

105.KSzWzPSPZOZ-DZP-2612-22/K/2026/WG

KLAUZULA BEZPIECZEŃSTWA INFORMACJI **dla Klientów, Dostawców, Wykonawców i Partnerów**

§1

Definicje

1. **Informacje Chronione** – wszelkie informacje, dane, dokumenty, materiały, systemy, zasoby teleinformatyczne, dane osobowe, tajemnice przedsiębiorstwa, informacje techniczne, organizacyjne lub handlowe, niezależnie od formy ich utrwalenia, przekazane lub udostępnione w związku z realizacją Umowy/Zlecenia.
2. **Incydent Bezpieczeństwa** – każde zdarzenie powodujące lub mogące powodować naruszenie poufności, integralności, dostępności, autentyczności lub odporności Informacji Chronionych albo systemów informacyjnych.
3. **Przepisy Bezpieczeństwa** – Norma ISO/IEC 27001, Dyrektywa NIS2, Ustawa o Krajowym Systemie Cyberbezpieczeństwa (UKSC), RODO oraz inne właściwe przepisy sektorowe.
4. **Podwykonawca** – każdy podmiot trzeci zaangażowany przez Stronę do realizacji zobowiązań wynikających z Umowy/Zlecenia.

§2

Ogólny obowiązek zapewnienia bezpieczeństwa informacji

1. Każda ze Stron zobowiązuje się wdrożyć, utrzymywać i doskonalić odpowiednie środki techniczne, organizacyjne, proceduralne i prawne zapewniające ochronę Informacji Chronionych zgodnie z aktualnym poziomem ryzyka, najlepszymi praktykami oraz Przepisami Bezpieczeństwa.
2. Strony potwierdzają stosowanie podejścia opartego na analizie ryzyka, obejmującego identyfikację zagrożeń, ocenę podatności oraz wdrażanie adekwatnych zabezpieczeń.

3. Strona realizująca usługi o znaczeniu krytycznym lub mające wpływ na ciągłość działania drugiej Strony zobowiązana jest stosować środki bezpieczeństwa odpowiadające wymaganiom NIS2 i UKSC.
4. W ramach realizacji usług dla Szpitala, Dostawcy, Wykonawcy, Partnerzy i Serwisanci zobowiązani są do przestrzegania zasad bezpieczeństwa informacji i cyberbezpieczeństwa, które stanowią załącznik nr 1 do niniejszej klauzuli.

§3

Poufność i tajemnica informacji

1. Strony zobowiązują się zachować w ścisłej poufności wszelkie Informacje Chronione.
2. Informacje Chronione mogą być wykorzystywane wyłącznie w celu należytego wykonania Umowy/Zlecenia.
3. Udostępnienie Informacji Chronionych osobom trzecim wymaga uprzedniej pisemnej zgody drugiej Strony, chyba że obowiązek taki wynika z przepisów prawa.
4. Obowiązek poufności obowiązuje przez cały okres obowiązywania Umowy oraz przez okres [5] lat po jej rozwiązaniu, chyba że przepisy szczególne wymagają dłuższego okresu ochrony.

§4

Kontrola dostępu i zarządzanie tożsamością

1. Dostęp do systemów i Informacji Chronionych przyznawany jest wyłącznie osobom upoważnionym, zgodnie z zasadą najmniejszych uprawnień oraz potrzebą biznesową.
2. Strony zobowiązują się stosować mechanizmy silnego uwierzytelniania, w szczególności MFA, dla dostępu uprzywilejowanego, zdalnego oraz do systemów krytycznych.
3. Uprawnienia dostępowe podlegają regularnym przeglądom oraz niezwłocznemu odebraniu po ustaniu podstawy dostępu.

§5

Minimalne środki techniczne i organizacyjne

1. Strony zobowiązują się co najmniej do:
 - a) szyfrowania danych w transmisji oraz – adekwatnie do ryzyka – w spoczynku;
 - b) prowadzenia rejestrów zdarzeń i monitorowania bezpieczeństwa;
 - c) zarządzania podatnościami, aktualizacjami i poprawkami bezpieczeństwa;
 - d) tworzenia kopii zapasowych oraz testowania odtwarzania;
 - e) segmentacji środowisk i zabezpieczeń sieciowych;
 - f) szkoleń personelu;
 - g) wdrożenia planów reagowania na incydenty i ciągłości działania.
2. Na żądanie Strony zobowiązanej, druga Strona przedstawi odpowiednie polityki, procedury lub inne racjonalne dowody spełnienia wymagań.

§6

Zarządzanie incydentami bezpieczeństwa

1. Strona, która wykryje Incydent Bezpieczeństwa mogący wpływać na drugą Stronę, zobowiązana jest poinformować drugą Stronę bez zbędnej zwłoki, nie później niż w terminie 24 godzin od wykrycia.
2. Zawiadomienie powinno obejmować co najmniej: charakter Incydentu, potencjalny wpływ, zastosowane środki zaradcze oraz plan dalszych działań.
3. Strony zobowiązują się współpracować przy analizie, ograniczeniu skutków, usunięciu przyczyn oraz realizacji obowiązków notyfikacyjnych wynikających z prawa.
4. Strona odpowiedzialna za Incydent prowadzi dokumentację oraz działania naprawcze.

§7

Łańcuch dostaw i podwykonawcy

1. Zaangażowanie Podwykonawcy mającego dostęp do Informacji Chronionych lub systemów wymaga zapewnienia przez daną Stronę, że Podwykonawca będzie związany obowiązkami bezpieczeństwa nie mniej rygorystycznymi niż przewidziane w Umowie/Zleceniu.

2. Strona korzystająca z Podwykonawców odpowiada za ich działania i zaniechania jak za własne.
3. Na żądanie drugiej Strony należy ujawnić listę krytycznych Podwykonawców związanych z realizacją Umowy/Zlecenia, z uwzględnieniem ograniczeń prawnych.

§8

Audyt, weryfikacja i prawo kontroli

1. Strona uprawniona ma prawo, z zachowaniem uzasadnionych zasad poufności i bezpieczeństwa, do przeprowadzenia audytu zgodności lub żądania przedstawienia dokumentacji potwierdzającej spełnianie wymagań bezpieczeństwa.
2. Audyt może być realizowany samodzielnie lub przez niezależny podmiot trzeci związany poufnością.
3. W przypadku stwierdzenia niezgodności, Strona zobowiązana wdroży plan działań naprawczych w uzgodnionym terminie.

§9

Ciągłość działania i odporność operacyjna

1. Strony zobowiązują się posiadać i utrzymywać adekwatne plany ciągłości działania (BCP) oraz odtwarzania po awarii (DRP).
2. Na żądanie, Strony określą parametry usługowe, w tym RTO/RPO, dla usług krytycznych.
3. Istotne zakłócenia operacyjne podlegają niezwłocznej komunikacji.

§10

Dane osobowe i zgodność regulacyjna

1. Jeżeli realizacja Umowy/Zlecenia obejmuje przetwarzanie danych osobowych, Strony zobowiązują się działać zgodnie z RODO oraz zawrzeć odrębne wymagane porozumienia, w tym umowę powierzenia przetwarzania danych, jeśli ma zastosowanie.

2. Strony zobowiązują się stosować *privacy by design (uwzględnienie ochrony danych w fazie projektowania)* oraz *privacy by default (zasada domyślnej ochrony danych)* tam, gdzie wymagają tego przepisy.
3. Każda ze Stron niezwłocznie informuje drugą o naruszeniach ochrony danych mających wpływ na realizację Umowy.

§11

Odpowiedzialność, naruszenia i środki naprawcze

1. Istotne naruszenie obowiązków bezpieczeństwa stanowi istotne naruszenie Umowy.
2. Strona naruszająca zobowiązana jest do:
 - a) niezwłocznego usunięcia naruszenia;
 - b) minimalizacji skutków;
 - c) pokrycia uzasadnionych szkód wynikających z naruszenia, zgodnie z Umową i prawem.
3. Strony mogą przewidzieć kary umowne za naruszenia określonych obowiązków bezpieczeństwa, bez uszczerbku dla prawa dochodzenia odszkodowania przewyższającego wysokość kary, o ile prawo właściwe na to zezwala.

§12

Rozwiązanie Umowy i zwrot informacji

1. Po zakończeniu współpracy Strona zobowiązana niezwłocznie zwróci lub bezpiecznie usunie Informacje Chronione, chyba że dalsze przechowywanie wynika z obowiązków prawnych.
2. Usunięcie danych powinno być potwierdzone stosownym oświadczeniem, jeśli druga Strona tego zażąda.

§13

Postanowienia końcowe

1. W przypadku sprzeczności pomiędzy niniejszymi klauzulami a mniej restrykcyjnymi postanowieniami operacyjnymi, pierwszeństwo mają postanowienia zapewniające wyższy poziom bezpieczeństwa.

2. Klauzule podlegają okresowym przeglądom w związku ze zmianami prawa, ryzyka lub środowiska operacyjnego.
3. Nieważność jednego z postanowień nie wpływa na ważność pozostałych.

Zasady bezpieczeństwa informacji i cyberbezpieczeństwa

1. Dostawca może uzyskać dostęp do infrastruktury teleinformatycznej, systemów informatycznych, urządzeń medycznych, sieci teleinformatycznej lub danych Zamawiającego wyłącznie w zakresie niezbędnym do realizacji Umowy/Zlecenia oraz po uprzednim uzyskaniu zgody Zamawiającego.
2. Dostęp do systemów lub infrastruktury Zamawiającego może zostać nadany wyłącznie:
 - a) imiennie wskazanym osobom,
 - b) po przeprowadzeniu weryfikacji tożsamości tych osób,
 - c) po akceptacji przez upoważnionego przedstawiciela Zamawiającego,
 - d) na czas określony i w zakresie minimalnych niezbędnych uprawnień.
3. Dostawca zobowiązuje się do każdorazowego zgłaszania:
 - a) planowanych prac serwisowych,
 - b) konieczności uzyskania dostępu zdalnego,
 - c) zmiany osób realizujących Umowę,
 - d) incydentów bezpieczeństwa lub podejrzeń naruszenia bezpieczeństwa.
4. Zamawiający ma prawo odmówić dostępu do infrastruktury lub systemów w przypadku:
 - a) braku możliwości potwierdzenia tożsamości osoby wykonującej prace,
 - b) braku wcześniejszego zgłoszenia prac,
 - c) naruszenia procedur bezpieczeństwa obowiązujących u Zamawiającego,
 - d) uzasadnionego podejrzenia zagrożenia dla bezpieczeństwa systemów lub danych.
5. Dostawca zobowiązuje się, że:
 - a) wykorzystywany sprzęt i oprogramowanie będą aktualne i wolne od znanych podatności krytycznych,
 - b) osoby realizujące Umowę będą posiadały aktualne upoważnienia i niezbędne kompetencje,

- c) dostęp zdalny będzie realizowany wyłącznie poprzez mechanizmy zaakceptowane przez Zamawiającego, w szczególności VPN lub dedykowane rozwiązania dostępu zdalnego.
6. Zabrania się:
- a) udostępniania kont dostępowych osobom trzecim,
 - b) korzystania z prywatnych nośników danych
 - c) instalowania nieautoryzowanego oprogramowania,
 - d) podłączania nieautoryzowanych urządzeń do sieci Zamawiającego.
7. Dostawca zobowiązuje się do niezwłocznego poinformowania Zamawiającego o każdym incydencie bezpieczeństwa mogącym mieć wpływ na:
- a) ciągłość działania systemów,
 - b) bezpieczeństwo danych,
 - c) dostępność usług medycznych,
 - d) bezpieczeństwo infrastruktury teleinformatycznej.
8. Po zakończeniu realizacji Umowy Dostawca zobowiązuje się do:
- a) niezwłocznego zaprzestania korzystania z dostępu,
 - b) usunięcia danych Zamawiającego znajdujących się w jego posiadaniu, jeżeli nie istnieje podstawa prawna do dalszego przetwarzania,
 - c) zwrotu wszelkich nośników, identyfikatorów i urządzeń udostępnionych przez Zamawiającego.
9. Zamawiający zastrzega sobie prawo do żądania od osób realizujących prace po stronie Dostawcy, w szczególności posiadających dostęp do infrastruktury krytycznej, systemów teleinformatycznych, danych medycznych, serwerowni, urządzeń sieciowych lub systemów bezpieczeństwa, przedłożenia aktualnego zaświadczenia o niekaralności lub innych dokumentów potwierdzających spełnienie wymagań bezpieczeństwa określonych przez Zamawiającego.
10. Odmowa przedstawienia dokumentów, o których mowa w ust. 9, może stanowić podstawę do odmowy dopuszczenia danej osoby do realizacji prac na terenie Zamawiającego lub uzyskania dostępu do systemów i infrastruktury Zamawiającego.
11. Naruszenie przez Dostawcę zasad bezpieczeństwa informacji i cyberbezpieczeństwa może stanowić podstawę do:
- a) natychmiastowego zablokowania dostępu,
 - b) wstrzymania realizacji prac,

- c) rozwiązania Umowy z winy Dostawcy,
- d) dochodzenia odszkodowania na zasadach ogólnych.