



Wymagania w zakresie przetwarzania danych osobowych RODO

1. Zamawiający wymaga, aby Wykonawca gwarantował bezpieczeństwo przetwarzania danych, zgodnie ze standardem Europejskiego Obszaru Gospodarczego, tj.:
 - 1.1. Wykonawca zagwarantuje, że wszystkie dane osobowe oraz zasoby cyfrowe (w tym kopie zapasowe) przetwarzane w ramach Systemu będą przechowywane i przetwarzane wyłącznie w centrach danych (serwerowniach) zlokalizowanych na terenie Europejskiego Obszaru Gospodarczego.
 - 1.2. Wykonawca zobowiązuje się, że dane podopiecznych i pracowników Zamawiającego nie będą przekazywane do państw trzecich (poza EOG) ani do organizacji międzynarodowych, chyba że obowiązek taki nakłada na Wykonawcę prawo Unii lub prawo państwa członkowskiego.
 - 1.3. W przypadku korzystania z usług poddostawców infrastruktury chmurowej (np. Microsoft Azure, AWS, Google Cloud), Wykonawca musi zapewnić i udokumentować, że fizyczna lokalizacja instancji serwerowych przypisanych do Zamawiającego znajduje się w regionie UE (np. Warszawa, Frankfurt).
 - 1.4. Zamawiający zastrzega sobie prawo do żądania od Wykonawcy wskazania dokładnego adresu fizycznego centrum danych, w którym przechowywane są dane, oraz przedstawienia dowodów potwierdzających stosowanie tam zabezpieczeń zgodnych z art. 32 RODO.
2. Zamawiający wymaga, aby Wykonawca spełnił wymagania dotyczące bezpieczeństwa, dostępności i infrastruktury systemu SaaS, tj.:
 - 2.1. Wykonawca musi legitymować się aktualnym certyfikatem ISO/IEC 27001 (System Zarządzania Bezpieczeństwem Informacji) obejmującym zakres usług przetwarzania danych w chmurze oraz wytwarzania oprogramowania.
 - 2.2. Kopia certyfikatu wraz z zakresem akredytacji musi zostać dostarczona Zamawiającemu na etapie składania ofert. Wykonawca zobowiązuje się do utrzymania ważności certyfikatu przez cały okres obowiązywania umowy.
 - 2.3. Wykonawca gwarantuje dostępność Systemu na poziomie minimum 99,5% w skali każdego miesiąca kalendarzowego.



- 2.4. Dostępność rozumiana jest jako możliwość poprawnego zalogowania się do Systemu oraz korzystania ze wszystkich jego funkcji przez użytkowników (zarówno w wersji stacjonarnej, jak i mobilnej).
- 2.5. Czas dostępności liczony jest w trybie 24/7/365. Za każdą rozpoczętą godzinę przerwy w dostępności Systemu powyżej dopuszczalnego limitu (0,5% czasu w miesiącu), Wykonawca zapłaci karę umowną zgodnie z zapisami zawartymi w postanowieniach umowy.
- 2.6. Wykonawca zobowiązany jest do wykonywania pełnych kopii zapasowych (backupów) bazy danych oraz wszystkich plików Systemu z częstotliwością minimum raz na 24 godziny.
- 2.7. Kopie zapasowe muszą być przechowywane w bezpiecznej lokalizacji fizycznej, innej niż lokalizacja serwera głównego (tzw. geo-redundancja), aby zapewnić odzyskanie danych w przypadku awarii całego centrum danych.
- 2.8. Wykonawca gwarantuje, że czas przywrócenia pełnej sprawności Systemu z kopii zapasowej w przypadku awarii krytycznej nie przekroczy 12 godzin.
- 2.9. Dostęp do Systemu (zarówno przez przeglądarkę WWW, jak i aplikację mobilną) musi odbywać się wyłącznie przez szyfrowany protokół HTTPS przy użyciu certyfikatu SSL/TLS w wersji minimum 1.2 (lub wyższej, jeśli standardy bezpieczeństwa ulegną zmianie).
- 2.10. Wykonawca odpowiada za zapewnienie i terminowe odnawianie certyfikatów bezpieczeństwa niezbędnych do poprawnego działania Systemu.
3. Zamawiający wymaga, aby Wykonawca spełnił wymagania dotyczące ochrony danych składowych:
 - 3.1. Wszystkie dane osobowe oraz informacje wrażliwe (dotyczące stanu zdrowia, sytuacji majątkowej i rodzinnej podopiecznych) zapisane w bazie danych u dostawcy muszą być objęte mechanizmem szyfrowania danych składowanych.
 - 3.2. Zastosowane algorytmy szyfrujące muszą uniemożliwiać odczyt danych osobom nieuprawnionym, w tym personelowi technicznemu dostawcy chmury oraz administratorom serwerowni, nieposiadającym dedykowanych kluczy deszyfrujących Zamawiającego.
 - 3.3. Klucze szyfrujące muszą być zarządzane w sposób bezpieczny, uniemożliwiający ich przejęcie przez osoby trzecie.
 - 3.4. System musi umożliwiać natychmiastowe zablokowanie dostępu do aplikacji mobilnej oraz panelu desktopowego w przypadku rozwiązania umowy z pracownikiem lub utraty urządzenia (zagubienie/kradzież telefonu). Wyłączenie lub usunięcie konta użytkownika nie może powodować utraty powiązanej z nim historii zdarzeń; system musi zapewniać trwałe przechowywanie logów i historii



działań do celów kontrolnych i archiwalnych, zgodnie z obowiązującymi przepisami prawa.

4. Wykonawca jako Podmiot Przetwarzający jest zobowiązany do podpisania z Zamawiającym – Administratorem Danych umowy powierzenia przetwarzania danych osobowych, w pełni zgodnej z wymaganiami art. 28 Rozporządzenia RODO, przed przystąpieniem do wdrożenia.
5. Zamawiający wymaga od Wykonawcy oświadczenia, że wdroży i utrzyma odpowiednie środki techniczne i organizacyjne, o których mowa w art. 32 RODO, w celu zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku naruszenia praw lub wolności osób fizycznych.
6. Zamawiający określa strategię wyjścia:
 - 6.1. Zamawiający jest wyłącznym właścicielem wszystkich danych wprowadzonych do Systemu. Wykonawca nie ma prawa do ich wykorzystywania w celach innych niż realizacja umowy.
 - 6.2. System musi umożliwiać Zamawiającemu samodzielny, nieograniczony eksport danych w dowolnym momencie trwania umowy do otwartych, powszechnie stosowanych formatów edytowalnych (np. .XLSX, .CSV, .XML).
 - 6.3. Zamawiający wymaga, aby Wykonawca w terminie 14 dni od wygaśnięcia lub rozwiązania umowy przekazał Zamawiającemu pełną kopię bazy danych (zrzut bazy SQL oraz wszystkie załączniki/skany/podpisy w formacie binarnym) w sposób umożliwiający ich odczyt i migrację do innego systemu.
 - 6.4. Po potwierdzeniu przez Zamawiającego poprawnego odbioru danych, Wykonawca zobowiązany jest do bezpowrotnego i bezpiecznego usunięcia wszystkich kopii danych Zamawiającego ze swoich serwerów oraz nośników backupowych, a następnie przedłożenia stosownego protokołu zniszczenia danych.
 - 6.5. Wszystkie czynności związane z wydaniem danych po zakończeniu umowy są wliczone w cenę oferty i nie mogą generować dodatkowych kosztów dla Zamawiającego.