# **PRZYKŁAD SzablonU szacowania ryzyka**

| **L.p.** | **Zagrożenie** | **Czynniki ograniczające ryzyko** | **Ocena ryzyka inherentnego** | | **Poziom ryzyka inherentnego (N/Ś/K)\*** | **Decyzja\*\*** | **Plan postępowania z ryzykiem** | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Prawdo  podo  bieństwo | Wpływ | Proponowane zabezpieczenia obniżające ryzyko | **Poziom ryzyka rezydualnego\*** | Osoba odpowiedzialna | Termin wdrożenia |
| **1.** | Rozproszenie geograficzne przetwarzanych informacji (VI.2.1.a) | Usługa chmury obliczeniowej świadczona jest w lokalizacjach:  1) ……..  2) ……. |  |  |  |  |  |  |  |  |
| **2.** | Możliwość utraty zgodności postępowania podmiotu nadzorowanego z przepisami prawa (w tym wydanych licencji i/lub zezwoleń) (VI.2.1.b) |  |  |  |  |  |  |  |  |  |
| **3.** | Dostęp do przetwarzanych informacji przez osoby nieuprawnione (VI.2.1.c) |  |  |  |  |  |  |  |  |  |
| **4.** | Jurysdykcja kraju, w którym odbywa się fizyczne przetwarzanie (lokalizacja CDP) w zakresie dostępu do informacji przez organy administracji krajowej lub międzynarodowej (VI.2.1.d) |  |  |  |  |  |  |  |  |  |
| **5.** | Przywiązanie do jednego Dostawcy usług chmury obliczeniowej (VI.2.1.e) |  |  |  |  |  |  |  |  |  |
| **6.** | Awarie i podatności elementów technologicznych Chmury obliczeniowej (VI.2.1.f) |  |  |  |  |  |  |  |  |  |
| **7.** | Podatność interfejsów zarządzających usługami (VI.2.1.g) |  |  |  |  |  |  |  |  |  |
| **8.** | Ograniczona możliwość wpływania na zakres, kształt i zmiany usług (VI.2.1.h) |  |  |  |  |  |  |  |  |  |
| **9.** | Ograniczona możliwość kontrolowania Dostawcy usług chmury obliczeniowej (VI.2.1.i) |  |  |  |  |  |  |  |  |  |
| **10.** | Podział odpowiedzialności (VI.2.1.j) |  |  |  |  |  |  |  |  |  |
| **11.** | Możliwość korzystania z usług w sposób niezgodny z intencjami podmiotu nadzorowanego (VI.2.2.a) |  |  |  |  |  |  |  |  |  |
| **12.** | Możliwość jednostronnej zmiany warunków technicznych korzystania z usługi (VI.2.2.b) |  |  |  |  |  |  |  |  |  |
| **13.** | Stosowanie domyślnych lub publicznie dostępnych parametrów konfiguracyjnych usług (VI.2.2.c) |  |  |  |  |  |  |  |  |  |
| **14.** | Stosowane mechanizmy uwierzytelniania (VI.2.2.d) |  |  |  |  |  |  |  |  |  |
| **15.** | Zasoby ludzkie (VI.2.3.a) |  |  |  |  |  |  |  |  |  |
| **16.** | Zgodność środowiska technologicznego (VI.2.3.b) |  |  |  |  |  |  |  |  |  |
| **17.** | Szyfrowanie informacji - zarządzanie kluczami (VI.2.5.b) |  |  |  |  |  |  |  |  |  |
| **18.** | Szyfrowanie informacji - wykorzystywane algorytmy (VI.2.5.c) |  |  |  |  |  |  |  |  |  |
| **19.** | Szyfrowanie informacji - "at rest" (VI.2.5.e) |  |  |  |  |  |  |  |  |  |
| **20.** | Szyfrowanie infromacji - "in transit" (VI.2.5.e) |  |  |  |  |  |  |  |  |  |
| **21.** | Szyfrowanie infromacji - kopie kluczy (utrata, poza kontrolą podmiotu nadzorowanego) (VI.2.5.f) |  |  |  |  |  |  |  |  |  |
| **22.** | Kontrola „łańcucha outsourcingowego” - prawne wymogi (VI.2.6.a) |  |  |  |  |  |  |  |  |  |
| **23.** | Kontrola „łańcucha outsourcingowego” - wykluczenia (VI.2.6.b) |  |  |  |  |  |  |  |  |  |
| **24.** | Umowa pomiędzy Dostawcą a Usługą chmury - prawo właściwe (VI.2.8.a) |  |  |  |  |  |  |  |  |  |
| **25.** | Opinia prawna dotycząca prawa państwa trzeciego (VI.2.8.b) |  |  |  |  |  |  |  |  |  |
| **26.** | Inne istotne zagrożenia (VI.9) - Spełnienie wymogów w zakresie RODO |  |  |  |  |  |  |  |  |  |
| **27.** | Inne istotne zagrożenia - monitoring bezpieczeństwa (VI.9) |  |  |  |  |  |  |  |  |  |
| **28.** | Inne istotne zagrożenia - anonimizacja danych (VI.9) |  |  |  |  |  |  |  |  |  |
| **29.** | Inne istotne zagrożenia - badanie podatności technicznych (VI.9) |  |  |  |  |  |  |  |  |  |
| **30.** | Inne istotne zagrożenia - bezpieczeństwo fizyczne CPD (VI.9) |  |  |  |  |  |  |  |  |  |

***\*Poziom ryzyka*** *– N – Niski, Ś – Średni, K – Krytyczny*

*\*\*****Decyzja*** *– oznacza strategię postępowania z ryzykiem, która może obejmować: akceptację (zachowanie), redukcję (modyfikowanie), przeniesienie (dzielenie) lub unikanie ryzyka.*