostatniej: efektywność kosztowa, skalowalność, bezpieczeństwo fizyczne, standardy zarządzania, etc. Tymczasem decyzja o korzystaniu

z Usług chmury obliczeniowej jest nie tylko decyzją techniczną, ale przede wszystkim zmianą organizacyjną i zmianą podejścia do przetwarzania – często prawnie chronionych – informacji.

4.2. Aby zrozumieć różnice w podejściu do przetwarzania informacji, warto porównać trzy klasyczne modele przetwarzania informacji: (i) we własnej serwerowni, (ii) w serwerowni lokalnej partnera technologicznego (na własnych, kolokowanych serwerach lub wynajętych) oraz (iii) w usługach chmury obliczeniowej, z punktu widzenia bezpieczeństwa przetwarzanych informacji.

4.3. Zwykle przyjmuje się, że przetwarzanie informacji we własnym (lokalnym) środowisku lub w ramach usług kolokacji jest mniej ryzykowne niż przetwarzanie informacji w usługach chmury obliczeniowej. Pogląd ten, z punktu widzenia bezpieczeństwa teleinformatycznego jest, co najwyżej, sporym, nieuprawnionym uproszczeniem. Abstrahując od skali inwestycji, które są rok do roku realizowane w ramach podniesienia bezpieczeństwa przez Dostawców Usług chmury obliczeniowej, sama koncepcja kompleksowego zapewnienia bezpieczeństwa informacji zarówno w warstwie fizycznej jak i logicznej, z narzędziami służącymi do projektowania, wdrażania i regularnego oceniania stanu bezpieczeństwa jest zasadniczo trudna do porównania z lokalną, choćby świetnie zarządzaną, serwerownią.

4.4. Jednak z punktu widzenia władztwa nad procesem przetwarzania informacji oraz ewentualnym wpływem podmiotów trzecich na samo przetwarzanie, własne zasoby dają komfort niezależności. Z drugiej jednak strony komfort ten wymaga sporych nakładów inwestycyjnych oraz pozyskania wiedzy nie tylko z zakresu systemów operacyjnych i sieci informatycznych, ale także z zakresu zarządzania infrastrukturą techniczną (serwery, macierze) i organizacją IT.

4.5. Oddając część tej niezależności podmiotom trzecim w formie kolokacji własnych zasobów w zewnętrznej, z reguły lokalnej, serwerowni uzyskujemy redukcję kosztów zarządzania infrastrukturą IT, nadal jednak przetwarzając informacje na własnych zasobach i z pewnym poczuciem niezależności od podmiotów trzecich. Z drugiej jednak strony ta optymalizacja wiąże się z koniecznością dostosowania do reguł ochrony fizycznej (zasady wejścia do obiektu) oraz spowolnieniem procesów zmian w przypadku awarii sprzętu (konieczność dojazdu, wymiany podzespołów, zmian w konfiguracji sprzętowej), co w sytuacji szybkich zmian rynkowych i stałej konieczności dostępu do informacji staje się co najmniej problematyczne.

4.6. Chmura obliczeniowa zmienia jednak te modele całkowicie. Po pierwsze przetwarzanie informacji odbywa się na infrastrukturze fizycznej, do której użytkownik nie ma dostępu – zarówno do lokalizacji przetwarzania (serwerownie – poza wybranymi trasami dla gości – są obiektami nieodstępnymi), jak i do sprzętu (operacje na infrastrukturze fizycznej są prowadzone wyłącznie przez pracowników i poddostawców dostawcy usług chmury obliczeniowej). Po drugie stosowanie (korzystanie) z Usług chmury obliczeniowej wymaga odpowiedniej, specjalistycznej wiedzy z zakresu poszczególnych Usług chmury obliczeniowej, zwłaszcza w kontekście jej bezpieczeństwa, co przy ciągłych zmianach wymaga stałego podnoszenia wiedzy w tym zakresie. Paradoksalnie jednak spora część usług (np. poczta email) jest wstępnie prekonfigurowana i gotowa do użycia w sposób niewymagający specjalnego przygotowania.

4.7. Korzystanie z Usług chmury obliczeniowej oznacza więc brak wpływu Radcy prawnego na infrastrukturę techniczną przetwarzania oraz konieczność dostosowania się do standardów

przetwarzania (technicznych, organizacyjnych i prawnych) oferowanych przez Dostawcę Usług chmury obliczeniowej. W porównaniu więc do środowisk *on premise*, chmura obliczeniowa oznacza utratę samodzielności Radcy prawnego w procesie przetwarzania informacji oraz związane z tym ryzyka wpływu podmiotów trzecich (Dostawców chmury obliczeniowej i ich Poddostawców) na sam proces przetwarzania oraz przetwarzane informacje. Przykładowo w przypadku sporu dotyczącego naruszenia warunków kontraktowych, Dostawca Usług chmury obliczeniowej ma możliwość jednostronnego wyłączenia usługi lub jej ograniczenia, co może skutkować utratą dostępu Radcy prawnego do przetwarzanych informacji i tym samym konsekwencjami dla ciągłości świadczenia pomocy prawnej.

4.8. Kluczem do zrozumienia tych ryzyk jest uświadomienie, że choć odpowiedzialność za przetwarzanie informacji spoczywa na Radcy prawnym w całości, to jednak w przypadku korzystania z Usług chmury obliczeniowej Radca prawny ma każdorazowo ograniczone możliwości wpływania na sposób tego przetwarzania.

Infrastruktura dostawcy

4.1. Ochrona wykorzystywanej do świadczenia usług infrastruktury powinna odbywać się zarówno w zakresie fizycznym jak i teleinformatycznym. Dostawcy usług chmury obliczeniowej z reguły deklarują zgodność (wykazaną certyfikatem wydanym przez niezależną jednostkę certyfikującą lub poprzez deklarację zgodności) z odpowiednimi standardami branżowymi w tym zakresie. Aspekty bezpieczeństwa fizycznego przetwarzania informacji w rozbudowanych i profesjonalnych data center obejmują m.in. nadmiarowość infrastruktury wykorzystywanej do świadczenia usług (łącza do sieci Internet, linie zasilające, podtrzymanie zasilania, etc.), zasady dostępu do poszczególnych stref przetwarzania, zasady postępowania z nośnikami, monitoring telewizji przemysłowej, ochronę fizyczną. Ochrona teleinformatyczna data center to dedykowane rozwiązania ochrony przed atakami oraz stały monitoring i zarządzanie infrastrukturą przez dedykowane zespoły inżynierów.

4.2. W przypadku przetwarzania przez Radcę prawnego informacji, stanowiących tajemnicę zawodową, w chmurze obliczeniową, Radca prawny powinien wymagać od wymagać od dostawcy deklaracji zgodności ze standardami: SOC2 Type 2 lub Tier III wg klasyfikacji Uptime Institute, lub klasa 3 wg PN-EN 50600 lub zawarcia w umowie opisu stosowanych zabezpieczeń infrastrukturalnych na równoważnym poziomie.

Dostęp do przetwarzanych informacji i podział odpowiedzialności za ich przetwarzanie w Usługach chmury obliczeniowej

4.3. Radca prawny jest odpowiedzialny za bezpieczeństwo informacji, które zamierza przetwarzać. Stwierdzenie to zdaje się być w pełni realizowalne w przypadku posiadania własnych zasobów (własna serwerownia) i w znacznej części podobnie realizowalnej dla kolokacji zasobów.

4.4. W chmurze obliczeniowej sytuacja jest inna. Klasyczny podział modeli dostarczania Usług chmury obliczeniowej (IaaS, PaaS, SaaS) jest jednocześnie klasycznym modelem podziału umownej odpowiedzialności za bezpieczeństwo przetwarzania i w istotnej części również odpowiada zasadom dostępu do przetwarzanych informacji.

4.5. Dostawca Usług chmury obliczeniowej jest odpowiedzialny za zapewnienie bezpieczeństwa fizycznego, poprawność działania infrastruktury teleinformatycznej (w tym telekomunikacyjnej) oraz ciągłość jej działania (w tym odporność na awarie całego systemu informatycznego). Dodatkowo – zależnie od konkretnej Usługi chmurowej – Dostawca może odpowiadać za aktualność wersji oprogramowania (np. systemu operacyjnego), poprawki bezpieczeństwa itp.

4.6. Należy podkreślić, że powyższe nie zmienia jednak ogólnej zasady pełnej odpowiedzialności Radcy prawnego za informacje, które przetwarza przy pomocy Usług chmury obliczeniowej, w szczególności za zapewnienie poufności tajemnicy zawodowej. W celu zapewnienia bezpieczeństwa informacji Dostawcy Usług chmury obliczeniowej przygotowali zestaw narzędzi, które Radca prawny może i powinien wykorzystać. Narzędzia te obejmują m.in. zarządzanie bezpiecznym dostępem do konfiguracji usług, szyfrowanie przetwarzanych informacji, raportowanie stanu usług.

4.7. Radca prawny musi być świadomy, że korzystanie z Usług chmury obliczeniowej bez zrozumienia i wdrożenia (konfiguracji) odpowiednich narzędzi bezpieczeństwa może skutkować (również niezamierzonym) ujawnieniem przetwarzanej informacji.

4.8. W szczególności w sytuacjach awaryjnych, gdy potrzebne jest wsparcie w rozwiązaniu problemu, Radca prawny może – a w razie zagrożenia dla bezpieczeństwa informacji objętej tajemnicą zawodową – powinien, poprosić o pomoc Dostawcę Usług chmury obliczeniowej. Dostawca (który z kolei może posługiwać się w tym zakresie wsparcie podwykonawców, w tym podwykonawcach zlokalizowanych w dowolnym miejscu na ziemi), może zatem potencjalnie uzyskiwać dostęp do informacji prawnie chronionej. W takim wypadku Radca prawny zobowiązany jest wymagać od Dostawcy zobowiązania się do zachowania przetwarzanych informacji w poufności i zapewnienia analogicznego zobowiązania po stronie jego podwykonawców. To zobowiązanie może mieć postać stosownego postanowienia umownego.

4.9. Podobnie w sytuacji zatrudniania do celów administracji środowiskiem chmury obliczeniowej zewnętrznych dostawców usług IT, należy upewnić się, że Dostawca rozumie ograniczenia wynikające ze szczególnej roli i wymagań wobec Radcy prawnego i ograniczeń związanych z przetwarzaniem informacji stanowiących tajemnicę zawodową lub dane osobowe. Jest to tym bardziej istotne, że niektóre z Usług chmury obliczeniowej mogą wiązać się z przetwarzaniem informacji w różnych regionach zlokalizowanych również poza EOG, na co Radca prawny może nie mieć wpływu lub wpływ ten jest pod warunkiem skorzystania z właściwej konfiguracji Usługi chmurowej.

4.10. Jak wynika z powyższych rozważań, korzystanie z Usług chmury obliczeniowej wymaga posiadania dedykowanych kompetencji, również w zakresie technicznym. Dlatego Radca prawny powinien rozważyć skorzystanie z pomocy osób lub podmiotów, które posiadają doświadczenie i umiejętności w planowaniu i konfiguracji Usług chmury obliczeniowej, z których zamierza skorzystać.

4.11. Korzystanie z Usług chmury obliczeniowej jest oparte o relację zaufania – Radca prawny ufa Dostawcy Usług chmury obliczeniowej, że przetwarzanie informacji będzie odbywało się zgodnie z deklarowanymi zasadami i dobrymi praktykami w obszarze teleinformatyki, włącznie z newralgicznymi aspektami cyberbezpieczeństwa. Z tego względu Radca prawny powinien poprzedzić rozpoczęcie korzystania z Usługi chmurowej oceną Dostawcy pod kątem dawania przez niego rękojmi prawidłowego, bezpiecznego przetwarzania danych.

W ocenie Dostawcy Usług chmury obliczeniowej pomocne będą deklaracje zgodności, certyfikaty oraz inne dokumenty, które mogą poświadczać, że przetwarzanie informacji odbywa się w oparciu o międzynarodowe standardy i w udokumentowany sposób. Rekomendowane jest, aby Dostawca Usług chmury obliczeniowej deklarował zgodność swojego postępowania z normą ISO 27001 (Zarządzanie bezpieczeństwem informacji) oraz innymi standardami, np. SOC. Niemniej należy też zaznaczyć, że certyfikaty czy deklaracje mogą być pomocne przykładowo w ocenie zasad zarządzania obszarem bezpieczeństwa przetwarzania, ale nie zastąpią procesu szacowania ryzyka.

KRYPTOGRAFIA A BEZPIECZEŃSTWO PRZETWARZANYCH INFORMACJI

4.12. Zrozumienie zasad używania technik kryptograficznych wbudowanych (implementowanych) w Usługi chmury obliczeniowej jest kluczowe dla poprawnego zabezpieczenia przetwarzanych informacji. Główni Dostawcy Usług chmury obliczeniowej zachęcają, a w przypadku niektórych Usług chmurowych, wręcz wymuszają korzystanie z kryptografii, choćby poprzez domyślne szyfrowanie najbardziej newralgicznych komponentów Usług chmury obliczeniowej, które z reguły zawierają przetwarzane przez klienta (Radcę prawnego) informacje.

4.13. W kontekście korzystania z Usług chmury obliczeniowej szczególną uwagę należy zwracać na szyfrowanie podczas przesyłania informacji oraz podczas ich składowania (przechowywania).

4.14. W pierwszym przypadku mamy do czynienia z szyfrowaniem „in transit", np. podczas łączenia się programu pocztowego Outlook zainstalowanego na komputerze z serwerami Microsoft w usłudze Microsoft365, w celu pobrania lub wysłania poczty elektronicznej. Zestawiane połączenie jest w tej usłudze zabezpieczone kryptograficznie, a przesyłane informacje są szyfrowane odpowiednim algorytmem szyfrującym przy użyciu klucza / kluczy szyfrujących.

4.15. W drugim przypadku mamy do czynienia z szyfrowaniem „at rest", np. podczas przechowywania plików w usłudze Microsoft OneDrive. Folder użytkownika Usługi chmurowej jest w tej usłudze zabezpieczony kryptograficznie, a przechowywane (zapisane) informacje w formie plików są zaszyfrowane odpowiednim algorytmem szyfrującym.

4.16. Obydwa powyższe stany nie wyczerpują zagadnień związanych z kryptografią, jednak w praktyce Radcy prawnego będą najczęściej używanymi i najbardziej newralgicznymi. Dla Radcy prawnego standardem przy korzystaniu z Usług chmury obliczeniowej powinno być każdorazowo weryfikowanie, czy łączenie się i przesyłanie informacji do i z Usługi chmury obliczeniowej odbywa się w zabezpieczony kryptograficznie sposób oraz czy przechowywane (zapisane, składowane) w Usłudze chmurowej informacje są szyfrowane. Zaniedbanie jednego z tych elementów w praktyce prowadzi do wysokiego ryzyka ujawnienia przetwarzanej informacji. Przypadki tzw. „wycieków informacji" z Usług chmury obliczeniowej są z reguły spowodowane nie wymyślnymi atakami hakerskimi, ale błędami w konfiguracji zabezpieczeń związanych z limitowaniem dostępu do przetwarzanych informacji lub właśnie brakiem szyfrowania (np. baz danych, kopii bezpieczeństwa).

4.17. **Szyfrowanie nie powoduje zmiany charakteru informacji jako takiej, w tym jej charakter tajemnicy zawodowej**. Zaszyfrowana informacja nadal podlega ochronie prawnej. Szyfrowanie nie powoduje więc zniesienia wymagań wobec Radcy prawnego

związane z ochroną informacji (w szczególności zapewnieniem poufności tajemnicy zawodowej). Szyfrowanie pozwala jednak na stosowanie standardów fizycznej ochrony przetwarzanych informacji na bardziej umiarkowanym poziomie, ponieważ ewentualne upublicznienie zaszyfrowanej informacji bez ujawnienia klucza szyfrującego – choć jest incydentem bezpieczeństwa – nie jest jednak tak groźne, jak ujawnienie informacji, czyli jej upublicznienie w postaci jawnej.

4.18. Co do zasady, szyfrowanie informacji powinno odbywać się za pomocą algorytmów, które nie są uznane za kryptograficznie skompromitowane (złamane) oraz przy wykorzystaniu kluczy szyfrujących zarządzanych (generowanych, odpowiednio stosowanych i usuwanych) przez Radcę prawnego. W praktyce, pierwszy z warunków jest stosunkowo łatwy do spełnienia w przypadku Usług chmury obliczeniowej: Dostawcy Usług chmury obliczeniowej aktualizują regularnie stosowane algorytmy szyfrowania eliminując te, które – w zgodnie z aktualnym stanem wiedzy w zakresie cyberbezpieczeństwa i kryptografii – mogłyby poprzez swoje słabości prowadzić do odszyfrowania informacji. Dodatkowo wśród największych Dostawców Usług chmury obliczeniowej standardem jest domyślne stosowanie szyfrowania.

4.19. Bardziej złożonym procesem jest spełnienie drugiego z warunków – samodzielnego zarządzania przez Radcę prawnego kluczami szyfrującymi, które wymaga z reguły nie tylko odpowiedniej infrastruktury, ale także specjalistycznej wiedzy. Dostrzegając ten problem, Dostawcy Usług chmury obliczeniowej wprowadzili możliwość zarządzania kluczami szyfrującymi w oparciu o własną infrastrukturę udostępnianą w formie usług, co – biorąc pod uwagę koszt utrzymywania dedykowanych rozwiązań we własnym zakresie – jest dobrą alternatywą. Radca prawny powinien być uprawniony do korzystania z Usług chmurowych Dostawców w zakresie zarządzania kluczami szyfrującymi, z wyjątkiem przypadków, gdy z procesu szacowania ryzyka wyniknie konieczność samodzielnego zarządzania kluczami przez Radę prawnego lub zlecenia zarządzania kluczami osobie trzeciej, w szczególności innemu Dostawcy Usługi chmurowej.

4.20. Szyfrowanie przetwarzanych informacji zarówno „at rest" jak i „in transit" powinno być standardem w przypadku korzystania z Usług chmury obliczeniowej, a w przypadku przetwarzania informacji kwalifikowanych jako tajemnica zawodowa – obowiązkiem.

5. TAJEMNICA ZAWODOWA

5.1. Ustawa o radcach prawnych przewiduje fundamentalny obowiązek zachowania przez Radcę prawnego w tajemnicy wszystkiego, o czym dowiedział się w związku z udzieleniem pomocy prawnej (art. 3 ust. 3 Urp).

ZAKRES PRZEDMIOTOWY I PODMIOTOWY TAJEMNICY ZAWODOWEJ

5.2. Przepisy odnoszące się do tajemnicy zawodowej nie definiują jej bezpośrednio. W celu określenia przedmiotu tajemnicy zawodowej, należy wskazać, że zgodnie z Urp Radca prawny zobligowany jest zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzielaniem pomocy prawnej. Oznacza to, że tajemnicą zawodową będą objęte także informacje, które dotyczą klienta, chociaż nie były wprost wykorzystywane przez niego w świadczeniu pomocy prawnej.

5.3. KERP doprecyzowuje powyższą, ogólną definicję, poprzez wskazanie, że obowiązująca Radców prawnych tajemnica zawodowa obejmuje:

5.3.1. **informacje dotyczące klienta i jego spraw**, ujawnione Radcy prawnemu przez klienta bądź uzyskane w inny sposób w związku z wykonywaniem przez niego jakichkolwiek czynności zawodowych, niezależnie od źródła tych informacji oraz formy i sposobu ich utrwalenia;

5.3.2. wszelkie tworzone przez Radcę prawnego **dokumenty;**

5.3.3. **korespondencję Radcy prawnego z klientem** i osobami uczestniczącymi w prowadzeniu sprawy - powstałe dla celów związanych ze świadczeniem pomocy prawnej;

5.3.4. **informacje ujawnione Radcy prawnemu przed podjęciem przez niego czynności zawodowych**, jeżeli z okoliczności sprawy wynika, że ujawnienie nastąpiło dla potrzeb świadczenia pomocy prawnej i uzasadnione było oczekiwaniem, że radca prawny będzie ją świadczył;

5.3.5. przebieg i treść **pertraktacji ugodowych**, w których brał czynny udział.

Warto zwrócić uwagę, że powyższy katalog ma charakter otwarty, a tajemnica zawodowa rozciąga się także na informacje, które Radca prawny uzyskał w inny sposób – np. takie, które zostały przekazane przez klienta nieświadomie bądź Radca prawny otrzymał od rodziny czy współpracowników klienta, o ile informacje te zostały przekazane przy okazji wykonywania obowiązków zawodowych Radcy prawnego.

5.4. Z perspektywy podmiotowego zakresu tajemnicy zawodowej, obowiązek ten obejmuje nie tylko Radców prawnych, lecz także aplikantów radcowskich. Każdorazowo należy także uwzględnić, że w szeroko rozumianym procesie świadczenia pomocy prawnej, profesjonalni pełnomocnicy wspierani są przez podmioty trzecie tj. personel administracyjny, a także inne osoby zatrudnione w Kancelarii lub osoby, którym radca prawny zleca czynności. Upr nie narzuca bezpośrednio obowiązku zachowania tajemnicy przez takie osoby. Kwestia ta została natomiast uwzględniona w art. 22 KERP, w którym na Radcę prawnego nałożony został nakaz zobowiązania osób z nim współpracujących do zachowania poufności. Obowiązek ten został doszczegółowienia w §6 Regulaminu, nakazujący żądanie złożenia pisemnego oświadczenia w tym zakresie.

5.5. Z perspektywy sposobu utrwalenia informacji, objęte tajemnicą będą nie tylko informacje przekazane w formie ustnej, papierowej, drogą elektroniczną czy za pomocą nośników informacji (np. na płycie CD, DVD, pendrive), **lecz także informacje utrwalone w chmurze obliczeniowej.**

5.6. Obowiązek zachowania tajemnicy zawodowej **nie może być ograniczony w czasie** i istnieje również po zaprzestaniu wykonywania zawodu. Zgodnie z art. 23 KERP Radca prawny obowiązany jest **zabezpieczyć przed niepowołanym ujawnieniem** wszelkie informacje objęte tajemnicą zawodową, **niezależnie od ich formy i sposobu utrwalenia**. Dokumenty i nośniki przechowywane w formie elektronicznej powinny być objęte odpowiednią kontrolą dostępu oraz zabezpieczeniem systemu przed zakłóceniem działania, uzyskaniem nieuprawnionego dostępu lub utratą danych.

5.7. Co do zasady tajemnica zawodowa Radcy prawnego powinna być postrzegana jako mająca charakter bezwzględny – nawet w sytuacjach, w których przepisy dopuszczają zwolnienie z niej Radcy prawnego. Samo naruszenie tego obowiązku może stanowić podstawę do odpowiedzialności dyscyplinarnej Radcy prawnego (art. 64 Urp).

5.8. Przepisy przewidują jednak zarówno wyłączenia przedmiotowe jak i możliwości zwolnienia z tajemnicy zawodowej.

Wyłączenia przedmiotowe

5.9. Bezpośrednio obowiązek zachowania tajemnicy zawodowej przez Radcę prawnego ustanawia art. 3 ust 6 Urp, zgodnie z którym obowiązek zachowania tajemnicy zawodowej nie dotyczy informacji (i) udostępnianych na podstawie przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (AML) oraz (ii) przekazywanych na podstawie przepisów rozdziału 11a działu III ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz.U. z 2019 r. poz. 900, z późn. zm.1) – w zakresie określonym tymi przepisami.

5.10. W świetle powyższych zasad, informacje podlegające raportowaniu na podstawie przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, są wyłączone z zakresu tajemnicy zawodowej. Wyłączenie to nie dotyczy jednak informacji uzyskanych podczas ustalania sytuacji prawnej klienta w związku z postępowaniem sądowym, wykonywaniem obowiązków polegających na obronie, reprezentowaniu lub zastępowaniu klienta w postępowaniu sądowym albo udzielaniu klientowi porady prawnej dotyczącej wszczęcia postępowania sądowego lub uniknięcia takiego postępowania, niezależnie od czasu uzyskania tych informacji (art. 75 ustawy AML). Informacje przekazywane właściwym organom podlegają – niezależnie od powyższego – autonomicznemu obowiązkowi zachowania tajemnicy na podstawie art. 54 ustawy AML.

5.11. Wprowadzenie uregulowań dotyczących ujawniania informacji o schematach podatkowych Szefowi Krajowej Administracji Skarbowej (KAS) wynika z wymogu wdrożenia postanowień Dyrektywy Rady (UE) 2018/822 z dnia 25 maja 2018 r. Nowe przepisy wprowadzające obowiązek informowania o schematach podatkowych przewidują szczególny tryb zwalniania z tajemnicy zawodowej. Zgodnie z art. 86b. § 1 Ordynacji podatkowej, Radca prawny działając jako promotor ma obowiązek przekazać szefowi KAS informację o schemacie podatkowym w ciągu 30 dni od udostępnienia schematu podatkowego, przygotowania do wdrożenia schematu podatkowego lub od dnia dokonania pierwszej czynności związanej z wdrażaniem schematu podatkowego. Przepisy ordynacji podatkowej nie wskazują jednak jednoznacznie trybu zwolnienia z tajemnicy, odnosząc się jedynie do możliwości zwolnienia z tajemnicy zawodowej przez korzystającego – czyli klienta. Powyższe pozostaje w sprzeczności z art. 180 § 2 Ustawy z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego (kpk), zgodnie z którym Radcowie prawni mogą odmówić zeznań co do faktów, na które rozciąga się tajemnica zawodowa, a z tajemnicy tej może ich zwolnić jedynie sąd.

5.12. Art. 86b § 7 Ordynacji podatkowej wymienia natomiast katalog działań Radcy prawnego, które nie stanowią naruszenia obowiązku zachowania prawnie chronionej tajemnicy zawodowej. I tak, naruszenia tej tajemnicy nie będzie stanowiło:

5.12.1. przekazanie informacji o schemacie podatkowym w sytuacji, w której przekazujący tę informację został zwolniony z obowiązku jej zachowania;

5.12.2. przekazanie informacji o schemacie podatkowym standaryzowanym;

5.12.3. przesłanie do szefa KAS informacji, że promotor powiadomił korzystającego o obowiązku zgłoszenia schematu podatkowego.

5.13. Należy wskazać że o wynikających z art. 3 ust 6 pkt 2) Urp zasadach krytycznie wypowiada się środowisko radcowskie – przede wszystkim wskazując na brak podstawy prawnej wprowadzenia przepisów Ordynacji podatkowych przewidujących możliwość zwolnienia Radcy prawnego przez klienta z tajemnicy zawodowej oraz podkreślając bezzasadność nałożenia na Radców prawnych obowiązków dotyczących raportowania w stopniu szerszym niż to wynika z Dyrektywy Rady (UE) 2018/822.

Zwolnienie z tajemnicy zawodowej

5.14. KERP stanowi, że „radca prawny powinien podejmować wszelkie przewidziane prawem środki dla uniknięcia lub ograniczenia określonego w przepisach prawa zwolnienia go z obowiązku zachowania tajemnicy zawodowej". Możliwość zwolnienia Radcy prawnego z obowiązku dochowania tajemnicy zawodowej dopuszczają przepisy kpk w zakresie przesłuchania i przeszukania, przepisy dotyczące sejmowej komisji śledczej w zakresie przesłuchania, ustawy o ochronie konsumentów i konkurencji w zakresie przeszukania oraz ustawy o policji w zakresie wykorzystywania informacji pocztowych, telekomunikacyjnych i internetowych.

5.15. Art. 180 § 2 kpk ustanawia możliwość przesłuchania Radcy prawnego co do faktów objętych tajemnicą zawodową, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu. Zastosowanie zwolnienia uzależnione jest więc od wystąpienia dwóch przesłanek: musi być to niezbędne dla dobra wymiaru sprawiedliwości oraz okoliczność nie może być ustalona na podstawie innego dowodu. W przypadku zwolnienia z tajemnicy zawodowej sąd przesłuchuje taką osobę z wyłączeniem jawności. Należy jednak podkreślić, że instytucja zwolnienia ma wyjątkowy charakter[2].

5.16. Możliwość zwolnienia z tajemnicy zawodowej nie obejmuje tajemnicy obrończej, mającej na mocy art. 178 pkt 1 kpk charakter bezwzględny.

5.17. Zarówno na gruncie postępowania cywilnego jak i administracyjnego, tajemnica zawodowa chroniona jest odmiennie niż w kpk – przez udzielenie Radcy prawnemu możliwości odmowy odpowiedzi. Postępowanie cywilne zasadniczo dopuszcza jako dowód przesłuchanie każdego, kto może mieć wiedzę na temat istotnych okoliczności sprawy. Jednakże zgodnie z art. 261 § 2 Ustawy z dnia 17 listopada 1964 r. - Kodeks postępowania cywilnego (kpc) Radca prawny, który został powołany na świadka może skorzystać z prawa odmowy odpowiedzi na pytanie, jeżeli zeznania mogłyby wiązać się z pogwałceniem istotnej tajemnicy zawodowej. Również art. 83 § 2 Ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (kpa) pozwala Radcy prawnemu odmówić odpowiedzi na pytanie, gdy w jego ocenie może naruszy to tajemnicę zawodowa. Powyższe potwierdza stanowisko Sądu Najwyższego: w przypadku w którym Radca prawny powoła się na bezwzględny zakaz ujawniania informacji uzyskanych od klienta i odmówi składania zeznań,

[2] Postanowienie SA w Katowicach z 19.6.2013 r. (II AKz 303/13, OSA 2013 Nr 3, poz. 1).

nie można skutecznie postawić zarzutu zatajenia prawdy - nawet jeśli sąd zwolni takiego Radcę prawnego z tajemnicy zawodowej[3].

Zgoda klienta na ujawnienie tajemnicy

5.18. Zgoda klienta nie zwalnia Radcy prawnego z obowiązku zachowania tajemnicy zawodowej. Zgodnie ze stanowiskiem Sądu Najwyższego złożenie przez Radcę prawnego zeznań w postępowaniu karnym toczącym się przeciwko jego klientowi, bez zwolnienia przez sąd z tajemnicy zawodowej jest przewinieniem, którego popełnienie może skutkować nałożeniem kary dyscyplinarnej[4]. Poniesienie odpowiedzialności dyscyplinarnej nie jest zatem zależne od tego, czy ujawnione przez pełnomocnika informacje szkodzą klientowi oraz czy klient wyraził zgodę na ujawnienie tych informacji. Samo zachowanie tajemnicy zawodowej Radcy prawnego ma charakter publiczno-prawny. W związku z tym to Radca prawny jest odpowiedzialny za zachowanie tajemnicy zawodowej – klient nie jest jej dysponentem i nie decyduje o zwolnieniu z jej zachowania Radcy prawnego[5].

Informowanie o wykonywaniu zawodu

5.19. Od powyższych rozważań odróżnić należy wyraźnie sytuację informowania przez Radcę prawnego o wykonywaniu zawodu, w tym realizowaniu określonych projektów na rzecz wskazanych klientów. akie sytuacje, uzasadnione zwyczajem i względami biznesowymi obejmują np. powoływanie się na referencje klienta czy informowanie o świadczeniu usług na rzecz określonego klienta w materiałach informacyjnych radcy prawnego – w każdym przypadku w zakresie zaakceptowanym przez klienta.

Ważność informacji

5.20. Z powyższych rozważań wynika, że poszczególne informacje przetwarzane przez Radcę prawnego mogą posiadać różny status, przy czym sam podział na tajemnicę zawodową i informacje nieobjęte tajemnicą zawodową nie jest jedynym, który należy uwzględnić. Sama tajemnica zawodowa ma charakter niejednolity, a jej niezamierzone ujawnienie może wiązać się ze skutkami różnej wagi (np. ujawnienie informacji, że firma X korzysta z usług Radcy prawnego skutkuje mniejszym zagrożeniem niż wyciek treści pozwu skierowanego przez Radcę prawnego w imieniu firmy X; ujawnienie informacji, że Jan Kowalski korzysta z usług Kancelarii, specjalizującej się w prawie karnym ma inną wagę niż ta sama informacja odnosząca się do korzystania z usług prawnika specjalizującego się w sprawach spadkowych).

5.21. Radca prawny, decydując się na umieszczenie chronionych tajemnicą zawodową informacji w infrastrukturze informatycznej zewnętrznego Dostawcy, powinien zatem uwzględnić, że chociaż tajemnica zawodowa rozciąga się na całość uzyskanych informacji, to możliwe jest dokonanie w pewnym zakresie różnicowania ważności tych informacji i tym samym – zróżnicowania sposobu szacowania ryzyka związanego z ujawnieniem objętych tajemnicą informacji. W tym celu należy brać pod uwagę kryteria odnoszące się np.: (i) do rodzaju informacji, w posiadanie których wchodzi Radca prawny, (ii) charakteru oraz doniosłości

[3] Uchwała składu 7 sędziów SN z 22 stycznia 2003 r., I KZP 39/02.
[4] Postanowienie Sądu Najwyższego z dnia 15 listopada 2012 r., SDI 32/12.
[5] Postanowienie Sądu Najwyższego z dnia 24 września 2019 r. II DSI 51/19.

prowadzonych spraw czy (iii) osoby klienta. Radca prawny powinien ocenić w tym świetle, w jaki sposób naruszenie bezpieczeństwa informacji wpłynie na bezpieczeństwo tajemnicy radcowskiej lub obrończej oraz ciągłość świadczenia pomocy prawnej, a w konsekwencji finanse i reputację Radcy prawnego. Ten ostatni aspekt również powinien mieć wpływ na ocenę ważności informacji, zważywszy, że zaufanie klienta do Radcy prawnego stanowi fundament świadczenia pomocy prawnej.

Czynny obowiązek ochrony tajemnicy zawodowej

5.22. Radca prawny zobowiązany jest nie tylko do zachowania w poufności informacji objętych tajemnicą zawodową (bierna ochrona informacji) ale także adekwatnie zabezpieczyć wszelkie informacje objęte tajemnicą zawodową (art. 23 KERP, § 6 Regulaminu).

5.23. Przetwarzanie danych oraz przechowywanie dokumentów w chmurze obliczeniowej nie zwalnia Radcy prawnego z obowiązku szczególnej ochrony informacji objętych tajemnicą zawodową i w żaden sposób nie ogranicza zakresu tej tajemnicy. Odpowiednio zastosowana technologia chmurowa może jednak pomóc w osiągnięciu relatywnie wyższego poziomu bezpieczeństwa informacji objętych tajemnicą w stosunku do standardowych rozwiązań opartych na fizycznym obiegu dokumentacji i korespondencji. Przykładowo – dzięki zapewnieniu odpowiedniego poziomu szyfrowania i uwierzytelniania – dokumentacja przechowywana i wymieniana w chmurze może być znacznie lepiej chroniona przed nieuprawnionym dostępem niż dokumenty przesyłane i przechowywane w postaci papierowej, a tym samym gwarantować wyższy stopień ochrony informacji objętych tajemnicą zawodową. Ocena zabezpieczeń powinna być jednak każdorazowo przeprowadzona w udokumentowanym procesie szacowania ryzyka.

6. PODEJŚCIE OPARTE NA RYZYKU

6.1. Dominującym podejściem organów samorządów zawodowych a także organów publicznoprawnych w poszczególnych sektorach gospodarki, jak pokazują przywołane wyżej standardy referencyjne, staje się podejście oparte na ryzyku.

6.2. Tego rodzaju zmiana w sposobie myślenia o tworzeniu regulacji, wytycznych i standardów. wynika z dynamicznych przemian otoczenia informatycznego (w tym w działalności Radców prawnych) i stale rosnącej rolę narzędzi teleinformatycznych takich jak Usługi przetwarzania w chmurze obliczeniowej. Z perspektywy działalności Radcy prawnego, podejście oparte na ryzyku umożliwia także dostosowanie podejmowanych działań do wielkości i charakteru organizacji, w tym Kancelarii.

6.3. Podejście oparte na ryzyku za punkt wyjścia przyjmuje proces zarządzania ryzykiem, rozumiany jako systematyczne stosowanie polityki, procedur i praktyki zarządzania do zadań ustalania kontekstu ryzyka, jego identyfikowania, analizowania, wyznaczania, postępowania z ryzykiem oraz monitorowania i komunikowania ryzyka[6]. Jest to tylko jedna z wielu definicji.

[6] Taką definicje podejścia opartego na ryzyku prezentowała m.in. norma ISO PN-IEC 62198:2005 zastąpiona PN-IEC 62198:2014.

6.4. Standardem europejskim mówiącym o zarządzaniu ryzykiem jest norma na podstawie ISO 31000 Zarządzanie ryzykiem - Zasady i wytyczne. W naukach informatycznych i działalności IT, w tym w szczególności w bezpieczeństwie informacji stosuje się przede wszystkim podejście oparte na szacowaniu ryzyka, które zawiera w sobie już elementy identyfikacji potencjalnych ryzyk oraz określa sposoby zarządzania tymi ryzykami. Najpowszechniej stosowanym standardem w tym zakresie jest norma PN-EN ISO/IEC 27001[7]. Wskazane dokumenty normalizacyjne zostały podane jako przykłady, i oczywiście mogą zostać ewentualnie wykorzystane w działalności całej organizacji i to nie tylko w procesach korzystania z Usług przetwarzania w chmurze obliczeniowej. Pokazują one, że podejście oparte na ryzyku jest podejściem sprawdzonym, sformalizowanym, o określonych regułach i zasadach postępowania, wymagającym wdrożenia wewnętrznych stałych reguł działania.

6.5. Podejście oparte na ryzyku jest procesem ciągłym, wymagającym stałej identyfikacji i szacowania poziomu ryzyka związanego z przetwarzaniem informacji podczas całego cyklu jej przetwarzania, od momentu wytworzenia informacji lub jej otrzymania, przez jej przekształcenia aż po jej usuniecie w sposób uniemożliwiający odtworzenie. **Naturalną konsekwencją zarządzania ryzykiem we wskazanych sposób, jest odejście od sztywnych, niezmiennych reguł dotyczących stosowanych zabezpieczeń i procedury operacyjnych, na rzecz elastycznego podejścia, pozwalającego na bieżąco reagować na zidentyfikowane zagrożenia i dobierać środki zaradcze stosownie do okoliczności, z zachowaniem zasady proporcjonalności.**

6.6. Podejście oparte na ryzyku zakłada, że pewna pula ryzyk (niepewności, niebezpieczeństw) jest możliwa do identyfikacji, a podmiot jest w stanie ocenić zakres i charakter ewentualnych szkodliwych konsekwencji wystąpienia zidentyfikowanych ryzyk. Zgodnie z tym założeniem, taki podmiot potrafi także ocenić możliwości uniknięcia tych konsekwencji oraz - co bardzo istotne - ocenić swój tzw. „apetyt na ryzyko".

6.7. Podejście oparte na ryzyku nie jest więc wyłącznie metodologią pozwalającą minimalizować szkody dla organizacji. Jest także cennym źródłem wiedzy dla podejmowania jak najbardziej racjonalnych decyzji w jej bieżącej działalności.

6.8. Wartością tego rodzaju podejścia jest zatem możliwość adaptacji do zmiennej sytuacji prawnej jak i faktycznej. Przykładem takiej sytuacji był wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-311/18 (*Schrems II*), w którym TSUE uchylił decyzję Komisji Europejskiej nr 2016/1250 w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności wymianie danych osobowych między UE a USA oraz wypowiedział się o sposobie stosowania standardowych klauzul umownych w przekazywaniu danych osobowych do państw trzecich, w tym do Stanów Zjednoczonych Ameryki. Podejście oparte na ryzyku pozwala w szybki sposób ustalić, czy dane które są przetwarzane w organizacji wchodzą w zakres objęty wyrokiem i jakie środki należy w związku z tym podjąć, aby zminimalizować ryzyko niezgodności regulacyjnej.

6.9. Od strony praktycznej podejście oparte na ryzyku powinno opierać się o zorganizowany system zarządzania ryzykiem (np. w postaci procedur lub instrukcji). W każdym przypadku system ten powinienem zapewniać podstawowe elementy, tj.:

[7] Zob. Norma PN-EN ISO/IEC 27001

6.9.1. określenie wykorzystywanych zasobów informacyjnych oraz identyfikacja narzędzi;

6.9.2. ustalenie kontekstu (procesu, informacji, jej charakteru, charakteru podmiotu skali przedsięwzięcia itp.);

6.9.3. identyfikacja zagrożeń oraz szacowanie ich wpływu na wybrane parametry działalności;

6.9.4. szacowanie prawdopodobieństwa wystąpienia zagrożenia;

6.9.5. szacowanie ryzyka i określenie strategii postępowania z ryzykiem;

6.9.6. ustalenie osób biorących udział w procesie zarządzania ryzykiem, ich ról i zakresu odpowiedzialności;

6.9.7. ustalenie osób nadzorujących proces zarządzania ryzykiem;

6.9.8. określenie zasad monitorowania ryzyka i raportowania wyników takiego monitorowania.

6.10. Podejście oparte na ryzyku w przypadku przetwarzania informacji w Kancelarii, w szczególności w przypadku planowanego skorzystania z Usług przetwarzania w chmurze winno stanowić podstawowe podejście. Radca prawny, decydując się na korzystanie z chmury obliczeniowej, powinien zatem stosować podejście oparte na ryzyku i podejmować decyzje w oparciu o szacowanie ryzyka. Standard proponuje określoną metodykę postępowania w tym zakresie, przez co może stanowić przydatne narzędzie dla Radcy prawnego; nie stanowi jednak jedynego możliwego podejścia do zarządzania ryzykiem.

WYBRANE STANDARDY REFERENCYJNE PRZETWARZANIA INFORMACJI PRZEZ PRAWNIKÓW

6.1. Poniżej wskazano wybrane standardy przetwarzania informacji przez prawników przy użyciu technologii informatycznych. Mimo że standardy te nie wiążą Radcy prawnego, powinny być traktowane jako jeden z punktów odniesienia dla zdefiniowania najlepszych praktyk w tym obszarze.

Przewodnik CCBE „Komunikacja elektroniczna i Internet" oraz „Wytyczne w sprawie używania usług w chmurze przez prawników" [8]

6.2. Przewodnik zawiera rekomendacje w zakresie m. in. obsługi poczty elektronicznej i stron internetowych, oprogramowania antywirusowego, a także dobrych praktyk w zakresie archiwizacji dokumentacji elektronicznej i poczty – z uwzględnieniem obowiązku ochrony tajemnicy zawodowej i danych osobowych. Przewodnik CCBE stanowi odpowiedni punkt wyjścia dla zasygnalizowania podstawowych wyzwań, którym sprostać muszą członkowie Izby rozpoczynający korzystanie z usług chmurowych. Dokument podkreśla m.in.

[8] CCBE, "Response regarding the European Commission Public Consultation on Cloud Computing" z 9 września 2011 oraz CCBE "Guidelines on the use of cloud computing services by lawyers" z 7 września 2012, wersja polska dostępna pod adresem: http://kirp.pl/wp-content/upload- s/2017/08/2012-09-07-wytyczne-ccbe-w-zakresie-korzystania-przez-prawni- kow-z-uslug-pracy-w-chmurze.pdf

konieczność uwzględnienia już na etapie rozważania poszczególnych rozwiązań chmurowych, norm regulujących ochronę danych osobowych oraz zasad etyki chroniących tajemnicę zawodową.

6.3. Jako główne ryzyko związane z wdrożeniem chmury obliczeniowej przez Kancelarie prawne Wytyczne wskazują szczególne wymogi nałożone na prawników (radców prawnych, adwokatów) w zakresie zapewnienia poufności danych klientów – chodzi tu przede wszystkim o kwestię dopuszczalności przechowywania danych poza Kancelarią oraz problem dostępu do danych osób trzecich.

6.4. Przed podjęciem decyzji o wyborze konkretnego Dostawcy, prawnik powinien w pierwszej kolejności zweryfikować doświadczenie, reputację, specjalizacje oraz siedzibę i lokalizację Dostawcy Usług chmurowych. Następnie należy przyjrzeć się takim kwestiom, jak wiarygodność, wypłacalność, potencjalny konflikt interesów czy zagadnienia związane z bezpieczeństwem własnością danych (lokalizacja serwerów, stosowane zabezpieczenia, ryzyko niedozwolonego wykorzystania zgromadzonych informacji). Zgodnie z Wytycznymi, w odniesieniu do środków bezpieczeństwa, prawnik powinien upewnić się, że wybrany Dostawca działa w oparciu o procedury zgodne z międzynarodowymi standardami zarządzania ryzykiem IT, takimi jak ISO 27001:2005 (zarządzanie bezpieczeństwem) lub ISO 9001 (zarządzanie jakością). Tym niemniej, dopuszcza się również korzystanie z certyfikatów wydanych przez uznanych audytorów IT.

Naczelna Rada Adwokacka w Wielkiej Brytanii: „Chmura obliczeniowa: względy bezpieczeństwa, które należy wziąć pod uwagę”[9]

6.5. Opracowanie skupia się głownie na ryzyku przechwytywania i wykorzystywania przechowywanych w chmurze danych klientów w celach przestępczych przed podmioty nieuprawnione. Jak podkreśla się w dokumencie, dane, którymi dysponują adwokaci bardzo często mają wysoce poufny charakter i mogą znacznie ułatwić popełnianie przestępstw, w szczególności finansowych. Aby temu zapobiec, Kancelarie powinny zapewnić, że stosowane są odpowiednie poziomy szyfrowania danych, uwierzytelniania, a także że wykorzystywany jest adekwatny system tworzenia kopii zapasowych na wypadek nieprawidłowości w infrastrukturze informatycznej. Poza szyfrowaniem zapewnianym przez Dostawcę, każdy prawnik powinien indywidualnie rozważyć zastosowanie na swoim komputerze dodatkowej warstwy szyfrowania, np. używając systemu operacyjnego w celu stworzenia szyfrowanego folderu w przestrzeni chmurowej (Mac OS oraz Windows 10 Professional posiadają funkcje umożliwiające tworzenie szyfrowanych folderów). Wartą rozważenia opcją jest również użycie specjalnych aplikacji szyfrujących, przy czym powinny być to aplikacje zapewniające szyfrowanie typu „0 wiedzy”, tj. nie dające dostawcy aplikacji dostępu do hasła użytkownika.

Izba Adwokacka Nowego Jorku: „Chmura i małe kancelarie prawne: względy biznesowe, etyczne oraz poufności”[10]

---

[9] The General Council of the Bar, „Cloud computing – security issues to consider”. Luty 2020. Dostęp pod adresem: https://www.barcouncilethics.co.uk/wp-content/uploads/2017/10/Cloud-computing-2020.pdf. [dostęp 23/08/2020]

[10] The New York City Bar Association, „The Cloud and the Small Law Firm: Business, Ethics and Privilege Considerations”. Listopad 2013 r. Dostęp pod adresem: https://www2.nycbar.org/pdf/report/uploads/20072378-TheCloudandtheSmallLawFirm.pdf

6.6. Opracowanie opiera się na założeniu, że Kancelarie prawne – aby nadążyć za rozwijającym się technologicznie biznesem – muszą pozostać otwarte na nowe rozwiązania, w szczególności te oparte na chmurze. W opracowaniu zwrócono uwagę, że większość Kancelarii prawnych oraz indywidualnych prawników już od dłuższego czasu wykorzystuje usługi chmurowe, często nie mając świadomości skutków, które się z tym wiążą – przede wszystkim w zakresie zapewnienia bezpieczeństwa danych klientów przed nieuprawnionym dostępem, kontroli przepływu danych oraz ochrony na wypadek awarii. Z tego względu, implementacja technologii chmury obliczeniowej w konkretnej Kancelarii prawnej powinna zostać poprzedzona analizą możliwości danej Kancelarii w zakresie zarządzania danymi przechowywanymi chmurze oraz zrozumieniem specyfiki funkcjonowania tej technologii.

6.7. Kluczowe jest przeprowadzenie dogłębnego badania *due diligence* wobec potencjalnego Dostawcy oraz zapewnienie, że dany dostawca posiada odpowiednie certyfikaty bezpieczeństwa pochodzące od niezależnych audytorów. Do międzynarodowych standardów wykorzystywanych przez takich audytorów należą m.in. SSAE, SOC2, SysTrust/Webtrust. Wykorzystując certyfikowanych Dostawców, prawnik – w razie potencjalnego sporu – ma wysokie szanse skutecznego wykazania, że dochował należytej staranności przy ocenie systemu bezpieczeństwa Dostawcy. Szczególnie istotne jest również zapewnienie odpowiedniego szyfrowania (za pomocą aplikacji szyfrujących) na wszystkich używanych w pracy prawnika urządzeniach, takich jak laptopy, smartfony, tablety lub dyski USC. Jako dobrą praktykę wytyczne wskazują informowanie klientów o przechowywaniu przez Kancelarię danych w chmurze.

Wskazówki i wytyczne Szwajcarskiej Federacji Adwokatów (Fédération Suisse des Avocats - FSA) dotyczące podwykonawstwa IT i korzystania z usług chmurowych[11]

6.8. W ocenie FSA, zapewnienie odpowiedniej efektywności pracy prawników wymaga zastosowania adekwatnie dobranych i zaawansowanych narzędzi informatycznych. Chmura obliczeniowa – poprzez zapewnienie relatywnie wysokiego poziomu bezpieczeństwa oraz dynamicznego rozwoju technologicznego – stanowi jeden ze sposobów dostarczenia prawnikom takich narzędzi. W wytycznych FSA podkreśla się jednakże, że to na adwokacie spoczywa odpowiedzialność za zapewnienie, że wykorzystywana w jego pracy infrastruktura informatyczna (w tym infrastruktura oparta na chmurze obliczeniowej) spełnia wszystkie mające zastosowanie wymogi prawne, w szczególności te z zakresu tajemnicy zawodowej i ochrony danych. Z tego względu, Kancelarie powinny przykładać szczególną uwagę do kwestii: (i) wyboru Dostawcy usług informatycznych, (ii) odpowiedniego skonstruowania umowy zawartej z wybranym Dostawcą oraz (iii) zapewnienia sobie możliwości kontroli wykonywania przez tego Dostawcę obowiązków umownych. Wykonywanie obowiązków przez Dostawcę usług powinno być przedmiotem nadzoru wykonywanego przez profesjonalny podmiot (niezależnego audytora), z punktu widzenia realizacji norm ISO 9001, ISO 27001 oraz odpowiednich standardów ochrony danych.

FAQ Paryskiej Izby Adwokackiej: „Vademecum deontologii cyfrowej”[12]

---

[11] Fédération Suisse des Avocats, „Indications et recommandations de la FSA pour la sous-traitance informatique et l’utilisation de services cloud”. Czerwiec 2019 r. Dostęp pod adresem: https://www.sav-fsa.ch/fr/documents/dynamiccontent/190408-sav-guidelines-outsourcing_f-(4).pdf. [dostęp 23/08/2020]

[12] L’Ordre des avocats au barreau de Paris, „Vademecum de la deontologie du numerique: Les FAQ de l’Ordre des avocats au barreau de Paris”. Grudzień 2013 r. Dostęp pod adresem: http://www.avocatparis.org/system/files/documents/vade_deonto.pdf

6.9. Vademecum określa działania, które adwokat powinien podjąć przed rozpoczęciem wykorzystywania chmury obliczeniowej w ramach swojej aktywności zawodowej, w szczególności przed umieszczeniem danych w chmurze obliczeniowej. Zgodnie z rekomendacjami, analizę powinno rozpocząć określenie, czy dany adwokat jest upoważniony do przechowywania danych klientów poza Kancelarią. Duży nacisk położony jest na odpowiednie skonstruowanie umowy z Dostawcą Usług chmurowych, aby odpowiednio zaadresować ryzyka w obszarze m.in. z bezpieczeństwa danych, lokalizacji danych, dostępu do danych, naprawy błędów oraz podziału odpowiedzialności. Adwokat chcący skorzystać z technologii chmurowej powinien upewnić się, że Dostawca spełnia odpowiednie normy bezpieczeństwa (ISO 27001, ISO 9001). W Vademecum podkreślono również konieczność zapewnienia przez Kancelarię odpowiedniego łącza internetowego. Jako praktykę mającą na celu zapewnienie transparentności świadczenia usług prawnych, dokument wskazuje informowanie klientów o wykorzystywaniu przez adwokata Usług chmurowych.

INNE STANDARDY REFERENCYJNE

Uchwała Rady Ministrów: Inicjatywa Wspólna Infrastruktura Informatyczna Państwa (WIIP)[13]

6.10. Inicjatywa WIIP została powołana na mocy Uchwały Rady Ministrów z dnia 24 września 2019 r. Stanowi polską odpowiedź na realizowaną w innych krajach politykę *Cloud First,* rekomendującą preferencję dla Usług chmurowych przy nabywaniu elementów infrastruktury informatycznej przez administrację publiczną. Zasadniczym celem WIIP jest upowszechnienie wykorzystania technologii chmury obliczeniowej w jednostkach administracji publicznej. Inicjatywa WIIP jest skierowana, co oczywiste, do jednostek sektora publicznego.

6.11. Mimo to, na zasadzie punktu odniesienia, należy zwrócić uwagę zwłaszcza na zawarty w uchwale wymóg klasyfikacji systemów informatycznych zgodnie z kryteriami w niej określonymi. Klasyfikacja opiera się o mieszane kryteria, odnoszące się zarówno do rodzaju danych przetwarzanych w systemie, jak i cel tego przetwarzania oraz rodzaj podmiotu korzystającego z systemu. W oparciu o klasyfikację systemów i przeprowadzoną analizę ryzyka, podmiot powinien podjąć decyzję o rodzaju Usług chmury obliczeniowej, z której chce skorzystać (publiczna, hybrydowa, rządowa itd.).

Komunikat Urzędu Komisji Nadzoru Finansowego (UKNF) dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej[14]

6.12. Dokument zawiera rekomendacje i oczekiwania UKNF co do możliwości zastosowania technologii chmury obliczeniowej przez podmioty nadzorowane (tj. przede wszystkim banki, ubezpieczycieli, inne instytucje finansowe). Komunikat m.in. definiuje usługę chmury

[13] Uchwała Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa". Dostępne pod adresem: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190000862/O/M20190862.pdf

[14] Urząd Komisji Nadzoru Finansowego, „Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej". Styczeń 2020 r. Dostępne pod adresem: https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_Chmura_Obliczeniowa_68669.pdf.

obliczeniowej, przewiduje nowe obowiązki notyfikacyjne podmiotów nadzorowanych oraz zawiera kompleksowe wytyczne w zakresie oceny ryzyka przez podmioty nadzorowane.

6.13. Zgodnie z wytycznymi Komunikatu, każdy proces korzystania z usług chmury obliczeniowej powinien być poprzedzony klasyfikacją i oceną informacji pod kątem jej dopuszczalności przetwarzania w chmurze. Zasadniczy ciężar odpowiedzialności podmiotu nadzorowanego leży natomiast w dokonaniu analizy ryzyka, uwzgledniającej szereg okoliczności stanowiących potencjalne źródła zagrożeń z perspektywy prawnej, organizacyjnej i technicznej. Podmiot nadzorowany powinien także zgromadzić i monitorować dokumentację określającą sposób przetwarzania informacji w chmurze, a także opracować plany rezygnacji z korzystania z chmury obliczeniowej w sposób zapewniający mu ciągłość działania. Czynności podejmowane w oparciu o Komunikat powinny być dokumentowane w celu zapewnienia rozliczalności.