Załącznik nr 2 do Regulaminu

Umowa powierzenia przetwarzania danych osobowych

§ 1.
Definicje

1. **Procesor –** Usługodawca w znaczeniu nadanym temu pojęciu w Regulaminie.
2. **ADO –** Usługobiorca w znaczeniu nadanym temu pojęciu w Regulaminie.
3. **Dane** – dane osobowe powierzone Procesorowi do przetwarzania przez ADO w związku z Umową podstawową.
4. **Kolejny przetwarzający** – kolejny podmiot przetwarzający, z usług którego korzysta Procesor w związku z realizacją Umowy podstawowej.
5. **Regulamin** – regulamin usługi, w ramach której Procesor udostępnia Abonentowi oprogramowanie służące do obsługi kancelarii prawnych oraz kancelarii doradcy restrukturyzacyjnego.
6. **RODO -** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („RODO").
7. **Umowa podstawowa** – umowa wraz z Regulaminem będąca w związku z Usługą, o której mowa w Regulaminie, która to umowa jest podstawą powierzenia Danych.

§ 2.
Postanowienia wstępne

1. W związku z zawarciem przez Strony Umowy podstawowej, Strony zawierają Umowę powierzenia przetwarzania Danych.
2. ADO powierza do przetwarzania Dane, w stosunku do których pełni rolę administratora danych osobowych w rozumieniu RODO, a Procesor zobowiązuje się do ich przetwarzania w granicach określonych Umową oraz powszechnie obowiązującymi przepisami prawa.
3. Każde przetwarzanie Danych przez Procesora odbywa się wyłącznie na udokumentowane polecenia ADO, w szczególności zawarte w Umowie podstawowej, a także wyrażone przez zamówienie kolejnych usług.
4. Dane przetwarzane są celu realizacji Umowy podstawowej i w zakresie niezbędnym do jej prawidłowego wykonania.
5. Niniejsza Umowa zastępuje wszelkie wcześniejsze umowy, ustalenia i porozumienia w tym zakresie.
6. ADO oświadcza i zapewnia, że posiada podstawy prawne przetwarzania Danych, a powierzenie Procesorowi Danych do przetwarzania nie naruszy praw i wolności podmiotów tych danych, a także przepisów prawa (w szczególności RODO).
7. Dane udostępniane będą Procesorowi wyłącznie w celu realizacji Umowy podstawowej.
8. ADO poinformuje Procesora o wszelkich działaniach właściwych organów administracji publicznej, związanych z przetwarzaniem Danych przez ADO.
9. Dostęp do Danych będą miały wyłącznie osoby upoważnione przez Procesora do przetwarzania danych, zobowiązane do prawidłowej ochrony tych Danych – zgodnie z wewnętrznymi procedurami bezpieczeństwa Procesora oraz przepisami RODO, a także zobowiązane do zachowania Danych w tajemnicy lub podlegające prawnemu obowiązkowi dochowania takiej tajemnicy.
10. Procesor podejmuje wszelkie środki wymagane przez właściwe przepisy prawa, zwłaszcza przez art. 32 RODO, zgodnie z którym Procesor wdraża odpowiednie środki techniczne oraz organizacyjne uwzględniając stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.
11. Przetwarzanie Danych odbywać się będzie w okresie obowiązywania Umowy podstawowej.
12. Poprzez zawarcie Umowy Usługobiorca poleca przetwarzanie Danych Usługodawcy, a także każdej osobie działającej z upoważnienia Usługodawcy mającej dostęp do Danych osobowych, co stanowi udokumentowane polecenie w rozumieniu art. 28 ust. 3 lit. a w zw. z art. 29 RODO.
13. Procesor posiada certyfikat zgodności z normą bezpieczeństwa ISO 27001.

§ 3.
Dane

1. Usługodawca może przetwarzać dane osobowe powierzone mu do przetwarzania przez Usługobiorcę w celu realizacji Umowy i w zakresie do tego niezbędnym, co obejmuje w szczególności dane osobowe zawarte w bazie danych Programu, Serwisu. Niektóre kategorie tych danych określone są poprzez funkcjonalności lub pola dostępne w Programie, Serwisie i należą do nich między innymi:
   - imiona, nazwiska, dane kontaktowe i dane identyfikacyjne osób fizycznych będących klientami Usługobiorcy oraz innych osób, których dane Usługobiorca wprowadził do Programu, Serwisu;
   - dane finansowe, w tym dane dot. płatności, numerów rachunków bankowych, kart kredytowych, etc.

   Nadto, z uwagi na przeznaczenie Programu jako wspierającego prowadzenie spraw prowadzonych przez doradcę restrukturyzacyjnego albo przez prawnika w ramach kancelarii, w Programie przetwarzane mogą być również dane osobowe identyfikacyjne (zawierające numery NIP, PESEL, itp.), a także dane należące do szczególnych kategorii (określane w RODO mianem „danych wrażliwych"), takie jak dane dotyczące karalności, stanu zdrowia, orientacji seksualnej, wyznania, pochodzenia, itp. Podkreśla się jednak, że każdorazowo to wyłącznie Usługobiorca decyduje o zakresie i kategoriach danych osobowych wprowadzanych przez Niego do Programu i tym samym objętych powierzeniem, z zastrzeżeniem wyjątków wynikających z Umowy, a Usługodawca zaznacza i zastrzega, że dane te:
   - powinny być ograniczone do minimum zgodnie z zasadą minimalizacji przetwarzania danych osobowych określoną w RODO, i z tego względu winny być w miarę możliwości poddane przez Usługobiorcę selekcji;
   - ich wprowadzenie do Programu, Serwisu nie może stanowić czynu naruszającego bezwzględnie obowiązujące przepisy prawa;
   - mogą być wprowadzane tylko w zgodzie z przeznaczeniem i funkcjonalnościami Programu.
2. Kategorie osób, których dane osobowe mogą być przetwarzane w ramach Programu i które w związku z tym objęte są powierzeniem ich przetwarzania Usługodawcy, określa się następująco: klienci Usługobiorcy; pracownicy, zleceniobiorcy, wspólnicy, praktykanci, współpracownicy klientów Usługobiorcy; inne osoby fizyczne, których dane osobowe Usługobiorca wprowadzi do Programu; przedstawiciele organów publicznych uczestniczących w postępowaniu prowadzonym przez doradcę restrukturyzacyjnego albo prawnika.
3. Przetwarzanie powierzonych Danych obejmuje następujące czynności przetwarzania: utrwalanie, organizowanie, porządkowanie, przechowywanie, pobieranie, przeglądanie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

§ 4.
Wsparcie i audyty

1. Uwzględniając charakter przetwarzania Procesor zapewni wsparcie ADO („**Wsparcie**"). W ramach Wsparcia Procesor w miarę możliwości pomoże ADO, poprzez odpowiednie środki techniczne i organizacyjne, wywiązać się z obowiązku odpowiadania na żądania osób, których Dane dotyczą, w zakresie wykonywania ich praw, określonych w rozdziale III RODO - jeśli w danym przypadku ciążą one na ADO, a także pomoże ADO wywiązać się z ciążących na ADO obowiązków określonych w art. 32 – 36 RODO – z uwzględnieniem dostępnych mu informacji.
2. Procesor zobowiązany jest do udostępnienia ADO wszelkich informacji niezbędnych do wykazania obowiązków określonych w art. 28 RODO oraz umożliwienia ADO lub upoważnionemu przez ADO audytorowi przeprowadzenia audytów, w tym inspekcji („**Audyt**") i przyczynienia się do nich.
3. W przypadku, gdy wydane przez ADO polecenia w związku z poprzednim ustępem, w ocenie Procesora stanowią naruszenie przepisów RODO lub innych przepisów prawa Unii lub prawa polskiego – Procesor niezwłocznie poinformuje o tym ADO.
4. Procesor może odmówić przekazania ADO informacji objętych tajemnicą prawnie chronioną, w tym tajemnicą przedsiębiorstwa Procesora lub podmiotów trzecich, a także informacji stanowiących dane osobowe nie będące Danymi, jeśli informacje te mogą zostać zastąpione innymi informacjami (w tym oświadczeniami Procesora), zaś w przypadku gdy nie będzie to możliwe – informacje te zostaną udostępnione ADO (lub wyznaczonym przez niego osobom) wyłącznie w siedzibie Procesora, po

uprzednim zawarciu przez ADO i wszystkie osoby działające na rzecz ADO, przedstawionej przez Procesora umowy zobowiązującej do należytej ochrony tych informacji.

5. Przeprowadzenie Audytu jest możliwe po uprzednim pisemnym poinformowaniu Procesora przez ADO o zamiarze jego przeprowadzenia z co najmniej trzydziestodniowym wyprzedzeniem, wraz ze wskazaniem listy osób zaangażowanych w przeprowadzenie Audytu po stronie ADO. Zawiadomienie powinno ponadto określać czas trwania Audytu oraz jego zakres.
6. W przypadku gdy Audyt nie jest bezpośrednio związany z działaniami uprawnionych organów administracji publicznej kierowanymi wobec ADO w związku z przetwarzaniem danych bądź stwierdzonym i udokumentowanym naruszeniem przetwarzania Danych przez Procesora – łączny czas trwania prowadzonych przez ADO Audytów nie może przekroczyć trzech dni w roku kalendarzowym.
7. Audyt może być przeprowadzony wyłącznie po uprzednim zawarciu przez ADO i wszystkie osoby działające na rzecz ADO, przedstawionej przez Procesora umowy zobowiązującej do należytej ochrony wszelkich informacji uzyskanych w związku z Audytem.
8. Audyt przeprowadzany jest w godzinach pracy Procesora i nie może w żaden sposób zakłócać ani negatywnie wpływać na bieżącą działalność Procesora.
9. Audyty przeprowadzane są na koszt ADO. Koszty sprawowania Wsparcia oraz nadzoru nad Procesorem przez ADO obciążają wyłącznie ADO. Za koszty wsparcia bądź nadzoru uznaje się w szczególności koszty ponoszone przez Procesora w związku z dokonywaniem kontroli, audytów, czy przygotowania dokumentów, udzielenia informacji lub pomocy ADO. W przypadku gdy koszty, o których mowa w niniejszym ustępie zostały poniesione przez Procesora – ADO niezwłocznie zwróci je Procesorowi. Stawka godzinowa za obsługę Audytu przez Procesora wynosi 350 zł netto/godzina/osoba.
10. Procesor współpracuje z organami właściwymi do spraw ochrony danych osobowych, w zakresie wykonywanych przez nie zadań.
11. Jeśli z przepisów prawa lub niniejszej Umowy nie wynika inny termin – wykonywanie czynności przez Procesora w związku z Umową, w tym udzielanie wszelkich informacji, będzie następować niezwłocznie, nie później niż w terminie 30 dni od otrzymania stosownego żądania.

§ 5.
Kolejny przetwarzający

1. Procesor może korzystać z usług Kolejnego przetwarzającego tylko za uprzednią szczegółową zgodą lub ogólną pisemną zgodą ADO.
2. Procesor nałoży na każdego Kolejnego przetwarzającego, w szczególności za pośrednictwem umowy, te same obowiązki ochrony Danych jak wynikające z Umowy, w szczególności obowiązek wdrożenia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom RODO.
3. W przypadku niewywiązania się przez Kolejnego przetwarzającego z ciążących na nim obowiązków w stosunku do Danych, pełna odpowiedzialność wobec ADO za spełnienie obowiązków przez Kolejnego przetwarzającego spoczywa na Procesorze.
4. ADO wyraża zgodę na korzystanie przez Procesora z Kolejnych przetwarzających wskazanych w załączniku nr 5 do Umowy podstawowej. Zmiana załącznika nie stanowi zmiany Umowy i postanowienia ust. 3-4 niniejszego paragrafu stosuje się do niej odpowiednio.
5. Powierzenie przetwarzania Danych Kolejnym przetwarzającym niewskazanym w załączniku nr 5 wymaga uprzedniego zgłoszenia tego faktu ADO – w celu umożliwienia mu sprzeciwu. Sprzeciw może zostać dokonany nie później niż na siedem dni przed powierzeniem Danych Kolejnemu przetwarzającemu. Zgłoszenie zamiaru powierzenia przez Procesora może zostać dokonane w szczególności w formie elektronicznej.
6. W przypadku braku sprzeciwu przyjmuje się, że ADO wyraził zgodę na korzystanie z Kolejnego przetwarzającego.
7. W przypadku zgłoszenia sprzeciwu przez ADO, Procesor nie może powierzyć danych Kolejnemu przetwarzającemu, którego sprzeciw dotyczy. Procesor będzie uprawniony do rozwiązania w takim przypadku Umowy podstawowej, ze skutkiem natychmiastowym, a ADO nie będzie przysługiwać z tego tytułu jakiekolwiek odszkodowanie.

§ 6

Naruszenie danych

1. Procesor jest obowiązany powiadomić ADO bez zbędnej zwłoki, jednak nie później niż w terminie 48 godzin od powzięcia wiedzy, o każdym przypadku wystąpienia lub podejrzenia wystąpienia incydentu bezpieczeństwa informacji związanego z powierzonymi Procesorowi Danymi, a w szczególności stanowiącym naruszenie ochrony danych osobowych.
2. Obowiązek Procesora, o którym mowa w ust. 1 powyżej nie jest i nie będzie interpretowany jako potwierdzenie przez Procesora wobec osób, których dane dotyczą, wystąpienia naruszenia ochrony danych osobowych.

§ 7.
Postanowienia Końcowe

1. Umowa ulega rozwiązaniu z chwilą rozwiązania Umowy podstawowej.
2. Procesor, po zakończeniu świadczenia usług związanych z przetwarzaniem Danych na rzecz ADO, w szczególności w przypadku rozwiązania niniejszej Umowy lub Umowy podstawowej, w zależności od decyzji ADO:
   a) usuwa Dane;
   b) zwraca ADO wszelkie Dane oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub polskie przepisy prawa powszechnie obowiązującego nakazują przechowywanie danych osobowych.
3. W przypadku wypowiedzenia Umowy podstawowej ADO powinien przekazać Procesorowi decyzję, o której mowa w poprzednim ustępie, nie później niż w ostatnim dniu obowiązywania Umowy. W przypadku braku przekazania takiej decyzji w tym terminie – przyjmuje się, że ADO nakazał Procesorowi usunięcie Danych i wszelkie związane z tym konsekwencje obciążają wyłącznie ADO.
4. W sprawach nieuregulowanych, w tym w zakresie zmiany Umowy, zastosowania mają postanowienia Umowy podstawowej.

Załącznik nr 3 do Regulaminu

Lista Kolejnych przetwarzających
ADO wyraża zgodę na powierzenie Danych przez Procesora następującym Kolejnym przetwarzającym:

1. Microsoft Corporation. One Microsoft Way. Redmond, Washington 98052-6399.

2. Amazon Web Services, 38 Avenue John F. Kennedy, L-1855, Luxembourg

3. Mixpanel, Inc., Mixpanel International, Inc., Mixpanel S.L., Mixpanel UK Limited, and Mixpanel APAC Pte. Ltd.

Załącznik nr 4 do Regulaminu

Minimalne standardy bezpieczeństwa

AWS, z którego usług serwerowych korzysta Usługodawca zapewnia wysoki standard bezpieczeństwa przetwarzania danych osobowych, spełniając m.in. następujące wymogi bezpieczeństwa:
- systemy szyfrowania połączeń internetowych i szyfrowania AES256 bazy danych (SSL, TLS, IPSec);
- fizyczne i cyfrowe środki zabezpieczeń technicznych serwerów i innych miejsc, w których przetwarzane są dane osobowe;
- zapewnia całkowitą kontrolę przepływu osób i pojazdów na terenie całego obszaru administracyjnego;
- obiekty podzielone są na strefy bezpieczeństwa a przemieszczanie w strefach wspierane jest Systemem Kontroli Dostępu zapewniającym całkowitą rozliczalność i kontrolę uprawnień dostępu;
- obiekty monitorowane są przez System Telewizji Dozorowej CCTV;
- obiekty posiadają System Sygnalizacji Włamania i Napadu;
- sygnały z systemów bezpieczeństwa są odbierane i monitorowane w trybie ciągłym (w tym dotyczące infrastruktury sieciowej, zasilania energetycznego i bezpieczeństwa serwerowni, obiektów administracyjno-biurowych i innych ważnych zasobów wykorzystywanych do świadczenia usług) – systemy te są regularnie testowane;
- stosuje politykę tworzenia kopii zapasowych (politykę backup),
- systemy informatyczne i aplikacje wykorzystywane i służące do przetwarzania danych osobowych są regularnie aktualizowane, weryfikowane pod kątem podatności oraz zabezpieczone przez systemy antywirusowe,
- stosuje ochronę przed nieuprawnionym dostępem do systemów i sieci przy pomocy systemów firewall,
- stosuje systemy monitorujące ruch sieciowy – wykryte anomalie są logowane i raportowane,
- świadczy na rzecz Usługodawcy następujące usługi: RDS (bazy danych), EC2 (wirtualne serwery), Lightsail (strona WWW), S3 (przechowywanie dokumentów), S3 Glacier (backupy), S3-Buckets;

- posiada certyfikat ISO 27001/9001;
- posiada certyfikat ISO 27017/27018;
- posiada certyfikat zgodności z CISPE Code of Conduct – kodeks dobrych praktyk dla usługodawców usług chmurowych potwierdzający zgodność z wymogami RODO.