Ul. Szczytnicka 11,
50-382 Wrocław
T +48 717 875 300
www.kantarmedia.com

WARUNKI WSPÓŁPRACY
(ZAKUP USŁUG)

1 DEFINICJE

1.1 Poniższe terminy i określenia stosowane w niniejszej Umowie mają następujące znaczenie:

„Umowa" oznacza łącznie Zamówienie (PO) oraz niniejszy Regulamin.

„Informacje Poufne" oznaczają wszelkie informacje dotyczące Klienta oraz/lub członków zarządu, dyrektorów, kierowników i pracowników Grupy Kantar oraz budżetu, cen, portfela zamówień, metodologii, rachunków, kwestionariuszy, finansów, spółek dominujących i zależnych, Danych Klienta oraz jego klientów i odbiorców.

„Klient" oznacza markę operacyjną Kantar wymienioną w Zamówieniu.

„Dane Klienta" oznaczają wszelkie dane (w tym wszelkie dane osobowe dotyczące pracowników, klientów/odbiorców lub dostawców Klienta lub jego klientów), dokumenty, teksty, rysunki, schematy, specyfikacje, obrazy (wraz z każdą utworzoną na ich podstawie bazą danych) dostarczone lub udostępnione Dostawcy przez Klienta lub jego klientów lub w ich imieniu, bądź które Dostawca jest zobowiązany wytworzyć, przetworzyć, przechowywać lub przekazać zgodnie z niniejszą Umową.

„Przepisy prawa w zakresie ochrony danych" oznaczają unijną dyrektywę o ochronie danych (95/46/WE) oraz europejską dyrektywę o prywatności i łączności elektronicznej (okresowo zmienianą) oraz wszelkie przepisy wykonawcze do tych dyrektyw w każdym kraju, a od dnia 25 maja 2018 r. – unijną dyrektywę o ochronie danych oraz rozporządzenie ogólne o ochronie danych osobowych (RODO).

„Produkty" oznaczają wszystkie towary, produkty, sprzęt i materiały, które mają być dostarczone w ramach Usług.

„Unijna dyrektywa o ochronie danych" oznacza dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych – z zastrzeżeniem punktu 1.1(1).

„Opłaty" oznaczają łączną kwotę przypadającą do zapłaty przez Klienta zgodnie z Zamówieniem.

„RODO" oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. 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).

„Prawa własności intelektualnej" oznaczają wszystkie patenty, prawa do wynalazków, prawa autorskie i prawa pokrewne, prawa osobiste, prawa do baz danych, prawa topograficzne półprzewodników, wzory użytkowe, prawa do wzorów, znaków towarowych, znaków usługowych, nazw handlowych, nazw domen, prawa do wartości firmy, prawa do nieujawnionych lub poufnych

informacji oraz inne podobne lub równoważne prawa lub formy ochrony, które mogą obecnie lub w przyszłości istnieć w dowolnym miejscu na świecie.

„Dane osobowe” mają znaczenie określone w Załączniku 3.

„Zamówienie” oznacza zamówienie zakupu dołączone do niniejszych „Warunków współpracy” lub inną formę pisemnego powiadomienia zawierającego numer Zamówienia, do którego mają zastosowanie niniejsze „Warunki współpracy”.

„Usługi” oznaczają usługi określone w Zamówieniu lub odwołanie do numeru Zamówienia określające usługi w innej formie pisemnej.

„Dostawca” oznacza podmiot wskazany w zamówieniu.

„Pracownicy Dostawcy” oznacza cały personel zobowiązany do świadczenia Usług.

„Polityka Dostawcy” oznacza wszelkie zasady lub kodeksy postępowania mające zastosowanie do dostawców Kantar i bezpośrednich lub pośrednich spółek zależnych Kantar, o których Klient okresowo informuje Dostawcę lub które są udostępniane w dowolnej sieci ekstranetowej prowadzonej przez Klienta na rzecz dostawców w tym między innymi Kodeks Postępowania Biznesowego Kantar (*Kantar Code of Business Conduct*) załączony do niniejszego dokumentu jako Załącznik 1 oraz wszelkie odnośne zasady antykorupcyjne stosowane przez Kantar Group.

2 USŁUGI

2.1 Do Usług mają zastosowanie niniejsze „Warunki współpracy”.

2.2 Zamówienie uważa się za przyjęte z chwilą rozpoczęcia świadczenia Usług. Dostawca świadczy Usługę od dnia określonego w Zamówieniu. Dostawca będzie świadczył Usługi na rzecz Klienta zgodnie z życzeniem Klienta, Polityką Dostawcy, najlepszymi praktykami branżowymi oraz warunkami niniejszej Umowy. Czas wykonywania Usług ma istotne znaczenie.

2.3 Dostawca gwarantuje, że każdy z Pracowników Dostawcy:
(a) przestrzega okresowo aktualizowanych Zasad Dostawcy
(b) jest odpowiednio wykwalifikowany i przeszkolony do świadczenia Usług;
(c) został odpowiednio sprawdzony zgodnie z ewentualnymi szczegółowymi instrukcjami wydanymi przez Klienta i nie był skazany prawomocnym wyrokiem; oraz
(d) ma uprawnienia do wykonywania pracy na terytorium, na którym świadczone są Usługi.

2.4 Dostawca na bieżąco gwarantuje, zobowiązuje się i oświadcza, że:
(a) posiada pełną zdolność i uprawnienia do zaciągania zobowiązań wynikających z niniejszej Umowy i do ich wypełniania;
(b) przestrzega wszystkich obowiązujących przepisów ustawowych, wykonawczych i kodeksów postępowania;
(c) nie będzie podejmować żadnych działań ani dopuszczać się zaniechań w związku z wykonywaniem swoich zobowiązań wynikających z niniejszej Umowy, które mają lub mogą mieć istotny negatywny wpływ na reputację Klienta lub jego klienta; oraz
(d) Produkty są kompletne, poprawne i zgodne pod każdym względem z niniejszą Umową oraz nie naruszają niczyich praw.

Ul. Szczytnicka 11,
50-382 Wrocław
T +48 717 875 300
www.kantarmedia.com

3 OPŁATY

3.1 Dostawca może wystawić Klientowi fakturę dopiero po wykonaniu Usług w sposób zadowalający dla Klienta. Klient zobowiązany jest do uiszczenia Opłat za Usługi w najbliższym terminie płatności realizowanych przez Klienta po upływie sześćdziesięciu (60) dni od końca miesiąca, w trakcie którego wpłynęła ważna faktura określająca prawidłowy numer zamówienia (PO). W przypadku, gdy usługi są nabywane od Dostawcy przez Klienta działającego na rzecz innego odbiorcy, Klient nie jest zobowiązany do zrealizowania płatności na rzecz Dostawcy do czasu otrzymania zapłaty od tego odbiorcy. Opłaty nie obejmują podatków od sprzedaży lub podobnych podatków. Klient jest uprawniony do dokonywania potrąceń lub odliczeń z kwoty Opłat, jeżeli jest to wymagane przez prawo.

3.2 Od bezspornych kwot zaległych Dostawca może naliczać odsetki w stosunku rocznym w wysokości 2% powyżej stopy bazowej

4 ROZWIĄZANIE UMOWY

4.1 Klient może w każdej chwili rozwiązać niniejszą Umowę w całości lub (z proporcjonalnym obniżeniem Opłat) w części:

(a) dla wygody, za trzydziestodniowym (30) pisemnym powiadomieniem Dostawcy; lub

(b) niezwłocznie, jeżeli Dostawca dopuścił się istotnego naruszenia niniejszej Umowy, które nie zostało naprawione w terminie 14 dni od wezwania Dostawcy przez Klienta do naprawienia naruszenia; lub

(c) niezwłocznie po wydaniu nakazu lub podjęciu uchwały o likwidacji przedsiębiorstwa Dostawcy, lub gdy Dostawca wyznaczy syndyka lub zarządcę dla dowolnej części swoich aktywów, lub gdy zaistnieją okoliczności uprawniające sąd lub wierzyciela do wyznaczenia syndyka lub zarządcy, uprawniające sąd do wydania nakazu likwidacji lub nakazu administracyjnego, lub okoliczności uprawniające do zawarcia ugody z wierzycielami, lub gdy Dostawca nie jest w stanie spłacić swoich długów w terminie ich wymagalności.

4.2 Po wygaśnięciu lub rozwiązaniu niniejszej Umowy lub zakończeniu realizacji dowolnej części Usług Dostawca dostarczy do Klienta wszystkie Informacje Poufne oraz będzie współpracować z Klientem oraz/lub stroną trzecią w celu zapewnienia satysfakcjonującego przekazania Informacji Poufnych.

4.3 Wygaśnięcie lub rozwiązanie niniejszej Umowy pozostaje bez uszczerbku dla wszelkich praw nabytych do dnia jej rozwiązania lub postanowień, które wyraźnie lub w sposób dorozumiany pozostają w mocy po rozwiązaniu Umowy.

5 AUDYT

5.1 Dostawca będzie utrzymywać i prowadzić w swojej głównej siedzibie zgodne z prawdą i dokładne pisemne księgi i rejestry związane z Usługami (w tym między innymi karty czasu pracy, rejestry roszczeń, faktury, wydatki, koszty, noty kredytowe) zgodnie z ogólnie przyjętymi zasadami rachunkowości i przechowywania dokumentów w ramach niniejszej Umowy oraz przez okres 6 lat po jej zawarciu, a także zezwoli Klientowi oraz/lub jego odbiorcy lub upoważnionemu

przedstawicielowi Klienta na kontrolowanie takich ksiąg i rejestrów – za odpowiednim pisemnym powiadomieniem – w celu oceny zgodności z niniejszą Umową (w tym, bez ograniczeń, kontrolowanie zgodności z ograniczeniami określonymi w punkcie 10).

5.2 Jeżeli w wyniku audytu Klient wykryje jakąkolwiek nadpłatę w związku z Usługami lub inne naruszenie warunków niniejszej Umowy, Dostawca niezwłocznie usunie taką niezgodność na własny koszt i zwróci Klientowi pełną kwotę każdej nadpłaty oraz koszty stosownego audytu.

6 ODPOWIEDZIALNOŚĆ I ODSZKODOWANIE

6.1 Żadne z postanowień niniejszej Umowy nie wyłącza ani nie ogranicza odpowiedzialności żadnej ze stron w odniesieniu do jakichkolwiek roszczeń:

(a) z powodu śmierci lub szkody na osobie spowodowanych niedbalstwem danej strony; lub

(b) w wyniku jakiegokolwiek oszustwa, w tym przedstawienia przez stronę fałszywych informacji; lub

(c) w przypadku których odpowiedzialność nie może być w inny sposób ograniczona lub wyłączona zgodnie z prawem; lub

(d) z tytułu jakiegokolwiek odszkodowania udzielonego Klientowi przez Dostawcę na podstawie niniejszej Umowy; lub

(e) w przypadku naruszenia przez Dostawcę postanowień punktów 8–10 włącznie lub punktu 12.1; lub

(f) w przypadku umyślnego lub celowego niewywiązania się Dostawcy z zobowiązań.

6.2 Z zastrzeżeniem postanowień punktu 6.1, Klient nie ponosi odpowiedzialności za jakiekolwiek pośrednie, szczególne lub wynikowe straty lub utratę zysków (bezpośrednich lub pośrednich), utratę wartości firmy, utratę zleceń, utratę przychodów lub utratę przewidywanych oszczędności.

6.3 Dostawca zwolni Klienta z wszelkich strat, kosztów, zobowiązań, szkód, wydatków, roszczeń i postępowań, które poniósł Klient w wyniku lub w związku z następującymi zdarzeniami:

(a) jakiekolwiek naruszenie niniejszej Umowy; lub

(b) utrata lub uszkodzenie własności Klienta w trakcie świadczenia Usług; lub

(c) jakiekolwiek zaniedbanie lub zaniechanie ze strony Dostawcy, Pracowników Dostawcy oraz/lub podwykonawców lub ich pracowników w związku z niniejszą Umową; lub

(d) wszelkie roszczenia dotyczące faktu, że korzystanie z Produktów oraz/lub Usług narusza prawa własności intelektualnej osób trzecich.

6.4 Z zastrzeżeniem punktów 6.1 i 6.2, łączna odpowiedzialność Klienta wynikająca z niniejszej Umowy lub z nią związana (czy to z tytułu umowy, czynu niedozwolonego, w tym zaniedbania, czy też z innego tytułu) nie może przekroczyć kwoty równej Opłatom uiszczonym lub należnym Dostawcy od Klienta na mocy niniejszej Umowy w ciągu dwunastu (12) miesięcy poprzedzających zdarzenie, które spowodowało powstanie takiej odpowiedzialności.

6.5 Z zastrzeżeniem punktów 6.1 i 6.2, łączna odpowiedzialność Dostawcy wynikająca z niniejszej Umowy lub z nią związana (czy to z tytułu umowy, czynu niedozwolonego, w tym zaniedbania, czy też z innego tytułu) nie może przekroczyć 10 000 000 GBP (dziesięciu milionów funtów szterlingów) na jedno roszczenie.

7 UBEZPIECZENIE

7.1 Dostawca powinien zawrzeć i utrzymywać umowę ubezpieczenia odpowiedzialności cywilnej z renomowanym ubezpieczycielem w celu pokrycia zobowiązań i odpowiedzialności Dostawcy wynikających z niniejszej Umowy oraz:

(a) w odniesieniu swojej odpowiedzialności publicznej – na kwotę minimum 1 000 000 GBP dla każdego zdarzenia i bez ograniczeń w odnośnym okresie ubezpieczenia;

(b) w odniesieniu do odpowiedzialności swojego pracodawcy – na kwotę minimum 5 000 000 GBP dla każdego zdarzenia i bez ograniczeń w danym okresie ubezpieczenia;

(c) w odniesieniu do swojej odpowiedzialności zawodowej – na kwotę minimum 1 000 000 GBP dla każdego zdarzenia i bez ograniczeń w odnośnym okresie ubezpieczenia.

7.2 Każda taka polisa winna wskazywać Klienta jako dodatkowego ubezpieczonego i zawierać klauzulę o odszkodowaniu dla zleceniodawcy. Żadna taka polisa nie będzie wymagała składki ze strony Klienta i nie będzie przekraczała jakiegokolwiek innego ubezpieczenia dostępnego dla Klienta. Klient nie ponosi odpowiedzialności za jakikolwiek należny udział własny, który nie może być niższy niż 50 000 GBP.

7.3 Dostawca zawrze dodatkową umowę o ochronę ubezpieczeniową, jakiej Klient będzie okresowo żądał w uzasadniony sposób.

8 OCHRONA DANYCH

8.1 Jeżeli świadczenie Usług wymaga przetwarzania danych osobowych przez Dostawcę w imieniu Klienta, Dostawca będzie przestrzegał siódmej zasady przepisów o ochronie danych oraz:

(a) będzie przestrzegać przepisów o ochronie danych;

(b) będzie działać wyłącznie na polecenie Klienta jako administratora danych;

(c) spełni warunki określone w Załączniku 2 (uzupełnienie do załącznika dotyczącego bezpieczeństwa informacji);

(d) w każdym czasie będzie podejmować wszelkie stosowne środki techniczne, operacyjne, zarządcze, fizyczne i organizacyjne zgodnie z obowiązującymi praktykami w zakresie dbałości, umiejętności, profesjonalizmu i staranności w celu ochrony przed nieuprawnionym lub bezprawnym przetwarzaniem danych osobowych oraz przed nieuprawnioną lub bezprawną przypadkową utratą, zniszczeniem lub uszkodzeniem danych osobowych oraz zapewni bezpieczeństwo takich danych osobowych;

(e) nie będzie kasować, przekazywać, usuwać ani w inny sposób przetwarzać żadnych danych Klienta, chyba że zrobi to zgodnie z jego instrukcjami lub warunkami niniejszej Umowy;

(f) zezwoli Klientowi lub jego przedstawicielowi, na koszt Klienta, w dowolnym czasie i za uprzednim odpowiednim pisemnym powiadomieniem (z co najmniej pięciodniowym wyprzedzeniem), na uzyskanie dostępu – w celu oceny i weryfikacji bezpieczeństwa – do odpowiedniej części pomieszczeń, systemów, wyposażenia lub innych materiałów i obiektów, w których Dostawca, jego dostawcy lub podwykonawcy przetwarzają dane osobowe; oraz

(g) niezwłocznie poinformuje Klienta w przypadku naruszenia lub podejrzenia naruszenia niniejszego punktu 8, lub gdy doszło do faktycznej lub podejrzewanej utraty, uszkodzenia, wykorzystania lub ujawnienia danych osobowych stronie trzeciej w inny sposób niż zgodnie z niniejszą Umową.

8.2 Dostawca zwolni Klienta z wszelkich strat, zobowiązań, roszczeń, wydatków, szkód i kosztów poniesionych lub poniesionych przez Klienta w wyniku nieprzestrzegania przez Dostawcę przepisów o ochronie danych osobowych – postanowień Załącznika 3.

8.3 Dostawca będzie przestrzegać szczegółowych warunków wymaganych przez RODO w odniesieniu do wszelkich Usług, które wymagają przetwarzania Danych osobowych zgodnie z Załącznikiem 3.

8.4 Dostawca gwarantuje, że wdroży środki, które obejmują normę bezpieczeństwa informacji ISO/IEC 27001 lub inną równoważną normę, która może ją okresowo zastępować.

9 PRAWA WŁASNOŚCI INTELEKTUALNEJ

9.1 Z zastrzeżeniem punktu 9.2 Klient jest właścicielem Praw Własności Intelektualnej do Produktów, a Dostawca niniejszym nieodwołalnie i bezwarunkowo przenosi na Klienta, z pełną gwarancją własności, wszelkie Prawa Własności Intelektualnej do Produktów w momencie ich powstania. Dostawca jest zobowiązany zagwarantować, aby Pracownicy Dostawcy zrzekli się na rzecz Klienta w sposób bezwzględny i nieodwołalny swoich ewentualnych praw osobistych w odniesieniu do takich Produktów.

9.2 Żadne z postanowień niniejszej Umowy nie ma na celu wywarcia wpływu na posiadanie przez Dostawcę materiałów używanych lub opracowanych przez niego w oderwaniu od Usług ani też ogólnych metodologii, narzędzi, technologii lub procesów Dostawcy, które są przez niego wykorzystywane (ale nie zostały przez niego opracowane) do świadczenia Usług (łącznie zwane **„Materiałami Dostawcy”**). Jeżeli istniejące Materiały Dostawcy (lub ich część) zostały włączone do Produktów lub są niezbędne do korzystania z Usług, Dostawca niniejszym udziela Klientowi wieczystej, ogólnoświatowej, nieodwołalnej, niewyłącznej, nieodpłatnej licencji na korzystanie z Materiałów Dostawcy w celu umożliwienia Klientowi czerpania pełnych korzyści z Usług.

9.3 Dostawca gwarantuje i oświadcza, że ma prawo do przeniesienia lub udzielenia licencji na wszystkie Prawa Własności Intelektualnej przyznane lub przeniesione zgodnie z niniejszą Umową oraz że udzielenie odnośnej cesji lub licencji i ich warunki nie naruszą Praw Własności Intelektualnej jakiejkolwiek osoby trzeciej.

9.4 Dostawca nie nabywa żadnych praw, tytułów ani udziałów w prawach własności intelektualnej, które należą do jakiejkolwiek strony trzeciej lub zostały udzielone Klientowi przez stronę trzecią na mocy licencji zawartej w niniejszej Umowie, a Dostawca przyjmuje do wiadomości, że wszystkie takie prawa własności intelektualnej pozostają własnością Klienta oraz/lub jego licencjodawców.

10 ZAKAZ KORUPCJI

10.1 Dostawca jest zobowiązany do przestrzegania amerykańskiej ustawy o zagranicznych praktykach korupcyjnych (Foreign Corrupt Practices Act, 15 U.S.C. §78dd-2) (dalej „**ustawa FCPA**”) oraz brytyjskiej ustawy o korupcji z 2010 r. (UK Bribery Act 2010) (dalej „**ustawa UKBA**”) oraz do zapewnienia zgodności z ustawami FCPA i UKBA przez spółki z jego grupy, współpracowników i każdego z ich dyrektorów, pracowników, przedstawicieli i pośredników i dowolną stronę, która świadczy usługi na rzecz Klienta („**Strony Powiązane**”).

10.2 Dostawca nie będzie podejmował następujących działań i będzie zabiegał o to, aby każda ze Stron Powiązanych nie podejmowała następujących działań: bezpośrednie lub pośrednie żądanie, wyrażenie zgody na otrzymywanie lub przyjmowanie środków finansowych lub innych środków stanowiące naruszenie obowiązku prawnego, wykorzystywanie swoich wpływów w celu wywarcia wpływu na jakiekolwiek działanie lub decyzje (w tym na niewłaściwe pełnienie jakiejkolwiek funkcji) w celu uzyskania lub utrzymania zleceń w ramach działalności gospodarczej na rzecz Klienta. Dostawca niezwłocznie powiadomi Klienta na piśmie w przypadku powzięcia wiadomości o jakimkolwiek naruszeniu ustawy FCPA, ustawy UKBA lub niniejszego punktu 10.

11 MATERIAŁY KLIENTA I ODBIORCY

11.1 Tytuł własności do materiałów Klienta lub odbiorcy Klienta przekazanych Dostawcy w celu wykonania Usług pozostaje własnością Klienta lub ewentualnie jego odbiorców (w zależności od konkretnego przypadku).

11.2 Klient lub jego odbiorca ma prawo w każdej chwili odebrać od Dostawcy swoją własność, pod warunkiem wcześniejszego zawiadomienia o tym z odpowiednim wyprzedzeniem.

11.3 Dostawca zapewni bezpieczeństwo znajdującego się w jego posiadaniu mienia będącego własnością Klienta lub któregokolwiek z jego odbiorców i nie może go zbywać w całości ani w części bez pisemnej zgody Klienta i jego odbiorcy, chyba że takie działanie jest niezbędne w celu świadczenia Usług.

11.4 Dostawca niniejszym zrzeka się prawa zastawu lub innego prawa, które mógłby mieć w stosunku do jakiejkolwiek własności Klienta lub odbiorcy Klienta i zobowiązuje się do tego, aby własność ta pozostała wolna od zastawu i innych obciążeń.

11.5 Dostawca będzie korzystał z materiałów będących własnością Klienta lub dowolnego odbiorcy Klienta w związku z wykonywaniem Usług, do których się odnoszą.

12 USTAWA O WSPÓŁCZESNYM NIEWOLNICTWIE

12.1 Dostawca gwarantuje, że:

(a) ani Dostawca, ani żaden z jego członków kadry kierowniczej, pracowników, przedstawicieli ani podwykonawców:

(i) nie popełnił przestępstwa określonego w ustawie o współczesnym niewolnictwie z 2015 r. (Modern Slavery Act 2015) (dalej: **„przestępstwo określone w MSA”**);

(ii) nie został powiadomiony o tym, że jest przedmiotem dochodzenia w związku z domniemanym przestępstwem określonym w MSA lub postępowaniem sądowym w związku ustawą o współczesnym niewolnictwie z 2015 r.;

(iii) nie są mu znane żadne okoliczności w swoim łańcuchu dostaw, które mogłyby stać się powodem wszczęcia dochodzenia w związku z domniemanym przestępstwem określonym w MSA lub postępowania sądowego w związku ustawą o współczesnym niewolnictwie z 2015 r.;

(b) przestrzega przepisów ustawy o współczesnym niewolnictwie z 2015 r.;

(c) niezwłocznie powiadomi Klienta na piśmie, jeżeli dowie się lub ma podstawy, aby sądzić, że on sam lub którykolwiek z jego członków kadry kierowniczej, pracowników, przedstawicieli lub podwykonawców naruszył lub mógł naruszyć którykolwiek z obowiązków Dostawcy wynikających z niniejszego punktu 12.

13 POSTANOWIENIA OGÓLNE

13.1 W trakcie obowiązywania niniejszej Umowy oraz przez okres 5 lat po jego upływie Dostawca będzie zachowywać poufność wszystkich Informacji Poufnych i nie będzie wykorzystywać ani ujawniać takich Informacji Poufnych osobom trzecim, chyba że będzie to bezwzględnie konieczne do wykonania Usług lub wymagane na mocy przepisów prawa.

13.2 Żadna ze stron nie może dokonać przeniesienia, podzlecenia ani w żaden sposób przenieść swoich praw lub obowiązków wynikających z niniejszej Umowy bez uprzedniej pisemnej zgody drugiej strony, z tym wyjątkiem, że Klient może dokonać przeniesienia swoich praw na dowolną spółkę zależną (bezpośrednią lub pośrednią) Kantar.

13.3 Każde postanowienie niniejszej Umowy można oddzielić i odróżnić od pozostałych jej postanowień. Nieważność lub niewykonalność danego postanowienia nie ma wpływu na pozostałe postanowienia niniejszej Umowy.

13.4 Niewykonanie lub opóźnienie w wykonaniu prawa lub skorzystaniu ze środków zaradczych przewidzianych w niniejszej Umowie lub w przepisach prawa albo wynikających z prawa własności nie jest równoważne ze zrzeczeniem się praw lub środków zaradczych, ani też żadnych innych praw lub środków zaradczych.

13.5 Żadne z postanowień niniejszej Umowy nie może być interpretowane jako ustanawiające lub sugerujące powstanie spółki lub relacji przedstawicielstwa między stronami.

13.6 Niniejsza Umowa zawiera całość uzgodnień oraz porozumień między jej stronami w odniesieniu do jej przedmiotu i zastępuje wszelkie wcześniejsze porozumienia między stronami dotyczące tegoż przedmiotu spraw. Zmiany niniejszej Umowy mogą być dokonywane wyłącznie w formie pisemnej za zgodą Klienta i Dostawcy.

13.7 Żadna osoba, która nie jest stroną niniejszej Umowy, nie ma żadnych praw na mocy brytyjskiej ustawy o umowach (Prawa Osób Trzecich) z 1999 roku (*Contracts (Rights of Third Parties) Act 1999*).

13.8 Wszelkie zawiadomienia wymagane na mocy niniejszej Umowy muszą mieć formę pisemną i będą skutecznie doręczone wyłącznie wtedy, gdy zostaną wysłane na adres podany w Zamówieniu osobiście, listem poleconym pierwszej klasy lub przesyłką nadzwyczajną.

13.9 Niniejsza Umowa oraz wszelkie zobowiązania pozaumowne podlegają prawu angielskiemu, a strony zgadzają się poddać wszelkie spory pod niewyłączną jurysdykcję sądów angielskich.

Ul. Szczytnicka 11,
50-382 Wrocław
T +48 717 875 300
www.kantarmedia.com

ZAŁĄCZNIK 1

Kodeks etyki biznesowej Kantar – wersja dla dostawców

Kantar oraz należące do niego spółki działają na wielu rynkach i w wielu państwach na całym świecie. W każdym przypadku stosujemy się do krajowych aktów prawnych oraz, w stosownych przypadkach, do wszelkich innych przepisów o zasięgu międzynarodowym, takich jak Brytyjska ustawa o łapownictwie, Amerykańska ustawa o zagranicznych praktykach korupcyjnych oraz Brytyjska ustawa o współczesnym niewolnictwie, jak również do zasad postępowania poszczególnych gałęzi gospodarki.

Dokładamy wszelkich starań, by postępować etycznie we wszystkich aspektach naszej działalności oraz by utrzymywać najwyższe standardy uczciwości i rzetelności.

Wymagamy od wszystkich naszych partnerów biznesowych, w tym dostawców, by wykazywali się takim samym zaangażowaniem w kwestiach etycznego działania, i w związku z tym prosimy Państwa o potwierdzenie, że akceptują Państwo nasze zasady postępowania (w pierwszej kolumnie) z późniejszymi zmianami na potrzeby podmiotów nienależących do Kantar (w drugiej kolumnie).

Oczekujemy, że wszyscy nasi dostawcy będą stosować odpowiednie systemy w celu ułatwienia i monitorowania zgodności z tymi standardami oraz przestrzegania przepisów lokalnych i międzynarodowych. Wymagamy, by nasi dostawcy wykazali się zaangażowaniem w przestrzeganie zasad niniejszego kodeksu i prowadzili ciągły proces zarządzania ryzykiem w celu identyfikacji zagrożeń środowiskowych, BHP, praktyk pracowniczych i zagrożeń etycznych związanych z działalnością dostawców.

Dostawcy powinni zachęcać pracowników do zgłaszania wątpliwości bez obawy przed groźbą lub odwetem, a także podjąć odpowiednie działania w razie nieprawidłowości.

Dostawcy powinni wprowadzić standardy analogiczne z niniejszym kodeksem dla własnego łańcucha dostaw

My, zarząd i pracownicy wszystkich firm w Grupie Kantar (zwanej dalej Grupą) uznajemy nasze zobowiązania wobec wszystkich, którzy mają udział w naszym sukcesie, włączając w to akcjonariuszy, klientów, pracowników i dostawców	Potwierdzają Państwo, że uznają nasze zobowiązania i nie będą działać w sposób szkodliwy względem nich.
Informacje o naszej działalności są przekazywane w sposób jasny i dokładny, w sposób niedyskryminacyjny i zgodnie z lokalnymi przepisami.	Potwierdzają Państwo, że będą traktować informacje dotyczące Grupy Kantar w opisany obok sposób.
Informacje o naszej działalności będą przekazywane w sposób zrozumiały i dokładny, z uniknięciem tonu dyskryminującego i zgodnie z lokalnymi przepisami.	Potwierdzają Państwo, że będą traktować informacje dotyczące Grupy Kantar w opisany obok sposób.
Uważamy, że miejsce pracy powinno być bezpieczne i zgodne z zasadami rozwiniętego społeczeństwa, nie będziemy tolerować molestowania seksualnego, dyskryminacji ani żadnego obraźliwego zachowania, w tym ciągłego poniżania	Potwierdzają Państwo, że stosują Państwo analogiczne zasady w swojej organizacji oraz że uszanują Państwo nasze miejsce pracy oraz pracowników w opisany obok sposób. W szczególności dotyczy to następujących sytuacji: • Podjęcie pracy jest dobrowolne; wymuszenia,

konkretnych osób poprzez słowa lub czyny, prezentowania lub rozprowadzania materiałów o obraźliwej treści ani używania i posiadania broni w obiektach należących do Kantara lub ich klientów.	wykorzystywanie lub jakakolwiek forma współczesnego niewolnictwa jest zabroniona. • Pracownicy nie mogą być zmuszani do zdania paszportu lub innego państwowego dowodu tożsamości jako warunku zatrudnienia. • Zakazana jest praca dzieci. • Odszkodowanie wypłacane pracownikom musi być zgodne ze wszystkimi obowiązującymi przepisami płacowymi. • Tydzień pracy nie może przekraczać czasu określonego przez lokalne prawo. • Zabrania się niehumanitarnego traktowania pracowników, w tym molestowania seksualnego, wykorzystywania seksualnego, kar cielesnych, przymusu fizycznego lub zniewag werbalnych. • Kantar oczekuje od swoich dostawców tworzenia i utrzymywania bezpiecznych warunków pracy dla wszystkich pracowników; • Narażenie pracowników na zagrożenia fizyczne powinno być wyeliminowane, a jeśli nie ma takiej możliwości – ściśle kontrolowane. • Dostawcy muszą dysponować odpowiednimi procedurami postępowania w sytuacja kryzysowych, jeśli wpływają one na pracowników. • Odpowiednie struktury obecne na miejscu muszą zarządzać, śledzić i zgłaszać do raportować wszelkie wypadki i choroby związane z pracą.
Nie będziemy tolerować używania, posiadania ani rozprowadzania nielegalnych środków odurzających. Nie zgadzamy się także, by nasi pracownicy zjawiali się w pracy pod wpływem narkotyków lub alkoholu.	Potwierdzają Państwo, że stosują Państwo analogiczne zasady w swojej organizacji oraz że uszanują Państwo nasze miejsce pracy oraz pracowników w opisany obok sposób.
Wszystkie informacje dotyczący działalności Grupy oraz jej klientów będziemy traktujemy jako tajne. W szczególności zakazany jest *insider trading*, a tajne informacje nie mogą być wykorzystane dla prywatnych korzyści.	Potwierdzają Państwo, że zgadzają się Państwo na naszą politykę w zakresie poszanowania informacji.
Dokładamy wszelkich starań, by chronić dane naszych konsumentów, klientów i pracowników zgodnie z prawem państwowym i zasadami postępowania poszczególnych gałęzi gospodarki.	Potwierdzają Państwo, że przyjmują Państwo w swojej organizacji analogiczną postawę, obejmującą wszystkie informacje uzyskane od i odnoszące się do naszej działalności oraz działalności naszych partnerów biznesowych.
Nie będziemy świadomie wykonywać pracy, która zawiera wypowiedzi, sugestie lub obrazy obraźliwe wobec ogólnego poczucia przyzwoitości, zwrócimy także należytą uwagę na wpływ naszej pracy na mniejszości	Tam, gdzie to istotne, potwierdzają Państwo, że mają analogiczne standardy w Państwa pracy.

społeczne, niezależnie czy chodzi o mniejszość pod względem rasy, religii, koloru skóry, płci, orientacji seksualnej, tożsamości płciowej i sposobu jej wyrażania, wieku lub niepełnosprawności.	
Nie będziemy angażować się w projekty, które mają na celu wprowadzenie w błąd, zwłaszcza w kwestiach związanych z zagadnieniami społecznymi, środowiskowymi i praw człowieka.	Tam, gdzie to istotne, potwierdzają Państwo, że mają analogiczne standardy w Państwa pracy.
Przed przyjęciem jakiegokolwiek zlecenia rozważymy potencjalne szkody, jakie zlecenie to lub klient może wyrządzić reputacji Grupy. Kwestia ta obejmuje uszczerbek na reputacji wynikający ze współpracy z klientami zaangażowanymi w działalność przyczyniającą się do łamania praw człowieka.	Dotyczy tylko członków Grupy Kantar.
Nie będziemy angażować się bezpośrednio lub pośrednio w jakiekolwiek działania konkurencyjne wobec firm należących do Grupy lub mających zobowiązania względem którejkolwiek z tych firm w celu osiągnięcia korzyści osobistych lub rodzinnych.	Dotyczy tylko członków Grupy Kantar.
Nie będziemy wręczać, proponować ani przyjmować łapówek, w gotówce ani w żadnej innej formie, żadnym osobom trzecim lub od nich. Za takie osoby uznaje się między innymi, lecz nie wyłącznie, urzędników państwowych, klientów, pośredników lub ich przedstawicieli. Zapewnimy sobie zrozumienie naszej polityki w tej kwestii przez wszystkich pracowników na drodze szkoleń, komunikacji i przykładu.	Dotyczy Państwa bezpośrednio.
Nie będziemy oferować żadnych dóbr, które mogłyby stanowić osobistą zachętę do zabezpieczenia relacji biznesowych. Ustalenie to nie ma na celu zakazania zapewniania klientom rozrywki lub wręczania im okazjonalnych podarunków o niskiej wartości, chyba że naszego klienta obowiązują zasady uniemożliwiające to.	Dotyczy Państwa bezpośrednio.
Nie będziemy przyjmować dla naszych osobistych korzyści żadnych przedmiotów czy usług o wartości wyższej niż nominalna od dostawców, potencjalnych dostawców lub osób trzecich.	Dotyczy Państwa bezpośrednio.
Nie będziemy dopuszczać do zaistnienia jakichkolwiek osobistych lub rodzinnych konfliktów interesów w ramach naszej działalności, w relacjach z naszymi dostawcami	Powinni mieć Państwo analogiczną politykę w swojej organizacji.

Ul. Szczytnicka 11,
50-382 Wrocław
T +48 717 875 300
www.kantarmedia.com

lub osobami trzecimi, z którymi wchodzimy w relacje biznesowe.	
Żadne darowizny korporacyjne jakiegokolwiek rodzaju – włączając w to świadczenie usług lub materiałów za wartość mniejszą niż rynkowa – nie mogą być przeznaczane dla polityków, partii politycznych lub komitetów wyborczych bez wcześniejszego pisemnego upoważnienia zarządu Kantar.	Powinni mieć Państwo własną politykę w kwestii takich darowizn, uwzględniającą procedury właściwej ich autoryzacji.
Będziemy nieustannie dążyć do tego, by wnosić pozytywny wkład w społeczeństwo i środowisko poprzez: utrzymywanie wysokich standardów etyki handlowej, poszanowanie praw człowieka, poszanowanie środowiska, wspieranie organizacji społecznościowych, wspieranie rozwoju pracowników oraz zarządzanie ryzykiem w ramach naszej sieci dostawców w oparciu o zasadę społecznej odpowiedzialności biznesu. Nasza Polityka zrównoważonego rozwoju i Oświadczenie o polityce praw człowieka zawierają więcej szczegółowych informacji o naszych zobowiązaniach w tym zakresie.	Powinni mieć Państwo analogiczną politykę w swojej organizacji. W szczególności dotyczy to następujących sytuacji: • Dostawcy muszą przestrzegać wymogów brytyjskiej ustawy o współczesnym niewolnictwie. • Dostawcy muszą posiadać wszelkie stosowne zezwolenia w zakresie ochrony środowiska, w tym dotyczące odpadów i emisji CO2. • Dostawcy muszą starać się zapobiegać zanieczyszczeniom poprzez wdrażanie środków ochronnych w swoich obiektach i działalności poprzez recykling, ponowne użycie i rozsądne zastępowanie materiałów.

Potwierdzamy, że będziemy przestrzegać zasad postępowania biznesowego spółek Kantar w stopniu kompatybilnym z wewnętrznymi regulacjami naszej organizacji. Poinformujemy Państwa niezwłocznie, jeśli dowiemy się o jakimkolwiek naruszeniu powyższych zasad w sprawach związanych z naszą współpracą z Państwa firmą, w szczególności dotyczących łapówki, nieodpowiednich prezentów i usług od lub dla Państwa organizacji albo osób trzecich, albo też naruszeniu dotyczącym innych kwestii mogących bezpośrednio lub niebezpośrednio zaszkodzić reputacji Kantar w związku z naszą współpracą.

Podpis:
Imię i nazwisko:
Pozycja w firmie:
Nazwa organizacji:
Data

Ul. Szczytnicka 11,
50-382 Wrocław
T +48 717 875 300
www.kantarmedia.com

ZAŁĄCZNIK 2

Dodatek dotyczący bezpieczeństwa informacji

1. Wprowadzenie. W niniejszym załączniku dotyczącym wymagań bezpieczeństwa („Załącznik") ustanawia się podstawowe wymagania dotyczące bezpieczeństwa informacji po stronie Dostawcy, niezbędne do zapewnienia poufności, dostępności i integralności Informacji Poufnych KLIENTA oraz Informacji Poufnych dotyczących odbiorców KLIENTA. Dostawca jest zobowiązany do przestrzegania tych wymogów w trakcie wykonywania przez Dostawcę usług na podstawie niniejszej Umowy.

2. Terminologia. Zgodnie z niniejszym załącznikiem, każde z poniższych określeń (bez względu na to, czy jest pisane od wielkiej czy od małej litery) ma odpowiednie znaczenie określone poniżej. Każdy inny termin pisany od wielkiej litery i używany w niniejszym dokumencie, ale tutaj nie zdefiniowany, ma znaczenie przypisane mu w niniejszej Umowie.

2.1. Wykonawca oznacza podwykonawcę, niezależnego wykonawcę, usługodawcę lub przedstawiciela Dostawcy, który przechowuje, przetwarza lub obsługuje dane lub ma dostęp do wszelkich Informacji Poufnych KLIENTA oraz Informacji Poufnych odbiorców KLIENTA.

2.2. Informacje Wrażliwe KLIENTA oznaczają wszelkie Informacje Poufne KLIENTA oraz Informacje Poufne odbiorców KLIENTA, które obejmują dane osobowe (adres e-mail, imię i nazwisko itp.), informacje na temat stanu zdrowia, informacje finansowe lub informacje o pakietach inwestycyjnych.

2.3. Szyfrowanie oznacza odwracalne przekształcenie danych z formatu oryginalnego (zwykłego tekstu) w format zaszyfrowany (tekst szyfrowany), co jest mechanizmem ochrony poufności, integralności oraz/lub autentyczności informacji. Szyfrowanie wymaga stosowania algorytmu szyfrowania i co najmniej jednego klucza szyfrowania.

2.4. Przechowywanie oznacza przechowywanie, archiwizowanie, tworzenie kopii zapasowych oraz/lub wykonywanie podobnych czynności.

3. Przeglądy bezpieczeństwa. Dostawca zapewni KLIENTOWI prawo do przeprowadzenia na miejscu corocznego przeglądu programu bezpieczeństwa Dostawcy przez cały okres, przez który Dostawca przetwarza, przechowuje Informacje Poufne KLIENTA i Informacje Poufne odbiorców KLIENTA lub w inny sposób ma do nich dostęp. Dostawca niezwłocznie (ale w żadnym wypadku nie później niż trzydzieści (30) dni po otrzymaniu prośby KLIENTA o zaplanowanie i przeprowadzenie takiej weryfikacji) zaplanuje taką weryfikację we wzajemnie dogodnym terminie. Dostawca zapewni KLIENTOWI dostęp do swojej polityki, procedur i innej stosownej dokumentacji oraz do Pracowników Dostawcy, jeśli jest to uzasadnione potrzebą ułatwienia realizacji takich przeglądów. Dostawca jest zobowiązany do przedłożenia KLIENTOWI planu działań naprawczych w ciągu trzydziestu (30) dni od zakończenia przeglądu, a ponadto Dostawca jest zobowiązany do niezwłocznego podjęcia działań naprawczych w każdej takiej sprawie zgodnie z harmonogramem działań naprawczych uzgodnionym przez strony.

4. Szczegółowe wymogi w zakresie bezpieczeństwa

4.1. Polityka bezpieczeństwa. Dostawca jest zobowiązany do utrzymywania wyczerpującego zestawu pisemnych zasad i procedur bezpieczeństwa, które obejmują co najmniej następujące elementy:

(i) zobowiązanie Dostawcy do zapewnienia bezpieczeństwa informacji;

(ii) klasyfikacja informacji, jej oznaczanie i obchodzenie się z nimi, a ponadto polityka i procedury związane z obsługą informacji muszą opisywać dopuszczalne metody przesyłania, przechowywania i niszczenia informacji, przy czym takie metody nie mogą być mniej wymagające niż metody określone w „Wytycznych dotyczących ochrony informacji dostawców KLIENTA" (*CUSTOMER Supplier Information Protection Guidelines*), o których mowa poniżej;

(iii) akceptowalne wykorzystywanie majątku Dostawcy, w tym systemów komputerowych, sieci i systemów przesyłania wiadomości;

(iv) zarządzanie incydentami związanymi z bezpieczeństwem informacji, w tym powiadamianie o naruszeniu bezpieczeństwa danych i procedura zbierania dowodów;

(v) zasady uwierzytelniania w odniesieniu do formatu i treści haseł i sposobu korzystania z haseł dla użytkowników końcowych, administratorów i systemów;

(vi) narzędzia kontroli dostępu, w tym okresowe przeglądy praw dostępu;

(vii) środki dyscyplinarne w stosunku do pracowników, którzy nie przestrzegają tych zasad i procedur; oraz

(viii) tematy opisane w pozostałej części niniejszego punktu 4 w sposób zgodny ze stosownymi wymogami dotyczącymi tych tematów, określonymi w niniejszym punkcie 4.

4.2. Odpowiedzialność za Program Bezpieczeństwa Informacji po stronie Dostawcy. Dostawca ponosi odpowiedzialność za bezpieczeństwo informacji, a jego pracownicy są wyznaczeni do prowadzenia programu bezpieczeństwa informacji u Dostawcy oraz do wykonywania zadań związanych z bezpieczeństwem informacji i zarządzaniem ryzykiem informacyjnym.

4.3. Audyty, przegląd i monitorowanie Programu Bezpieczeństwa Informacji po stronie Dostawcy. Dostawca będzie regularnie monitorować i oceniać swój program bezpieczeństwa informacji w celu zapewnienia odpowiednich zabezpieczeń tak, aby ograniczyć ryzyko dotyczące Informacji Poufnych KLIENTA i Informacji Poufnych odbiorców KLIENTA.

4.4. Zarządzanie aktywami i informacjami. Dostawca jest zobowiązany:

(i) prowadzić wykaz wszystkich Informacji Poufnych KLIENTA i Informacji Poufnych odbiorców KLIENTA, które Dostawca przetwarza lub przechowuje;

(ii) prowadzić wykaz sprzętu komputerowego i oprogramowania wykorzystywanego przez Dostawcę do wykonywania czynności podejmowanych na mocy niniejszej Umowy; oraz

(iii) postępować zgodnie z określonymi niżej „Wytycznymi dotyczącymi ochrony informacji dostawców KLIENTA" (*CUSTOMER Supplier Information Protection Guidelines*) podczas obsługiwania, przetwarzania i przechowywania Informacji Poufnych KLIENTA oraz Informacji Poufnych odbiorców KLIENTA.

4.5. Bezpieczeństwo fizyczne i środowiskowe. Dostawca jest zobowiązany:

(i) ograniczyć dostęp do obszaru(-ów) po stronie Dostawcy, gdzie Informacje Poufne KLIENTA i Informacje Poufne odbiorców KLIENTA są przechowywane, udostępniane lub przetwarzane tak, aby dostęp ten mieli wyłącznie upoważnieni pracownicy Dostawcy;

(ii) wdrożyć w uzasadnionym zakresie najlepsze praktyki w zakresie systemów infrastruktury, w tym systemów przeciwpożarowych, systemów chłodzenia i zasilania, systemów awaryjnych oraz bezpieczeństwa pracowników;

(iii) zapewnić fizyczną kontrolę dostępu do wszystkich obszarów, w których przechowywane, udostępniane lub przetwarzane są Informacje Poufne KLIENTA i Informacje Poufne odbiorców KLIENTA tak, aby kontrola ta była współmierna do stopnia wrażliwości Informacji Poufnych KLIENTA i Informacji Poufnych odbiorców KLIENTA;

(iv) regularnie monitorować obszary, w których obsługiwane, przechowywane oraz/lub przetwarzane są Informacje Poufne KLIENTA i Informacje Poufne odbiorców KLIENTA.

4.6. Sprawy pracownicze. Dostawca jest zobowiązany:

(i) przeprowadzić weryfikację swoich pracowników pod kątem karalności (w tym także – jeśli zezwala na to prawo – analogiczną weryfikację Wykonawców mających dostęp do Informacji Poufnych KLIENTA i Informacji Poufnych odbiorców KLIENTA, z wyjątkiem przypadków ograniczonych lub zabronionych przez obowiązujące prawo); weryfikacji takiej należy dokonać przed udzieleniem takiej osobie dostępu do Informacji Poufnych KLIENTA oraz Informacji Poufnych odbiorców KLIENTA, a Dostawca nie zezwoli żadnej osobie, która nie przeszła pomyślnie weryfikacji, na uzyskanie dostępu do Informacji Poufnych KLIENTA i Informacji Poufnych odbiorców KLIENTA;

(ii) przeszkolić swoich nowych pracowników (w tym Wykonawców) w zakresie dopuszczalnego wykorzystania i postępowania z informacjami poufnymi Dostawcy i powierzonymi Dostawcy informacjami poufnymi innych firm (na przykład z Informacjami Poufnymi KLIENTA i Informacjami Poufnymi odbiorców KLIENTA);

(iii) zapewnić swoim pracownikom (w tym Wykonawcom) kształcenie i szkolenia w zakresie bezpieczeństwa oraz prowadzić rejestr osób, które ukończyły takie kształcenie; oraz

(iv) wdrożyć formalną procedurę rejestracji i wyrejestrowania użytkownika w celu udzielenia i cofnięcia dostępu do systemów i usług informatycznych Dostawcy; po rozwiązaniu umowy z pracownikami Dostawcy (w tym także z Wykonawcami) Dostawca cofnie danej osobie dostęp do Informacji Poufnych KLIENTA i Informacji Poufnych odbiorców KLIENTA możliwie jak najszybciej, ale w żadnym wypadku nie później niż dwa (2) dni robocze po rozwiązaniu umowy z taką osobą.

4.7. Komunikacja i działalność operacyjna. Dostawca jest zobowiązany:

(i) regularne sporządzać kopie zapasowe wystarczające do przywrócenia usług na rzecz KLIENTA w uzgodnionych terminach przywracania usług (lub – jeżeli strony nie uzgodniły konkretnych terminów przywracania usług – w terminie racjonalnym z biznesowego punktu widzenia);

(ii) szyfrować wszystkie nośniki kopii zapasowych zawierające Informacje Poufne KLIENTA i Informacje Poufne odbiorców KLIENTA zgodnie z przedstawionymi niżej „Wytycznymi dotyczącymi ochrony informacji dostawców KLIENTA" (*CUSTOMER Supplier Information Protection Guidelines*);

(iii) nie przechowywać ani nie powielać żadnych Informacji Poufnych KLIENTA ani Informacji Poufnych odbiorców KLIENTA poza siedzibą Dostawcy bez uzyskania uprzedniej pisemnej zgody KLIENTA;

(iv) nie przekazywać i nie dostarczać żadnych Informacji Poufnych KLIENTA ani Informacji Poufnych odbiorców KLIENTA jakimkolwiek osobom trzecim oraz nie udzielać osobom trzecim dostępu do jakichkolwiek Informacji Poufnych KLIENTA i ani Informacji Poufnych odbiorców KLIENTA bez uzyskania uprzedniej pisemnej zgody KLIENTA;

(v) jeżeli jakiekolwiek działania opisane w punktach (iii) i (iv) wyżej zostały zatwierdzone przez KLIENTA – prowadzić wykaz osób trzecich oraz/lub lokalizacji poza siedzibą Dostawcy, w których przechowuje lub powiela się jakiekolwiek Informacje Poufne KLIENTA oraz Informacje Poufne odbiorców KLIENTA; wykaz osób trzecich, które otrzymują informacje lub dostęp do Informacji Poufnych KLIENTA oraz Informacji Poufnych odbiorców KLIENTA w celu ich przechowywania, powielania, dostarczania lub udostępniania takich Informacji Poufnych KLIENTA oraz Informacji Poufnych odbiorców KLIENTA; wykaz metod przekazania lub transmisji takich Informacji Poufnych KLIENTA oraz Informacji Poufnych odbiorców KLIENTA do strony trzeciej; wykaz metod lub protokołów transmisji i szyfrowania/ochrony danych (w stosownych przypadkach) wykorzystywanych do przekazywania lub innego dostarczania takich Informacji Poufnych KLIENTA oraz Informacji Poufnych odbiorców KLIENTA; sporządzić opis Informacji Poufnych KLIENTA i Informacji Poufnych odbiorców KLIENTA, które zostały przekazane lub w inny sposób dostarczone stronie trzeciej wraz z nazwiskiem pracownika KLIENTA, który wyraził zgodę na takie działania oraz datę uzyskania takiej zgody;

(vi) podczas usuwania lub niszczenia Informacji Poufnych KLIENTA i Informacji Poufnych odbiorców KLIENTA – stosować procedury niszczenia danych, które spełniają lub przekraczają standardy Departamentu Obrony [USA] w zakresie bezpiecznego usuwania danych (Secure Data Sanitization – DOD 5220.22M). Dostawca niezwłocznie usunie lub zniszczy wszelkie Informacje Poufne Klienta i Informacje Poufne odbiorców KLIENTA na pisemny wniosek KLIENTA;

(vii) podczas przesyłania lub transportu Informacji Poufnych KLIENTA oraz Informacji Poufnych odbiorców KLIENTA – postępować zgodnie z przedstawionymi poniżej „Wytycznymi dotyczącymi ochrony informacji dostawców KLIENTA" (*CUSTOMER Supplier Information Protection Guidelines*), w tym z wytycznymi dotyczącymi szyfrowania;

(viii) stosować szyfrowanie twardego dysku na wszystkich laptopach, na których przechowywane są jakiekolwiek Informacje Poufne KLIENTA i Informacje Poufne odbiorców KLIENTA lub które są wykorzystywane przez Pracowników Dostawcy w celu uzyskania dostępu do jakichkolwiek Informacji Poufnych KLIENTA i Informacji Poufnych odbiorców KLIENTA, przy czym szyfrowanie będzie zgodne z przedstawionymi poniżej „Wytycznymi dotyczącymi ochrony informacji dostawców KLIENTA" (*CUSTOMER Supplier Information Protection Guidelines*);

(ix) zapewniać aktualne programy do wykrywania i zapobiegania złośliwemu oprogramowaniu na serwerach Dostawcy oraz/lub ma platformach użytkowników końcowych, którzy przesyłają, uzyskują dostęp, przetwarzają lub przechowują Informacje Poufne KLIENTA oraz Informacje Poufne odbiorców KLIENTA;

(x) utrzymywać wzmocniony obwód internetowy oraz bezpieczną infrastrukturę przy użyciu zapór sieciowych (*firewall*), programów antywirusowych i zapobiegających złośliwemu oprogramowaniu, systemów wykrywania włamań i innych technologii ochrony uzasadnionych z biznesowego punktu widzenia; oraz

(xi) wdrożyć regularne zarządzanie poprawkami oraz konserwację systemu dla wszystkich systemów Dostawcy wykorzystywanych do przekazywania, uzyskiwania dostępu, przetwarzania lub przechowywania Informacji Poufnych KLIENTA oraz Informacji Poufnych odbiorców KLIENTA.

4.8. Kontrola dostępu. Dostawca jest zobowiązany:

(i) egzekwować stosowanie najlepszych praktyk uwierzytelniania użytkowników; jeżeli do uwierzytelniania osób lub zautomatyzowanych procesów dostępu do Informacji Poufnych KLIENTA i Informacji Poufnych odbiorców KLIENTA stosowane są hasła, hasła te muszą być zgodne z bieżącymi najlepszymi praktykami w zakresie używania, tworzenia, przechowywania i ochrony haseł (patrz niżej: „Wytyczne dotyczącymi ochrony informacji dostawców KLIENTA").

(ii) zapewnić, aby identyfikatory użytkownika były niepowtarzalne dla poszczególnych osób fizycznych i nie były współdzielone;

(iii) przydzielać prawa dostępu w oparciu o stopień wrażliwości Informacji Poufnych KLIENTA i Informacji Poufnych odbiorców KLIENTA, wymagania związane ze stanowiskiem pracy danej osoby oraz potrzebę posiadania informacji przez daną osobę fizyczną w odniesieniu do konkretnych Informacji Poufnych KLIENTA i Informacji Poufnych odbiorców KLIENTA;

(iv) co najmniej raz w roku dokonywać przeglądu praw dostępu Pracowników Dostawcy (w tym Wykonawców) w celu zapewnienia aktualności ograniczeń związanych z zasadą ograniczonego dostępu;

(v) regularnie dokonywać przeglądu raportów o wejściu użytkowników do pomieszczeń Dostawcy, w których znajdują się Informacje Poufne KLIENTA i Informacje Poufne odbiorców KLIENTA; oraz

(vi) nie pozostawiać w swoich pomieszczeniach Informacji Poufnych KLIENTA i Informacji Poufnych odbiorców KLIENTA bez nadzoru na komputerach stacjonarnych, drukarkach lub w innych miejscach w sposób niezabezpieczony.

4.9. Rozwój aplikacji. Testy podatności na zagrożenia i testy penetracyjne. Dostawca jest zobowiązany:

(i) wdrażać bezpieczną metodologię rozwoju aplikacji, uwzględniającą kwestie bezpieczeństwa w całym cyklu rozwoju aplikacji;

(ii) opracowywać bezpieczne standardy kodowania i egzekwować ich stosowane;

(iii) przeprowadzać przeglądy bezpiecznego kodowania przy użyciu automatycznych narzędzi skanujących dla wszystkich aplikacji wykorzystywanych w kontakcie z odbiorcami zewnętrznymi oraz dla każdego oprogramowania opracowanego przez Dostawcę (lub Wykonawcę) i dostarczonego do KLIENTA;

(iv) przynajmniej raz na kwartał przeprowadzać skanowanie podatności na zagrożenia dla wszystkich zewnętrznych aplikacji, za pomocą których Dostawca otrzymuje, uzyskuje dostęp, przetwarza lub przechowuje Informacje Poufne KLIENTA i Informacje Poufne odbiorców KLIENTA; na żądanie KLIENTA Dostawca jest zobowiązany potwierdzić na piśmie, że przeprowadził takie skanowanie podatności na zagrożenia z wynikiem pozytywnym;

(v) przynajmniej raz w roku przeprowadzać testy penetracyjne dla wszystkich aplikacji wykorzystywanych w kontakcie z odbiorcami zewnętrznymi, za pomocą których Dostawca otrzymuje, uzyskuje dostęp, przetwarza lub przechowuje Informacje Wrażliwe KLIENTA; takie testy penetracyjne są przeprowadzane przez usługodawcę Dostawcy świadczącego usługi testowania, który to usługodawca został zatwierdzony przez KLIENTA; na żądanie KLIENTA Dostawca potwierdza na piśmie, że takie testy penetracyjne zostały przeprowadzone z wynikiem pozytywnym; Dostawca jest zobowiązany naprawić wszelkie istotne problemy wykryte podczas testów penetracyjnych przeprowadzonych przez Dostawcę lub w jego imieniu w ciągu trzydziestu (30) dni lub – jeśli nie można ich naprawić w ciągu trzydziestu (30) dni – Dostawca dokona naprawy w terminie wspólnie uzgodnionym przez Dostawcę i KLIENTA.

4.10. Wykonawcy. Dostawca jest zobowiązany:

(i) podjąć uzasadnione kroki w celu wyboru i utrzymania Wykonawców zdolnych do utrzymania środków bezpieczeństwa służące ochronie Informacji Poufnych KLIENTA i Informacji Poufnych odbiorców KLIENTA zgodnie z obowiązującymi przepisami ustawowymi i wykonawczymi oraz w sposób zapewniający nie mniejszą ochronę niż wymogi określone w niniejszej Umowie, w tym w niniejszym Załączniku; ponadto Dostawca jest zobowiązany utrzymywać z każdym takim Wykonawcą pisemną umowę, na mocy której Wykonawca ma obowiązek wdrożenia i utrzymywania takich środków bezpieczeństwa;

(ii) nie zapewniać żadnemu Wykonawcy możliwości uzyskania dostępu, przetwarzania, przechowywania, przeglądania lub innego kontaktu z Informacjami Poufnymi KLIENTA i Informacjami Poufnymi odbiorców KLIENTA bez uzyskania uprzedniej pisemnej zgody KLIENTA;

(iii) ponosić odpowiedzialność wobec KLIENTA w związku z wszelkimi działaniami i zaniechaniami każdego Wykonawcy, w tym w związku z nieprzestrzeganiem przez Wykonawcę postanowień niniejszej Umowy, w tym niniejszego Załącznika; oraz

(iv) regularnie przeprowadzać przegląd współpracy z każdym Wykonawcą, w tym przegląd zasad polityki i praktyk Wykonawcy w zakresie bezpieczeństwa informacji.

5. Zarządzanie incydentami związanymi z bezpieczeństwem informacji. Dostawca jest zobowiązany:

(i) wprowadzić, testować i utrzymywać procedurę reagowania na incydenty zagrażające bezpieczeństwu informacji, która obejmuje między innymi procesy przechowywania dowodów, informowania i współpracy z organami ścigania, organami władz i – w stosownych przypadkach – z podobnymi stronami, a także przeprowadzanie analiz kryminalistycznych;

(ii) powiadamiać KLIENTA na piśmie o wszelkich incydentach związanych z bezpieczeństwem informacji dotyczących Informacji Poufnych KLIENTA i Informacji Poufnych odbiorców KLIENTA, w tym o wszelkich rzeczywistych lub domniemanych przypadkach nieautoryzowanego dostępu do Informacji Poufnych KLIENTA i Informacji Poufnych odbiorców KLIENTA lub incydentach związanych z bezpieczeństwem systemów, sprzętu, wyposażenia, urządzeń lub komputerów Wykonawcy, lub incydentach w inny sposób związanych z pracownikami Wykonawcy; Dostawca jest zobowiązany do niezwłocznego powiadomienia o każdym takim zdarzeniu, jednak nie później niż dwadzieścia cztery (24) godziny po dniu, w którym po raz pierwszy dowiedział się o takim zdarzeniu. Następnie Dostawca będzie regularnie informował KLIENTA o prowadzonym postępowaniu wyjaśniającym i podejmowanych środkach naprawczych. Dostawca zezwala KLIENTOWI lub osobom przez niego wyznaczonym na udział we wszystkich aspektach postępowania wyjaśniającego. Dostawca pokrywa wszelkie koszty poniesione

przez dowolną stronę w związku z takimi incydentami, w tym między innymi w związku z powiadomieniem osób, których dane dotyczą, dochodzeniem kryminalistycznym, monitorowaniem kredytowym dla osób, których dane dotyczą oraz w związku z innymi działaniami naprawczymi i środkami prawnymi; oraz

(iii) w przypadku każdego takiego incydentu – nie później niż dziesięć (10) dni po zamknięciu incydentu przez Dostawcę dostarczyć KLIENTOWI ostateczne pisemne powiadomienie zawierające szczegółowe informacje dotyczące głównej przyczyny incydentu, podjętych działań i planów mających na celu zapobieżenie wystąpieniu podobnego incydentu w przyszłości.

6. Zarządzanie ciągłością działania. Dostawca jest zobowiązany:

(i) sporządzać i utrzymywać kompleksowy plan ciągłości działania obejmujący przywrócenie działania urządzeń technicznych, jak i operacji biznesowych w przypadku nieplanowanego zdarzenia; (ii) testować lub dokonywać przeglądu swojego planu ciągłości działania co najmniej raz w roku w sposób, jaki uzna za stosowny według własnego uznania.

7. Zgodność z prawem i przepisami. Dostawca jest zobowiązany:

(i) przestrzegać „Wytycznych dotyczących ochrony informacji dostawców KLIENTA" przedstawionych poniżej;

(ii) wprowadzić i utrzymywać wspólnie uzgodnione zasady i praktyki dotyczące przechowywania dokumentacji i niszczenia danych, mające zastosowanie do Informacji Poufnych KLIENTA i Informacji Poufnych odbiorców KLIENTA oraz wszelkich innych informacji wytworzonych w trakcie działalności Dostawcy na mocy niniejszej Umowy lub w inny sposób związanych z taką działalnością;

(iii) wprowadzić kodeks etyczny i zobowiązać pracowników do zapoznania się z nimi i corocznego potwierdzania jego znajomości (chyba że jest to zabronione przez prawo i w zakresie, w jakim jest to zabronione).

8. Ocena ryzyka dostawcy. Jeżeli KLIENT przeprowadził wcześniej kontrolę bezpieczeństwa lub przeprowadzi kontrolę u Dostawcy oraz/lub w jednym lub większej liczbie pomieszczeń Dostawcy (lub jego Wykonawców, stosownie do okoliczności) i w wyniku tej kontroli stwierdzono, że istnieje istotne ryzyko dla KLIENTA, Dostawca jest zobowiązany: (a) jeżeli nie zrobił tego wcześniej – do podejmowania odpowiedniej współpracy z KLIENTEM w celu niezwłocznego opracowania wzajemnie uzgodnionego planu działań naprawczych w celu naprawy problemów oraz (b) do niezwłocznego wdrożenia działań określonych w planie naprawczym nie później niż w odpowiednim terminie wskazanym w planie naprawczym.

9. Kradzież tożsamości. Jeżeli Dostawca przetwarza lub obsługuje dane bądź ma dostęp do Danych Osobowych, Dostawca niezwłocznie powiadomi KLIENTA w przypadku, gdy w trakcie działań Dostawcy wykonywanych na mocy niniejszej Umowy pracownicy Dostawcy powezmą wiadomość o potencjalnej kradzieży tożsamości dotyczącej osoby lub osób, których dotyczą te Dane Osobowe.

10. Aktualizacje. KLIENT może uaktualnić niniejszy **„Dodatek dotyczący bezpieczeństwa informacji"** w dowolnym czasie pod warunkiem powiadomienia Dostawcy na piśmie z trzydziestodniowym (30) wyprzedzeniem. Jeżeli Dostawca uzna, że nie może zastosować się do aktualizacji niniejszego Dodatku, powiadomi o tym na piśmie KLIENTA w ciągu trzydziestu (30) dni, określając konkretne postanowienia, do których Dostawca nie może się zastosować. W takim przypadku KLIENT zastrzega sobie prawo do

Ul. Szczytnicka 11,
50-382 Wrocław
T +48 717 875 300
www.kantarmedia.com

wypowiedzenia niektórych lub wszystkich usług lub projektów realizowanych we współpracy z Dostawcą bez ponoszenia odpowiedzialności i kar z tytułu zakończenia współpracy w takiej sytuacji.

Ul. Szczytnicka 11,
50-382 Wrocław
T +48 717 875 300
www.kantarmedia.com

Wytyczne dotyczące ochrony informacji dostawców KLIENTA

Macierz klasyfikacji i przetwarzania informacji KLIENTÓW

Nie ograniczając obowiązków Dostawcy określonych w niniejszej Umowie, w tym w niniejszym Załączniku, w poniższej tabeli przedstawiono podsumowanie niektórych szczegółowych wymogów mających zastosowanie podczas przesyłania (lub przenoszenia), przechowywania lub niszczenia Informacji Poufnych KLIENTA oraz Informacji Poufnych odbiorców KLIENTA, w tym Informacji Wrażliwych KLIENTA.

Klasyfikacja informacji	Przykłady	Przekazywanie	Przechowywanie	Niszczenie
Informacje Poufne KLIENTA i Informacje Poufne odbiorców KLIENTA inne niż Informacje Wrażliwe KLIENTA	Strategie i plany biznesowe; Raporty z audytu; Informacje marketingowe przed wprowadzeniem produktu lub usługi na rynek; Oprogramowanie opracowane przez KLIENTA; Specyfikacje techniczne lub architektura systemów	Format elektroniczny: Szyfrowanie w przypadku transmisji w sieciach publicznych lub przekazywania poza pomieszczenia Dostawcy na nośnikach lub urządzeniach przenośnych bądź innych nośnikach elektronicznych; Wydruki: Wysyłanie pocztą kurierską (w tym przesyłką kurierską z dostawą na następny dzień) lub listem poleconym z numerem umożliwiającym śledzenie przesyłki.	Ograniczenie dostępu tylko do kręgu upoważnionych pracowników; wykonywanie kwartalnych przeglądów praw dostępu. W przypadku magazynowania danych preferowane jest ich szyfrowanie.	Format elektroniczny: Należy stosować procedurę DOD 5220.22M lub równoważne procedury. Wydruki: Niszczyć w niszczarce.
Informacje Wrażliwe KLIENTA	Dane osobowe (w tym imię i nazwisko, adres e-mail, numer telefonu, adres	Tak jak wyżej	Ograniczenie dostępu tylko do kręgu upoważnionych pracowników;	Tak jak wyżej

	pocztowy, lub numer konta) Informacje o finansach osobistych Informacje na temat stanu zdrowia osoby		wykonywanie kwartalnych przeglądów praw dostępu. W przypadku magazynowania danych wymagane jest ich szyfrowanie.	

Szyfrowanie

Poniżej przedstawiono obecne preferowane przez KLIENTA algorytmy szyfrowania oraz aktualne dodatkowe akceptowane algorytmy szyfrowania. Podczas szyfrowania Informacji Poufnych KLIENTA oraz Informacji Poufnych odbiorców KLIENTA Dostawca ma obowiązek stosować jeden z preferowanych algorytmów szyfrowania, chyba że jest to niewykonalne z racjonalnego punktu widzenia. W takim przypadku podczas szyfrowania Informacji Poufnych KLIENTA oraz Informacji Poufnych odbiorców KLIENTA Dostawca ma obowiązek stosować jeden z dodatkowych akceptowanych algorytmów szyfrowania.

Preferowane algorytmy szyfrowania

Cel	Algorytmy	Minimalna długość klucza (bity)
Wymiana kluczy	RSA Diffie-Hellman	preferowana długość: 2048, jeśli jest to niemożliwe, wtedy 1024
Ochrona danych	AES w trybie CBC 3DES w trybie CBC EDE3	preferowana długość: 256, jeśli jest to niemożliwe, wtedy 128 168
Hash	SHA-256	nie dotyczy
HMAC	HMAC SHA-256	256
Podpis elektroniczny	RSA z SHA-256 DSA z SHA-256	preferowana długość: 2048, jeśli jest to niemożliwe, wtedy 1024

Dodatkowe akceptowane algorytmy szyfrowania

Cel	Algorytmy	Minimalna długość klucza (bity)
Ochrona danych	AES w trybie CTR RC4 RC5 w trybie CBC Blowfish w trybie CBC	preferowana długość: 2048, jeśli jest to niemożliwe, wtedy 128

	CAST-128 w trybie CBC IDEA w trybie CBC	
Hash	preferowany: SHA-2, jeśli nie jest to możliwe, wtedy: Nigdy nie należy stosować SHA-1 MD5, chyba że niezbędny jest wyjątek ze względów technicznych.	nie dotyczy
HMAC	preferowany: HMAC SHA-2, jeśli nie jest to możliwe, wtedy: SHA-1 Nigdy nie należy stosować MD5, chyba że niezbędny jest wyjątek ze względów technicznych.	160 128
Podpis elektroniczny	ECC z SHA-256, SHA-2 RSA z SHA-2 jest preferowany, jeśli nie jest to możliwe, wtedy SHA-1 DSA z SHA-2 jest preferowany, jeśli nie jest to możliwe, wtedy SHA-1	160 min. preferowana długość: 2048, jeśli jest to niemożliwe, wtedy 1024

Wytyczne dotyczące uwierzytelniania za pomocą hasła

Wszystkie hasła administrowane lub kontrolowane przez Dostawcę (lub Wykonawcę) muszą być zgodne z poniższymi wymogami:

Kryterium	Wymogi
Minimalna długość hasła	8 znaków
Stopień złożoności hasła	Hasło powinno zawierać 2 spośród 4 rodzajów znaków (wielkie litery, małe litery, cyfry, znaki specjalne); hasło nie powinno być łatwo kojarzone z daną osobą lub procesem; hasło nie może być wyrazem występującym w słowniku i nie może być zmieniane według określonego wzoru. Zdecydowanie zaleca się, aby hasła zawierały 3 spośród 4 wskazanych wyżej rodzajów znaków.
Maksymalny okres stosowania hasła	Maksymalnie 90 dni
Maksymalna długość historii hasła	1 dzień

Ul. Szczytnicka 11,
50-382 Wrocław
T +48 717 875 300
www.kantarmedia.com

Ochrona w trakcie przesyłania danych	Obowiązkowa. Przy przesyłaniu danych hasła muszą być szyfrowane.
Ochrona przy przechowywaniu	Obowiązkowa. Hasła muszą być „hashowane” przy użyciu zatwierdzonego algorytmu hash (patrz tabela powyżej).

Załącznik 3

Ochrona danych: RODO

1. OCHRONA DANYCH

1.1 W niniejszym załączniku 3:

(a) terminy użyte, ale nie zdefiniowane w inny sposób w niniejszej Umowie, mają znaczenie nadane im w rozporządzeniu UE o ochronie danych osobowych (RODO).

(b) **dane osobowe** mają znaczenie nadane im w rozporządzeniu UE o ochronie danych, ale dane te są również danymi osobowymi do celów niniejszej Umowy, jeżeli:

(i) dotyczą osób prawnych, a przetwarzanie tych danych na mocy niniejszej umowy lub w związku z nią podlega przepisom o ochronie danych mającym zastosowanie do danych dotyczących osób prawnych, jak również danych dotyczących osób fizycznych; lub

(ii) zawierają jedną z poniższych informacji, a ich przetwarzanie na mocy niniejszej umowy lub w związku z nią podlega jakimkolwiek przepisom lub regulacjom federalnym lub stanowym w USA: imię i nazwisko, adres, numer telefonu, numer faksu, numer ubezpieczenia społecznego, numer DEA, inny identyfikator wydany przez władze, dane karty kredytowej, identyfikatory ubezpieczenia medycznego, adresy IP, adresy e-mail oraz informacje dotyczące przeszłego, obecnego lub przyszłego stanu zdrowia lub kondycji (fizycznej lub psychicznej) danej osoby;

(c) **dane osobowe objęte Umową** oznaczają wszelkie dane osobowe, które są przetwarzane przez Dostawcę w trakcie świadczenia Usług lub wykonywania przez niego innych zobowiązań wynikających z niniejszej Umowy;

(d) **zabezpieczenia danych** oznaczają zabezpieczenia administracyjne, techniczne i fizyczne, które chronią je przed zagrożeniami lub ryzykiem dla integralności i bezpieczeństwa danych, nieuprawnionym lub przypadkowym zniszczeniem, utratą, zmianą lub wykorzystaniem danych oraz nieuprawnionym dostępem do danych osobowych objętych Umową, a także są zgodne z najlepszymi praktykami branżowymi;

(e) **wzorcowe warunki** oznaczają standardowe klauzule umowne zatwierdzone decyzją Komisji Europejskiej z dnia 5 lutego 2010 r. (2010/87/UE) w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich (ale wykluczające wszelkie klauzule umowne uznane przez Komisję Europejską w tej decyzji za fakultatywne), okresowo zmieniane lub zastępowane przez Komisję Europejską;

f) **państwo członkowskie** oznacza państwo członkowskie Unii Europejskiej na chwilę obecną;

(g) kiedy mowa o przekazywaniu danych z jakiegokolwiek kraju lub terytorium, uwzględnia się tu także zdalny dostęp do tych danych spoza tego kraju lub terytorium;

(h) odniesienia do prawa właściwego w punktach 1.4(c) i 1.8 (a)(iii) ograniczają się do prawa Unii Europejskiej lub prawa państwa członkowskiego, któremu podlega Dostawca, w zakresie, w jakim klauzule te mają zastosowanie do danych osobowych objętych Umową, których przetwarzanie podlega prawu Unii Europejskiej lub prawu państwa członkowskiego; oraz

(i) od dnia 25 maja 2018 r. odniesienia do unijnego rozporządzenia o ochronie danych osobowych należy rozumieć jako odniesienia do RODO, a zawarte w pkt 1.5(a)(ii) odniesienie do art. 25 ust. 6 unijnego rozporządzenia o ochronie danych odczytuje się jako odniesienie do art. 45 ust. 3 RODO.

1.2 Każdy z Dostawców i Klientów będzie przez cały czas wypełniał swoje obowiązki wynikające ze wszystkich przepisów dotyczących ochrony danych osobowych oraz wszystkich stosownych Zasad Dostawcy związanych z niniejszą Umową.

1.3 Dostawca nie jest uprawniony do wykorzystywania lub przetwarzania w inny sposób danych osobowych objętych Umową w żadnym innym celu niż w celu świadczenia Usług i wykonywania innych zobowiązań wynikających z niniejszej Umowy.

1.4 Dostawca obowiązany jest do:

(a) przetwarzania danych osobowych objętych Umową wyłącznie w oparciu o pisemne instrukcje Klienta i zgodnie z nimi;

(b) niezwłocznego powiadamiania Klienta o wszelkich błędach lub nieścisłościach w danych osobowych objętych Umową;

(c) zapewnienia, aby – o ile Klient nie wyda innych pisemnych instrukcji lub nie jest to wymagane na mocy prawa o ochronie danych – wszelkie kopie danych osobowych objętych Umową będące w posiadaniu lub pod kontrolą Dostawcy, podwykonawcy lub personelu Dostawcy zostały trwale zniszczone, gdy nie będą już potrzebne do wykonania zobowiązań Dostawcy wynikających z niniejszej Umowy;

(d) zapewnienia, aby dane osobowe objęte Umową były dostępne wyłącznie dla pracowników Dostawcy, którzy: (i) muszą mieć dostęp do danych, aby móc pełnić swoją rolę w realizacji zobowiązań Dostawcy wynikających z niniejszej Umowy; (ii) zostali odpowiednio przeszkoleni w zakresie wymogów przepisów o ochronie danych mających zastosowanie do przetwarzania, przechowywania i postępowania z danymi; oraz (iii) podlegają umownym lub ustawowym zobowiązaniom do zachowania poufności w odniesieniu do danych osobowych w zakresie objętym niniejszą Umową; oraz

(e) z zastrzeżeniem pkt 1.12 – zapewnienia Klientowi takiej współpracy, pomocy i informacji oraz sporządzenia wszystkich dokumentów, jakich może on w uzasadniony sposób zażądać, aby pomóc mu w wypełnieniu zobowiązań wynikających z przepisów o ochronie danych w zakresie, w jakim odnoszą się one do danych osobowych objętych Umową, oraz do współpracy i przestrzegania wskazówek lub decyzji wszelkich właściwych organów ochrony danych lub prywatności w odniesieniu do takich danych oraz w każdym przypadku podejmowania takich działań w takim czasie, aby pomóc Klientowi i dotrzymać wszelkich terminów nałożonych przez przepisy o ochronie danych lub organy ochrony danych.

1.5 W odniesieniu do danych osobowych, których przetwarzanie podlega prawu Unii Europejskiej lub prawu państwa członkowskiego, Dostawca ma obowiązek:

a) nieprzekazywania takich danych z jakiegokolwiek kraju lub terytorium i dopilnować, aby żaden podwykonawca nie przekazywał takich danych z jakiegokolwiek kraju lub terytorium, ani niewymagania od Klienta takiego przekazania, z wyjątkiem przekazywania danych:

(i) pomiędzy państwami członkowskimi Europejskiego Obszaru Gospodarczego;

(ii) z dowolnego państwa członkowskiego Europejskiego Obszaru Gospodarczego do dowolnego kraju lub terytorium, które w tym czasie podlegają aktualnym ustaleniom Komisji Europejskiej na mocy art. 25 ust. 6 rozporządzenia UE o ochronie danych mającego zastosowanie do przekazywania danych pod warunkiem, że Dostawca w wystarczającym stopniu powiadomił Klienta o przekazywaniu danych oraz podał informacje dotyczące takiego przekazywania w sposób rozsądny, aby Klient mógł spełnić wszelkie wymagania dotyczące powiadamiania, rejestracji lub zatwierdzania zawarte w przepisach o ochronie danych w odniesieniu do przekazywania danych;

(iii) w przypadku, gdy przekazanie jest kontynuowane i jest dokonywane we wszystkich istotnych aspektach w taki sam sposób, jak przekazanie danych dokonane z Klientem przed datą wejścia w życie (chyba że na mocy innego postanowienia niniejszej Umowy wymaga się zaprzestania przekazywania danych); lub

(iv) na podstawie pisemnej instrukcji Klienta, a następnie z zastrzeżeniem wszelkich uzasadnionych dodatkowych ograniczeń ustanowionych przez Klienta; oraz

(b) w dowolnym czasie w związku z przekazywaniem danych, o którym mowa w pkt 1.5 (a)(iii) lub pkt 1.5 (a)(iv) – niezwłocznie zawrzeć umowę (lub – w przypadku przekazywania danych przez podwykonawcę lub na rzecz podwykonawcy – zażądać niezwłocznego zawarcia przez niego umowy z Klientem) według Wzorcowych Warunków, które pozostaną bez zmian, lecz zostaną

uzupełnione w sposób, którego Klient może w sposób uzasadniony zażądać, lub w innej formie uzgodnionej przez Strony.

1.6 W odniesieniu do danych osobowych objętych Umową, a nieobjętych punktem 1.5, których przetwarzanie podlega przepisom o ochronie danych, zakazującym lub ograniczającym (a) przekazywanie danych osobowych objętych Umową do dowolnego kraju lub terytorium lub (b) przetwarzanie danych osobowych objętych Umową w dowolnym kraju lub terytorium, Dostawca nie będzie przekazywał ani przetwarzał takich danych osobowych objętych umową wbrew takiemu zakazowi lub ograniczeniu z wyjątkiem sytuacji, gdy przekazywanie danych dokonywane jest w ramach kontynuacji i jest dokonywane we wszystkich istotnych aspektach w taki sam sposób, jak przekazywanie danych, które miało miejsce w relacji z Klientem przed datą wejścia w życie (chyba że na mocy innego postanowienia niniejszej Umowy przekazywanie danych powinno ustać).

1.7 Dostawca:

(a) w każdym czasie posiada Przedstawiciela Dostawcy (i na bieżąco informować na piśmie inspektora ochrony danych Klienta o tożsamości Przedstawiciela Dostawcy), odpowiedzialnego za udzielanie Klientowi pomocy w odpowiedzi na zapytania otrzymywane od osób, których dane dotyczą, lub od jakiegokolwiek właściwego organu ds. ochrony danych lub prywatności;

(b) zapewnia, aby Przedstawiciel Dostawcy, o którym mowa w pkt 1.7(a), zawsze szybko i rozsądnie odpowiadał na zapytania, o których mowa w tym punkcie, w pełni uwzględniając odpowiednie wymogi przepisów o ochronie danych dotyczące terminowości udzielanych odpowiedzi; oraz

(c) nie podejmuje żadnych kroków w związku z zapytaniem, o którym mowa w pkt 1.7(a), z wyjątkiem pisemnych instrukcji otrzymanych od odnośnego Klienta.

1.8 Dostawca:

(a) nie ujawnia ani nie przekazuje żadnych danych osobowych objętych Umową osobom trzecim, z wyjątkiem sytuacji, kiedy:
  (i) ujawnienie lub przekazanie danych następuje zgodnie z pisemnymi instrukcjami Klienta;
  (ii) dane są przekazywane lub ujawniane podwykonawcy zgodnie z punktem 1.8 (b); lub
  (iii) dane są przekazywane lub ujawniane w zakresie wymaganym przez przepisy o ochronie danych osobowych lub inne postanowienia niniejszej Umowy;

(b) w odniesieniu do przetwarzania danych objętych Umową przez podwykonawcę Dostawca:
  (i) stosuje się do postanowień pkt 13.2 (Cesja, Podwykonawstwo);
  (ii) zapewnia, aby przetwarzanie danych przez podwykonawcę odbywało się na podstawie pisemnej umowy nakładającej na podwykonawcę takie same obowiązki, jakie zostały nałożone na Dostawcę na mocy niniejszego Załącznika 3 (*Ochrona danych: RODO*);
  (iii) zapewnia, aby podwykonawca wykonywał te obowiązki i przestrzegał ich; oraz
  (iv) jeżeli Klient tego zażąda – Dostawca zapewnia, aby podwykonawca zawarł z Klientem pisemną umowę nakładającą na niego takie same obowiązki, jak obowiązki Dostawcy wynikające z niniejszego Załącznika 3 (*Ochrona danych: RODO*),

1.9 Dostawca:

(a) przyjmuje, wdraża i utrzymuje zabezpieczenia danych, w tym w ramach zabezpieczeń danych – przyjmuje, wdraża i utrzymuje procedury i praktyki bezpieczeństwa mające na celu zapobieganie nieuprawnionemu lub przypadkowemu dostępowi do danych osobowych objętych Umową lub zniszczeniu, utracie, modyfikacji, wykorzystaniu lub ujawnieniu takich danych;

(b) gwarantuje wobec Klienta, że posiada spisaną politykę, procedury i praktyki bezpieczeństwa, które są zgodne z obowiązkami Dostawcy w zakresie bezpieczeństwa danych wynikającymi z przepisów o ochronie danych;

(c) utrzymuje i egzekwuje zabezpieczenia danych w każdym obiekcie, z którego Dostawca świadczy Usługi, oraz we wszystkich sieciach wykorzystywanych do przetwarzania danych osobowych objętych Umową; oraz

(d) okresowo dokonuje przeglądu i weryfikacji zabezpieczeń danych zgodnie z obowiązującymi praktykami branżowymi oraz na uzasadnione żądanie Klienta niezwłocznie dostarcza mu szczegółowe informacje na temat takich zmienionych zabezpieczeń danych na piśmie.

1.10 W przypadku nieautoryzowanego lub przypadkowego dostępu do danych osobowych objętych Umową, wykorzystania lub ujawnienia jakichkolwiek danych osobowych objętych Umową lub gdy Dostawca ma uzasadnione przekonanie, że taki dostęp, wykorzystanie lub ujawnienie miało miejsce lub istnieje takie ryzyko (przy czym chodzi między innymi o utratę lub całkowitą niemożność zlokalizowania nośników, urządzeń lub sprzętu, na których dane osobowe objęte Umową są lub mogą być przechowywane), Dostawca ma obowiązek:

(a) niezwłocznie, a w każdym razie w ciągu dwudziestu czterech (24) godzin, powiadomić Klienta, przedstawiając wystarczająco szczegółowe informacje na temat skutków dla Klienta wynikających z dostępu, wykorzystania lub ujawnienia danych objętych Umową oraz działań naprawczych podjętych i planowanych przez Dostawcę;

(b) z zastrzeżeniem punktu 1.12 – podjąć niezwłocznie wszelkie niezbędne i odpowiednie działania naprawcze mające na celu usunięcie przyczyn, które spowodowały dostęp, wykorzystanie lub ujawnienie danych

(c) podjąć wszelkie działania związane z dostępem, wykorzystaniem lub ujawnieniem danych wymagane na mocy przepisów o ochronie danych, w tym, bez ograniczeń, na wniosek Klienta – powiadomić osoby, których dane osobowe mogły zostać naruszone bez względu na to, czy takie zawiadomienie jest wymagane na mocy przepisów o ochronie danych czy nie; oraz

(d) jeżeli dostęp, wykorzystanie lub ujawnienie danych umożliwiłoby dostęp do informacji finansowych podmiotu, którego dotyczą dane, lub mogłoby spowodować uzasadnione ryzyko kradzieży tożsamości lub oszustwa w tym zakresie, Dostawca ma obowiązek przez racjonalnie określony okres nie krótszy niż jeden (1) rok świadczyć usługi w zakresie monitorowania zdolności kredytowej na rzecz takiego podmiotu, którego dotyczą dane.

1.11 Klient:

(a) jest samodzielnie odpowiedzialny za poinstruowanie Dostawcy o podjęciu takich kroków w ramach przetwarzania danych osobowych w imieniu Klienta, które są racjonalnie konieczne do wykonywania zobowiązań Dostawcy wynikających z niniejszej Umowy; oraz

(b) upoważnia Dostawcę – w zakresie dozwolonym przez przepisy o ochronie danych osobowych – do wydania równoważnych instrukcji podwykonawcom w imieniu Klienta.

1.12 Koszty i wydatki poniesione przez Dostawcę w związku z przestrzeganiem postanowień punktów 1.4 (e), 1.10 (b), 1.10 (c) i 1.10 (d) ponosi:

(a) Dostawca – w przypadkach, gdy działanie, którego obowiązkowe podjęcie przez Dostawcę wynika z naruszenia niniejszej Umowy lub zaniedbania, umyślnego lub oszukańczego działania lub zaniechania po stronie Dostawcy (w tym niezastosowania się do RODO), podwykonawcy lub pracowników Dostawcy; oraz

(b) Klient – w innych przypadkach.

Podpisano w imieniu Dostawcy.

PODPIS _____

IMIĘ I NAZWISKO (DRUKIEM) _____

STANOWISKO _____

DATA _____