Komisja
LegalTech
Okręgowej Izby
Radców Prawnych
w Warszawie

MARUTA \

STANDARD PRZETWARZANIA INFORMACJI W CHMURZE OBLICZENIOWEJ PRZEZ RADCÓW PRAWNYCH

PROCEDURA SZACOWANIA RYZYKA PRZETWARZANIA INFORMACJI W CHMURZE OBLICZENIOWEJ – WZÓR

METRYKA DOKUMENTU	
AUTOR	© Kancelaria Maruta Wachta
WERSJA DOKUMENTU	1.0
DATA DOKUMENTU	14 grudnia 2020 r.
LICZBA STRON	13
SPIS TREŚCI	

OBJAŚNIENIA

Procedura stanowi wzór odwołujący się do Standardu przetwarzania danych w chmurze i zasad tam określonych. Radca prawny lub Kancelaria, wdrażając procedurę, samodzielnie ocenia przydatność poniższego wzoru i konieczność wprowadzenia ewentualnych modyfikacji.

Poniższy wzór opracowany jest przy założeniu jego wykorzystania w **Kancelarii** prowadzonej w formie spółki prawa handlowego. Stosowanie Procedury przez Radców prawnych wykonujących działalność zawodową w innej formie organizacyjnej wymaga ewentualnego dostosowania.

1. DEFINICJE

1.1. **Kancelaria** – […].

1.2. **Koordynator usług chmurowych** albo **Koordynator** – wyznaczona w Kancelarii osoba odpowiedzialna za obszar bezpieczeństwa przetwarzania informacji w chmurze obliczeniowej.

Koordynatorem powinna zostać osoba posiadająca wiedzę w obszarze bezpieczeństwa informacji i zarządzania ryzykiem, upoważniona do dostępu do informacji podlegających klasyfikacji i ocenie. W szczególności taką osobą może być Radca prawny pełniący w Kancelarii funkcję Inspektora Ochrony Danych.

1.3. **Procedura** – niniejsza Procedura szacowania Ryzyka przetwarzania informacji w chmurze obliczeniowej.

1.4. **Proces –** zespół następujących po sobie czynności realizowanych w celu osiągnięcia określonego celu biznesowego, z reguły przy udziale kilku jednostek organizacyjnych Kancelarii. Proces definiowany jest pomocniczo przez określenie jego danych wejściowych i wyjściowych, stanowiących z reguły dane wejściowe dla innego Procesu.

1.5. **Usługa chmury obliczeniowej, Usługa chmurowa** – usługa chmury obliczeniowej w rozumieniu Standardu.

1.6. **Radca prawny** – radca prawny w rozumieniu Standardu, świadczący pomoc prawną w ramach Kancelarii, który wytworzył informację lub który zamówił informację poza Kancelarią w celu jej przetwarzania przez Kancelarię.

1.7. **Ryzyko** – niepewność związana z procesem korzystania z Usługi chmury obliczeniowej oraz obiektywnym brakiem możliwości kontrolowania i wpływania na aspekty prawne, technologiczne i organizacyjne świadczonej Usługi chmury obliczeniowej oraz sposobu jej wykorzystania.

1.8. **Standard** – standard przetwarzania informacji w chmurze obliczeniowej przez Radców prawnych dostępny na stronie […], określający minimalne rekomendowane warunki korzystania z chmury obliczeniowej.

1.9. **Ważność informacji** – właściwość informacji odnosząca się do wpływu naruszenia bezpieczeństwa informacji na bezpieczeństwo tajemnicy radcowskiej lub obrończej, ciągłość świadczenia pomocy prawnej, finanse i reputację Radcy prawnego oraz statusu informacji jako objętej tajemnicą radcowską lub obrończą.

1.10. **Zagrożenie** – potencjalna przyczyna niepożądanego zdarzenia, którego skutkiem może być szkoda w zakresie bezpieczeństwa tajemnicy zawodowej (tj. jej poufności, integralności i dostępności), ciągłości świadczenia pomocy prawnej, finansów lub reputacji Radcy prawnego.

Pojęcie niezdefiniowane w Procedurze, a pisane wielką literą, mają znaczenie nadane im w Standardzie.

2. ZASADY OGÓLNE

2.1. Procedura znajduje zastosowanie do Procesów, w ramach których informacje przetwarzane są, w jakimkolwiek zakresie, przy użyciu publicznej lub hybrydowej chmury obliczeniowej, lub w odniesieniu do których planowane jest użycie publicznej lub hybrydowej chmury obliczeniowej. W przypadku, w którym Dostawca chmury obliczeniowej korzysta z usług wykorzystujących Usługi chmury obliczeniowej, w Procedurze uwzględnia się także tę drugą usługę. W przypadku, gdy Kancelaria korzysta z usług podmiotów niebędących Dostawcami chmury obliczeniowej, którzy korzystają z Usług chmury obliczeniowej, Procedurę stosuje się odpowiednio.

2.2. Procedura określa zasady szacowania ryzyka związanego z wykorzystaniem Usług chmury obliczeniowej przez Kancelarię oraz zasady określania i realizacji planu postępowania z oszacowanym ryzykiem.

2.3. Uruchomienie Procedury wymaga uprzedniego przeprowadzenia inwentaryzacji Procesu (lub jego części) realizowanego za pomocą Usług chmury obliczeniowej oraz wykonania klasyfikacji i oceny informacji przetwarzanych w Procesie zgodnie z procedurą klasyfikacji i oceny informacji przyjętą w Kancelarii.

3. ROLE I ODPOWIEDZIALNOŚĆ

Podział ról i odpowiedzialności został wskazany przykładowo. W każdym przypadku podział zadań powinien zostać odpowiednio dostosowany do uwarunkowań konkretnego przypadku. W szczególności:

- *Zadania przypisane wspólnikom mogą być przypisane, w zależności od charakteru organizacji, partnerom zarządzającym (w przypadku spółki prawniczej) lub szefom działów prawnych (w przypadku przedsiębiorstwa);*
- *Zadania przypisane Koordynatorowi mogą być przypisane, w zależności od charakteru organizacji, pracownikowi merytorycznemu (np. Radcy prawnemu lub innemu prawnikowi), z zachowaniem wymogów prawnych, w szczególności w zakresie udzielenia dostępu do tajemnicy zawodowej i tajemnicy przedsiębiorstwa.*

3.1. Wspólnicy odpowiadają za:

3.1.1. określanie ogólnej strategii postępowania z Ryzykiem w Kancelarii;

3.1.2. zapewnienie zasobów i narzędzi niezbędnych do zarządzania Ryzykiem w Kancelarii;

3.1.3. zatwierdzanie wyników szacowania Ryzyka i planu postępowania z Ryzykiem w przypadkach określonych w Procedurze.

3.2. Koordynator odpowiada za:

3.2.1. prowadzenie analizy Ryzyka w odniesieniu do przetwarzania informacji w Procesie z wykorzystaniem Usług chmury obliczeniowej;

3.2.2. sporządzenie i realizację planu postępowania z Ryzykiem w przypadkach wskazanych w Procedurze;

3.2.3. wdrożenie mechanizmów kontrolnych zarządzania Ryzykiem i monitorowanie ich skuteczności.

3.3. Radca prawny odpowiada za:

3.3.1. przekazanie Koordynatorowi Usług chmurowych wszelkich informacji nt. Procesu, którego dotyczy ocena;

3.3.2. wsparcie Koordynatora w zakresie szacowania Ryzyka.

4. SZACOWANIE RYZYKA

4.1. Szacowanie ryzyka w Spółce obejmuje:

4.1.1. identyfikację Zagrożeń;

4.1.2. ocenę skutków wystąpienia zagrożenia (ocena wpływu);

4.1.3. ocenę prawdopodobieństwa wystąpienia zagrożeń; oraz

4.1.4. szacowanie ryzyka.

4.2. Szacowania ryzyka zgodnie z Procedurą dokonuje się, gdy:

4.2.1. Kancelaria zamierza przetwarzać w Usługach chmury obliczeniowej nowy rodzaj informacji;

4.2.2. Kancelaria zamierza wykorzystywać nową Usługę chmury obliczeniowej;

4.2.3. przetwarzanie informacji w Usługach chmury obliczeniowej jest realizowane przez Kancelarię w ramach istniejącego Procesu, ale szacowanie Ryzyka dla danego Procesu nie było dotychczas przeprowadzone.

4.3. W procesie szacowania Ryzyka, w zależności od potrzeb:

4.3.1. korzysta się ze zweryfikowanych, aktualizowanych źródeł informacji o zagrożeniach;

4.3.2. korzysta się z pomocy osób o specjalistycznych kompetencjach w obszarze cyberbezpieczeństwa i Usług chmury obliczeniowej;

4.3.3. uwzględnia się dostępne wyniki audytów Usługi chmury obliczeniowej oraz procesu zarządzania bezpieczeństwem informacji oraz dostępne certyfikaty Dostawcy w tym zakresie.

4.4. Wyniki szacowania Ryzyka powinny być regularnie przeglądane, nie rzadziej jednak niż raz w roku. Szacowanie Ryzyka powinno być aktualne i wykonywane ponownie każdorazowo, gdy:

4.4.1. dla istniejącej Usługi chmury obliczeniowej zmieniają się parametry technologiczne lub warunki korzystania;

4.4.2. monitorowanie źródeł informacji wskazuje na możliwość wystąpienia nowego Zagrożenia;

4.4.3. dla monitorowanego Zagrożenia zmienia się ocena wpływu lub ocena prawdopodobieństwa wystąpienia;

4.4.4. zaistnieje zmiana prawa / zmiana regulacji wewnętrznych lub umów, których stroną jest Kancelaria, która wpływa lub może wpływać na zgodność postępowania Radcy prawnego w kontekście przetwarzania informacji w Usługach chmury obliczeniowej;

4.4.5. istotnie zmienia się skala przetwarzania informacji w ramach Procesu;

4.4.6. istotnie zmienia się Ważność informacji przetwarzanych w ramach Procesu;

4.4.7. zaistnieje zmiana innych istotnych okoliczności, wpływających na bezpieczeństwo przetwarzania informacji w Usługach chmury obliczeniowej.

4.5. Odpowiedzialność za poprawność merytoryczną szacowania Ryzyka ponosi Koordynator.

4.6. Szacowania Ryzyka dokonuje się przy wykorzystaniu Formularza B: **Szacowanie ryzyka** we właściwym wariancie (wariant podstawowy i wariant pogłębiony).

4.7. Formularz B: **Szacowanie ryzyka** i szczegółowa Instrukcja szacowania Ryzyka stanowią załączniki do Procedury.

5. STRATEGIA POSTĘPOWANIA Z RYZYKIEM

5.1. W oparciu o dokonane szacowanie ryzyka Koordynator określa strategię postępowania z Ryzykiem:

5.1.1. **redukcja** – podjęcie działań prowadzących do zmniejszenia lub wyeliminowania oszacowanego poziomu Ryzyka; w tym w szczególności zmiana zakresu lub zwiększenie intensywności stosowania środków bezpieczeństwa;

5.1.2. **unikanie** – zaprzestanie realizacji procesu (lub jego części), którego dotyczy Ryzyko, lub zmniejszenie skali jego realizacji, lub zmiana sposobu realizacji;

5.1.3. **przeniesienie** (**dzielenie się**) – całkowita lub częściowa alokacja Ryzyka po stronie podmiotu trzeciego, w szczególności poprzez ubezpieczenie lub zmianę odpowiedzialności;

5.1.4. **akceptacja** – kontynuowanie realizacji analizowanego procesu w niezmienionej formie, bez podejmowania środków zaradczych.

5.2. Ryzyko wysokie nie może być zaakceptowane, jeżeli:

5.2.1. dotyczy ono naruszenia bezpieczeństwa informacji stanowiącej treść pomocy prawnej;

5.2.2. w pozostałych przypadkach, jeśli takiej strategii nie zaakceptował Wspólnik Kancelarii.

5.3. W odniesieniu do każdego zidentyfikowanego Ryzyka, należy wyznaczyć osobę odpowiedzialną za jego monitorowanie oraz podejmowanie wskazanych środków mitygujących Ryzyko.

5.4. Nie rzadziej niż raz do roku Koordynator dokonuje weryfikacji i w razie potrzeb aktualizacji strategii postępowania z Ryzykiem.

6. DOKUMENTOWANIE CZYNNOŚCI

6.1. Wszystkie czynności dokonywane w oparciu o Procedurę są dokumentowane w postaci pisemnej lub elektronicznej, w sposób zapewniający identyfikację osoby dokonującej czynności oraz integralność sporządzonej informacji.

7. ZAŁĄCZNIKI

7.1. Następujące załączniki stanowią integralną część Procedury:

7.1.1. Załącznik 1 – **Instrukcja szacowania ryzyka**;

7.1.2. Formularz B – **Szacowanie ryzyka**.

8. POSTANOWIENIA KOŃCOWE

8.1. Wyniki szacowania Ryzyka oraz przyjęta strategia postępowania z Ryzykiem są uwzględniane w znajdującej zastosowanie dokumentacji Kancelarii.

8.2. Procedura wchodzi w życie dnia [●] roku.

Załącznik 1 – **Instrukcja szacowania Ryzyka**

1. ZASADY OGÓLNE

1.1. Ryzyko szacuje się przy użyciu arkusza Formularza B: **Szacowanie Ryzyka**, stanowiącego załącznik do Procedury.

1.2. Ryzyko szacuje się w przypadkach wskazanych w Procedurze.

1.3. Szacowanie Ryzyka w Spółce obejmuje:

1.3.1. identyfikację Zagrożeń;

1.3.2. ocenę skutków wystąpienia Zagrożenia (ocena wpływu);

1.3.3. ocenę prawdopodobieństwa wystąpienia Zagrożeń; oraz

1.3.4. szacowanie Ryzyka.

1.4. Ryzyko podlega szacowaniu w wariancie podstawowym lub pogłębionym, zgodnie z poniższą macierzą:

Klasa / Ważność	MAŁA	ŚREDNIA	DUŻA
A	Wariant podstawowy	Wariant podstawowy	Wariant podstawowy
B	Wariant podstawowy	Wariant podstawowy	Wariant podstawowy
C	Wariant podstawowy	Wariant pogłębiony	Wariant pogłębiony
D	Wariant podstawowy	Wariant pogłębiony	Wariant pogłębiony
E	Wariant pogłębiony	Wariant pogłębiony	Wariant pogłębiony

1.5. W każdym przypadku, w którym zgodnie z Procedurą, wystarczające jest szacowanie Ryzyka w wariancie podstawowym, Koordynator może, a na żądanie Wspólnika powinien przeprowadzić szacowanie Ryzyka w wariancie pogłębionym.

1.6. Narzędzia służące do szacowania Ryzyka w poszczególnych wariantach określone są w kolejnych zakładkach Formularza B: **Szacowanie ryzyka**.

2. OPIS PROCESU

2.1. Przed przystąpieniem do szacowania Ryzyka Koordynator sporządza opis Procesu poddawanego szacowaniu Ryzyka przez uzupełnienie zakładki „Opis Procesu" Formularza B.

2.2. Opis Procesu powinien zawierać w szczególności:

2.2.1. przebieg operacyjny procesu;

2.2.2. opisanie architektury wykorzystywanego rozwiązania;

2.2.3. wskazanie dokumentacji uwzględnianej w procesie szacowania Ryzyka (np. umowa z Dostawcą Usługi chmurowej, regulaminy, procedury wewnętrzne itd.).

Wskazanie elementów, o których mowa powyżej, może polegać na zawarciu w arkuszu hiperłącza do właściwej dokumentacji.

Koordynator odpowiada za uzyskanie informacji technicznych (w szczególności architektury rozwiązania) od Dostawcy usługi lub innej właściwej osoby.

3. SZACOWANIE RYZYKA – WARIANT PODSTAWOWY

3.1. Szacowanie Ryzyka w wariancie podstawowym odbywa się poprzez wypełnienie zakładki „Szacowanie ryzyka_podstawowe" Formularza B.

4. SZACOWANIE RYZYKA – WARIANT POGŁĘBIONY

4.1. Szacowanie Ryzyka w wariancie pogłębionym odbywa się poprzez wypełnienie zakładki „Szacowanie ryzyka_pogłębione" Formularza B.

IDENTYFIKACJA ZAGROŻEŃ

4.2. Koordynator identyfikuje Zagrożenia w kontekście przeprowadzonej klasyfikacji i oceny informacji przetwarzanych w Procesie z wykorzystaniem określonych Usług chmury obliczeniowej.

4.3. Lista podstawowych potencjalnych Zagrożeń dotyczących przetwarzania danych przy użyciu Usług chmury obliczeniowej określona została w Formularzu B: **Szacowanie ryzyka**. Nie wyklucza to jednak możliwości ujęcia w procesie szacowania Ryzyka dodatkowych Zagrożeń w razie ich identyfikacji ani nie zwalnia z obowiązku weryfikacji, czy takie inne Zagrożenia występują w danym Procesie.

4.4. Koordynator zapewnia sporządzenie opisu zidentyfikowane Zagrożenia oraz przypisania każdemu zidentyfikowanemu Zagrożeniu podstawy zagrożenia (wskazanie jego źródła) przez właściwe osoby. Zagrożenie może mieć charakter prawny, organizacyjny lub techniczny, a także zostać zaliczone do więcej niż jednej z tych kategorii.

OCENA WPŁYWU ZAGROŻENIA

4.5. Dla każdego zidentyfikowanego Zagrożenia należy wskazać wpływ materializacji tego Zagrożenia na:

4.5.1. bezpieczeństwo informacji stanowiących tajemnicę zawodową;

4.5.2. ciągłość świadczenia pomocy prawnej;

4.5.3. stan finansowy Radcy prawnego (Kancelarii)

4.5.4. reputację Radcy prawnego (Kancelarii).

4.6. Opisowi skutku materializacji zagrożenia należy przypisać wartość wpływu Zagrożenia, od 1 do 3, gdzie:

1 – oznacza brak wpływu lub nieistotny wpływ na wskazane wyżej aspekty związane z działalnością Spółki;

2 – oznacza średni wpływ na co najmniej jeden ze wskazanych wyżej aspektów związanych z działalności Spółki;

3 – oznacza istotny wpływ na co najmniej jeden ze wskazanych wyżej aspektów związanych z działalności Spółki.

4.7. Wartość wpływu Zagrożenia stanowi najwyższa ze wskazanych wartości.

OCENA PRAWDOPODOBIEŃSTWA WYSTĄPIENIA ZAGROŻENIA

4.8. Dla każdego Zagrożenia należy ocenić prawdopodobieństwo jego wystąpienia w kontekście konkretnego Procesu i konkretnej Usługi chmury obliczeniowej (rozważanej lub już wykorzystywanej), przy czym należy wziąć pod uwagę zarówno warunki normalne świadczenia Usługi chmury obliczeniowej, jak i warunki niestandardowe (np. możliwa awaria wymagająca zmiany metod uwierzytelniania).

4.9. Ocena prawdopodobieństwa wystąpienia Zagrożenia powinna opierać się na udokumentowanych źródłach informacji lub wiedzy eksperckiej. Źródłami informacji są w szczególności:

4.9.1. portale branżowe i tematyczne;

4.9.2. opisy reakcji Dostawcy Usług chmury obliczeniowej na incydenty bezpieczeństwa;

4.9.3. udokumentowane przypadki użycia;

4.9.4. opinie prawne i techniczne;

4.9.5. wyniki audytów i przeglądów;

4.9.6. dokumentacja techniczna i projektowa;

4.9.7. niezależne oceny i opinie;

4.9.8. wyniki testów.

4.10. Ocena prawdopodobieństwa wystąpienia danego Zagrożenia powinna uwzględniać w szczególności następujące czynniki:

4.10.1. statystyki dotyczące podobnych zdarzeń w przeszłości (dane historyczne);

4.10.2. atrakcyjność aktywów informacyjnych podlegających zabezpieczeniom, przy uwzględnieniu przypisanej im klasy, kontekstu ich przetwarzania i potencjalnych możliwości ich wykorzystania;

4.10.3. czynniki środowiskowe.

4.11. Ocena prawdopodobieństwa uwzględnia aktualnie stosowane przez Radcę prawnego zabezpieczenia.

4.12. Ocena prawdopodobieństwa wystąpienia danego Zagrożenia odbywa się poprzez przypisanie szacowanemu prawdopodobieństwu wartości liczbowej od 1 do 3, gdzie:

1 – oznacza niskie prawdopodobieństwo wystąpienia Zagrożenia;

2 – oznacza średnie prawdopodobieństwo wystąpienia Zagrożenia;

3 – oznacza wysokie prawdopodobieństwo wystąpienia Zagrożenia.

OCENA RYZYKA

4.13. Dla zidentyfikowanych Zagrożeń należy wyliczyć wartość Ryzyka, która jest iloczynem wartości wpływu Zagrożenia oraz wartości prawdopodobieństwa wystąpienia Zagrożenia:

wartość Ryzyka = wartość wpływu Zagrożenia x wartość prawdopodobieństwa

4.14. Właściciel biznesowy definiuje (opisuje) środki zaradcze co najmniej dla Ryzyk zaklasyfikowanych jako ŚREDNIE lub WYSOKIE, uwzględniając ekonomiczne aspekty wdrożenia środków zaradczych poprzez porównanie do Ważności informacji przetwarzanych w Procesie.

4.15. Zdefiniowane środki zaradcze zostają przypisane do realizacji poprzez odniesienie do uprawnień i odpowiedzialności stanowisk / osób w Spółce, a ich realizacja podlega monitorowaniu i okresowemu sprawdzaniu. Jakiekolwiek zmiany w realizacji uzgodnionych środków zaradczych wymagają przeprowadzenia powtórnej oceny Ryzyka w odniesieniu do korespondujących Zagrożeń.

4.16. Środki zaradcze mogą w szczególności:

4.16.1. uniemożliwiać wystąpienie danego Zagrożenia lub zmniejszać prawdopodobieństwo jego wystąpienia;

4.16.2. umożliwić Spółce uniknięcie wpływu wystąpienia danego Zagrożenia lub zmniejszać ten wpływ.

4.17. Zastosowanie środków zaradczych powoduje konieczność dokonania ponownej oceny wpływu i prawdopodobieństwa wystąpienia danego Zagrożenia oraz ustalenia poziomu Ryzyka szczątkowego. W przypadku, braku stosowania środków zaradczych, wartość Ryzyka szczątkowego jest równa wartości Ryzyka ustalonego zgodnie z pkt 4.13.

4.18. Ryzyko wyliczone zgodnie z niniejszą Procedurą określa się jako:

4.18.1. niskie – dla wartości Ryzyka mniejszej niż 3;

4.18.2. średnie – dla wartości Ryzyka równej lub większej niż 3 i mniejszej niż 6;

4.18.3. wysokie – dla wartości Ryzyka równej lub większej niż 6.

ZARZĄDZANIE RYZYKIEM

4.19. Koordynator wskazuje osobę odpowiedzialną za zarządzanie poszczególnymi ryzykami i realizację środków zaradczych oraz wskazuje termin raportowania koordynatorowi

4.20. W oparciu o informacje i działania wyznaczonych osób, Koordynator podejmuje może podjąć decyzję o konieczności ponownej oceny ryzyka.