Załącznik nr 11 do SIWZ, załącznik nr 9 do umowy, załącznik nr 1 do umowy powierzenia przetwarzania danych osobowych - Wykaz środków organizacyjnych i technicznych stosowanych przez Podmiot przetwarzający

Wykonawca (podmiot przetwarzający) oświadcza, co następuje:

L.p.	ZAKRES	ODPOWIEDŹ
1.	Podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych	TAK
2.	Podmiot przetwarzający jest w stanie wykazać przestrzeganie danych osobowych, m.in. przez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych	TAK
3.	Podmiot przetwarzający zapewnia, że nowo zatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych zostanie odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa	TAK
4.	Podmiot przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników dzięki cyklicznym szkoleniom oraz innym działaniom mającym na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych	TAK
5.	Pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych, zostali zobowiązani do zachowania ich w tajemnicy	TAK
6.	Podmiot przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 Rozporządzenia, lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 Rozporządzenia	TAK
7.	W ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych	TAK
8.	Podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych / podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych	TAK
9.	Podmiot przetwarzający zastosował środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu	TAK
10.	Podmiot przetwarzający zapewnił fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez jego organizację od tych, które należą do innych organizacji	TAK

11.	Dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona) bądź dostęp ten jest szczegółowo nadzorowany	TAK
12.	Każdy pracownik podmiotu przetwarzającego otrzymuje imienny identyfikator do systemów informatycznych	TAK
13.	Systemy informatyczne podmiotu przetwarzającego zapewniają wymuszanie na użytkownikach okresowych zmian haseł oraz zmian w razie zaistniałej potrzeby	TAK
14.	Pracownicy podmiotu przetwarzającego zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów przez blokadę ekranu lub w inny równoważny sposób	TAK
15.	Pracownicy podmiotu przetwarzającego zostali zobowiązani do niezwłocznego odbierania z drukarek wydruków zawierających dane osobowe lub inne poufne informacje. Wskazana zasada jest przestrzegana przez pracowników.	TAK
16.	W organizacji podmiotu przetwarzającego jest stosowana polityka czystego biurka.	TAK
17.	Dane osobowe gromadzone w formie papierowej są przechowywane, po godzinach pracy organizacji podmiotu przetwarzającego, w zamykanych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych.	TAK
18.	Podmiot przetwarzający zapewnił oprogramowanie antywirusowe na wszystkich stacjach.	TAK
19.	Oprogramowanie jest licencjonowane i jest na bieżąco aktualizowane.	TAK
20.	Podmiot przetwarzający stosuje szyfrowanie dysków komputerów przenośnych.	TAK
21.	Urządzenia mobilne mają skonfigurowaną kontrolę dostępu.	TAK
22.	Podmiot przetwarzający stosuje techniki kryptograficzne wobec urządzeń mobilnych.	TAK
23.	Na urządzeniach mobilnych zainstalowano oprogramowanie antywirusowe.	TAK
24.	Zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.	TAK
25.	Przyjęto odpowiedni zakres oraz częstotliwość tworzenia kopii zapasowych do zdefiniowanego ryzyka utraty danych.	TAK
26.	Podmiot przetwarzający posiada procedury odtwarzania systemu po awarii oraz ich testowania.	TAK
27.	Podmiot przetwarzający wdraża nowe rozwiązania zgodnie z zasadą „privacy by design”.	TAK

28.	Podmiot przetwarzający działa zgodnie z zasadą „privacy by default”.	TAK
29.	Podmiot przetwarzający prowadzi ocenę skutków dla ochrony danych.	TAK
30.	Podmiot przetwarzający gwarantuje realizację praw osób, których dane dotyczą, tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym.	TAK
31.	W okresie ostatnich trzech lat pomiot przetwarzający nie przegrał sporów lub postępowań sądowych w sprawie nieodpowiedniej jakości, sposobu wykonania lub zakresu wykonanych przez Państwo zleceń.	TAK
32.	Żaden z pracowników podmiotu przetwarzającego przypisanego do obsługi Zamawiającego nie jest na okresie próbnym.	TAK
33.	Żaden z pracowników podmiotu przetwarzającego przypisanego do obsługi Zamawiającego nie jest w okresie wypowiedzenia.	TAK
34.	Podmiot przetwarzający posiada dedykowany helpdesk - wsparcie użytkowników zewnętrznych.	TAK
35.	Zaimplementowane zostały wewnętrzne regulacje dotyczące bezpieczeństwa informacji.	TAK
36.	Zaimplementowana zostały wewnętrzne regulacje dotyczące bezpieczeństwa systemów informatycznych.	TAK
37.	Zaimplementowana została klasyfikacja informacji.	TAK
38.	Zaimplementowana została politykę bezpieczeństwa danych osobowych oraz instrukcję (instrukcje) zarządzania systemem informatycznym.	TAK
39.	Powołany został Inspektora Ochrony Danych (IOD).	TAK
40.	Pracownicy podmiotu przetwarzającego, przetwarzający dane osobowe, posiadają stosowne do tego upoważnienia i je podpisali.	TAK
41.	Wdrożone zostały wszystkie wymogi unijnego rozporządzenia dotyczącego ochrony danych osobowych (GDPR/RODO).	TAK
42.	W ostatnich trzech latach nie miał miejsce u pomiotu przetwarzającego incydent (incydenty) dotyczący danych osobowych.	TAK
43.	W ostatnich trzech latach przeprowadzony został przynajmniej jeden udokumentowany audyt wewnętrzny zgodności przetwarzania danych osobowych z przepisami prawa.	TAK
44.	W ostatnich trzech latach przeprowadzony został przynajmniej jeden udokumentowany audyt zewnętrzny zgodności przetwarzania danych osobowych z przepisami prawa.	TAK
45.	Budynek podmiotu przetwarzającego objęty jest ciągłym dozorem fizycznym/interwnecyjnym.	TAK
46.	Budynek podmiotu przetwarzającego objęty jest ciągłym monitoringiem wizyjnym.	TAK

47.	Realizowany jest wymóg bezpieczeństwa kodu źródłowego tworzonych modułów i aplikacji.	TAK
48.	Zabezpieczony jest dostęp do kodów źródłowych systemów przez dostępem dla innych podmiotów.	TAK
49.	Kody źródłowe są zabezpieczone przed nieautoryzowaną modyfikacją.	TAK
50.	Kopie zapasowe kodów źródłowych są szyfrowane.	TAK
51.	Dla bezpieczeństwa sieci firmowej są wykorzystywane urządzenia klasy UTM/IPS/IDS/firewalle sprzętowe/antyspamy lub urządzenia typu NAP?	TAK
52.	Prowadzona imienna lista pracowników mających zdalny dostęp do zasobów firmowych z wykazem udostępnionych systemów oraz aplikacji.	TAK
53.	Zaimplementowane są polityki dostępu do sieci firmowej.	TAK
54.	Urządzenia firmowe są monitorowane pod kątem wycieku danych.	TAK
55.	Urządzenia firmowe pracowników na okresie próbnym lub w okresie wypowiedzenia są objęte szczególnymi politykami bezpieczeństwa.	TAK
56.	Używane są szyfrowane połączeń SSL z ważnymi certyfikatami kwalifikowanymi wystawionymi przez zaufane podmioty.	TAK
57.	Systemy operacyjne preinstalowane na wykorzystywanych urządzeniach posiadają aktualne wsparcie producenta.	TAK
58.	Na wykorzystywanych urządzeniach podmiotu przetwarzającego jest zainstalowane oprogramowanie antywirusowe.	TAK
59.	Oprogramowanie antywirusowe automatycznie skanuje podłączony nośnik zewnętrznych przed umożliwieniem jego zasobów.	TAK
60.	Na wykorzystywanych urządzeniach podmiotu przetwarzającego są uruchomione inne aplikacje / usługi monitorujące potencjalne zagrożenia.	TAK
61.	W podmiocie przetwarzającym jest określona lista dopuszczonego oprogramowania do użytkowania.	TAK
62.	Podmiot przetwarzający korzysta z podpisu cyfrowego dla wiadomości elektronicznych.	TAK
63.	Podmiot przetwarzający korzysta z rozwiązań kryptograficznych dla treści bądź załączników wiadomości elektronicznych.	TAK
64.	Zaimplementowana jest procedura zarządzania incydentami.	TAK
65.	Zaimplementowana została procedura informowania klientów o incydencie.	TAK
66.	Zarządzanie incydentami podlega okresowej sprawozdawczości.	TAK

Zamawiający dopuszcza w powyższej tabeli maksymalnie 10 odpowiedzi przeczących (w trzeciej kolumnie wpisane „NIE”).