WYMAGANIA BEZPIECZEŃSTWA W ZWIĄZKU Z POWIERZENIEM PRZETWARZANIA DANYCH OSOBOWYCH POZA INFRASTRUKTURĄ PSG W MODELU CHMURY OBLICZENIOWEJ LUB HOSTINGU,

ZWANE DALEJ „WYMAGANIAMI BEZPIECZEŃSTWA"

- ZAŁĄCZNIK NR 1 DO UMOWY O POWIERZENIU PRZETWARZANIA DANYCH OSOBOWYCH NR [***]

§ 1. POSTANOWIENIA OGÓLNE

1. Wykonawca, któremu PSG powierza przetwarzanie danych osobowych, o których mowa w § 1.1 Umowy (**Dane**) poza infrastrukturą PSG w modelu chmury obliczeniowej lub hostingu, zapewnia, że będzie przetwarzać powierzone Dane zgodnie z Umową oraz przepisami prawa (**Usługa**), przy czym Dane oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Jeżeli w wyniku zmiany stanu prawnego na Wykonawcy będą ciążyć dalej idące obowiązki związane z zapewnianiem bezpieczeństwa Danych niż te, które wynikają z Umowy, Wykonawca zobowiązuje się takie obowiązki wypełniać bez potrzeby zmiany Umowy.

2. Wykonawca oświadcza, że posiada niezbędne doświadczenie i zapewnia warunki techniczne i organizacyjne oraz prawne niezbędne do prawidłowego wykonania Umowy oraz że personel realizujący w jego imieniu Umowę posiada niezbędne kompetencje oraz podlega regularnym szkoleniom z zakresu bezpieczeństwa danych. Wykonawca zobowiązuje się ujawnić PSG wszelkie informacje mogące w istotny sposób wpłynąć na jego zdolność do wykonania zleconych mu w ramach Umowy Usług.

3. Wykonawca wskazuje następujące pełne informacje o wszystkich fizycznych lokalizacjach (tj. miasto i kraj), w tym o miejscach przechowywania kopii zapasowych oraz centrach przetwarzania wykorzystywanych na potrzeby Disaster Recovery, w których są oraz mogą być przetwarzane powierzone przez PSG Dane w rozbiciu na umiejscowienie serwerów i miejsc zdalnego dostępu do powierzonych Danych:

   1) [***],

   2) [***].

   O wszelkich zmianach informacji wskazanych w zdaniu pierwszym Wykonawca ma obowiązek niezwłocznie pisemnie poinformować PSG na adres wskazany w § 7.1.1) Umowy, przy czym Strony zastrzegają, że zmiana informacji wskazanych w zdaniu pierwszym nie wymaga zawarcia pisemnego aneksu do Umowy. Wykonawca jest zobowiązany uzyskać uprzednią zgodę PSG, jeśli zamierza rozszerzyć obszar przetwarzania powierzonych Danych o miejsca zlokalizowane poza Europejskim Obszarem Gospodarczym, co będzie wiązało się z koniecznością zawarcia aneksu do Umowy.

4. Wykonawca zobowiązuje się wskazać PSG pełną listę podwykonawców biorących udział w realizacji Usługi w terminie 3 (słownie: 3) dni od dnia zawarcia Umowy.

5. W przypadku dalszego powierzenia przetwarzania danych przez Wykonawcę, za zgodą PSG wyrażoną w trybie określonym w Umowie, Wykonawca nałoży na podwykonawcę obowiązek przestrzegania wszelkich zasad, reguł i zobowiązań określonych w Wymaganiach Bezpieczeństwa, w zakresie, w jakim odnosić się one będą do zakresu prac danego podwykonawcy, pozostając jednocześnie gwarantem ich wykonania oraz przestrzegania przez podwykonawcę. Jeśli wykonanie Umowy przez podwykonawcę wiąże się ze zmianą miejsc przetwarzania Danych, Wykonawca zobowiązany jest zaktualizować wykaz zgodnie z ust. 3. Wykonawca na każde żądanie PSG dostarczy listę wszystkich podwykonawców wraz z dokładnym zakresem realizowanych przez nich zadań przy przetwarzaniu powierzonych Danych.

6. PSG jest uprawniona do obciążenia Wykonawcy karą umowną w wysokości 100.000,00 zł (słownie: sto tysięcy złotych) za każdy stwierdzony incydent związany z bezpieczeństwem Danych. Incydent związany z bezpieczeństwem Danych (**Incydent**) stanowi pojedyncze zdarzenie lub serię niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem Danych, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu Danych.

7. Wykonawca jest zobowiązany do zapłaty naliczonych przez PSG kar umownych w terminie 14 dni od dnia doręczenia noty obciążeniowej wystawionej przez PSG. Nota zostanie przesłana Wykonawcy na adres wskazany w § 7.1.2) Umowy.

8. PSG jest uprawniony do dochodzenia odszkodowania przewyższającego wysokość zastrzeżonych kar umownych, na zasadach ogólnych.

9. Postanowienia dotyczące kar umownych są postanowieniami o charakterze samoistnym, a odstąpienie od Umowy lub przedterminowe wygaśnięcie Umowy z innych przyczyn, niezależnie od podstawy prawnej, nie powoduje utraty przez nie mocy.

§ 2. BEZPIECZEŃSTWO DANYCH

1. Wszystkie Dane których przetwarzanie PSG powierza Wykonawcy w związku z zawarciem Umowy Głównej stanowią własność PSG. Dla uniknięcia wątpliwości, PSG zachowuje własność Danych również w sytuacji jakiejkolwiek zmiany stanu prawnego Wykonawcy, w tym jego przekształcenia, łączenia, podziału lub zmiany struktury właścicielskiej, jak również likwidacji lub ogłoszenia upadłości Wykonawcy. Wykonawca jest zobowiązany do poinformowania o jakichkolwiek zdarzeniach mogących mieć wpływ na bezpieczeństwo Danych, w szczególności w razie złożenia wniosku o upadłość Wykonawcy, rozpoczęcia postępowania likwidacyjnego lub też wystąpienia okoliczności w jakiejkolwiek jurysdykcji, które mają wobec Wykonawcy podobny skutek. Informacja, o której mowa w zdaniu trzecim powinna zostać przekazana PSG, na adres wskazany w § 7.1.1) Umowy, niezwłocznie, jednakże nie później niż w terminie 3 dni od zaistnienia zdarzenia, którego dotyczy. Wykonawca zapewnia i gwarantuje PSG pełen dostęp do Danych przez cały okres obowiązywania Umowy Głównej, a w razie rozwiązania lub wygaśnięcia Umowy Głównej, również przez okres niezbędny dla PSG do odzyskania całości przekazanych Danych, jednakże nie krótszy niż 90 dni od dnia, w którym z jakichkolwiek przyczyn Umowa Główna została skutecznie rozwiązana lub wygasła.

2. Wykonawca zobowiązuje się zapewnić PSG pełen dostęp do powierzonych Danych w zakresie i w czasie wskazanym przez PSG. Wykonawca zapewni możliwość pobrania przez PSG w dowolnym momencie obowiązywania Umowy całości powierzonych Danych w formie standardowych formatów danych eksportowych zapewniających ich przenośność oraz biznesową przydatność, a operacja ta nie może wymagać zmian konfiguracyjnych lub być uzależniona od jakiejkolwiek innej operacji po stronie Wykonawcy.

3. Wykonawca zapewnia, że użytkownicy innych klientów Wykonawcy nie będą mieli dostępu do przetwarzanych w ramach Umowy Danych oraz że Dane będą odseparowane co najmniej w sposób logiczny od informacji jakichkolwiek innych podmiotów, w tym innych klientów Wykonawcy zgodnie z postanowieniami § 3.

4. Wykonawcy oraz jego podwykonawcom nie przysługuje prawo wykorzystywania przetwarzanych Danych dla celów innych niż wykonanie Umowy, w tym m.in. ich łączenia z innymi Danymi.

5. Wykonawca zobowiąże wszystkie osoby z jego personelu zatrudnione przy przetwarzaniu powierzanych Danych do zachowania w poufności ich treści oraz sposobów ich zabezpieczenia i wykorzystywania ich tylko w celach określonych w Umowie.

§ 3. BEZPIECZEŃSTWO TELEINFORMATYCZNE

1. Wykonawca zobowiązuje się wdrożyć określone w niniejszym paragrafie skuteczne i adekwatne organizacyjno – techniczno - prawne mechanizmy gwarantujące bezpieczeństwo przetwarzania Danych oraz poufność, integralność, dostępność i rozliczalność powierzonych Danych.

2. Obowiązek, o którym mowa w ust. 1, Wykonawca realizuje poprzez wdrożenie zabezpieczeń chroniących Dane przed ich przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą, zmianą, nieupoważnionym ujawnieniem lub dostępem, w szczególności poprzez:

   1) szyfrowanie Danych, które stosuje się zarówno wobec „informacji w tranzycie", jak i informacji przechowywanych na serwerach, w kopiach zapasowych oraz wobec mechanizmów autoryzacji,

   2) bezpieczne składowanie kluczy szyfrujących, w tym w szczególności poprzez składowanie ich w odseparowaniu od serwera/serwerów, w których zlokalizowane będą Dane podlegające szyfrowaniu oraz wdrożenie procedury zarządzania dostępem do tych Danych gwarantującej ich bezpieczeństwo oraz dostęp wyłącznie upoważnionym przedstawicielom PSG,

   3) wirtualne środowiska dedykowane wyłącznie na potrzeby PSG dostępne wyłącznie przez kanał VPN i tylko z klasy adresowej IP PSG z wdrożonymi mechanizmami separującymi (co najmniej na poziomie logicznym) Dane od danych osobowych osób trzecich (innych odbiorców usług Wykonawcy) lub inne, zaakceptowane przez PSG rozwiązanie zapewniające separację Danych od danych osobowych osób trzecich,

   4) opracowanie i wdrożenie procedury dostępu do Danych zapewniającej:

      a) dostęp do Danych wyłącznie dla osób upoważnionych przez PSG (**Użytkowników Usługi**),

      b) silne dwuskładnikowe uwierzytelnianie,

      c) bezpieczne przechowywanie danych uwierzytelniających Użytkowników Usługi,

      d) rozliczalność, rozumianą jako możliwość jednoznacznego przypisania działań do konkretnego Użytkownika Usługi,

   5) usunięcie przez Wykonawcę z nośników wycofywanych z eksploatacji wszystkich powierzonych Danych z tym zastrzeżeniem, że usunięcie Danych musi być dokonane w sposób bezpowrotny (czyli w taki sposób, żeby ich ponowne odtworzenie ani w całości, ani w części nie było możliwe), a w przypadku, gdy bezpowrotne usunięcie Danych z ww. nośników metodą programową nie jest możliwe, nośniki, na których przetwarzane są Dane muszą zostać fizycznie zniszczone; Wykonawca jest zobowiązany dostarczyć protokół z czynności wymienionych w niniejszym punkcie opisujący szczegółowo co zostało wykonane, przez kogo, z zastosowaniem jakich narzędzi i algorytmów oraz jakich/których Danych te czynności dotyczyły.

3. Wykonawca zobowiązuje się do opracowania i wdrożenia procedur identyfikacji i zarządzania podatnościami bezpieczeństwa, w tym dokonywania regularnych aktualizacji oprogramowania komponentów infrastruktury i oprogramowania znajdujących się pod kontrolą Wykonawcy.

4. Wykonawca zobowiązuje się do stosowania skutecznych środków zapewniających ciągłość świadczenia Usługi, w tym do:

   1) stosowania adekwatnych systemów, zasobów i procedur pozwalających na zachowanie ciągłości i regularności działania Usługi, w tym tworzenie aktualnych kopii zapasowych umożliwiających w sytuacji awaryjnej lub w przypadku katastrofy odtworzenie informacji wraz z oprogramowaniem oraz przygotowanie i wdrożenie procedur zapewniających ich regularne testowanie oraz odtwarzanie,

   2) opracowania i testowania procedur awaryjnych i okresowego testowania infrastruktury rezerwowej. Wykonawca jest zobowiązany przedstawiać PSG niezwłocznie do wglądu raporty z przedmiotowych testów,

   3) zabezpieczenia przed utratą połączenia sieciowego, awarią zasilania, przerwą w dostawie prądu, uszkodzeniem sprzętu,

   4) zabezpieczenia przed atakiem typu DDoS (*distributed denial of service).*

5. Wszystkie komponenty Usługi są wolne od znanych podatności.

6. Usługa nie będzie posiadała znanych podatności technicznych, będzie na bieżąco aktualizowana (min. raz w miesiącu) o poprawki udostępniane przez producenta danego rozwiązania.

7. Usługa podlegać będzie cyklicznemu procesowi utwardzania konfiguracji np. zgodnie z ogólnodostępnymi dla danego rozwiązania zaleceniami (np. CIS Benchmark).
8. Wszystkie komponenty Usługi, w tym system operacyjny, serwery baz danych i aplikacyjne będą stosowane w aktualnej, oficjalnie wspieranej przez ich producenta wersji.
9. Wszystkie komputery i serwer, na którym będą przetwarzane Dane będą wyposażone w komercyjny program antywirusowy z automatycznie aktualizowaną na bieżąco bazą sygnatur.
10. Wszystkie stosowanie w Usłudze połączenia sieciowe będą szyfrowane za pomocą protokołów, algorytmów i ich konfiguracji powszechnie uznawanych za bezpieczne (np. TLS 1.3).
11. Każdy z Użytkowników Usługi będzie posiadał indywidualne konto, pozwalające na jednoznaczną identyfikację osoby fizycznej, która uzyskała dostęp do Danych.
12. Każdy z Użytkowników Usługi będzie korzystał z mocnych haseł lub z metod mocnego uwierzytelnienia.
13. Hasło Użytkownika Usługi musi składać się z minimum 12 znaków. Hasło musi zawierać:
    1) małe litery łacińskie,
    2) duże litery łacińskie,
    3) cyfry,
    4) znaki specjalne.
14. W przypadku jeżeli Usługa dostępna jest w sieci publicznej, każdy z Użytkowników Usługi (w tym też administratorzy komponentów systemowych) będą mogli uzyskać dostęp tylko po mocnej autoryzacji (wymagane jest MFA – multifactor authentication).
15. W przypadku dostępu do Usługi poprzez sieć Internet (zdalnie) wymagane jest stosowanie mocnej autoryzacji (np. dla połączenia VPN) tj. wymagane jest MFA – multifactor authentication.
16. Usługa musi posiadać możliwość konfigurowalnego raportowania i automatycznego monitorowania i logowania aktywności Użytkowników Usługi.
17. W Usłudze zostały zaprojektowane role wraz ze wskazaniem ich zakresu zadań i odpowiedzialności.
18. W Usłudze uwzględniono zasadę przyznawania Użytkownikom Usługi minimalnych uprawnień, niezbędnych do wykonywania obowiązków służbowych.
19. Sposobem transmisji danych do przeglądarki WWW jest szyfrowanie przepływu danych, w szczególności należy wykorzystać szyfrowanie danych protokołem TLS (w jego bezpiecznej wersji np. TLS 1.3) podczas komunikacji przy pomocy przeglądarki. Usługa jest wyposażona w certyfikaty SSL (w jego bezpiecznej wersji) dla serwerów WWW, a transmisja danych powinna odbywać się z wykorzystaniem do tego celu protokołu HTTPS.
20. Ruch sieciowy pomiędzy wszystkimi elementami Usługi musi być szyfrowany za pomocą protokołów i algorytmów kryptograficznych uznanych powszechnie za bezpieczne. Wymagane jest stosowanie protokołów TLSv1.2, TLS1.3 lub ich nowszych wersji, preferowane jest stosowanie protokołu TLSv1.3. Nie jest dopuszczalne stosowanie protokołu IPSec oraz protokołów SSL 2.0, SSL 3.0, TLS 1.0 i TLS 1.1 i starszych.
21. Wymagane jest stosowanie protokołów, algorytmów oraz ich konfiguracji powszechnie uznanych za bezpieczne.
22. Wymagane jest stosowanie zaufanych certyfikatów X.509 dostarczonych przez komercyjne, globalnie zaufane CA. Dopuszczalne jest też stosowanie certyfikatów dostarczonych przez PSG. Wymagana, minimalna długość klucza dla ECC to 384 bitów, dla RSA to 2048 bitów. Usługa jest objęta archiwizacją danych.
23. Usługa umożliwia przechowywanie i zarządzanie zdarzeniami (logi) oraz ich eksport. Strony ustalają następujące zasady dotyczące procedury przechowywania i zarządzania zdarzeniami (logi) oraz ich eksportu:
    1) [***],
    2) [***].

24. Mechanizmy śledzenia zdarzeń i rozliczalności oraz informacje w dziennikach zdarzeń (logi) są chronione przed manipulacją i nieuprawnionym dostępem.
25. Do dzienników zdarzeń lub ich archiwów, mogą mieć dostęp wyłącznie osoby uprawnione. Usługa musi zapewniać integralność dzienników zdarzeń.
26. Pola zawierające dane uwierzytelniające nie są uzupełniane przez Usługę.
27. Wszystkie operacje dotyczące uwierzytelniania (takie jak rejestracja, aktualizacja profilu, przypomnienie loginu, przypomnienie hasła), które powodują odzyskanie dostępu do konta, posiadają przynajmniej takie same zabezpieczenia jak podstawowe mechanizmy uwierzytelniania.
28. Funkcja zmiany hasła zawiera konieczność podania hasła obecnie używanego, nowego hasła oraz konieczność ponownego wpisania nowego hasła.
29. Mechanizmy odzyskiwania hasła nie ujawniają dotychczasowych haseł i nowe hasło nie jest przesyłane w formie jawnej do Użytkownika Usługi.
30. Nie jest możliwa enumeracja wykorzystująca loginy Użytkowników Usługi, funkcję resetowania hasła lub funkcjonalność przypomnienia nazwy Użytkownika Usługi.
31. Platforma lub inne komponenty, z których korzysta Usługa nie używają domyślnych haseł (np. admin/password).
32. Wdrożono mechanizmy przeciwdziałające automatyzacji, aby zapobiegać testowaniu ujawnionych danych uwierzytelniających, atakom brute force i atakom blokującym konta.
33. Wdrożono mechanizmy blokujące użycie znanych lub słabych haseł.
34. Interfejs administracyjny nie jest dostępny dla stron niezaufanych.
35. Sesje są unieważniane po wylogowaniu się Użytkownika Usługi.
36. Usługa nie jest podatna na atak LDAP Injection lub mechanizmy bezpieczeństwa zapobiegają wystąpieniu takiego ataku.
37. Środowisko uruchomieniowe nie jest podatne na atak wstrzyknięcia komend systemu operacyjnego lub mechanizmy bezpieczeństwa zapobiegają wystąpieniu takiego ataku.
38. Usługa nie jest podatna na ataki zdalnego lub lokalnego dołączenia plików (Remote File Inclusion - RFI lub Local File Inclusion - LFI) gdy wykorzystywana jest treść będąca ścieżką do plików.
39. Usługa nie jest podatna na ataki XML Injection, XML External Entity, XPath query lub mechanizmy bezpieczeństwa zapobiegają wystąpieniu takich ataków.
40. Usługa jest zabezpieczona przed atakami typu HTTP Parametr Pollution.
41. Dane zapisywane po uwierzytelnieniu w pamięci przeglądarki np. w DOM są czyszczone po zakończeniu sesji.
42. Identyfikatory sesji nigdy nie są ujawniane w URL, w komunikatach błędów lub logach.
43. Każde pomyślne uwierzytelnienie, a także ponowne uwierzytelnienie, tworzy nową sesję z nowym identyfikatorem.
44. Identyfikatory sesji przechowywane w ciasteczkach mają ustawioną ścieżkę z wartością odpowiednio restrykcyjną dla danej aplikacji i tokeny sesji uwierzytelniania mają dodatkowo ustawione atrybuty "HttpOnly" i "secure”.
45. Została wdrożona zasada minimalnych uprawnień – Użytkownicy Usługi powinni mieć dostęp tylko do funkcji, plików, linków URL, usług oraz innych zasobów do których posiadają zezwolenie.
46. Usługa nie zwraca komunikatów o błędach lub śladów stosu (stack traces), które zawierają dane które mogą pomóc atakującym. Zawierają się w tym identyfikatory sesji, wersje oprogramowania / platformy.
47. Dla wszystkich połączeń (zewnętrznych i wewnętrznych), które są uwierzytelniane lub związane z danymi wymienionymi w ust. 46 lub funkcjami, jest wykorzystywany TLS a także nie jest możliwe pogorszenie parametrów połączenia do połączenia niezabezpieczonego. Preferowany jest najsilniejszy dostępny algorytm szyfrowania.

48. Wszystkie połączenia do zewnętrznych systemów są uwierzytelniane.

49. Nagłówki HTTP Strict Transport Security są włączone do wszystkich zapytań i dla wszystkich poddomen.

50. Używane są tylko silne algorytmy, szyfry i protokoły w ramach całej hierarchii certyfikatów, włącznie z certyfikatem root i certyfikatami pośrednimi w ramach wybranego urzędu certyfikacji.

51. Konfiguracja TLS jest zgodna z bieżącymi najlepszymi praktykami szczególnie dlatego, że popularne ustawienia, szyfry i algorytmy z czasem mogą okazać się niebezpieczne.

52. Usługa akceptuje tylko zdefiniowany zestaw metod zapytań HTTP, takich jak GET i POST oraz nieużywane metody (takie jak TRACE, PUT, DELETE) są w sposób wyraźny zablokowane.

53. Każda odpowiedź HTTP zawiera nagłówek „content type", określający bezpieczny zestaw znaków (np. UTF-8, ISO 8859-1).

54. Nagłówki HTTP lub jakakolwiek część odpowiedzi HTTP nie ujawniają szczegółowej informacji o wersjach komponentów Usługi.

§ 4. PUNKTY KONTAKTU ORAZ POSTĘPOWANIE NA WYPADEK INCYDENTU

1. Strony ustalają następujące punkty kontaktu we wszelkich sprawach związanych z bezpieczeństwem Usługi:

   1) PSG – adres: [***], tel. [***], e-mail: [***],

   2) Wykonawca – adres: [***], tel. [***], e-mail: [***].

2. Wykonawca zobowiązuje się do:

   1) niezwłocznego, nie później jednak niż w ciągu 6 godzin od chwili otrzymania informacji o Incydencie, raportowania do PSG oraz dostarczania informacji niezbędnych do prawidłowej jego obsługi,

   2) aktywnego uczestniczenia w procesie obsługi Incydentu w zakresie wymaganym przez PSG oraz udzielania wsparcia pracownikom PSG zaangażowanym w proces obsługi Incydentów.

3. W każdym wypadku otrzymania wiadomości o Incydencie (niezależnie od źródła pochodzenia tych informacji), Wykonawca ma obowiązek niezwłocznego podjęcia skutecznych działań mających na celu zapewnienie bezpieczeństwa urządzeń Wykonawcy wykorzystywanych do świadczenia Usługi.

4. W sytuacji wystąpienia Incydentu Wykonawca na wniosek PSG wyznaczy osobę do bezpośredniej współpracy z PSG i - jeśli zajdzie taka konieczność - do ustalenia z PSG harmonogramu postępowania prowadzonego w celu z obsługi Incydentu, minimalizacji skutków oraz zapobiegania wystąpieniom Incydentów w przyszłości. Strony oświadczają jednocześnie, że dołożą najwyższej staranności przy podejmowaniu działań mających na celu szybką i skuteczną obsługę wykrytego Incydentu oraz zapobieganiu wystąpieniu Incydentów w przyszłości.

5. PSG zastrzega sobie prawo do zbierania i zabezpieczania wszelkich dowodów wskazujących na wystąpienie Incydentu i jego skutków. Wykonawca zobowiązany będzie do zbierania i zabezpieczania wszelkich dowodów wskazujących na wystąpienie Incydentu.

§ 5. NADZÓR NAD DZIAŁALNOŚCIĄ WYKONAWCY

1. Wykonawca ma obowiązek informować PSG o stosowanych przez Wykonawcę mechanizmach kontrolnych w zakresie stosowanych zabezpieczeń.

2. Wykonawca jest zobowiązany do przeprowadzania przez niezależny uznany podmiot trzeci (uzgodniony i zaakceptowany przez PSG) regularnych (nie rzadziej niż raz na 12 miesięcy) audytów bezpieczeństwa mających na celu zbadanie zgodności stosowanych zabezpieczeń z uznanymi międzynarodowymi standardami (w tym co najmniej ISO/IEC 27018 oraz ISO/IEC 27001) i niezwłocznego przedstawienia ich wyników PSG.

3. Wykonawca ma obowiązek przeprowadzać regularne, nie rzadziej niż raz na 12 miesięcy, testy bezpieczeństwa systemów oraz infrastruktury Wykonawcy służącej do świadczenia Usługi na rzecz PSG oraz niezwłocznie dostarczyć PSG wyniki z przeprowadzonych testów.

4. W przypadku wystąpienia Incydentu, na żądanie PSG, Wykonawca jest zobowiązany przeprowadzić uzupełniające testy bezpieczeństwa lub audyt uzupełniający w zakresie wskazanym w rekomendacjach z obsługi Incydentu, opracowanych przez PSG i przekazanych Wykonawcy.

5. W sytuacji uzasadnionej okolicznościami, w szczególności w przypadku wystąpienia Incydentu związanego z realizacją Umowy lub w sytuacji, gdy Wykonawca nie dysponuje lub nie przedstawi PSG wyników raportu z audytu bezpieczeństwa przeprowadzonego w trybie ust. 2, PSG zastrzega sobie prawo do przeprowadzenia samodzielnie lub za pośrednictwem wykwalifikowanego podmiotu zewnętrznego, kontroli zastosowanych przez Wykonawcę rozwiązań organizacyjno-techniczno-prawnych, w tym zgodności zaimplementowanych zabezpieczeń z obowiązującym prawem i Umową w zakresie, w jakim jest to niezbędne do oceny jakości usług i zdolności Wykonawcy do świadczenia Usług w sposób należyty i nieprzerwany. Wykonawca zobowiązuje się współpracować z PSG w celu umożliwienia przeprowadzenia ww. kontroli poprzez zapewnienie przedstawicielom PSG dostępu do pomieszczeń, w których świadczone są przez Wykonawcę Usługi oraz do dokumentacji i zasobów teleinformatycznych Wykonawcy związanych ze świadczeniem Usługi. PSG przeprowadzi kontrolę w dni robocze, tj. od poniedziałku do piątku (**Dni Robocze)**) w standardowych godzinach pracy, tj. między 08:00 a 18:00 czasu polskiego, chyba że specyfika pracy będzie wymagała innych godzin, które zostaną uzgodnione z Wykonawcą oraz w sposób najmniej uciążliwy dla działalności gospodarczej Wykonawcy. PSG nie będzie uprawniona do przeprowadzania kontroli obszarów niezwiązanych z przedmiotem Umowy. O terminie kontroli Wykonawca będzie informowany z co najmniej 24 – godzinnym wyprzedzeniem na adres wskazany w § 4.1.1) Powiadomienie będzie określało przedmiot kontroli oraz wskazanie osób upoważnionych do prowadzenia kontroli w imieniu PSG. W przypadku stwierdzenia uchybień w zakresie objętym kontrolą, PSG ma prawo wezwać Wykonawcę do podjęcia działań w celu ich usunięcia w wyznaczonym terminie. Termin będzie uwzględniać poziom krytyczności stwierdzonego uchybienia. Strony ustalają, że uchybienia o charakterze krytycznym, Wykonawca usunie niezwłocznie.

6. Strony ustalają, że niezależnie od postanowień ust. 4, PSG przysługuje prawo do przeprowadzenia testów bezpieczeństwa (testów penetracyjnych) systemów oraz infrastruktury Wykonawcy służącej do przetwarzania Danych. Informację o planowanych testach bezpieczeństwa PSG przekaże Wykonawcy z wyprzedzeniem minimum 2 Dni Roboczych na adres wskazany w § 4.1.1) W przypadku wykrycia przez PSG luki bezpieczeństwa, PSG może zwrócić się do Wykonawcy o podjęcie działań w celu jej usunięcia w wyznaczonym przez PSG terminie.

7. Nieusunięcie przez Wykonawcę uchybień lub luk bezpieczeństwa, o których mowa w ust. 6 powyżej, w wyznaczonym przez PSG terminie może być uznane przez PSG za rażące naruszenie postanowień Umowy i może stanowić podstawę do odstąpienia od Umowy przez PSG.

§ 6. OBOWIĄZKI WYKONAWCY W ZWIĄZKU Z ZAKOŃCZENIEM UMOWY

Wykonawca zapewnia, bez prawa do żądania z tego tytułu jakiegokolwiek wynagrodzenia, iż po zakończeniu obowiązywania Umowy dokona zwrotu na rzecz PSG Danych w formie standardowych formatów ustalonych przez Strony na etapie realizacji Umowy, zaakceptowanych przez PSG.

Zaopiniowano pozytywnie radca prawny

Podpisano przez/ Signed by:
WITOLD
JARZYŃSKI
Data/ Date: 24.11.2026 10:19
mSzafir