UMOWA O POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w Warszawie, dnia _____ _____ roku (dalej „**Umowa**"), pomiędzy:

„_____", z siedzibą w _____,, ul. _____ wpisaną do rejestru przedsiębiorców przez Sąd Rejonowy dla Warszawy, Wydział _____ Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS _____ posiadającą kapitał zakładowy w wysokości _____, legitymującą się Numerem Identyfikacji Podatkowej (NIP): _____, reprezentowaną przez: _____, zwaną(ym) dalej „Administratorem**"**

a

Wirtualna Polska Media S.A z siedzibą w Warszawie, ul. Żwirki i Wigury 16, 02-092 Warszawa, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XIII Wydział Gospodarczy - KRS pod numerem KRS: 0000580004, NIP: 5272645593, REGON: 142742958, kapitał zakładowy 320.005.950,00 zł (opłacony w całości) zwaną dalej „**Przetwarzającym**"

1. DEFINICJE

Dla potrzeb Umowy, Administrator i Przetwarzający ustalają następujące znaczenie niżej wymienionych pojęć:

a. **Czynności Przetwarzania** – oznaczają wszelkie operacje na Danych Osobowych, które będzie wykonywał Przetwarzający na polecenie Administratora w celu świadczenia Usługi, w tym: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

b. **Dane Osobowe** – dane osobowe w rozumieniu art. 4 pkt 1) Rozporządzenia 2016/679, powierzone do przetwarzania Przetwarzającego przez Administratora, niezależnie czy Administrator powierza ich przetwarzanie Przetwarzającemu jako Administrator czy jako tzw. podpowierzający.

c. **Dane Osobowe Podpowierzone –** Dane Osobowe, których przetwarzanie Administrator powierza Przetwarzającemu jako podpowierzający.

d. **Przetwarzanie Danych osobowych** – wszelkie operacje które będzie wykonywał Przetwarzający na polecenie Administratora Danych na podstawie Umowy wykonywane na Danych Osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, odczyt danych i ich usuwanie w rozumieniu art. 4 pkt 2) Rozporządzenia 2016/679;

e. **Umowa** – niniejsza umowa;

f. **Usługa** – usługa świadczona zgodnie z Regulaminem usługi konta poczty elektronicznej w ramach której Przetwarzający przetwarza Dane Osobowe, powierzone przez Administratora.

g. **Rozporządzenie 2016/679** - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) oraz wszelkie akty wykonawcze do tego Rozporządzenia 2016/679 , jak również wszystkie wiążące wytyczne organów powołanych do kontroli wykonywania Rozporządzenia 2016/679.

2. PRZEDMIOT UMOWY ORAZ ZAKRES I CEL PRZETWARZANIA DANYCH OSOBOWYCH

2.1. **[Przedmiot Umowy]** Administrator powierza Przetwarzającemu do przetwarzania Dane Osobowe, a Przetwarzający zobowiązuje się przetwarzać je zgodnie z Umową oraz obowiązującym prawem.

2.2. **[Zakres przetwarzanych Danych Osobowych]** Rodzaj Danych Osobowych, kategorie osób, których Dane Osobowe podlegają przetwarzaniu, Czynności Przetwarzania określa Załącznik nr 1 do Umowy.

2.3. **[Cel przetwarzania Danych Osobowych]** Celem przetwarzania Danych Osobowych jest wykonanie Usługi, z tym zastrzeżeniem, że Dane Osobowe mogą być przetwarzane przez Przetwarzającego wyłącznie w celu niezbędnym do wykonania tej Usługi w zakresie wskazanym w Regulaminie usługi konta poczty elektronicznej.

3. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

3.1. **[Oświadczenia Stron]** Strony oświadczają, co następuje: (a) Strony oświadczają, że Umowa została zawarta w celu wykonania obowiązków, o których mowa w art. art. 28 Rozporządzenia 2016/679, w związku ze świadczeniem Usługi, (b) Administrator oświadcza, iż jest administratorem Danych Osobowych w rozumieniu art. 4 pkt 7) Rozporządzenia 2016/79, tj. podmiotem decydującym o celach i środkach/sposobach przetwarzania Danych Osobowych, oraz, że jest uprawniony do powierzenia Danych Osobowych do przetwarzania, (c) Przetwarzający

oświadcza, że jest w stosunku do Danych osobowych „podmiotem przetwarzającym" w rozumieniu art. 4 pkt 8) Rozporządzenia 2016/679 oraz, że dysponuje środkami (w tym organizacyjnymi i technicznymi zgodnie z Załącznikiem nr 2 do Umowy) umożliwiającym mu prawidłowe wykonanie Umowy, w tym przetwarzanie Danych Osobowych zgodnie z Umową oraz obowiązującym prawem, w tym Rozporządzeniem 2016/679, (d) Administrator oświadcza, że zapoznał się z wykazem wdrożonych przez Przetwarzającego środków organizacyjnych i technicznych służących ochronie informacji, w tym danych osobowych, stanowiącym Załącznik nr 2 do Umowy oraz uznaje je za odpowiednie i wystarczające dla ochrony praw osób, których dane dotyczą.

3.2. **[Ogólne zasady przetwarzania]** Przetwarzający zobowiązuje się: (a) przetwarzać Dane Osobowe wyłącznie w zakresie i celu przewidzianym w Umowie, zgodnie z Umową oraz obowiązującym prawem, w tym Rozporządzeniem 2016/679 (b) przetwarzać Dane Osobowe wyłącznie na udokumentowane polecenie Administratora, z tym zastrzeżeniem że niniejsza Umowa stanowi udokumentowane polecenie przetwarzania Danych Osobowych w zakresie i celu niezbędnym do świadczenia przez Przetwarzającego Usługi.

3.3. [**Szczegółowe zasady przetwarzania**] Przetwarzający zobowiązuje się: (a) stosować środki techniczne i organizacyjne zgodnie z Załącznikiem nr 2 by przetwarzanie Danych Osobowych spełniało wymogi Rozporządzenia 2016/679 i chroniło prawa osób, których dane dotyczą, w tym środki techniczne i organizacyjne zapewniające bezpieczeństwo przetwarzania, o których mowa w art. 32 Rozporządzenia 2016/679; (b) uaktualniać te środki, jeśli według Przetwarzającego okaże się to niezbędne, aby zapewnić zgodne z prawem przetwarzanie Danych Osobowych powierzonych Przetwarzającemu; (c) pomagać Administratorowi w wywiązywaniu się z obowiązków określonych w art. 32-36 Rozporządzenia 2016/679; w szczególności, Przetwarzający zobowiązuje się przekazywać Administratorowi informacje oraz wykonywać jego polecenia dotyczące stosowanych środków zabezpieczania Danych Osobowych, przypadków naruszenia ochrony Danych Osobowych oraz zawiadamiania o tym organu nadzorczego lub osób, których Dane Osobowe dotyczą, przeprowadzenia oceny skutków dla ochrony danych, oraz przeprowadzania uprzednich konsultacji z organem nadzorczym i wdrożenia zaleceń organu; (d) pomagać Administratorowi poprzez odpowiednie środki techniczne i organizacyjne, o których mowa w Załączniku nr 2 w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w art. 15-22 Rozporządzenia 2016/679; (e) niezwłocznie informować Administratora, jeżeli zdaniem Przetwarzającego wydane jej polecenie stanowi naruszenie Rozporządzenia 2016/679 lub innych przepisów o ochronie danych; (f) stosować się do ewentualnych wskazówek lub zaleceń, wydanych przez organ nadzoru lub unijny organ doradczy zajmujący się ochroną danych osobowych, dotyczących przetwarzania danych osobowych, w szczególności w zakresie stosowania Rozporządzenia 2016/679.

3.4. **[Podpowierzenie]** Administrator dopuszcza możliwość podpowierzenia przetwarzania powierzonych Danych Osobowych podwykonawcom Przetwarzającego. Przetwarzający może według własnego uznania podpowierzyć przetwarzanie Danych Osobowych swoim podwykonawcom. Przetwarzający zapewni, aby podmioty, o których mowa powyżej (subprocesorzy), stosowały co najmniej równorzędny poziom ochrony Danych Osobowych, co Przetwarzający, który postępuje zgodnie z Umową.

3.5. **[Weryfikacja]** Administrator jest uprawniony do weryfikacji przetwarzania przez Przetwarzającego Danych Osobowych pod kątem zgodności z Umową oraz Rozporządzeniem 2016/679. W tym zakresie Administrator jest uprawniony do uzyskania od Przetwarzającego informacji dotyczących powierzonych Danych Osobowych oraz ich przetwarzania przez Przetwarzającego, w terminie nie krótszym niż 14 dni.

4. OBOWIĄZYWANIE UMOWY I ZASADY POSTĘPOWANIA PO JEJ WYGAŚNIĘCIU

4.1. **[Data zawarcia Umowy oraz okres obowiązywania]** Umowa wchodzi w życie z dniem jej zawarcia i obowiązuje przez cały okres świadczenia Usługi oraz wykonania wszystkich zobowiązań wynikających z Umowy.

4.2. **[Wypowiedzenie Umowy i Postępowanie po wygaśnięciu Umowy]** Do wypowiedzenia i postępowania po wygaśnięciu umowy stosuje się odpowiednio postanowienia Regulaminu usługi konta poczty elektronicznej .

5. POSTANOWIENIA KOŃCOWE

5.1. W celach kontaktowych w ramach Umowy Strony podają dane kontaktowe w Załączniku nr 1 do Umowy.

5.2. Umowa została sporządzona w dwóch egzemplarzach, po jednym dla każdej ze Stron.

W imieniu Administratora	W imieniu Przetwarzającego

ZAŁĄCZNIK NR 1

ZAKRES POWIERZENIA DANYCH OSOBOWYCH ORAZ DANE KONTAKTOWE STRON

1. Czynności przetwarzania: ☐ przechowywanie / ☐ utrwalanie / ☐ modyfikowanie /

   ☐ inne (jakie?) .....

2. Kategorie osób, których dane dotyczą:

   ☐Pracownicy;

   ☐Klienci;

   ☐Kontrahenci;

   ☐inne (jakie?) .....

   ☐inne (jakie?) .....

3. Rodzaje danych osobowych:

   ☐Imię

   ☐Nazwisko

   ☐Pseudonim

   ☐Adres e-mail

   ☐Numer telefonu

   ☐Adres (Ulica i nr, Województwo, Kod pocztowy, Miejscowość, Kraj)

   ☐inne (jakie?) .....

   ☐inne (jakie?) .....

4. Dane kontaktowe Stron:

   a. Wszelka korespondencja w sprawach związanych z Umową będzie kierowana na następujące dane kontaktowe: ....., ul. ....., ..., tel. 22 ....., email: xxxxxxxxx@wp.pl;
   b. Wszelka korespondencja w sprawach związanych z Umową będzie kierowana do WP na następujące dane kontaktowe: adres: Wirtualna Polska Media S.A., ul. Żwirki i Wigury 16, 02-092 Warszawa, tel. ....., email: .....

ZAŁĄCZNIK NR 2

Wykaz wdrożonych środków organizacyjnych i technicznych służących ochronie informacji, w tym danych osobowych

OBSZAR	OPIS ŚRODKA BEZPIECZEŃSTWA
Polityki bezpieczeństwa informacji	Został opracowany, zatwierdzony przez kierownictwo, opublikowany i zakomunikowany pracownikom oraz właściwym stronom zewnętrznym zbiór polityk ochrony danych osobowych (w tym m.in. polityka realizacji praw podmiotów danych, procedura postępowania z incydentem bezpieczeństwa, procedura wyboru procesora).
	Polityki ochrony danych osobowych są poddawane przeglądom w zaplanowanych odstępach czasu oraz wtedy, gdy wystąpią istotne zmiany.
	Została opracowana procedura nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osób odpowiedzialnych za te czynności.
	Została opracowana procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczona dla użytkowników systemu informatycznego.
Organizacja bezpieczeństwa informacji	Została określona i przypisana odpowiedzialność za ochronę danych osobowych.
	Są utrzymywane stosowne kontakty z grupami zainteresowanych specjalistów lub innymi specjalistycznymi forami oraz stowarzyszeniami zawodowymi z obszaru bezpieczeństwa i ochrony danych osobowych.
	Ochrona danych osobowych jest uwzględniana w zarządzaniu projektami niezależnie od rodzaju projektu.
Bezpieczeństwo zasobów ludzkich	Kierownictwo wymaga, aby wszyscy pracownicy i kontrahenci stosowali zasady ochrony danych osobowych zgodnie z obowiązującymi w organizacji politykami i procedurami.
	Wszyscy pracownicy organizacji oraz, w stosownych wypadkach, kontrahenci przechodzą stosowne kształcenie i szkolenie uświadamiające z zakresu ochrony danych osobowych oraz regularnie otrzymują aktualizacje polityk i procedur związanych z bezpieczeństwem informacji na ich stanowiskach pracy.
Bezpieczeństwo fizyczne i środowiskowe	Wprowadzono politykę czystego biurka dla dokumentów papierowych i przenośnych nośników pamięci oraz politykę czystego ekranu dla środków przetwarzania informacji.
	Przed zbyciem lub przekazaniem sprzętu do ponownego użycia są sprawdzane wszystkie jego składniki zawierające nośniki informacji, dla zapewnienia, że wszystkie wrażliwe dane i licencjonowane programy zostały usunięte lub bezpiecznie nadpisane.
	Sprzęt umieszcza się i chroni w taki sposób, aby zredukować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz okazje do nieuprawnionego dostępu.

	Sprzęt chroni się przed awariami zasilania oraz innymi przerwami dostaw spowodowanymi awariami systemów wspomagających.
	Określono granice bezpieczeństwa i wykorzystuje się je do zabezpieczenia obszarów zawierających wrażliwe lub krytyczne informacje oraz środki przetwarzania informacji.
	Zapewniono, że bezpieczne strefy są chronione odpowiednimi zabezpieczeniami wejść zapewniającymi dostęp wyłącznie osobom uprawnionym.
	Zaprojektowano i stosuje się fizyczne zabezpieczenia biur, pomieszczeń i obiektów.
	Zaprojektowano i stosuje się fizyczne zabezpieczenia przed katastrofami naturalnymi, wrogim atakiem lub wypadkami.
	Jest sprawowany nadzór nad punktami dostępu takimi jak obszary dostaw i załadunku oraz innymi punktami, przez które nieuprawnione osoby mogą wejść do pomieszczeń i jeśli to możliwe, izoluje się je od środków przetwarzania informacji, aby zapobiec nieuprawnionemu dostępowi.
Relacje z dostawcami	Uzgadnia się z dostawcą i udokumentowuje wymagania dotyczące ochrony danych osobowych celem zmniejszenia ryzyk związanych z dostępem dostawcy do aktywów organizacji.
Zarządzanie incydentami związanymi z bezpieczeństwem informacji	Pracownicy oraz kontrahenci korzystający z systemów i usług informacyjnych organizacji zostali zobowiązani do odnotowania i zgłaszania wszelkich zaobserwowanych lub podejrzewanych słabości związanych z bezpieczeństwem danych osobowych w systemach lub usługach.
	Wiedzę zdobytą podczas analizy i rozwiązywania incydentów związanych z ochroną danych osobowych wykorzystuje się do zredukowania prawdopodobieństwa wystąpienia lub skutków przyszłych incydentów.
	Ustanowiono odpowiedzialność kierownictwa oraz procedury zapewniające szybką, skuteczną i zorganizowaną reakcję na incydenty związane z bezpieczeństwem danych osobowych.
	Organizacja określiła i stosuje procedury identyfikacji, gromadzenia, pozyskiwania i utrwalania informacji, które mogą stanowić materiał dowodowy.
	Zdarzenia związane z bezpieczeństwem danych osobowych są zgłaszane odpowiednimi kanałami zarządczymi tak szybko, jak tylko to jest możliwe.
	Zdarzenia związane z bezpieczeństwem danych osobowych są oceniane i są podejmowane decyzje w sprawie zakwalifikowania ich jako incydentów lub naruszeń ochrony danych osobowych.
	Reakcja na incydenty związane z bezpieczeństwem danych osobowych są zgodne z udokumentowanymi procedurami.
Kontrola dostępu	Została ustanowiona, udokumentowana i poddawana przeglądom zgodnie z wymaganiami biznesowymi i wymaganiami ochrony danych osobowych Polityka kontroli dostępu.
	Użytkownicy mają dostęp wyłącznie do tych sieci i usług sieciowych, do których otrzymali wyraźne uprawnienia.

	W celu umożliwienia przydzielania praw dostępu wdrożono formalny proces rejestrowania i wyrejestrowywania użytkowników.
	Wdrożono formalny proces przydzielania dostępu użytkownikom w celu nadawania lub odbierania praw dostępu do wszystkich systemów i usług wszystkim kategoriom użytkowników.
	Przydzielanie i wykorzystanie praw uprzywilejowanego dostępu jest ograniczone i nadzorowane.
	Przydzielanie poufnych informacji uwierzytelniających powinno podlegać formalnemu procesowi zarządzania.
	Przegląd praw dostępu użytkowników w zakresie sprzętu i oprogramowania użytkownika, takie jak tablety, przeglądarki internetowe, telewizory z dostępem do Internetu itp., komputery przekaźniki telekomunikacyjne, napędy USB, dyski twarde itp.
	Przydzielone pracownikom i użytkownikom zewnętrznym prawa dostępu do informacji i środków przetwarzania informacji są odbierane po zakończeniu zatrudnienia, umowy lub porozumienia lub są dostosowywane do zaistniałych zmian.
	Użytkownicy mają obowiązek przestrzegania przyjętych w organizacji zasad stosowania poufnych informacji uwierzytelniających (polityka haseł).
	Dostęp do informacji oraz funkcji systemu aplikacyjnego jest ograniczony zgodnie z Polityką kontroli dostępu.
	Dostęp do kodu źródłowego programów jest ograniczony.
Zarządzanie aktywami	Inwentaryzacja aktywów w zakresie sprzętu użytkownika, takiego jak smartfony, tablety, przeglądarki internetowe, telewizory z dostępem do Internetu itp., komputery przekaźniki telekomunikacyjne, napędy USB, dyski twarde itp. oraz oprogramowanie użytkownika takie jak systemy operacyjne, komunikatory, bazy danych, aplikacje biznesowe itp.
	Określona została własność aktywów w zakresie sprzętu użytkownika takiego jak smartfony, tablety, przeglądarki internetowe, telewizory z dostępem do Internetu itp., komputery przekaźniki telekomunikacyjne, napędy USB, dyski twarde itp. oraz oprogramowanie takie jak systemy operacyjne, komunikatory, bazy danych, aplikacje biznesowe itp.
	Nośniki, które nie będą dłużej wykorzystywane, są bezpiecznie wycofywane, zgodnie z formalnymi procedurami.
	Nośniki zawierające informacje są chronione przed nieuprawnionym dostępem, nadużyciem oraz utratą integralności podczas transportu.
Bezpieczna eksploatacja	Monitoruje się i dostosowuje wykorzystanie zasobów oraz przewiduje wymaganą pojemność w przyszłości, dla zapewnienia właściwej wydajności systemu.
	Zapasowe kopie informacji, oprogramowania i obrazów systemów są regularnie wykonywane i testowane, zgodnie z ustaloną polityką kopii zapasowych.

	Zegary wszystkich istotnych systemów przetwarzania informacji w organizacji lub domenie bezpieczeństwa są zsynchronizowane z jednym wzorcowym źródłem czasu.
	Wdrożono procedury nadzoru nad instalacją oprogramowania w systemach produkcyjnych.
	Oddziela się środowiska deweloperskie, testowe i produkcyjne celem redukcji ryzyk związanych z nieuprawnionym dostępem lub zmianami w środowisku produkcyjnym.
	Wdrożono zabezpieczenia wykrywające, zapobiegające i odtwarzające, które służą ochronie przed szkodliwym oprogramowaniem, w połączeniu z właściwym uświadamianiem użytkowników.
	Środki służące rejestrowaniu zdarzeń oraz informacje w dziennikach zdarzeń są chronione przed manipulacją i nieuprawnionym dostępem.
	Informacje o podatnościach technicznych wykorzystywanych systemów informacyjnych są niezwłocznie pozyskiwane, dokonuje się oceny stopnia narażenia organizacji na te podatności i podejmuje odpowiednie środki w celu przeciwdziałania związanemu z nimi ryzyku.
	Zostały ustanowione i wdrożone zasady instalowania oprogramowania przez użytkowników.
Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania	Organizacja określiła wymagania dotyczące ochrony danych osobowych i ciągłości zarządzania bezpieczeństwem informacji w niekorzystnych sytuacjach np. w czasie kryzysu lub katastrofy.
	Środki przetwarzania informacji są wdrażane z nadmiarem wystarczającym do spełnienia wymagań dostępności. Redundancja.
	Organizacja ustanowiła, udokumentowała, wdrożyła i utrzymuje procesy, procedury i zabezpieczenia dla zapewnienia w niekorzystnej sytuacji wymaganego poziomu ciągłości ochrony danych osobowych.
Pozyskiwanie, rozwój i utrzymanie systemów	Wymagania dotyczące ochrony danych osobowych są włączane do wymagań stawianych nowym systemom informacyjnym lub rozbudowie systemów istniejących.
	Ustanowiono zasady prac nad rozwojem oprogramowania i systemów oraz stosuje się je w pracach rozwojowych prowadzonych wewnątrz organizacji.
	Nadzoruje się zmiany w systemach podczas ich cyklu rozwojowego przy użyciu formalnych procedur kontroli zmian.
	Po dokonaniu zmian w platformach produkcyjnych przeprowadza się przegląd krytycznych aplikacji biznesowych oraz testuje je, aby uzyskać pewność, że zmiany nie miały niekorzystnego wpływu na działalność organizacji lub bezpieczeństwo.
	Modyfikacje w pakietach oprogramowania są dokonywane z rozwagą i ograniczają się do zmian niezbędnych, a wszystkie takie zmiany są ściśle nadzorowane.
	Ustanowiono, udokumentowano i utrzymuje się zasady projektowania bezpiecznych systemów oraz stosuje się je do wszystkich prac implementacyjnych nad systemami informacyjnymi.

	Ustanowiono i odpowiednio się chroni bezpieczne środowiska rozwojowe przeznaczone do rozwoju systemów oraz prac integracyjnych obejmujących całość cyklu rozwojowego systemów.
	Organizacja nadzoruje i monitoruje prace rozwojowe nad systemami zlecone podmiotom zewnętrznym.
	Funkcje bezpieczeństwa są testowane w czasie prac rozwojowych.
	Dla nowych systemów informacyjnych, ich modernizacji i nowych wersji systemów ustanawia się programy testów akceptacyjnych i kryteria z nimi związane.
	Dane testowe są starannie wybierane, chronione i nadzorowane.
Bezpieczeństwo komunikacji	Wdrożono formalne polityki przesyłania informacji, procedury i zabezpieczenia w celu ochrony wymiany informacji przesyłanych przy użyciu wszystkich rodzajów środków łączności.