UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH
(„UMOWA")

zawarta [.] 2018 roku pomiędzy:

[.] z siedzibą w [.] ([.]) przy ulicy [.], zarejestrowaną przez Sąd Rejonowy [.] pod numerem KRS [.], NIP [.], REGON [.], o kapitale zakładowym [.] złotych / zarejestrowaną w Centralnej Ewidencji i Informacji o Działalności Gospodarczej
reprezentowaną/-ym przez [.]
zwaną dalej „**Firma"**

a

[.] z siedzibą w [.] ([.]) przy ulicy [.], zarejestrowaną przez Sąd Rejonowy [.] pod numerem KRS [.], NIP [.], REGON [.], o kapitale zakładowym [.] złotych / zarejestrowaną w Centralnej Ewidencji i Informacji o Działalności Gospodarczej
reprezentowaną/-ym przez [.]
zwaną/-ym dalej „**Klient**"

Klient i Firma są w dalszej części Umowy zwani także osobno „**Stroną**" lub łącznie „**Stronami**".

Zważywszy, że:

1. Usługa świadczona Klientowi przez Firmę („**Usługa**") może wymagać przetwarzania Danych Osobowych (określonych poniżej) przez Firmę, Strony chcą zapewnić zgodność przetwarzania Danych Osobowych z przepisami prawa, w szczególności z Rozporządzeniem 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 ("**RODO**") - od momentu kiedy będzie miało zastosowanie - oraz z innymi znajdującymi zastosowanie przepisami prawa regulującymi ochronę danych osobowych;
2. Klient jest administratorem danych osobowych, które są przetwarzane przy wykorzystaniu Usługi („(„**Dane Osobowe**") bądź też działa na podstawie upoważnienia administratora Danych Osobowych, jako podmiot przetwarzający w imieniu administratora. Szczegółowy opis rodzaju Danych Osobowych oraz kategorie osób, których Dane Osobowe dotyczą znajduje się w **Załączniku nr 1**;
3. Klient i Firma zawarli w dniu [.] [.] r. Umowę o Świadczenie Usługi (**Umowa o Świadczenie Usługi**"), której niniejsza Umowa stanowi integralną część.

Strony postanowiły, co **następuje:**

§1 PRZEDMIOT UMOWY

1. Zgodnie z art. 28 ust. 3 RODO, Klient powierza Firmie przetwarzanie Danych Osobowych, a Firma powierzenie przyjmuje.
2. Firma zobowiązuje się do przetwarzania Danych Osobowych: (i) zgodnie z obowiązującym prawem oraz Umową, (ii) wyłącznie w celu świadczenia przez Firmę Usługi na rzecz Klienta, (iii) w zakresie, celu oraz w ramach czynności i charakteru opisanych w **Załączniku nr 1** oraz (iv) od momentu rozpoczęcia świadczenia Usługi do momentu rozwiązania Umowy, z zastrzeżeniem §7 ust. 2 Umowy.
3. Rola Firmy ograniczona jest do udostępnienia Klientowi narzędzi Usługi do wykorzystania w celu przetwarzania Danych Osobowych. Firma nie ma wpływu na zakres Danych Osobowych przetwarzanych przez Klienta w Usłudze poza wskazaniem minimalnego zakresu Danych Osobowych niezbędnych do prawidłowego korzystania z Usługi, nie ustala celów i sposobów ich przetwarzania i nie monitoruje zakresu tych danych, legalności podstaw ich przetwarzania

ani poprawności przetwarzania przez Klienta.

§2 OŚWIADCZENIA KLIENTA

1. Klient oświadcza, iż Dane Osobowe zostały pozyskane i są przetwarzane przez niego zgodnie z obowiązującymi przepisami prawa, w tym zgodnie z RODO. Klient potwierdza w szczególności, że (i) zebrał i posiada wymagane przepisami zgody na prowadzenie działań marketingu bezpośredniego, w tym zgody na przesyłanie informacji handlowych drogą elektroniczną oraz na używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego – w przypadku gdy prowadzi takie działania, (ii) przekazał osobom, których dane dotyczą informacje o przetwarzaniu ich danych w zakresie i w sposób wymagany przez RODO, oraz że (iii) jest uprawniony do przetwarzania Danych Osobowych i powierzenia ich do przetwarzania Firmie w zakresie i celu określonym w **Załączniku nr 1** do Umowy. Ponadto, jeśli Klient nie jest administratorem Danych Osobowych, potwierdza, że uzyskał wymaganą przepisami RODO zgodę właściwego administratora na powierzenie Firmie dalszego przetwarzania Danych Osobowych w takim celu i zakresie.
2. Klient potwierdza, że techniczne i organizacyjne środki wdrożone przez Firmę, określone w **Załączniku nr 2**, są odpowiednie i wystarczające dla ochrony praw osób, których Dane Osobowe dotyczą, i uznaje, że Firma zapewnia wystarczające gwarancje w tym zakresie.
3. Niezależnie od powyższego, Klient zobowiązuje się, zgodnie z zasadami Umowy, do korzystania z Usługi w sposób bezpieczny i zgodny z prawem, w tym do odpowiedniego zabezpieczenia danych uwierzytelniających do Konta klienta, zapewnienia bezpieczeństwa Danych Osobowych podczas przekazywania ich do Usługi, podejmowania odpowiednich działań mających na celu bezpieczne szyfrowanie lub tworzenie we własnym zakresie kopii zapasowych Danych Osobowych powierzonych Firmie oraz ochrony Danych Osobowych przed nieuprawnionym dostępem osób trzecich. Klient potwierdza, że przyjmuje do wiadomości, iż w związku ze świadczeniem Usługi, Firma stosuje pliki cookie i inne podobne technologie służące śledzeniu aktywności użytkowników. Klient zobowiązuje się stosować odpowiednie powiadomienia, uzyskać odpowiednie zgody i posiadać mechanizmy ich wycofywania (opt-in i opt-out) wymagane przepisami prawa, aby umożliwić Firmie stosowanie tych technologii zgodnie z prawem i gromadzenie danych z urządzeń Kontaktów zgodnie z Polityką Cookie i w sposób tam opisany.
4. Klient obowiązany jest powiadomić Firmę bez zbędnej zwłoki o każdej kontroli wykonywanej przez Generalnego Inspektora Ochrony Danych Osobowych („**GIODO**"), a od chwili jego powołania – przez Prezesa Urzędu Ochrony Danych Osobowych („**PUODO**"), która ma związek z przetwarzaniem powierzonych Danych Osobowych oraz o każdym piśmie GIODO lub PUODO dotyczącym składania wyjaśnień w zakresie tychże Danych Osobowych.

§3 POLECENIA KLIENTA

1. Firma jest zobowiązana do przetwarzania Danych Osobowych wyłącznie zgodnie z poleceniami przekazanymi przez Klienta, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego stanowi inaczej. W tym drugim przypadku stosuje się §4 ust.6 a Umowy.
2. Polecenia Klienta znajdują się w Umowie oraz Umowie o Świadczenie Usługi lub są zlecane i wykonywane za pośrednictwem funkcjonalności udostępnionych przez Firme w Usłudze. Klient jest zobowiązany zapewnić, że wszelkie polecenia przekazywane Firmie są zgodne z obowiązującymi przepisami o ochronie danych osobowych.
3. Wszelkie dalsze polecenia, które wykraczają poza polecenia określone w ust. 2 powyżej, muszą dotyczyć przedmiotu Umowy lub Umowy o Świadczenie Usługi. Jeżeli wdrożenie dalszych poleceń skutkuje kosztami dla Firmy, Firma poinformuje Klienta o takich kosztach wraz z wyjaśnieniem wysokości kosztów przed wykonaniem polecenia. Po potwierdzeniu przez Klienta, że poniesie on koszty wykonania polecenia oraz po ich zapłacie przez Klienta, Firma jest zobowiązana do realizacji dalszego polecenia pod warunkiem, że pozwalają na to możliwości techniczne i organizacyjne Firmy. Klient udziela dalszych poleceń na piśmie, chyba że pilny charakter lub inne szczególne okoliczności uzasadniają udzielenie poleceń w

formie elektronicznej. Polecenia w formie innej niż pisemna powinny być niezwłocznie odpowiednio udokumentowane.

4. Firma niezwłocznie informuje Klienta, jeżeli jego zdaniem polecenie narusza RODO lub inne przepisy prawa powszechnie obowiązującego Unii Europejskiej lub państwa członkowskiego i zwraca się do Klienta o wycofanie, zmianę lub potwierdzenie kwestionowanego polecenia. W oczekiwaniu na decyzję Klienta Firma jest uprawniony do zawieszenia wykonania kwestionowanego polecenia. W przypadku, w którym wykonanie polecenia Klienta mimo złożenia wyjaśnień prowadziłoby do naruszenia powszechnie obowiązujących przepisów prawa Unii Europejskiej lub państwa członkowskiego, Firma jest uprawniony do wstrzymania się od realizacji tego polecenia.

§4 OŚWIADCZENIA I ZOBOWIĄZANIA FIRMA

1. Uwzględniając ryzyko naruszenia praw i wolności osób fizycznych oraz stan wiedzy technicznej, koszty wdrażania, zakres, charakter, kontekst oraz cele przetwarzania Danych Osobowych, Firma oświadcza, iż zgodnie z art. 32 RODO, wdrożył odpowiednie środki techniczne i organizacyjne, mające na celu zabezpieczenie przetwarzania Danych Osobowych. Opis wdrożonych środków znajduje się w **Załączniku nr 2**. Firma może w każdym czasie zmienić wdrożone środki, pod warunkiem, że nie będą one zapewniały niższego poziomu ochrony niż środki obowiązujące w momencie zawarcia Umowy. Informacja o aktualnych środkach technicznych i organizacyjnych wraz z informacjami o zmianach w zakresie wdrożonych środków będzie dostępna w Koncie Klienta od dnia 25 maja 2018 r. Na uzasadniony wniosek Klienta Firma przekaże Klientowi dalsze informacje niezbędne Klientowi do wykazania spełnienia obowiązków określonych w art. 28 RODO. Postanowienie §4 ust. 5 zdanie ostatnie stosuje się odpowiednio.
2. Firma zobowiązuje się do zabezpieczenia Danych Osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, uszkodzeniem, zniszczeniem lub utratą i podejmie wszelkie niezbędne kroki służące zachowaniu w tajemnicy Danych Osobowych oraz sposobu ich zabezpieczenia zgodnie z obowiązującymi przepisami.
3. Firma oświadcza, że wszystkie osoby upoważnione do przetwarzania Danych Osobowych zobowiązały się do zachowania ich w tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy zgodnie z art. 28 ust. 3 lit. b RODO, a za ich działanie lub zaniechanie Firma odpowiada jak za swoje własne.
4. Na Kliencie spoczywa obowiązek wykonania żądań osób, których dotyczą Dane Osobowe oraz przygotowania odpowiedzi na te żądania. Firma zobowiązuje się do wsparcia Klienta, w miarę swoich możliwości i w rozsądnym zakresie, w wywiązywaniu się przez niego z tego obowiązku, w szczególności poprzez zastosowanie odpowiednich i możliwych środków technicznych i organizacyjnych niezbędnych Klientowi do umożliwienia skorzystania przez osoby z uprawnień przysługujących im na mocy Rozdziału III RODO.
5. Firma jest zobowiązany do wspierania Klienta w wykonywaniu zadań przewidzianych w art. 32 - 36 RODO w odniesieniu do Usługi, przekazując Klientowi niezbędne informacje. W odniesieniu do wspierania Klienta w prowadzeniu oceny skutków dla ochrony danych (art. 35 RODO) oraz uprzednich konsultacji z organem nadzorczym (art. 36 RODO), Firma jest zobowiązany udzielić pomocy tylko w takim zakresie, w jakim obowiązki Klienta nie mogą być wypełnione przez Klienta za pomocą innych środków. Firma poinformuje Klienta o kosztach takiej pomocy i po potwierdzeniu przez Klienta poniesienia tych kosztów, Firma zapewni wymagane wsparcie.
6. Firma jest zobowiązany do powiadomienia Klienta bez zbędnej zwłoki od momentu powzięcia wiarygodnej, potwierdzonej wiadomości:
    a. o zobowiązaniu Firma lub jego podwykonawcy na podstawie prawa Unii Europejskiej lub prawa państwa członkowskiego, któremu podlega, do przetwarzania Danych Osobowych w sposób wykraczający poza polecenia Klienta; w takim przypadku przed rozpoczęciem takiego przetwarzania Firma poinformuje Klienta o tym obowiązku prawnym, chyba że prawo zabrania udzielania takiej informacji z uwagi na ważny interes publiczny; w takim przypadku powiadomienie dla Klienta określi wymóg prawny wynikający z prawa Unii Europejskiej lub państwa członkowskiego;

b. o stwierdzonym naruszeniu ochrony Danych Osobowych przez Firma lub jego podwykonawcę, które ma wpływ na Dane Osobowe Klienta objęte Umową. W takim przypadku Firma zobowiązany jest do wsparcia Klienta w zakresie wykonania przez Klienta, w stosownych przypadkach, obowiązków poinformowania organu nadzorczego lub osoby, której dane dotyczą, dostarczając dostępnych dla Firma informacji zgodnie z art. 33 ust. 3 RODO.

§5 KORZYSTANIE Z PODWYKONAWCÓW (DALSZE POWIERZENIE)

1. W celu zapewnienia prawidłowego świadczenia Usługi, Klient wyraża zgodę na korzystanie przez Firma z podwykonawców oraz na dalsze powierzenie im przetwarzania Danych Osobowych. Dla uniknięcia wątpliwości oraz nie ograniczając ogólnej zgody udzielonej Firma w zdaniu poprzednim, Klient wyraża w szczególności zgodę na podwykonawców wskazanych w **Załączniku nr 3**.
2. Aktualna lista podwykonawców Firma będzie dostępna w Koncie Klienta od dnia 25 maja 2018 r. Firma poinformuje Klienta o wszelkich planowanych zmianach w zakresie podwykonawców, na rzecz których będzie dokonywał dalszego powierzenia przetwarzania Danych Osobowych. Poinformowanie Klienta odbywa się za pomocą informacji przekazanej poprzez Konto Klienta i z odpowiednim wyprzedzeniem. Klient ma prawo do wyrażenia sprzeciwu (drogą elektroniczną lub listownie) odnośnie korzystania przez Firma ze wskazanego podwykonawcy w ciągu 14 dni od otrzymania informacji o planowanej zmianie. Jeśli Klient nie wyrazi sprzeciwu w ciągu 14 dni od otrzymania informacji o planowanej zmianie, uznaje się, że wyraża zgodę na taką zmianę. Po otrzymaniu sprzeciwu Klienta, Firma ma 30 dni na ustalenie dalszego postępowania w związku z otrzymanym sprzeciwem. Po tym okresie, każda ze Stron może wypowiedzieć Umowę zgodnie z postanowieniami Umowy o Świadczenie Usługi. W przypadku, jeśli Umowa o Świadczenie Usługi zawarta jest na czas określony, Strony ustalają, że sprzeciw wobec podwykonawcy stanowi przesłankę rozwiązania Umowy o Świadczenie Usługi i obie umowy rozwiązują się z terminem wypowiedzenia 14 dni na koniec okresu rozliczeniowego. Niezależnie od powyższego, Firma zastrzega, że sprzeciw Klienta odnośnie wyboru podwykonawcy może uniemożliwić Klientowi korzystanie z wszystkich funkcjonalności Usługi.
3. Dalsze powierzenie przetwarzania Danych Osobowych może nastąpić wyłącznie w granicach i w celu realizacji Usługi. Firma oświadcza, że (i) wybrani przez niego podwykonawcy spełniają wszelkie wymogi wynikające z RODO oraz właściwych przepisów o ochronie danych osobowych, (ii) zgodnie z art. 28 ust. 4 RODO zawarł umowy z podwykonawcami w zakresie przetwarzania Danych Osobowych i że zawierają one postanowienia zobowiązujące podwykonawców do analogicznych obowiązków, jakie zostały określone w Umowie wobec Firma oraz że (iii) standard ochrony danych osobowych obowiązujący u współpracujących z nim podwykonawców jest co najmniej równy standardowi ochrony danych obowiązującej w Firma.

§6 UPRAWNIENIA KONTROLNE KLIENTA

1. Klientowi przysługuje prawo kontroli zgodności przetwarzania Danych Osobowych przez Firma z postanowieniami Umowy („**Audyt**"). Audyt może odbyć się również za pośrednictwem niezależnego audytora upoważnionego przez Klienta, pod warunkiem uprzedniego zawarcia między audytorem a Firma umowy o zachowaniu poufności.
2. Klient zobowiązuje się, że jako upoważniony audytor nie zostanie wyznaczony podmiot prowadzący pośrednio lub bezpośrednio działalność konkurencyjną w stosunku do działalności prowadzonej przez Firma. Przez działalność konkurencyjną rozumie się każdą działalność, odpłatną lub nieodpłatną, w kraju lub za granicą, niezależnie od formy prawnej, która jest prowadzona w tym samym lub takim samym zakresie przedmiotowym i skierowana do tego samego kręgu odbiorców, pokrywająca się – chociażby częściowo – z zakresem działalności podstawowej lub ubocznej Firma lub podmiotów z grupy Firma na świecie. Dla oceny czy dany podmiot jest konkurencyjny, brany pod uwagę będzie nie tylko przedmiot działalności takiego podmiotu wynikający z treści umowy lub innego dokumentu stanowiącego

podstawę jego funkcjonowania, ale również przedmiot działalności faktycznie wykonywanej przez ten podmiot. W przypadku zlecenia przeprowadzenia Audytu podmiotom konkurencyjnym w stosunku do Firma, Firma jest uprawniony do odmowy przeprowadzenia Audytu do czasu wyznaczenia innego podmiotu przeprowadzającego Audyt w imieniu Klienta lub do czasu ustalenia dalszego sposobu postępowania pomiędzy Firma a Klientem.

3. Audyt podlega następującym warunkom: (i) może dotyczyć jedynie Danych Osobowych powierzonych do przetwarzania Firma na podstawie Umowy i będzie ograniczony do siedziby Firma i urządzeń służących do przetwarzania Danych Osobowych oraz personelu zaangażowanego w czynności przetwarzania objęte zakresem Umowy; (ii) będzie prowadzony sprawnie i tak szybko jak to jest możliwe, nie dłużej niż przez 2 dni robocze (iii) będzie odbywać się nie częściej niż raz w roku, chyba że Audyt jest wymagany zgodnie z wymogami prawa lub przez właściwy organ nadzorczy, bądź też ma miejsce niezwłocznie po stwierdzeniu istotnego naruszenia Danych Osobowych przetwarzanych na podstawie Umowy, (iv) może być wykonywany w zwykłych godzinach pracy Firma, w sposób nie zakłócający działalności gospodarczej Firma i zgodnie z politykami bezpieczeństwa Firma; (v) Klient powiadomi Firma o zamiarze przeprowadzenia Audytu drogą elektroniczną lub listownie co najmniej na 14 dni roboczych przed planowanym terminem Audytu. W przypadku niezależnej od Firma niemożliwości przeprowadzenia Audytu w planowanym terminie lub innych niespodziewanych przeszkód, Firma powiadomi Klienta o takich okolicznościach i zaproponuje nowy termin Audytu, nie później jednak niż w ciągu 7 dni roboczych od terminu wskazanego przez Klienta; (vi) Klient ponosi wszelkie koszty wynikające z lub poniesione w związku z Audytem, z wyjątkiem przypadków, w których ujawnione zostanie poważne naruszenie zasad bezpieczeństwa Danych Osobowych, dotyczące lub zagrażające Danym Osobowym Klienta; (vii) Audyt nie może zmierzać ani prowadzić do ujawnienia tajemnic prawnie chronionych (w tym tajemnicy przedsiębiorstwa Firma). Klient jest zobowiązany do utworzenia raportu z Audytu podsumowującego ustalenia z tego audytu. Raport zostanie przekazany Firma i będzie stanowić informacje poufne o Firma, które nie mogą być ujawniane stronom trzecim bez pisemnej zgody Firma, chyba że wymaga tego obowiązujące prawo.
4. W przypadku posiadania przez Firma certyfikacji, o której mowa w art. 42 RODO lub stosowania kodeksu postępowania, o którym mowa w art. 40 RODO, uprawnienia kontrolne Klienta mogą być realizowane również poprzez odwołanie się przez Firma do wyników monitorowania zasad certyfikacji lub kodeksu postępowania. W takim wypadku, Audyt będzie dotyczyć jedynie kwestii, które nie mogą zostać dostatecznie wyjaśnione poprzez przedstawienie takich wyników przez Firma.

§7 ZWROT LUB USUNIĘCIE DANYCH OSOBOWYCH

1. Po zakończeniu stosunku powierzenia przetwarzania Danych Osobowych, Firma wedle oświadczenia Klienta, usunie Dane Osobowe (usuwając wszystkie istniejące kopie Danych Osobowych) lub zwróci je Klientowi (o ile będzie to możliwe wraz z nośnikami, na których są one przechowywane), chyba że prawo nakazuje lub upoważnia Firma do przechowywania danych osobowych w oparciu o niezależną podstawę prawną przez dłuższy okres. W przypadku nieotrzymania przez Firma oświadczenia, o którym mowa w zdaniu poprzedzającym, drogą elektroniczną lub listownie, w terminie 5 dni od zakończenia stosunku powierzenia Danych Osobowych, uznaje się, że Klient żąda usunięcia powierzonych Danych Osobowych. W przypadku wyboru zwrócenia Danych Osobowych, Firma przekaże lub umożliwi Klientowi pobranie danych w powszechnie używanym formacie służącym do zapisu maszynowego.
2. Klient może uzyskać kopię przetwarzanych Danych Osobowych w trakcie trwania Umowy o Świadczenie Usługi, lecz nie później niż w ciągu 30 (trzydziestu) dni po zamknięciu Konta, w czasie których Dane Osobowe będą przetwarzane przez Firma wyłącznie w celu ewentualnej reaktywacji konta przez Klienta. Firma zobowiązuje się do przetwarzania Danych Osobowych w czasie 30 (trzydziestu) dni po zamknięciu Konta jedynie poprzez przechowywanie Danych Osobowych na rzecz Klienta z wyłączeniem jakichkolwiek innych operacji na tych Danych, z zastrzeżeniem odmiennych obowiązków Firma wskazanych w obowiązujących przepisach prawa lub nałożonych na Firma przez uprawnione organy. Po upływie tego terminu Dane

Osobowe zostaną usunięte z bazy głównej i nie będzie możliwe ich odzyskanie. Przez czas określony kolejnych 15 (piętnastu) dni Dane Osobowe będą przechowywane w postaci zaszyfrowanej jedynie w kopiach zapasowych, który to okres wymagany jest ze względu na specyfikę działania kopii zapasowych do całkowitego usunięcia Danych Osobowych.

§8 ODPOWIEDZIALNOŚĆ

1. Odpowiedzialność kontraktowa oraz deliktowa Firma ograniczona jest do bezpośrednich strat poniesionych przez Klienta. Firma nie ponosi odpowiedzialności za utracone korzyści, niezależnie od ich źródła, z wyjątkiem przypadków winy umyślnej lub rażącego niedbalstwa.
2. Całkowita odpowiedzialność Firma, niezależnie od liczby i podstawy roszczeń Klienta ograniczona jest do równowartości opłaty abonamentowej za okres 3 (trzech) miesięcy, zapłaconej przez Klienta za Usługę w okresie rozliczeniowym bezpośrednio poprzedzającym datę, w której doszło do zdarzenia wywołującego szkodę, z wyłączeniem kwot składających się na opłaty instalacyjne lub wszelkiego rodzaju opłaty dodatkowe. Klient zwalnia Firma z wszelkich zobowiązań przekraczających powyższe ograniczenie.
3. Firma nie ponosi odpowiedzialności za nienależyte wykonanie lub niewykonanie Umowy wskutek Siły Wyższej.
4. Strony zgodnie postanawiają, że Klient jest odpowiedzialny za zaspokojenie roszczeń osób, których Dane Osobowe są przetwarzane, z tytułu szkód wywołanych na skutek nieprawidłowego przetwarzania Danych Osobowych w ramach Umowy, chyba że wykaże, że szkoda wynikła z wyłącznej winy Firma lub jego podwykonawców. W przypadku niewykazania powyższego, Klient ma obowiązek bezwarunkowego zwolnienia Firma z odpowiedzialności z tytułu wszelkich roszczeń zgłaszanych przez podmioty, których Dane Osobowe przetwarza Firma na podstawie Umowy, w związku z przetwarzaniem tych danych w ramach Umowy. W przypadku wszczęcia postępowania sądowego przeciwko Firma, Klient ma obowiązek na żądanie Firma wstąpić do takiego postępowania w charakterze strony i przejąć odpowiedzialność z tytułu zgłoszonego roszczenia.

§9 POSTANOWIENIA KOŃCOWE

1. Strony zgodnie potwierdzają, że z zastrzeżeniem wyjątków wskazanych w Umowie, wynagrodzenie Firma z tytułu czynności realizowanych w ramach Umowy uwzględnione jest w wynagrodzeniu należnym z tytułu świadczenia Usługi na rzecz Klienta.
2. Umowa została zawarta na czas nieokreślony, z zastrzeżeniem, że Umowa ulega rozwiązaniu najpóźniej z dniem usunięcia lub zwrotu Danych Osobowych stosownie do postanowień §7 Umowy.
3. Umowa zastępuje wszelkie istniejące między Stronami porozumienia dotyczące powierzenia Danych Osobowych, które Strony zawarły wcześniej w związku z Usługą, niezależnie od formy takich porozumień.
4. Zmiany Umowy wymagają formy pisemnej, w tym formy elektronicznej.
5. Wszelka komunikacja pomiędzy stronami Umowy będzie odbywała się wyłącznie na adresy wymienione poniżej:
    a. Firma – adres email [.]
    b. Klient – adres email [.]
6. Prawem obowiązującym dla Umowy jest prawo polskie. W sprawach nieuregulowanych w Umowie zastosowanie będą mieć przepisy RODO oraz inne właściwe przepisy prawa polskiego, a także postanowienia Polityki Prywatności dostępnej na stronie www. oraz Umowy o Świadczenie Usługi. Terminy pisane wielką literą (np. Kontakty, Siła Wyższa itp.), niezdefiniowane w Umowie, mają znaczenie nadane im w Umowie o Świadczenie Usługi. W przypadku niezgodności zapisów Umowy o Świadczenie Usługi z Umową, zapisy Umowy w odniesieniu do ochrony danych osobowych mają przeważające znaczenie.
7. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze Stron.

Firma Klient

_____ _____

Załącznik 1 – Opis przetwarzania Danych Osobowych

1. Cel przetwarzania powierzonych Danych

Dane Osobowe będą przetwarzane przez Firma w celu korzystania przez Klienta z Usługi świadczonej przez Firma.

2. Charakter i czynności przetwarzania

Przetwarzanie Firma będzie miało charakter zautomatyzowany oraz niezautomatyzowany. Przetwarzanie Danych Osobowych przez Firma następować będzie przy wykorzystaniu systemów informatycznych dostarczanych w ramach Usługi i obejmować będzie następujące czynności przetwarzania: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, wykonywanie kopii zapasowych Danych Osobowych, a także inne operacje niezbędne do realizacji Usługi.

W ramach przetwarzania Danych Osobowych Firma nie będzie komunikował się w imieniu Klienta bezpośrednio z osobami, których dane dotyczą.

Rola Firma ograniczona jest do udostępnienia Klientowi narzędzi Usługi do wykorzystania w celu przetwarzania Danych Osobowych. Firma nie ma wpływu na zakres Danych Osobowych przetwarzanych przez Klienta w Usłudze, nie ustala celów i sposobów ich przetwarzania i nie monitoruje zakresu takich Danych.

3. Kategorie osób, których dotyczą dane

Klient powierza Firma przetwarzanie Danych Osobowych następujących kategorii osób:

a. Kontakty – w tym osoby, których Dane Osobowe znajdują się na Liście Kontaktów lub których Dane Osobowe są zbierane i przechowywane przy pomocy Usługi, lub do których Klient będzie kierował komunikację za pomocą Usługi, w szczególności mogą nimi być kontrahenci, klienci, potencjalni klienci, osoby kontaktowe u partnerów biznesowych Klienta, subskrybenci newslettera Klienta;
b. uczestnicy webinarów;
c. osoby, których dane gromadzone są poprzez formularze i ankiety;
d. osoby upoważnione do korzystania z Konta przez Klienta (Współpracownicy).

Co do zasady, Usługa nie jest przeznaczona do przetwarzania szczególnych kategorii danych osobowych, o których mowa w art. 9 RODO, danych osobowych dotyczących wyroków skazujących i naruszeń prawa o których mowa w art. 10 RODO, ani też danych osobowych dzieci. Jednakże, decyzja co do zakresu danych, które Klient przekazuje Firma w Usłudze należy do Klienta. Decydując się umieścić w usłudze takie dane, Klient potwierdza, że środki zabezpieczeń wdrożone przez Firma są w jego ocenie wystarczające do ochrony powierzonych Danych Osobowych.

4. Kategorie powierzonych Danych Osobowych

Klient powierza Firma do przetwarzania następujące kategorie Danych Osobowych:

a. w odniesieniu do Kontaktów: adres e-mail.

Usługa daje możliwość przetwarzania również dodatkowych informacji, tj.:

- imię i nazwisko
- numer telefonu służbowego, telefonu prywatnego, telefonu komórkowego, numeru faksu
- adres url strony www, poprzez którą Kontakt przekazał Klientowi swoje dane
- dane adresowe Kontaktu
- adres strony, z której Kontakt został przekierowany [http_referer]
- płeć, wiek, data urodzin
- miejsce pracy

- Dane Osobowe zawarte w treściach wysyłanych przez Klienta przy pomocy Usługi
- dodatkowe informacje o Kontakcie [comment] oraz inne informacje na podstawie pól zdefiniowanych przez Klienta przy gromadzeniu danych Kontaktów w formularzach lub ankietach.

b. w odniesieniu do uczestników webinarów: adres email.
   Usługa daje możliwość przetwarzania również dodatkowych informacji, tj.:
   - imię i nazwisko,
   - nickname
   - adres strony, z której Kontakt został przekierowany [http_referer]
   - dodatkowe informacje o uczestniku webinaru, zebrane przez Klienta na formularzu rejestracji, podczas webinaru lub czatu.
c. w odniesieniu do osób, których dane gromadzone są przez formularze i ankiety: adres email.
   Usługa daje możliwość przetwarzania również dodatkowych informacji, tj.:
   - imię i nazwisko,
   - dodatkowe informacje na podstawie pól zdefiniowanych przez Klienta.
d. w odniesieniu do Współpracowników Klienta: adres email, nazwa użytkownika.
e. w odniesieniu do wszystkich powyższych kategorii: dane przetwarzane automatycznie w toku korzystania z Usługi (dane o korzystaniu z Usługi; dane gromadzone przy użyciu plików cookie lub innych technologii służących do śledzenia aktywności użytkowników; dane IP urządzenia, z którego dokonano zapisu Kontaktu do listy Kontaktów Klienta lub na którym otworzył maila wysłanego do niego przez Klienta w ramach korzystania z Usługi; dane o lokalizacji, dane o przeglądarce internetowej).

Załącznik nr 2. Opis wdrożonych środków organizacyjnych i technicznych służących ochronie danych osobowych.

A. Organizacyjne środki bezpieczeństwa.

I. Organizacja Systemu Zarzadzania Bezpieczeństwem Informacji.

1. Opracowano ogólną politykę bezpieczeństwa oraz szczegółowe polityki bezpieczeństwa dotyczące bezpieczeństwa organizacji, bezpieczeństwa informacji, bezpieczeństwa systemów informatycznych oraz bezpieczeństwa osób i mienia, w których określono podstawowe cele jakim mają służyć działania związane z realizacją polityk.
2. Określono ogólne i szczególne standardy bezpieczeństwa realizujące założenia polityk bezpieczeństwa w zakresie bezpieczeństwa informacji, bezpieczeństwa systemów informatycznych, bezpieczeństwa osób i mienia.
3. Opracowano szczegółowe procedury i instrukcje postępowania dotyczące realizacji standardów bezpieczeństwa w zakresie bezpieczeństwa informacji, bezpieczeństwa systemów informatycznych, bezpieczeństwa osób i mienia.
4. Polityki, standardy, procedury i instrukcje podlegają okresowym przeglądom i aktualizacjom zatwierdzanym przez najwyższe kierownictwo Spółki.
5. Opracowano, wdrożono i zapewniono utrzymanie ciągłości działania systemu monitorowania zmian w obowiązujących przepisach prawa dotyczących zasad przetwarzania danych osobowych.

II. Role i zadania

1. Określono role i zadania w procesach związanych z zarządzaniem bezpieczeństwem - wyznaczono osoby odpowiedzialne za realizację każdej polityki bezpieczeństwa.
2. Dla każdego zasobu (fizycznego i elektronicznego), mającego wartość dla organizacji, wyznaczono osobę odpowiedzialną (Właściciela Zasobu), której przypisano odpowiedzialność za zarządzanie bezpieczeństwem danego zasobu.
3. W celu zapewnienia właściwego poziomu realizacji ochrony danych osobowych wyznaczono i powołano niezależnego Administratora Bezpieczeństwa Informacji, który od dnia stosowania RODO zostanie zastapiony przez Inspektora Ochrony Danych.
4. Zapewniono bezpośrednią podległość Administratora Bezpieczeństwa Informacji, a następnie Inspektora Ochrony Danych pod najwyższe kierownictwo Spółki.
5. Zapewniono włączenie Administratora Bezpieczeństwa Informacji, a następnie Inspektora Ochrony Danych we wszystkie procesy związane z przetwarzaniem danych osobowych.
6. Zapewniono Administratorowi Bezpieczeństwa Informacji, a następnie Inspektorowi Ochrony Danych Osobowych odpowiedni dostęp do informacji i dokumentacji związanej z przetwarzaniem danych osobowych.
7. Osoby przetwarzające dane osobowe na zlecenie i w imieniu Spółki otrzymały imienne upoważnienie do przetwarzania danych osobowych.
8. Wszystkie osoby upoważnione do przetwarzania danych osobowych zostały objęte systemem wewnętrznych szkoleń z zakresu bezpieczeństwa i ochrony danych osobowych.
9. Wszystkie osoby upoważnione do przetwarzania danych osobowych zostały zobowiązane do zachowania poufności w czasie trwania stosunku pracy oraz po jego ustaniu.

III. Zarządzanie uprawnieniami i dostępami

1. Opracowano system zarządzania uprawnieniami dostępu do nośników danych, pomieszczeń, stref, budynków oraz systemów informatycznych i elementów infrastruktury informatycznej oraz sieci.
2. Zapewniono, iż osobom uprawnionym do przetwarzania danych osobowych przydzielane są minimalne uprawnienia dostępu, uzależnione od realizowanych zadań.
3. Zapewniono, iż uprawnienia dostępu do danych osobowych są doraźnie oraz okresowo monitorowane i kontrolowane.
4. Zapewniono, iż klucze, kody dostępu oraz uprawnienia dostępu w systemie kontroli dostępu do budynków, stref, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe, przydzielane są osobom upoważnionym do przetwarzania danych osobowych zgodnie z zakresem upoważnienia i zakresem zadań realizowanych na danym stanowisku pracy.
5. Zapewniono, iż budynki, strefy, pomieszczenia lub części pomieszczeń, w których przetwarzane są dane osobowe, zabezpiecza się przed dostępem osób nieuprawnionych, w czasie nieobecności osób uprawnionych do przebywania w tych pomieszczeniach. Osoby nieuprawnione do przebywania w pomieszczeniach służących do przetwarzania danych osobowych mogą przebywać w nich jedynie pod nadzorem osób uprawnionych.
6. Opracowano i wdrożono proces nadawania i odbierania uprawnień dostępu do danych osobowych, w szczególności systemów informatycznych.
7. Zapewniono, iż dla każdej osoby uprawnionej do dostępu do systemu informatycznego, elementu infrastruktury informatycznej lub sieci nadawany jest unikalny identyfikator, który nie może zostać przypisany innej osobie.
8. Przeprowadzane są i udokumentowane okresowe przeglądy dostępu wszystkich użytkowników, kont systemowych, kont testowych oraz kont ogólnych.
9. Zapewniono, iż dla każdej osoby uprawnionej do dostępu do systemu informatycznego, elementu infrastruktury informatycznej lub sieci autoryzacja

realizowana jest przy użyciu bezpiecznych metod transmisji danych służących do uwierzytelnienia.
10. Zapewniono, iż ustanowione dla każdej osoby uprawnionej do dostępu do systemu informatycznego, elementu infrastruktury informatycznej lub sieci hasło dostępu podlega procedurom audytu oraz zmianie w ustalonym okresie czasu.
11. Opracowano i wdrożono standard bezpiecznego przekazywania haseł w przypadku konieczności przekazania użytkownikowi systemu informatycznego hasła tymczasowego.
12. Opracowano i wdrożono standard dotyczący tworzenia bezpiecznych haseł użytkowników systemów informatycznych.

IV. Bezpieczeństwo Usługi

1. Elementy infrastruktury sieciowej służącej do przetwarzania danych osobowych zabezpiecza się przed utratą dostępności poprzez zastosowanie i zapewnienie usług serwisowych świadczonych przez producentów i dystrybutorów.
2. Przeprowadzane są okresowe niezależne testy podatności systemów informatycznych przetwarzających dane osobowe na zagrożenia.
3. Przeprowadzane jest okresowe skanowanie luk bezpieczeństwa na platformach i sieciach przetwarzających dane osobowe w celu zapewnienia zgodności z powszechnymi normami bezpieczeństwa związanymi konkretnie z wzmocnieniem systemu.
4. W wyniku testów penetracji, skanowania podatności na atak oraz oceny zgodności, prowadzony jest okresowo program naprawczy w podejściu opartym o ryzyko w celu wykorzystania uzyskanych wniosków.
5. Opracowano i zapewniono program szkoleń z zakresu zasad bezpiecznego wytwarzania oprogramowania.
6. Opracowano i zapewniono program testów bezpieczeństwa oprogramowania.
7. Opracowano zasady wyboru podwykonawców i dostawców gwarantujące zapewnienie odpowiedniego poziomu bezpieczeństwa technicznego i organizacyjnego świadczonych usług i realizowanych zadań.
8. Opracowano standardy i mechanizmy kontroli podwykonawców i dostawców usług oraz zagwarantowano ich realizację.

V. Zarządzanie zmianą i incydentami

1. Opracowano i wdrożono zasady zarzadzania zmianą w zakresie zatwierdzania, klasyfikacji i testowania planu back-out oraz rozdzielenie obowiązków pomiędzy wniosek, zatwierdzenie a wdrożenie.
2. Opracowano i wdrożono standard bezpiecznego wytwarzania oprogramowania.
3. Wdrożono procedury zarządzania i reagowania na incydenty naruszenia bezpieczeństwa, które umożliwiają wykrywanie, badanie, reagowanie, łagodzenie skutków i powiadamianie o zdarzeniach, które obejmują zagrożenie dla poufności, integralności i/lub dostępności do danych osobowych. Procedury reagowania i zarządzania są udokumentowane, sprawdzone i przynajmniej raz do roku podlegają przeglądom.

VI. Ochrona prywatności

1. Opracowano i wdrożono standard dotyczący analizy ryzyka naruszenia praw podstawowych i wolności osób których dane dotyczą oraz utraty poufności, dostępności i integralności danych osobowych na każdym etapie cyklu życia produktu.
2. Opracowano standard dotyczący zachowania zasady ochrony prywatności w fazie projektowania oprogramowania.
3. Opracowano standard dotyczący zachowania zasady ochrony prywatności w ustawieniach domyślnych w fazie projektowania oprogramowania.

B. Techniczne środki bezpieczeństwa.

I. Bezpieczeństwo obszaru przetwarzania

1. Ustalono minimalny zakres stosowania technicznych środków bezpieczeństwa w celu zapewnienia bezpieczeństwa danych osobowych. Rodzaj i zakres stosowanych dodatkowych technicznych środków bezpieczeństwa ustalany jest indywidualnie w zależności od zidentyfikowanych zagrożeń, wymaganego stopnia ochrony i możliwości technicznych.
2. Budynki i obszary, w których znajdują się pomieszczenia i ich części służące do przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych poprzez zastosowanie systemów kontroli dostępu, systemu sygnalizacji włamania i napadu, systemu dozoru realizowanego przez pracowników ochrony fizycznej, zamków mechanicznych lub szyfrowych.
3. Budynki i obszary, w których znajdują się pomieszczenia i ich części służące do przetwarzania danych zabezpiecza się przed pożarem poprzez zastosowanie drzwi o podwyższonej klasie odporności na ogień.
4. Budynki i obszary, w których znajdują się pomieszczenia i ich części służące do przetwarzania danych zabezpiecza się przed zniszczeniem na skutek pożaru lub zalania poprzez zastosowanie systemu alarmu pożarowego oraz systemu sygnalizacji włamania i napadu.
5. Budynki i obszary, w których znajdują się pomieszczenia i ich części służące do przetwarzania danych zabezpiecza się w celu monitorowania oraz identyfikowania zagrożeń i zdarzeń niepożądanych przez zastosowanie systemu telewizji przemysłowej.

II. Bezpieczeństwo transmisji danych

1. Dane osobowe przekazywane drogą teletransmisji zabezpiecza się przed utratą poufności i integralności przy pomocy kryptograficznych środków ochrony danych osobowych (szyfrowanie danych w tranzycie).

2. Dane osobowe przekazywane drogą teletransmisji zabezpiecza się przed utratą poufności poprzez zastosowanie segmentacji sieci teleinformatycznych (segmentacja sieci).
3. Klucze szyfrujące służące do zabezpieczenia teletransmisji danych przechowywane są w bezpiecznym miejscu z zarządzaniem dostępem do nich oraz z wykazaną możliwością odtwarzania klucza.

III. Bezpieczeństwo nośników danych

1. Dane osobowe przechowywane na nośnikach danych w stanie spoczynku zabezpiecza się przed utratą poufności i integralności przy pomocy kryptograficznych środków ochrony danych osobowych. (szyfrowanie danych w spoczynku)
2. Dane osobowe przechowywane na nośnikach danych zabezpiecza się przed utratą poufności poprzez zastosowanie fizycznej lub logicznej separacji danych. (separacja danych)
3. Dane osobowe przechowywane na nośnikach danych zabezpiecza się przed utratą dostępności i integralności poprzez zastosowanie mechanizmów tworzących kopie danych w czasie rzeczywistym. (replikacja danych)
4. Dane osobowe przechowywane na nośnikach danych zabezpiecza się przed utratą dostępności i integralności poprzez zastosowanie mechanizmów tworzących przyrostowe lub całościowe kopie bezpieczeństwa danych w ustalonym interwale czasowym. (backup danych)
5. Dane osobowe przechowywane na nośnikach danych zabezpiecza się przed utratą dostępności poprzez zastosowanie mechanizmów i procedur przywracania danych, przełączania źródeł danych oraz odtwarzania kopii bezpieczeństwa danych.
6. Nośniki danych (dyski twarde) służące do przetwarzania danych osobowych, przed zainstalowaniem w urządzeniu, zabezpiecza się przed dostępem osób nieuprawnionych poprzez ograniczenie i kontrolę dostępu realizowaną za pomocą szaf pancernych i sejfów.
7. Nośniki danych (dyski twarde) służące do przetwarzania danych osobowych zabezpiecza się przed utratą poufności danych przez zastosowanie wbudowanych procedur kryptograficznej ochrony danych. (kryptograficzna ochrona nośników danych)
8. Nośniki danych (dyski twarde) służące do przetwarzania danych osobowych zabezpiecza się przed utratą dostępności poprzez zastosowanie systemów automatycznego monitoringu działania, wykorzystania pojemności i czasu dostępności.
9. Nośniki danych służące do przetwarzania danych osobowych zabezpiecza się przed niedozwolonym wykorzystaniem poprzez zastosowanie procedur użycia i konfiguracji elementów infrastruktury informatycznej (zarządzanie konfiguracją).
10. Nośniki danych służące do przetwarzania danych osobowych przeznaczone do ponownego wykorzystania zabezpiecza się przed ujawnieniem danych osobie nieuprawnionej lub systemowi informatycznemu poprzez zastosowanie bezpiecznych metod usuwania danych.
11. Nośniki danych służące do przetwarzania danych osobowych przeznaczone do likwidacji zabezpiecza się przed ponownym wykorzystaniem poprzez trwałe i celowe mechaniczne uszkodzenie.

IV. Bezpieczeństwo baz danych

1. Dane osobowe przechowywane w bazach danych zabezpiecza się przed utratą integralności poprzez zastosowanie reguł spójności w zakresie semantycznym (definicja typu danych), zakresie encji (definicja kluczy podstawowych) oraz w zakresie referencyjnym (definicja kluczy obcych).
2. Dane osobowe zabezpiecza się przed utratą rozliczalności poprzez zastosowanie rozwiązań pozwalających przypisać określone działania konkretnej osobie lub systemowi informatycznemu.

V. Bezpieczeństwo infrastruktury informatycznej

1. Dane osobowe zabezpiecza się przed utratą poufności za pomocą bezpiecznych metod uwierzytelniania dostępu dla osób i systemów informatycznych.
2. Dane osobowe zabezpiecza się przed utratą poufności i dostępności za pomocą monitorowania poprawności działania oraz sposobu użycia bezpiecznych metod uwierzytelniania dostępu dla osób i systemów informatycznych.
3. Dane osobowe zabezpiecza się przed utratą dostępności poprzez zastosowanie dodatkowych, zapasowych i awaryjnych źródeł zasilania infrastruktury informatycznej służącej do przetwarzania danych osobowych.
4. Elementy infrastruktury informatycznej służącej do przetwarzania danych osobowych (komputery, serwery, urządzenia sieciowe) zabezpiecza się przed dostępem osób nieuprawnionych oraz systemów informatycznych przez zastosowanie bezpiecznych metod uwierzytelniania dostępu.
5. Elementy infrastruktury informatycznej służącej do przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych, systemów informatycznych oraz utratą dostępności poprzez monitorowanie aktualności systemu operacyjnego i zainstalowanego oprogramowania.
6. Elementy infrastruktury informatycznej służącej do przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych, systemów informatycznych oraz utratą dostępności poprzez zastosowanie oprogramowania typu Firewall, Intrusion Detection Systems, Intrusion Prevention Systems, Anty DDOS.
7. Elementy infrastruktury informatycznej służącej do przetwarzania danych osobowych zabezpiecza się przed utratą dostępności poprzez zastosowanie zwielokrotnienia, wirtualizacji i automatycznych procedur skalowania.
8. Elementy infrastruktury informatycznej służącej do przetwarzania danych osobowych zabezpiecza się przed utratą dostępności poprzez zastosowanie

automatycznych procesów monitorowania dostępności, obciążenia i wydajności.

9. Elementy infrastruktury informatycznej służącej do przetwarzania danych osobowych zabezpiecza się przed utratą dostępności poprzez zastosowanie zapasowych źródeł zasilania oraz automatycznych procedur zmiany źródła zasilania.

Załącznik nr 3 – Lista podwykonawców Firma

Podczas świadczenia Usługi, Firma korzysta ze wsparcia spółek z grupy przedsiębiorstw Firma oraz zewnętrznych podwykonawców. Podwykonawcy wskazani poniżej świadczą usługi obejmujące niektóre funkcjonalności Usługi (webinary), usługi hostingu i kolokacji, wsparcia w obsłudze Klienta, a także usługi związane ze śledzeniem incydentów bezpieczeństwa, reagowaniem na nie, diagnozowaniem i rozwiązywaniem problemów w Usłudze.

Firma Podwykonawcy	Siedziba
XXX	Polska
YYY	Polska
ZZZ	Francja