UMOWA

NR [●]

NA PRZYGOTOWANIE KONCEPCJI I WDROŻENIE ROZWIĄZANIA DO ZARZĄDZANIA UŻYTKOWNIKAMI I UPRAWNIENIAMI DLA HYBRYDOWEJ ARCHITEKTURY SYSTEMÓW SAP W OPARCIU O ROZWIĄZANIA SAP GRC ACCESS CONTROL ORAZ SAP CLOUD IDENTITY ACCESS GOVERNANCE

(dalej jako: „Umowa”)

zawarta w dniu złożenia kwalifikowanego podpisu elektronicznego, o którym mowa w art. 781 kodeksu cywilnego przez osobę reprezentującą Stronę podpisującą jako ostatnia, pomiędzy:

**ORLEN spółka akcyjna** z siedzibą w Płocku przy ul. Chemików 7, 09-411 Płock, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS: 0000028860, której dokumentacja rejestrowa jest przechowywana przez Sąd Rejonowy dla Łodzi-Śródmieścia w Łodzi XX Wydział Gospodarczy – Krajowego Rejestru Sądowego, NIP: 7740001454, REGON: 610188201, BDO: 000007103, o kapitale zakładowym w wysokości   
1 451 177 561,25 zł, opłaconym w całości,

zwaną dalej „**Zamawiającym**” lub „**ORLEN S.A.**”,

reprezentowaną przez:

1. […] – […],

2. […] – […]

oraz

**[•]** z siedzibą w [•] przy [adres], [kod pocztowy] [miejscowość], wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS: [•], której dokumentacja rejestrowa jest przechowywana przez Sąd Rejonowy dla [•], Wydział [•] Gospodarczy Krajowego Rejestru Sądowego, NIP: [•], REGON: [•], o kapitale zakładowym w wysokości [•] zł, *opłaconym w [•],*

zwaną dalej „**Wykonawcą**”,

reprezentowaną przez:

1. […] – […],
2. […] – […]

- zgodnie z informacją odpowiadającą odpisowi aktualnemu z rejestru przedsiębiorców KRS i odpowiednim pełnomocnictwem (jeśli dotyczy) stanowiącym(i) Załącznik nr 7 do Umowy

zwanymi dalej łącznie „**Stronami**” lub każdy z osobna – „**Stroną**”.

**SPIS TREŚCI**

[1. DEFINICJE 3](#_Toc5704534)

[2. PRZEDMIOT UMOWY 9](#_Toc5704535)

[3. PODSTAWOWE ZASADY REALIZACJI UMOWY 10](#_Toc5704536)

[4. WSPÓŁDZIAŁANIE ZAMAWIAJĄCEGO, WYMIAROWANIE INFRASTRUKTURY, SZKOLENIA 13](#_Toc5704537)

[5. ZARZĄDZANIE UMOWĄ 14](#_Toc5704538)

[6. ZARZĄDZANIE PERSONELEM. PODWYKONAWCY 15](#_Toc5704539)

[7. HARMONOGRAM I PRZEBIEG WDROŻENIA 18](#_Toc5704540)

[8. PRAWA WŁASNOŚCI INTELEKTUALNEJ 21](#_Toc5704541)

[9. WYNAGRODZENIE ORAZ ZASADY PŁATNOŚCI 21](#_Toc5704542)

[10. ZARZĄDZANIE ZMIANĄ UMOWY 22](#_Toc5704543)

[11. ZLECENIA 23](#_Toc5704544)

[12. ODPOWIEDZIALNOŚĆ STRON 23](#_Toc5704545)

[13. ODSTĄPIENIE 25](#_Toc5704546)

[14. POSTANOWIENIA KOŃCOWE 28](#_Toc5704547)

# DEFINICJE

## Na potrzeby Umowy Strony uzgadniają definicje wskazane w tabeli poniżej.

## Pojęciom pisanym wielką literą w załącznikach do Umowy (dalej jako: „**Załączniki**”), Strony nadają znaczenie zgodne z definicjami wskazanymi w Umowie, chyba że Załącznik wprost definiuje dane pojęcie inaczej.

|  |  |
| --- | --- |
| **POJĘCIE** | **DEFINICJA** |
| **Akceptacja** | potwierdzenie przez Zamawiającego wykonania Zlecenia zgodnie z Umową i treścią tego Zlecenia. Dowodem dokonania Akceptacji jest odpowiedni Protokół Akceptacji. Zasady i warunki Akceptacji określone są w rozdziale 11. Umowy. |
| **Koncepcja Biznesowa i Techniczna** | Etap I, mający na celu przygotowanie dokumentów koncepcji biznesowej i technicznej Wdrożenia, w tym architektury Systemów przy zachowaniu sposobu realizacji wymagań Zamawiającego określonych w Załączniku nr 1 [**Zakres Wdrożenia**]. |
| **Implementacja Rozwiązania** | Etap II, mający na celu implementację produktów: SAP GRC Access Control oraz SAP Cloud Identity Access Governance Integration Edition, wraz z zakładaną i wypracowaną w Etapie I konfiguracją, zgodnie z zakresem wskazanym w Załączniku nr 1 [**Zakres Wdrożenia**]. |
| **Awaria** | Nieprawidłowość powodująca albo całkowity brak możliwości korzystania z Systemu, albo takie ograniczenie możliwości korzystania z Systemu, że przestaje on spełniać swoje podstawowe funkcje. |
| **Błąd** | Nieprawidłowość powodująca ograniczenie możliwości korzystania z Systemu przy zachowaniu spełniania przez System jego podstawowych funkcji. |
| **Czas Naprawy** | czas między dokonaniem Zgłoszenia a dostarczeniem przez Wykonawcę Naprawy. |
| **Czas Reakcji** | czas między dokonaniem Zgłoszenia a uzyskaniem potwierdzenia przystąpienia do usunięcia Nieprawidłowości przez Wykonawcę. |
| **Dane** | wszelkie informacje przetwarzane w ramach Systemu lub które mogą być dostępne za pośrednictwem Systemu. |
| **Dokument Koncepcji Biznesowej i Technicznej** | Produkt Etapu I, stanowiący zestaw szczegółowej dokumentacji sporządzonej przez Wykonawcę i odebranej przez Zamawiającego, wykonanej w ramach Etapu I, określający docelowe procesy dotyczące zarządzania użytkownikami i sposób ich wsparcia przez narzędzia, a także architekturę systemów wchodzących w skład procesu zarzadzania użytkownikami oraz implementację produktów: SAP GRC Access Control oraz SAP Cloud Identity Access Governance Integration Edition, w tym w szczególności:  (1) opis tworzenia i zarządzania kontami użytkowników w GK ORLEN (IDM);  (2) nadawanie i zmianę uprawnień dla użytkowników;  (3) definiowanie i zmianę ról z uprawnieniami,  (4) kontrolę i przypisanie licencji dla użytkownika,  (5) przeglądy okresowe uprawnień i użytkowników  (6) definicję raportów;  (7) opracowanie uprawnień (opracowanie uprawnień wymaganych do pracy w GRC, dla wszystkich aktorów)  - zgodnie z zakresem wskazanym w Załączniku nr 1 [**Zakres Wdrożenia**]. |
| **Dokumentacja** | łącznie Dokumentacja Projektowa i Dokumentacja Standardowa. Wymagania dotyczące Dokumentacji określone są w Załączniku nr 16 [**Dokumentacja**]. |
| **Dokumentacja Projektowa** | dokumentacja dotycząca prac Wykonawcy w ramach realizacji Umowy, która powstanie bezpośrednio w ramach realizacji Umowy i nie stanowi Dokumentacji Standardowej.  Dokumentacja Projektowa stanowi Utwór Dedykowany. |
| **Dokumentacja Standardowa** | dokumentacja standardowa Wykonawcy, wytworzona przed rozpoczęciem realizacji Umowy, która zostanie przekazana Zamawiającemu w ramach realizacji Umowy.  Dokumentacja Standardowa stanowi Utwór Standardowy. |
| **Dzień Roboczy** | dzień od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy w Polsce. |
| **Etap** | wyodrębniona część realizacyjna Wdrożenia, obejmująca wykonanie określonych Faz lub Produktów lub innych rezultatów prac Wykonawcy objętych Umową. Etapy podlegają Odbiorom. |
| **Faza** | wyodrębniona część realizacyjna Etapu w ramach Wdrożenia, obejmująca wykonanie określonych Produktów lub innych rezultatów prac Wykonawcy objętych Umową. .  Opis i lista Faz stanowią Załącznik nr 1 [**Zakres Wdrożenia**]. |
| **Grupa ORLEN / GK ORLEN** | Zamawiający oraz jego podmioty zależne każdego szczebla oraz podmioty powiązane z Zamawiającym, niezależnie od miejsca siedziby tych podmiotów, przy czym za podmiot zależny (odpowiednio: podmiot powiązany), rozumie się każdy podmiot, który co najmniej według jednej z poniższych ustaw jest spółką/podmiotem/jednostką zależną od Zamawiającego (odpowiednio: spółką/jednostką powiązaną z Zamawiającym): ustawy z dnia ustawy z dnia 15 września 2000 r. Kodeks spółek handlowych, ustawy z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych oraz ustawy z dnia 29 września 1994 r. o rachunkowości. |
| **Harmonogram** | dokument określający kluczowe daty realizacji Wdrożenia, w tym daty zakończenia realizacji poszczególnych Etapów i Faz. Harmonogram stanowi Załącznik nr 2 [**Harmonogram**]. Zmiana Harmonogramu zrealizowana zgodnie z procedurą zarządzania zmianą Umowy opisaną w Rozdziale 10 Umowy nie wymaga zawarcia aneksu w formie pisemnej pod rygorem nieważności. |
| **Infrastruktura** | sprzęt oraz oprogramowanie konieczne do działania Systemu, zapewniane przez Zamawiającego, opisane w Załączniku nr 4 [**Specyfikacja Infrastruktury**]. |
| **Integracja** | integracja Systemu z innymi systemami Zamawiającego. Zakres Integracji oraz podział zadań Stron w ramach Integracji zostanie ustalony przez Strony podczas realizacji Etapu I (Koncepcja Biznesowa i Techniczna) i będzie stanowił załącznik do Dokumentu Koncepcji Biznesowej. Integracja stanowi Produkt. |
| **Kierownik Projektu** | osoba wyznaczona przez Stronę do bieżących kontaktów z drugą Stroną, nadzoru nad realizacją Umowy i innych czynności określonych w Umowie. |
| **Kod Źródłowy** | zestaw plików zawierających nieskompilowany kod oprogramowania stanowiącego Utwór Dedykowany, napisany w języku programowania, wynikającym z przyjętej technologii rozwiązania oraz w formie czytelnej dla człowieka, normalnie używanej dla umożliwienia wprowadzania modyfikacji (w tym również komentarze oraz kody proceduralne, takie jak skrypty w języku opisu prac i skrypty do sterowania kompilacją i instalowaniem), jak również Dokumentacja niezbędna do użycia takiego Kodu Źródłowego.  Wymagania dotyczące Kodu Źródłowego określone są w Załączniku nr 18 [**Kod Źródłowy**]. |
| **Komitet Sterujący** | zespół funkcjonujący w ramach realizacji Umowy, składający się z przedstawicieli Zamawiającego i Wykonawcy, powołany w celu zarządzania realizacją Umowy oraz podejmowania określonych kluczowych decyzji w ramach realizacji Umowy. |
| **Migracja** | migracja Danych do Systemu. Zakres Danych do Migracji oraz podział zadań Stron w ramach Migracji będzie ustalony przez Strony podczas Etapu I (Koncepcja Biznesowa i Techniczna) i będzie stanowił załącznik do Dokumentu Koncepcji Biznesowej. Migracja stanowi Produkt. |
| **Nieprawidłowość** | jakiekolwiek nieprawidłowe działanie Systemu (tj. odstępstwo od zamierzonego działania Systemu) lub jego elementu. Strony rozróżniają następujące kategorie Nieprawidłowości: Awaria, Błąd i Usterka. |
| **Naprawa** | trwałe usunięcie Nieprawidłowości, skutkujące przywróceniem pełnej sprawności Systemu, w tym przywróceniem poprawnego działania Danych, których niepoprawne działanie jest skutkiem tej Nieprawidłowości. |
| **Obejście** | przywrócenie funkcjonowania Systemu poprzez zminimalizowanie uciążliwości Nieprawidłowości i doprowadzenie Systemu do działania zgodnego z wymaganiami wynikającymi z Umowy bez usuwania przyczyny wystąpienia Nieprawidłowości. Obejście nie stanowi Naprawy, jednak pozwala korzystać nieprzerwanie z wszystkich funkcjonalności Systemu. |
| **Odbiór** | potwierdzenie przez Zamawiającego zgodnego z Umową wykonania Etapu lub Wdrożenia (Odbiór Końcowy) w ramach Wdrożenia. Zasady i warunki Odbiorów określone są w Załączniku nr 11 [**Odbiory i wzory Protokołów Odbioru**]. |
| **Odbiór Końcowy** | Odbiór polegający na potwierdzeniu przez Zamawiającego zgodnego z Umową wykonania Wdrożenia. Zasady i warunki Odbiorów określone są w Załączniku nr 11 [**Odbiory i wzory Protokołów Odbioru**]. |
| **Okres Stabilizacji** | okres mający na celu każdorazowo ustabilizowanie działania Systemu w pełnym zakresie, przy użyciu rzeczywistych Danych, przy realizacji rzeczywistych procesów biznesowych Zamawiającego, na środowisku produkcyjnym. |
| **Personel Wykonawcy** | osoby fizyczne oddelegowane przez Wykonawcę do czynności związanych z wykonaniem Umowy, zatrudnione u Wykonawcy na podstawie umowy o pracę lub innej umowy cywilnoprawnej, w tym osoby fizyczne prowadzące jednoosobową działalność gospodarczą stale współpracujące z Wykonawcą. |
| **Personel Kluczowy** | osoby fizyczne będące członkami Personelu Wykonawcy, oddelegowane do realizacji Umowy, których praca (i niezmienność składu) jest istotnym z punktu widzenia Zamawiającego elementem realizacji Umowy. |
| **Podwykonawca** | osoba (podmiot) nienależąca do Personelu Wykonawcy, której Wykonawca powierza wykonanie części swoich zobowiązań wynikających z Umowy. |
| **Prace Dodatkowe** | opcjonalne prace dodatkowe poza zakresem Wdrożenia, w tym w zakresie rozwoju i utrzymania Systemu, a także consultingu, realizowane przez Wykonawcę na rzecz Zamawiającego w okresie trwania Wdrożenia oraz 12 miesięcy od dokonania przez Zamawiającego Odbioru Końcowego na podstawie Zleceń w ramach limitu w wysokości […] (słownie: […]) zł (300 MD). Zakres Prac Dodatkowych zostanie każdorazowo wskazany w Zleceniu.  Prace Dodatkowe obejmują w szczególności:   1. przygotowanie podstawowej matrycy uprawnień bazując na wkładzie merytorycznym z projektu wzorca; 2. zasady rozwoju reguł SOD; 3. narzędzia umożliwiające zarządzanie matrycą uprawnień); 4. integrację z systemami chmurowymi (w tym uruchomienie rozwiązania dla systemów chmurowych); 5. inne prace rozwojowe. |
| **Produkt** | oznaczony rezultat prac Wykonawcy w ramach Fazy (np. dostarczenie wyodrębnionego elementu oprogramowania, konfiguracja Systemu, szkolenia, testy, opracowanie elementu Dokumentacji).  Opis i lista Produktów stanowi Załącznik nr 1 [**Zakres Wdrożenia**]. |
| **Protokół Akceptacji** | dokument stanowiący potwierdzenie dokonania Akceptacji, sporządzony przez Zamawiającego zgodnie ze wzorem stanowiącym Załącznik nr 13 [**Protokół Akceptacji**]. |
| **Protokół Odbioru** | dokument sporządzony przez Zamawiającego, stanowiący potwierdzenie dokonania Odbioru lub Odbioru z zastrzeżeniami, o którym mowa w Załączniku nr 11 [**Odbiory i wzory Protokołów Odbioru**]. |
| **Protokół Rozbieżności** | dokument sporządzony przez Zamawiającego, stanowiący o braku dokonania Odbioru przez Zamawiającego i wskazujący rozbieżności będące przyczyną braku jego dokonania, o którym mowa w Załączniku nr 11 [**Odbiory i wzory Protokołów Odbioru**]. |
| **Roboczodzień (MD)** | 8 godzin pracy członka Personelu Wykonawcy (1 godzina to 60 minut). |
| **Start Produkcyjny Systemu** | każdorazowe uruchomienie Systemu na środowisku produkcyjnym Zamawiającego lub innych spółek z GK ORLEN wskazanych w Umowie lub Koncepcji Biznesowej w pełnym zakresie, w ramach bieżących procesów biznesowych Zamawiającego lub odpowiednio - innych spółek z GK ORLEN wskazanych w Umowie lub Koncepcji Biznesowej i wszystkich funkcjonalności Systemu. |
| **System** | rozwiązania informatyczne do zarzadzania użytkownikami i uprawnieniami dla hybrydowej architektury (opartej o systemy on-premise i cloud) nowo wdrażanych u Zamawiającego systemów SAP w oparciu o rozwiązania SAP GRC Access Control oraz SAP Cloud Identity Access Governance Integration Edition działające we współpracy z Infrastrukturą, spełniające wszystkie wymagania funkcjonalne i pozafunkcjonalne wynikające z Umowy, w tym z Załącznika nr 1 [**Zakres Wdrożenia**] oraz z Dokumentu Koncepcji Biznesowej i Technicznej, z zastrzeżeniem zmian Umowy dokonanych zgodnie z procedurą zarządzania zmianą Umowy opisaną w Rozdziale 10 Umowy.  Systemy stanowią Produkt. |
| **Usterka** | Nieprawidłowość niebędąca ani Awarią ani Błędem. |
| **Utwór** | wszelkie utwory w rozumieniu przepisów ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. 1994 Nr 24, poz. 83, ze zm.).  Utwory dzielą się na Utwory Dedykowane, Utwory Standardowe i Utwory Osób Trzecich. |
| **Utwór Dedykowany** | wszelkie Utwory niestanowiące Utworów Standardowych oraz Utworów Osób Trzecich, wykonane przez Wykonawcę bezpośrednio w ramach realizacji Umowy na rzecz Zamawiającego. |
| **Utwór Standardowy** | Utwory standardowe Wykonawcy, dostarczone przez Wykonawcę w ramach realizacji Umowy Zamawiającemu, do których autorskie prawa majątkowe przysługują Wykonawcy.  Lista Utworów Standardowych stanowi Załącznik nr 22 [**Lista Utworów Standardowych**].  Strony zgodnie potwierdzają, że licencja na korzystanie z Utworów Standardowych w każdym wypadku będzie licencją w modelu enterprise tzn. modelu licencyjnym, który umożliwia ORLEN S.A. udostępnianie Utworów Standardowych spółkom z Grupy ORLEN. |
| **Utwór Osób Trzecich** | Utwory dostarczone przez Wykonawcę w ramach realizacji Umowy Zamawiającemu, do których autorskie prawa majątkowe przysługują osobom trzecim.  Lista Utworów Standardowych stanowi Załącznik nr 23 [**Lista i warunki korzystania z Utworów Osób Trzecich**].  Strony zgodnie potwierdzają, że licencja na korzystanie z Utworów Osób Trzecich w każdym wypadku będzie licencją w modelu enterprise tzn. modelu licencyjnym, który umożliwia ORLEN S.A. udostępnianie Utworów Osób Trzecich spółkom z Grupy ORLEN. |
| **Wdrożenie** | ogół działań realizowanych przez Wykonawcę na podstawie Umowy zgodnie z Załącznikiem nr 1 [**Zakres Wdrożenia**], których rezultatem ma być dzieło w myśl przepisów ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. Nr 16 poz. 93, ze zm. – dalej jako: **Kodeks cywilny**). |
| **Wynagrodzenie za Wdrożenie** | wynagrodzenie netto należne Wykonawcy z tytułu należytej realizacji Wdrożenia. |
| **Wynagrodzenie za Zlecenie** | wynagrodzenie netto należne Wykonawcy z tytułu należytej realizacji Zlecenia. |
| **Zgłoszenie** | poinformowanie Wykonawcy przez Zamawiającego lub inną spółkę z GK ORLEN wskazaną w Umowie lub Koncepcji Biznesowej o wystąpieniu Nieprawidłowości w sposób wskazany w Umowie. |
| **Zlecenie** | zlecenie Prac Dodatkowych przez Zamawiającego Wykonawcy, zgodnie z procedurą określoną w Umowie. Zlecenia podlegają Akceptacji. |

# PRZEDMIOT UMOWY

## Przedmiotem Umowy jest:

### realizacja przez Wykonawcę Wdrożenia, zgodnie z zakresem wskazanym w Załączniku nr 1 [**Zakres Wdrożenia**] oraz w Dokumencie Koncepcji Biznesowej i Technicznej;

### określenie procedury realizacji oraz Akceptacji Zleceń;

### wykonanie innych świadczeń Wykonawcy opisanych w Umowie.

## W ramach Wdrożenia Wykonawca w szczególności:

### w ramach Etapu I (Koncepcja Biznesowa i Techniczna) opracuje Dokument Koncepcji Biznesowej i Technicznej;

### określi zapotrzebowania na instalację, oraz konfigurację środowisk dla systemów produkcyjnych, oraz nieprodukcyjnych (nie więcej niż 3);

### dostarczy, zainstaluje, skonfiguruje oraz sparametryzuje w pełni funkcjonalny System spełniający wymagania opisane w Umowie, w tym w Załączniku nr 1 [**Zakres Wdrożenia**] oraz w Dokumencie Koncepcji Biznesowej i Technicznej;

### przetestuje w pełni funkcjonalny System, zgodnie ze szczegółowymi wymogami określonymi w Umowie oraz w Dokumencie Koncepcji Biznesowej i Technicznej;

### opracuje i przekaże Zamawiającemu Kody Źródłowe oraz Dokumentację;

### przygotuje i przeprowadzi szkolenia, o których mowa w pkt. 4.7. poniżej;

### przeniesie autorskie prawa majątkowe do Utworów Dedykowanych oraz przeniesie wyłączne prawo zezwalania na wykonywanie autorskich praw zależnych do opracowań Utworów Dedykowanych (tj. do rozporządzania i korzystania z takich opracowań) na warunkach określonych w Umowie;

### udzieli Zamawiającemu licencji na korzystanie z Utworów Standardowych na warunkach określonych w Umowie;

### zapewni udzielenie licencji na korzystanie z Utworów Osób Trzecich na rzecz Zamawiającego na warunkach określonych w Umowie;

### wykona inne obowiązki oraz świadczenia opisane w Umowie.

# PODSTAWOWE ZASADY REALIZACJI UMOWY

## **[Wymagana staranność]**

## Wykonawca zobowiązuje się wykonać przedmiot Umowy z zachowaniem najwyższej profesjonalnej staranności właściwej dla czołowych firm branży IT, z uwzględnieniem światowych standardów profesjonalnej obsługi projektów dot. systemów informatycznych, przy wykorzystaniu całej posiadanej wiedzy i doświadczenia.

## **[Oświadczenia i zapewnienia Wykonawcy]**

## Wykonawca oświadcza, że:

### posiada wszelkie wymagane uprawnienia (w tym prawa własności intelektualnej) by zawrzeć i należycie wykonać Umowę;

### zawarcie przez niego Umowy oraz jej wykonanie nie narusza norm prawa, praw jakichkolwiek osób trzecich, ani też nie uniemożliwia lub istotnie nie utrudnia wykonania jakiegokolwiek zobowiązania zaciągniętego przez Wykonawcę;

### nie jest w stanie upadłości i nie zachodzą przesłanki do zgłoszenia wniosku o jego upadłość.

## Wykonawca zapewnia, iż System będzie rozwiązaniem:

### zabezpieczającym integralność, poufność oraz bezpieczeństwo Danych oraz zabezpieczonym przed nieautoryzowanym dostępem osób trzecich;

### skalowalnym oraz zintegrowanym z innymi systemami Zamawiającego oraz spółek GK ORLEN wskazanych w Umowie lub Koncepcji Biznesowej i Technicznej;

### umożliwiającym integrację z innymi rozwiązaniami informatycznymi osób trzecich;

### zapewniającym możliwość dalszego rozwoju Systemu samodzielnie przez Zamawiającego, inne spółki GK ORLEN wskazane w Umowie lub Koncepcji Biznesowej i Technicznej lub osoby trzecie

- w zakresie określonym w Umowie, w szczególności w Załączniku nr 1 [**Zakres Wdrożenia**].

## **[Zgodność z przepisami prawa]**

## Wykonawca gwarantuje, że realizacja Umowy będzie zgodna z przepisami prawa obowiązującymi w Polsce.

## Wykonawca zobowiązuje się do zapewnienia zgodności Systemu z przepisami prawa obowiązującymi w Polsce, przy czym taka ocena zgodności Systemu z przepisami prawa będzie dokonywana na dzień Startu Produkcyjnego Systemu, z zastrzeżeniem, że w razie zmiany przepisów prawa, z których będzie wynikać potrzeba dokonania zmian w Systemie celem zapewnienia ww. zgodności:

## przed dniem dokonania Odbioru Dokumentu Koncepcji Biznesowej i Technicznej – Wykonawca jest zobowiązany do wprowadzenia tych zmian w ramach Wynagrodzenia za Wdrożenie;

## po dniu dokonania Odbioru Dokumentu Koncepcji Biznesowej i Technicznej – Wykonawca jest zobowiązany do wprowadzenia tych zmian w ramach Zlecenia, o ile Strony uzgodnią potrzebę dokonania takich zmian.

## **[Wpływ Wdrożenia na inne systemy Zamawiającego]**

## Wykonawca zobowiązuje się do realizacji Umowy w sposób niepowodujący zaprzestania lub zakłócenia pracy innych systemów informatycznych Zamawiającego oraz spółek GK ORLEN wskazanych w Umowie lub Koncepcji Biznesowej i Technicznej lub bieżących procesów biznesowych Zamawiającego oraz spółek GK ORLEN wskazanych w Umowie lub Koncepcji Biznesowej i Technicznej, o ile takie zaprzestanie lub zakłócenie pracy innych systemów informatycznych lub bieżących procesów biznesowych Zamawiającego lub spółek GK ORLEN wskazanych w Umowie lub Koncepcji Biznesowej i Technicznej było możliwe do przewidzenia przez Wykonawcę przy uwzględnieniu staranności wymaganej Umową.

## Jeżeli realizacja obowiązków Wykonawcy wynikających z Umowy wymagać będzie wyłączenia lub ograniczenia korzystania z innych komponentów informatycznych Zamawiającego lub spółek GK ORLEN wskazanych w Umowie lub Koncepcji Biznesowej i Technicznej (np. inny system informatyczny), Wykonawca zobowiązuje się do minimalizacji czasu, na jaki konieczne będzie wyłączenie lub ograniczenie pracy takich komponentów. Wszelkie ewentualne wyłączenia komponentów Zamawiającego lub odpowiednio – innych spółek GK ORLEN wskazanych w Umowie lub Koncepcji Biznesowej i Technicznej zostanie uprzednio uzgodnione przez Kierowników Projektu Stron.

## **[Regulacje Zamawiającego]**

## W przypadku, gdy w związku z realizacją Umowy, zaistnieje konieczność dostępu lub przekazania do Wykonawcy danych osobowych, Wykonawca zobowiązany jest do zawarcia z Zamawiającym, przed rozpoczęciem przetwarzania takich danych, odpowiedniej, odrębnej umowy, której przedmiotem będą zasady i warunki ochrony oraz przetwarzania tych danych.Wzór umowy powierzenia przetwarzania danych osobowych stanowi Załącznik nr 23 [**Wzór PPDO**].

## Zasady wykorzystania oprogramowania komputerowego dystrybuowanego na warunkach tzw. licencji otwartych (dalej: „**Oprogramowanie Open Source**”) w ramach realizacji Umowy określa Załącznik nr 5 [**Oprogramowanie Open Source**].

## Wykonawca zobowiązuje się, w ramach realizacji Umowy, do przestrzegania zasad dotyczących:

## komunikacji zewnętrznej;

## ochrony Tajemnicy Przedsiębiorstwa i Tajemnicy Spółki ORLEN S.A.;

## postępowania w zakresie wymiany informacji stanowiących Tajemnicę Spółki ORLEN S.A.;

## polityki sankcyjnej;

## zasad przeciwdziałania korupcji

## - określonych w Załączniku nr 14 [**Regulacje Zamawiającego**].

## Wykonawca zobowiązuje się do przestrzegania w ramach realizacji Umowy wymagań dotyczących bezpieczeństwa aplikacji, stanowiących Załącznik nr 8 [**Wymagania bezpieczeństwa dla aplikacji w ORLEN S.A**].

## Wykonawca jest zobowiązany do podpisania dokumentu wskazanego w pkt. 2.4. Załącznika 20 [**Klauzula Grupy ORLEN**], regulującego współpracę pomiędzy Wykonawcą a podmiotem z Grupy ORLEN w zakresie opisanym Umową.

## **[Lokalizacja]**

## W ramach Wdrożenia i Zleceń prace Wykonawcy standardowo będą realizowane w oparciu o zdalny dostęp, z zastrzeżeniem punktu następnego. W przypadku prowadzenia przez Wykonawcę prac w ramach Wdrożenia lub Zleceń w oparciu o zdalny dostęp ich prowadzenie wymaga spełnienia przez Wykonawcę warunków wskazanych w Załączniku nr 15 [**Zasady bezpieczeństwa teleinformatycznego**]. Wszelkie koszty związane z zapewnieniem po stronie Wykonawcy narzędzi do realizacji prac w oparciu o zdalny dostęp obciążają Wykonawcę.

## Kierownicy Projektu Stron mogą ustalić, że Wykonawca będzie realizował dane prace w ramach Wdrożenia lub Zleceń stacjonarnie w lokalizacjach wskazanych przez Zamawiającego, uzgadniając zakres i czas czynności, które mają zostać wykonane w danej lokalizacji. W takim przypadku Wykonawca zobowiązuje się przestrzegać wewnętrznych regulaminów i zasad dotyczących pracy na terenie lokalizacji wskazanej przez Zamawiającego, o ile Zamawiający przekazał Wykonawcy takie regulaminy i zasady z chwilą rozpoczęcia realizacji świadczeń przez Personel Wykonawcy w lokalizacji wskazanej przez Zamawiającego oraz zgodnie z zasadami obowiązującymi u Zamawiającego w tym zakresie.

**[Postęp prac i komunikacja]**

## Wykonawca zobowiązany jest na bieżąco informować Zamawiającego o wszelkich zagrożeniach związanych z wykonywaniem Umowy, o których wie lub – przy uwzględnieniu staranności wymaganej Umową – powinien wiedzieć, w tym także o okolicznościach leżących po stronie Zamawiającego, które mogą mieć wpływ na jakość, termin bądź zakres prac – niezwłocznie po powzięciu przez Wykonawcę informacji o zaistnieniu takich okoliczności. Informacje te powinny być niezwłocznie przekazywane Kierownikowi Projektu Zamawiającego wraz z propozycjami działań zaradczych.

## Wykonawca zobowiązuje się do informowania Zamawiającego w formie pisemnej lub poprzez wiadomość e-mail wysłaną na adres Kierownika Projektu Zamawiającego o przebiegu realizacji Umowy na żądanie Zamawiającego, przekazane w formie pisemnej lub poprzez wiadomość e-mail wysłaną na adres Kierownika Projektu Wykonawcy.

## Niezależnie od innych postanowień Umowy, Wykonawca zobowiązany będzie do:

### monitorowania zagrożeń dla prawidłowości i terminowości realizacji Umowy oraz realizacji działań zaradczych w tym zakresie;

### zarządzania procesem realizacji Umowy.

## Wszelka komunikacja w ramach Umowy, jak również wszelkie Produkty, w tym Dokumentacja, sporządzane będą w języku polskim, ze wskazaniem, że w zakresie Utworów Standardowych oraz Utworów Osób Trzecich Strony dopuszczają także stosowanie języka angielskiego.

# WSPÓŁDZIAŁANIE ZAMAWIAJĄCEGO, WYMIAROWANIE INFRASTRUKTURY, SZKOLENIA

**[Współdziałanie Zamawiającego]**

## Zamawiający jest świadomy, że realizacja Wdrożenia wymaga jego współdziałania z Wykonawcą. Zakres koniecznego współdziałania jest określony w Załączniku nr 9 [**Zakres współdziałania Zamawiającego**]. Wykonawca oświadcza w stosunku do zakresu współdziałania określonego w powyższym Załączniku, że jest on wystarczający dla realizacji Wdrożenia, za wyjątkiem sytuacji, których Wykonawca nie mógł przewidzieć pomimo dochowania staranności wymaganej Umową.

## Strony mogą dokonać zmian zakresu współdziałania określonego w Załączniku nr 9 [**Zakres współdziałania Zamawiającego**] w trybie określonym w Rozdziale 10 poniżej.

## O ile nic innego nie wynika wprost z Umowy, Dokumentu Koncepcji Biznesowej i Technicznej lub zgodnej decyzji Komitetu Sterującego lub Kierowników Projektu Stron, Wykonawca jest zobowiązany zapewnić wszelkie zasoby, w tym w szczególności narzędzia, środki łączności i oprogramowanie, potrzebne mu do realizacji Umowy.

**[Wymiarowanie Infrastruktury]**

## Wykonawca oświadcza, że przed zawarciem Umowy przedstawił Zamawiającemu do akceptacji specyfikację sprzętu i oprogramowania koniecznych do zakupienia/zainstalowania w ramach Infrastruktury, tak aby zapewniała ona należyte wykonanie Umowy przez Wykonawcę, w tym możliwość realizacji Wdrożenia oraz działania Systemu zgodnie z Umową, w tym Załącznikiem nr 1 [**Zakres Wdrożenia**]. Specyfikacja Infrastruktury określona jest w Załączniku nr 4 [**Specyfikacja Infrastruktury**].

## Specyfikacja, o której mowa powyżej, może być zmieniona w czasie realizacji Etapu I (Koncepcja Biznesowa i Techniczna). Zmiany takie będą dokonywane w ramach procedury „Odstępstw od Umowy”, zgodnie z procedurą opisaną w pkt. 7.5. – 7.8. poniżej.

## Wykonawca zobowiązuje się, że Infrastruktura, nie będzie zwymiarowana nadmiarowo, w sposób gospodarczo lub technologicznie nieuzasadniony.

**[Szkolenia]**

## Wykonawca, w zamian za Wynagrodzenie za Wdrożenie, w terminach i na zasadach określonych przez Strony w ramach realizacji Umowy przeprowadzi szkolenia dla personelu Zamawiającego oraz innych spółek GK ORLEN wskazanych w Umowie lub Koncepcji Biznesowej i Technicznej.

# ZARZĄDZANIE UMOWĄ

## Strony powołują Kierowników Projektu:

### ze strony Zamawiającego: [imię i nazwisko], [telefon], [e-mail];

### ze strony Wykonawcy: [imię i nazwisko], [telefon], [e-mail].

## Strony powołują Komitet Sterujący. W skład Komitetu Sterującego wchodzą:

### ze strony Zamawiającego:

### [imię i nazwisko], [telefon], [e-mail];

### [imię i nazwisko], [telefon], [e-mail];

### [imię i nazwisko], [telefon], [e-mail].

### ze strony Wykonawcy:

### [imię i nazwisko], [telefon], [e-mail];

### [imię i nazwisko], [telefon], [e-mail];

### [imię i nazwisko], [telefon], [e-mail].

## Kompetencje Kierowników Projektów i Komitetu Sterującego oraz procedurę zmiany Kierowników Projektu lub członków Komitetu Sterującego określa Załącznik nr 3 [**Struktura zarządzania Umową**].

# ZARZĄDZANIE PERSONELEM PODWYKONAWCY

**[Personel Wykonawcy]**

## Wykonawca oddeleguje do wykonania Umowy odpowiedni Personel Wykonawcy.

## Wykonawca oświadcza, że w ramach Personelu Wykonawcy dysponuje osobami posiadającymi niezbędną wiedzę i kwalifikacje konieczne do właściwego wykonania Umowy, a w szczególności, że dysponuje osobami o wszystkich profilach kompetencji zawodowych niezbędnych do realizacji Umowy. Wykonawca zobowiązuje się do niedokonywania zmian członków Personelu Wykonawcy bez ważnej przyczyny oraz uzyskania uprzedniej akceptacji takiej zmiany od Kierownika Projektu Zamawiającego, wyrażonej w formie pisemnej lub poprzez wiadomość e-mail wysłaną na adres Kierownika Projektu Wykonawcy pod rygorem nieważności.

## W razie zmiany członka Personelu Wykonawcy w trakcie wykonywania Umowy, zadania wykonywane przez osobę, która została zmieniona, zostaną powierzone osobie posiadającej umiejętności i doświadczenia co najmniej równoważne umiejętnościom i doświadczeniu osoby zmienionej.

## Wykonawca bierze pełną odpowiedzialność za działania i zaniechania osób lub podmiotów zaangażowanych w realizację Umowy po stronie Wykonawcy.

## Bez uszczerbku dla innych postanowień Umowy, zmiana członka Personelu Wykonawcy jest skuteczna z chwilą poinformowania o tym Kierownika Projektu Zamawiającego poprzez wiadomość e-mail wysłaną na adres Kierownika Projektu Zamawiającego.

## Dla uniknięcia wątpliwości Strony ustalają, że w każdym przypadku dokonania zmiany członka Personelu Wykonawcy w trakcie wykonywania Umowy, koszty ewentualnego przeszkolenia nowego członka Personelu Wykonawcy obciążają wyłącznie Wykonawcę.

**[Zmiana członka Personelu Wykonawcy na wniosek Zamawiającego]**

## Kierownik Projektu Zamawiającego ma prawo zwrócić się do Kierownika Projektu Wykonawcy z uzasadnionym wnioskiem o odsunięcie konkretnego członka Personelu Wykonawcy od realizacji Umowy. Odsunięcie takiej osoby od realizacji Umowy nastąpi w terminie 5 Dni Roboczych od otrzymania przez Wykonawcę wniosku Zamawiającego, a w przypadku naruszenia prawa lub warunków Umowy, w szczególności zasad poufności, odsunięcie nastąpi natychmiast.

## W sytuacjach określonych w pkt. 6.7. powyżej Wykonawca niezwłocznie powiadomi Zamawiającego o wyznaczeniu nowego członka Personelu Wykonawcy o kwalifikacjach i doświadczeniu co najmniej równoważnych umiejętnościom i doświadczeniu jego poprzednika. W terminie 5 Dni Roboczych od przedstawienia Zamawiającemu nowego członka Personelu Wykonawcy, Zamawiający ma prawo zgłosić uzasadniony sprzeciw wobec takiego nowego członka Personelu Wykonawcy. Zgłoszenie sprzeciwu oznaczać będzie zobowiązanie Wykonawcy do usunięcia takiej osoby z Personelu Wykonawcy oraz zobowiązanie do niezwłocznego przedstawienia nowego członka Personelu Wykonawcy. W takiej sytuacji zasady opisane w punkcie powyżej stosuje się odpowiednio. Nieprzekazanie Wykonawcy przez Zamawiającego informacji o sprzeciwie w powyższym terminie oznaczać będzie akceptację nowego członka Personelu Wykonawcy.

## **[Personel Kluczowy]**

## Wykonawca, w ramach Personelu Wykonawcy, zobowiązuje się do oddelegowania Personelu Kluczowego do realizacji Umowy, w skład którego wchodzić będą osoby wskazane w Załączniku nr 19 [**Personel Kluczowy**].

## Wykonawca zobowiązuje się do zachowania stałości składu osobowego Personelu Kluczowego. Członkowie Personelu Kluczowego nie mogą być odsunięci od wykonywania przedmiotu Umowy bez uprzedniej zgody Zamawiającego (wyrażonej w formie pisemnej lub poprzez wiadomość e-mail wysłaną na adres Kierownika Projektu Wykonawcy pod rygorem nieważności) na samą zmianę oraz na kandydaturę nowego członka Personelu Kluczowego, z wyjątkiem przypadków, gdy odsunięcie od wykonywania przedmiotu Umowy następuje z przyczyn pozostających poza kontrolą Wykonawcy, takich jak choroba członka Personelu Kluczowego, ustanie stosunku pracy lub innego tytułu zatrudnienia danego członka Personelu Kluczowego lub z powodu innego zdarzenia losowego, uniemożliwiającego członkowi Personelu Kluczowego pełnienie swoich funkcji.

## Również tymczasowa niedostępność członka Personelu Kluczowego wymaga uprzedniej zgody Kierownika Projektu Zamawiającego wyrażonej w trybie wskazanym w pkt. 6.9. powyżej.

## Niezależnie od powyższego, w przypadku niedostępności członka Personelu Kluczowego, Wykonawca, na własny koszt, zobowiązany jest do podjęcia wszelkich działań w celu uniknięcia takiego ryzyka, w tym w szczególności oddelegowania do prac na potrzeby Umowy dodatkowego członka do Personelu Kluczowego. W przypadku powyższym Wykonawca zobowiązany jest zapewnić nowego członka Personelu Kluczowego o porównywalnym doświadczeniu, kompetencjach oraz stażu pracy (lub współpracy) u Wykonawcy nie krótszym niż staż pracy (lub współpracy) zastępowanego członka Personelu Kluczowego.

## Za trwałe odsunięcie członka Personelu Kluczowego od realizacji Umowy (nawet jeśli doszło do oddelegowania nowego członka Personelu Kluczowego) Zamawiający będzie uprawniony do naliczenia Wykonawcy kary umownej, o której mowa w pkt. 12.8.5. poniżej, z wyjątkiem przypadków, gdy odsunięcie od realizacji Umowy wynika z okoliczności, o których mowa w pkt. 6.9. powyżej, albo gdy Kierownik Projektu Zamawiającego wyrazi zgodę na taką zmianę.

## Zamawiający ma prawo w dowolnym momencie zwrócić się do Wykonawcy z wnioskiem o odsunięcie danego członka Personelu Kluczowego od wykonywania Umowy. Wniosek taki składany jest przez Kierownika Projektu Zamawiającego Kierownikowi Projektu Wykonawcy. Po otrzymaniu wniosku o odsunięcie takiej osoby od wykonywania Umowy Kierownik Projektu Wykonawcy w ciągu 3 Dni Roboczych przedstawi Kierownikowi Projektu Zamawiającego do zatwierdzenia propozycję osoby zastępującej taką osobę. Kierownik Projektu Zamawiającego w ciągu 3 Dni Roboczych zaakceptuje proponowanego nowego członka Personelu Kluczowego lub też odmówi jego akceptacji. Odmowa akceptacji nie zostanie dokonana bez uzasadnionych przyczyn. Jeżeli nowy członek Personelu Kluczowego nie zostanie zaakceptowany w pierwszym terminie, powyższa procedura zostanie powtórzona, przy czym od decyzji Kierownika Projektu Zamawiającego zależy to, czy dany członek Personelu Kluczowego może nadal wykonywać Umowę, czy ma zostać odsunięty od wykonywania Umowy mimo braku osoby go zastępującej. W przypadku naruszenia przez danego członka zespołu Personelu Kluczowego opisanych w Umowie zasad poufności lub bezpieczeństwa danych odsunięcie danego członka Personelu Kluczowego nastąpi niezwłocznie.

## W celu uniknięcia wątpliwości Strony stwierdzają, że zmiana członka Personelu Kluczowego oddelegowanego do realizacji Umowy i wynikająca z niej konieczność aktualizacji Załącznika nr 19 [**Personel Kluczowy**] nie wymagają zawarcia odrębnego aneksu w formie pisemnej pod rygorem nieważności.

**[Podwykonawcy]**

## W toku realizacji Umowy Wykonawca jest uprawniony do powierzenia realizacji prac w ramach Umowy Podwykonawcom, przy zachowaniu następujących warunków:

### skorzystanie ze świadczeń Podwykonawcy jest dopuszczalne wyłącznie po uzyskaniu uprzedniej zgody Kierownika Projektu Zamawiającego, udzielonej w formie pisemnej lub poprzez wiadomość e-mail wysłaną na adres Kierownika Projektu Wykonawcy pod rygorem nieważności;

### w każdym wypadku korzystania ze świadczeń Podwykonawcy, niezależnie od wyrażenia zgody przez Kierownika Projektu Zamawiającego, Wykonawca ponosi pełną odpowiedzialność za wykonywanie zobowiązań oraz szkody wyrządzone przez Podwykonawcę w ramach realizacji Umowy oraz przy jej okazji, jak za własne działania lub zaniechania;

### korzystając ze świadczeń Podwykonawcy, Wykonawca nałoży na niego obowiązek przestrzegania wszelkich zasad, reguł i zobowiązań określonych w Umowie, w zakresie w jakim odnosić się one będą do zakresu prac danego Podwykonawcy, pozostając jednocześnie gwarantem ich wykonania oraz przestrzegania przez Podwykonawcę.

# HARMONOGRAM I PRZEBIEG WDROŻENIA

**[Harmonogram]**

## Realizacja Wdrożenia przebiegać będzie, w terminach określonych w Harmonogramie, w następujących Etapach i Fazach:

### Etap I – Koncepcja Biznesowa i Techniczna;

### Etap II – Implementacja Rozwiązania – w tym instalacja narzędzi i konfiguracja Systemów, zgodnie z Koncepcją Biznesową i Techniczną;

### Etap III Wdrożenie pierwszego Systemu, a w jego ramach:

### Faza I – Dostosowanie i konfiguracja,

### Faza II – Konfiguracja workflow i przygotowanie Systemu do testów;

### Faza III – Testy;

### Faza IV – Uruchomienie Systemu (Go-live);

### Faza V – Stabilizacja (2 tygodniowy okres hypercare);

### Faza VI – Dwumiesięczne wsparcie po zakończeniu Fazy V (Stabilizacja);

### Etap IV Wdrożenie drugiego Systemu:

### Faza I – Przegląd i dostosowanie konfiguracji;

### Faza II – Konfiguracja workflow i przygotowanie Systemu do testów

### Faza III – Testy;

### Faza IV – Uruchomienie Systemu (Go-live);

### Faza V – Stabilizacja (2 tygodniowy okres hypercare);

### Faza VI – Dwumiesięczne wsparcie po zakończeniu Fazy v (Stabilizacja);

### Etap V Wdrożenie trzeciego Systemu:

### Faza I – Przegląd i dostosowanie konfiguracji;

### Faza II – Konfiguracja workflow i przygotowanie Systemu do testów;

### Faza III – Testy;

### Faza IV – Uruchomienie Systemu (Go-live);

### Faza V – Stabilizacja (2 tygodniowy okres hypercare);

### Faza VI – Dwumiesięczne wsparcie po zakończeniu Fazy V (Stabilizacja);

### Etap VI Wdrożenie czwartego Systemu (opcjonalny):

### Faza I – Przegląd i dostosowanie konfiguracji;

### Faza II – Konfiguracja workflow i przygotowanie Systemu do testów;

### Faza III – Testy;

### Faza IV – Uruchomienie Systemu (Go-live);

### Faza V– Stabilizacja (2 tygodniowy okres hypercare);

### Faza VI – Dwumiesięczne wsparcie po zakończeniu Fazy V (Stabilizacja).

## Szczegółowy opis Etapów i Faz wskazany został w Załączniku nr 1 [**Zakres Wdrożenia**].

## Zamawiający zastrzega sobie prawo decyzji co do możliwości kolejności rozpoczęcia Etapów IV-VI w zależności od jego potrzeb biznesowych na etapie ustalania Koncepcji Biznesowej i Technicznej.

## Zamawiający zastrzega sobie prawo decyzji co do możliwości przeprowadzenia w ramach Wdrożenia Etapu VI najpóźniej do dokonania Odbioru Etapu V (Etap VI traktowany jest jako opcjonalny w ramach Wdrożenia) – Zamawiający poinformuje Wykonawcę o swojej decyzji co do przeprowadzenia lub nie Etapu VI poprzez wiadomość elektroniczną przesłaną na adres e-mail Kierownika Projektu Wykonawcy.

## Strony nie dopuszczają możliwości rozpoczęcia realizacji prac w ramach Etapu II przed dokonaniem Odbioru Etapu I i Etapu III przed dokonaniem Odbioru Etapu II, chyba że wyrazi na to zgodę Komitet Sterujący w formie co najmniej dokumentowej. Wykonując takie prace poza przypadkiem wskazanym powyżej, Wykonawca działa na swoje ryzyko.

## Strony nie dopuszczają możliwości rozpoczęcia realizacji prac w ramach kolejnej Fazy przed zakończeniem wszystkich czynności do wykonania w ramach Fazy bezpośrednio jej poprzedzającej, chyba że wyrazi na to zgodę Komitet Sterujący w formie pisemnej pod rygorem nieważności. Wykonując takie prace poza przypadkami wskazanymi powyżej, Wykonawca działa na swoje ryzyko.

## W razie zwłoki Wykonawcy w stosunku do terminów realizacji Wdrożenia wynikających z Harmonogramu, Wykonawca będzie zobowiązany do wykonywania wszelkich dodatkowych prac koniecznych z uwagi na zaistnienie takiego przekroczenia, które okażą się niezbędne do pełnej realizacji Umowy, bez prawa do dodatkowego wynagrodzenia z tego tytułu. Powyższe nie uchybia uprawnieniom Zamawiającego wynikającym z Rozdziałów 12 i 13 poniżej.

**[Faza IV – Uruchomienie Systemu]**

## Rezultatem Fazy IV (Uruchomienie Systemu) będzie System prawidłowo funkcjonujący w środowisku produkcyjnym Zamawiającego (po Starcie Produkcyjnym).

## Bez uszczerbku dla innych postanowień Umowy, w ramach realizacji Fazy IV (Uruchomienie Systemu), w szczególności na zasadach określonych w Załączniku nr 1 [**Zakres Wdrożenia**], przeprowadzony zostanie Start Produkcyjny.

## W celu uniknięcia wątpliwości, uprawnienie do wyznaczenia daty Startu Produkcyjnego jest wyłącznym uprawnieniem Zamawiającego. Data Startu Produkcyjnego nie może być jednak wyznaczona na datę wcześniejszą niż data wskazana w Harmonogramie, a Wykonawca jest zobowiązany do wykonania Systemu i przygotowania go do Startu Produkcyjnego do dnia wskazanego w Harmonogramie. W przypadku braku opóźnień Zamawiający wyznaczy datę Startu Produkcyjnego na dzień wskazany w Harmonogramie.

**[Faza V – Stabilizacja]**

## Z chwilą zakończenia Fazy IV (Uruchomienie Systemu) rozpoczyna się każdorazowo Faza V (Stabilizacja).

## Okres Stabilizacji ma każdorazowo na celu ustabilizowanie Systemu, przy użyciu rzeczywistych Danych, przy realizacji rzeczywistych procesów biznesowych Zamawiającego.

## Bez uszczerbku dla innych postanowień Umowy, w szczególności określonych w Załączniku nr 1 [**Zakres Wdrożenia**], Wykonawca, w ramach Wynagrodzenia za Wdrożenie, będzie obsługiwał Nieprawidłowości pojawiające się w Okresie Stabilizacji na zasadach zawartych w Załączniku nr 6 [**Obsługa Nieprawidłowości**]. Zamawiający jest uprawniony do zgłaszania Nieprawidłowości do ostatniego dnia trwania Okresu Stabilizacji, także w okresie jego przedłużenia, zgodnie z postanowieniami poniżej.

## W razie dokonania zmian w Systemie w ramach Okresu Stabilizacji, Wykonawca niezwłocznie opracuje i przekaże Zamawiającemu odpowiednio zmienioną Dokumentację. Brak dostarczenia zaktualizowanej Dokumentacji uprawnia do odmowy dokonania Etapu, w ramach którego nie została przekazana.

## Okres Stabilizacji trwa 2 tygodnie od Odbioru Fazy IV (Uruchomienie Systemu),

## Po zakończeniu Okresu Stabilizacji rozpoczyna się Faza VI, w ramach której Wykonawca udzieli Zamawiającemu 2-mieisęcznego wsparcia (liczone od zakończenia Fazy V) w związku z Systemem, którego dotyczy dany Etap na zasadach wskazanych w Umowie.

## Odbiór ostatniego Etapu w ramach Wdrożenia stanowi Odbiór Końcowy.

# PRAWA WŁASNOŚCI INTELEKTUALNEJ

## W zamian za Wynagrodzenie za Wdrożenie oraz Wynagrodzenie za Zlecenie, Wykonawca:

### przeniesie na rzecz Zamawiającego autorskie prawa majątkowe do Utworów Dedykowanych oraz przeniesie wyłączne prawo zezwalania na wykonywanie autorskich praw zależnych do opracowań Utworów Dedykowanych (tj. do rozporządzania i korzystania z takich opracowań);

### udzieli Zamawiającemu licencji na Utwory Standardowe; oraz

### dokona pozostałych rozporządzeń w zakresie własności intelektualnej

### - na warunkach określonych w Załączniku nr 17 [**Prawa własności intelektualnej**].

**[Kod Źródłowy]**

## Bez uszczerbku dla innych postanowień Umowy, warunkiem Odbioru Etapu jest każdorazowo przekazanie przez Wykonawcę Zamawiającemu Kodów Źródłowych, spełniających warunki określone w Załączniku nr 18 [**Kod Źródłowy**], aktualnych na dzień Odbioru Etapu. Kody Źródłowe będą przekazywane w formie [#].

## W razie dokonania zmian w Systemie w ramach któregokolwiek Okresu Stabilizacji, Wykonawca każdorazowo niezwłocznie opracuje i przekaże Zamawiającemu odpowiednio zmieniony Kod Źródłowy, spełniający warunki określone w Załączniku nr 18 [**Kod Źródłowy**], w formie [#]. Brak dostarczenia zaktualizowanego Kodu Źródłowego uprawnia do odmowy dokonania Odbioru Etapu w ramach którego jest realizowany ten Okres Stabilizacji.

# WYNAGRODZENIE ORAZ ZASADY PŁATNOŚCI

## Z tytułu realizacji Umowy Zamawiający zapłaci Wykonawcy Wynagrodzenie za Wdrożenie i Wynagrodzenie za Zlecenie opisane Załącznikiem nr 10 [**Wynagrodzenie i zasady płatności**], na zasadach opisanych w tym Załączniku.

## Wynagrodzenie za Wdrożenie i Wynagrodzenie za Zlecenie o którym mowa powyżej, obejmować będzie w szczególności wynagrodzenie za:

## przeniesienie przez Wykonawcę na Zamawiającego autorskich praw majątkowych do Utworów Dedykowanych oraz

## przeniesienie przez Wykonawcę na Zamawiającego wyłącznego prawa zezwalania na wykonywanie autorskich praw zależnych do opracowań Utworów Dedykowanych

## - na wszystkich polach eksploatacji wskazanych w Załączniku nr 17 [**Prawa własności intelektualnej**].

## udzielenie Zamawiającemu przez Wykonawcę licencji na korzystanie z Utworów Standardowych Utwory

## - na wszystkich polach eksploatacji wskazanych w Załączniku nr 17 [**Prawa własności intelektualnej**]; a także

## **9.2.4.** zapewnienie udzielenia Zamawiającemu przez Wykonawcę licencji na korzystanie z Utworów Osób Trzecich na warunkach określonych przez Strony.

## Wykonawca nie otrzyma odrębnego wynagrodzenia za prace wykonane po odmowie dokonania Odbioru Fazy, Etapu lub Wdrożenia przez Zamawiającego, polegające na doprowadzeniu rezultatów odpowiednio – Fazy, Etapu lub Wdrożenia do zgodności z treścią Umowy.

## Działając na podstawie art. 4c ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych, Zamawiający oświadcza, że posiada status dużego przedsiębiorcy.

# ZARZĄDZANIE ZMIANĄ UMOWY

## Bez uszczerbku dla innych postanowień Umowy, Strony ustalają możliwość zmiany Umowy bez wymogu zachowania formy pisemnej pod rygorem nieważności, na zasadach i w granicach oznaczonych w niniejszym Rozdziale.

## Komitet Sterujący, na wniosek Kierownika Projektu jednej ze Stron, może postanowić o dokonaniu zmiany:

### terminu wynikającego z Harmonogramu;

### zakresu przedmiotowego Umowy, w tym wynikającego z Dokumentu Koncepcji Biznesowej i Technicznej. Zmiana taka może polegać w szczególności na wyłączeniu danego Systemu z zakresu Wdrożenia, zastąpieniu go innym lub rozszerzeniem zakresu Umowy o nowe Produkty lub inne świadczenia, a także dokonaniu zmian w Systemie wynikających ze zmiany przepisów prawa obowiązujących w Polsce po dokonaniu Odbioru Dokumentu Koncepcji Biznesowej i Technicznej. Strony zgodnie potwierdzają, że wszelkie zmiany (zarówno poszczególne zmiany, jak i wszystkie zmiany łącznie), o których mowa w niniejszym punkcie nie mogą prowadzić do takiego podwyższenia Wynagrodzenia za Wdrożenie, które skutkowałoby przekroczeniem maksymalnej wartości Umowy, wskazanej w pkt. 2.1. Załącznika nr 10 [**Wynagrodzenie i zasady płatności**];

### zasad wykonywania Umowy.

## Kierownik Projektu, wnioskując o dokonanie przez Komitet Sterujący zmiany, o której mowa powyżej, jest zobowiązany przedstawić w formie pisemnej lub wiadomości e-mail uzasadnienie takiej zmiany – w ciągu 5 Dni Roboczych od dnia złożenia wniosku. Uzasadnienie to powinno w szczególności przedstawiać przyczyny potrzeby zmiany, cel zmiany oraz jej wpływ na inne aspekty Umowy – zwłaszcza odnośnie Wynagrodzenia, Harmonogramu i zakresu współdziałania Zamawiającego.

## Posiedzenie Komitetu Sterującego, na którym zostanie podjęta decyzja o zmianie, o której mowa powyżej, zostanie zorganizowane w ciągu 7 Dni Roboczych od dnia złożenia wniosku przez Kierownika Projektu, chyba że wcześniej zostało ono wyznaczone w dacie poprzedzającej upływ tego terminu – wówczas wniosek ten zostanie rozpatrzony na tym posiedzeniu. Posiedzenie nie będzie zwoływane również, jeśli Komitet Sterujący podejmie decyzję w sposób określony w pkt. 2.14. Załącznika nr 3 [**Struktura zarządzania Umową**].

**[Prace związane ze zmianami zakresu Wdrożenia]**

## W przypadku zmiany Umowy zgodnie z postanowieniami powyższymi, która wiąże się z koniecznością wykonania przez Wykonawcę prac związanych ze zmianą zakresu Wdrożenia prace te zostaną wykonane przez Wykonawcę na podstawie Zlecenia na Prace Dodatkowe, a wynagrodzenie Wykonawcy z tytułu wykonywania tych prac zostanie obliczone w oparciu o stawki określone w Załączniku nr 10 [**Wynagrodzenie i zasady płatności**].

# ZLECENIA

**[Procedura zawierania Zlecenia]**

## Zamawiający może zamawiać na podstawie Zleceń wykonanie Prac Dodatkowych w ramach limitu w wysokości […] (słownie: […]) zł (300 MD) w całym okresie obowiązywania Umowy (tj. od momentu zawarcia Umowy do momentu upływu 12 miesięcy od dnia dokonania Odbioru Końcowego) w drodze uzgodnień między Kierownikami Projektu, dokonywanych w formie wiadomości e-mail, przesyłanych między Kierownikami Projektu.

## Zlecenie będzie każdorazowo wskazywało: (i) przedmiot Prac Dodatkowych, (ii) kwotę Wynagrodzenia za Zlecenie obliczoną zgodnie z Załącznikiem nr 10 [**Wynagrodzenie i zasady płatności**] oraz (iii) termin przedstawienia Zlecenia do Akceptacji.

## Bez uszczerbku dla postanowienia określonego w pkt. 11.1. i 11.2. powyżej, Zlecenie, w terminie 14 dni od jego zawarcia, zostanie każdorazowo potwierdzone przez Kierowników Projektu Stron w formie pisemnej pod rygorem nieważności.

## Zasady obliczania Wynagrodzenia za Zlecenie wskazane zostały w Załączniku nr 10 [**Wynagrodzenie i zasady płatności**]

## Strony oświadczają, że wyłączają pomiędzy nimi, w zakresie dotyczącym Zlecenia, stosowanie art. 68, art. 681, art. 682 oraz art. 69 Kodeksu cywilnego

## W celu uniknięcia wątpliwości Strony potwierdzają, że z Umowy nie wynika dla Wykonawcy żadne roszczenie o zawarcie jakiejkolwiek Zlecenia (Zamawiający nie jest zobowiązany do zawierania Zleceń)

**[Procedura Akceptacji Zlecenia]**

## Wykonanie prac Wykonawcy w ramach Zleceń będzie potwierdzone przez podpisanie przez osobę upoważnioną po stronie Zamawiającego Protokołu Akceptacji. Szczegółowe warunki i procedura Akceptacji Zlecenia będą określone w danym Zleceniu.

## Za datę Akceptacji uważa się datę podpisania odpowiedniego Protokołu Akceptacji, chyba że inna data została wskazana w samym Protokole Akceptacji

## Bez uszczerbku dla innych postanowień Umowy, warunkiem Akceptacji Zlecenia jest każdorazowo przekazanie przez Wykonawcę Zamawiającemu Dokumentacji dotyczącej tego Zlecenia, aktualnej na dzień Akceptacji.

## Wykonawca dokona zgłoszenia gotowości Zlecenia do Akceptacji w terminie wskazanym w tym Zleceniu, a jeśli brak takiego terminu – w terminie wskazanym przez Kierownika Projektu Zamawiającego. Wraz ze zgłoszeniem gotowości Zlecenia do Akceptacji Wykonawca przedstawi Zamawiającemu zestawienie prac dot. takiego Zlecenia. Bez uszczerbku dla innych postanowień Umowy, warunkiem dokonania Akceptacji jest każdorazowo zaakceptowanie przez Zamawiającego zestawienia prac.

# ODPOWIEDZIALNOŚĆ STRON

**[Postanowienia ogólne]**

## Wykonawca ponosi odpowiedzialność za niewykonanie lub nienależyte wykonanie Umowy poprzez zapłatę kar umownych lub na zasadach ogólnych opisanych w przepisach powszechnie obowiązującego prawa.

## Z zastrzeżeniem odmiennych postanowień Umowy, całkowity łączny rozmiar odpowiedzialności każdej ze Stron z tytułu szkód wyrządzonych drugiej Stronie w związku z Umową jest ograniczony do kwoty równej 100 % kwoty wskazanej w pkt. 2.1. Załącznika nr 10 [**Wynagrodzenie i zasady płatności**].

## Jakiekolwiek ograniczenia odpowiedzialności Wykonawcy, w tym w szczególności określone w pkt.12.2 powyżej nie odnoszą się do:

### szkód wyrządzonych umyślnie lub w wyniku rażącego niedbalstwa;

### szkód wynikających z naruszenia przez Wykonawcę jakiegokolwiek zobowiązania określonego w Załączniku nr 14 [**Regulacje Zamawiającego**];

### szkód wynikających z naruszenia przez Wykonawcę zobowiązań określonych w Załączniku nr 15 [**Zasady bezpieczeństwa teleinformatycznego**];

### szkód wynikających z naruszenia przez Wykonawcę jakiejkolwiek zasady ochrony lub przetwarzania danych osobowych wynikającej z przepisów prawa, Umowy lub umowy o powierzeniu przetwarzania danych osobowych zawartej przez Strony;

### szkód wynikających z wad prawnych dostarczonych Utworów lub ich poszczególnych elementów, a w szczególności w związku z roszczeniami osób trzecich podniesionymi w związku z naruszeniem przez Zamawiającego lub podmioty z Grupy ORLEN ich praw własności intelektualnej.

**[Kary umowne – zasady ogólne]**

## Kary umowne są niezależne od siebie i należą się w pełnej wysokości, nawet w przypadku, gdy z powodu jednego zdarzenia naliczona jest więcej niż jedna kara umowna.

## Kary umowne przewidziane Umową płatne będą w terminie 14 dni od daty doręczenia Wykonawcy pisemnego wezwania do zapłaty.

## Naliczenie kar umownych Wykonawcy nie wyłącza możliwości dochodzenia przez Zamawiającego odszkodowania na zasadach ogólnych, do pełnej wysokości poniesionej szkody. Zasada powyższa dotyczy wszystkich kar umownych zastrzeżonych w Umowie na rzecz Zamawiającego.

## W zakresie kar umownych przewidzianych w pkt. 12.8.2. poniżej, odpowiedzialność za opóźnienie oznacza przyjęcie przez Wykonawcę odpowiedzialności za przekroczenie terminu na zasadzie ryzyka, od której może się uwolnić wyłącznie wykazując, że opóźnienie nastąpiło z przyczyn, za które odpowiedzialność ponosi Zamawiający lub że było spowodowane przyczynami o charakterze siły wyższej. W przypadku kar umownych, które przewidują odpowiedzialność za zwłokę, odpowiedzialność za zwłokę oznacza przyjęcie przez Wykonawcę odpowiedzialności za przekroczenie terminu na zasadzie winy.

**[Kary umowne – przesłanki]**

## Zamawiający jest uprawiony do naliczenia Wykonawcy kar umownych w przypadku:

* + 1. zwłoki w dostarczeniu przez Wykonawcę prawidłowo wykonanego Etapu do Odbioru –w wysokości 0,005% Wynagrodzenia za Wdrożenie za każdy rozpoczęty dzień zwłoki;

### przekroczenia Czasu Naprawy w ramach Okresu Stabilizacji:

### dla Awarii – w wysokości 2000 zł za każdą rozpoczętą godzinę opóźnienia;

### dla Błędu – w wysokości 300zł za każdą rozpoczętą godzinę opóźnienia;

### dla Usterki – w wysokości 200 zł za każdą rozpoczętą godzinę opóźnienia;

### dopuszczenia do realizacji Wdrożenia Podwykonawcy bez zgody Zamawiającego, o której mowa w pkt 6.16.1 – w wysokości 50.000,00 zł za każdy przypadek naruszenia;

### odstąpienia przez Zamawiającego od Umowy z przyczyn leżących po stronie Wykonawcy – w wysokości 20% Wynagrodzenia za Wdrożenie;

### trwałego odsunięcia członka Personelu Kluczowego od realizacji Umowy bez uprzedniego uzgodnienia z Zamawiającym – w wysokości 50.000,00 zł za każdy przypadek naruszenia;

### zwłoki w przedstawieniu prawidłowo wykonanego Zlecenia do Akceptacji, w terminie wynikającym każdorazowo z tego Zlecenia – w wysokości 0,1 % Wynagrodzenia za Zlecenie za każdy rozpoczęty dzień zwłoki (podstawą obliczenia wysokości kary umownej jest maksymalna wartość Wynagrodzenia za Zlecenie, wskazana w tym Zleceniu);

### innych przypadkach określonych w Umowie, w tym w Załącznikach.

# ODSTĄPIENIE

**[Odstąpienie przez Wykonawcę]**

## Jeżeli Zamawiający odmówi współdziałania przewidzianego postanowieniami Umowy koniecznego do wykonania Umowy, Wykonawca wezwie Zamawiającego, w formie pisemnej pod rygorem nieważności, do odpowiedniego współdziałania, opisując zakres braku współdziałania i wskazując, w jakim zakresie brak współdziałania uniemożliwia dokończenie Umowy, określając zakres działań, których wymaga i wyznaczając odpowiedni termin, nie krótszy niż 30 dni do zapewnienia takiego współdziałania. Po bezskutecznym upływie tego terminu, Wykonawca wyznaczy dodatkowy termin, w formie pisemnej pod rygorem nieważności, nie krótszy niż 30 dni, z zastrzeżeniem, iż po jego upływie Wykonawca będzie uprawniony do odstąpienia od Umowy. Po upływie tego dodatkowego terminu Wykonawca ma prawo do odstąpienia od Umowy. Niniejsza klauzula stanowi modyfikację przepisu art. 640 Kodeksu cywilnego, w możliwie najszerszym zakresie w jakim jest to dopuszczalne.

## Jeżeli – w zakresie wynagrodzenia z tytułu realizacji Umowy – Zamawiający pozostaje w zwłoce przekraczającej 30 dni, Wykonawca wezwie Zamawiającego, w formie pisemnej pod rygorem bezskuteczności wezwania, do zapłaty zaległych kwot w terminie nie krótszym niż 30 dni od daty otrzymania takiego wezwania. Po upływie tego dodatkowego terminu Wykonawca ma prawo do odstąpienia od Umowy. Intencją Stron jest dokonanie niniejszym postanowieniem modyfikacji przepisów Kodeksu cywilnego dotyczących odstąpienia od umowy w razie zwłoki dłużnika w najdalszym dopuszczalnym przez przepisy powszechnie obowiązującego prawa zakresie. W celu uniknięcia wątpliwości Strony potwierdzają, że powyższe uprawnienie do odstąpienia nie przysługuje Wykonawcy w sytuacji, gdy Zamawiający złożył oświadczenie o potrąceniu roszczenia Wykonawcy o zapłatę Wynagrodzenia z własnymi roszczeniami względem Wykonawcy, np. roszczeniami o zapłatę kar umownych.

**[Odstąpienie przez Zamawiającego]**

## Zamawiający będzie miał umowne prawo odstąpienia od Umowy z winy Wykonawcy w przypadku:

### niewykonania lub nienależytego wykonania Etapu I (Koncepcja Biznesowa i Techniczna);

### zwłoki w przedstawieniu przez Wykonawcę prawidłowo zrealizowanego Etapu do Odbioru o co najmniej 30 dni, pod warunkiem uprzedniego wezwania do przedstawienia prawidłowo zrealizowanego Etapu do Odbioru w dodatkowym terminie 14 dni, po bezskutecznym upływie tego terminu;

### dostarczenia Zamawiającemu jakiegokolwiek Utworu obarczonego wadą prawną;

### naruszenia przez Wykonawcę jakiejkolwiek zasady ochrony lub przetwarzania danych osobowych wynikającej z przepisów prawa, Umowy lub umowy o powierzeniu przetwarzania danych osobowych zawartej przez Strony;

### dopuszczenia do realizacji Wdrożenia Podwykonawcy bez zgody Zamawiającego;

## Wykonawca naruszył jakiekolwiek zobowiązanie określone w Załączniku nr 14 [**Regulacje Zamawiającego**];

### naruszenia przez Wykonawcę jakiejkolwiek zasady dotyczącej bezpieczeństwa teleinformatycznego;

### dostarczenia przez Wykonawcę jakiegokolwiek oprogramowania niespełniającego jakiegokolwiek z wymagań bezpieczeństwa dla aplikacji, określonych w Załączniku nr 8 [**Wymagania bezpieczeństwa dla aplikacji w ORLEN S.A.**].

## Niezależnie od powyższego, Zamawiający ma prawo do odstąpienia od Umowy w terminie 30 dni od dnia dokonania Odbioru Etapu I (Koncepcja Biznesowa i Techniczna) nawet w przypadku prawidłowej realizacji Umowy (umowne prawo odstąpienia).

**[Skutki odstąpienia]**

## W razie odstąpienia od Umowy przez Zamawiającego na podstawie pkt. 13.3. powyżej:

### Zamawiający poinformuje Wykonawcę w oświadczeniu o odstąpieniu od Umowy czy chce zachować jakiekolwiek rezultaty dostarczone mu w ramach realizacji Umowy, a jeśli tak – to które i w jakim zakresie. Brak takiej informacji oznacza, iż Zamawiający nie chce zachować żadnych rezultatów prac Wykonawcy.

### Jeżeli Zamawiający nie zachowuje jakichkolwiek rezultatów prac Wykonawcy:

### Zamawiający zwróci Wykonawcy wszelkie odebrane dotychczas Produkty lub rezultaty pracy Wykonawcy lub dokona ich zniszczenia lub usunięcia w taki sposób, aby nie było możliwe produkcyjne korzystanie z nich. Zamawiający ma prawo zachowania pojedynczych egzemplarzy lub kopii tych rezultatów lub Produktów na potrzeby ewentualnego postępowania sądowego – do czasu upływu okresu przedawnienia roszczeń Stron, bez prawa produkcyjnego wykorzystania tak zachowanych egzemplarzy lub kopii;

### Wykonawca zwróci otrzymane wynagrodzenie w terminie 14 dni od daty otrzymania oświadczenia Zamawiającego o odstąpieniu od Umowy;

### Wykonawca zobowiązuje się do niepodnoszenia jakichkolwiek roszczeń w stosunku do Zamawiającego wynikających z używania odebranych przez Zamawiającego rezultatów lub Produktów w okresie od ich odebrania do dnia ich zniszczenia lub zwrotu Wykonawcy lub ww. upływu terminu przedawnienia roszczeń;

### jeżeli Zamawiający zachowuje rezultaty prac Wykonawcy:

### Zamawiający wskaże, w terminie 14 dni od doręczenia Wykonawcy oświadczenia o odstąpieniu od Umowy przez Zamawiającego, które rezultaty (nawet nieukończone) i w jakim zakresie mają dla niego samodzielne znaczenie i chce je zatrzymać;

### Wykonawca zachowa prawo do wynagrodzenia za te rezultaty; wysokość wynagrodzenia zostanie ustalona w oparciu o Wynagrodzenie, a jeżeli będzie to niewystarczające (np. w przypadku niedokończonych Produktów) – w stosunku do nakładu pracy niezbędnej do wykonania tych prac;

### Zamawiający zachowa lub nabędzie wszystkie wskazane rezultaty prac Wykonawcy, w tym zachowa lub odpowiednio nabędzie uprawnienie do korzystania z nich zgodnie z zasadami wyrażonymi w Rozdziale 8 Umowy.

## W razie odstąpienia od Umowy przez Zamawiającego na podstawie pkt. 13.4. powyżej lub przez Wykonawcę na podstawie pkt. 13.1. i 13.2. powyżej, Zamawiający:

### Zamawiający zapłaci Wykonawcy wynagrodzenie za wszystkie wykonane zgodnie z Umową rezultaty prac Wykonawcy, w szczególności wykonane Produkty, wykonane do dnia odstąpienia od Umowy, przy czym wysokość wynagrodzenia zostanie ustalona zgodnie z Umową, a jeżeli będzie to niewystarczające – w stosunku do nakładu pracy niezbędnej do wykonania prac;

### Zamawiający zachowa lub nabędzie wszystkie wskazane rezultaty prac Wykonawcy, w tym zachowa lub odpowiednio nabędzie uprawnienie do korzystania z nich zgodnie z zasadami wyrażonymi w Rozdziale 8 Umowy.

## Bez uszczerbku dla innych postanowień Umowy, wysokość wynagrodzenia Wykonawcy należnego za Fazę, w trakcie realizacji której którakolwiek ze Stron odstąpiła od Umowy, nie może przekroczyć wynagrodzenia za jej realizację, określonego w Załączniku nr 10 [**Wynagrodzenia i zasady płatności**].

**[Oświadczenie o odstąpieniu]**

## Oświadczenie o odstąpieniu wymaga zachowania formy pisemnej pod rygorem nieważności.

## W celu uniknięcia wątpliwości Strony potwierdzają, że jeśli w danym postanowieniu o odstąpieniu wprost nie przewidziały dodatkowego wezwania albo dodatkowego terminu, to oświadczenie o odstąpieniu będzie skuteczne bez ich wyznaczania.

## Poza przypadkiem wskazanym w pkt. 13.4. powyżej, każde ze wskazanych w Umowie umownych praw odstąpienia, może zostać wykonane nie później niż do dnia podpisania przez Zamawiającego Protokołu Odbioru Końcowego Wdrożenia jako całości.

# POSTANOWIENIA KOŃCOWE

## Wszelka korespondencja będzie wysyłana na adresy wskazane przy oznaczeniu Stron. Zmiana adresu nie wymaga zawarcia odrębnego aneksu w formie pisemnej pod rygorem nieważności, lecz poinformowania o tym drugiej Strony w formie pisemnej lub poprzez wiadomość e-mail wysłaną na adres Kierownika Projektu drugiej Strony pod rygorem uznania oświadczenia złożonego na poprzedni adres za doręczone.

## Wykonawca nie ma prawa dokonywać cesji, przeniesienia bądź obciążenia swoich praw lub obowiązków wynikających z Umowy ani w inny sposób dążyć do ich zbycia bez uprzedniej zgody Zamawiającego wyrażonej w formie pisemnej pod rygorem nieważności.

## Zamawiający uprawniony jest do przeniesienia całości albo części praw lub obowiązków wynikających z Umowy na dowolny podmiot z Grupy ORLEN a Wykonawca niniejszym wyraża zgodę na takie przeniesienie praw i/lub obowiązków lub – jeżeli przepis tak stanowi – wyrazi zgodę odrębnym oświadczeniem woli, niezwłocznie po wezwaniu do tego przez Zamawiającego.

## Wszelkie spory pozostające w związku z Umową będą rozwiązywane w drodze wzajemnych uzgodnień Stron. Jeśli rozwiązanie sporu nie zostanie uzgodnione w ciągu 30 dni, spór będzie poddany pod rozstrzygnięcie sądu powszechnego właściwego miejscowo ze względu na siedzibę Zamawiającego.

## W granicach wyznaczonych przez bezwzględnie obowiązujące przepisy prawa, nieważność któregokolwiek z postanowień Umowy, w tym również postanowienia zawartego w Załącznikach, pozostaje bez wpływu na ważność pozostałych postanowień Umowy. W przypadku uznania niektórych postanowień Umowy za nieważne, Strony będą dążyć do zastąpienia nieważnych postanowień postanowieniami wywołującymi taki sam skutek biznesowy.

## Prawem właściwym dla Umowy jest prawo polskie.

## Zmiana Umowy wymaga zachowania formy pisemnej pod rygorem nieważności, z zastrzeżeniem zmian, co do których Umowa wyraźnie przewiduje brak konieczności zawarcia odrębnego aneksu w formie pisemnej pod rygorem nieważności.

## Umowa została sporządzona w jednym elektronicznym egzemplarzu.

## W razie rozbieżności pomiędzy postanowieniami Umowy a postanowieniami Załączników, podstawą wykładni woli Stron będą postanowienia Umowy.

## Załączniki do Umowy stanowią jej integralną część. Lista załączników jest następująca:

## Załącznik nr 1 – Zakres Wdrożenia;

## Załącznik nr 2 – Harmonogram;

## Załącznik nr 3 – Struktura zarządzania Umową;

## Załącznik nr 4 – Specyfikacja Infrastruktury;

## Załącznik nr 5 – Oprogramowanie Open Source;

## Załącznik nr 6 – Obsługa Nieprawidłowości;

## Załącznik nr 7 - Informacja odpowiadającą aktualnemu odpisowi z rejestru przedsiębiorców KRS dla Wykonawcy, ew. pełnomocnictwa;

## Załącznik nr 8 – Wymagania bezpieczeństwa dla aplikacji w ORLEN S.A;

## Załącznik nr 9 – Zakres współdziałania Zamawiającego;

## Załącznik nr 10 – Wynagrodzenie i zasady płatności;

## Załącznik nr 11 – Odbiory i wzory Protokołów Odbioru;

## Załącznik nr 12 - Lista i warunki korzystania z Utworów Osób Trzecich;

## Załącznik nr 13 – Protokół Akceptacji;

## Załącznik nr 14 – Regulacje Zamawiającego;

## *Załącznik nr 14A – Obowiązki informacyjne spółki publicznej – wersja dla przedsiębiorcy, którego instrumenty finansowe są notowane na GPW;*

## *Załącznik nr 14B – Obowiązki informacyjne spółki publicznej – wersja dla przedsiębiorcy, którego instrumenty finansowe nie są notowane na GPW;*

## Załącznik nr 15 – Zasady bezpieczeństwa teleinformatycznego;

## Załącznik nr 16 – Dokumentacja;

## Załącznik nr 17 – Prawa własności intelektualnej;

## Załącznik nr 18 – Kod Źródłowy;

## Załącznik nr 19 – Personel Kluczowy;

## Załącznik nr 20 – Klauzula Grupy ORLEN;

## Załącznik nr 21 – Klauzule KSEF;

## Załącznik nr 22 – Lista Utworów Standardowych;

## Załącznik nr 23 – Wzór PPDO.

|  |  |
| --- | --- |
| **Umowę podpisali** | |
| **za Zamawiającego:** | **za Wykonawcę:** |

**Załącznik nr 1 do UMOWY WDROŻENIOWEJ [ZAKRES WDROŻENIA]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# ZAKRES WDROŻENIA

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ETAP** | **ETAP** | **FAZA** | | **NAZWA ZADANIA / PRODUKT** | **WYCENA** | **PRODUKT** | **ZAKRES PRAC** |
| 1 | Koncepcja Biznesowa i Techniczna | ND | KONCEPCJA | Koncepcja biznesowa | FIX (w ramach projektu) | P01 Koncepcja Biznesowa | A. Przygotowanie dokumentu opisującego docelowe procesy dotyczące zarządzania użytkownikami i sposób ich wsparcia przez narzędzia, w tym: |
| a. Opis tworzenia i zarządzania kontami użytkowników w GK Orlen |
| b. Nadawanie i zmianę uprawnień dla użytkowników |
| c. definiowanie i zmianę ról z uprawnieniami, |
| d. kontrolę i przypisanie licencji dla użytkownika, |
| e. przeglądy okresowe uprawnień i użytkowników |
| f. Definicję raportów |
| g. Opracowanie uprawnień (opracowanie uprawnień wymaganych do pracy w GRC, dla wszystkich aktorów) |
| ND | KONCEPCJA | Koncepcja techniczna | FIX (w ramach projektu) | P02 Koncepcja Techniczna | A. Przygotowanie dokumentu opisującego architekturę systemów wchodzących w skład procesu zarządzania użytkownikami oraz  implementację produktów: SAP GRC Access Control oraz SAP Cloud Identity Access Governance  Integration Edition |
| 2 | Implementacja rozwiązania - w tym instalacja narzędzi i konfiguracja systemów zgodnie z Koncepcją Biznesową i Techniczną | ND | WDROŻENIE | Instalacja narzędzi i konfiguracja systemów | FIX (w ramach projektu) | P03 Zainstalowane narzędzia | A. Instalacja, konfiguracja, testy i uruchomienie narzędzi do zarządzania użytkownikami zgodnie z wypracowaną koncepcją techniczną i biznesową |
| P04 Skonfigurowane systemy SAP | B. Konfiguracja systemów skomunikowanych z GRC (systemy SAP), w tym wsparcie przy instalacji niezbędnych addonów na tych systemach |
| P05 Zintegrowany System GRC | C. Integracja systemu GRC z wdrażanym rozwiązaniem zarządzania tożsamościami użytkowników, oraz dostępem do systemów SAP (IDM, ORLEN Entra ID, SAP Cloud Identity Services). Integracja z systemami zgodnie z ustaleniami wypracowanymi na etapie budowania koncepcji, w tym ze środowiskami nieprodukcyjnymi |
| 3 | Wdrożenie 1 systemu, a w jego ramach: | 1 | WDROŻENIE | Dostosowanie i konfiguracja | FIX   (w ramach projektu) | P06 Wykonane niezbędne dostosowania i konfiguracje | A.Przegląd konfiguracji wykonanej w Etapie 2, identyfikacja brakujących elementów, oraz wykonanie wymaganych dostosowań i brakujących konfiguracji |
| 2 | Konfiguracja workflow i przygotowanie systemu do testów | FIX   (w ramach projektu) | P07 Skonfigurowane workflow | A. Przygotowanie ścieżek procesu akceptacji, w tym: |
| a. Użytkownicy – tworzenie, zmiany, blokowanie |
| b. Uprawnienia – tworzenie, zmiany, blokowanie |
| c. Dostęp uprzywilejowany (w tym dla konsultantów) - tworzenie, zmiany, blokowanie |
| d. Matryca uprawnień (SOD) - przygotowanie narzędzi do zarządzania SOD w procesach definiowania ról, nadawania uprawnień. |
| e. Przeglądy okresowe – automatyzacja procesu weryfikacji i akceptacji przeglądów okresowych uprawnień i użytkowników |
| P08 Przygotowane procedury, katalogi i reguły dostepów | B. Reguły zarządzania dostępem uprzywilejowanym |
| a. Procedury dostępu do poszczególnych środowisk |
| b. Zbudowanie katalogu dostępów krytycznych (technicznych), które zostaną wykluczone ze standardowych uprawnień. Opracowanie reguł dostępu do takich uprawnień |
| 3 | Testy | FIX   (w ramach projektu) | P09 Scenariusze testowe | A. Przygotowanie scenariuszy testowych, |
| P10 Odebrane testy UAT | B. Przeprowadzenie testów UAT |
| 4 | Uruchomienie Systemu (Go-live) | FIX   (w ramach projektu) | P11 Cut-over plan | A. Przygotowanie szczegółowego planu go-live |
| P12 Go-live | B. uruchomienie GRC dla konkretnego systemu SAP |
| P13 Dokumentacja projektowa | C. Przygotowanie niezbędnej dokumentacji technicznej (tj.instrukcje, procedury i.in.) |
| P14 Warsztaty | D. Realizacja max.2 dniowego warsztatu dla osób dedykowanych do obsługi wdrożonej funkcjonalności |
| 5 | Stabilizacja | FIX  (w ramach projektu) | P15 Odebrana usługa stabilizacji | A. 2 tygodniowy okres hypercare |
| 6 | WSPARCIE | Wsparcie po starcie | FIX  (w ramach projektu) | P16 Odebrana usługa wsparcia | A. 2 miesięczne wsparcie po starcie każdego zrealizowanego go-live |
|  |
| 4 | Wdrożenie 2 systemu, a w jego ramach: | 1 | WDROŻENIE | Przegląd i dostosowanie konfiguracji | FIX   (w ramach projektu) | P06 Wykonane niezbędne dostosowania i konfiguracje | A. Przegląd konfiguracji wykonanej w Etapie 2, identyfikacja brakujących elementów, oraz wykonanie wymaganych dostosowań i brakujących konfiguracji |  |
| 2 | Konfiguracja workflow i przygotowanie systemu do testów | FIX   (w ramach projektu) | P07 Skonfigurowane workflow | A. Przygotowanie ścieżek procesu akceptacji, w tym: |  |
| a. Użytkownicy – tworzenie, zmiany, blokowanie |  |
| b. Uprawnienia – tworzenie, zmiany, blokowanie |  |
| c. Dostęp uprzywilejowany (w tym dla konsultantów) - tworzenie, zmiany, blokowanie |  |
| d. Matryca uprawnień (SOD) - przygotowanie narzędzi do zarządzania SOD w procesach definiowania ról, nadawania uprawnień. |  |
| e. Przeglądy okresowe – automatyzacja procesu weryfikacji i akceptacji przeglądów okresowych uprawnień i użytkowników |  |
| P08 Przygotowane procedury, katalogi i reguły dostepów | B. Reguły zarządzania dostępem uprzywilejowanym |  |
| a. Procedury dostępu do poszczególnych środowisk |  |
| b. Zbudowanie katalogu dostępów krytycznych (technicznych), które zostaną wykluczone ze standardowych uprawnień. Opracowanie reguł dostępu do takich uprawnień |  |
| 3 | Testy | FIX   (w ramach projektu) | P09 Scenariusze testowe | A. Przygotowanie scenariuszy testowych, |  |
| P10 Odebrane testy UAT | B. Przeprowadzenie testów UAT |  |
| 4 | Uruchomienie Systemu (Go-live) | FIX   (w ramach projektu) | P11 Cut-over plan | A. Przygotowanie szczegółowego planu go-live |  |
| P12 Go-live | B. uruchomienie GRC dla konkretnego systemu SAP |  |
| P13 Dokumentacja projektowa | C. Przygotowanie niezbędnej dokumentacji technicznej (tj.instrukcje, procedury i.in.) |  |
| P14 Warsztaty | D. Realizacja max.2 dniowego warsztatu dla osób dedykowanych do obsługi wdrożonej funkcjonalności |  |
| 5 | Stabilizacja | FIX  (w ramach projektu) | P15 Odebrana usługa stabilizacji | A. 2 tygodniowy okres hypercare |  |
| 6 | WSPARCIE | Wsparcie po starcie | FIX  (w ramach projektu) | P16 Odebrana usługa wsparcia | A. 2 miesięczne wsparcie po starcie każdego zrealizowanego go-live |  |
|  |
| 5 | Wdrożenie 3 systemu, a w jego ramach: | 1 | WDROŻENIE | Przegląd i dostosowanie konfiguracji | FIX   (w ramach projektu) | P06 Wykonane niezbędne dostosowania i konfiguracje | A. Przegląd konfiguracji wykonanej w Etapie 2, identyfikacja brakujących elementów, oraz wykonanie wymaganych dostosowań i brakujących konfiguracji |  |
| 2 | Konfiguracja workflow i przygotowanie systemu do testów | FIX   (w ramach projektu) | P07 Skonfigurowane workflow | A. Przygotowanie ścieżek procesu akceptacji, w tym: |  |
| a. Użytkownicy – tworzenie, zmiany, blokowanie |  |
| b. Uprawnienia – tworzenie, zmiany, blokowanie |  |
| c. Dostęp uprzywilejowany (w tym dla konsultantów) - tworzenie, zmiany, blokowanie |  |
| d. Matryca uprawnień (SOD) - przygotowanie narzędzi do zarządzania SOD w procesach definiowania ról, nadawania uprawnień. |  |
| e. Przeglądy okresowe – automatyzacja procesu weryfikacji i akceptacji przeglądów okresowych uprawnień i użytkowników |  |
| P08 Przygotowane procedury, katalogi i reguły dostepów | B. Reguły zarządzania dostępem uprzywilejowanym |  |
| a. Procedury dostępu do poszczególnych środowisk |  |
| b. Zbudowanie katalogu dostępów krytycznych (technicznych), które zostaną wykluczone ze standardowych uprawnień. Opracowanie reguł dostępu do takich uprawnień |  |
| 3 | Testy | FIX   (w ramach projektu) | P09 Scenariusze testowe | A. Przygotowanie scenariuszy testowych, |  |
| P10 Odebrane testy UAT | B. Przeprowadzenie testów UAT |  |
| 4 | Uruchomienie Systemu (Go-live) | FIX   (w ramach projektu) | P11 Cut-over plan | A. Przygotowanie szczegółowego planu go-live |  |
| P12 Go-live | B. uruchomienie GRC dla konkretnego systemu SAP |  |
| P13 Dokumentacja projektowa | C. Przygotowanie niezbędnej dokumentacji technicznej (tj.instrukcje, procedury i.in.) |  |
| P14 Warsztaty | D. Realizacja max.2 dniowego warsztatu dla osób dedykowanych do obsługi wdrożonej funkcjonalności |  |
| 5 | Stabilizacja | FIX  (w ramach projektu) | P15 Odebrana usługa stabilizacji | A. 2 tygodniowy okres hypercare |  |
| 6 | WSPARCIE | Wsparcie po starcie | FIX  (w ramach projektu) | P16 Odebrana usługa wsparcia | A. 2 miesięczne wsparcie po starcie każdego zrealizowanego go-live |  |
|  |
| 6 | Wdrożenie 4 systemu, a w jego ramach: | 1 | WDROŻENIE | Przegląd i dostosowanie konfiguracji | FIX   (w ramach projektu) | P06 Wykonane niezbędne dostosowania i konfiguracje | A. Przegląd konfiguracji wykonanej w Etapie 2, identyfikacja brakujących elementów, oraz wykonanie wymaganych dostosowań i brakujących konfiguracji |  |
| 2 | Konfiguracja workflow i przygotowanie systemu do testów | FIX   (w ramach projektu) | P07 Skonfigurowane workflow | A. Przygotowanie ścieżek procesu akceptacji, w tym: |  |
| a. Użytkownicy – tworzenie, zmiany, blokowanie |  |
| b. Uprawnienia – tworzenie, zmiany, blokowanie |  |
| c. Dostęp uprzywilejowany (w tym dla konsultantów) - tworzenie, zmiany, blokowanie |  |
| d. Matryca uprawnień (SOD) - przygotowanie narzędzi do zarządzania SOD w procesach definiowania ról, nadawania uprawnień. |  |
| e. Przeglądy okresowe – automatyzacja procesu weryfikacji i akceptacji przeglądów okresowych uprawnień i użytkowników |  |
| P08 Przygotowane procedury, katalogi i reguły dostepów | B. Reguły zarządzania dostępem uprzywilejowanym |  |
| a. Procedury dostępu do poszczególnych środowisk |  |
| b. Zbudowanie katalogu dostępów krytycznych (technicznych), które zostaną wykluczone ze standardowych uprawnień. Opracowanie reguł dostępu do takich uprawnień |  |
| 3 | Testy | FIX   (w ramach projektu) | P09 Scenariusze testowe | A. Przygotowanie scenariuszy testowych, |  |
| P10 Odebrane testy UAT | B. Przeprowadzenie testów UAT |  |
| 4 | Uruchomienie Systemu (Go-live) | FIX   (w ramach projektu) | P11 Cut-over plan | A. Przygotowanie szczegółowego planu go-live |  |
| P12 Go-live | B. uruchomienie GRC dla konkretnego systemu SAP |  |
| P13 Dokumentacja projektowa | C. Przygotowanie niezbędnej dokumentacji technicznej (tj.instrukcje, procedury i.in.) |  |
| P14 Warsztaty | D. Realizacja max.2 dniowego warsztatu dla osób dedykowanych do obsługi wdrożonej funkcjonalności |  |
| 5 | Stabilizacja | FIX  (w ramach projektu) | P15 Odebrana usługa stabilizacji | A. 2 tygodniowy okres hypercare |  |
| 6 | WSPARCIE | Wsparcie po starcie | FIX  (w ramach projektu) | P16 Odebrana usługa wsparcia | A. 2 miesięczne wsparcie po starcie każdego zrealizowanego go-live |  |
|  |
| ND | Zlecenia | ND | WDROŻENIE + 12 MIESIĘCY po zakończeniu wsparcia dla ostatniego planowanego Go-live | Prace dodatkowe / Consultingowe | T&M 300MD | Produkty zostaną zdefiniowane każdorazowo przy zawieraniu Zleceń | A. Matryca uprawnień: |  |
| a. Przygotowanie podstawowej matrycy uprawnień bazując na wkładzie merytorycznym z projektu wzorca |  |
| b. Zasady rozwoju reguł SOD |  |
| c. Narzędzia umożliwiające zarządzanie matrycą uprawnień) |  |
| B. Integracja z systemami chmurowymi (w tym uruchomienie rozwiązania dla systemów chmurowych) |  |
| C. Prace rozwojowe |  |
| D. Inne zdefiniowane w ramach potrzeb |  |

**Załącznik nr 2 do UMOWY WDROŻENIOWEJ [HARMONOGRAM]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# HARMONOGRAM

**Załącznik nr 3 do UMOWY WDROŻENIOWEJ [STRUKTURA ZARZĄDZANIA UMOWĄ]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# STRUKTURA ZARZĄDZANIA UMOWĄ

## **[Kierownicy Projektu]**

## Do kompetencji Kierowników Projektu należą:

### bieżący nadzór nad realizacją Umowy;

### bieżąca komunikacja w ramach Umowy;

### organizowanie spotkań Komitetu Sterującego;

### przyjmowanie pism i oświadczeń składanych przez Kierownika Projektu drugiej Strony w przypadkach wskazanych w Umowie;

### bieżące zarządzanie Umową, które jednak nie może prowadzić do zmiany zakresu przedmiotowego Umowy;

### uczestniczenie w procedurze zarządzania zmianą Umowy, o której mowa w Rozdziale 10 Umowy;

### inne czynności określone w Umowie.

## Kierownicy Projektu podejmują decyzje odnośnie realizacji Umowy jednomyślnie.

## W celu uniknięcia wątpliwości Strony potwierdzają, że Kierownicy Projektu nie są uprawnieni do składania w imieniu reprezentowanej przez siebie Strony: oświadczeń o zmianie Umowy, oświadczeń o odstąpieniu od Umowy, ani zawarcia porozumienia o rozwiązaniu Umowy.

## Kierownik Projektu może udzielić innej osobie pełnomocnictwa do realizacji kompetencji dla niego zastrzeżonych. O fakcie udzielenia pełnomocnictwa, o którym mowa w zdaniu pierwszym, oraz o jego zakresie, Kierownik Projektu poinformuje Kierownika Projektu drugiej Strony w formie pisemnej lub poprzez wiadomość e-mail wysłaną na Kierownika Projektu drugiej Strony.

## Bieżąca komunikacja pomiędzy Kierownikami Projektu może odbywać się w formie wiadomości e-mail, wysyłanych na adresy Kierowników Projektu.

## **[Komitet Sterujący]**

## W posiedzeniach Komitetu Sterującego mogą brać udział również osoby trzecie wskazane przez Zamawiającego.

## Zamawiający wyznacza przewodniczącego Komitetu Sterującego.

## Do kompetencji Komitetu Sterującego należy:

### bieżące monitorowanie postępu prac w ramach realizacji Umowy;

### podejmowanie decyzji w sprawach przekazanych przez Kierowników Projektu;

### podejmowanie decyzji w ramach procedury zarządzania zmianą Umowy, o której mowa w Rozdziale 10 Umowy.

## Strony oświadczają, że osoby wchodzące w skład Komitetu Sterującego posiadają umocowanie wystarczające do realizacji kompetencji Komitetu Sterującego przewidzianych Umową.

## Zebrania Komitetu Sterującego będą odbywać się w siedzibie Zamawiającego, ilekroć zajdzie taka potrzeba, jednak nie rzadziej niż raz na 14 dni, chyba że Przewodniczący Komitetu Sterującego zdecyduje inaczej.

## Komitet Sterujący podejmuje decyzje jednomyślnie, w obecności co najmniej dwóch członków – po jednym z każdej ze Stron.

## W głosowaniach dotyczących Odbiorów lub innych decyzji zastrzeżonych w Umowie dla Zamawiającego nie biorą udziału członkowie Komitetu Sterującego ze strony Wykonawcy.

## Przebieg posiedzenia Komitetu Sterującego oraz treść podjętych w jego czasie decyzji zostanie utrwalona w formie pisemnego protokołu. Protokół będzie każdorazowo sporządzany przez członka Komitetu Sterującego ze strony Zamawiającego. Jego kopia będzie przekazywana Wykonawcy w ciągu 3 Dni Roboczych od dnia, w którym odbyło się posiedzenie Komitetu Sterującego.

## Na wniosek członka Komitetu Sterującego jednej ze Stron, sprawy przedłożone Komitetowi Sterującemu do decyzji, mogą być rozpatrywane w formie obiegowej: tj. poprzez doręczenie sobie nawzajem przez członków Komitetu Sterującego dokumentów, w formie pisemnej pod rygorem nieważności, zawierających oświadczenia w danej sprawie. Decyzję uznaje się za podjętą z chwilą dokonania ostatniego doręczenia i tylko jeśli odpowiednie dokumenty wystosują wszyscy członkowie Komitetu Sterującego. Zamawiający będzie przechowywał wszystkie wskazane wyżej dokumenty.

## **[Zmiana Kierownika Projektu lub członka Komitetu Sterującego]**

## Każda ze Stron ma prawo zmiany członków Komitetu Sterującego lub Kierownika Projektu, przy czym zmiany wchodzą w życie od chwili poinformowania o nich poprzez wiadomość e-mail wysłaną na adres Kierownika Projektu drugiej Strony. Strony zobowiązują się nie dokonywać zmian bez istotnych powodów.

## W celu uniknięcia wątpliwości Strony stwierdzają, że zmiana Kierownika Projektu lub członka Komitetu Sterującego nie wymaga zawarcia odrębnego aneksu w formie pisemnej pod rygorem nieważności.

**Załącznik nr 4 do UMOWY WDROŻENIOWEJ [SPECYFIKACJA INFRASTRUKTURY]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# SPECYFIKACJA INFRASTRUKTURY

**Załącznik nr 5 do UMOWY WDROŻENIOWEJ [OPROGRAMOWANIE OPEN SOURCE]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# OPROGRAMOWANIE OPEN SOURCE

## Z zastrzeżeniem postanowień poniższych, Wykonawca może podczas realizacji Umowy wykorzystać Oprogramowanie Open Source.

## W każdym przypadku wykorzystania Oprogramowania Open Source Wykonawca zapewnia, że jego wykorzystanie na potrzeby Umowy będzie zgodne z postanowieniami odpowiednich licencji przypisanych do danego Oprogramowania Open Source.

## Wykonawca oświadcza i gwarantuje, że wykorzystanie Oprogramowania Open Source nie będzie ograniczać Zamawiającego w zakresie rozpowszechniania innego oprogramowania połączonego z Oprogramowaniem Open Source, w tym nie może nakładać na Zamawiającego obowiązku rozpowszechniania takiego połączonego oprogramowania wraz z Kodem Źródłowym. W przypadku, w którym dana licencja na Oprogramowanie Open Source uzależnia zakres takich obowiązków od sposobu połączenia Oprogramowania Open Source z innym oprogramowaniem, Wykonawca zobowiązany jest do zrealizowania takiego połączenia w sposób nienakładający na Zamawiającego obowiązku rozpowszechniania połączonego oprogramowania wraz z Kodem Źródłowym.

## Wykonawca oświadcza i gwarantuje, że licencja na Oprogramowanie Open Source nie będzie nakładać na Zamawiającego obowiązku odprowadzania jakichkolwiek opłat lub wynagrodzenia na rzecz podmiotów uprawnionych do takiego Oprogramowania Open Source.

## Niezależnie od innych postanowień Umowy, fakt występowania Oprogramowania Open Source w Systemie przy naruszeniu przez Wykonawcę którejkolwiek z zasad warunkujących wykorzystanie Oprogramowanie Open Source, będzie traktowane przez Strony jako wada prawna oprogramowania, dostarczonego lub wykonanego przez Wykonawcę w ramach Umowy, uprawniająca w szczególności do nieodebrania przez Zamawiającego Wdrożenia.

## Bez uszczerbku dla punktów powyżej, lista Oprogramowanie Open Source wraz z określeniem rodzaju licencji, które Wykonawca może wykorzystać w ramach realizacji Umowy zawarta jest poniżej:

## [#].

## Dostarczona przez Wykonawcę lista Oprogramowania Open Source, wskazana w pkt. 2.6 powyżej, musi zawierać nazwę Oprogramowania Open Source oraz jego wersję.

## Niezależnie od punktów powyżej, jeżeli Wykonawca zamierza wykorzystać Oprogramowanie Open Source inne niż wymienione w pkt. 2.6., Wykonawca zobowiązuje się poinformować Kierownika Projektu Zamawiającego o tym fakcie, wraz z informacją o nazwie komponentu oraz rodzaju licencji, które Wykonawca zamierza wykorzystać w ramach realizacji Umowy, w formie pisemnej lub formie wiadomości e-mail wysłanej na adres Kierownika Projektu Zamawiającego. Dany komponent Oprogramowania Open Source może zostać wykorzystane przez Wykonawcę w ramach realizacji Umowy wyłącznie po uprzedniej akceptacji danego komponentu przez Kierownika Projektu Zamawiającego, dokonanej w formie pisemnej lub wiadomości e-mail wysłanej na adres Kierownika Projektu Wykonawcy, w terminie 14 dni od dnia otrzymania informacji o zamiarze wykorzystania danego Oprogramowania Open Source przez Wykonawcę.

## W przypadku identyfikacji podatności cyberbezpieczeństwa w wykorzystanym przy realizacji Umowy przez Wykonawcę Oprogramowaniu Open Source, Zamawiający może zdecydować o konieczności rezygnacji z wykorzystywanego Oprogramowania Open Source. Prawo to przysługuje Zamawiającemu na każdym etapie realizacji Umowy. W takiej sytuacji Wykonawca może skorzystać z innej wersji wskazanego Oprogramowania Open Source, wolnej od zidentyfikowanej podatności cyberbezpieczeństwa lub skorzystać z innego Oprogramowania Open Source (wolnego od zidentyfikowanej podatności cyberbezpieczeństwa), przy czym skorzystanie z tego Oprogramowania Open Source za każdym razem wymaga wyraźnej uprzedniej zgody Zamawiającego. Za zmiany wynikające z konieczności dostosowania dostarczanego rozwiązania do nowej wersji Oprogramowania Open Source lub do innego rozwiązania, Wykonawcy nie przysługuje dodatkowe wynagrodzenie.

## Przez cały okres trwania Umowy Wykonawca zobowiązuje się do nieodpłatnych aktualizacji oprogramowania dostarczonego lub wykonanego przez Wykonawcę w ramach Umowy, gdy zostanie zidentyfikowana i zgłoszona Wykonawcy podatność cyberbezpieczeństwa wykorzystanego przez Wykonawcę Oprogramowania Open Source. Czas na dostarczenie aktualizacji będzie każdorazowo uzgadniany przez Zamawiającego i Wykonawcę, po analizie wpływu danej podatności na bezpieczeństwo oprogramowania, dostarczonego lub wykonanego przez Wykonawcę w ramach Umowy.

**Załącznik nr 6 do UMOWY WDROŻENIOWEJ [OBSŁUGA NIEPRAWIDŁOWOŚCI]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# OBSŁUGA NIEPRAWIDŁOWOŚCI

# [Obsługa Nieprawidłowości]

## W przypadku wykrycia przez Zamawiającego Nieprawidłowości, Zamawiający dokona jego Zgłoszenia za pomocą:

## numeru telefonu: [#], albo

## poczty elektronicznej na adres e-mail: [#]

## (dalej: „**Kanały Komunikacji**”).

## Zgłoszenie będzie zawierać co najmniej następujące informacje:

* + 1. opis Nieprawidłowości;
    2. kategorię Nieprawidłowości;
    3. dane osoby upoważnionej do dokonania Zgłoszenia Nieprawidłowości;
    4. [#].

## Zgłoszenie uważa się za dokonane skutecznie z chwilą, gdy dotarło do Wykonawcy lub zostało wprowadzone do odpowiedniego Kanału Komunikacji w taki sposób, aby Wykonawcy mógł zapoznać się z jego treścią.

## Wykonawca ma prawo zgłosić do Zamawiającego wniosek o uzupełnienie Zgłoszenia o konkretnie wskazane informacje niezbędne do usunięcia Nieprawidłowości. W takim przypadku Zamawiający niezwłocznie uzupełni takie informacje, o ile jest w ich posiadaniu. Zgłoszenie wniosku, o którym mowa w zdaniu poprzedzającym nie wpływa na obliczanie Czasu Reakcji oraz Czasu Naprawy, chyba że dane Zgłoszenie nie zawiera informacji opisanych w pkt. 2.2. powyżej.

## Wykonawca zobowiązuje się dotrzymać Czasów Reakcji i Czasów Naprawy zgodnie z poniższą tabelą:

|  |  |  |
| --- | --- | --- |
|  | **Czas Reakcji** | **Czas Naprawy** |
| **Awaria** | 1 godzina | 8 godzin |
| **Błąd** | 2 godziny | 24 godziny |
| **Usterka** | 2 godziny | 80 godzin |

## Wykonawca zapewni obsługę Zgłoszeń – w okresie pomiędzy godz. 9.00 a godz. 17.00 od poniedziałku do piątku (dalej: „**Okno Zgłoszeń**”). Zdanie poprzedzające nie dotyczy Zgłoszeń Awarii, których obsługę Wykonawca zapewni w trybie 24/7/365(366).

## Czas Reakcji i Czas Naprawy liczone są od chwili dokonania Zgłoszenia w Oknie Zgłoszeń. W przypadku Zgłoszeń dokonanych poza Oknem Zgłoszeń, Zgłoszenie uznaje się za dokonane o godz. 9:00 w kolejnym, odpowiednim Oknie Zgłoszeń. Zdania poprzedzające nie dotyczą Zgłoszeń Awarii, których Czas Reakcji i Czas Naprawy liczone są od chwili dokonania ich Zgłoszenia.

## Czas Reakcji uważa się za dochowany z chwilą potwierdzenia przyjęcia Zgłoszenia przez Wykonawcę za pomocą odpowiedniego Kanału Komunikacji.

## Czas Naprawy uważa się za dochowany z chwilą zgłoszenia usunięcia Nieprawidłowości za pomocą odpowiedniego Kanału Komunikacji, jeżeli Nieprawidłowość została faktycznie usunięta. Zamawiający dokona weryfikacji usunięcia Nieprawidłowości niezwłocznie. Jeżeli podczas weryfikacji okaże się, że Nieprawidłowość nie została usunięta, Czas Naprawy ulega wznowieniu począwszy od momentu poinformowania Wykonawcy o tym fakcie. W takim przypadku Czas Naprawy jest dochowany dopiero z chwilą zgłoszenia poprawki faktycznie usuwającej Nieprawidłowość, z wyłączeniem czasu weryfikacji usunięcia Nieprawidłowości po stronie Zamawiającego.

## Jeśli w Czasie Naprawy, Wykonawca dostarczy Obejście, Czas Naprawy wydłuża się dwukrotnie. Powyższe dotyczy wyłącznie Awarii i Błędów.

## Wykonawca wykona i dostarczy Zamawiającemu raport dotyczący obsługi Nieprawidłowości w terminie do 5 Dni Roboczych:

### od zakończenia Okresu Stabilizacji*.*

## Raport, o którym mowa powyżej, będzie każdorazowo zawierał co najmniej:

### liczbę zgłoszonych Nieprawidłowości w okresie, którego raport dotyczy, wraz z podaniem ich kategorii oraz informacją o dotrzymaniu / niedotrzymaniu Czasu Reakcji oraz Czasu Naprawy.

# Załącznik nr 7 do UMOWY WDROŻENIOWEJ [INFORMACJA ODPOWIADAJĄCĄ AKTUALNEMU ODPISOWI Z REJESTRU PRZEDSIĘBIORCÓW KRS DLA WYKONAWCY, EW. PEŁNOMOCNICTWA]

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# INFORMACJA ODPOWIADAJĄCĄ AKTUALNEMU ODPISOWI Z REJESTRU PRZEDSIĘBIORCÓW KRS DLA WYKONAWCY

## Informacja odpowiadającą aktualnemu odpisowi z rejestru przedsiębiorców KRS dla Wykonawcy została zamieszczony poniżej.

# PEŁNOMOCNICTWA (jeśli dotyczy)

## Pełnomocnictwa przedstawicieli Wykonawcy zostały zamieszczone poniżej.

**Załącznik nr 8 do UMOWY WDROŻENIOWEJ [WYMAGANIA BEZPIECZEŃSTWA DLA APLIKACJI W ORLEN S.A.]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# WYMAGANIA BEZPIECZEŃSTWA DLA APLIKACJI W ORLEN S.A.

Niniejszy dokument zawiera uszczegółowione wymagania bezpieczeństwa dla aplikacji, która jest przedmiotem RFP. Wymagania podzielone są na 10 obszarów:

1. Architektura
2. Kontrola dostępu,
3. Identyfikacja i uwierzytelnianie
4. Kontrola integralności i ochrona przed złośliwym oprogramowaniem,
5. Kryptografia,
6. Logowanie zdarzeń i kontrola rozliczalności,
7. Dokumentacja i szkolenia,
8. Ciągłość działania,
9. Warunki wsparcia.
10. Zgodność ze standardem korporacyjnym

Prosimy o podanie informacji, czy aplikacja spełnia wymagania zawarte w tabeli. Możliwe jest również wprowadzenie dodatkowego komentarza o sposobie realizacji wymagania.

## Architektura

| Lp. | Opis | SPEŁNIA / NIESPEŁNIA | Uwagi/Uzasadnienie warunkowego odstąpienia |
| --- | --- | --- | --- |
|  | Architektura systemu musi być co najmniej trójwarstwowa przy czym podstawowy podział na warstwy musi uwzględniać:  warstwa danych (np. bazy danych, pliki), warstwa aplikacyjna (serwery aplikacyjne), warstwa prezentacji (serwery  obsługujące interfejsy użytkownika, dostęp kliencki do systemu). |  |  |
|  | Architektura systemu powinna pozwalać na fizyczną lub logiczną separacje poszczególnych jego warstw w odniesieniu do  maszyn, segmentów sieci (np. VLAN), technologii NAT/PAT oraz umożliwiać separację za pomocą firewalli lub ruterów. |  |  |
|  | Poszczególne komponenty systemu muszą potrafić komunikować się w warunkach opisanych powyżej przy czym połączenia pomiędzy tymi komponentami muszą być precyzyjnie zdefiniowane z dokładnością do portów i protokołów. Każdy z otwieranych portów czy protokołów musi być uzasadniony. Nie jest dopuszczalne otwieranie zakresu portów  w celu uproszczenia definicji połączeń lub z powodu braku znajomości bardziej ograniczonej ich listy. |  |  |
|  | System powinien posiadać fizyczną separację danych dostępnych dla:   * użytkowników wewnętrznych (np. pracownicy Orlen) * zewnętrznych (np. klienci).   W przypadku braku takiej możliwości powinna istnieć logiczna separacja oparta na sprawdzonych mechanizmach uwierzytelniania i autoryzacji. |  |  |
|  | Architektura systemu musi umożliwić separację dostępu. Użytkownik zewnętrzny nie może mieć możliwości uzyskania dostępu za pomocą dedykowanych kanałów dla użytkowników wewnętrznych (np. VPN) i na odwrót. |  |  |
|  | System powinien posiadać oddzielne mechanizmy uwierzytelniania użytkowników wewnętrznych i zewnętrznych. W  szczególności nie jest dopuszczalne logowanie domenowe bezpośrednio z sieci Internet. |  |  |
|  | Użytkownik może komunikować się wyłącznie przy użyciu warstwy prezentacji. Nie jest dozwolony bezpośredni  dostęp użytkowników do pozostałych warstw/komponentów systemu (serwery aplikacyjne, bazy danych, systemy plików). |  |  |
|  | Poszczególne moduły systemu muszą pracować z najmniejszymi możliwymi uprawnieniami. Nie jest dozwolone wymaganie uprawnień administracyjnych do zwykłej pracy tych modułów. |  |  |
|  | Dostęp do danych (o ile to możliwe) powinien być ograniczony na poziomie bazy danych a nie aplikacji. Nie jest dopuszczalna praca aplikacji na bazie danych z uprawnieniami DBA. |  |  |
|  | Niedozwolone jest wykorzystywanie protokołów uważanych powszechnie za niebezpieczne (tftp, NFS, SMB) przy komunikacji pomiędzy sieciami o różnym poziomie zaufanie (szczególne przy przepływnie z sieci o mniejszym zaufaniu do sieci o większym zaufaniu). W przypadku, gdy koniecznie użycie jest niebezpiecznych protokołów rekomendowane jest zastosowanie protokołu zabezpieczającego taką komunikację (np. TLS, IPSec). |  |  |
|  | Jeśli aplikacja oparta o technologie WWW używa protokołu https wymagane jest, aby ruch szyfrowany mógł być terminowany na brzegowych firewallach aplikacyjnych a następnie w zależności od potrzeby zestawiany drugi tunel z tych urządzeń bezpośrednio do aplikacji (lub przepuszczony ruch nieszyfrowany - http). Jest to wymaganie opcjonalne, zależne od decyzji ORLEN S.A. |  |  |

## Kontrola dostępu

| Lp. | Opis | SPEŁNIA / NIESPEŁNIA | Uwagi/Uzasadnienie warunkowego odstąpienia |
| --- | --- | --- | --- |
|  | Mechanizmy kontroli dostępu zaimplementowane w aplikacji muszą egzekwować zasadę ograniczonego dostępu – „wszystko, co nie jest wyraźnie dozwolone, jest zabronione”. Tym samym, muszą skutecznie blokować dostęp użytkowników do wszystkich chronionych usług, funkcji, danych i obiektów (plików, katalogów, danych w bazie danych, URL[[1]](#footnote-2)) z wyłączeniem tych, do których posiadają przyznane uprawnienia. |  |  |
|  | Zalecanym mechanizmem kontroli dostępu jest Mandatory Access Control[[2]](#footnote-3). |  |  |
|  | Użytkownicy mogą mieć dostęp jedynie do tych adresów URL, do których posiadają konkretne uprawnienia. |  |  |
|  | Użytkownicy mogą mieć dostęp jedynie do tych plików, do których posiadają konkretne uprawnienia. |  |  |
|  | Jeżeli w ramach aplikacji funkcjonują użytkownicy o zróżnicowanych uprawnieniach, mechanizmy kontroli dostępu zaimplementowane w tej aplikacji muszą zapewniać możliwość stosowania zasady minimalnych uprawnień, czyli możliwość przydzielania użytkownikom wyłącznie tych uprawnień, które są im niezbędne do wykonywania niezbędnych działań. |  |  |
|  | Aplikacja powinna bazować co najmniej na mechanizmach opartych o role (Role Based Access Control[[3]](#footnote-4)). |  |  |
|  | Dostęp do części administracyjnej aplikacji i części zarządzania treścią merytoryczną aplikacji nie może być udostępniony w sieci Internet. Dostęp do tych części może być możliwy wyłącznie z sieci wewnętrznych. |  |  |
|  | Powinien istnieć scentralizowany mechanizm zabezpieczający dostęp do każdego typu chronionych zasobów. |  |  |
|  | Część administracyjna i część zarządzania treścią powinna być odseparowana od części biznesowej aplikacji poprzez uruchomienie tych części, jako niezależne procesy systemowe, w kontekście uprawnień różnych nieuprzywilejowanych użytkowników, nasłuchujące na odrębnych portach (lub jako odrębne instancje serwerów www i serwerów aplikacyjnych). |  |  |
|  | Jeżeli w ramach pojedynczej aplikacji lub wielu instancji tej samej aplikacji funkcjonują użytkownicy przetwarzający odrębne zestawy danych, niepowiązane ze sobą (np. aplikacja jest wykorzystywana przez niezależne podmioty), zaimplementowane mechanizmy kontroli dostępu muszą skutecznie separować dostęp do zestawów danych poszczególnych użytkowników aplikacji, niezależnie od posiadanych uprawnień. To znaczy, że zaimplementowana separacja musi funkcjonować zarówno na poziomie uprawnień zwykłych użytkowników, jak również na poziomie uprawnień użytkowników uprzywilejowanych zarządzających uprawnieniami lub danymi. |  |  |
|  | Aplikacja musi chronić bezpośrednie odniesienia do obiektów tak, aby tylko uprawnione obiekty lub dane były dostępne dla użytkownika (np. ochrona przed manipulacją bezpośrednimi odniesieniami do obiektów). |  |  |
|  | Wszystkie ustalone reguły kontroli dostępu do usług, funkcji, danych i obiektów muszą być wymuszane po stronie serwera. Ponadto, mechanizmy kontroli dostępu muszą skutecznie blokować dostęp do reguł i atrybutów kontroli dostępu, tak, aby nie była możliwa ich nieautoryzowana modyfikacja przez użytkowników aplikacji, chyba, że są oni do tego uprawnieni. |  |  |
|  | Uprawnienia nie mogą być zaszywane (ang. hardcoding) w kodzie aplikacji |  |  |
|  | Decyzje dotyczące przydzielania uprawnień dostępu nie mogą bazować wyłącznie na parametrach przekazywanych w polach formularzy, ukrytych polach, lub innych parametrach przekazywanych do serwera. |  |  |
|  | Dostęp do bazy danych musi być filtrowany zgodnie z uprawnieniami użytkowników aplikacji. |  |  |
|  | W przypadku, gdy używany jest wyłącznie jeden użytkownik bazodanowy dalej dostęp do danych w aplikacji musi być filtrowany zgodnie z uprawnieniami użytkownika aplikacyjnego. Dodatkowo w każdym zapytaniu SQL musi być przesyłany identyfikator użytkownika aplikacyjnego. |  |  |
|  | Mechanizmy kontroli dostępu, które kończą pracę niepowodzeniem muszą to robić w sposób bezpieczny, tzn. nie może nastąpić nieautoryzowane dopuszczenie użytkownika do chronionych zasobów oraz wyjątek, który miał miejsce musi być prawidłowo obsłużony. Poprzez prawidłową obsługę przyjmuje się odnotowanie zdarzenia w logach i wyświetlenie użytkownikowi dostosowanego komunikatu zawierającego identyfikator błędu, bez ujawniania szczegółów technicznych funkcjonowania samej aplikacji lub jej otoczenia infrastrukturalnego. |  |  |
|  | Aplikacja musi logować zdarzenia dotyczące kontroli dostępu. |  |  |
|  | Aplikacja musi logować zmiany konfiguracji. |  |  |
|  | Muszą być logowane decyzje o próbie dostępu zakończonej niepowodzeniem. |  |  |
|  | Powinna być możliwość logowania decyzji zakończonych sukcesem. |  |  |
|  | Mechanizmy kontroli dostępu zaimplementowane w aplikacji muszą utrzymywać aktualny stan uprawnień użytkowników i w przypadku zmiany, ich egzekwowanie powinno być realizowane w trybie natychmiastowym. |  |  |
|  | Wszystkie informacje i pliki konfiguracyjne związane z bezpieczeństwem aplikacji muszą być przechowywane w miejscach chronionych przed nieautoryzowanym dostępem. |  |  |
|  | Konfiguracja serwera WWW musi zapobiegać indeksowaniu katalogów. |  |  |
|  | Mechanizmy kontroli dostępu zaimplementowane w aplikacji muszą skutecznie wymuszać ustalone reguły przepływu pracy w aplikacji (przyjęta kolejność realizacji zadań) oraz nałożone limity (wielkość załącznika, ilość operacji, ilość transakcji, ilość zmian, itp.). |  |  |
|  | Aplikacja powinna wykorzystywać sprawdzone mechanizmy kontroli dostępu, które oferowane są przez system operacyjny, powiązane usługi i zastosowany framework[[4]](#footnote-5). |  |  |
|  | Aplikacja uruchamiana na serwerze WWW powinna być uruchamiana z minimalnymi uprawnieniami (np. Microsoft IIS[[5]](#footnote-6) – LowPrivilege Application Pool Identity). |  |  |
|  | Jeśli to technicznie możliwe (i uzasadnione biznesowo) kontrola dostępu do aplikacji powinna być zintegrowana z systemem operacyjnym i korzystać z natywnych funkcji właściwego systemu (np. Single Sign-On [[6]](#footnote-7) – zintegrowane uwierzytelnianie w przypadku Windows). |  |  |
|  | Jeśli to możliwe, aplikacja powinna korzystać z mechanizmów typu sandbox[[7]](#footnote-8)lub izolacji procesów. |  |  |
|  | Aplikacja lub framework musi generować silne, losowe tokeny anty-CSRF unikalne dla użytkownika, jako część wszystkich istotnych operacji lub przy dostępie do wrażliwych danych. Aplikacja musi weryfikować obecność tego tokenu przy przetwarzaniu wskazanych zapytań. |  |  |
|  | Zdalne obiekty IFRAME oraz wymiana zasobów pomiędzy domenami nie mogą pozwalać na zawieranie dowolnych treści zewnętrznych.  Flash, Silverlight lub polityka wymiany zasobów pomiędzy domenami innej aplikacji internetowej musi być skonfigurowana tak by zapobiegać nieuwierzytelnionemu dostępowi zdalnemu. |  |  |

## Identyfikacja i uwierzytelnianie

| Lp. | Opis | SPEŁNIA / NIE SPEŁNIA | Uwagi/Uzasadnienie warunkowego odstąpienia |
| --- | --- | --- | --- |
|  | Wszyscy użytkownicy aplikacji lub procesy wykonywane w imieniu tych użytkowników muszą być jednoznacznie zidentyfikowani przed uzyskaniem dostępu. |  |  |
|  | Wszyscy użytkownicy aplikacji lub procesy wykonywane w imieniu tych użytkowników muszą przechodzić proces uwierzytelnienia. |  |  |
|  | Wymuszanie uwierzytelniania użytkowników musi być realizowane po stronie serwera. |  |  |
|  | Wszystkie mechanizmy uwierzytelniania (również biblioteki wywołujące zewnętrzne usługi uwierzytelniania) muszą być zaimplementowane centralnie. |  |  |
|  | Wykonanie wrażliwych operacji w aplikacji powinno być poprzedzone ponownym uwierzytelnieniem. |  |  |
|  | W przypadku uwierzytelniania użytkowników na bazie certyfikatów PKI[[8]](#footnote-9), mechanizm uwierzytelniania w aplikacji musi zapewniać: budowę i weryfikację pełnej ścieżki zaufania dla certyfikatu użytkownika uwzględniając wytyczne standardu X.509, weryfikację ważności certyfikatu, weryfikację braku unieważnienia certyfikatu z aktualną w danej chwili listą certyfikatów unieważnionych, weryfikację zgodności wystawcy z zaufanymi i autoryzowanymi wystawcami certyfikatów, istnienia powiązania certyfikatu z kontem w aplikacji oraz weryfikację podpisu cyfrowego użytkownika. |  |  |
|  | W przypadku uwierzytelniania użytkowników na bazie certyfikatów PKI, klucz prywatny z certyfikowanej pary kluczy musi być zabezpieczony hasłem dostępowym ustalanym przez użytkownika. Rekomendowaną polityką haseł jest polityka haseł dostępowych. |  |  |
|  | Aplikacja powinna wymagać, aby wszystkie funkcje operujące na czynnikach uwierzytelniania danej tożsamości (np. rejestracja, aktualizacja profilu, przypomnienie loginu/hasła), które mogą przywrócić dostęp do konta są co najmniej tak odporne na ataki jak główny mechanizm uwierzytelniający. |  |  |
|  | Wszystkie strony oraz zasoby muszą wymagać uwierzytelnienia za wyjątkiem tych specjalnie przeznaczonych na dostęp publiczny. |  |  |
|  | Muszą istnieć mechanizmy pozwalające na zarządzanie informacjami uwierzytelniającymi, tj. nadawaniem, zmianą, blokowaniem, czasem życia i przechowywaniem konta. |  |  |
|  | Aplikacja nie może pozwalać na odzyskanie utraconego hasła. |  |  |
|  | Aplikacja musi posiadać mechanizm pozwalający na zmianę utraconego hasła w sposób bezpieczny z wykorzystaniem dodatkowego kanału komunikacji (np. e-mail lub SMS). Mechanizm zmiany hasła powinien być odporny na ataki przynajmniej w takim stopniu jak podstawowy mechanizm uwierzytelniania. W przypadku wiadomości e-mail mechanizm zmiany hasła powinien wykorzystywać unikatowy adres URL wygenerowany dla danego użytkownika, przy czym część unikatowa powinna być nie krótsza niż 128 bitów. W przypadku wiadomości SMS, użytkownik powinien otrzymać kod SMS, nie krótszy niż 8 znaków alfanumerycznych. Czas ważności danych pozwalających na zmianę hasła powinien być nie dłuższy niż 15 minut. |  |  |
|  | Hasła do kont muszą być tworzone z użyciem ciągu zaburzającego (ang. salt) dla danego konta (np. wewnętrzny identyfikator użytkownika, czas utworzenia konta) i przekształcane przy użyciu mechanizmu hashowania[[9]](#footnote-10) przed ich zapisaniem. |  |  |
|  | Wszystkie dane uwierzytelniające służące do uzyskiwania dostępu do usług zewnętrznych względem aplikacji muszą być zaszyfrowane i przechowywane w zabezpieczonej lokalizacji. |  |  |
|  | W przypadku innego sposobu uwierzytelniania niż Active Directory muszą istnieć mechanizmy pozwalające na konfigurację złożoności haseł dla użytkowników, tj. budowy hasła (małe, wielkie litery, znaki specjalne, cyfry), długości hasła oraz czasu życia hasła. |  |  |
|  | Domyślna polityka haseł powinna wymuszać tworzenie haseł o długości minimum 8 znaków, zawierających co najmniej jedną małą i dużą literę, cyfrę oraz znak specjalny. |  |  |
|  | System powinien pamiętać co najmniej 6 ostatnio stosowanych haseł. |  |  |
|  | Domyślna polityka haseł powinna wymuszać minimalny oraz maksymalny czas życia haseł. Domyślny minimalny czas życia haseł powinien wynosić 1 dzień, a maksymalny 30-180 dni. |  |  |
|  | Aplikacja powinna pozwalać na ustawianie długich i skomplikowanych haseł oraz powinna wymagać minimalnej złożoności haseł w celu zapobiegania stosowaniu powszechnie używanych haseł. |  |  |
|  | Jakiekolwiek domyślne hasła używane inicjalnie w systemie muszą być przed wdrożeniem produkcyjnym zmienione na zgodne z polityka haseł (opisaną w tym dokumencie). |  |  |
|  | Muszą istnieć mechanizmy zapewniające kontrolę sesji uwierzytelnionego użytkownika (np. zamykanie nieaktywnych sesji po określonym czasie). |  |  |
|  | Identyfikator sesji nie może być krótszy niż 128 bitów. |  |  |
|  | Identyfikator sesji musi być losowy. |  |  |
|  | Identyfikator sesji musi być generowany z jak najszerszego zestawu znaków. |  |  |
|  | Identyfikator sesji musi być unikatowy dla użytkowników danej aplikacji. |  |  |
|  | Identyfikator sesji musi być zmieniany przy logowaniu użytkownika. |  |  |
|  | Identyfikator sesji musi być zmieniany przy ponownym uwierzytelnieniu. |  |  |
|  | Identyfikator sesji musi być zmieniany przy przejściu pomiędzy HTTP[[10]](#footnote-11) i HTTPS[[11]](#footnote-12). |  |  |
|  | Może być akceptowany za poprawny tylko ten identyfikator, który został wygenerowany przez aplikację. |  |  |
|  | Identyfikator sesji musi być unieważniany po określonym czasie bezczynności użytkownika. |  |  |
|  | Identyfikatory sesyjne nigdy nie mogą być przekazywane inaczej niż poprzez nagłówek cookie, w szczególności w adresie URL, wiadomościach błędu lub logach. Wlicza się w to wyłączenie wsparcia tzw. URL rewriting dla ciasteczek sesyjnych. |  |  |
|  | Identyfikator sesji nie może być ujawniany w komunikatach błędów i logach. |  |  |
|  | Identyfikator sesji musi być unieważniany i zmieniany lub usuwany przy wylogowaniu użytkownika. |  |  |
|  | Identyfikator sesji nie może być zapamiętywany w przeglądarce (brak funkcji zapamiętaj mnie). |  |  |
|  | Maksymalny okres bezczynności użytkownika powinien wynosić 15 minut. Upłynięcie maksymalnego czasu bezczynności musi skutkować unieważnieniem sesji po stronie serwera oraz klienta (wylogowaniem). |  |  |
|  | Powinno być możliwe zdefiniowanie bezwzględnego maksymalnego czasu życia sesji. |  |  |
|  | Wszystkie strony, do których dostęp wymaga uwierzytelnienia muszą zawierać linki umożliwiające wylogowanie. |  |  |
|  | Cookie[[12]](#footnote-13) zawierające uwierzytelnione tokeny[[13]](#footnote-14) / identyfikatory sesji muszą mieć ustawione atrybuty domain i path odpowiednio dla lokalizacji. |  |  |
|  | Mechanizmy uwierzytelniania użytkowników, które kończą pracę niepowodzeniem muszą to robić w sposób bezpieczny, tzn. nie może nastąpić dopuszczenie użytkownika do chronionych zasobów oraz wyjątek, który miał miejsce musi być prawidłowo obsłużony. Poprzez prawidłową obsługę przyjmuje się odnotowane zdarzenia w logach i wyświetlenie użytkownikowi dostosowanego komunikatu zawierającego identyfikator błędu, bez ujawniania szczegółów technicznych funkcjonowania samej aplikacji lub jej otoczenia infrastrukturalnego. |  |  |
|  | Aplikacja musi mieć możliwość uwierzytelniania użytkowników w oparciu o powszechnie używane i popularne metody uwierzytelniania. |  |  |
|  | Aplikacja powinna umożliwiać uwierzytelnianie Single Sign-On w oparciu o mechanizm zintegrowanego uwierzytelniania Windows. |  |  |
|  | Aplikacja powinna umożliwiać uwierzytelnianie Single Sign-On z wykorzystaniem kont domenowych systemu Windows. |  |  |
|  | Aplikacja powinna wykorzystywać domyślną implementację mechanizmu zarządzania sesją, dostarczaną przez stosowany framework. |  |  |
|  | W przypadku kont uprzywilejowanych (np. administratorów) powinno być zastosowane dwuskładnikowe uwierzytelnianie. |  |  |
|  | Dane uwierzytelniające nie mogą być zaszywane (ang. hardcoding) w kodzie aplikacji lub przekazywane w parametrach adresu URL. |  |  |
|  | W aplikacjach dostępnych w sieciach publicznych (np. sieci Internet), uwierzytelnianie w celu dostępu do zasobów związanych z czynnościami administracyjnymi powinno być możliwe jedynie z sieci wewnętrznej. |  |  |
|  | Aplikacja musi posiadać mechanizm ochrony przez atakami siłowymi (ang. brute-force)[[14]](#footnote-15) na dane uwierzytelniające, blokujący kolejne próby uwierzytelnienia na zdefiniowany okres czasu. |  |  |
|  | Aplikacja powinna stosować domyślną politykę blokowania ataków siłowych. Blokowanie możliwości uwierzytelnienia powinno następować po 5 nieudanych próbach. Okres blokowania powinien trwać minimum 15 minut, a licznik blokowania konta powinien być zerowany po 5 minutach. Aplikacja powinna posiadać mechanizm pozwalający na bezwzględne blokowanie konta, po przekroczeniu ustalonej liczby nieudanych prób uwierzytelnienia. |  |  |
|  | Wszystkie pola służące do wprowadzania haseł nie mogą pokazywać haseł użytkowników w czasie ich wpisywania oraz muszą mieć wyłączoną funkcję automatycznego uzupełnienia. |  |  |
|  | Mechanizm autouzupełniania haseł oraz wrażliwych danych (np. PIN) musi być wyłączony. |  |  |
|  | Wszystkie decyzje dotyczące wyników uwierzytelniania muszą być logowane, zarówno te zakończone sukcesem jak i te zakończone porażką. |  |  |
|  | Odpowiedzi aplikacji powinny zawierać nagłówki HTTP zwiększające poziom bezpieczeństwa użytkowników aplikacji |  |  |
|  | Odpowiedzi aplikacji muszą zawierać następujące nagłówki HTTP definiujące podstawową politykę bezpieczeństwa adresów, z którymi aplikacja może nawiązywać połączenie: Content-Security-Policy (Google Chrome), X-Content-Security-Policy (Firefox), X-WebKit-CSP (przeglądarki oparte na WebKit, np. Safari). |  |  |
|  | Nagłówek Content Security Policy musi mieć zdefiniowany atrybut default-src oraz (jeżeli to konieczne) atrybuty script-src, img-src, frame-src, connect-src tak, aby zezwolone były połączenia jedynie z zaufanymi adresami, np. „Content-Security-Policy: default-src 'self'”. |  |  |
|  | Aplikacja musi wymuszać używanie filtrów Cross-Site Scripting zaimplementowanych wprzeglądarkach poprzez ustawienie nagłówka odpowiedzi HTTP: „X-XSS-Protection: 1; mode=block;” |  |  |
|  | Odpowiedzi HTTPS aplikacji muszą zawierać nagłówek „Strict-Transport-Security: max-age=31536000; includeSubDomains” |  |  |
|  | Aplikacja powinna wykrywać oraz blokować próby zautomatyzowanego logowania się na konta użytkowników z jednym hasłem (tzw. bruteforce horyzontalny) |  |  |
|  | Aplikacja musi zapobiegać enumeracji użytkowników przez logowanie, resetowanie hasła lub funkcjonalność przypomnienia loginu. |  |  |
|  | Aplikacja nie może używać domyślnych haseł dla frameworka aplikacji lub jakichkolwiek komponentów użytych przez aplikację. |  |  |
|  | Wszystkie dane uwierzytelniające służące do uzyskania dostępu do zewnętrznych usług muszą być zaszyfrowane oraz przechowywane w bezpiecznym miejscu (nie w kodzie źródłowym). |  |  |
|  | Funkcja przypomnienia hasła nie może blokować lub w inny sposób wyłączać konta dopóki użytkownik nie zmieni hasła z powodzeniem. Należy jednak zabezpieczać się przed uporczywymi próbami przypomnienia hasła. |  |  |
|  | Aplikacja nie może używać powszechnie znanych pytań/odpowiedzi (tzw. "tajne" pytania i odpowiedzi). |  |  |
|  | Aplikacja nie może zezwalać na równoczesne działanie wielu sesji tego samego użytkownika pochodzących z różnych maszyn. |  |  |
|  | Każdy użytkownik powinien mieć unikatowy identyfikator, który jest niezmienny przez cały czas istnienia tego użytkownika  w systemie. |  |  |
|  | Identyfikator użytkownika wyrejestrowanego z systemu nie może być przypisany innemu użytkownikowi. |  |  |
|  | Po zalogowaniu do systemu użytkownik powinien uzyskać informacje o błędnych próbach logowania do jego konta (a przynajmniej o ostatniej błędnej próbie) oraz ostatniej pozytywnej próbie logowania do systemu. Wymaganie opcjonalne zależne od decyzji ORLEN. |  |  |
|  | W przypadku systemów, gdzie nie ma zastosowania mechanizm SSO musi być możliwość automatycznego lub ręcznego blokowania kont użytkowników np. ze względu na wygaśnięcie ważności konta. |  |  |

## Kontrola integralności i ochrona przed złośliwym oprogramowaniem

| Lp. | Opis | SPEŁNIA / NIESPEŁNIA | Uwagi/Uzasadnienie warunkowego odstąpienia |
| --- | --- | --- | --- |
|  | Muszą istnieć mechanizmy lub proces potwierdzający autentyczność instalowanej aplikacji (sprawdzanie sum kontrolnych). |  |  |
|  | Muszą istnieć mechanizmy potwierdzające spójność krytycznych plików w systemie. |  |  |
|  | Muszą istnieć mechanizmy potwierdzające integralność kodu, bibliotek i plików wykonywalnych (w tym kodu i plików wytworzonych przez zewnętrznych dostawców). |  |  |
|  | Muszą istnieć mechanizmy potwierdzające integralność plików konfiguracyjnych. |  |  |
|  | Muszą istnieć mechanizmy zapewniające kontrolę integralności sesji użytkownika. |  |  |
|  | Aplikacja nie może zawierać złośliwego kodu (w tym kodu, który mógłby zostać użyty do nawiązywania sesji z pominięciem mechanizmów uwierzytelniania – np. backdoor). |  |  |
|  | Muszą istnieć mechanizmy zapewniające kontrolę wprowadzanych danych (w przypadku wprowadzania ciągów znaków - ich format i składnię). |  |  |
|  | Wszystkie źródła wejścia w aplikacji muszą mieć zdefiniowane i zastosowane wzorce pozytywnej walidacji. |  |  |
|  | Walidacja wejścia w aplikacji zakończona niepowodzeniem musi odrzucać lub oczyszczać przyjmowane dane. |  |  |
|  | Wszystkie źródła wejścia muszą posiadać zdefiniowaną stronę kodową np. UTF-8. |  |  |
|  | Cała walidacja danych wejściowych lub mechanizmy enkodowania muszą być realizowane po stronie serwera. |  |  |
|  | Aplikacja musi wykorzystywać jeden mechanizm walidacji danych wejściowych dla każdego typu przyjmowanych danych. |  |  |
|  | Wszystkie walidacje wejścia zakończone niepowodzeniem muszą być logowane. |  |  |
|  | Przez rozpoczęciem walidacji wszystkie dekodery lub interpretery muszą otrzymywać dane wejściowe w postaci ustandaryzowanej. |  |  |
|  | Aplikacja musi filtrować i nadzorować manipulowanie parametrami HTTP, zwłaszcza, jeśli framework nie odróżnia źródła parametrów (metod GET, POST, ciasteczek, nagłówków). |  |  |
|  | Muszą istnieć mechanizmy kontroli rodzaju, zawartości, zakresu, nazwy, formatu i wielkości plików w przypadku funkcjonalności związanych z importem plików (upload) oraz pobieraniem plików (download). |  |  |
|  | Zawartość importowanych plików musi być sprawdzana pod kątem zawierania złośliwego kodu. |  |  |
|  | Muszą istnieć mechanizmy uniemożliwiające wykonanie kodu zawartego w importowanych plikach. |  |  |
|  | Nazwy plików oraz ścieżek otrzymane z niezaufanych źródeł muszą być znormalizowane w celu wyeliminowania ataków manipulacją ścieżką (pathtraversal). |  |  |
|  | Parametry uzyskane z niezaufanych źródeł nie mogą być użyte przy tworzeniu nazw plików, ścieżek lub jakichkolwiek obiektów systemu plików bez poprzedniego znormalizowania, walidowania danych wejściowych oraz enkodowania danych wyjściowych. |  |  |
|  | Pliki otrzymane z niezaufanych źródeł muszą być przetrzymywane poza katalogiem głównym (webroot). |  |  |
|  | Serwer aplikacyjny musi być skonfigurowany tak by domyślnie blokować dostęp do zdalnych zasobów lub systemów poza serwerem aplikacyjnym. |  |  |
|  | Aplikacja musi mieć zaimplementowane mechanizmy enkodowania/escapowania[[15]](#footnote-16) danych wyjściowych. |  |  |
|  | Wszystkie niezaufane dane, których wynikiem jest kod HTML[[16]](#footnote-17) (elementy HTML, atrybuty HTML, wartości danych javascript[[17]](#footnote-18), bloki CSS[[18]](#footnote-19) i atrybuty URI[[19]](#footnote-20)) muszą podlegać escapowaniu odpowiednio do kontekstu. |  |  |
|  | Wszystkie mechanizmy enkodowania / escapowania muszą być zaimplementowane po stronie serwera. |  |  |
|  | Mechanizmy enkodowania / escapowania danych wyjściowych muszą enkodować wszystkie znaki, które nie są uważane za bezpieczne dla danego interpretera. |  |  |
|  | Dla każdego typu enkodowania / escapowania wyjścia wykonywanego przez aplikację musi istnieć pojedynczy mechanizm bezpieczeństwa dla tego typu docelowych danych wyjściowych. |  |  |
|  | Wszystkie niezaufane dane wyjściowe trafiające do interpreterów SQL[[20]](#footnote-21) muszą używać parametryzowanych interfejsów (ang. preparedstatements), przygotowanych instrukcji lub być właściwie escapowane. |  |  |
|  | Wszystkie niezaufane dane wyjściowe, których wynikiem jest XML [[21]](#footnote-22)muszą używać parametryzowanych interfejsów lub być właściwie escapowane. |  |  |
|  | Wszystkie niezaufane dane używane w zapytaniach LDAP[[22]](#footnote-23) muszą być właściwie escapowane. |  |  |
|  | Wszystkie niezaufane dane używane, jako parametry poleceń systemu operacyjnego muszą być właściwie escapowane. |  |  |
|  | Wszystkie niezaufane dane przekazywane do interpreterów innych niż ww., również muszą być właściwie escapowane. |  |  |
|  | Wszystkie połączenia wykorzystywane do komunikacji z innymi elementami aplikacji lub systemami podmiotów zewnętrznych, przez które przesyłane są dane wrażliwe, muszą być zabezpieczone kryptograficznie oraz strony takich połączeń muszą być uwierzytelnione. |  |  |
|  | Aplikacja oraz otoczenie infrastrukturalne, w którym funkcjonuje aplikacja nie może pozwalać na realizację połączeń niezabezpieczonych w przypadku, gdy nie powiodła się próba nawiązania połączenia bezpiecznego. |  |  |
|  | Czas w aplikacji musi być synchronizowany z zaufanym źródłem czasu. |  |  |
|  | Naruszenia integralności muszą być logowane oraz objęte właściwą obsługą. |  |  |
|  | Aplikacja musi mieć możliwość współpracy z zastosowanymi wewnętrznie ustawieniami zabezpieczeń klienta WWW (używanej w Organizacji przeglądarki WWW). |  |  |
|  | Aplikacja nie może wysyłać żadnych informacji do serwerów w sieci Internet (w szczególności informacji o charakterze poufnym). |  |  |
|  | W aplikacji musi być możliwość pobierania uaktualnień z wewnętrznego serwera (zalecane, aby odbywało się to w sposób automatyczny). |  |  |
|  | Środowisko uruchomieniowe aplikacji musi wykorzystywać mechanizmy zapobiegające wystąpieniu błędów przepełnienia bufora pamięci. |  |  |
|  | W przypadku, gdy w aplikacji wykorzystywane są zewnętrzne biblioteki, czy framework-i należy wykorzystywać wyłącznie aktualne wersje. |  |  |
|  | Aplikacja nie może polegać na skryptach znajdujących się na serwerach firm trzecich. Gdy jednak jest to konieczne, wykonawca musi o tym fakcie powiadomić ORLEN S.A. i uzyskać pisemną zgodę. |  |  |
|  | Dostawca powinien dostarczyć aplikację razem z kodem źródłowym. |  |  |
|  | Kod źródłowy aplikacji musi zostać poddany analizie bezpieczeństwa. |  |  |

## Kryptografia

| Lp. | Opis | SPEŁNIA / NIESPEŁNIA | Uwagi/Uzasadnienie warunkowego odstąpienia |
| --- | --- | --- | --- |
|  | Transmisja informacji wrażliwych przekazywanych za pośrednictwem publicznych sieci musi odbywać się wyłącznie w postaci zaszyfrowanej i tylko z wykorzystaniem protokołów komunikacji zapewniających wysoki poziom poufności. |  |  |
|  | Wszystkie połączenia do zewnętrznych systemów, które dotyczą wrażliwych informacji lub funkcji muszą być uwierzytelnione. |  |  |
|  | Wszystkie połączenia do zewnętrznych systemów, które dotyczą wrażliwych informacji lub funkcji muszą używać konta o minimalnych przywilejach koniecznych do właściwej pracy aplikacji. |  |  |
|  | Składowanie i przetwarzanie wrażliwych informacji w systemach, aplikacjach i bazach danych powinno być możliwe jedynie w postaci zaszyfrowanej (np. z użyciem natywnych mechanizmów szyfrujących). |  |  |
|  | Wszystkie wrażliwe dane, w cache lub kopiach tymczasowych, przechowywane na serwerze muszą być chronione przed nieautoryzowanym dostępem lub czyszczone / unieważniane po uzyskaniu dostępu do danych wrażliwych przez upoważnionego użytkownika. |  |  |
|  | Każdy typ wrażliwych danych musi być usuwany z aplikacji wraz z końcem wymaganego terminu ich przetrzymywania. |  |  |
|  | Dane wrażliwe nie mogą być nigdzie przechowywane w postaci jawnej. System powinien zapewniać kryptograficzne środki ochrony przechowywanych danych wrażliwych. |  |  |
|  | Składowanie informacji uwierzytelniającej (hasła, tokeny oraz klucze prywatne) musi odbywać się jedynie w zabezpieczonej przestrzeni (np. zewnętrznym serwerze uwierzytelniającym, urządzeniu HSM[[23]](#footnote-24)). |  |  |
|  | Dostęp do wszystkich kluczy master secret[[24]](#footnote-25)musi być chroniony przed nieuprawnionym dostępem. |  |  |
|  | Stosowane informacje uwierzytelniające nie powinny być dostępne w kodzie źródłowym aplikacji (ang. hardcoding). |  |  |
|  | Przechowywanie informacji uwierzytelniającej w pamięci aplikacji musi odbywać się w sposób uniemożliwiający proste jej odczytanie (np. przechowywanie hasła w postaci jawnego tekstu jest niedopuszczalne). |  |  |
|  | Należy stosować mechanizmy zapobiegające przechowywaniu wrażliwych informacji po stronie użytkownika. |  |  |
|  | Wszystkie formularze zawierające dane wrażliwe nie powinny być cache’owane po stronie klienta, włączając w to funkcjonalność automatycznego wypełniania pól. |  |  |
|  | Wszystkie wrażliwe dane, w cache lub kopiach tymczasowych, przesyłane do klienta muszą być chronione przed nieautoryzowanym dostępem lub czyszczone / unieważniane po uzyskaniu dostępu do danych wrażliwych przez upoważnionego użytkownika (np. powinny być ustawiane odpowiednie nagłówki kontrolne Cache-Control: no-cache i no-store). |  |  |
|  | Aplikacja WWW udostępniona w sieci Internet (szczególnie służąca do komercyjnego udostępniania usług) musi stosować certyfikaty SSL wystawione przez zewnętrzne zaufane centrum certyfikacji. Dla szczególnie istotnych usług powinien to być certyfikat typu Extended ValidationCertificate (EV SSL, ang. certyfikaty rozszerzonej walidacji). |  |  |
|  | Podejrzanie zwiększona ilość zapytań informacyjnych lub zapytań wywołujących krytyczne transakcje muszą być blokowane. |  |  |
|  | Obsługa protokołu HTTP/HTTPS musi następować w zgodnie z najlepszymi praktykami bezpieczeństwa (np. ustawianie wymaganych nagłówków HTTP oraz ich atrybutów, konfiguracja protokołu TLS[[25]](#footnote-26)). |  |  |
|  | Musi być możliwe zbudowanie ścieżki z zaufanego CA[[26]](#footnote-27) do każdego serwowanego certyfikatu TLS i każdy certyfikat serwera musi być ważny. |  |  |
|  | Nieudane połączenia TLS nie mogą być powtórnie nawiązywane, jako połączenia niezabezpieczone. |  |  |
|  | TLS musi być używany dla wszystkich połączeń (zewnętrznych i backendowych), które są uwierzytelnione lub są związane z wrażliwymi danymi lub funkcjami. |  |  |
|  | Nieudane backendowe połączenia TLS muszą być logowane. |  |  |
|  | Ścieżki certyfikatów muszą być budowane i weryfikowane dla wszystkich certyfikatów klienckich przy użyciu skonfigurowanych powiązań zaufania i informacji nt. unieważniania certyfikatów. |  |  |
|  | Wykorzystywana konfiguracja protokołu SSL/TLS powinna być wolna od znanych błędów bezpieczeństwa np. podatności na ataki DoS[[27]](#footnote-28) wykorzystujący renegocjację połączeń inicjowaną przez klienta, atak BEAST[[28]](#footnote-29), atak CRIME[[29]](#footnote-30), atak MITM[[30]](#footnote-31)plaintextinjection[[31]](#footnote-32) wykorzystujący niebezpieczną renegocjację połączeń itp. |  |  |
|  | Wykorzystywana konfiguracja protokołu SSL/TLS powinna stosować wyłącznie zestawy szyfrów powszechnie uznawane za silne. |  |  |
|  | Dla wszystkich połączeń powinno zostać zdefiniowane kodowanie znaków. |  |  |
|  | Przekierowania HTTP nie mogą zawierać danych pozbawionych walidacji. |  |  |
|  | Aplikacja musi akceptować wyłącznie zdefiniowany zestaw metod zapytań HTTP, takich jak GET i POST. |  |  |
|  | Każda odpowiedź HTTP musi zawierać nagłówek Content-type, określający zestaw bezpiecznych znaków (np. UTF-8). |  |  |
|  | Flaga HttpOnly musi być wykorzystywana dla wszystkich cookie, do których nie jest wymagany dostęp z JavaScript. |  |  |
|  | Flaga secure musi być wykorzystywana dla wszystkich cookie, które zawierają wrażliwe informacje, włączając w to cookie sesyjne. |  |  |
|  | Wszystkie strony zwracane od serwera powinny zawierać nagłówek X-Frame-Options, ustalony na wartość DENY lub SAMEORIGIN. Nagłówek ten aktywuje politykę po stronie przeglądarki, ograniczającą możliwość używania mechanizmu ramek IFRAME i ładowania danej strony do ramki (DENY) lub zezwalającą wyłącznie na ładowanie danej strony do ramki pochodzącej z tego samego serwera i numeru portu, co sama strona (SAMEORIGIN). Dodatkowo, aplikacja powinna posiadać mechanizmy wykrywające i blokujące ładowanie treści strony w ramkę pływającą IFRAME poprzez zastosowanie mechanizmu framebusting. |  |  |
|  | Nagłówki HTTP i/lub inne mechanizmy dla starszych przeglądarek muszą być załączone by zapobiegać atakom Clickjacking. |  |  |
|  | Nagłówki HTTP dodane przez frontend (np. X-Real-IP) wykorzystane w aplikacji muszą być chronione przed zmianą przez użytkownika końcowego. |  |  |
|  | Nagłówki HTTP nie mogą ujawniać szczegółowych informacji o wersji komponentów. |  |  |
|  | Nagłówki HTTP w zapytaniach i odpowiedziach muszą zawierać wyłącznie drukowalne znaki ASCII. |  |  |
|  | Aplikacja musi generować silne losowe tokeny będące częścią linków i formularzy powiązanych z transakcjami lub mających dostęp do wrażliwych danych, a także w trakcie przetwarzania takich zapytań aplikacja musi sprawdzać obecność tego tokena oraz poprawność jego wartości odpowiednio dla bieżącego użytkownika. |  |  |
|  | Wszystkie dane wrażliwe muszą być przesyłane do serwera wewnątrz wiadomości HTTP (tzn. parametry URL nie są używane do przesyłania danych wrażliwych). |  |  |
|  | Stosowane moduły kryptograficzne muszą pracować w trybie zapewniającym należyty stopień bezpieczeństwa (stosowanie odpowiedniego źródła losowości, należyta obsługa błędów, zgodność z normami, standardami i wewnętrznymi politykami, a także najlepszymi praktykami w dziedzinie kryptografii). |  |  |
|  | Wszystkie liczby losowe, losowe nazwy plików, losowe GUID’y[[32]](#footnote-33) oraz losowe ciągi znaków, których napastnik nie powinien odgadnąć muszą być generowane z wykorzystaniem zatwierdzonego generatora liczb losowych z modułu kryptograficznego. |  |  |
|  | Wszystkie moduły kryptograficzne, które kończą pracę niepowodzeniem muszą robić to w sposób bezpieczny. |  |  |
|  | Próby naruszenia ochrony kryptograficznej oraz jej błędne działanie muszą być logowane. |  |  |
|  | Moduły kryptograficzne wykorzystywane przez aplikację powinny być zatwierdzone w zakresie zgodności ze standardem FIPS 140-2[[33]](#footnote-34) lub jego odpowiednikiem, poziom (Level) certyfikacji może zostać ustalony w sposób ekspercki po analizie wrażliwości przetwarzanych danych. |  |  |
|  | Moduły kryptograficzne powinny pracować w trybie zgodnym z opublikowanymi politykami bezpieczeństwa dla danego modułu. |  |  |
|  | Wszystkie funkcje kryptograficzne służące do zabezpieczania danych poufnych przed użytkownikiem aplikacji muszą być zaimplementowane po stronie serwera. |  |  |
|  | Implementacja mechanizmów kryptograficznych w aplikacji musi wykorzystywać standardowe, powszechnie używane i akceptowane biblioteki kryptograficzne. Nie jest akceptowane implementowanie algorytmów, bibliotek i protokołów kryptograficznych we własnym zakresie. |  |  |
|  | Implementacja kryptograficznych mechanizmów bezpieczeństwa nie może wykorzystywać powszechnie uznanych za podatne lub o słabej mocy kryptograficznej protokołów (takich, jak np. SSL v3, TLS 1.1). Użycie takich protokołów powinno być wyłączone po stronie serwera. |  |  |
|  | Aplikacja powinna mieć możliwość implementacji polityk określających zarządzanie kluczami kryptograficznymi (np. generowanie, rozprowadzanie, unieważnianie, w jaki sposób wygasają). |  |  |
|  | Aplikacja musi pozwalać na implementacje funkcji (dla zidentyfikowanych wrażliwych danych) przetwarzania, przechowywana i przesyłana tych danych zgodnie z określoną polityką, które może regulować kwestie kontroli dostępu do tych danych oraz kiedy te dane muszą podlegać szyfrowaniu. |  |  |
|  | Musi istnieć metoda usunięcia z aplikacji każdego typu wrażliwych danych na końcu ich wymaganego okresu ważności. |  |  |
|  | Wrażliwe dane muszą być usuwane z pamięci tak szybko jak tylko nie będą potrzebne i używane przez funkcje oraz techniki wspierane przez framework/bibliotekę/system operacyjny. |  |  |
|  | Jeżeli dane transmitowane są w tunelu SSL VPN, to musi być on zgodny ze specyfikacją transmisji danych protokołem HTTPS z użyciem obustronnego uwierzytelniania za pomocą certyfikatów PKI (niekwalifikowanych). |  |  |
|  | Jeżeli dane transmitowane są w tunelu IPSec VPN[[34]](#footnote-35), to musi on spełniać następujące wymagania:   * Tryb pracy IPSec: ESP w trybie tunelowym; * Protokół negocjacji parametrów: IKE; * Metoda uwierzytelniania stron:   + Użytkownicy:     - Certyfikat PKI (niekwalifikowany);   + Systemy:     - Certyfikat PKI (niekwalifikowany); * Symetryczne algorytmy szyfrowania:   + AES;   + Minimalna długość klucza: 128 bitów. * Funkcje skrótu: HMAC-SHA-256 lub dłuższa; * Grupy Diffie-Hellman:   + Modular Exponential (MODP), grupy 5, lub 14-18.   + Elliptic Curve Group over GF[2^N] (EC2N), grupa 4; * Tryb negocjacji w fazie I:   + Mainmode,   + Aggressivemode (zabroniony); * Czas ważności kluczy: 3600 sekund. |  |  |
|  | Rekomendowane jest składowanie danych na dyskach twardych w postaci zaszyfrowanej algorytmem zapewniającym należyty stopień poufności np. AES-128. |  |  |
|  | Parametry wykorzystywanych certyfikatów PKI powinny spełniać poniższe wytyczne:   * Algorytmy asymetryczne: RSA * Długość kluczy: 2048 bitów * Algorytm podpisu: SHA1-with-RSA * Maksymalny okres ważności certyfikatów: 1 rok * Regeneracja kluczy w trakcie odnowienia certyfikatów |  |  |
|  | Parametry haseł użytkowników aplikacji webowych powinny spełniać poniższe wytyczne:   * Hasła tworzone i przechowywane z użyciem soli * Długość soli: co najmniej 32 bajty * Sól[[35]](#footnote-36) generowana losowo * Inna sól dla każdego konta * Dopuszczalne algorytmy dla zabezpieczania haseł:   + Funkcje skrótu: SHA256, SHA512   + Scrypt, PBKDF2 (liczba iteracji: 64 000). |  |  |
|  | W przypadku budowy aplikacji z wykorzystaniem usług serwisowych (web services) należy stosować mechanizmy zapewniające poufność i integralność przesyłanych danych. |  |  |
|  | W celu zapewnienia poufności komunikacji należy stosować mechanizmy szyfrowania z wykorzystaniem SSL/TLS. |  |  |
|  | Należy poprawnie stosować mechanizmy uwierzytelniania serwera (certyfikat serwera musi być wydany przez zaufane CA) oraz jeśli jest to wymagane – uwierzytelniania użytkowników (również z wykorzystaniem certyfikatów). |  |  |
|  | W celu zapewnienia integralności przesyłanych informacji należy stosować SSL/TLS. |  |  |
|  | W przypadku, gdy przesyłane wiadomości są szczególnie wrażliwe, należy je szyfrować za pomocą silnych mechanizmów szyfrujących (należy wtedy wykorzystywać szyfrowanie na poziomie przesyłanych wiadomości a nie wyłącznie warstwie transportowej SSL/TLS). |  |  |
|  | Należy stosować mechanizmy chroniące przez atakami XML Denial of Service. |  |  |

## Logowanie zdarzeń i kontrola rozliczalności

| Lp. | Opis | SPEŁNIA / NIESPEŁNIA | Uwagi/Uzasadnienie warunkowego odstąpienia |
| --- | --- | --- | --- |
|  | Aplikacja musi rejestrować wszystkie zdarzenia, które mogą być pomocne w monitorowaniu poziomu bezpieczeństwa, analizie, ewentualnym dochodzeniu lub zgłoszeniu objawów naruszenia bezpieczeństwa, w tym jako min.:   * udane i nieudane próby uwierzytelnienia, * założenie i usunięcie konta użytkownika * zablokowanie i odblokowanie konta użytkownika * aktywacja i dezaktywacja kont użytkowników, * zmiany ról i uprawnień użytkowników, * zmiany parametrów konfiguracyjnych, * próby przekraczania uprawnień. |  |  |
|  | Wszystkie mechanizmy logowania muszą być zaimplementowane na serwerze. |  |  |
|  | Zarejestrowane zdarzenia muszą mieć określoną strukturę, zakres oraz miejsce składowania. |  |  |
|  | Logowane zdarzenia na serwerze WWW muszą być zgodne ze znanym standardem (np. W3C) i jako minimum muszą zawierać informacje o:   * żądanym adresie URL * zastosowanej metodzie protokołu HTTP, * adresie IP użytkownika, * dacie i czasie wykonania żądania, * zwróconym kodzie serwera HTTP, * ilości przesłanych danych, * nagłówku user-agent oprogramowania użytkownika, * poziom ważności zdarzenia. |  |  |
|  | Logowane zdarzenia z aplikacji binarnych muszą korzystać z natywnych funkcji systemu operacyjnego (np. Event Log w systemach Windows). |  |  |
|  | Struktura logów aplikacji musi pozwalać na korelację zdarzeń z innymi systemami, w tym z systemami służącymi do analizy logów np. SIEM[[36]](#footnote-37). |  |  |
|  | Logi powinny być spójne dla całego systemu a jeśli są one generowane osobno dla każdego z modułów systemu, powinna  istnieć korelacja pomiędzy nimi, aby można było odtworzyć na ich podstawie spójny ciąg zdarzeń. W systemach o wysokim stopniu komplikacji i budowie modułowej wymagane jest aby moduł odpowiedzialny za logowanie/raportowanie był odrębnym, dedykowanym modułem. |  |  |
|  | Logi aplikacji przetwarzających wrażliwe informacje muszą zapewniać możliwość odtworzenia całego przebiegu przetwarzania tych informacji wraz z możliwością odtworzenia każdej wprowadzonej zmiany przez poszczególnych użytkowników. |  |  |
|  | Pola logów z zaufanych oraz niezaufanych źródeł muszą być rozróżniane w dziennikach zdarzeń. |  |  |
|  | Zarejestrowane zdarzenia muszą być przechowywane w bezpieczny sposób i chronione przed nieautoryzowanym ujawnieniem lub modyfikacją przez zdefiniowany okres czasu. |  |  |
|  | Informacje o zarejestrowanych zdarzeniach z krytycznych elementów aplikacji powinny być przesyłane do systemu, który pełni rolę centralnego serwera logów. W przypadku zastosowania centralnego serwera logów, rejestrowane zdarzenia muszą dodatkowo posiadać informację o urządzeniu/systemie/aplikacji, która jest ich źródłem. |  |  |
|  | Rejestrowane zdarzenia muszą być chronione przed nieautoryzowanym ujawnieniem, zmianą i zniszczeniem. Wszystkie dzienniki zdarzeń muszą mieć ustalone restrykcyjne prawa dostępu. Dla szczególnie wrażliwych komponentów aplikacji, rejestrowane zdarzenia muszą być przechowywane z zapewnieniem zachowania ich integralności poprzez zastosowanie mechanizmów kryptograficznej ochrony informacji (np. znakowanie czasem lub podpisy cyfrowe gromadzonych zdarzeń). |  |  |
|  | Informacje o zarejestrowanych zdarzeniach muszą być przechowywane w trybie dostępu przez minimum 90 dni. Po upływie tego czasu informacje o zdarzeniach mogą być archiwizowane lub usuwane, z zachowaniem zgodności z przepisami prawa |  |  |
|  | Zdarzenia dla wszystkich komponentów aplikacji powinny być rejestrowane z uwzględnieniem strefy czasowej: CET (UTC+1). |  |  |
|  | Znaczniki czasu uwzględniane w rejestrowanych informacjach o zdarzeniach powinny pochodzić z wiarygodnego źródła czasu (wymagana synchronizacja czasu aplikacji z wiarygodnym źródłem czasu). |  |  |
|  | Wszyscy użytkownicy aplikacji muszą być jednoznacznie zidentyfikowani (poprzez przydzielanie unikatowych identyfikatorów). |  |  |
|  | Wszystkie operacje wykonywane w aplikacji muszą być jednoznacznie powiązane z odpowiedzialnymi za ich wykonanie użytkownikami. |  |  |
|  | Komunikaty błędów widoczne dla użytkowników nie mogą zawierać danych potencjalnie wrażliwych (np. dane osobowe, dane nt. konfiguracji serwera, identyfikatory sesyjne użytkowników, kod aplikacji, ślady stosu). |  |  |
|  | Logowane zdarzenia nie mogą zawierać danych wrażliwych (np. dane osobowe, identyfikatory sesyjne, dane konfiguracyjne serwera, hasła). |  |  |
|  | Moduł służący do przeglądania logów musi posiadać mechanizmy ochrony przez wykonaniem (potraktowaniem jako kod) niezaufanych danych będących treścią logów aplikacji. |  |  |
|  | W przypadku uwierzytelniania w oparciu o identyfikator i hasło, aplikacja musi wyświetlać ogólny komunikat, z którego nie będzie można wywnioskować czy błędnie został podany identyfikator czy hasło dostępowe. |  |  |
|  | Oprogramowanie musi używać jednej implementacji logowania zdarzeń aplikacyjnych. |  |  |
|  | Wszystkie niedrukowalne znaki oraz separatory pól muszą być poprawnie enkodowane w dziennikach zdarzeń. |  |  |
|  | Logowanie zdarzenia musi wystąpić przed wykonaniem akcji. Jeżeli logowanie się nie powiodło (np. przez brak miejsca na dysku, brakujące uprawnienia) aplikacja powinna kończyć pracę bezpiecznie. |  |  |
|  | Logi techniczne aplikacji (np. debugowe) powinny być oddzielone od logów audytowych. |  |  |
|  | System powinien zapewniać rozliczalność działań administracyjnych. Między innymi w tym celu powinny istnieć indywidualne konta administracyjne (niedopuszczalne jest tworzenie administracyjnych kont grupowych). |  |  |

## Dokumentacja i szkolenia

| Lp. | Opis | SPEŁNIA / NIESPEŁNIA | Uwagi/Uzasadnienie warunkowego odstąpienia |
| --- | --- | --- | --- |
|  | Dostarczenie dokumentacji projektu aplikacji. |  |  |
|  | Dostarczenie dokumentacji instalacji aplikacji. |  |  |
|  | Dostarczenie dokumentacji konfiguracji aplikacji i oprogramowania zawierającej opis zastosowanych zabezpieczeń, które wynikały z przedstawionych wymagań oraz schemat architektury rozwiązania (z wymienionymi portami i protokołami używanymi do komunikacji i transmisji informacji). |  |  |
|  | Dostarczenie dokumentacji użytkowej (eksploatacyjnej) aplikacji z podziałem dla odbiorców (użytkowników biznesowych i technicznych). |  |  |
|  | Dostarczenie dokumentacji związanej z usystematyzowaniem obsługi błędów i incydentów bezpieczeństwa. |  |  |
|  | Dostarczenie dokumentacji związanej z innymi elementami, np. procedurami pracy (monitorowanie poprawności działania, tworzenia kopii zapasowych i odtwarzania ich po awarii), zgodności z regulacjami (np. Ustawą o Ochronie Danych Osobowych), zastosowanymi interfejsami do innych aplikacji i systemów. |  |  |
|  | Dostarczenie szkolenia lub szkoleń związanych z zapewnianiem bezpieczeństwa aplikacji (integralności, poufności i dostępności). |  |  |

## Ciągłość działania

| Lp. | Opis | SPEŁNIA / NIESPEŁNIA | Uwagi/Uzasadnienie warunkowego odstąpienia |
| --- | --- | --- | --- |
|  | Każdy element dostarczanej aplikacji (np. front-end, repozytorium danych) powinien umożliwiać zastosowanie dodatkowych elementów realizujących redundancje. |  |  |
|  | Dla wszystkich elementów krytycznych dla zapewnienia ciągłości działania aplikacji powinna zostać zastosowana nadmiarowość (w postaci zapewnienia redundancji tych zasobów). |  |  |
|  | W przypadku aplikacji intranetowych aplikacja musi być zgodna z przeglądarką z aktualnego Korporacyjnego Standardu Informatycznego(KSI). Zgodność aplikacji internetowej z wiodącymi na rynku przeglądarkami internetowymi (Internet Explorer w wersji 7,8,9,10,11 oraz najaktualniejszymi wersjami: Google Chrome, Mozilla Firefox, Safari, Opera) powinna być zapewniona przez ustalony okres czasu. |  |  |
|  | Zgodność aplikacji z wiodącymi na rynku systemami operacyjnymi powinna być zapewniona przez ustalony okres czasu. |  |  |
|  | Wszystkie podatności krytyczne, wysokie i średnie powinny być wyeliminowane przed fazą produkcyjną. |  |  |
|  | Środowisko produkcyjne musi być pozbawione wszelkich zbędnych dla działania produkcyjnego komponentów, pakietów a zwłaszcza narzędzi developerskich, kompilatorów, itp. |  |  |
|  | Musi być zapewniona możliwość logowania się administratora do systemu operacyjnego na którym uruchomiona jest aplikacja. |  |  |

## Warunki wsparcia

| Lp. | Opis | SPEŁNIA / NIESPEŁNIA | Uwagi/Uzasadnienie warunkowego odstąpienia |
| --- | --- | --- | --- |
|  | Firma dostarczająca aplikację powinna zapewnić wsparcie. |  |  |
|  | W umowie serwisowej uwzględnione powinny być elementy takie jak czas reakcji, czas naprawy, RPO, RTO[[37]](#footnote-38). |  |  |
|  | Zgłoszenia powinny być przyjmowane przynajmniej jedną z dróg: telefoniczną, za pomocą e-mail czy dedykowanego serwisu internetowego. |  |  |
|  | Powinna zostać ustalona priorytetyzacja zgłoszeń oraz czas reakcji dotyczący zgłoszeń o danym priorytecie. |  |  |
|  | Wszystkie podatności muszą być naprawione przez dostawcę. Podatność rozumiana jest jako opisana i wciągnięta do ewidencji luka w zabezpieczeniach opublikowana w powszechnie znanych, publicznych i uznawanych za wiarygodne katalogach takich, jak CVE, CCE, biuletyn bezpieczeństwa Microsoft i innych (np. dostępnych poprzez http://web.nvd.nist.gov/view/vuln/search). |  |  |

## Zgodność ze standardem korporacyjnym

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Opis | SPEŁNIA / NIESPEŁNIA | Uwagi/Uzasadnienie warunkowego odstąpienia |
|  | Aplikacja powinna być pisana w sposób kompatybilny z aktualnie obowiązującym Korporacyjnym Standardem Informatycznym w ORLEN S.A. |  |  |

**Załącznik nr 9 do UMOWY WDROŻENIOWEJ [ZAKRES WSPÓŁDZIAŁANIA ZAMAWIAJĄCEGO]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# ZAKRES WSPÓŁDZIAŁANIA ZAMAWIAJĄCEGO

**Załącznik nr 10 do UMOWY WDROŻENIOWEJ [****WYNAGRODZENIE I ZASADY PŁATNOŚCI]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# WYNAGRODZENIE

## Maksymalna wartość Umowy wynosi [#] złotych netto. Łączne Wynagrodzenie, za Wdrożenie i Wynagrodzenie za Zlecenie nie może przekroczyć kwoty wskazanej w zdaniu poprzedzającym.

## W zamian za należytą realizację Wdrożenia, Zamawiający zapłaci Wykonawcy Wynagrodzenie za Wdrożenie w wysokości [#] zł netto.

## Wynagrodzenie za Wdrożenie płatne będzie po Odbiorze Etapu, z wykonaniem którego związana jest dana płatność stosownie do poniższego harmonogramu płatności:

|  |  |
| --- | --- |
|  | **Kwota Wynagrodzenia** |
| Odbiór Etapu I | [#] zł netto |
| Odbiór Etapu II | [#] zł netto |
| Odbiór Etapu III | [#] zł netto |
| Odbiór Etapu IV | [#] zł netto |
| Odbiór Etapu V | [#] zł netto |
| Odbiór Etapu VI (opcjonalnie) | [#] zł netto |

## W zamian za należytą realizację Zlecenia w zakresie Prac Dodatkowych, Zamawiający zapłaci Wykonawcy Wynagrodzenie za Zlecenie zgodnie z pkt. 2.5. poniżej.

## Wynagrodzenie za Zlecenie będzie obliczone zgodnie z zasadami poniżej:

* + 1. maksymalne Wynagrodzenie za Zlecenie będzie każdorazowo obliczane jako iloczyn stawki za Roboczodzień zgodnie z pkt. 2.6. poniżej oraz maksymalnej pracochłonności Zlecenia (liczby Roboczodni);
    2. w przypadku, gdy faktyczna liczba Roboczodni w ramach realizacji Zlecenia będzie mniejsza od maksymalnej pracochłonności danego Zlecenia, Wynagrodzenie za Zlecenie zostanie obliczone jako iloczyn stawki za jeden Roboczodzień wskazanej w pkt. 2.6. poniżej oraz faktycznej liczby Roboczodni poświęconych przez Wykonawcę na realizację danego Zlecenia;
    3. w przypadku, gdy faktyczna liczba Roboczodni w ramach realizacji Zlecenia będzie równa albo większa od maksymalnej pracochłonności danego Zlecenia, Wynagrodzenie za Zlecenie będzie równe maksymalnemu wynagrodzeniu za dane Zlecenie.

## Na potrzeby obliczania Wynagrodzenia za Zlecenie na Prace Dodatkowe Strony przyjmują następujące stawki dla poszczególnych specjalistów w ramach Personelu Wykonawcy:

* + 1. Architekt - [#] zł netto / 1 Roboczodzień pracy on-site;
    2. Architekt - [#] zł netto / 1 Roboczodzień pracy off-site;
    3. Programista - [#] zł netto / 1 Roboczodzień pracy on-site;
    4. Programista - [#] zł netto / 1 Roboczodzień pracy off-site;
    5. Konsultant - [#] zł netto / 1 Roboczodzień pracy on-site;
    6. Konsultant - [#] zł netto / 1 Roboczodzień pracy off-site.

## Maksymalny limit netto na Prace Dodatkowe realizowane w ramach Zleceń (stanowiący maksymalną sumę Wynagrodzenia za Zlecenia realizowane w ramach Umowy) wynosi […] (słownie: […]) zł.

# ZASADY PŁATNOŚCI

## Wykonawca może wystawić fakturę nie wcześniej niż po podpisaniu przez Zamawiającego Protokołu Odbioru lub Protokołu Akceptacji i nie później niż w terminie 7 dni od dnia ich podpisania. Podpisany przez Strony Protokół Odbioru lub odpowiednio – Protokół Akceptacji stanowi podstawę do wystawienia faktury przez Wykonawcę.

## Płatności wynikające z Umowy będą dokonywane przez Zamawiającego na rachunek bankowy Wykonawcy wskazany na fakturze, w terminie 60 dni od doręczenia faktury. W przypadku dostarczenia faktury bez podpisanego Protokołu Odbioru Zamawiającemu przysługuje prawo do wstrzymania płatności faktury, a termin płatności będzie liczony od daty uzupełnienia dokumentacji przez Wykonawcę.

## W przypadku wynagrodzenia Wykonawcy opiewającego na kwotę w walucie innej niż złote polskie, wartość do zapłaty stanowić będzie równowartość stosownej kwoty określonej w Umowie w walucie przeliczonej na złote polskie według kursu średniego NBP ogłaszanego dla dnia poprzedzającego dzień wystawienia faktury, powiększonej o podatek VAT (kurs i tabela powinny zostać podane na fakturze).

## Wynagrodzenie określone w Umowie będzie wynagrodzeniem w kwocie netto. Na fakturach wystawianych przez Wykonawcę podatek VAT zostanie każdorazowo doliczony do wynagrodzenia, zgodnie z obowiązującymi przepisami.

## Faktura zawierająca następujące dane Zamawiającego:

## ORLEN S.A, ul. Chemików 7, 09 - 411 Płock, NIP 774-00 -01- 454,

## oraz numer Umowy

## w przypadku faktur wysyłanych drogą elektroniczną będzie doręczona zgodnie z porozumieniem w sprawie przesyłania faktur w formie elektronicznej stanowiącej Dodatek nr 1 do niniejszego Załącznika; albo

## w przypadku faktur sporządzonych w formie pisemnej będzie doręczona do ORLEN S.A. listem poleconym oraz przesłana listem poleconym z dopiskiem „faktura" na kopercie, za zwrotnym potwierdzeniem odbioru na adres:

## ORLEN S.A., ul. Chemików 7, 09 - 411 Płock

## - będzie uznawana za dostarczoną do Zamawiającego w dacie widniejącej na zwrotnym potwierdzeniu odbioru.

## Na mocy odrębnego porozumienia Zamawiający dopuszcza możliwość otrzymywania faktur w formie elektronicznej. Strony wraz z zawarciem Umowy podpiszą porozumienie w sprawie przesyłania faktur w formie elektronicznej stanowiącej Dodatek nr 1 do niniejszego Załącznika – będzie to równoznaczne z zaakceptowaniem przez Wykonawcę wysyłania do Zamawiającego faktur drogą elektroniczną oraz akceptacją Zamawiającego w zakresie ich otrzymania. Forma elektroniczna będzie miała pierwszeństwo przed innymi formami wystawiania faktur przez Wykonawcę (w szczególności przed formą opisaną w pkt. 3.5. lit. b).

## Zamawiający oświadcza, że jest czynnym podatnikiem podatku od towarów i usług (VAT) i posiada numer NIP 774-00-01-454. Dla transakcji zawieranych z Wykonawcą Zagranicznym, Zamawiający oświadcza, iż jest podatnikiem podatku od towarów i usług (VAT) i posiada Europejski Numer NIP (Numer VAT-UE): PL7740001454.

## Wykonawca oświadcza, że posiada Numer Identyfikacji Podatkowej (NIP), wskazany w komparycji Umowy, i jest czynnym podatnikiem podatku od towarów i usług (VAT).

## Faktura niespełniająca wymagań określonych w niniejszym paragrafie nie będzie akceptowana przez Zamawiającego.

## Wykonawca zobowiązuje się do zachowania statusu podatnika VAT czynnego przynajmniej do dnia wystawienia ostatniej faktury dla ORLEN S.A. W przypadku gdy Wykonawca zostanie wykreślony z rejestru VAT na podstawie przesłanek wskazanych w ustawie o VAT, jest on zobowiązany do niezwłocznego powiadomienia ORLEN S.A. o tym fakcie. W przypadku gdy Wykonawca nie powiadomi ORLEN S.A. o wykreśleniu z rejestru VAT, o którym mowa w zdaniu poprzedzającym, postanowienia pkt 3.11. poniżej stosuje się odpowiednio, z wyjątkiem przypadku gdy Wykonawca w terminie 30 (trzydziestu) dni od dnia pozyskania informacji o wykreśleniu go z rejestru VAT przedstawi ORLEN S.A. dokumenty, z których wynika, że rejestracja została przywrócona. Niezależnie od powyższych postanowień, Wykonawca najpóźniej przed podpisaniem Umowy, zobowiązuje się do przedstawienia aktualnego urzędowego zaświadczenia potwierdzającego zarejestrowanie Wykonawca jako podatnika podatku VAT czynnego.

## Wykonawca gwarantuje i ponosi odpowiedzialność za prawidłowość zastosowanych stawek podatku VAT, co oznacza, że w przypadku zakwestionowania przez organy podatkowe prawa ORLEN S.A. do odliczenia podatku z tego powodu, iż zgodnie z przepisami dana transakcja nie podlegała opodatkowaniu lub była zwolniona od podatku, Wykonawca – na pisemne żądanie ORLEN S.A. oraz w terminie w nim wskazanym – dokona odpowiedniej korekty faktury oraz zwróci ORLEN S.A. powstałą różnicę w terminie 21 (dwudziestu jeden) dni od dnia wystawienia tego żądania. W przypadku odmowy wystawienia przez Wykonawcę faktury korygującej, Wykonawca zgadza się na zwrot ORLEN S.A. równowartości podatku VAT zakwestionowanego przez organy podatkowe, przy czym zwrot ten nastąpi na podstawie noty księgowej wystawionej przez ORLEN S.A., w terminie 21 (dwudziestu jeden) dni od dnia jej wystawienia przez ORLEN S.A. W każdym z powyższych przypadków Wykonawca zwróci ORLEN S.A. także równowartość sankcji, odsetek, kar i innych obciążeń dodatkowo poniesionych przez ORLEN S.A. bądź nałożonych przez władze podatkowe, przy czym zwrot ten nastąpi w sposób opisany w zdaniu poprzednim. Powyższe postanowienia znajdą odpowiednio zastosowanie również w przypadku, gdy ORLEN S.A. do sprzedaży towarów zastosuje stawkę podatku VAT wskazaną przez Wykonawcę na fakturach dokumentujących dostawy towarów dla ORLEN S.A., a następnie będzie ona kwestionowana przez organy podatkowe. Strony zgodnie postanawiają, że zobowiązanie opisane w niniejszym punkcie obowiązuje niezależnie od rozwiązania, wygaśnięcia lub uchylenia bądź zniweczenia skutków prawnych Umowy.

## Płatność wynikająca z Umowy będzie realizowana w mechanizmie podzielonej płatności, o którym mowa w ustawie z dnia 11 marca 2004 r. o podatku od towarów i usług, wyłącznie na wskazany przez Wykonawcę rachunek bankowy figurujący w wykazie podatników VAT prowadzonym przez właściwy organ administracji (tzw. Białej Liście). Dotyczy to zarówno rachunków bankowych prowadzonych w złotych polskich, jak i walutach obcych.

## W przypadku niemożności dokonania płatności w sposób wskazany w pkt 3.12. powyżej z uwagi na:

* + 1. brak na Białej liście wskazanego przez Wykonawcę numeru rachunku bankowego lub
    2. brak wskazania przez Wykonawcę jako właściwego do zapłaty części ceny brutto odpowiadającej podatkowi VAT numeru rachunku bankowego w złotych polskich figurującego na Białej liście (dotyczy przypadków wskazania przez Wykonawcę do zapłaty ceny netto rachunku bankowego w walucie obcej),

Zamawiający będzie uprawniony do wstrzymania płatności na rzecz Wykonawcy odpowiednio: wynagrodzenia (w przypadku wskazanym w pkt. 3.13.1.powyżej) lub części wynagrodzenia odpowiadającej podatkowi VAT (w przypadku wskazanym w pkt. 3.13.2. powyżej).

## W sytuacji wskazanej w pkt. 3.13. powyżej płatność nastąpi nie później niż w terminie 7 Dni Roboczych od (odpowiednio): dnia następnego po przekazaniu Zamawiającemu przez Wykonawcę informacji o pojawieniu się jego numeru rachunku bankowego na Białej liście (w przypadku wskazanym w pkt. 3.13.1. powyżej) lub dnia następnego po wskazaniu Zamawiającemu przez Wykonawcę numeru rachunku bankowego w złotych polskich figurującego na Białej liście (w przypadku, o którym mowa w pkt. 3.13.2. powyżej).

## Strony zgodnie przyjmują, że wystąpienie okoliczności, o których mowa w pkt. 3.13. powyżej, zwalnia Zamawiającego z obowiązku zapłaty odsetek za zwłokę za okres pomiędzy ustalonym w umowie terminem płatności a dniem zrealizowania przez Zamawiającego na rzecz Wykonawcy płatności, o których mowa w pkt. 3.14. powyżej.

## Niezależnie od powyższych postanowień, od dnia, w którym Wykonawca zostanie prawnie zobowiązany do wystawiania i udostępnienia Zamawiającemu faktur ustrukturyzowanych przy użyciu Krajowego Systemu e-Faktur na podstawie przepisów ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług, zastosowanie znajdą postanowienia zawarte w Załączniku nr 21 [**Klauzule KSEF**].

**DODATEK NR 1 [POROZUMIENIE W SPRAWIE PRZESYŁANIA FAKTUR W FORMIE ELEKTRONICZNEJ] DO ZałącznikA NR 10 DO UMOWY WDROŻENIOWEJ [WYNAGRODZENIE i ZASDAY PŁATNOŚCI]**

miejscowość i data

Porozumienie w sprawie przesyłania faktur w formie elektronicznej

Odbiorca:

ORLEN Spółka Akcyjna z siedzibą w Płocku

ul. Chemików 7

09-411 Płock

wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Łodzi- Śródmieścia w Łodzi, XX Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000028860, NIP 774-00-01-454, kapitał zakładowy/ kapitał wpłacony w całości: 1.451.177.561,25 zł

**Wystawca** (pełną nazwa i adres siedziby Kontrahenta):

[nazwa spółki] z siedzibą w [siedziba spółki]

ul. [adres]

[kod pocztowy] [miejscowość poczty]

wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd [#], [#]Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS [#], NIP [#], kapitał zakładowy */ kapitał wpłacony w całości*: [#]

1. Działając na podstawie ustawy z 11 marca 2004 r. o podatku od towarów i usług Odbiorca akceptuje przesyłanie mu przez Wystawcę faktury w formie elektronicznej z chwilą podpisania Porozumienia przez ORLEN S.A.
2. E-faktury, e-faktury korekta, duplikaty e-faktur, e-noty księgowe będą przesyłane pocztą elektroniczną w postaci plików PDF z poniższego/ych adresu/adresów mailowych Wystawcy: [#] (zgodnie z warunkami zawartymi w Instrukcji przesyłania faktur w formie elektronicznej do ORLEN S.A., będącej załącznikiem do niniejszego Porozumienia).
3. Adresem właściwym do przesyłania Odbiorcy dokumentów wymienionych w pkt. 2 niniejszego Porozumienia będzie: [**efaktura@orlen.pl**](mailto:efaktura@orlen.pl)
4. Adresem właściwym dla potwierdzenia Wystawcy odbioru dokumentów wymienionych w pkt. 2 niniejszego Porozumienia będzie: [#].

Brak wskazania przez Wystawcę adresu do wysyłania potwierdzeń odbioru dokumentu oznacza rezygnację z potwierdzania odbioru. Potwierdzenie odbioru e-faktury zostanie wysłane przez system pocztowy Odbiorcy w momencie wprowadzenia dokumentu do systemu księgowego, przy czym datą otrzymania będzie data wpływu e- faktury na skrzynkę pocztową Odbiorcy.

1. W przypadku zmiany adresu/adresów e-mail, wskazanych w punkcie 2, 3 i 4 powyżej, Strony zobowiązują się do poinformowania się o dokonanych zmianach w formie pisemnej lub mailowej.
2. W przypadku, gdyby przeszkody formalne lub techniczne uniemożliwiły wystawienie i przesyłanie faktur w formie elektronicznej, wówczas faktury zostaną przesłane w formie papierowej.
3. Niniejsza akceptacja może zostać cofnięta przez Odbiorcę w każdym czasie. Wówczas Wystawca faktur traci prawo do wystawiania i przesyłania faktur w formie elektronicznej od następnego dnia od daty otrzymania informacji o cofnięciu akceptacji.
4. Akceptując niniejsze Porozumienie Wystawca oświadcza, że zapoznał się z dołączoną do niego Instrukcją przesyłania faktur w formie elektronicznej do ORLEN S.A. i będzie stosował się do zwartych w niej wytycznych.
5. Osobami właściwymi do kontaktu w sprawach dotyczących Porozumienia są:

Ze strony Odbiorcy: efaktura.info@orlen.pl

Ze strony Wystawcy: [#]

1. Podpisane przez Wystawcę Porozumienie należy odesłać na adres Odbiorcy z dopiskiem „Porozumienie e-faktura zakupu”.

|  |  |
| --- | --- |
| **Odbiorca** | **Wystawca** |
| *podpis osoby uprawnionej* | *podpis osoby uprawnionej* |

**Instrukcja przesyłania faktur w formie elektronicznej do ORLEN S.A.**

**Definicje**

**e-faktura** - faktura, faktura korygująca, duplikat faktury, nota księgowa w formie dokumentu elektronicznego, który spełnia wymogi określone w przepisach prawa dotyczących sposobu przesyłania i zasad przechowywania faktur w formie elektronicznej;

**Odbiorca** - ORLEN S.A.;

**Wystawca** - podmiot, u którego ORLEN S.A. dokonuje zakupu i który wystawia dokumenty w formie elektronicznej;

**Porozumienie** - dokument wyrażający akceptację Odbiorcy na przesyłanie mu e-faktur;

**Postanowienia ogólne**

1. Niniejsza Instrukcja określa zasady przesyłania e-faktur przez Wystawcę do Odbiorcy.
2. Warunkiem korzystania przez Wystawcę z możliwości wysyłania e-faktur do Odbiorcy jest łączne spełnienie wymogów opisanych poniżej:
3. otrzymanie zaakceptowanego przez Odbiorcę Porozumienia z Wystawcą na przesyłanie e-faktur,
4. zastosowanie się do wymogów opisanych poniżej w niniejszej Instrukcji.

**Warunki przesyłania faktur elektronicznych**

1. E-faktury powinny być wysyłane wyłącznie w postaci plików w formacie PDF. Faktury w innych formatach nie zostaną przyjęte przez Odbiorcę.
2. E-faktury powinny być wysyłane z adresu lub adresów zadeklarowanych przez Wystawcę w Porozumieniu.

E-faktury wysłane z innych adresów, bez wcześniejszego poinformowania o tym Odbiorcy, nie zostaną przyjęte przez Odbiorcę.

1. E-faktury powinny być wysyłane na adres: [**efaktura@orlen.pl**](mailto:faktura@orlen.pl)
2. E-faktury powinny być przesyłane w stosunku 1:1, przez co rozumie się jeden załącznik z fakturą dołączony do jednej wiadomości e-mail.
3. Wszelkie załączniki (protokoły wykonania usług, wydania w-z, specyfikacje techniczne itp.) powinny stanowić kolejne strony pliku z fakturą, nie przekraczającego 10 MB.
4. **Niedopuszczalne** jest dołączanie do wiadomości e-mail, zwłaszcza w stopce, innych plików graficznych (np. JPEG, TIF, BMP). Wiadomość zawierająca oprócz pliku PDF inny plik w w/w formacie nie zostanie przyjęta przez Odbiorcę. Pliki nie powinny być skompresowane, np. w formacie .ZIP, ani być zamieszczane pośrednio w wiadomości będącej załącznikiem innej wiadomości.
5. Wiadomości e-mail powinny zawierać w temacie odpowiednie zapisy umożliwiające identyfikację nr dokumentu.
6. Na adres zadeklarowany przez Wystawcę w Porozumieniu Odbiorca może wysłać e-mail potwierdzający odbiór faktury. W przypadku zadeklarowania przez wystawcę kilku adresów, z których będą wpływały e-faktury, Wystawca powinien wskazać w Porozumieniu jeden adres, na który będą wysyłane potwierdzenia przez Odbiorcę.
7. Każdorazowa zmiana adresu lub adresów, o którym mowa w pkt. 2 i 4 Porozumienia, wymaga poinformowania Odbiorcy o tym fakcie mailem przesłanym na adres wskazany w pkt. 9 Porozumienia.
8. Odbiorca nie przyjmuje e-faktur wystawianych za pośrednictwem portali internetowych i nie przesyłanych automatycznie w postaci plików PDF na adres: [**efaktura@orlen.pl.**](mailto:faktura@orlen.pl)

W przypadku stosowania powyższego rozwiązania Wystawca zobowiązany jest do zapewnienia automatycznego przesyłania e-faktur, bądź przesłania e-faktur po uprzednim ich pobraniu z portalu.

1. Wystawca jest zobowiązany do archiwizowania kopii e-faktur, w postaci wysłanych plików PDF stanowiących dla Odbiorcy podstawę do obniżenia podatku VAT należnego o kwotę podatku VAT naliczonego. W razie niedopełnienia powyższego wymogu, lub w razie gdyby archiwizowana przez Wystawcę kopia e-faktury była nieprawidłowa ze względów formalnych, prawnych lub rzeczowych, Wystawca zobowiązany jest do wyrównania Odbiorcy szkody powstałej w wyniku wymierzenia Odbiorcy przez organ podatkowy zobowiązania podatkowego, wraz z sankcjami i odsetkami w kwotach wynikających z decyzji tego organu.
2. Wystawca zobowiązuje się do archiwizowania kopii e-faktur, o których mowa w pkt. 13 powyżej zgodnie z powszechnie obowiązującymi przepisami prawa podatkowego w tym zakresie.

**Postanowienia końcowe**

1. Przesyłanie e-faktur przez Wystawcę może nastąpić już w kolejnym dniu roboczym po otrzymaniu od Odbiorcy zaakceptowanego Porozumienia.
2. Akceptacja elektronicznej formy przesyłania faktur może zostać wycofana przez Odbiorcę w każdym momencie, w szczególności w przypadku nie stosowania przez Wystawcę postanowień niniejszej Instrukcji.

Cofnięcie akceptacji nastąpi poprzez wysłanie przez Odbiorcę pisma na adres e-mail Wystawcy zadeklarowany w punkcie 4 i 2 Porozumienia.

1. Wystawca może zrezygnować z przesyłania e-faktur, informując o tym Odbiorcę mailem przesłanym na adres wskazany w pkt. 9 Porozumienia.
2. Pytania i wątpliwości proszę kierować na adres u Odbiorcy wskazany w punkcie 9 Porozumienia.

**Załącznik nr 11 do Umowy WDROŻENIOWEJ [Odbiory i wzory protokołów odbioru]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# PROCEDURY ODBIORU

**[Postanowienia ogólne]**

* 1. Odbiory polegają na weryfikacji, czy przedmiot Odbioru został wykonany należycie, w tym czy spełnia wymagania określone w Umowie i Dokumencie Koncepcji Biznesowej i Technicznej.
  2. Odbiorom podlegają Etapy.
  3. Po przeprowadzeniu procedury Odbioru Zamawiający może:
     1. dokonać Odbioru – poprzez podpisanie Protokołu Odbioru;
     2. dokonać Odbioru z zastrzeżeniami – poprzez podpisanie Protokołu Odbioru z zastrzeżeniami, wraz ze wskazaniem zgłaszanych zastrzeżeń, jeśli dany przedmiot Odbioru nie spełnia kryteriów Odbioru które, w ocenie Zamawiającego, nie uniemożliwiają lub znacząco nie utrudniają korzystanie z przedmiotu Odbioru;
     3. odmówić dokonania Odbioru – poprzez podpisanie Protokołu Rozbieżności wraz ze wskazaniem rozbieżności wstrzymujących Odbiór, jeśli dany przedmiot Odbioru nie spełnia kryteriów Odbioru.
  4. Protokoły Odbioru oraz Protokoły Rozbieżności są sporządzane w formie pisemnej pod rygorem nieważności zgodnie ze wzorami wskazanymi poniżej.
  5. Zamawiający ma prawo do weryfikacji należytego wykonania przedmiotu Odbioru dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. W szczególności uzgodnienie przez Strony scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami.
  6. Odbiory są czynnościami jednostronnie dokonywanymi przez Zamawiającego. Protokoły Odbioru Etapów są podpisywane przez Kierownika Projektu, po akceptacji zrealizowanego Etapu przez członków Komitetu Sterującego ze strony Zamawiającego.
  7. Za datę Odbioru uważa się datę podpisania odpowiedniego Protokołu Odbioru, chyba że inna data została wskazana w samym Protokole Odbioru.
  8. Sporządza się każdorazowo dwa Protokoły Odbioru – po jednym dla każdej ze Stron.
  9. Dokonanie Odbioru nie wpływa na możliwość skorzystania przez Zamawiającego z uprawnień przysługujących mu na mocy przepisów prawa lub Umowy w przypadku nienależytego Etapu, a w szczególności na prawo naliczenia kar umownych, dochodzenia odszkodowań oraz odstąpienia od Umowy, jeżeli fakt nienależytego wykonania Umowy zostanie ujawniony po dokonaniu Odbioru.
  10. Strony potwierdzają, że Odbiory Produktów, Faz oraz Etapów I – V (lub I – IV w przypadku decyzji Zamawiającego o braku realizacji opcjonalnego Etapu VI). nie stanowią odbiorów w rozumieniu przepisów Kodeksu cywilnego o umowie o dzieło, a mają jedynie charakter roboczej weryfikacji poprawności postępu prac w ramach Wdrożenia. Odbiór Końcowy stanowi natomiast odbiór dzieła w rozumieniu art. 643 Kodeksu cywilnego.

**[Procedura Odbioru Etapów]**

* 1. Po wykonaniu Etapu, wykonana zostanie następująca procedura Odbioru Etapu:
     1. Wykonawca przedstawi Zamawiającemu do Odbioru Etap, w terminie wynikającym z uzgodnionego Harmonogramu;
     2. Zamawiający, w terminie do 10 Dni Roboczych od daty przedstawienia Etapu do Odbioru, zweryfikuje Etap pod kątem jego zgodności z Umową oraz Dokumentem Koncepcji Biznesowej i Technicznej. Wynik weryfikacji zostanie sformułowany w postaci Protokołu Odbioru / Protokołu Odbioru z zastrzeżeniami lub w postaci Protokołu Rozbieżności;
     3. jeżeli w przeciągu 10 Dni Roboczych od przedstawienia Etapu do Odbioru Zamawiający nie przekaże Wykonawcy odpowiednio Protokołu Odbioru, Protokołu Odbioru z zastrzeżeniami lub Protokołu Rozbieżności, Wykonawca przekaże Kierownikowi Projektu ze strony Zamawiającego wezwanie do potwierdzenia braku uwag do Produktu i podpisania Protokołu Odbioru. Zamawiający jest uprawniony do dostarczenia Wykonawcy podpisanego Protokołu Odbioru, Protokołu Odbioru z zastrzeżeniami lub Protokołu Rozbieżności w terminie do 10 Dni Roboczych od wezwania;
     4. w przypadku wskazania przez Zamawiającego, odpowiednio, zastrzeżeń lub rozbieżności, Wykonawca poprawi lub uzupełni Etap o wszystkie kwestie wskazane przez Zamawiającego, odpowiednio, w Protokole Odbioru z zastrzeżeniami lub w Protokole Rozbieżności. W przypadku wątpliwości co do zasadności wskazania przez Zamawiającego określonej kwestii jako zastrzeżenia lub rozbieżności – na Wykonawcy spoczywa obowiązek uzasadnienia swojego stanowiska w oparciu o kryteria zgodności Etapu z Umową lub Dokumentem Koncepcji Biznesowej i Technicznej, stanowiące podstawę oceny jakości. W celu uniknięcia wątpliwości Strony potwierdzają, że uzasadnienie stanowiska Wykonawcy nie wpływa na terminy, o których mowa w pkt. 2.11.5. oraz 2.11.6. poniżej;
     5. w przypadku podpisania przez Zamawiającego Protokołu Rozbieżności:
  2. prace związane z poprawą lub uzupełnieniem Produktu o zgłoszone w Protokole Rozbieżności uwagi Zamawiającego, Wykonawca wykona w wyznaczonym terminie, nie dłuższym niż 10 Dni Roboczych od dnia otrzymania Protokołu Rozbieżności. Po wprowadzeniu wymaganych korekt i uzupełnień do Etapu Wykonawca ponownie przedstawi Etap do Odbioru zgodnie z niniejszą procedurą;
  3. jeśli w drugiej iteracji (po wprowadzeniu korekt, o których mowa w pkt. 2.11.5. powyżej) Protokół Odbioru Etapu nie zostanie podpisany, kwestia niezgodności Etapu będzie przedmiotem eskalacji na obrady Komitetu Sterującego;
     1. w przypadku podpisania przez Zamawiającego Protokołu Odbioru z zastrzeżeniami:

1. prace związane z poprawą lub uzupełnieniem Etapu o zgłoszone w Protokole Odbioru z zastrzeżeniami uwagi Zamawiającego, Wykonawca wykona w terminie wskazanym przez Zamawiającego (jednak nie później niż do dnia Odbioru następnego Etapu, chyba że dotyczy to ostatniego z Etapów – w takiej sytuacji Zamawiający wyznaczy maksymalny termin na wykonanie prac związanych z poprawa lub uzupełnieniem, jednak nie krótszy niż 10 Dni Roboczych), a następnie przedstawi Zamawiającemu Etap do ponownej weryfikacji. Usunięcie wszystkich nieprawidłowości Etapu wskazanych w Protokole Odbioru z zastrzeżeniami najpóźniej do dnia Odbioru następnego Etapu (lub w terminie wskazanym przez Zamawiającego w przypadku ostatniego z Etapów ) jest jednym z kryteriów Odbioru następnego (lub ostatniego) Etapu.
   1. W celu uniknięcia wątpliwości, Fazy nie podlegają odrębnym Odbiorom, niemniej wykonywana jest kontrola jakości wykonania danej Fazy ukierunkowana na weryfikację stopnia zgodności osiągnięcia celów określonych w Umowie oraz w Dokumencie Koncepcji Biznesowej i Technicznej z poziomem oczekiwanym na koniec danej Fazy, wyrażonym zestawem odpowiednio sformułowanych poniżej kryteriów. Wykonanie wszystkich Produktów w ramach Fazy jest warunkiem koniecznym, ale niewystarczającym do uznania Fazy za pozytywnie zakończoną, a w konsekwencji dokonania Odbioru Etapu, który je obejmuje.
   2. Każdy Etap uznany zostanie za kwalifikujący się do Odbioru, jeśli spełnione zostaną łącznie następujące kryteria akceptacji Fazy:
      1. w odniesieniu do wszystkich Produktów przewidzianych do wykonania / dostarczenia w ramach Fazy – zostały one dostarczone i wykonane ;
      2. wszystkie testy Systemu wykonywane lub przewidziane do wykonania w ramach Fazy, zostały pozytywnie zakończone w całości;
      3. spełnione są wszystkie dodatkowe kryteria akceptacji Fazy uzgodnione przez Strony w Umowie i w trakcie realizacji Umowy.
   3. Każdorazowo test akceptacyjny Systemu gotowego do Startu Produkcyjnego uważa się za pozytywnie zakończony, o ile System pozbawiony jest jakichkolwiek Nieprawidłowości albo spełnione zostaną następujące maksymalne kryteria ilościowe dotyczące wykrytych Nieprawidłowości (obowiązujące łącznie):
2. nie więcej niż 0 (zero) Awarii,
3. nie więcej niż 5 (pięć) Błędów,
4. nie więcej niż 10 (dziesięć) Usterek.
   1. W przypadku braku Nieprawidłowości albo spełnienia powyższych kryteriów ilościowych Zamawiający dokonuje Odbioru danego Etapu poprzez podpisanie Protokołu Odbioru (przy czym w przypadku Systemu posiadającego Nieprawidłowości w liczbie nieprzekraczającej powyższych kryteriów ilościowych jest to Odbiór z zastrzeżeniami). Po dokonaniu Odbioru (z zastrzeżeniami)Etapu, w którym System posiada Nieprawidłowości, Wykonawca jest zobowiązany usunąć wszystkie Nieprawidłowości Systemu w terminie wskazanym przez Zamawiającego (jednak nie później niż do dnia kolejnego Etapu, a w przypadku ostatniego z Etapów – w terminie ustalonym przez Strony, nie dłuższym jednak niż 10 Dni Roboczych) a następnie przedstawić System do weryfikacji (z zastrzeżeniem, że ponowne testy będą prowadzone tak, by możliwe było stwierdzenie występowania ewentualnych Nieprawidłowości, jakie mogły pojawić się w testowanym Systemie w trakcie procesu usuwania wcześniej istniejących Nieprawidłowości  tzw. test regresji).

**[Procedura Odbioru Fazy III – Stabilizacja]**

* 1. Faza V ( Stabilizacja), uznana zostanie za kwalifikującą się do zaakceptowania w ramach Odbioru Etapu, jeśli spełnione zostaną kryteria wskazane w pkt. 2.13. powyżej oraz usunięto wszystkie Nieprawidłowości Systemu, będącego przedmiotem Odbioru w ramach Etapu, który odebrano z zastrzeżeniami i który posiadał Nieprawidłowości w liczbie nieprzekraczającej kryteriów ilościowych wskazanych w pkt. 2.14. powyżej.
  2. Z zastrzeżeniem postanowień powyższych, System może zostać uznany za stabilny w środowisku Zamawiającego, wyłącznie w przypadku, gdy na koniec Fazy VI (Stabilizacja) liczba Nieprawidłowości będzie wynosić (łącznie):

1. 0 (zero) Awarii,
2. 0 (zero) Błędów,
3. 0 (zero) Usterek,

dalej również jako „**Stan Stabilności**”.

**[Procedura Odbioru Końcowego]**

* 1. Odbiór ostatniego z Etapów w ramach Wdrożenia jest jednoznaczny z dokonaniem Odbioru Końcowego.

**PROTOKÓŁ ODBIORU**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Protokół Odbioru Etapu** | | | | |
| Data: |  | Miejsce: | |  |
| Zamawiający: |  | | | |
| Wykonawca: |  | | | |
| Nazwa Systemu: |  | | | |
| Wersja Systemu: |  | | | |
| Data rozpoczęcia: |  | Data zakończenia: | |  |
| Wykonany Etap: | | | | |
| Zamawiający potwierdza należyte wykonanie Etapu. | | | | |
| Czy Zamawiający zgłasza zastrzeżenia: | | | | |
| ***TAK\**** | | | ***NIE\**** | |
| Lista zgłaszanych zastrzeżeń (w przypadku oznaczenia „TAK” w poprzedniej kolumnie): | | | | |
| Termin na usunięcie zastrzeżeń: | | | | |
| Podpisy: | | | | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Imię i nazwisko  *Kierownik Projektu Zamawiającego* | | | | |

\*niepotrzebne skreślić

**PROTOKÓŁ ROZBIEŻNOŚCI**

|  |  |  |  |
| --- | --- | --- | --- |
| **Protokół rozbieżności Etapu** | | | |
| Data: |  | Miejsce: |  |
| Zamawiający: |  | | |
| Wykonawca: |  | | |
| Nazwa Systemu: |  | | |
| Wersja Systemu: |  | | |
| Data rozpoczęcia: |  | Data zakończenia: |  |
| Wykonany Etap: | | | |
|  | | | |
| Lista rozbieżności do usunięcia przez Wykonawcę: | | | |
| Termin na usunięcie rozbieżności: | | | |
| Podpisy: | | | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Imię i nazwisko  *Kierownik Projektu Zamawiającego* | | | |

\*niepotrzebne skreślić

**Załącznik nr 12 do UMOWY WDROŻENIOWEJ [LISTA I WARUNKI KORZYSTANIA Z UTWORÓW OSÓB TRZECICH**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# LISTA I WARUNKI KORZYSTANIA Z UTWORÓW OSÓB TRZECICH

**Załącznik nr 13 do UMOWY WDROŻENIOWEJ [PROTOKÓŁ AKCEPTACJI]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# PROTOKÓŁ AKCEPTACJI

**PROTOKÓŁ AKCEPTACJI**

|  |  |  |  |
| --- | --- | --- | --- |
| **Protokół Akceptacji** | | | |
| Data: |  | Miejsce: |  |
| Zamawiający: | ORLEN S.A. | | |
| Wykonawca: |  | | |
| Nazwa Systemu: |  | | |
| Wersja Systemu: |  | | |
| Data rozpoczęcia: |  | Data zakończenia: |  |
| Wykonane Zlecenie : | | | |
| Zamawiający potwierdza należyte wykonanie Zlecenia. | | | |
| Uwagi: | | | |
| PODPIS:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Imię i nazwisko  Przedstawiciel Zamawiającego | | | |

## 

**Załącznik nr 14 do UMOWY WDROŻENIOWEJ [REGULACJE ZAMAWIAJĄCEGO]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, Strony nadają następujące znaczenie:

# TAJEMNICA PRZEDSIĘBIORSTWA I TAJEMNICA SPÓŁKI ORLEN S.A.

**I. Tajemnica Przedsiębiorstwa**

## Wykonawca zobowiązuje się do zachowania w tajemnicy informacji przekazanych bezpośrednio lub pośrednio przez Zamawiającego (w jakiejkolwiek formie tj. w szczególności ustnej, pisemnej, elektronicznej), a także informacji uzyskanych przez Wykonawcę w inny sposób w trakcie wzajemnej współpracy, w tym w związku z zawarciem i realizacją Umowy, które to informacje dotyczą bezpośrednio lub pośrednio Zamawiającego, spółek z Grupy ORLEN lub ich kontrahentów, w tym treści Umowy. Strony przyjmują, że wszelkie informacje techniczne, technologiczne, organizacyjne lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, co do których Zamawiający, jako podmiot uprawniony do korzystania z ww. informacji i rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności, przekazane przez Zamawiającego lub w jego imieniu lub uzyskane przez Wykonawcę w inny sposób w trakcie negocjowania, zawarcia i wykonywania Umowy należy traktować jako tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji (dalej: „**Tajemnica Przedsiębiorstwa**”), chyba że w chwili przekazania, osoba przekazująca określi na piśmie lub w formie elektronicznej odmienny, od określonego powyżej, charakter takich informacji.

## Przez zobowiązanie do zachowania w tajemnicy informacji wskazanych w pkt. 2.1. powyżej, Strony rozumieją zakaz wykorzystywania, ujawniania oraz przekazywania tych informacji w jakikolwiek sposób oraz jakimkolwiek osobom trzecim, za wyjątkiem następujących sytuacji:

## ujawnienie lub wykorzystanie informacji jest konieczne do prawidłowego wykonania Umowy i zgodne z tą Umową lub

## informacje w chwili ich ujawnienia są już publicznie dostępne, a ich ujawnienie zostało dokonane przez Zamawiającego lub za jego zgodą lub w sposób inny niż poprzez niezgodne z prawem lub jakąkolwiek umową działanie lub zaniechanie lub

## Wykonawca został zobowiązany do ujawnienia informacji przez sąd lub uprawniony organ lub w przypadku prawnego obowiązku takiego ujawnienia, z zastrzeżeniem, że Wykonawca, niezwłocznie pisemnie poinformuje Zamawiającego o obowiązku ujawniania informacji i ich zakresie, a także uwzględni, w miarę możliwości, rekomendacje Zamawiającego co do ujawniania informacji, w szczególności w zakresie złożenia wniosku o wyłączenie jawności, zasadności złożenia stosownego środka zaskarżenia, odwołania lub innego równoważnego środka prawnego oraz poinformuje sąd lub uprawniony organ o chronionym charakterze przekazanych informacji lub

## Zamawiający wyraził Wykonawcy pisemną zgodę na ujawnienie lub wykorzystanie informacji w określonym celu, we wskazany przez Zamawiającego sposób.

## Wykonawca zobowiązany jest przedsięwziąć takie środki bezpieczeństwa i sposoby postępowania, jakie będą odpowiednie i wystarczające, dla zapewnienia bezpiecznego, w tym zgodnego z Umową i przepisami prawa, przetwarzania Tajemnicy Przedsiębiorstwa, aby zapobiec jakiemukolwiek nieautoryzowanemu wykorzystaniu, przekazaniu, ujawnieniu, czy dostępowi do tych informacji. Wykonawca nie będzie, w szczególności kopiował lub utrwalał Tajemnicy Przedsiębiorstwa, jeżeli nie będzie to uzasadnione należytym wykonaniem przez Wykonawcę Umowy. Wykonawca zobowiązany jest do niezwłocznego powiadomienia Zamawiającego o zaistniałych naruszeniach zasad ochrony lub nieuprawnionym ujawnieniu lub wykorzystaniu Tajemnicy Przedsiębiorstwa przetwarzanej w związku z realizacją niniejszej umowy.

## Obowiązek zachowania w tajemnicy informacji, o których mowa w pkt. 2.1. powyżej rozciąga się również na pracowników Wykonawcy i inne osoby, w tym w szczególności audytorów, doradców i podwykonawców, którym Wykonawca udostępni takie informacje. Wykonawca zobowiązany jest do zobowiązania na piśmie ww. osób do ochrony Tajemnicy Przedsiębiorstwa na warunkach, co najmniej takich jak określone w Umowie. Wykonawca ponosi pełną odpowiedzialność za działania lub zaniechania osób, które uzyskały dostęp do Tajemnicy Przedsiębiorstwa, w tym odpowiedzialność, o której mowa w pkt. 2.8. poniżej.

## Wykonawca zobowiązany jest na każde żądanie Zamawiającego, w terminie nie dłuższym niż 5 dni, przesłać Zamawiającemu listę osób i podmiotów, które za pośrednictwem Wykonawcy uzyskały dostęp do Tajemnicy Przedsiębiorstwa. Niewywiązanie się z obowiązku, o którym mowa w niniejszym punkcie będzie traktowane jako nieuprawnione ujawnienie Tajemnicy Przedsiębiorstwa skutkujące odpowiedzialnością, o której mowa w pkt. 2.8. poniżej.

## Zobowiązanie do zachowania w tajemnicy informacji wiąże w czasie obowiązywania Umowy, jak również w okresie 10 lat po jej rozwiązaniu, wygaśnięciu lub uchyleniu bądź zniweczeniu skutków prawnych. Jeżeli mimo upływu, wskazanego w zdaniu poprzednim, okresu ochrony Tajemnicy Przedsiębiorstwa, informacje te nadal podlegają ochronie w oparciu o wewnętrzne regulacje lub decyzje Zamawiającego lub w oparciu o szczególne przepisy prawa, Zamawiający powiadomi Wykonawcę na piśmie, o przedłużeniu okresu ochrony, o dodatkowy wskazany przez Zamawiającego okres (nie dłuższy jednak niż 10 lat), na co Wykonawca niniejszym wyraża zgodę. Powiadomienie, o którym mowa w zdaniu powyższym, nastąpi przed wygaśnięciem 10-cio letniego okresu ochrony, o którym mowa w zdaniu pierwszym niniejszego ustępu, nie później jednak niż na 10 Dni Roboczych przed zakończeniem obowiązywania powyższego zobowiązania. Strony zgodnie postanawiają, że zobowiązanie opisane w niniejszym ustępie obowiązuje niezależnie od rozwiązania, wygaśnięcia lub uchylenia bądź zniweczenia skutków prawnych Umowy.

## Nie później niż w terminie 3 Dni Roboczych po upływie okresu ochrony, o którym mowa w pkt. 2.6. powyżej Wykonawca oraz wszelkie osoby, którym Wykonawca przekazał Tajemnicę Przedsiębiorstwa zobowiązane są zwrócić Zamawiającemu lub zniszczyć wszelkie materiały ją zawierające.

## W przypadku nieuprawnionego wykorzystania, przekazania lub ujawnienia przez Wykonawcę Tajemnicy Przedsiębiorstwa, Zamawiający uprawniony jest do żądania od Wykonawcy zapłaty kary umownej w wysokości 100.000,00 zł za każdy przypadek nieuprawnionego wykorzystania, przekazania lub ujawnienia ww. informacji. Zapłata kary umownej wskazanej powyżej nie ogranicza prawa Zamawiającego do dochodzenia od Wykonawcy odszkodowania na zasadach ogólnych w przypadku, gdy wysokość poniesionej szkody przewyższa zastrzeżoną w Umowie wysokość kary umownej. Powyższe nie wyłącza w żaden sposób innych sankcji i uprawnień Zamawiającego określonych w przepisach prawa, w tym w ustawie z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji.

## W przypadku, gdy w trakcie realizacji Umowy, zaistnieje konieczność dostępu lub przekazania Wykonawcy, w jakiejkolwiek formie, informacji stanowiących Tajemnicę Spółki ORLEN S.A. rozumianej jako szczególnie chroniony rodzaj Tajemnicy Przedsiębiorstwa Zamawiającego, co do której podjęto szczególne działania określone w aktach wewnętrznych Zamawiającego, w celu zachowania jej w tajemnicy i której wykorzystanie, przekazanie lub ujawnienie osobie nieuprawnionej w znacznym stopniu zagraża lub narusza interesy Zamawiającego, Wykonawca zobowiązuje się do stosowania zasad i warunków ochrony Tajemnicy Spółki ORLEN S.A. określonych w punkcie II.

## Dla uniknięcia wątpliwości Strony potwierdzają, że Wykonawca, niezależnie od obowiązków określonych w Umowie, zobowiązany jest także do przestrzegania dodatkowych wymogów dotyczących ochrony określonych rodzajów informacji (np. danych osobowych, informacji poufnych) wynikających z obowiązujących przepisów prawa.

## Wykonawca zobowiązany jest do wypełnienia, w imieniu Zamawiającego jako Administratora danych w rozumieniu obowiązujących przepisów prawa o ochronie danych osobowych, niezwłocznie, jednakże nie później niż w terminie 30 (trzydzieści) dni od dnia zawarcia Umowy z Zamawiającym, obowiązku informacyjnego wobec osób fizycznych zatrudnionych przez Wykonawcę lub współpracujących z Wykonawcą przy zawarciu lub realizacji Umowy – bez względu na podstawę prawną tej współpracy – których dane osobowe udostępnione zostały Zamawiającemu przez Wykonawcę w związku z zawarciem lub realizacją Umowy. Obowiązek, o którym mowa w zdaniu poprzedzającym, powinien zostać spełniony poprzez przekazanie tym osobom klauzuli informacyjnej zawartej w Dodatku nr 3 do niniejszego Załącznika [**Klauzula informacyjna**], przy jednoczesnym zachowaniu zasady rozliczalności.

**II. Tajemnica Spółki ORLEN S.A.**

## Wykonawca przyjmuje do wiadomości, że informacje oznaczone klauzulą „Tajemnica Spółki” lub „Tajemnica Spółki ORLEN S.A.” stanowią szczególnie chroniony, kwalifikowany rodzaj Tajemnicy Przedsiębiorstwa, co do których podjęto szczególne działania określone w aktach wewnętrznych Zamawiającego, w celu zachowania ich w tajemnicy i których wykorzystanie, przekazanie lub ujawnienie, w całości lub choćby w części, osobie nieuprawnionej, w znacznym stopniu zagraża lub narusza istotne interesy Zamawiającego (dalej: „**Tajemnica Spółki ORLEN S.A.**”).

## Za informacje stanowiące Tajemnicę Spółki ORLEN S.A., uważa się również nieoznaczone informacje przetwarzane w systemach informatycznych lub teleinformatycznych, o których Zamawiający poinformuje Wykonawcę w formie pisemnej lub elektronicznej, że stanowią one Tajemnicę Spółki ORLEN S.A.

## Wykonawca będzie zobowiązany do stosowania do Tajemnicy Spółki PKN ORLEN S.A. oprócz postanowień rozdziału I (Tajemnica Przedsiębiorstwa), także postanowień niniejszego rozdziału II (Tajemnica Spółki ORLEN S.A.). W razie rozbieżności pomiędzy postanowieniami regulującymi zasady ochrony Tajemnicy Przedsiębiorstwa a postanowieniami dotyczącymi Tajemnicy Spółki ORLEN S.A., rozstrzygające znaczenie mają postanowienia przewidujące dalej idącą ochronę.

## Wykonawca niezwłocznie, jednakże nie później niż w terminie 5 Dni Roboczych od zawarcia Umowy, zobowiązany jest do przekazania Zamawiającego jednego egzemplarza wykazu osób, którego wzór stanowi Dodatek nr 1 do niniejszego Załącznika oraz oświadczeń podpisanych przez osoby wskazane w wykazie, których wzór stanowi Dodatek nr 2 do niniejszego Załącznika.

## Wykonawca zobowiązany jest do zapoznania osób, o których mowa w pkt. 2.15. powyżej z zasadami ochrony Tajemnicy Spółki ORLEN S.A. obowiązującymi u Zamawiającego, w uzgodnionej pomiędzy Stronami formie i terminie, ale nie później niż przed rozpoczęciem przetwarzania Tajemnicy Spółki ORLEN S.A.

## Wykonawca zobowiązany jest uzyskać uprzednią pisemną zgodę Zamawiającego na udostępnienie Tajemnicy Spółki ORLEN S.A. osobom trzecim.

## Wykonawca nie jest uprawniony do kopiowania materiałów przekazanych przez Zamawiającego i zawierających Tajemnicę Spółki ORLEN S.A., bez uzyskania uprzedniej pisemnej zgody Zamawiającego.

## Nie później niż w terminie 3 miesięcy po rozwiązaniu, wygaśnięciu lub uchyleniu bądź zniweczeniu skutków prawnych Umowy Wykonawca oraz wszelkie osoby, którym Wykonawca przekazał Tajemnicę Spółki ORLEN S.A. zobowiązane są zwrócić Zamawiającemu lub zniszczyć wszelkie dokumenty, nośniki i pliki ją zawierające oraz przedstawić stosowne oświadczenie o dokonaniu zniszczenia lub zwrotu wszystkich powyższych materiałów. Powyższy obowiązek nie będzie dotyczyć informacji, których przetwarzanie jest niezbędne do wykonywania obowiązków wynikających z bezwzględnie obowiązujących przepisów prawa.

## Wykonawca nie jest uprawniony do oznaczania materiałów zawierających Tajemnicę Spółki ORLEN S.A. innymi niż „TAJEMNICA SPÓŁKI ORLEN S.A.” klauzulami lub oznaczeniami.

## Za każdorazowe naruszenie wynikających z Umowy obowiązków dotyczących ochrony informacji stanowiących Tajemnicę Spółki ORLEN S.A., Zamawiający uprawniony jest do żądania od Wykonawcy zapłaty kary umownej w wysokości 100.000,00 zł za każdy przypadek nieuprawnionego wykorzystania, przekazania lub ujawnienia ww. informacji. Zapłata kary umownej wskazanej powyżej nie ogranicza prawa Zamawiającego do dochodzenia od Wykonawcy odszkodowania na zasadach ogólnych w przypadku, gdy wysokość poniesionej szkody przewyższa zastrzeżoną w Umowie wysokość kary umownej. Powyższe nie wyłącza w żaden sposób innych sankcji i uprawnień Zamawiającego określonych w Umowie oraz przepisach prawa, w tym w ustawie z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji.

## W przypadkach konieczności wymiany materiałów zawierających Tajemnicę Spółki ORLEN S.A. w formie elektronicznej zastosowanie znajdują zasady postępowania określone w Rozdziale 3 poniżej.

# ZASADY POSTĘPOWANIA W ZAKRESIE WYMIANY INFORMACJI STANOWIĄCYCH TAJEMNICĘ SPÓŁKI ORLEN S.A. W FORMIE ELEKTRONICZNEJ

## W przypadkach podyktowanych koniecznością szybkiej wymiany informacji stanowiących Tajemnicę Spółki ORLEN S.A. w formie elektronicznej, Zamawiający dopuszcza możliwość przekazywania ich za pośrednictwem poczty elektronicznej, wyłącznie w formie załączników, z uwzględnieniem poniższych zasad wynikających z polityki bezpieczeństwa informacji obowiązującej u Zamawiającego:

## przetwarzane załączniki zawierające informacje stanowiące Tajemnicę Spółki ORLEN S.A. podlegają zabezpieczeniu kryptograficznemu z użyciem algorytmu AES256 lub silniejszego, uzgodnionego pomiędzy Stronami (np. oprogramowanie archiwizujące z wbudowanym algorytmem szyfrującym);

## hasło zabezpieczające (klucz szyfrujący), zapewniające ochronę przed nieuprawnionym odszyfrowaniem załącznika, składa się z co najmniej 8 (ośmiu) znaków, z jednoczesnym użyciem 3 spośród 4 grup znaków (małe litery i duże litery, cyfry i znaki specjalne);

## nadawca, po uzyskaniu od odbiorcy potwierdzenia otrzymania zabezpieczonych załączników, przekazuje odbiorcy hasło zabezpieczające (klucz szyfrujący) poprzez przesłanie go pocztą elektroniczną (email), za pośrednictwem wiadomości sms lub w drodze połączenia telefonicznego, z zachowaniem zasady nieujawniania hasła osobom nieuprawnionym;

## przesyłanie zaszyfrowanego załącznika odbywa się pomiędzy kontami pocztowymi Stron. Wykonawca zobowiązany jest do zapewnienia, aby zabezpieczenia kont pocztowych, wykorzystywanych do przesyłania zaszyfrowanych załączników, zapobiegały ich utracie i dostępowi osób nieuprawnionych.

## W przypadkach podyktowanych koniecznością wymiany informacji stanowiących Tajemnicę Spółki ORLEN S.A. w formie elektronicznej, Zamawiający dopuszcza możliwość przekazywania ich z wykorzystaniem elektronicznych nośników informacji, z uwzględnieniem poniższych zasad bezpieczeństwa wynikających z polityki bezpieczeństwa informacji obowiązującej u Zamawiającego:

## wymiana elektronicznych nośników informacji odbywa się pomiędzy upoważnionymi osobami reprezentującymi Strony;

## informacje stanowiące Tajemnicę Spółki ORLEN S.A., zapisane do postaci pliku, podlegają zabezpieczeniu kryptograficznemu z użyciem algorytmu AES256 lub silniejszego (np. oprogramowanie archiwizujące z wbudowanym algorytmem szyfrującym);

## hasło zabezpieczające (klucz szyfrujący), zapewniające ochronę przed nieuprawnionym odszyfrowaniem pliku, składa się z co najmniej 8 (ośmiu) znaków, z jednoczesnym użyciem 3 spośród 4 grup znaków (małe litery i duże litery, cyfry i znaki specjalne);

## odbiorca potwierdza nadawcy fakt otrzymania nośnika z zaszyfrowanym plikiem;

## nadawca przekazuje hasło zabezpieczające (klucz szyfrujący) odbiorcy z zachowaniem zasady nieujawniania hasła osobom nieuprawnionym;

## nadawca odpowiada za właściwe zabezpieczenie chroniące nośnik przed jego fizycznym uszkodzeniem;

## opis nośnika nie ujawnia charakteru zawartych na nim informacji.

## Wykonawca zobowiązuje się chronić własne zasoby teleinformatyczne uczestniczące bezpośrednio lub pośrednio w procesie przetwarzania informacji stanowiących Tajemnicę Spółki ORLEN S.A., przed ryzykiem wystąpienia zdarzeń mogących wpłynąć na naruszenie bezpieczeństwa informacji stanowiących Tajemnicę Spółki ORLEN S.A.

# KOMUNIKACJA ZEWNĘTRZNA

## Wykonawca zobowiązuje się uzyskać uprzednią zgodę Zamawiającego, wyrażoną w formie pisemnej pod rygorem nieważności, na zamieszczenie firmy spółki, znaku towarowego lub logo Zamawiającego na swojej stronie internetowej, liście kontrahentów, w broszurach, reklamie oraz wszelkich innych materiałach reklamowych i marketingowych. W takim przypadku, Wykonawca zobowiązuje się do przedłożenia do Zamawiającego, wraz z wnioskiem o wyrażenie zgody, projektu materiałów, w których takie dane miałyby zostać zamieszczone.

## Wykonawca zobowiązuje się również do uzyskania uprzedniej zgody Zamawiającego, wyrażonej w formie pisemnej pod rygorem nieważności, na przekazanie środkom masowego przekazu takim jak prasa, radio, TV, Internet jakichkolwiek informacji dotyczących Umowy. W takim przypadku, Wykonawca zobowiązuje się do przedłożenia do Zamawiającego, wraz z wnioskiem o wyrażenie zgody, treści informacji jaka miałaby zostać wykorzystana w środkach masowego przekazu.

## Obowiązek uzyskania zgody, o której mowa w pkt. 4.1. i pkt. 4.2. powyżej, nie dotyczy:

## przypadku posługiwania się przez Wykonawcę uzyskanymi od Zamawiającego listami referencyjnymi, jednakże brak obowiązku uzyskania zgody obejmuje tylko i wyłącznie uprawnienie Wykonawcy do złożenia listów referencyjnych wraz z ofertą składaną przez niego oznaczonemu indywidualnie adresatowi;

## przypadku wypełniania przez Wykonawcę będącego spółką publiczną obowiązków informacyjnych wynikających z obowiązujących takie spółki przepisów prawa.

## W razie niewykonania lub nienależytego wykonania zobowiązań określonych w pkt. 4.1. i 4.2. powyżej, Zamawiający jest uprawniony do naliczenia kary umownej w wysokości 100.000,00 zł (słownie: sto tysięcy złotych) za każdy przypadek naruszenia. Zapłata kary umownej, o której mowa w zdaniu poprzedzającym, nie ogranicza prawa Zamawiającego do dochodzenia odszkodowania uzupełniającego na zasadach ogólnych, w przypadku, gdy wysokość poniesionej szkody przewyższa zastrzeżoną wysokość kary umownej.

# PRZECIWDZIAŁANIE KORUPCJI

## Każda ze Stron zaświadcza, że w związku z wykonywaniem niniejszej Umowy zachowa należytą staranność i stosować się będzie do wszystkich obowiązujących Strony przepisów prawa w zakresie przeciwdziałania korupcji wydanych przez uprawnione organy w Polsce i na terenie Unii Europejskiej, zarówno bezpośrednio, jak i działając poprzez kontrolowane lub powiązane podmioty gospodarcze Stron.

## Każda ze Stron zaświadcza, że wdrożyła procedury przeciwdziałania korupcji i konfliktowi interesów.

## Każda ze Stron dodatkowo zaświadcza, że w związku z wykonywaniem niniejszej Umowy stosować się będzie do wszystkich obowiązujących Strony wymagań i regulacji wewnętrznych odnośnie standardów etycznego postępowania, przeciwdziałania korupcji, zgodnego z prawem rozliczania transakcji, kosztów i wydatków, konfliktu interesów, wręczania i przyjmowania upominków oraz anonimowego zgłaszania i wyjaśniania nieprawidłowości, zarówno bezpośrednio, jak i działając poprzez kontrolowane lub powiązane podmioty gospodarcze Stron.

## Strony zapewniają, że w związku z zawarciem i realizacją niniejszej Umowy żadna ze Stron, ani żaden z ich właścicieli, udziałowców, akcjonariuszy, członków zarządu, dyrektorów, pracowników, podwykonawców, ani też żadna inna osoba działająca w ich imieniu, nie dokonywała, nie proponowała, ani nie obiecywała, że dokona, nie zaproponuje, ani też nie obieca, że dokona, ani nie upoważni do dokonania żadnej płatności lub innego przekazu stanowiącego korzyść finansową, ani też żadnej innej korzyści bezpośrednio lub pośrednio żadnemu z niżej wymienionych:

## członkowi zarządu, dyrektorowi, pracownikowi, ani agentowi Strony lub któregokolwiek kontrolowanego lub powiązanego podmiotu gospodarczego Stron,

## funkcjonariuszowi publicznemu, rozumianemu jako osobie fizycznej pełniącej funkcję publiczną w znaczeniu nadanym temu pojęciu w systemie prawnym kraju, w którym dochodzi do realizacji niniejszej Umowy, lub w którym znajdują się zarejestrowane siedziby Stron lub któregokolwiek kontrolowanego lub powiązanego podmiotu gospodarczego Stron;

## partii politycznej, członkowi partii politycznej, ani kandydatowi na urząd państwowy;

## agentowi ani pośrednikowi w zamian za opłacenie kogokolwiek z wyżej wymienionych; ani też

## innej osobie lub podmiotowi – w celu uzyskania ich decyzji, wpływu lub działań mogących skutkować jakimkolwiek niezgodnym z prawem uprzywilejowaniem lub też w dowolnym innym niewłaściwym celu, jeżeli działanie takie narusza lub naruszałoby przepisy prawa w zakresie przeciwdziałania korupcji wydane przez uprawnione organy w Polsce i na terenie Unii Europejskiej, zarówno bezpośrednio, jak i działając poprzez kontrolowane lub powiązane podmioty gospodarcze Stron.

## Strony są zobowiązane do niezwłocznego wzajemnego informowania się o każdym przypadku naruszenia postanowień niniejszej klauzuli antykorupcyjnej. Na pisemny wniosek każdej ze Stron, druga Strona niezwłocznie dostarczy informacje i udzieli odpowiedzi na uzasadnione pytania, które dotyczyć będą wykonywania niniejszej Umowy w zakresie zgodności z postanowieniami niniejszej klauzuli antykorupcyjnej.

## Każda ze Stron zaświadcza, iż w okresie realizacji niniejszej Umowy zapewnia każdej osobie działającej w dobrej wierze możliwość zgłaszania naruszeń prawa za pośrednictwem poczty elektronicznej na adres: [naruszenieprawa@orlen.pl](mailto:naruszenieprawa@orlen.pl) lub pod numerem telefonu: +48 800 322 323 – bez identyfikacji numeru osoby dzwoniącej.

## W przypadkach stwierdzenia podejrzenia działań korupcyjnych dokonanych w związku lub w celu wykonania niniejszej Umowy przez jakichkolwiek przedstawicieli każdej ze Stron, Strony zobowiązują się do współpracy w dobrej wierze w celu wyjaśnienia okoliczności dotyczących możliwych działań korupcyjnych.

# KLAUZULA SANKCYJNA

## **Oświadczenia Wykonawcy**

Wykonawca oświadcza, że zgodnie z jego najlepszą wiedzą, na dzień zawarcia Umowy zarówno on, jak i jego podmioty zależne, dominujące oraz członkowie jego organów oraz osoby działające w jego imieniu i na jego rzecz:

* + 1. pozostają w zgodności z przepisami sankcyjnymi wprowadzonymi przez Organizację Narodów Zjednoczonych, Unię Europejską, państwa członkowskie Unii Europejskiej i Europejskiego Obszaru Gospodarczego, Stany Zjednoczone Ameryki Północnej, Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej, a także inne podmioty o podobnym charakterze oraz organy działające w ich imieniu (dalej: „**Przepisy Sankcyjne**”);
    2. nie są objęte jakimikolwiek sankcjami, w tym ekonomicznymi, embargami handlowymi lub innymi środkami restrykcyjnymi nałożonymi na podstawie Przepisów Sankcyjnych oraz nie są osobami prawnymi lub fizycznymi, z którymi Przepisy Sankcyjne zabraniają przeprowadzenia transakcji (dalej: „**Podmiot Objęty Sankcjami**”);
    3. nie są bezpośrednio lub pośrednio własnością lub nie są kontrolowane przez osoby prawne lub fizyczne spełniające kryteria opisane w pkt. (ii) powyżej;
    4. nie zamieszkują lub nie posiadają siedziby lub głównego miejsca działalności w państwie objętym Przepisami Sankcyjnymi lub nie są utworzone pod prawem państwa objętego Przepisami Sankcyjnymi;
    5. nie uczestniczą w żadnym postępowaniu lub dochodzeniu prowadzonym przeciwko nim w związku z naruszeniem jakichkolwiek Przepisów Sankcyjnych.

## **Zobowiązania Wykonawcy**

Wykonawca zobowiązuje się, że w okresie obowiązywania Umowy:

zarówno on, jak i jego podmioty zależne oraz członkowie jego organów oraz osoby działające w jego imieniu i na jego rzecz będą prowadzić działalność zgodnie z Przepisami Sankcyjnymi;

jakiekolwiek przysługujące mu na podstawie Umowy wynagrodzenie nie będzie bezpośrednio lub pośrednio dostępne dla Podmiotu Objętego Sankcjami lub nie zostanie użyte do osiągnięcia korzyści przez Podmiot Objęty Sankcjami, w zakresie, w jakim takie działanie jest niedozwolone na mocy Przepisów Sankcyjnych;

wszelkie oświadczenia złożone w pkt. 6.1. pozostaną prawdziwe.

## W przypadku, gdy którekolwiek oświadczenie złożone w pkt. 6.1. stanie się nieprawdziwe, niezwłocznie, jednak nie później niż w terminie 30 dni od powzięcia o takim przypadku informacji Kontrahent poinformuje, o ile nie będzie to prawnie zakazane, ORLEN S.A. o każdym takim przypadku oraz o podjętych działaniach zmierzających do przywrócenia prawdziwości takich oświadczeń.

## W przypadku naruszenia zobowiązań określonych w pkt. 6.2. ORLEN S.A. uprawniony będzie do rozwiązania Umowy z winy Kontrahenta oraz do odszkodowania pokrywającego wszelkie szkody z tym związane.

## Ponadto, jeżeli wskutek naruszenia zobowiązań określonych w pkt. 6.1 lub pkt. 6.2 ORLEN S.A. zostanie poddany jakimkolwiek restrykcjom, sankcjom czy ograniczeniom ze strony podmiotów wymienionych w pkt. 6. 1 (i), ORLEN S.A. uprawniony będzie do odszkodowania pokrywającego wszelkie szkody związane z takimi restrykcjami, sankcjami czy ograniczeniami.

**DODATEK NR 1 [WYKAZ OSÓB Z DOSTĘPEM DO TAJEMNICY SPÓŁKI ORLEN S.A.] DO ZAŁĄCZNIKA** **nr 14 DO UMOWY WDROŻENIOWEJ [REGULACJE ZAMAWIAJĄCEGO]**

Wykaz osób, które będą miały dostęp do Tajemnicy Spółki ORLEN S.A.

WYKAZ OSÓB\* które będą miały dostęp do informacji stanowiących Tajemnicę Spółki ORLEN S.A. i/lub Tajemnicę Spółki innej Spółki, wchodzącej w skład GK ORLEN

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Dotyczy realizacji umowy nr** **[●]** **z dnia [\_]** | | | | | |
| **Lp.** | **Imię i nazwisko osoby składającej oświadczenie** | **Stanowisko osoby składającej oświadczenie**\*\* | **Firma** | **Data złożenia oświadczenia** | **Uwagi** |
| 1 | 2 | 3 | 4 | 5 | 6 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

*\* - Podmiot zewnętrzny zobowiązany jest do wskazania w wykazie wszelkich osób fizycznych, które w związku z realizacją Umowy mogą uzyskać dostęp do informacji stanowiących Tajemnicę Spółki ORLEN S.A., lub Tajemnicy Spółki innej Spółki, wchodzącej w skład GK ORLEN w tym m.in.: pracowników podmiotów zewnętrznego, podwykonawców, doradców, audytorów oraz osób świadczących usługi na podstawie umów cywilnoprawnych*

*\*\* - dotyczy osób zatrudnionych na umowę o pracę*

…………………………………………………  
Data i podpis przedstawiciela podmiotu

odpowiedzialnego za realizację Umowy z ORLEN S.A.

**Otrzymują:**

1 x komórka organizacyjna ORLEN S.A. odpowiedzialna za realizację umowy (oryginał)

1 x Podmiot zewnętrzny realizujący umowę z ORLEN S.A. (oryginał)

1 x Biuro Nadzoru nad Bezpieczeństwem Infrastruktury i Informacji (oryginał)

**DODATEK NR 2 [WZÓR OŚWIADCZENIA] DO ZałącznikA NR 14 DO UMOWY WDROŻENIOWEJ [REGULACJE ZAMAWIAJĄCEGO]**

*Wzór oświadczenia przeznaczony dla osób zatrudnionych w podmiocie zewnętrznym / świadczących usługi na rzecz podmiotu zewnętrznego o nieujawnianiu informacji stanowiących Tajemnicę Spółki ORLEN S.A. i/lub Tajemnicę Spółki innej Spółki*

.....................................................  
(miejscowość, data)

..............................................................................  
(nazwisko i imię osoby składającej oświadczenie)

....................................................................................................................................................   
(nazwa i adres siedziby podmiotu, w którym zatrudniona jest osoba składająca oświadczenie lub na rzecz którego świadczy usługi)

..............................................................................  
(zajmowane stanowisko osoby składającej oświadczenie\*)

**O Ś W I A D C Z E N I E**

W związku z wykonywaniem czynności służbowych wynikających z zawartej pomiędzy …………………………..a ORLEN S.A. Umowy nr [●]z dnia ………………..………… („Umowa”) niniejszym potwierdzam, własnoręcznym podpisem, że jestem świadomy(a) odpowiedzialności z tytułu naruszenia zasad ochrony Tajemnicy Spółki ORLEN S.A. / Tajemnicę Spółki innej Spółki wchodzącej w skład GK ORLEN\*\*, wynikających z obowiązujących przepisów prawa w tym zakresie.

Zobowiązuję się nie ujawniać, nie przekazywać oraz nie wykorzystywać informacji stanowiących Tajemnicę Spółki ORLEN S.A. / Tajemnicę Spółki innej Spółki wchodzącej w skład GK ORLEN\*\*, dla celów innych niż prawidłowe wykonanie Umowy, przez czas jej obowiązywania i okres 10 (dziesięciu) lat od jej rozwiązania, wygaśnięcia lub uchylenia bądź zniweczenia skutków prawnych, chyba że Strony określą w Umowie dłuższy okres ochrony.

........................................................................................

**(podpis osoby składającej oświadczenie)**

**Rozdzielnik:**

1 x osoba składająca oświadczenie (oryginał)

1 x komórka organizacyjna ORLEN S.A. odpowiedzialna za realizację ww. umowy (oryginał)

1 x Biuro Nadzoru nad Bezpieczeństwem Infrastruktury i Informacji (oryginał)

*\* dotyczy osób zatrudnionych na podstawie umowy o pracę*

*\*\* należy wybrać właściwy zapis w zależności od tego, czy na podstawie Umowy przekazywana będzie Tajemnica Spółki ORLEN S.A. / Tajemnica Spółki innej Spółki, wchodzącej w skład GK ORLEN*

**DODATEK NR 3 [KLAUZULA INFORMACYJNA] DO ZałącznikA NR 14 DO UMOWY WDROŻENIOWEJ [REGULACJE ZAMAWIAJĄCEGO]**

**Obraz zawierający logo, Grafika, Czcionka, czerwony

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.**

**KLAUZULA INFORMACYJNA**

**dla osób reprezentujących Wykonawcę, wskazanych do kontaktu lub współpracujących z Wykonawcą przy zawarciu i realizacji umów z ORLEN S.A.**

**Kto jest administratorem Twoich danych osobowych?**

Administratorem Twoich danych jest ORLEN S.A. z siedzibą w Płocku, ul. Chemików 7. Telefon kontaktowy: (24) 256 00 00, (24) 365 00 00, (22) 778 00 00.

**Jak możesz się skontaktować z Inspektorem Ochrony Danych?**

Możesz napisać na adres e-mail: daneosobowe@orlen.pl lub listownie na adres ORLEN S.A. z dopiskiem „Inspektor Ochrony Danych”. Więcej informacji znajdziesz na www.orlen.pl w zakładce „Kontakty”.

**Jakie dane przetwarzamy?**

W zależności od rodzaju współpracy:

* imię i nazwisko,
* stanowisko i funkcja,
* służbowy numer telefonu i e-mail,
* numer PESEL,
* informacje o uprawnieniach i kwalifikacjach.

**W jakim celu przetwarzamy dane?**

Dane są przetwarzane, aby:

* realizować umowy z Kontrahentami (np. kontakt, weryfikacja uprawnień, kwalifikacji i oświadczeń, wydawanie pełnomocnictw, wymiany korespondencji, należytego wykonania umowy, kontroli, rozliczenia umowy, zachowania zasad poufności oraz bezpieczeństwa i higieny pracy),
* dochodzić i bronić roszczeń,
* spełnić obowiązki prawne (np. wynikające z ustawy o przeciwdziałaniu praniu pieniędzy, prawa budowlanego, przepisów UE).

**Na jakiej podstawie prawnej przetwarzamy dane?**

* prawnie uzasadniony interes ORLEN S.A. (art. 6 ust. 1 lit. f RODO),
* obowiązki wynikające z przepisów prawa (art. 6 ust. 1 lit. c RODO).

**Kto może mieć dostęp do Twoich danych?**

Dane mogą być przekazywane spółkom z Grupy ORLEN i innym podmiotom współpracującym, podmiotom biorącym udział w procesach zakupowych, oraz takim podmiotom jak: firmy informatyczne, kurierskie, ochrony, BHP, prawne, doradcze czy archiwizacyjne.

**Jak długo przetwarzamy dane?**

Dane są przetwarzane przez czas potrzebny do realizacji celów oraz obowiązków prawnych. Mogą być przechowywane dłużej tylko, jeśli wymagają tego przepisy prawa.

**Jakie masz prawa?**

Masz prawo do:

* dostępu do swoich danych,
* ich sprostowania, usunięcia lub ograniczenia przetwarzania,
* wniesienia sprzeciwu (jeśli przetwarzamy dane na podstawie uzasadnionego interesu),
* złożenia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

Wnioski możesz kierować na: daneosobowe@orlen.pl lub listownie z dopiskiem „Inspektor Ochrony Danych”.

## ***ZAŁĄCZNIK NR 14A DO UMOWY WDROŻENIOWEJ [OBOWIĄZKI INFORMACYJNE SPÓŁKI******PUBLICZNEJ – WERSJA DLA PRZEDSIĘBIORCY, KTÓREGO INSTRUMENTY FINANSOWE SĄ NOTOWANE NA GPW]***

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

## Niniejsze postanowienia dotyczą przedsiębiorstw, których instrumenty finansowe są notowane na giełdzie papierów wartościowych w państwie członkowskim Unii Europejskiej.

# OBOWIĄZKI INFORMACYJNE SPÓŁKI PUBLICZNEJ

## Na obu stronach ciążą obowiązki informacyjne wobec rynku kapitałowego, które uregulowane są w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) NR 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku (rozporządzenie w sprawie nadużyć na rynku) oraz uchylającym dyrektywę 2003/6/WE Parlamentu Europejskiego i Rady i dyrektywy Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE ze zm. (dalej: „**Rozporządzenie MAR**”).

## W związku z tym, stosując przepisy powyższego rozporządzenia:

## Każda ze Stron poinformuje drugą o zamiarze przekazania do publicznej wiadomości informacji dotyczącej Umowy, jeśli uzna ją za informację poufną w rozumieniu Rozporządzenia MAR;

## Informacja poufna w rozumieniu Rozporządzenia MAR nie może być przez drugą Stronę Umowy i osoby pracujące na jej rzecz wykorzystywana lub bezprawnie ujawniana. W razie wykorzystywania informacji poufnych lub ich bezprawnego ujawnienia mają zastosowanie sankcje przewidziane w Rozporządzeniu MAR;

## W przypadku gdy obie Strony uznają Umowę za informację poufną w rozumieniu Rozporządzenia MAR, Strony dopuszczają możliwość przedstawienia sobie do konsultacji zakresu informacji będących przedmiotem oficjalnych komunikatów giełdowych dotyczących tej Umowy.

***ZAŁĄCZNIK NR 14B DO UMOWY WDROŻENIOWEJ [OBOWIĄZKI INFORMACYJNE SPÓŁKI******PUBLICZNEJ – WERSJA DLA PRZEDSIĘBIORCY, KTÓREGO INSTRUMENTY FINANSOWE NIE SĄ NOTOWANE NA GPW]***

1. **POSTANOWIENIA OGÓLNE**
   1. Niniejszy Załącznik stanowi integralną część Umowy.
   2. Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.
   3. Niniejsze postanowienia dotyczą przedsiębiorstw, których instrumenty finansowe nie są notowane na giełdzie papierów wartościowych w państwie członkowskim Unii Europejskiej.
2. **OBOWIĄZKI INFORMACYJNE SPÓŁKI PUBLICZNEJ**
   1. Na ORLEN S.A. ciążą obowiązki informacyjne wobec rynku kapitałowego, które uregulowane są w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) NR 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku (rozporządzenie w sprawie nadużyć na rynku) oraz uchylającym dyrektywę 2003/6/WE Parlamentu Europejskiego i Rady i dyrektywy Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE ze zm. (dalej: „**Rozporządzenie MAR**”).
   2. W związku z tym, stosując przepisy powyższego rozporządzenia:
      1. ORLEN S.A. poinformuje drugą Stronę Umowy o zamiarze przekazania do publicznej wiadomości informacji dotyczącej Umowy, jeśli uzna ją za informację poufną w rozumieniu Rozporządzenia MAR;
      2. Informacja poufna w rozumieniu Rozporządzenia MAR nie może być przez drugą Stronę Umowy i osoby pracujące na jej rzecz wykorzystywana lub bezprawnie ujawniana. W razie wykorzystywania informacji poufnych lub ich bezprawnego ujawnienia mają zastosowanie sankcje przewidziane w Rozporządzeniu MAR.

**Załącznik nr 15 do UMOWY WDROŻENIOWEJ [ZASADY BEZPIECZEŃSTWA TELEINFORMATYCZNEGO]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# ZASADY BEZPIECZEŃSTWA TELEINFORMATYCZNEGO (CYBERBEZPIECZEŃSTO)

## Podczas wykonywania Umowy, Wykonawca zobowiązany jest do przestrzegania zasad cyberbezpieczeństwa określonych w Umowie.

## Wykonawca zobowiązany jest posiadać politykę cyberbezpieczeństwa, która ma wyraźne zastosowanie do prac realizowanych w ramach Umowy.

## Wykonawca zobowiązany jest zapewnić, że zarządzanie infrastrukturą teleinformatyczną wykorzystywaną do realizacji Umowy jest prowadzone zgodnie z powszechnie stosowanymi standardami i normami funkcjonującymi w obszarze cyberbezpieczeństwa.

## W przypadku uzasadnionej konieczności Zamawiający udzieli upoważnionym osobom ze strony Wykonawcy dostępu logicznego (wyłącznie z wewnętrznej sieci teleinformatycznej) lub fizycznego do zasobów teleinformatycznych Zamawiającego na zasadach opisanych w dokumencie Zasady dostępu do zasobów teleinformatycznych Zamawiającego - dostęp fizyczny i logiczny wskazanych w dodatku nr 1 do niniejszego Załącznika [**Zasady dostępu do zasobów teleinformatycznych Zamawiającego – dostęp fizyczny i logiczny**].

## W przypadku uzasadnionej konieczności Zamawiający może udzielić zdalnego dostępu do zasobów teleinformatycznych Zamawiającego. Warunkiem koniecznym do udzielenia zdalnego dostępu jest podpisanie przez Wykonawcę porozumienia VPN będącego standardem ORLEN S.A. znajdującym się w dokumencie Porozumienie o zdalnym dostępie do zasobów teleinformatycznych znajdującym się w dodatku nr 2 do niniejszego Załącznika [**Wzór Porozumienia o zdalnym dostępie**].

## Wykonawca zobowiązuje się do niezwłocznego powiadamiania Zamawiającego o zaistniałych w infrastrukturze Wykonawcy naruszeniach lub incydentach cyberbezpieczeństwa mogących mieć wpływ na poziom cyberbezpieczeństwa Zamawiającego w związku z udzielonym dostępem do zasobów teleinformatycznych Zamawiającego.

## Incydenty cyberbezpieczeństwa mogące mieć wpływ na poziom cyberbezpieczeństwa Zamawiającego należy zgłaszać do CERT ORLEN wykorzystując poniższe kanały komunikacji:

1. Adres e-mail: [cert@orlen.pl](mailto:cert@orlen.pl) przy czym godziny pracy CERT ORLEN to regularne godziny pracy w dni robocze (09:00-17:00 od poniedziałku do piątku)
2. Poza wymienionymi godzinami z CERT ORLEN należy kontaktować się, w pierwszej kolejności, z Działem SOC, który działa w trybie 24/7, poprzez:

• adres e-mail: soc@orlen.pl

• tel. 24 256 90 90.

## Wykonawca zobowiązuje się także do niezwłocznego powiadamiania Zamawiającego o zmianach w otoczeniu wewnętrznym i zewnętrznym otoczeniu, które mogą mieć wpływ na działalność Wykonawcy, a w szczególności na przedmiot Umowy.

## Wykonawca zobowiązuje się do wykonywania obowiązków wynikających z Umowy w sposób zapobiegający utracie poufności, integralności i dostępności danych. W przypadku, gdy wykonanie Umowy wiąże się z ryzykiem utraty ww. atrybutów bezpieczeństwa danych, Wykonawca zobowiązany jest poinformować o tym Zamawiającego przed przystąpieniem do wykonywania jakichkolwiek prac oraz umożliwić Zamawiającemu przeprowadzenie działań zapewniających zachowanie ww. atrybutów.

## W sprawach określonych w niniejszym Załączniku Wykonawca odpowiada za skutki działań pracowników oraz osób trzecich, którym powierzył wykonanie czynności na rzecz Zamawiającego tak, jak za czynności własne.

## W przypadku naruszenia przez Wykonawcę zasad cyberbezpieczeństwa , Zamawiający może żądać zapłaty przez Wykonawcę kary umownej w wysokości 100.000,00 zł (słownie: sto tysięcy złotych) za każdy przypadek naruszenia. Uprawnienie do żądania kary umownej, o której mowa w zdaniu poprzedzającym nie wyłącza uprawnienia Zamawiającego do dochodzenia odszkodowania uzupełniającego na zasadach ogólnych, w przypadku, gdy wysokość poniesionej szkody przewyższa zastrzeżoną wysokość kary umownej.

## W przypadku decyzji Zamawiającego o wykonaniu weryfikacji cyberbezpieczeństwa (między innymi testów penetracyjnych) aplikacji lub systemów (w tym internetowych) służących do realizacji Umowy lub aplikacji lub systemu będącego przedmiotem Umowy, Wykonawca umożliwi taką weryfikację i w przypadku zidentyfikowania podatności zastosuje się do rekomendacji Zamawiającego.

# DODATEK NR 1 [ZASADY DOSTĘPU DO ZASOBÓW TELEINFORMATYCZNYCH ZAMAWIAJĄCEGO – DOSTĘP FIZYCZNY I LOGICZNY] DO ZAŁĄCZNIKA NR 15 [ZASADY BEZPIECZEŃSTWA TELEINFORMATYCZNEGO]

**Zasady dostępu logicznego i technicznego do zasobów informatycznych Zamawiającego**

1. Zamawiający udzieli upoważnionym osobom ze strony Wykonawcy dostępu logicznego z wewnętrznej sieci teleinformatycznej do zasobów teleinformatycznych Zamawiającego z wykorzystaniem komputerów udostępnionych przez Zamawiającego lub stanowiących własność Wykonawcy, które będą spełniały wymagania polityki bezpieczeństwa teleinformatycznego obowiązującej u Zamawiającego.
2. Dostęp, o którym mowa w pkt. 1. powyżej, zostanie przydzielony nie wcześniej niż po zawarciu Umowy i na okres nie dłuższy niż okres jej obowiązywania oraz po spełnieniu wymagań bezpieczeństwa określonych w Umowie.
3. Wykaz osób ze strony Wykonawcy upoważnionych do dostępu określonego w pkt. 1. powyżej, poziom uprawnień oraz oświadczenie o spełnieniu wymagań określonych w Umowie zostały zawarte w informacji w pkt. 1. załączniku do niniejszego dodatku.
4. Każdorazowa zmiana niniejszego załącznika musi być potwierdzona, w terminie do 2 Dni Roboczych, pisemnym wnioskiem z podpisem Kierownika Projektu Wykonawcy i przesłana do Kierownika Projektu Zamawiającego w celu uzyskania jego pisemnej (pod rygorem nieważności) akceptacji. Taka zmiana nie wymaga aneksu do Umowy pod rygorem nieważności.
5. Dla każdej z osób wymienionych w pkt. 3. powyżej zostaną założone wymagane konta w poszczególnych udostępnianych im zasobach teleinformatycznych oraz nadane stosowne uprawnienia do tych zasobów.
6. Osoby wymienione w pkt. 3. powyżej zobowiązane są do:
   1. przestrzegania zasad bezpieczeństwa teleinformatycznego określonych w Umowie;
   2. stosowania się do obowiązujących u Zamawiającego procedur i zasad bezpieczeństwa teleinformatycznego, w zakresie wynikającym z przedmiotu Umowy;
   3. zapobiegania nieuprawnionemu dostępowi do zasobów teleinformatycznych Zamawiającego;
   4. zabezpieczenia eksploatowanego sprzętu komputerowego i przetwarzanych przy jego pomocy informacji przed dostępem osób nieuprawnionych;
   5. nieujawniania aktualnych lub poprzednio używanych haseł osobistych, haseł grup roboczych oraz innych środków służących do uwierzytelniania w zasobach teleinformatycznych Zamawiającego;
   6. korzystania wyłącznie z udostępnianych przez Zamawiającego protokołów komunikacyjnych;
   7. korzystania z udostępnionych zasobów teleinformatycznych wyłącznie w celu realizacji przedmiotu Umowy, w zakresie posiadanych, zatwierdzonych uprawnień i z zachowaniem należytej staranności przy ich używaniu.
7. Wykonawca zobowiązuje się wdrożyć na własny koszt oraz stosować uzgodnione w ramach Umowy procedury, zabezpieczenia fizyczne, organizacyjne i technologiczne (w tym zabezpieczenia chroniące przed działaniem szkodliwego oprogramowania) zapewniające ochronę tych spośród własnych zasobów teleinformatycznych, które uczestniczą bezpośrednio lub pośrednio w realizacji Umowy.
8. Stosowane przez Wykonawcę zabezpieczenia muszą być adekwatne do występujących zagrożeń dla utraty bezpieczeństwa teleinformatycznego, w tym uniemożliwiać dostęp osobom nieuprawnionym do zasobów teleinformatycznych Zamawiającego.
9. Zamawiający zastrzega sobie prawo do monitorowania i rejestrowania działań osób upoważnionych ze strony Wykonawcy do dostępu do zasobów teleinformatycznych Zamawiającego w zakresie spełniania przez nie obowiązujących procedur i zasad bezpieczeństwa teleinformatycznego oraz natychmiastowego zablokowania dostępu takiej osoby w przypadku stwierdzenia naruszenia przez nią obowiązujących zasad bezpieczeństwa teleinformatycznego, w tym m.in.:
   1. ujawnienia powierzonych lub stosowanych haseł do zasobów teleinformatycznych;
   2. wykorzystywania przydzielonych uprawnień do zasobów teleinformatycznych do celów innych, niż związane z realizacją Umowy;
   3. niedopełnienia obowiązku zabezpieczenia powierzonego sprzętu komputerowego oraz środków technicznych wykorzystywanych do realizacji dostępu do zasobów teleinformatycznych Zamawiającego;
   4. samowolnego instalowania oprogramowania, zmiany konfiguracji powierzonego przez Zamawiającego sprzętu komputerowego, chyba, że czynności te są objęte zakresem Umowy. W takim przypadku należy poinformować osobę odpowiedzialną za realizację Umowy ze strony Zamawiającego o zasadności instalacji dodatkowego oprogramowania lub zmiany konfiguracji, w celu uzyskania jej akceptacji. Wszelkie zmiany, o których wyżej mowa, należy przeprowadzić zgodnie z procedurami obowiązującymi u Zamawiającego;
   5. niestosowania się do zasad bezpieczeństwa teleinformatycznego określonych w Umowie.
10. Wykonawca zobowiązuje się do niezwłocznego powiadamiania Zamawiającego o zaistniałych naruszeniach lub incydentach bezpieczeństwa teleinformatycznego oraz bezpieczeństwa Tajemnicy Przedsiębiorstwa Zamawiającego (w tym – jeśli dotyczy – Tajemnicy Spółki ORLEN S.A.) w związku z udzielonym dostępem do zasobów teleinformatycznych Zamawiającego.
11. Po zakończeniu obowiązywania Umowy, Wykonawca zobowiązany jest do zwrócenia Zamawiającemu wszelkich udostępnionych środków technicznych wykorzystywanych do realizacji dostępu do zasobów teleinformatycznych Zamawiającego.
12. Wykonawca przyjmuje do wiadomości, że ponosi pełną odpowiedzialność za szkody wynikłe dla Zamawiającego z zaistnienia incydentów bezpieczeństwa teleinformatycznego, będących następstwem naruszenia lub niestosowania zasad określonych w Umowie i niniejszym załączniku przez osoby określone  
    w pkt. 3 powyżej.

**Załącznik NR 1 DO DODATKU NR 1 [ZASADY DOSTĘPU LOGICZNEGO DO ZASOBÓW INFORMATYCZNYCH ZAMAWIAJĄCEGO] DO ZAŁĄCZNIKA NR 15 [ZASADY BEZPIECZEŃSTWA TELEINFORMATYCZNEGO]**

**Wykaz osób upoważnionych oraz oświadczenie o spełnieniu wymagań określonych w Umowie**

1. **Wykaz osób ze strony Wykonawcy upoważnionych do dostępu logicznego do zasobów teleinformatycznych z wewnętrznej sieci teleinformatycznej Zamawiającego z wykorzystaniem komputerów Wykonawcy.**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Imię Nazwisko** | **Poziom uprawnień** | **Nazwa zasobu / usługi** | **Środowisko** | **Nazwa konta** | **Okres ważności uprawnień** | **Model oraz nr seryjny komputera** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

*Legenda:*

*Poziom uprawnień: u – użytkownik, a – administrator, d – programista,*

*Nazwa zasobu / usługi: nazwa hosta oraz zakres udostępnianych usług,*

*Środowisko: p – produkcja, t – test, r – rozwój,*

*Nazwa konta: nazwa indywidualnego konta w udostępnianych zasobach,*

*Okres ważności uprawnień: od dnia ……. do dnia ……..*

|  |  |
| --- | --- |
| ZAMAWIAJĄCY  ……………………………………  Imię i Nazwisko (czytelnie), data, podpis | WYKONAWCA  ……………………………………  Imię i Nazwisko (czytelnie), data, podpis |

1. **Oświadczenie Wykonawcy**

Stosownie do ust. 3 *Zasad dostępu logicznego z wewnętrznej sieci teleinformatycznej Zamawiającego*, stanowiących część umowy ramowej zawartej w dniu […], pomiędzy Polskim Koncernem Naftowym ORLEN S.A. a […] („**Umowa**”);

**[…] oświadcza, że:**

1. akceptuje i zobowiązuje się do przestrzegania zasad bezpieczeństwa teleinformatycznego obowiązujących przy realizacji Umowy;
2. sprzęt komputerowy wykorzystywany w celu realizacji przedmiotu Umowy, posiadający dostęp do zasobów teleinformatycznych Zamawiającego spełnia wymagania w zakresie bezpieczeństwa teleinformatycznego, w tym m.in.:
   1. w zakresie zainstalowanego i funkcjonującego na komputerze oprogramowania:
   * szyfrującego zawartość całego dysku twardego;
   * antywirusowego oraz firewalla osobistego (z aktualizowanymi na bieżąco sygnaturami);
   1. w zakresie konfiguracji komputera:
   * komputer zabezpieczony jest hasłem dostępu do BIOS oraz aktywną ochroną polegającą na konieczności spersonalizowanego logowania do systemu operacyjnego przy każdym uruchomieniu systemu;
   * w komputerze zablokowano możliwość uruchomienia systemu operacyjnego z wymiennych nośników elektronicznych;
   * nie później niż po 6 - minutowym okresie bezczynności użytkownika następuje automatyczne blokowanie komputera hasłem o długości co najmniej 8 znaków z zachowaną złożonością, tj. z wymuszonym stosowaniem 3 z 4 grup znaków (małe litery, duże litery, cyfry lub znaki specjalne);
   * na komputerze nie działa oprogramowanie typu IM (Instant Messaging) oraz P2P (Peer-to-Peer);
   * na komputerze nie jest zainstalowane i wykorzystywane oprogramowanie umożliwiające nieautoryzowaną ingerencję w zasoby teleinformatyczne Zamawiającego.
3. Osoby ze strony Wykonawcy uprawnione do dostępu do zasobów teleinformatycznych Zamawiającego zostały poinformowane o obowiązku stosowania zasad bezpieczeństwa teleinformatycznego obowiązujących przy realizacji przedmiotu Umowy oraz podpisały stosowne oświadczenia o przestrzeganiu tych zasad.

WYKONAWCA

……………………………………

# DODATEK NR 2 [POROZUMIENIE O UDOSTĘPNIENIU ZDALNEGO DOSTĘPU] DO ZAŁĄCZNIKA NR 15 [ZASADY BEZPIECZEŃSTWA TELEINFORMATYCZNEGO]

**Porozumienie o udostępnieniu zdalnego dostępu**

**do Zasobów TELEINFORMATYCZNYCH**

Zawarte dnia …………………………… w Płocku, pomiędzy:

**Polski Koncern Naftowy ORLEN spółka akcyjna** z siedzibą w Płocku przy ul. Chemików 7, 09-411 Płock, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS: 0000028860, której dokumentacja rejestrowa jest przechowywana przez Sąd Rejonowy dla Łodzi-Śródmieścia w Łodzi XX Wydział Gospodarczy – Krajowego Rejestru Sądowego, NIP: 7740001454, REGON: 610188201, BDO: 000007103, o kapitale zakładowym w wysokości 1 451 177 561,25 zł, opłaconym w całości,

zwanym dalej **„Zamawiającym”,**

reprezentowanym przez:

1. […]

a

**[…]** z siedzibą w […], ul. […], […] […], wpisaną do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla […], […] Wydział Gospodarczy KRS, pod numerem KRS […], NIP […] z kapitałem zakładowym w wysokości […] PLN, opłaconym w całości, zwanym dalej **„Wykonawcą”,**

reprezentowaną przez:

1. […]

zwanymi są dalej łącznie **„Stronami”**.

Niniejsze porozumienie („**Porozumienie**”) Strony zawierają dla ustalenia zasad udzielenia Wykonawcy zdalnego dostępu do zasobów teleinformatycznych w celu umożliwienia Wykonawcy realizacji jego zobowiązań określonych w umowie ramowej o numerze […] z dn. […],

zwanej dalej (łącznie ze wszystkimi Załącznikami do ww. umowy ramowej) „**Umową**”.

**§ 1**

**Przedmiot Porozumienia**

1. Zamawiający udostępni Wykonawcy zdalny dostęp do zasobów teleinformatycznych (zwany dalej ,,**Zdalnym Dostępem**’’) na zasadach określonych w niniejszym Porozumieniu.
2. Niniejsze Porozumienie ma również zastosowanie do każdego podmiotu, któremu Wykonawca zleci, po uzyskaniu pisemnej zgody od Zamawiającego, wykonanie Umowy (w tym jej części) z wykorzystaniem Zdalnego Dostępu. W takiej sytuacji Wykonawca odpowiada za skutki działań osób trzecich, którym powierzył wykonanie Umowy, tak jak za czynności własne.

**§ 2**

**Udostępnienie**

1. Zdalny Dostęp możliwy jest wyłącznie po podpisaniu Porozumienia oraz po spełnieniu przez Wykonawcę wymagań dotyczących Zdalnego Dostępu i ochrony informacji określonych w Umowie i Porozumieniu (w tym w Załączniku nr 2 do Porozumienia).
2. Zakres Zdalnego Dostępu oraz lista osób uprawnionych po stronie Wykonawcy do Zdalnego Dostępu została określona w Załączniku nr 1 do Porozumienia.
3. Każdorazowa zmiana informacji w Załączniku nr 1 do Porozumienia musi być potwierdzona pisemnym wnioskiem z podpisem przedstawiciela Wykonawcy (określonego w § 5 ust. 4) i przesłana w terminie do 2 Dni Roboczych do przedstawiciela Zamawiającego (określonego w § 5 ust. 4), w celu uzyskania jego pisemnej akceptacji. Taka zmiana nie wymaga aneksowania Porozumienia.
4. Zdalny Dostęp zostanie udostępniony wyłącznie osobom uprawnionym po stronie Wykonawcy w terminie do 10 Dni Roboczych liczonych od dnia wejścia w życie Porozumienia pod warunkiem spełnienia przez Wykonawcę zasad określonych w załączniku nr 2 do Porozumienia.
5. Spełnienie zasad określonych w ust. 4 powyżej zostanie potwierdzone przez Wykonawcę w drodze złożenia oświadczenia, które stanowi Załącznik nr 3 do Porozumienia.

**§ 3**

**Okres udzielenia Zdalnego Dostępu**

1. Zdalny Dostęp udostępniony zostanie na okres wskazany w załączniku nr 1 do Porozumienia, z zastrzeżeniem postanowień ust. 2. poniżej.
2. Zdalny Dostęp może zostać zablokowany przez Zamawiającego, co jest jednoznaczne z rozwiązaniem niniejszego Porozumienia przez Zamawiającego bez zachowania okresu wypowiedzenia, w przypadku:
   1. naruszenia postanowień § 4, § 5, bądź § 6 Porozumienia;
   2. niespełnienia wymogów potwierdzonych w oświadczeniu, o którym mowa w § 2 ust. 5. powyżej;
   3. wniosku o zablokowanie Zdalnego Dostępu złożonego przez właściciela biznesowego zasobu teleinformatycznego (po stronie Zamawiającego), do którego realizowany jest dostęp;
   4. rozwiązania lub wygaśnięcia Umowy, a także uchylenia bądź zniweczenia skutków prawnych Umowy;
   5. wykrycia szkodliwego oprogramowania na komputerze korzystającym ze Zdalnego Dostępu lub innego oprogramowania zagrażającego bezpieczeństwu zasobów teleinformatycznych Zamawiającego;
   6. spowodowania incydentu związanego z bezpieczeństwem teleinformatycznym zasobów Zamawiającego lub bezpieczeństwem informacji Zamawiającego.
3. W przypadku, o którym mowa w § 3 ust. 2. powyżej, Zamawiający uprawniony będzie do wszczęcia procedury zablokowania Zdalnego Dostępu.

**§ 4**

**Zasady korzystania**

1. Zasoby teleinformatyczne Zamawiającego udostępnione poprzez Zdalny Dostęp mogą być wykorzystywane przez Wykonawcę, w tym przez osoby uprawnione do korzystania ze Zdalnego Dostępu wyłącznie zgodnie z ich przeznaczeniem.
2. Wykonawca oraz osoby uprawnione po jego stronie do korzystania ze Zdalnego Dostępu zobowiązani są do:
   1. korzystania ze Zdalnego Dostępu wyłącznie w celu realizacji Umowy, w zakresie posiadanych, zatwierdzonych uprawnień i z zachowaniem należytej staranności przy ich używaniu;
   2. pozyskiwania i przetwarzania wyłącznie informacji niezbędnych do realizacji Umowy;
   3. niewykorzystywania nieautoryzowanych przez Zamawiającego mechanizmów służących do uzyskiwania Zdalnego Dostępu;
   4. korzystania ze Zdalnego Dostępu wyłącznie w miejscach i w taki sposób, aby zapewnić ochronę informacji Zamawiającego, wyświetlanych na ekranie lub do których dostęp możliwy jest z wykorzystaniem urządzenia, z którego realizowany jest Zdalny Dostęp;
   5. zapewnienia ochrony dla informacji dotyczących parametrów technicznych i technologicznych Zdalnego Dostępu, w szczególności nieprzekazywania tych informacji osobom nieuprawnionym;
   6. stosowania się do obowiązujących u Zamawiającego procedur i zasad bezpieczeństwa teleinformatycznego, w zakresie wynikającym z Umowy, realizacji przedmiotu Umowy oraz niniejszego Porozumienia.
3. Wykonawca odpowiada wobec Zamawiającego za zapewnienie dostępu do środków uwierzytelniających wyłącznie osobom uprawnionym oraz zapewni właściwą ochronę przed dostępem do tych środków osób nieuprawnionych.
4. Wykonawca bez zbędnej zwłoki powiadomi przedstawiciela Zamawiającego, określonego w § 5 ust. 4., o każdym zauważonym przez niego zakresie dostępu, który jest nieadekwatny do zakresu uprawnień określonych w Porozumieniu oraz nieadekwatny do realizacji przedmiotu Umowy.

**§ 5**

**Współdziałanie Stron**

1. Strony są zobowiązane do współpracy w zakresie nadzoru nad realizacją Porozumienia.
2. Osoby uprawnione do korzystania ze Zdalnego Dostępu zobowiązane są do bezzwłocznego informowania przedstawiciela Zamawiającego o każdym:
   1. zauważonym przypadku naruszenia bezpieczeństwa zasobów teleinformatycznych Zamawiającego, bezpieczeństwa informacji Zamawiającego lub bezpieczeństwa zasobów teleinformatycznych Wykonawcy wykorzystywanych do Zdalnego Dostępu;
   2. stwierdzonym przypadku naruszenia integralności sprzętu, oprogramowania bądź podejrzeniu próby takiego naruszenia;
   3. podejrzeniu ujawnienia indywidualnych środków uwierzytelniających wykorzystywanych do Zdalnego Dostępu.
3. Wykonawca zobowiązany jest do poinformowania Zamawiającego w terminie do 2 dni roboczych w przypadku jakiejkolwiek zmiany dotyczącej osób uprawnionych po stronie Wykonawcy do korzystania ze Zdalnego Dostępu, wymienionych w Załączniku nr 1 do Porozumienia.
4. Strony będą dokonywały bieżących uzgodnień dotyczących Zdalnego Dostępu poprzez swoich przedstawicieli odpowiedzialnych za realizację Porozumienia:

Przedstawiciel Zamawiającego:

……

Tel. :

Fax :

Adres e-mail :

Przedstawiciel Wykonawcy:

……

Tel. :

Fax :

Adres e-mail :

1. Zmiana przedstawiciela, numeru telefonu, numeru faksu i adresu e-mail, o których mowa w ust. 4 powyżej, nie stanowi zmiany Porozumienia i jest skuteczna z chwilą powiadomienia drugiej Strony o dokonanej zmianie w formie pisemnej lub za pomocą poczty elektronicznej. Uzgodnienia i decyzje przedstawicieli będą wiążące dla Stron, tak długo jak nie zmieniają postanowień Porozumienia.
2. Wszelkie incydenty związane z bezpieczeństwem teleinformatycznym dotyczące Zdalnego Dostępu oraz ewentualne problemy ze Zdalnym Dostępem należy zgłaszać do przedstawiciela Zamawiającego, określonego w ust. 4 powyżej.

**§ 6**

**Prawo kontroli**

1. Zamawiający ma prawo do kontroli sposobów wykorzystywania Zdalnego Dostępu przez Wykonawcę odnośnie zobowiązań, o których mowa w Porozumieniu, w formie kontroli przeprowadzanej przez przedstawicieli Zamawiającego lub przeprowadzanej przez podmiot zewnętrzny działający na jego koszt i zlecenie oraz do żądania złożenia pisemnych wyjaśnień przez Wykonawcę, w terminie 5 Dni Roboczych od dnia doręczenia Wykonawcy żądania złożenia wyjaśnień przez Zamawiającego.
2. Po kontroli, o której mowa w ust. 1. powyżej, Zamawiający może zredagować zalecenia pokontrolne i żądać ich wykonania oraz określić termin ich realizacji.
3. Zamawiający realizować będzie prawo kontroli w godzinach pracy Wykonawcy i po uprzednim powiadomieniu Wykonawcy.
4. Wykonawca zobowiązany jest do umożliwienia przeprowadzenia kontroli, o której mowa w ust. 1. powyżej.
5. Wykonawca gwarantuje, że na żądanie Zamawiającego udostępni obowiązującą dokumentację bezpieczeństwa teleinformatycznego oraz urządzenia i systemy informatyczne wykorzystywane przy Zdalnym Dostępie do kontroli pod kątem zastosowania w nich wymaganych zabezpieczeń technicznych i organizacyjnych.
6. Kontrola, o której mowa w ust. 1. powyżej, zostanie przeprowadzona wyłącznie pod względem oceny zgodności z wymaganiami określonymi w Porozumieniu.
7. Zamawiający zastrzega sobie prawo do monitorowania i rejestrowania działań osób uprawnionych do korzystania ze Zdalnego Dostępu w zakresie spełniania przez nie obowiązujących zasad bezpieczeństwa teleinformatycznego, jakie powinny być stosowane przy Zdalnym Dostępie oraz natychmiastowego zablokowania dostępu takiej osoby w przypadku stwierdzenia naruszenia przez nią tych zasad, w tym m.in.:
   1. ujawnienia powierzonych lub stosowanych haseł oraz środków służących do uwierzytelnienia w zasobach teleinformatycznych;
   2. wykorzystywania przydzielonych uprawnień do zasobów teleinformatycznych do celów innych, niż związane z realizacją Umowy;
   3. niedopełnienia obowiązku odpowiedniego zabezpieczenia urządzeń oraz środków technicznych i organizacyjnych służących do realizacji Zdalnego Dostępu;
   4. samowolnego instalowania oprogramowania lub zmiany konfiguracji udostępnionych zasobów teleinformatycznych, chyba że czynności te są objęte zakresem Umowy i zostały uzgodnione przez Strony;
   5. niestosowania się do zasad bezpieczeństwa określonych w Porozumieniu.

**§ 7**

**Odpowiedzialność**

1. Wykonawca jest odpowiedzialny za niewykonanie lub nienależyte wykonanie zobowiązań określonych w Porozumieniu, w tym za udostępnienie lub wykorzystanie Zdalnego Dostępu niezgodnie z niniejszym Porozumieniem, a w szczególności za naruszenie postanowień § 4, § 5 i § 6 oraz za naruszenie zasad bezpieczeństwa teleinformatycznego określonych w załączniku nr 2 do Porozumienia.
2. W sytuacjach, o których mowa w ust. 1. powyżej, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 50.000 zł (słownie: pięćdziesiąt tysięcy) złotych za każde naruszenie.
3. Uprawnienie do otrzymania kary umownej nie ogranicza prawa Zamawiającego do dochodzenia od Wykonawcy odszkodowania na zasadach ogólnych w przypadku, gdy wysokość poniesionej szkody przewyższa zastrzeżoną wysokość kary umownej.
4. W przypadku naruszenia postanowień Porozumienia z przyczyn leżących po stronie Wykonawcy, w następstwie czego Zamawiający zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Wykonawca zobowiązuje się zrekompensować Zamawiającemu wszelkie poniesione z tego tytułu szkody, w tym straty.
5. W przypadku braku możliwości skorzystania przez Wykonawcę ze Zdalnego Dostępu odpowiedzialność odszkodowawcza Zamawiającego, bez względu na jej podstawę, jest wyłączona.
6. Odpowiedzialność Wykonawcy wynikająca z Porozumienia lub z nim związana nie podlega jakimkolwiek ograniczeniom.

**§ 8**

**Dostępność**

1. Zamawiający dołoży wszelkich starań, aby zapewnić dostępność Zdalnego Dostępu do zasobów teleinformatycznych, jednak nie gwarantuje ciągłości takiego dostępu.
2. Zamawiający może ograniczyć lub czasowo zawiesić Zdalny Dostęp w dowolnym momencie, gdy uzna to za konieczne.
3. Brak możliwości skorzystania przez Wykonawcę ze Zdalnego Dostępu nie zwalnia Wykonawcy z odpowiedzialności za niewykonanie lub nienależyte wykonanie Umowy.

**§ 9**

**Rozwiązanie Porozumienia**

1. Niniejsze Porozumienie może zostać rozwiązane w każdym czasie w drodze porozumienia Stron, zawartego na piśmie pod rygorem nieważności.
2. Niniejsze Porozumienie może zostać rozwiązane w drodze pisemnego (pod rygorem nieważności) oświadczenia o wypowiedzeniu Porozumienia, z zachowaniem 30 dniowego okresu wypowiedzenia.
3. Niniejsze Porozumienie może zostać rozwiązane przez Zamawiającego w drodze wypowiedzenia bez zachowania okresu wypowiedzenia w przypadkach zagrożenia bezpieczeństwa zasobów teleinformatycznych Zamawiającego, a także w przypadkach wskazanych w § 3 ust. 2. Porozumienia.

**§ 10**

**Postanowienia końcowe**

1. Niniejsze Porozumienie wchodzi w życie z dniem jego podpisania przez Strony. Od dnia wejścia w życie Porozumienie stanowi integralną część Umowy.
2. Strony postanawiają, iż wszelkie spory związane z wykonaniem Porozumienia rozwiązywane będą polubownie. W przypadku braku polubownego zakończenia sporu sądem właściwym dla jego rozstrzygnięcia będzie sąd właściwy ze względu na siedzibę Zamawiającego.
3. Wszelkie zmiany i uzupełnienia niniejszego Porozumienia będą sporządzone w formie pisemnej pod rygorem nieważności.
4. Załączniki do niniejszego Porozumienia stanowią jego integralną część.
5. Porozumienie sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

**ZAMAWIAJĄCY WYKONAWCA**

Załączniki:

Załącznik nr 1 – Zakres Zdalnego Dostępu i Lista Osób Uprawnionych

Załącznik nr 2 – Zasady bezpieczeństwa teleinformatycznego stosowane przy Zdalnym Dostępie

Załącznik nr 3 – Oświadczenie Wykonawcy

**Załącznik nr 1 do Porozumienia - Zakres Zdalnego Dostępu i Lista Osób Uprawnionych**

1. **Zakres Zdalnego Dostępu:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Imię i nazwisko** | **Nazwa zasobu, usługi / PORTY** | **Adres IP** | **Środowisko** | **Nazwa konta** | **Poziom uprawnień** | **Okres ważności uprawnień** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

* Nazwa zasobu / usługi: dokładna nazwa systemu, aplikacji lub usługi do którego ma zostać przydzielony Zdalny Dostęp oraz zakres udostępnianych usług,
* Adres IP: adres IP urządzenia, które wchodzi w skład danego systemu, np. adres IP serwera testowego
* Środowisko: p – produkcja, t – test, r – rozwój,
* Nazwa konta: nazwa indywidualnego konta w udostępnianych zasobach,
* Poziom uprawnień: U – użytkownik, A – administrator, P – programista, T – tester
* Okres ważności uprawnień: od dnia … do dnia …

1. **Lista osób uprawnionych**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Imię i nazwisko** | **Numer telefonu komórkowego** | **Adres e-mail** | **Model oraz nr seryjny komputera** |
| 1. |  |  |  |  |
| 2. |  |  |  |  |
| 3. |  |  |  |  |
| 4. |  |  |  |  |

|  |  |
| --- | --- |
| **ZAMAWIAJĄCY**  ……………………………………  Imię i Nazwisko (czytelnie), data, podpis | **WYKONAWCA**  ……………………………………  Imię i Nazwisko (czytelnie), data, podpis |

**Załącznik nr 2 do Porozumienia - Zasady bezpieczeństwa teleinformatycznego stosowane przy Zdalnym Dostępie**

1. Zdalny Dostęp, realizowany poprzez połączenie typu VPN do określonych w Porozumieniu zasobów teleinformatycznych jest przyznawany po podpisaniu Porozumienia oraz po spełnieniu przez Wykonawcę wymagań określonych w Umowie i Porozumieniu (w tym niniejszym Załączniku do Porozumienia).
2. W celu uzyskania Zdalnego Dostępu wymagane jest korzystanie z dostarczonych przez Zamawiającego środków uwierzytelniających.
3. Wykonawca jest zobowiązany posiadać politykę bezpieczeństwa teleinformatycznego, która ma wyraźne zastosowanie do prac realizowanych w ramach Umowy, zdalnych zasobów i wykorzystywanej infrastruktury teleinformatycznej.
4. Wykonawca jest zobowiązany zapewnić, że zarządzanie infrastrukturą teleinformatyczną wykorzystywaną do realizacji Zdalnego Dostępu jest prowadzone zgodnie z dobrymi, uznanymi praktykami bezpieczeństwa teleinformatycznego.
5. Stosowane przez Wykonawcę procedury i zabezpieczenia muszą być adekwatne do występujących zagrożeń dla utraty bezpieczeństwa teleinformatycznego udostępnianych zasobów, w tym uniemożliwiać osobom nieuprawnionym dostęp do zasobów Zamawiającego i Wykonawcy oraz przetwarzanych w nich informacji.
6. Wykonawca jest zobowiązany, aby przez cały okres korzystania ze Zdalnego Dostępu, komputery osób uprawnionych do korzystania ze Zdalnego Dostępu:
   1. posiadały zabezpieczony hasłem dostęp do BIOS;
   2. posiadały system operacyjny wraz z zainstalowanymi dla niego wszystkimi dostępnymi aktualizacjami, zabezpieczony hasłem konstruowanym z wykorzystaniem co najmniej 3 spośród 4 grup znaków (małe litery, duże litery, cyfry lub znaki specjalne), składającym się przynajmniej z 8 znaków;
   3. posiadały zabezpieczenia uniemożliwiające uruchomienie systemu operacyjnego z wymiennych nośników elektronicznych;
   4. posiadały aktualne i aktywne oprogramowanie antywirusowe;
   5. posiadały włączone zabezpieczenia typu firewall;
   6. posiadały aktywny wygaszacz ekranu blokowany hasłem o parametrach określonych w ppkt. b powyżej, uruchamiany automatycznie po upływie najwyżej 10 minut bezczynności użytkownika;
   7. w przypadku komputerów przenośnych, posiadały środki zapewniające szyfrowanie zawartości całego dysku twardego;
   8. nie były wykorzystywane do udostępniania Zdalnego Dostępu dalej na inne komputery lub urządzenia Wykonawcy lub osób nieuprawnionych.
7. Wykonawca jest zobowiązany zapewnić, że wszelka komunikacja w ramach Zdalnego Dostępu z udostępnionymi zasobami teleinformatycznymi będzie się odbywała wyłącznie za pomocą bezpiecznych tj. szyfrowanych protokołów komunikacyjnych.
8. Wykonawca jest zobowiązany zapewnić, że wszystkie informacje związane ze Zdalnym Dostępem i bezpieczeństwem Zdalnego Dostępu są utrzymywane w poufności oraz, że żaden sprzęt wykorzystywany w celach związanych ze Zdalnym Dostępem (łącznie ze środkami uwierzytelniającymi) – zarówno ewentualny sprzęt dostarczony przez Zamawiającego jak i ten będący własnością Wykonawcy – nie jest przekazywany stronom trzecim, innym niż te, którym Wykonawca zleca, po uzyskaniu pisemnej zgody Zamawiającego, wykonywanie Umowy (w tym jej części) łącznie ze Zdalnym Dostępem do obsługiwanych systemów.
9. Wykonawca jest zobowiązany zapewnić, że urządzenia i zasoby teleinformatyczne wykorzystywane przez niego przy Zdalnym Dostępie są chronione odpowiednimi zabezpieczeniami fizycznymi, które zapewniają, że wyłącznie uprawniony personel Wykonawcy, wymieniony w Załączniku nr 1 do Porozumienia, może uzyskać fizyczny dostęp do nich.
10. Wykonawca jest zobowiązany bezzwłocznie informować przedstawiciela Zamawiającego, określonego w § 5 ust. 4. Porozumienia, o wszelkich kwestiach związanych z bezpieczeństwem Zdalnego Dostępu do zasobów teleinformatycznych Zamawiającego.
11. Wykonawca poinformuje osoby uprawnione do korzystania ze Zdalnego Dostępu o wymaganiach technicznych i organizacyjnych oraz o zasadach bezpieczeństwa przy korzystaniu ze Zdalnego Dostępu.
12. Wykonawca uzyska od osób uprawnionych do korzystania ze Zdalnego Dostępu podpisane oświadczenia o przestrzeganiu zasad bezpieczeństwa teleinformatycznego określonych w Porozumieniu.

**Załącznik nr 3 do Porozumienia**

**Oświadczenie Wykonawcy**

Stosownie do §2 ust. 5. Porozumienia o udostępnieniu zdalnego dostępu do zasobów teleinformatycznych zawartego pomiędzy Polskim Koncernem Naftowym ORLEN S.A., a ….. w dniu …………… („**Porozumienie**”)

…… („**Wykonawca**”) oświadcza, że:

1. Akceptuje i zobowiązuje się do przestrzegania zasad bezpieczeństwa obowiązujących przy korzystaniu ze Zdalnego Dostępu, które zostały określone w Porozumieniu.
2. Spełnił wymogi techniczne i organizacyjne określone w Załączniku nr 2 do Porozumienia
3. Osoby uprawnione do korzystania ze Zdalnego Dostępu, wymienione w Załączniku nr 1 do Porozumienia, zostały poinformowane o obowiązku stosowania zasad bezpieczeństwa teleinformatycznego obowiązujących przy korzystaniu ze Zdalnego Dostępu oraz podpisały stosowne oświadczenia o przestrzeganiu tych zasad.

WYKONAWCA

……………………………………

**Załącznik nr 16 do UMOWY WDROŻENIOWEJ [DOKUMENTACJA]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# DOKUMENTACJA

## W ramach realizacji Umowy, Wykonawca zobowiązuje się do tworzenia Dokumentacji zgodnie z dobrymi praktykami rynkowymi obowiązującymi w tym obszarze usług informatycznych.

## Dokumentacja obejmowała będzie w szczególności pełną dokumentację powykonawczą (projektową, techniczną, funkcjonalną), w formacie umożliwiającym eksport Dokumentacji do standardowych formatów plików (.docx). Dokumentacja zawierać będzie wszelkie informacje pozwalające Zamawiającemu na samodzielne korzystanie z Systemu, którego Dokumentacja dotyczy.

## Wykonawca jest zobowiązany dostarczyć komplet Dokumentacji w zakresie i na zasadach określonych w Umowie.

## Wykonawca będzie dostarczał Zamawiającemu Dokumentację w postaci elektronicznej, poprzez [#].

## Wraz z wygaśnięciem Umowy, bez względu na przyczynę wygaśnięcia, Wykonawca zobowiązany jest do wydania Zamawiającemu Dokumentacji kompletnej i aktualnej na dzień jej wygaśnięcia.

**Załącznik nr 17 do UMOWY WDROŻENIOWEJ [PRAWA WŁASNOŚCI INTELEKTUALNEJ]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# PRAWA WŁASNOŚCI INTELEKTUALNEJ

[Postanowienia ogólne]

## Wykonawca oświadcza i gwarantuje, że jest uprawniony do transferu praw do Utworów na Zamawiającego, w zakresie określonym poniżej.

## Wykonawca oświadcza i gwarantuje, że przekazane przez niego w ramach realizacji Umowy Utwory nie będą dotknięte żadnymi wadami prawnymi.

## Wykonawca zobowiązuje się i gwarantuje, że osoby uprawnione z tytułu autorskich praw osobistych do Utworów Dedykowanych i Utworów Standardowych, nie będą wykonywać tych praw w stosunku do Zamawiającego lub osób trzecich działających w imieniu lub na rzecz Zamawiającego oraz następców prawnych Zamawiającego.

## Niezależnie od powyższego, w przypadku zgłoszenia przez osobę trzecią jakiegokolwiek roszczenia związanego z wadą prawną jakiegokolwiek dobra własności intelektualnej, w tym Utworu, dostarczonego przez Wykonawcę, Zamawiający poinformuje Wykonawcę o tym fakcie i o takich roszczeniach, a Wykonawca podejmie niezbędne działania mające na celu zażegnanie sporu i poniesie koszty z tym związane. W szczególności, w przypadku wytoczenia przeciwko Zamawiającemu lub innemu podmiotowi uprawnionemu na podstawie Umowy, powództwa z tytułu naruszenia praw osoby trzeciej, Wykonawca wstąpi do postępowania w charakterze strony pozwanej, a w razie braku takiej możliwości, wystąpi z interwencją uboczną po stronie pozwanej oraz pokryje wszelkie koszty i odszkodowania związane z obroną przed roszczeniami, w tym koszty sądowe, koszty obsługi prawnej, w szczególności zastępstwa procesowego poniesione przez Zamawiającego lub inny podmiot uprawniony lub ugody.

## W razie przekazania przez Wykonawcę Zamawiającemu jakichkolwiek Utworów utrwalonych na fizycznych nośnikach, Wykonawca, w zamian za Wynagrodzenie, przeniesie własność tych nośników na Zamawiającego z chwilą ich przekazania.

## W razie stworzenia w związku z realizacją Umowy bazy danych w rozumieniu ustawy z dnia 27 lipca 2001 r. o ochronie baz danych, wskazane w art. 6 ust. 1 w/w ustawy prawo pobierania danych i wtórnego ich wykorzystania w całości lub w istotnej części, co do jakości lub ilości (dalej: „**Prawo Sui Generis**”), przysługuje Zamawiającemu jako producentowi takiej bazy danych. W przypadku, gdyby wbrew woli Stron wyrażonej w zdaniu poprzednim, Prawo Sui Generis faktycznie przysługiwało Wykonawcy, Wykonawca zobowiązuje się, w ramach Wynagrodzenia, do przeniesienia na rzecz Zamawiającego Prawa Sui Generis z chwilą faktycznego udostępnienia bazy danych. Postanowienia zawarte w niniejszym punkcie pozostają bez wpływu na przeniesienie autorskich praw majątkowych do bazy danych stanowiącej Utwór zgodnie z pozostałymi postanowieniami niniejszego załącznika.

[Przeniesienie autorskich praw majątkowych do Utworów Dedykowanych]

## Wykonawca, w zamian za Wynagrodzenie za Wdrożenie oraz Wynagrodzenie za Zlecenie, zobowiązuje się przenieść na Zamawiającego autorskie prawa majątkowe do Utworów Dedykowanych na polach eksploatacji obejmujących:

* + 1. w odniesieniu do Utworów Dedykowanych stanowiących programy komputerowe:
       1. trwałe lub czasowe zwielokrotnianie Utworów Dedykowanych w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie, w tym zwielokrotnianie Utworów Dedykowanych dokonywane podczas wprowadzania, wyświetlania, stosowania, przekazywania lub przechowywania Utworów Dedykowanych, w tym także utrwalanie i zwielokrotnianie Utworów Dedykowanych dowolną techniką, w tym techniką zapisu magnetycznego lub techniką cyfrową, taką jak zapis na płycie CD, DVD, Blu-ray, urządzeniu z pamięcią flash lub jakimkolwiek innym nośniku pamięci;
       2. tłumaczenie, przystosowywanie, zmiana układu lub jakiekolwiek inne zmiany w Utworach Dedykowanych,
       3. obrót Utworami Dedykowanymi, w tym wprowadzanie do obrotu, użyczanie lub najem Utworów Dedykowanych, a także rozpowszechnianie Utworów Dedykowanych w inny sposób, w tym ich publiczne wykonywanie, wystawianie, wyświetlanie, odtwarzanie, a także publiczne udostępnianie w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i w czasie przez siebie wybranym;
    2. w odniesieniu do Utworów Dedykowanych niestanowiących programów komputerowych:
       1. w zakresie utrwalania i zwielokrotniania Utworów Dedykowanych – wytwarzanie określoną techniką egzemplarzy Utworów Dedykowanych, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową,
       2. w zakresie obrotu oryginałem albo egzemplarzami, na których Utwory Dedykowane utrwalono – wprowadzenie do obrotu, użyczenie lub najem oryginału albo egzemplarzy,
       3. w zakresie rozpowszechniania Utworów Dedykowanych w sposób inny niż obrót oryginałem albo egzemplarzami, na których Utwory utrwalono – publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie, a także publiczne udostępnianie Utworów Dedykowanych w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i w czasie przez siebie wybranym.

## Wraz z przeniesieniem autorskich praw majątkowych do Utworów Dedykowanych, Wykonawca zobowiązuje się przenieść na Zamawiającego wyłączne prawo zezwalania na wykonywanie autorskiego prawa zależnego do opracowań Utworów Dedykowanych (tj. do rozporządzania i korzystania z takich opracowań) – na wskazanych w pkt. 2.7. powyżej polach eksploatacji.

## Przeniesienie praw oraz przeniesienie wyłącznego prawa zezwalania na wykonywanie autorskiego prawa zależnego, o których mowa wyżej, nastąpi z chwilą udostępnienia Utworów Dedykowanych w jakikolwiek sposób i w jakiejkolwiek formie Zamawiającemu.

[Udzielenie licencji na Utwory Standardowe]

## W ramach Wynagrodzenia za Wdrożenie oraz Wynagrodzenia za Zlecenie, Wykonawca udzieli na rzecz Zamawiającego wyłącznej licencji na korzystanie z Utworów Standardowych bez ograniczeń terytorialnych (tj. na terytorium całego świata), na następujących polach eksploatacji*:*

* + 1. w odniesieniu do Utworów Standardowych stanowiących programy komputerowe – na polach eksploatacji obejmujących:
       1. […];
       2. […];
    2. w odniesieniu do Utworów Standardowych niestanowiących programów komputerowych – na polach eksploatacji obejmujących:
       1. […]
       2. [....]

- (dalej: „**Licencja**”).

## W ramach Licencji, Zamawiający będzie uprawniony do udzielania sublicencji na rzecz spółek GK ORLEN wskazanych w Umowie oraz Koncepcji Biznesowej na polach eksploatacji wskazanych w pkt. 2.10. powyżej.

## Udzielenie Licencji nastąpi z chwilą wydania Utworu Standardowego w jakiejkolwiek postaci.

[Wypowiedzenie Licencji]

## Intencją Stron – w przypadku zawarcia Licencji – jest zawarcie umowy zbliżonej do umowy o charakterze jednorazowej transakcji podobnej do sprzedaży, gdzie w zamian za uiszczoną opłatę licencyjną (stanowiącą w przypadku Umowy element Wynagrodzenia za Wdrożenie lub Wynagrodzenia za Zlecenie) Zamawiający otrzymuje ciągłe, stałe i niewypowiadalne prawo do korzystania z Utworów, będących przedmiotem Licencji.

## W przypadku, gdyby postanowienie o niewypowiadalności Licencji przewidziane w punkcie poprzednim okazało się nieskuteczne lub nieważne, a Wykonawca byłby uprawniony do wypowiedzenia Licencji, Strony uzgadniają dla Wykonawcy 10-letni (słownie: dziesięcioletni) termin jej wypowiedzenia ze skutkiem na koniec roku kalendarzowego, z zastrzeżeniem punktu następnego.

## Wykonawca zobowiązuje się nie korzystać z uprawnienia do wypowiedzenia Licencji z wyjątkiem przypadków, w których Zamawiający naruszy autorskie prawa majątkowe do Utworów Standardowych oraz nie zaniecha tego naruszenia, mimo wezwania Zamawiającego i wyznaczenia mu w tym celu odpowiedniego terminu, nie krótszego niż 90 dni. Wezwanie musi być wystosowane w formie pisemnej pod rygorem braku skutków i musi zawierać wyraźne zastrzeżenie, że Wykonawca będzie uprawniony do wypowiedzenia Licencji w przypadku niezaprzestania dopuszczania się przez Zamawiającego wyraźnie i precyzyjnie wymienionych naruszeń. W przypadku wypowiedzenia Licencji z tej przyczyny termin wypowiedzenia Licencji wynosi 1 (słownie: jeden) rok, ze skutkiem na koniec roku kalendarzowego.

## W przypadku, gdy Wykonawca, mimo zobowiązania, o którym mowa w punkcie poprzednim, złoży oświadczenie o wypowiedzeniu Licencji, Wykonawca będzie zobowiązany do zapłaty na rzecz Zamawiającego, na jego żądanie, kwoty odpowiadającej rzeczywiście poniesionym przez Zamawiającego kosztom zapewnienia (w tym uzyskania licencji i wdrożenia) rozwiązania zastępczego.

**Załącznik nr 18 do UMOWY WDROŻENIOWEJ [KOD ŹRÓDŁOWY]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# KOD ŹRÓDŁOWY

## Wykonawca udostępni Zamawiającemu Kod Źródłowy, wykonany w ramach Umowy, w terminach i w formie w niej określonych.

## Wykonawca, udostępni Zamawiającemu Kod Źródłowy wraz ze skryptami kompilacyjnymi i uruchomieniowymi, plikami konfiguracyjnymi oraz niezbędną Dokumentacją pozwalającą na jego rozwijanie przez Zamawiającego lub przez podmioty, którym Zamawiający takie czynności zlecił.

## Bez uszczerbku dla postanowień, o których mowa poniżej, Wykonawca zobowiązuje się, że tworzenie Kodu Źródłowego na potrzeby realizacji Umowy będzie realizowane zgodnie z najlepszymi światowymi standardami rynkowymi obowiązującymi w tym obszarze usług informatycznych.

## Wraz z Kodem Źródłowym Wykonawca zobowiązany jest dostarczyć kompletny wykaz narzędzi programistycznych, bibliotek i innych elementów niezbędnych do doprowadzenia takiego Kodu Źródłowego do formy wykonywalnej. Ponadto na żądanie Zamawiającego Wykonawca zobowiązany jest udzielić Zamawiającemu lub osobie wskazanej przez Zamawiającego dodatkowych informacji niezbędnych do doprowadzenia danego Kodu Źródłowego do formy wykonywalnej.

## Kod Źródłowy zawierać będzie komentarze, w szczególności komentarze umieszczone w trakcie realizacji Umowy, wykonane zgodnie z regułami sztuki i metodyką prowadzenia prac programistycznych stosowaną przez Wykonawcę. Wykonawca nie będzie usuwał komentarzy oraz innych informacji technicznych z Kodu Źródłowego, przed jego dostarczeniem Zamawiającemu.

## Wykonawca nie jest również uprawniony do stosowania jakichkolwiek technik lub ograniczeń, które uniemożliwiłyby Zamawiającemu odczyt lub zapisywanie Kodu Źródłowego.

## Wraz z wygaśnięciem Umowy, bez względu na przyczynę wygaśnięcia, Wykonawca zobowiązany jest do wydania Zamawiającemu kompletnego i aktualnego na dzień wygaśnięcia Umowy Kodu Źródłowego.

## W przypadku decyzji Zamawiającego o wykonaniu weryfikacji cyberbezpieczeństwa Kodu Źródłowego i w następstwie identyfikacji podatności cyberbezpieczeństwa, Wykonawca zastosuje się do rekomendacji Zamawiającego i usunie wskazane podatności cyberbezpieczeństwa w Kodzie Źródłowym na własny koszt i ryzyko.

**Załącznik nr 19 do UMOWY WDROŻENIOWEJ [PERSONEL KLUCZOWY]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# PERSONEL KLUCZOWY

## [imię i nazwisko] – [funkcja];

## [imię i nazwisko] – [funkcja];

## [imię i nazwisko] – [funkcja];

## [imię i nazwisko] – [funkcja];

## [imię i nazwisko] – [funkcja].

**Załącznik nr 20 do UMOWY WDROŻENIOWEJ [KLAUZULA GRUPY ORLEN]**

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# KLAUZULA GRUPY ORLEN

## Wolą Stron Umowy jest rozszerzanie współpracy pomiędzy Wykonawcą, a spółkami z Grupy ORLEN.

## W przypadku zaistnienia potrzeby zakupu usług i/lub towarów stanowiących przedmiot Umowy przez spółki z Grupy ORLEN, Wykonawca zobowiązuje się do zaoferowania, nie mniej korzystnych niż określone w Umowie, warunków handlowych spółkom z Grupy ORLEN.

## Dla realizacji powyższego, Wykonawca wyraża zgodę na udostępnienie przez Zamawiającego spółkom z Grupy ORLEN treści Umowy oraz na bieżące przekazywanie pomiędzy tymi spółkami a Zamawiającym informacji dotyczących poziomu obrotu osiąganego w związku z zawarciem umów z Wykonawcą.

## Wykonawca jest zobowiązany *do zawarcia odrębnej umowy na warunkach handlowych nie mniej korzystnych niż uzgodnione w Umowie / do podpisania porozumienia o przystąpieniu do Umowy*, które stanowi Dodatek nr 1 do niniejszego Załącznika [**Porozumienie o przystąpieniu**], *pozwalające na przyłączenie się podmiotowi z Grupy ORLEN do warunków współpracy opisanych Umową*. Wykonawca zobowiązuje się do każdorazowego powiadomienia Zamawiającego o zawarciu *umowy z nowym podmiotem / przystąpieniu do Umowy nowego podmiotu* z Grupy ORLEN.

## Zamawiający oraz podmioty z Grupy ORLEN będą ponosiły odrębnie od siebie odpowiedzialność za wszystkie działania lub zaniechania na podstawie poszczególnych umów zawartych przez nie z Wykonawcą, w szczególności Zamawiający nie będzie ponosił odpowiedzialności za zapłatę jakichkolwiek kwot, do których zapłacenia na rzecz Wykonawcy zobowiązane będą podmioty z Grupy ORLEN.

## W przypadku, gdy pomiędzy Wykonawcą, a spółką z Grupy ORLEN zostały zawarte wcześniej umowy ramowe obejmujące swoim zakresem przedmiot Umowy, Wykonawca zobowiązuje się do dostosowania zapisów wcześniej zawartych umów do warunków wynikających z Umowy w przypadku, jeśli są one korzystniejsze dla spółki.

**DODATEK NR 1 [POROZUMIENIE O PRZYSTĄPIENIU] DO ZałącznikA NR 20 DO UMOWY WDROŻENIOWEJ [KLAUZULA GRUPY ORLEN]**

**POROZUMIENIE O PRZYSTĄPIENIU DO UMOWY**

Numer ………………….. [numer umowy lokalnej w spółce]

Nazwa spółki:

Siedziba spółki:

NIP spółki:

Działając w imieniu………………………………………………………………………………………………...

z siedzibą w………………………………………………………………………………………………………...

zarejestrowaną w…………………………………………………………………………………………………..

(dalej zwaną „**PODMIOTEM PRZYSTĘPUJĄCYM**” lub „**Spółką**”), będąc uprawnionym/nymi do reprezentowania Spółki zgodnie z zasadą reprezentacji Spółki ujawnioną w odpisie z rejestru przedsiębiorców Krajowego Rejestru Sądowego, stanowiącym załącznik do niniejszego porozumienia, oświadczam/my, że:

Przystępujemy do Umowy ramowej / o współpracy o numerze …………….……………… [numer umowy w ORLEN S.A.] zawartej w dniu …………………………….. (dalej zwanej „**Umową**”) pomiędzy ……………………………………………………………………………………………………… (zwany dalej Sprzedającym/Dostawcą/Wykonawcą\*) a **ORLEN Spółką Akcyjną z siedzibą** w Płocku, ul. Chemików 7, 09-411 Płock, wpisanym do KRS pod numerem: 0000028860 (dalej zwanym „**Zamawiającym**” lub „**ORLEN S.A.**”) ze skutkiem prawnym od dnia otrzymania przez Sprzedającego/Dostawcę/Wykonawcę\* niniejszego porozumienia.

Dalej oświadczam/my, że zapoznałem/łam/liśmy się z treścią i warunkami Umowy, nie zgłaszam/my do treści żadnych zastrzeżeń i akceptujemy ją w całości.

Integralną częścią porozumienia jest aktualny odpis z rejestru przedsiębiorców Krajowego Rejestru Sądowego, zaświadczenie o nadaniu NIP oraz zaświadczenie o numerze identyfikacyjnym REGON PODMIOTU PRZYSTĘPUJĄCEGO.

Jednocześnie udzielamy pełnomocnictwa spółce:

**ORLEN Spółka Akcyjna** z siedzibą w Płocku przy ul. Chemików 7, 09-411 Płock, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS: 0000028860, której dokumentacja rejestrowa jest przechowywana przez Sąd Rejonowy dla Łodzi-Śródmieścia w Łodzi XX Wydział Gospodarczy – Krajowego Rejestru Sądowego, NIP: 7740001454, REGON: 610188201, BDO: 000007103, o kapitale zakładowym w wysokości 1 451 177 561,25 zł, opłaconym w całości(dalej zwaną„**ORLEN S.A.**”)

do dokonywania zmian (aneksowania) w naszym imieniu Umowy na warunkach według uznania ORLEN S.A.

ORLEN S.A. może ustanawiać innych pełnomocników (substytutów).

Sprzedający/Dostawca/Wykonawca\* oraz PODMIOT PRZYSTĘPUJĄCY ustalają następujące zasady realizacji zleceń/zamówień i dokonywania rozliczeń na podstawie zawartego porozumienia o przystąpieniu do Umowy:

* Obowiązujący maksymalny limit realizacji zleceń/zamówień przez PODMIOT PRZYSTĘPUJĄCY:

…………………………………………………………………………………………………………………

* Forma wystawiania zleceń/zamówień w ramach zawartego porozumienia o nr:

…………………………………………………………………………………………………………………

………………………………….……………………………………………………………………………..

* Fakturowanie i płatności:

PODMIOT PRZYSTĘPUJĄCY oświadcza, że jest czynnym podatnikiem podatku VAT, posiada NIP………………………………. i jest uprawniony do otrzymywania faktur.

Faktury za realizację zleceń/zamówień wystawiane będą na adres PODMIOTU PRZYSTĘPUJĄCEGO:

……………………………………………………………………………………………………………………….

Faktury za realizację zleceń/zamówień będą zawierały dodatkowe informacje:

* numer porozumienia;
* numer zlecenia/zamówienia;
* imię i nazwisko osoby zlecającej zlecenie/zamówienie.

Wynagrodzenie za realizację przedmiotu Umowy będzie płatne na rachunek bankowy Sprzedającego/Dostawcy/Wykonawcy\* każdorazowo wskazany na fakturze, na podstawie wystawionej właściwej, pod względem merytorycznym i formalnym, faktury.

Termin płatności wynosi …………………….. dni od daty wpływu prawidłowo wystawionej faktury (w tym faktury korygującej) do siedziby PODMIOTU PRZYSTĘPUJĄCEGO.

Płatność wynikająca z faktur będzie realizowana w mechanizmie podzielonej płatności zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2021 r., poz. 685 ze zm.).

ORLEN S.A. oraz PODMIOT PRZYSTĘPUJĄCY będą ponosiły odrębnie od siebie odpowiedzialność za wszystkie działania lub zaniechania na podstawie zawartych przez nie umów ze Sprzedawcą/Dostawcą/Wykonawcą\*, w szczególności ORLEN S.A. nie będzie ponosił odpowiedzialności za zapłatę jakichkolwiek kwot, do których zapłacenia na rzecz Sprzedawcy/Dostawcy/Wykonawcy\* zobowiązany jest PODMIOT PRZYSTĘPUJĄCY.

Sprzedawca/Dostawca/Wykonawca\* zobowiązany jest do wypełnienia, w imieniu PODMIOTU PRZYSTĘPUJĄCEGO jako Administratora danych w rozumieniu obowiązujących przepisów prawa o ochronie danych osobowych, niezwłocznie, jednakże nie później niż w terminie 30 (trzydzieści) dni od dnia zawarcia niniejszego porozumienia ze Sprzedawcą/Dostawcą/Wykonawcą\*, obowiązku informacyjnego wobec osób fizycznych zatrudnionych przez Sprzedawcę/Dostawcę/Wykonawcę\* lub współpracujących ze Sprzedawcą/Dostawcą/Wykonawcą\* przy zawarciu lub realizacji Umowy - bez względu na podstawę prawną tej współpracy, w tym także członków organów Sprzedawcy/Dostawcy/Wykonawcy\*, prokurentów lub pełnomocników reprezentujących Sprzedawcę/Dostawcę/Wykonawcę\* - których dane osobowe udostępnione zostały do PODMIOTU PRZYSTĘPUJĄCEGO przez Sprzedawcę/Dostawcę/Wykonawcę\* w związku z zawarciem lub realizacją niniejszego porozumienia. Obowiązek, o którym mowa w zdaniu poprzedzającym powinien zostać spełniony poprzez przekazanie tym osobom klauzuli informacyjnej stanowiącej Załącznik nr 1 do niniejszego porozumienia, przy jednoczesnym zachowaniu zasady rozliczalności.

Załącznik nr 1 [Zasady przetwarzania przez PODMIOT PRZYSTĘPUJĄCY danych osobowych pracowników, współpracowników, reprezentantów, pełnomocników Sprzedającego/Dostawcy/Wykonawcy]\*\*

------------------------------------------------------- --------------------------------------------------------

Podpis i pieczęć Podpis i pieczęć

Sprzedającego/Dostawcy/Wykonawcy\* PODMIOTU PRZYSTĘPUJĄCEGO

*\*stosowny wariant do wyboru*

*\*\* załącznik nr 1 [Zasady przetwarzania przez PODMIOT PRZYSTĘPUJĄCY danych osobowych pracowników, współpracowników, reprezentantów, pełnomocników Sprzedającego/Dostawcy/Wykonawcy] załączany jest przez PODMIOT PRZYSTĘPUJĄCY na etapie zawarcia niniejszego porozumienia*

# Załącznik nr 21 do UMOWY WDROŻENIOWEJ [KLAUZULE KSEF]

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# KLAUZULE KSEF

1. Poniższe postanowienia będą miały zastosowanie od dnia, w którym Wykonawca zostanie zobowiązany do wystawiania i udostępnienia Zamawiającemu faktur ustrukturyzowanych przy użyciu Krajowego Systemu e-Faktur (dalej: **KSeF**) na podstawie przepisów ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (dalej: **ustawa o VAT**) i od tego dnia będą miały pierwszeństwo w przypadku rozbieżności z innymi postanowieniami Umowy.

2. Wykonawca wystawi i udostępni Zamawiającemu fakturę z wykorzystaniem KSeF, chyba że zaistnieją przypadki, o których mowa w ustawie o VAT uniemożliwiające takie działanie lub uprawniające Wykonawcę do innego działania – w takim przypadku faktura zostanie wystawiona i udostępniona Zamawiającemu z uwzględnieniem zasad określonych w ustawie o VAT i niżej wskazanych ustępów.

3. Zapłata należnego Wykonawcy wynagrodzenia nastąpi w oparciu o wystawioną na zasadach określonych w ust. 2 powyżej fakturę na numer rachunku bankowego [**…**] oraz w terminie 60 dni od dnia doręczenia faktury.

4. Za datę wystawienia faktury ustrukturyzowanej uznaje się datę przesłania faktury przez Wykonawcę do KSeF, a w przypadku faktury, o której mowa w art. 106 nda ust. 1 lub ust. 16 ustawy o VAT lub faktur wystawianych w okresie awarii lub niedostępności KSeF – datę wystawienia wskazaną przez Wykonawcę na tej fakturze.

5. Za dzień skutecznego doręczenia faktury Zamawiającemu uznaje się dzień jej otrzymania w rozumieniu przepisów ustawy o VAT; w przypadku faktury ustrukturyzowanej będzie to zatem dzień przydzielenia jej indywidualnego numeru identyfikującego tę fakturę w KSeF.

6. Jeżeli ustawa o VAT dopuszcza możliwość udostępnienia Zamawiającemu faktury w sposób inny niż przy użyciu KSeF, taka faktura może zostać doręczona Zamawiającemu na jeden z następujących adresów:

a) Biuro Zakupów 09-411 Płock ul. Chemików 7 (za datę skutecznego doręczenia faktury w takim przypadku będzie uznawana data doręczenia Zamawiającemu przesyłki listowej zawierającej ww. fakturę, oznaczoną odpowiednimi kodami zgodnie z ustawą o VAT (z zastrzeżeniem, że w przypadku braku odbioru takiej przesyłki faktura będzie uznana za skutecznie doręczoną po upływie 14 dni od pozostawienia pierwszego zawiadomienia o próbie doręczenia takiej przesyłki) lub data nadania fakturze numeru identyfikującego KSeF – w zależności od tego, która z wymienionych sytuacji nastąpi pierwsza).

b) e-mail: [efaktura@orlen.pl](mailto:efaktura@orlen.pl) (za datę skutecznego doręczenia faktury w takim przypadku będzie uznawana data wysłania przez Wykonawcę do Zamawiającego wiadomości e-mail zawierającej ww. fakturę, np. w formacie pdf, oznaczoną odpowiednimi kodami zgodnie z ustawą o VAT lub data nadania fakturze numeru identyfikującego w KSeF – w zależności od tego, która z wymienionych sytuacji nastąpi pierwsza).

7. Faktura będzie uznana za prawidłowo wystawioną, jeżeli zostanie wystawiona z uwzględnieniem zasad wystawiania faktur określonych w ustawie o VAT.

8. Zasady o których mowa w ust. 5 i 6 powyżej stosuje się odpowiednio do załączników ustrukturyzowanych.

# Załącznik nr 22 do UMOWY WDROŻENIOWEJ [LISTA UTWORÓW STANDARDOWYCH]

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# LISTA UTWORÓW STANDARDOWYCH

# Załącznik nr 23 do UMOWY WDROŻENIOWEJ [WZÓR PPDO]

# POSTANOWIENIA OGÓLNE

## Niniejszy Załącznik stanowi integralną część Umowy.

## Pojęciom pisanym w Załączniku wielką literą, które nie zostały w niniejszym Załączniku zdefiniowane, Strony nadają znaczenie przyjęte w Umowie.

# WZÓR PPDO

POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH (PPDO)

1. OŚWIADCZENIA STRON
2. Strony oświadczają, że PPDO reguluje kwestie, o których mowa w art. 28 Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 (dalej: RODO) w związku z zawarciem Umowy (czyli umowy głównej, do której PPDO stanowi załącznik).
3. [ORLEN S.A.][[38]](#footnote-39) oświadcza, iż jest administratorem danych osobowych w rozumieniu art. 4 pkt 7) RODO, tj. podmiotem który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
4. Przetwarzający […][[39]](#footnote-40) oświadcza, iż jest podmiotem przetwarzającym w rozumieniu art. 4 pkt. 8) RODO i dysponuje środkami, doświadczeniem, wiedzą i wykwalifikowanym personelem, co umożliwia mu prawidłowe wykonanie postanowień PPDO, w tym zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane będzie przetwarzał na podstawie Umowy.
5. Administrator oświadcza, że w sprawach związanych z przetwarzaniem danych osobowych możliwy jest kontakt z nim za pośrednictwem poczty elektronicznej na adres: […] lub pisemnie na adres siedziby Administratora wskazany w komparycji Umowy.
6. Przetwarzający oświadcza, że w sprawach związanych z przetwarzaniem danych osobowych możliwy jest kontakt z nim za pośrednictwem poczty elektronicznej na adres: […] lub pisemnie na adres siedziby Przetwarzającego wskazany w komparycji Umowy.
7. Wszelka korespondencja dotycząca PPDO będzie kierowana przez Strony na wskazane w pkt 1.4 – 1.5 adresy e-mail.
8. PRZEDMIOT, CEL I PODSTAWOWE ZASADY POWIERZENIA PRZETWARZANIA
9. Administrator powierza Przetwarzającemu do przetwarzania dane osobowe, a Przetwarzający zobowiązuje się do ich przetwarzania wyłącznie na udokumentowane polecenie Administratora, zgodnie z zakresem określonym w PPDO oraz innymi udokumentowanymi instrukcjami przekazanymi przez Administratora, zgodnie z obowiązującym prawem.
10. Przetwarzanie danych osobowych odbywa się w celu wykonania Umowy, zgodnie z jej przedmiotem oraz zakresem i sposobem przetwarzania określonym w PPDO.
11. Zakres powierzonych do przetwarzania danych na podstawie PPDO obejmuje:

|  |  |
| --- | --- |
| **Kategorie osób**, których dane powierzono do przetwarzania | [Przykłady do weryfikacji w przypisie dolnym][[40]](#footnote-41) |
| **Kategorie przetwarzanych danych** (rodzaj powierzonych danych osobowych) | [Przykłady do weryfikacji w przypisie dolnym][[41]](#footnote-42) |
| **Charakter i cel przetwarzania** (czynności przetwarzania podejmowane w kontekście charakteru i celu przetwarzania z Umowy) | [Przykłady do weryfikacji w przypisie dolnym][[42]](#footnote-43) |

1. W przypadku braku określenia zakresu powierzonych do przetwarzania danych w pkt 2.3, PPDO stanowi jedynie wzór i nie wywołuje skutków prawnych do czasu wskazania zakresu danych przez Administratora w sposób określony w pkt 2.5 – 2.8.
2. Zmiana zakresu powierzonych do przetwarzania danych osobowych następuje w formie pisemnej, w tym elektronicznej, poprzez przesłanie przez Administratora oświadczenia zawierającego nowy zakres danych na wskazany w pkt 1.5 adres e-mail Przetwarzającego, bez konieczności sporządzania aneksu.
3. Przetwarzający zobowiązany jest do niezwłocznego potwierdzenia otrzymania oraz wdrożenia zmiany zakresu danych osobowych, przesyłając potwierdzenie zwrotne na adres e-mail Administratora wskazany w pkt 1.4, nie później niż w ciągu 2 dni roboczych od otrzymania oświadczenia.
4. Wszelka korespondencja dotycząca zmiany zakresu danych osobowych powinna być archiwizowana przez obie Strony w sposób umożliwiający jej późniejsze udokumentowanie na potrzeby ewentualnych kontroli lub postępowań.
5. Zmiana zakresu danych osobowych staje się skuteczna z chwilą otrzymania przez Administratora potwierdzenia wdrożenia zmiany przez Przetwarzającego.
6. Dane osobowe mogą być przetwarzane przez Przetwarzającego zarówno w formie elektronicznej (w systemach informatycznych), jak i w formie papierowej – w zależności od potrzeb i charakteru realizowanych czynności przetwarzania.
7. Przy przetwarzaniu danych osobowych, Przetwarzający powinien przestrzegać zasad wskazanych w PPDO oraz w RODO, a także w innych przepisach prawa powszechnie obowiązującego regulujących ochronę danych osobowych.
8. Przetwarzający przyjmuje do wiadomości, że przetwarzanie przez niego powierzonych danych osobowych w szerszym zakresie lub dla realizacji innych celów niż wskazane w pkt 2.2 – 2.3 PPDO, przy braku dysponowania odpowiednią podstawą prawną, będzie stanowiło naruszenie przepisów RODO oraz istotnych postanowień Umowy, oraz może stanowić podstawę do jej wypowiedzenia w trybie natychmiastowym oraz wyciągnięcia konsekwencji z niej wynikających lub przewidzianych przepisami prawa.
9. SZCZEGÓŁOWE ZASADY POWIERZENIA PRZETWARZANIA

3.1 Przed rozpoczęciem przetwarzania danych osobowych Przetwarzający musi podjąć środki zabezpieczające dane osobowe, o których mowa w art. 32 RODO w szczególności:

1. uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, zastosować środki techniczne i organizacyjne zapewniające bezpieczeństwo przetwarzanych danych osobowych. Przetwarzający powinien odpowiednio udokumentować zastosowanie tych środków,
2. umożliwiać Administratorowi, efektywne przeprowadzenie audytu lub inspekcji, o których mowa w pkt 9 poniżej,
3. zapewnić, by każda osoba fizyczna działająca z upoważnienia Przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie Administratora, została przeszkolona z zasad ochrony danych osobowych oraz została zobowiązana do zachowania ich w tajemnicy,

3.2 Przetwarzający nie będzie kopiować, powielać (z zastrzeżeniem pkt 4.2 g)) lub w jakikolwiek sposób rozpowszechniać danych osobowych, z wyjątkiem sytuacji, gdy działanie takie jest konieczne w celu wykonania Umowy.

* 1. Przetwarzający zobowiązuje się niezwłocznie informować Administratora, jeżeli zdaniem Przetwarzającego wydane mu polecenie stanowi naruszenie RODO lub innych przepisów o ochronie danych osobowych.

1. MINIMALNE WYMAGANIA FORMALNE I TECHNICZNE

4.1 Wymagania formalne:

1. Przetwarzający zobowiązany jest zapewnić, aby zarządzanie infrastrukturą teleinformatyczną oraz aplikacjami wykorzystywanymi do realizacji Umowy jest prowadzone zgodnie z dobrymi, uznanymi praktykami bezpieczeństwa teleinformatycznego,
2. Przetwarzający zobowiązuje się do niezwłocznego powiadamiania Administratora o zaistniałych naruszeniach lub incydentach bezpieczeństwa teleinformatycznego mających bezpośredni wpływ na powierzone dane osobowe,
3. w przypadku, gdy wykonanie Umowy wiąże się z ryzykiem utraty atrybutów bezpieczeństwa danych (poufności, integralności i dostępności danych), Przetwarzający zobowiązany jest poinformować o tym Administratora przed przystąpieniem do wykonywania jakichkolwiek prac oraz umożliwić Administratorowi przeprowadzenie działań zapewniających zachowanie ww. atrybutów,
4. Przetwarzający odpowiada za skutki działań pracowników oraz osób trzecich, którym powierzył wykonanie czynności na rzecz Administratora tak, jak za czynności własne.
5. Wymagania techniczne (dla systemów teleinformatycznych Przetwarzającego):
6. Przetwarzający zobowiązuje się do zapewnienia kontroli dostępu w systemach teleinformatycznych.
7. logowanie do systemów teleinformatycznych możliwe jest wyłącznie w oparciu o indywidualny login użytkownika i hasło lub inne środki zapewniające atrybut rozliczalności.
8. Przetwarzający zobowiązany jest posiadać działające mechanizmy usuwania danych na wniosek Administratora.
9. Przetwarzający zobowiązany jest posiadać zabezpieczenia systemów teleinformatycznych przed złośliwym oprogramowaniem, w tym przed kradzieżą lub zniszczeniem danych.
10. Przetwarzający zobowiązany jest do zapewnienia zabezpieczenia dostępu zdalnego do systemów teleinformatycznych poprzez stosowanie bezpiecznych i szyfrowanych połączeń VPN.
11. Przetwarzający zobowiązany jest do zarządzania podatnościami w systemach teleinformatycznych, w tym m.in.: testowania cyberbezpieczeństwa infrastruktury i aplikacji, procedury zarządzania aktualizacjami.
12. Przetwarzający zobowiązany jest do zarządzania ciągłością działania, w tym m.in. tworzenia kopii zapasowych i testów przywracania z kopii zapasowych oraz stosowania mechanizmów zapewniających wysoką dostępność systemów.
13. Przetwarzający zobowiązany jest posiadać systemy monitorowania infrastruktury oraz sieci teleinformatycznych pod kątem cyberbezpieczeństwa.
14. OBOWIĄZKI PRZETWARZAJĄCEGO
15. Przetwarzający zobowiązuje się pomagać Administratorowi w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO. W szczególności, Przetwarzający zobowiązuje się przekazywać Administratorowi informacje oraz wykonywać jego polecenia dotyczące stosowanych środków zabezpieczania danych osobowych oraz przypadków naruszenia ochrony danych osobowych. Przetwarzający ma ponadto obowiązek:
16. przekazania Administratorowi informacji dotyczących zdarzenia mogącego stanowić naruszenie ochrony danych osobowych niezwłocznie, jednak nie później niż w ciągu 24 godzin od wykrycia zdarzenia na adres e-mail wskazany w pkt 1.4. Zgłoszenia zdarzenia musi zawierać informacje o zdarzeniu (dacie, godzinie jego wystąpienia/identyfikacji), charakteru i rodzaju zdarzenia, zakresu naruszenia, środkach zaradczych i podjętych działaniach, ocenę ryzyka (jeśli możliwa), wstępną ocenę ryzyka dla praw i wolności osób fizycznych, załączniki (logi systemowe, raporty, zrzuty ekranu, inne dokumenty pomocnicze).
17. wyznaczenia osób odpowiedzialnych za podjęcie działań w celu zaradzenia negatywnym skutkom naruszenia i podjęcia w uzgodnieniu z Administratorem działań naprawczych oraz ograniczających ryzyko ponownego wystąpienia naruszenia ochrony danych osobowych;
18. udzielania Administratorowi informacji potrzebnych do dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, o których mowa w art. 35 RODO;
19. udzielania Administratorowi informacji potrzebnych do konsultacji z organem nadzorczym w zakresie oceny skutków dla ochrony danych, o których mowa w art. 35 oraz art. 36 RODO.
20. Przetwarzający zobowiązuje się pomagać Administratorowi, w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w art. 15-22 RODO. W szczególności, Przetwarzający zobowiązuje się:
21. w razie zgłoszenia przez osobę, której dane dotyczą żądania prawa dostępu, o którym mowa w art. 15 RODO, do przygotowania raportu dla Administratora umożliwiającego przedstawienie osobie, której dane dotyczą przez Administratora informacji, o których mowa w art. 15 ust. 1 RODO.
22. w razie zgłoszenia przez osobę, której dane dotyczą prawa do sprostowania danych, o którym mowa w art. 16 RODO, do odnotowania żądania osoby, której dane dotyczą poprzez nadpisanie danych osobowych tej osoby w systemach Przetwarzającego,
23. w razie zgłoszenia przez osobę, której dane dotyczą prawa do bycia zapomnianym, o którym mowa w art. 17 RODO, do usunięcia danych osobowych ze wszystkich systemów Przetwarzającego, w których mogą się znaleźć dane osobowe tej osoby, w szczególności z systemów źródłowych agregujących dane. Po upływie 90 dni od zgłoszenia żądania Przetwarzający przeprowadza szczegółową analizę czy dane osoby, która zgłosiła żądanie zostały usunięte ze wszystkich systemów Przetwarzającego oraz przedstawia wyniki tej analizy Administratorowi w formie raportu,
24. w razie zgłoszenia przez osobę, której dane dotyczą prawa do ograniczenia przetwarzania, o którym mowa w art. 18 RODO, do czasowego zablokowania możliwości edycji rekordów związanych z osobą, której dane dotyczą niezwłocznie, nie później niż w ciągu 24 godzin od przedstawienia takiego polecenia przez Administratora,
25. w razie zgłoszenia przez osobę, której dane dotyczą prawa do przenoszenia danych, o którym mowa w art. 20 RODO, do wyeksportowania do Administratora wszystkich danych osobowych dotyczących tej osoby przetwarzanych elektronicznie,
26. w razie zgłoszenia przez osobę, której dane dotyczą prawa do sprzeciwu, o którym mowa w art. 21 RODO, do przekazania informacji Administratorowi.
27. W celu wywiązywania się z obowiązków, o których mowa w pkt 5.2, Administrator może zobowiązać Przetwarzającego do wprowadzenia do systemu informatycznego Przetwarzającego funkcjonalności umożliwiających co najmniej: sporządzenie kopii danych, usuwanie danych, sprostowanie danych, ograniczenie przetwarzania danych, sporządzenie pliku umożliwiającego przenoszalność danych i odnotowywanie zgłoszenia sprzeciwu.

5.4 Przetwarzający zobowiązuje się udostępnić Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków przez Administratora oraz Przetwarzającego, o których mowa w art. 28 RODO.

1. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o:
2. jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania danych osobowych przez Przetwarzającego,
3. jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania danych osobowych, skierowanej do Przetwarzającego,
4. wszelkich audytach, kontrolach i inspekcjach dotyczących przetwarzania danych osobowych przez Przetwarzającego, w szczególności prowadzonych przez organ nadzorczy,
5. jakimkolwiek żądaniu sądów, organów ścigania lub innych urzędów państwowych polskich lub międzynarodowych dotyczących ujawnienia lub udostępnienia danych osobowych, chyba, że poinformowanie Administratora nie jest dozwolone na podstawie przepisów obowiązującego prawa.
6. ZASADY ZABEZPIECZENIA DANYCH OSOBOWYCH PRZEKAZYWANYCH W POSTACI ELEKTRONICZNEJ

W przypadku konieczności wymiany danych osobowych w postaci elektronicznej, Administrator dopuszcza możliwość przekazywania ich wyłącznie w formie plików, z uwzględnieniem poniższych zasad:

1. pliki podlegają zabezpieczeniu kryptograficznemu i są zabezpieczone hasłem;
2. nadawca, po uzyskaniu od odbiorcy potwierdzenia otrzymania zabezpieczonych załączników, przekazuje odbiorcy hasło zabezpieczające (klucz szyfrujący) poprzez przesłanie go innym kanałem komunikacji np. w drodze połączenia telefonicznego lub SMS,
3. przesyłanie plików odbywa się pomiędzy kontami pocztowymi Administratora, a kontami pocztowymi Przetwarzającego udostępnionymi w związku z realizacją Umowy.
4. TRANSFER DANYCH OSOBOWYCH
5. Przetwarzający zapewnia, że dane osobowe nie będą przekazywane poza Europejski Obszar Gospodarczy lub do krajów/organizacji, dla których Komisja Europejska nie potwierdziła zapewnienia odpowiedniego stopnia ochrony danych osobowych.
6. W przypadku innym niż określony w punkcie 8.1, Przetwarzający zobowiązany jest pozyskać uprzednią zgodę Administratora na przekazanie danych osobowych do państwa trzeciego, które znajduje się poza Europejskim Obszarem Gospodarczym, co najmniej w formie dokumentowej. Zgoda wyrażana jest po spełnieniu poniższych warunków:
7. państwo docelowe zapewnia, zgodnie z odpowiednią decyzją Komisji Europejskiej, adekwatny poziom ochrony danych osobowych do tego, który obowiązuje w Unii Europejskiej; lub
8. Przetwarzający i podprocesor zawarli umowę z wykorzystaniem standardowych klauzul umownych oraz wdrożyli inny środek uzupełniający określony w Zaleceniach 01/2020 Europejskiej Rady Ochrony Danych, z dnia 10.11.2020r., oraz
9. Przetwarzający udostępnił Administratorowi ocenę, której celem jest ustalenie czy prawo państwa trzeciego zapewnia właściwą, w świetle prawa Unii, ochronę przekazywanych danych osobowych (Tranfer Impact Assessment, TIA).
10. PODPOWIERZENIE PRZETWARZANIA
11. Przetwarzający jest uprawniony do korzystania z podprocesora wyłącznie po uzyskaniu uprzedniej zgody Administratora wyrażonej w formie dokumentowej pod rygorem bezskuteczności.
12. W przypadku wystąpienia o zgodę, o której mowa w pkt 8.1 powyżej Przetwarzający przekazuje Administratorowi informacje na temat podprocesora (firmę oraz dane kontaktowe podmiotu), a także informacje o charakterze i czasie trwania podpowierzenia, zakresie i celu przetwarzania danych osobowych, rodzaju (kategoriach) danych osobowych i kategoriach osób, których dane miałyby być podpowierzone.
13. Podpowierzenie przetwarzania danych osobowych przez Przetwarzającego jest dopuszczalne tylko na podstawie umowy podpowierzenia. Na podstawie umowy podpowierzenia podprocesor zobowiąże się do spełniania tych samych obowiązków i wymogów, które na mocy Umowy nałożone są na Przetwarzającego.
14. W zawartej umowie podpowierzenia, Przetwarzający zapewni w szczególności, iż:
15. Administratorowi będą przysługiwały uprawnienia wynikające z umowy podpowierzenia bezpośrednio wobec podprocesora,
16. podprocesor będzie stosować co najmniej równorzędny poziom ochrony danych osobowych co Przetwarzający,
17. podprocesor w żadnym przypadku nie będzie uprawniony do dalszego powierzania przetwarzania danych osobowych.
18. Jeżeli podprocesor nie wywiąże się ze spoczywających na nim obowiązków ochrony danych osobowych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków tego podmiotu spoczywa na Przetwarzającym.
19. Przetwarzający zobowiązany jest prowadzić aktualną listę podprocesorów. Przetwarzający zobowiązany jest przekazać taką listę Administratorowi na jego każde żądanie.
20. AUDYT I INSPEKCJA PRZETWARZAJĄCEGO
21. Administrator jest uprawniony do weryfikacji przestrzegania zasad przetwarzania danych osobowych wynikających z RODO oraz PPDO przez Przetwarzającego, poprzez prawo żądania w każdym czasie, także po utracie mocy obowiązującej przez Umowę lub PPDO, udzielenia wszelkich informacji lub udostępnienia wszelkich dokumentów, procedur i rejestrów dotyczących powierzonych danych osobowych, w tym informacji o lokalizacji przetwarzania danych osobowych przez Przetwarzającego.
22. Administrator ma także prawo przeprowadzania audytów lub inspekcji Przetwarzającego w zakresie zgodności operacji przetwarzania z prawem i z PPDO, za pośrednictwem upoważnionych pracowników Administratora, podmiotu dominującego w Grupie Kapitałowej Administratora lub zewnętrznego podmiotu profesjonalnie zajmującego się oceną i kontrolą procesów bezpieczeństwa danych osobowych i informacji („Audytorzy Administratora”).
23. Administrator poinformuje Przetwarzającego o planowanym audycie lub inspekcji, w formie dokumentowej co najmniej na 7 (siedem) dni przed planowanym terminem ich rozpoczęcia, ze wskazaniem w formie dokumentowej Audytorów Administratora.
24. W przypadku powzięcia przez Administratora uzasadnionych informacji odnośnie zagrożenia bezpieczeństwa przetwarzania danych osobowych przez Przetwarzającego lub któregokolwiek z podprocesorów lub zaistnienia naruszenia ochrony danych osobowych Administrator uprawniony jest do przeprowadzenia audytów lub inspekcji po zawiadomieniu Przetwarzającego o takim zamiarze, co najmniej na 1 (jeden) dzień przed planowanym terminem rozpoczęcia audytu lub inspekcji.
25. W trakcie audytu lub inspekcji, Audytorzy Administratora mają prawo do:
26. wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z powierzeniem przetwarzania na podstawie PPDO,
27. przeprowadzania oględzin urządzeń, nośników danych oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych włącznie z ich zawartością,
28. żądania złożenia wyjaśnień przez Przetwarzającego oraz pracowników Przetwarzającego w określonej przez Administratora formie i w zakresie niezbędnym do ustalenia stanu faktycznego.
29. Administrator jest uprawniony do przeprowadzenia audytu lub inspekcji w dniach roboczych, w godzinach pracy podmiotu audytowanego.
30. Przetwarzający zapewnia Audytorom Administratora warunki i środki niezbędne do sprawnego przeprowadzenia audytu lub inspekcji, a w szczególności sporządza we własnym zakresie kopie lub wydruki dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub w systemach służących do przetwarzania danych osobowych.
31. Po zakończeniu audytu lub inspekcji Audytor Administratora przedstawia Przetwarzającemu raport z audytu, lub w przypadku inspekcji, informację w formie pisemnej.
32. W przypadku ujawnienia jakichkolwiek nieprawidłowości, naruszeń lub innych okoliczności, które zostaną uznane przez Administratora za niezgodne z warunkami Umowy w tym PPDO lub przepisami prawa obowiązującego w okresie obowiązywania Umowy („Niezgodność/Niezgodności”), Przetwarzający oraz każdy z podprocesorów, których dotyczy taka Niezgodność, są zobowiązani do jej usunięcia na własny koszt w terminie wskazanym w formie dokumentowej w rekomendacji Administratora, w zależności od uznania Audytora Administratora.
33. Dla uniknięcia jakichkolwiek wątpliwości, Przetwarzający oraz podprocesor, wyrażają zgodę na przeprowadzenie audytu i/lub inspekcji, o której mowa w niniejszym punkcie oraz zobowiązują się do pełnej współpracy z Administratorem oraz Audytorami Administratora w trakcie audytów oraz inspekcji. Jakiekolwiek uniemożliwianie, utrudnianie lub inne podobne działania podejmowane przez Przetwarzającego lub podprocesora, wobec Administratora lub Audytorów Administratora mogą być podstawą do rozwiązania Umowy.
34. ODPOWIEDZIALNOŚĆ PRZETWARZAJĄCEGO
35. Przetwarzający odpowiada za szkody, jakie powstaną u Administratora lub osób trzecich w wyniku niezgodnego z przepisami prawa lub PPDO przetwarzania przez Przetwarzającego oraz podprocesora, a w szczególności w związku z udostępnianiem danych osobowych osobom nieupoważnionym.
36. Z zastrzeżeniem poniższych punktów, Przetwarzający ponosi względem Administratora odpowiedzialność za zasadach ogólnych. W przypadku niewykonania lub nienależytego wykonania przez Przetwarzającego PPDO, Przetwarzający zobowiązuje się do zapłaty odszkodowania na zasadach ogólnych.
37. Administrator jest uprawniony do naliczenia Przetwarzającemu następujących kar umownych[[43]](#footnote-44):
38. z tytułu opóźnienia w zgłoszeniu naruszenia w terminie określonym w pkt. 5 PPDO w wysokości 10000,00 złotych za każdą godzinę opóźnienia,
39. z tytułu niezastosowania któregokolwiek z zabezpieczeń wymienionych w PPDO, w wysokości 100000,00 złotych za każdy stwierdzony przypadek,
40. z tytułu naruszenia obowiązku uzyskania zgody Administratora na podpowierzenie przetwarzania danych osobowych – w wysokości 100000,00 złotych za każdy stwierdzony przypadek,
41. z tytułu nie zawarcia w umowie podpowierzenia postanowień, o których mowa w pkt. 8 PPDO – w wysokości 100000,00 złotych za każdy stwierdzony przypadek,
42. z tytułu uniemożliwienia Administratorowi przeprowadzenia audytu lub inspekcji, o których mowa w pkt. 9 PPDO, w wysokości 100000,00 złotych za każdy przypadek,
43. z tytułu naruszenia obowiązku uzyskania zgody Administratora na transfer danych poza obszar EOG, w wysokości 100000,00 złotych za każdy stwierdzony przypadek,
44. z tytułu niewykonania przez Przetwarzającego lub podmiot, którym posługuje się Przetwarzający zobowiązania, o którym mowa w pkt 12.3 i 12.4, Administrator jest uprawniony do naliczenia Przetwarzającemu kary umownej w wysokości do 100000,00 za każdy przypadek naruszenia.
45. W przypadku wszczęcia przeciwko Administratorowi przez osobę trzecią jakiegokolwiek postępowania (w tym sądowego) dotyczącego naruszenia przepisów RODO lub innych przepisów prawa w związku z przetwarzaniem danych osobowych przez Przetwarzającego lub podprocesora, Przetwarzający zobowiązuje się do zapewnienia Administratorowi na swój koszt ochrony sądowej na zasadach wskazanych przez Administratora, a także do poniesienia wszelkich konsekwencji takiego postępowania, w tym w szczególności kosztów wszelkich decyzji administracyjnych, wyroków sądowych, orzeczeń oraz ugód (regres).
46. WYNAGRODZENIE

Wynagrodzenie z tytułu wykonania przedmiotu PPDO należne Przetwarzającemu zawarte jest w Wynagrodzeniu, o którym mowa w Umowie.

1. CZAS TRWANIA PRZETWARZANIA
2. PPDO obowiązuje Przetwarzającego przez czas obowiązywania Umowy, z zastrzeżeniem pkt 12.5.
3. Administrator jest uprawniony do wypowiedzenia Umowy bez terminów wypowiedzenia w przypadku istotnego naruszenia przepisów prawa lub zapisów PPDO przez Przetwarzającego, w szczególności gdy:
4. organ nadzorczy stwierdzi, iż Przetwarzający lub podmiot, którym Przetwarzający się posługuje, nie przestrzegają zasad przetwarzania danych osobowych,
5. prawomocne orzeczenie sądu powszechnego wykaże, że Przetwarzający lub podprocesor, nie przestrzegają zasad przetwarzania danych osobowych,
6. przetwarzania przez Przetwarzającego lub podprocesora, jakichkolwiek danych osobowych niezgodnie z celem i zakresem Umowy oraz PPDO lub umowy podpowierzenia,
7. przetwarzania przez Przetwarzającego lub podprocesora, jakichkolwiek danych osobowych niezgodnie z RODO lub poleceniami Administratora,
8. utrudniania lub uniemożliwiania Administratorowi prowadzenia czynności kontrolnych, o których mowa w pkt. 9,
9. dopuszczenia do przetwarzania danych osobowych osób nieupoważnionych przez Przetwarzającego lub podprocesora,
10. zawarcia umowy podpowierzenia bez zgody Administratora, o którym mowa w pkt. 8,
11. naruszenia obowiązków, o których mowa w pkt 5.
12. Po zakończeniu obowiązywania Umowy lub w przypadku wystąpienia okoliczności wskazanych w 12.2, Przetwarzający zobowiązuje się, w terminie 14 dni kalendarzowych od ich zaistnienia, zwrócić Administratorowi wszystkie powierzone dane osobowe lub, po uzyskaniu zgody Administratora, trwale je usunąć ze wszystkich nośników, także tych używanych przez podprocesora. Zwrot lub usunięcie danych musi zostać potwierdzony protokołem przekazania lub zniszczenia, którego skan należy przesłać Administratorowi w ciągu 3 dni roboczych od wykonania czynności na adres wskazany w pkt 1.4.
13. Administratorowi przysługuje prawo kontroli i nadzoru wykonywania zobowiązań Przetwarzającego, o których mowa w pkt 12.3 powyżej poprzez przeprowadzenie audytu lub inspekcji na zasadach wskazanych w pkt 9.
14. Strony ustalają, iż pomimo wygaśnięcia Umowy bez względu na okoliczności, o których mowa w pkt 12.1 i 12.2 powyżej, pozostają w mocy postanowienia nakładające lub mogące nałożyć jakiekolwiek zobowiązanie na Przetwarzającego, po terminie wygaśnięcia Umowy, w tym w szczególności postanowienia (dotyczące współpracy oraz regresu).

1. **URL (ang. Uniform Resource Locator)** – oznacza ujednolicony format adresowania zasobów (informacji, danych, usług) stosowany w Internecie i w sieciach lokalnych. [↑](#footnote-ref-2)
2. **MAC (ang. Mandatory Access Control - obowiązkowa kontrola dostępu)** – sposób kontroli dostępu w systemie komputerowym. W MAC wyróżnia się podmioty (ang. subject) oraz obiekty (ang. object). Podmiot to użytkownik lub proces. Obiektami mogą być przykładowo: pliki, katalogi, urządzenia, klucze rejestru. Zarówno podmioty jak i obiekty posiadają określone atrybuty bezpieczeństwa. System posiada również zestaw reguł (ang. rule) określających zasady dostępu, zwany polityką (ang. policy). System operacyjny na podstawie atrybutów bezpieczeństwa i polityki udziela bądź odmawia podmiotowi dostępu do obiektu. Zarówno atrybuty bezpieczeństwa jak i polityka są ustalane wyłącznie przez administratora systemu. W odróżnieniu od DAC, użytkownik nie ma wpływu na działanie mechanizmów kontroli dostępu. [↑](#footnote-ref-3)
3. **RBAC (ang. Role Based Access Control)** – sposób kontroli dostępu w systemach komputerowych. W RBAC głównym elementem są role pełnione przez użytkowników w systemie. Dostęp określany jest na podstawie roli jaką pełni użytkownik. [↑](#footnote-ref-4)
4. **Framework (platforma programistyczna)** – jest szkieletem do budowy aplikacji. Definiuje on strukturę aplikacji oraz ogólny mechanizm jej działania, a także dostarcza zestaw komponentów i bibliotek ogólnego przeznaczenia do wykonywania określonych zadań. Programista tworzy aplikację, rozbudowując i dostosowując poszczególne komponenty do wymagań realizowanego projektu, tworząc w ten sposób gotową aplikację. [↑](#footnote-ref-5)
5. **Internet Information Services** (**IIS**) – jest zbiorem usług internetowych dla systemów rodziny Microsoft Windows. [↑](#footnote-ref-6)
6. **Single Sign-on (logowanie pojedyczne)** – możliwość jednorazowego zalogowania się do usługi sieciowej i uzyskania dostępu do wszystkich autoryzowanych zasobów zgodnych z tą usługą. [↑](#footnote-ref-7)
7. **Sandbox (piaskownica)** – mechanizm izolacji uruchomionych procesów mający na celu separację uruchomionego kodu od pozostałych procesów działających w systemie. [↑](#footnote-ref-8)
8. **Infrastruktura klucza publicznego (ang. Public KeyInfrastructure (PKI))** – w ogólności jest to zespół urządzeń, oprogramowania, ludzi, polityk oraz procedur umożliwiający tworzenie, przechowywanie, zarządzanie i rozprowadzanie cyfrowych certyfikatów klucza publicznego. W szczególności jest to szeroko pojęty kryptosystem, w skład którego wchodzą urzędy certyfikacyjne (CA), urzędy rejestracyjne (RA), subskrybenci certyfikatów klucza publicznego (użytkownicy), oprogramowanie oraz sprzęt. Infrastruktura klucza publicznego tworzy hierarchiczną strukturę zaufania, której podstawowym dokumentem jest certyfikat klucza publicznego. Najpopularniejszym standardem certyfikatów PKI jest X.509 w wersji trzeciej. [↑](#footnote-ref-9)
9. **Hash** – liczba obliczona przez funkcję hashującą (jednokierunkową funkcję skrótu). [↑](#footnote-ref-10)
10. **HTTP (ang. Hypertext Transfer Protocol – protokół przesyłania dokumentów hipertekstowych**) - to protokół sieci WWW (ang. World Wide Web). Obecną definicję HTTP stanowi RFC 2616. Za pomocą protokołu HTTP przesyła się żądania udostępnienia dokumentów WWW i informacje o kliknięciu odnośnika oraz informacje z formularzy. Zadaniem stron WWW jest publikowanie informacji – natomiast protokół HTTP właśnie to umożliwia. [↑](#footnote-ref-11)
11. **HTTPS (ang.HyperText Transfer Protocol Secure)** – szyfrowana wersja protokołu HTTP. W przeciwieństwie do komunikacji niezaszyfrowanego tekstu w HTTP klient-serwer, szyfruje go za pomocą protokołu SSL. Zapobiega to przechwytywaniu i zmienianiu przesyłanych danych. [↑](#footnote-ref-12)
12. **Cookie (ciasteczko)** – niewielkie informacje tekstowe, wysyłane przez serwer WWW i zapisywane po stronie użytkownika (zazwyczaj na twardym dysku). Domyślne parametry ciasteczek pozwalają na odczytanie informacji w nich zawartych jedynie serwerowi, który je utworzył. Ciasteczka są stosowane najczęściej w przypadku liczników, sond, sklepów internetowych, stron wymagających logowania, reklam i do monitorowania aktywności odwiedzających. [↑](#footnote-ref-13)
13. **Token**– losowa liczba, która jednoznacznie identyfikuje sesję użytkownika. [↑](#footnote-ref-14)
14. **Atak siłowy (ang. brute-force)** – określenie algorytmu, który opiera się na sukcesywnym sprawdzeniu wszystkich możliwych kombinacji hasła dostępowego. [↑](#footnote-ref-15)
15. **Enkodowanie/Escapowanie** – mechanizm polegający na usuwaniu i/lub kodowaniu znaków specjalnych w sposób który uniemożliwi systemowi ich interpretację w sposób inny niż przewidział to programista. [↑](#footnote-ref-16)
16. **HTML (ang. HyperTextMarkup Language)** – hipertekstowy język znaczników, obecnie szeroko wykorzystywany do tworzenia stron internetowych. [↑](#footnote-ref-17)
17. **JavaScript, JS** – skryptowy język programowania, stworzony przez firmę Netscape, najczęściej stosowany na stronach internetowych. Pod koniec lat 90. XX wieku organizacja ECMA wydała na podstawie JavaScriptu standard języka skryptowego o nazwie ECMAScript. [↑](#footnote-ref-18)
18. **CSS** – Kaskadowe arkusze stylów (ang. Cascading Style Sheets ; w skrócie CSS) to język służący do opisu formy prezentacji (wyświetlania) stron WWW. CSS został opracowany przez organizację W3C w 1996 r. jako potomek języka DSSSL przeznaczony do używania w połączeniu z SGML-em. [↑](#footnote-ref-19)
19. **URI** – Uniform Resource Identifier (ang.Uniform Resource Identifier) jest standardem internetowym umożliwiającym łatwą identyfikację zasobów w sieci. Zdefiniowany jest w dokumencie RFC 2396. URI jest zazwyczaj łańcuchem znaków, zapisanym zgodnie ze składnią określoną w standardzie. Łańcuch ten określa nazwę (URN) lub adres (URL) zasobu, identyfikowanego przez dany URI. URI może zostać sklasyfikowane jako URL (ang. Uniform Resource Locator) lub URN (ang. Uniform Resource Name). Szczególnym przypadkiem URI jest URL, który oprócz identyfikacji zasobu wskazuje również sposób dostępu do niego. [↑](#footnote-ref-20)
20. **SQL (ang. Structured Query Language)** – strukturalny język zapytań używany do tworzenia, modyfikowania baz danych oraz do umieszczania i pobierania danych z baz danych. [↑](#footnote-ref-21)
21. **XML (ang. ExtensibleMarkup Language)** – uniwersalny język formalny przeznaczony do reprezentowania różnych danych w strukturalizowany sposób. [↑](#footnote-ref-22)
22. **LDAP (ang. Lightweight Directory Access Protocol )** – protokół przeznaczony do korzystania z usług katalogowych, bazujący na standardzie X.500. Jest to również nazwa usługi katalogowej pozwalającej na wymianę informacji za pośrednictwem TCP/IP. [↑](#footnote-ref-23)
23. **HSM (ang. Hardware Security Module)** – Sprzętowy moduł kryptograficzny. System służący między innymi do bezpiecznego przechowywania kluczy poufnych. [↑](#footnote-ref-24)
24. **Master secret –** jest to kluczy tajny (kluczy asymetryczny) powiązany z użytkownikiem. [↑](#footnote-ref-25)
25. **TLS (ang. Transport Layer Security)** – przyjęte jako standard w Internecie rozwinięcie protokołu **SSL (ang. SecureSocketLayer)**, zaprojektowanego pierwotnie przez Netscape Communications. TLS zapewnia poufność i integralność transmisji danych, a także uwierzytelnienie serwera, a niekiedy również klienta. Opiera się na szyfrowaniu asymetrycznym oraz certyfikatach X.509. [↑](#footnote-ref-26)
26. **CA** – Urząd certyfikacji, centrum certyfikacji (ang. certificate authority lub certification authority, w skrócie CA) – w kryptografii jest to podmiot, który wystawia certyfikaty cyfrowe. Certyfikat potwierdza własność klucza publicznego poprzez wskazanie podmiotu certyfikatu. Pozwala to innym powołującym się stronom polegać na podpisach lub zapewnieniach złożonych przez klucz prywatny odpowiadającemu kluczowi publicznemu, który jest certyfikowany. W tym modelu relacji zaufania CA jest zaufaną stroną trzecią, której zawierzają zarówno podmiot (właściciel) certyfikatu oraz strona polegająca. Urzędy certyfikacji są charakterystyczne dla wielu systemów infrastruktury klucza publicznego (PKI). [↑](#footnote-ref-27)
27. **DoS (ang. Denial of Service – odmowa usługi)** – atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania. [↑](#footnote-ref-28)
28. **Atak BEAST (BrowserExploitAgainst SSL/TLS)** – atak na protokół SSL/TLS mający na celu deszyfrację komunikacji. [↑](#footnote-ref-29)
29. **Atak CRIME (Compression Ratio Info-leakMadeEasy)** – atak na protokół SSL/TLS mający na celu deszyfrację komunikacji. [↑](#footnote-ref-30)
30. **MITM (ang. Man in the middle) –** atak kryptologiczny polegający na podsłuchu i modyfikacji wiadomości przesyłanych pomiędzy dwiema stronami bez ich wiedzy. [↑](#footnote-ref-31)
31. **MITM PlaintextInjection (ang. SSL/TLS RenegotiationHandshakes MITM Plaintext Data Injection)** – rodzaj ataku polegający na wymuszeniu renegocjacji komunikacji SSL/TLS. [↑](#footnote-ref-32)
32. **GUID (ang. GloballyUniqueIdentifier)** – identyfikator globalnie unikatowy – jest identyfikatorem obiektów w systemie Windows. GUID jest generowany między innymi na podstawie czasu wygenerowania oraz liczb pseudolosowych. Ma on postać 32-znakowego ciągu heksadecymalnego. [↑](#footnote-ref-33)
33. **FIPS 140-2** – standard opracowany i wymagany przez rząd amerykański. Standard dotyczy akredytacji modułów kryptograficznych. [↑](#footnote-ref-34)
34. **VPN/IPsec (Virtual Private Network)** – wirtualna sieć prywatna. Można ją opisać jako "tunel", przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej, jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. Taki kanał może opcjonalnie kompresować lub szyfrować w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa przesyłanych danych. [↑](#footnote-ref-35)
35. **Sól (ang. Salt)** – są to dane dodawane podczas szyfrowania lub przygotowywania skrótu wiadomości (w tym skrótu hasła). [↑](#footnote-ref-36)
36. **SIEM (ang. Security Information and Event Management)** – system do archiwizacji oraz korelacji zdarzeń. Dodatkową funkcją jest możliwość wykrywania incydentów bezpieczeństwa w oparciu o zdarzenia pochodzące z systemów teleinformatycznych. [↑](#footnote-ref-37)
37. **Recovery Point Objective** – określa moment w przeszłości, w którym po raz ostatni została wykonana kopia danych i od którego to momentu będzie można odzyskać dane z backupu. Recovery Time Objective – określa maksymalny czas po awarii potrzebny do przywrócenia działania aplikacji systemów i procesów biznesowych. [↑](#footnote-ref-38)
38. Należy wskazać właściwy podmiot z GK ORLEN, który zawiera umowę. [↑](#footnote-ref-39)
39. Należy wskazać nazwę podmiotu. [↑](#footnote-ref-40)
40. Interesanci, pracownicy, współpracownicy, kandydaci do pracy/współpracy, klienci, klienci biznesowi (prowadzący działalność gospodarczą), potencjalni klienci, praktykanci/stażyści, uczestnicy i laureaci konkursu, członkowie rodzin pracowników oraz byłych pracowników, emeryci i renciści i członkowie ich rodzin. [↑](#footnote-ref-41)
41. dane kontaktowe, PESEL, służbowe dane kontaktowe, dane ewidencyjne dotyczące prowadzonej działalności gospodarczej, dane osobowe wprowadzane do systemu informatycznego XXXX, dane osobowe wprowadzane do aplikacji mobilnej XXXX, dane osobowe zawarte w dokumentacji składanej w związku z zawartą umową, dane osobowe zawarte w dokumentacji pracowniczej, dane osobowe zawarte w formularzach stosowanych w związku z realizacją konkursu XXX, dane osobowe wprowadzane do księgi wejść i wyjść, dane osobowe w postaci nagrania monitoringu, dane osobowe w postaci nagrania rozmowy Contact Center, dane osobowe zawarte w korespondencji przychodzącej i wychodzącej, dane osobowe dotyczące rozliczeń umowy. [↑](#footnote-ref-42)
42. zbieranie, utrwalanie, porządkowanie, przechowywanie, wykorzystywanie (do celów wskazanych w pkt 2.2 powyżej), ujawnianie innym podmiotom zgodnie z przepisami prawa, postanowieniami Umowy lub na polecenie Administratora, usuwanie. [↑](#footnote-ref-43)
43. Właściciel merytoryczny może podjąć decyzję o zmniejszeniu lub zwiększeniu kary. [↑](#footnote-ref-44)