Komisja
**LegalTech**
Okręgowej Izby
Radców Prawnych
w Warszawie

MARUTA \

# STANDARD PRZETWARZANIA INFORMACJI W CHMURZE OBLICZENIOWEJ PRZEZ RADCÓW PRAWNYCH

## PROCEDURA KLASYFIKACJI I OCENY INFORMACJI

**na cele przetwarzania w chmurze obliczeniowej**

**– WZÓR**

| METRYKA DOKUMENTU | |
|---|---|
| **AUTOR** | © Kancelaria Maruta Wachta |
| **WERSJA DOKUMENTU** | 1.0 |
| **DATA DOKUMENTU** | 14 grudnia 2020 r. |
| **LICZBA STRON** | 12 |
| **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** – każda organizacyjnoprawna forma wykonywania zawodu radcy prawnego przewidziana w ustawie o radcach prawnych.

**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 klasyfikacji i oceny informacji.

**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** – usługi przetwarzania w chmurze w rozumieniu Standardu.

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

**1.7.** **Standard** – standard przetwarzania danych w chmurze obliczeniowej przez Radców prawnych dostępny na stronie […] określający minimalne rekomendowane zasady korzystania z chmury obliczeniowej.

**1.8.** **Ważność informacji** – właściwość informacji, której wartość określa Radca prawny, uwzględniająca:

**1.8.1.** status informacji jako objętej tajemnicą zawodową (radcowską lub obrończą) oraz

1.8.2. potencjalny wpływ naruszenia bezpieczeństwa informacji na bezpieczeństwo tajemnicy radcowskiej lub obrończej, ciągłość świadczenia pomocy prawnej, finanse i reputację Radcy prawnego.

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

## 2. ZASADY OGÓLNE

**2.1.** Procedura określa:

**2.1.1.** przyjętą w Kancelarii klasyfikację informacji w odniesieniu do Procesów, o których mowa w pkt 2.2;

**2.1.2.** zasady dokonywania klasyfikacji i oceny informacji przetwarzanych w środowisku chmury obliczeniowej.

**2.2.** 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, zarówno bezpośrednio, jak i za pośrednictwem Dostawcy korzystającego z Usług chmury obliczeniowej. W przypadku, w którym Dostawca chmury obliczeniowej korzysta z usług, wykorzystujących Usługi chmury obliczeniowej, w Procedurze uwzględnia się także tę drugą usługę.

**2.3.** Zasady klasyfikacji i oceny informacji określone w Procedurze są zgodne ze Standardem przetwarzania informacji w chmurze obliczeniowej.

## 3. ROLE I ODPOWIEDZIALNOŚĆ

*Podział ról i odpowiedzialności zostały wskazane przykładowo. W każdym przypadku podział zadań powinien zostać odpowiednio dostosowany do uwarunkowań konkretnego przypadku. W szczególności: 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 ogólny nadzór nad przestrzeganiem Procedury.

**3.2.** Radca prawny odpowiada za:

**3.2.1.** zlecenie Koordynatorowi przeprowadzenie klasyfikacji i oceny informacji w odniesieniu do Procesów, za które odpowiada;

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

**3.2.3.** dokonanie oceny skutków naruszenia bezpieczeństwa, w procesie klasyfikacji i oceny informacji;

**3.2.4.** spełnienie warunków dopuszczalności korzystania z chmury obliczeniowej, w razie stwierdzenia ich występowania w procesie klasyfikacji i oceny informacji;

**3.2.5.** informowanie Koordynatora o wszelkich okolicznościach mogących skutkować koniecznością dokonania ponownej klasyfikacji i oceny, zgodnie z pkt 4.2

**3.3.** Koordynator Usług chmurowych odpowiada za:

**3.3.1.** inwentaryzację informacji;

**3.3.2.** klasyfikację informacji;

**3.3.3.** ocenę informacji;

**3.3.4.** archiwizację dokumentów wytworzonych w związku z realizacją Procedury.

**3.4.** Każdy członek personelu Kancelarii zobowiązany jest do wsparcia Koordynator w wykonywaniu jego zadań poprzez niezwłoczne przekazywanie informacji, wyjaśnień lub dokumentów, w zakresie przez niego żądanym.

## 4. INWENTARYZACJA INFORMACJI

**4.1.** Inwentaryzacja informacji obejmuje sporządzenie precyzyjnego opisu Procesów, w ramach których wykorzystywane są lub w odniesieniu do których zakłada się korzystanie z Usługi chmury obliczeniowej. Inwentaryzację przeprowadza Koordynator na zlecenie Radcy Prawnego odpowiedzialnego za dany Proces.

**4.2.** Inwentaryzację, a następnie klasyfikację i ocenę informacji przeprowadza się:

**4.2.1.** okresowo raz do roku;

**4.2.2.** w przypadku, gdy Kancelaria zamierza przetwarzać nowy rodzaj informacji;

**4.2.3.** w przypadku, gdy Kancelaria zamierza wykorzystywać nową Usługę chmury obliczeniowej;

**4.2.4.** w przypadku, gdy zaistnieje zmiana prawa / zmiana regulacji wewnętrznych lub umów, których stroną jest Kancelaria, która wpływa lub może wpływać na zgodność postępowania Kancelarii w kontekście przetwarzania informacji w chmurze obliczeniowej;

**4.2.5.** w przypadku, gdy istotnie zwiększa lub zmniejsza się skala przetwarzania informacji w ramach Procesu;

**4.2.6.** w przypadku, gdy zmienia się ważność przetwarzanych informacji w ramach Procesu;

**4.2.7.** w przypadku zmiany innych istotnych okoliczności, wpływających na bezpieczeństwo przetwarzania informacji w chmurze obliczeniowej.

**4.3.** Inwentaryzację przeprowadza się w oparciu o Formularz A: **Klasyfikacja i ocena informacji**, stanowiący załącznik do Procedury.

## 5. KLASYFIKACJA I OCENA INFORMACJI

**5.1.** Klasyfikację i ocenę informacji przeprowadza Koordynator na zlecenie Radcy prawnego, bezpośrednio po dokonaniu inwentaryzacji informacji.

**[KLASYFIKACJA INFORMACJI]**

**5.2.** W oparciu o wyniki inwentaryzacji, Koordynator zalicza zidentyfikowane rodzaje informacji do właściwych klas, oddających wagę informacji dla Kancelarii, przy pomocy Formularza A: **Klasyfikacja i ocena informacji** i zgodnie z instrukcją zawartą w Załączniku 1: **Instrukcja inwentaryzacji informacji oraz klasyfikacji i oceny informacji**.

**5.3.** Na potrzeby przetwarzania danych przy użyciu chmury obliczeniowej, w Kancelarii wyróżnione zostały następujące klasy informacji:

*Zaproponowana klasyfikacja odnosi się do informacji przetwarzanych przy użyciu chmury obliczeniowej. Rekomendujemy jednak jej stosowanie w odniesieniu do wszystkich zasobów informacyjnych wykorzystywanych w Kancelarii.*

**5.3.1.** Klasa A – informacje publiczne

Klasa obejmuje informacje, które mogą być ujawniane osobom trzecim (na zewnątrz Kancelarii) bez żadnych ograniczeń, a ich utrata nie ma negatywnych skutków dla Kancelarii.

**5.3.2.** Klasa B – informacje wewnętrzne

Klasa obejmuje informacje, które mogą być ujawniane personelowi Kancelarii oraz w miarę potrzeby także podwykonawcom / Dostawcom.

**5.3.3.** Klasa C – informacje ważne

Klasa obejmuje informacje, niepodlegające zaliczeniu do klasy D lub E, które z uwagi na swą wagę lub powiązane z nimi wymaganie prawne powinny być ujawniane jedynie uprawnionym osobom lub podmiotom (wewnątrz Kancelarii lub osobom trzecim), z zachowaniem szczególnych warunków.

**5.3.4.** Klasa D – informacje szczególnie chronione

Klasa obejmuje informacje objęte tajemnicą radcowską, stanowiące treść pomocy prawnej, o ile nie podlegają one zaklasyfikowaniu do klasy E.

**5.3.5.** Klasa E – informacje zastrzeżone

Klasa obejmuje informacje, które z uwagi na swą wagę lub powiązane z nimi wymaganie prawne z zasady nie powinny być ujawniane osobom lub podmiotom

innym, niż te, które wytworzyły informacje, najwyższemu kierownictwu i podmiotom przez nie wskazanym.

**5.4.** Szczegółowy opis poszczególnych klas, wraz z przykładami, zawarty jest w Formularzu A: **Klasyfikacja i ocena informacji**.

**5.5.** W przypadku, gdy dana informacja mogłaby zostać zaliczona do więcej niż jednej klasy, należy zaliczyć ją do najwyższej z nich.

**[ocena informacji]**

**5.6.** Celem oceny informacji jest ustalenie dopuszczalności przetwarzania informacji w chmurze obliczeniowej i ewentualnych warunków dopuszczalności takiego działania. Ocenę informacji przeprowadza się w oparciu o wyniki inwentaryzacji i klasyfikacji informacji, przy wykorzystaniu Formularza A: **Klasyfikacja i ocena informacji**.

**5.7.** Ocenę informacji przeprowadza Koordynator lub wskazana przez niego osoba z zespołu Koordynatora, z zastrzeżeniem elementów, wyraźnie przypisanych w Procedurze Radcy Prawnemu.

**5.8.** Szczegółowe zasady przeprowadzania oceny informacji zawiera Załącznik 1 do Procedury: **Instrukcja inwentaryzacji informacji oraz klasyfikacji i oceny informacji**.

**5.9.** Odpowiedzialność za poprawność merytoryczną klasyfikacji i oceny ponosi Koordynator, z zastrzeżeniem elementów, wyraźnie przypisanych w Procedurze Radcy prawnemu.

**5.10.** Koordynator informuje Radcę prawnego o wynikach przeprowadzonej klasyfikacji i oceny informacji oraz o warunkach dopuszczalności skorzystania z chmury obliczeniowej.

## 6. PRZEGLĄD KLASYFIKACJI I OCENY INFORMACJI

**6.1.** Nie rzadziej niż raz do roku, Koordynator dokonuje przeglądu Procedury i przyjętej metodologii klasyfikacji i oceny informacji oraz szacowania ryzyka i stosownie do okoliczności może zarekomendować wprowadzenie zmian w Procedurze.

**6.2.** Nie rzadziej niż raz do roku Koordynator dokonuje przeglądu i aktualizacji dokonanej inwentaryzacji oraz klasyfikacji i oceny informacji przetwarzanych w ramach Procesów, za które odpowiada.

## 7. DOKUMENTOWANIE CZYNNOŚCI

**7.1.** 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.

*Sposób dokumentowania czynności do ustalenia stosownie do uwarunkowań; jednym z rekomendowanych rozwiązań jest stosowanie kwalifikowanych podpisów elektronicznych w celu zapewnienia integralności tworzonych dokumentów.*

## 8. ZAŁĄCZNIKI

**8.1.** Następujące załączniki stanowią integralną część Procedury:

**8.1.1.** Załącznik 1 – **Instrukcja inwentaryzacji informacji oraz klasyfikacji i oceny informacji**;

**8.1.2.** Formularz A – **Klasyfikacja i ocena informacji**.

## 9. POSTANOWIENIA KOŃCOWE

**9.1.** Procedura wchodzi w życie [●] r.

# ZAŁĄCZNIK 1 – INSTRUKCJA INWENTARYZACJI INFORMACJI ORAZ KLASYFIKACJI I OCENY INFORMACJI

## 1. INWENTARYZACJA INFORMACJI – OPIS PROCESU

1.1. Koordynator uzupełnia Formularz A: **Klasyfikacja i ocena informacji** do Procedury odrębnie w odniesieniu do każdego Procesu, w ramach którego informacje przetwarzane są lub mają być przetwarzane z wykorzystaniem chmury obliczeniowej.

1.2. Dla każdego Procesu należy wyczerpująco opisać rodzaj informacji przetwarzanych w jego ramach. W przypadku, gdy w ramach danego Procesu przetwarzany jest więcej niż jeden rodzaj informacji, każdy rodzaj informacji dla danego Procesu powinien zostać wskazany w odrębnych (kolejnych) wierszach.

1.3. Poszczególne pola Formularza A: **Klasyfikacja i ocena informacji** należy wypełniać zgodnie z poniższymi objaśnieniami:

### 1.3.1. Krótki opis Procesu

Należy zwięźle opisać przebieg Procesu (ze wskazaniem zaangażowanych w jego realizację jednostek organizacyjnych) oraz jego cel biznesowy. W miarę możliwości, należy wskazać dane wejściowe i wyjściowe Procesu.

### 1.3.2. Rodzaj informacji

W kolejnych wierszach należy wskazać wszystkie rodzaje informacji, które są przetwarzane (wykorzystywane) w Procesie. Rodzaje informacji zawarte są w liście rozwijanej, a ich definicje znajdują się w zakładce „Klasy informacji" w tym samym arkuszu xls.

W przypadku, gdy określonych informacji nie da się zakwalifikować do żadnego ze zdefiniowanych rodzajów, należy wybrać pole „inne" i opisać te informacje w kolumnie C.

### 1.3.3. Kategorie informacji

Należy możliwie szczegółowo opisać, jakie (konkretnie) informacje przetwarzane są w ramach Procesu. Opis może mieć charakter zbiorczy, odnoszący się do wszystkich wskazanych kategorii lub też odnosić się odrębnie do każdego rodzaju informacji.

W przypadkach, w których wskazanie konkretnych („pojedynczych") informacji byłoby niemożliwe, utrudnione, lub niecelowe (w szczególności na znaczny wolumen takich informacji), określenie rodzaju informacji może odbyć się przez referencję do innego dokumentu lub przez wskazanie lokalizacji lub programu, w którym wskazano te informacje.

Przykład:

„**informacje o klientach – osoby fizyczne nieprowadzące działalności gospodarczej":** imię i nazwisko, nr PESEL, nr identyfikacyjny projektu,

albo

„**informacje o klientach – B2B**”: dane kontaktowe, dane adresowe, informacje dotyczące projektu wskazane w zakładce „klient” w systemie XYZ.

#### 1.3.4. Skala przetwarzania

Należy wskazać wolumen danych, w miarę możliwości odnosząc się liczby rekordów lub innych obiektywnych kryteriów i wybrać odpowiedź z listy rozwijanej (mała / średnia / duża).

W kolumnie E należy zawrzeć uzasadnienie wskazanej skali przetwarzania.

## 2. KLASYFIKACJA INFORMACJI

2.1. W kolumnie F należy wskazać, do jakiej klasy informacji zalicza się wskazany rodzaj informacji. Definicje klas informacji zawarte są w zakładce „Klasy informacji” Formularza A: **Klasyfikacja i ocena informacji**.

## 3. OGRANICZENIA KONTRAKTOWE I ORGANIZACYJNE

3.1. **Ograniczenia kontraktowe i organizacyjne**

W kolumnach G i H należy odnieść się do mających zastosowanie w Procesie umów, regulaminów, regulacji wewnętrznych lub innych ograniczeń, które wyłączają lub ograniczają możliwość korzystania z chmury obliczeniowej w ramach Procesu.

Dokumentacja, odnosząca się do wskazanych ograniczeń (np. właściwe postanowienia umów) powinna zostać wskazana lub załączona do tabeli (kolumna I).

## 4. OCENA SKUTKÓW NARUSZENIA

4.1. Oceny skutków naruszenia dokonuje Radca prawny odpowiedzialny za Proces podlegający ocenie.

4.2. Dla każdego pytania (kolumny od J do L) należy wybrać odpowiedź zgodnie z listą rozwijaną oraz objaśnieniami, dokonując oceny skutków potencjalnego (abstrakcyjnego) naruszenia bezpieczeństwa informacji w analizowanym Procesie dla:

**4.2.1.** dla bezpieczeństwa tajemnicy radcowskiej lub obrończej;

**4.2.2.** dla ciągłości świadczenia pomocy prawnej;

**4.2.3.** dla finansów;

**4.2.4.** dla reputacji.

W celu udzielenia odpowiedzi należy oszacować wagę skutków w danym aspekcie, w przypadku naruszenia bezpieczeństwa analizowanych informacji, **zgodnie z kryteriami zawartymi w zakładce „Kryteria oceny skutków”**.

Przez naruszenie bezpieczeństwa należy uznać naruszenie któregokolwiek z atrybutów bezpieczeństwa informacji, w tym jej **dostępności, poufności, integralności lub rozliczalności.**

Naruszenie bezpieczeństwa może zostać w szczególności spowodowane:

a) **siłą wyższą** (np. uderzenie pioruna w serwerownię, awaria techniczna);

b) intencjonalnym **działaniem zewnętrznym** (np. atak DDOS);

c) **błędami organizacyjnymi** (np. brak dostępnego personelu odpowiedzialnego za utrzymanie systemu w sezonie urlopowym);

d) **nieprzestrzeganiem procedur** (np. zaniechanie ustawienia bezpiecznego hasła).

Należy oceniać skutki przy założeniu **najmniej korzystnego** dla Kancelarii scenariusza wydarzeń.

## 5. CHARAKTER INFORMACJI

5.1. Należy wybrać odpowiedź zgodnie z listą rozwijaną (kolumna M).

## 6. WAŻNOŚĆ INFORMACJI

**6.1.** Pole „ważność informacji" (kolumna N) zostanie uzupełnione automatycznie, w oparciu o następujące założenia:

**6.1.1.** Ważność informacji jest **duża**, w przypadku gdy:

**a)** poziom skutków naruszenia bezpieczeństwa informacji dla bezpieczeństwa tajemnicy radcowskiej lub obrończej, ciągłości świadczenia usług prawnych, finansów lub skutków dla reputacji Radcy prawnego został oceniony jako wysoki; lub

**b)** analizowana informacja jest objęta tajemnicę obrończą .

**6.1.2.** Ważność informacji jest **średnia**, w przypadku gdy poziom skutków naruszenia bezpieczeństwa informacji dla bezpieczeństwa tajemnicy radcowskiej lub obrończej, ciągłości świadczenia usług prawnych lub skutków dla finansów lub reputacji Radcy prawnego został oceniony jako średni, a analizowana informacja jest objęta tajemnicą radcowską.

**6.1.3.** Ważność informacji jest **niska** w pozostałych przypadkach.

## 7. OCENA INFORMACJI

7.1. W celu określenia dopuszczalności przetwarzania informacji w chmurze obliczeniowej, Właściciel biznesowy uzupełnia część zatytułowaną „Ocena informacji" w ramach Formularza A: **Klasyfikacja i ocena informacji**.

7.2. Pole O „Dopuszczalność korzystania z chmury obliczeniowej" zostaje uzupełnione automatycznie.

7.3. Koordynator określa na jakich warunkach dopuszczalne jest skorzystanie z chmury obliczeniowej w ramach Procesu. Warunki korzystania z chmury obliczeniowej należy ogólnie opisać w kolumnie P.

7.4. W kolumnie Q należy zawrzeć uzasadnienie dokonanej oceny. Wypełnienie kolumny Q jest bezwzględnie obowiązkowe.

7.5. Koordynator może wskazać dodatkowe uwagi, istotne z perspektywy ocenianego procesu lub ułatwiające analizę wypełnionego arkusza, wypełniając kolumnę R – „Uwagi”.