Załącznik nr 2 do Regulaminu Platformy Ragnar Shield

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

(Data Processing Agreement - DPA)

Niniejsza umowa powierzenia przetwarzania danych osobowych („**DPA**") stanowi Załącznik nr 2 do Regulaminu Platformy Ragnar Shield i określa zasady przetwarzania danych osobowych powierzonych Operatorowi w związku z korzystaniem z Platformy, API, świadczeniem Usług, wykonywaniem Umowy albo Umowy Partnerskiej. DPA ma zastosowanie odpowiednio do Klienta albo Partnera jako podmiotu powierzającego Operatorowi przetwarzanie danych osobowych.

Na potrzeby DPA przez „**Podmiot Powierzający**" rozumie się Klienta albo Partnera, który powierza Operatorowi przetwarzanie danych osobowych. Podmiot Powierzający może działać jako administrator danych osobowych albo jako podmiot przetwarzający powierzający Operatorowi dalsze przetwarzanie danych osobowych. Operator działa odpowiednio jako podmiot przetwarzający albo dalszy podmiot przetwarzający w rozumieniu art. 28 RODO.

§ 1. Przedmiot i zakres powierzenia

1. Operator przetwarza dane osobowe wyłącznie na udokumentowane polecenie Podmiotu Powierzającego, w zakresie, celu i przez czas niezbędny do świadczenia Usług, obsługi Platformy lub API, wykonywania Umowy albo Umowy Partnerskiej oraz realizacji obowiązków określonych w Regulaminie, Order Form lub innej dokumentacji zaakceptowanej przez Strony.
2. Przetwarzanie może dotyczyć w szczególności Usług obejmujących skanowanie i monitoring infrastruktury IT, testy penetracyjne, analizę OSINT, ocenę zgodności regulacyjnej, skanowanie bezpieczeństwa kodu aplikacji oraz obsługę Raportów generowanych w ramach Platformy.

§ 2. Kategorie danych i osób

1. Kategorie osób, których dane mogą być przetwarzane w ramach DPA, obejmują w szczególności: Klientów, Partnerów, Klientów Końcowych, osoby reprezentujące te podmioty, osoby kontaktowe, Użytkowników, Użytkowników Klientów Końcowych,

pracowników, współpracowników, członków organów, klientów lub kontrahentów Klienta, Partnera albo Klienta Końcowego, a także osoby wskazane do analizy OSINT lub objęte inną Usługą, o ile Podmiot Powierzający posiada odpowiednią podstawę prawną do przekazania ich danych Operatorowi.

2. Kategorie danych osobowych mogą obejmować w szczególności dane identyfikacyjne, dane kontaktowe, dane dotyczące stanowiska, funkcji lub roli organizacyjnej, dane techniczne, adresy IP, logi, identyfikatory urządzeń, dane dotyczące konfiguracji systemów, dane publicznie dostępne w Internecie lub pozyskiwane w ramach analizy OSINT, dane zawarte w kodzie źródłowym, dokumentacji technicznej, opisach procesów, materiałach przekazanych do analizy oraz dane wynikające z Raportów.

3. Zakres powierzonych danych zależy każdorazowo od rodzaju Usługi zleconej przez Klienta, zakresu danych przekazanych Operatorowi oraz konfiguracji Platformy wykorzystywanej przez Klienta.

4. Charakter przetwarzania obejmuje zbieranie, utrwalanie, porządkowanie, przechowywanie, analizowanie, pobieranie, przeglądanie, dopasowywanie, udostępnianie Podmiotowi Powierzającemu, usuwanie i anonimizowanie danych w zakresie niezbędnym do świadczenia Usług. Celem przetwarzania jest wykonanie Usług, zapewnienie działania Platformy i API, obsługa Raportów, wsparcie techniczne, bezpieczeństwo, rozliczenia w zakresie dotyczącym powierzonych danych oraz wykonanie obowiązków określonych w DPA. Czas przetwarzania odpowiada okresowi świadczenia Usług oraz okresom retencji określonym w Regulaminie, Polityce Prywatności, Order Form lub udokumentowanych poleceniach Podmiotu Powierzającego.

§ 3. Obowiązki Operatora jako podmiotu przetwarzającego

1. Operator zobowiązuje się do:

1) przetwarzania danych osobowych wyłącznie na udokumentowane polecenie Podmiotu powierzającego, w zakresie i celu określonym w DPA, Regulaminie oraz ewentualnych dalszych instrukcjach Podmiotu powierzającego, chyba że obowiązek przetwarzania wynika z przepisów prawa; w takim przypadku Operator, przed rozpoczęciem takiego przetwarzania, informuje Podmiot powierzający o tym obowiązku prawnym, o ile prawo nie zakazuje udzielenia takiej informacji;

2) zapewnienia, że osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności albo podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
3) wdrożenia i utrzymywania odpowiednich środków technicznych i organizacyjnych wymaganych na podstawie art. 32 RODO, z uwzględnieniem charakteru, zakresu, kontekstu i celu przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych;
4) przestrzegania warunków korzystania z usług dalszych podmiotów przetwarzających, określonych w § 5 poniżej;
5) biorąc pod uwagę charakter przetwarzania oraz w zakresie, w jakim jest to możliwe, pomagania Podmiotowi powierzającemu poprzez odpowiednie środki techniczne i organizacyjne w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą;
6) pomagania Podmiotowi powierzającemu, z uwzględnieniem charakteru przetwarzania oraz informacji dostępnych Operatorowi, w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO;
7) po zakończeniu świadczenia Usług związanych z przetwarzaniem danych osobowych, w zależności od decyzji Podmiotu powierzającego, usunięcia albo zwrócenia Podmiotowi powierzającemu wszelkich danych osobowych oraz usunięcia ich istniejących kopii, chyba że przepisy prawa nakazują dalsze przechowywanie danych osobowych;
8) udostępniania Podmiotowi powierzającemu informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwienia Podmiotowi powierzającemu lub audytorowi upoważnionemu przez Podmiot powierzający przeprowadzania audytów, w tym inspekcji, na zasadach określonych w DPA;
9) niezwłocznego informowania Podmiotu powierzającego, jeżeli w ocenie Operatora wydane mu polecenie narusza RODO lub inne przepisy prawa,
10) Partner zobowiązuje się zapewnić, aby Klienci Końcowi, którzy zlecają analizę OSINT, dysponowali odpowiednią podstawą prawną przetwarzania danych oraz spełnili wobec osób objętych analizą obowiązki informacyjne wynikające z art. 13 lub art. 14 RODO, o ile obowiązki te znajdują zastosowanie. Operator może udostępnić Partnerowi wzór klauzuli informacyjnej art. 14 RODO dla osób objętych analizą OSINT, który Partner może przekazywać Klientom Końcowym jako materiał

pomocniczy. Partner zobowiązuje się nie przedstawiać tego wzoru jako indywidualnej porady prawnej ani gwarancji zgodności po stronie Operatora,

11) Partner zobowiązuje się do przeprowadzania, przed zarejestrowaniem Klienta Końcowego w Platformie albo przed rozpoczęciem oferowania mu Usług, weryfikacji Klienta Końcowego, osób go reprezentujących oraz - w rozsądnym i możliwym zakresie - jego beneficjentów rzeczywistych pod kątem list sankcyjnych, ograniczeń eksportowych, państw lub terytoriów wyłączonych oraz innych ograniczeń wskazanych przez Operatora. Weryfikacja obejmuje co najmniej listy sankcyjne Unii Europejskiej i Organizacji Narodów Zjednoczonych, a także OFAC lub inne listy, jeżeli ich stosowanie wynika z Order Form, wymogów Operatora, dostawców technologicznych albo przepisów prawa mających zastosowanie do Stron. Partner nie jest uprawniony do oferowania Usług Klientom Końcowym objętym sankcjami, prowadzącym działalność w państwach lub terytoriach wyłączonych przez Operatora, działającym na rzecz takich podmiotów albo takim, wobec których świadczenie Usług mogłoby powodować istotne ryzyko prawne, regulacyjne, bezpieczeństwa, sankcyjne lub reputacyjne dla Operatora. Operator jest uprawniony do odmowy realizacji Usługi, zawieszenia dostępu Klienta Końcowego do Usług, odmowy rejestracji Klienta Końcowego albo żądania zaprzestania obsługi danego Klienta Końcowego przez Partnera, jeżeli poweźmie uzasadnione wątpliwości co do zgodności takiej obsługi z przepisami sankcyjnymi, ograniczeniami eksportowymi, wymogami bezpieczeństwa albo polityką zgodności Operatora.

1. Audyty, o których mowa powyżej, będą przeprowadzane po uprzednim uzgodnieniu przez Strony terminu i zakresu audytu, w sposób niezakłócający normalnej działalności Operatora oraz z poszanowaniem poufności, tajemnicy przedsiębiorstwa, bezpieczeństwa systemów informatycznych oraz praw i interesów innych klientów Operatora. Podmiot powierzający jest uprawniony do przeprowadzenia audytu nie częściej niż raz w roku, chyba że częstszy audyt jest uzasadniony wystąpieniem naruszenia ochrony danych osobowych, żądaniem właściwego organu nadzorczego lub inną istotną przyczyną związaną z bezpieczeństwem przetwarzania danych osobowych. Audyt może być przeprowadzony przez Podmiot powierzający albo niezależnego audytora upoważnionego przez Podmiot powierzający, pod warunkiem zobowiązania takiego audytora do zachowania poufności. Operator może odmówić udziału w audycie osobie lub podmiotowi, który prowadzi działalność konkurencyjną

wobec Operatora albo którego udział mógłby stwarzać ryzyko naruszenia tajemnicy przedsiębiorstwa, bezpieczeństwa systemów lub praw osób trzecich.

2. W pierwszej kolejności Operator może wykazać spełnienie obowiązków wynikających z art. 28 RODO przez udostępnienie Podmiotowi powierzającemu odpowiednich informacji, dokumentów, certyfikatów, raportów z audytów, opisów środków technicznych i organizacyjnych lub innych materiałów potwierdzających zgodność przetwarzania z DPA i RODO. Audyt w formie inspekcji w siedzibie Operatora lub bezpośredniego dostępu do systemów Operatora może zostać przeprowadzony wyłącznie wtedy, gdy przedstawione informacje okażą się niewystarczające do wykazania zgodności albo gdy wymagają tego przepisy prawa, organ nadzorczy lub istotne okoliczności związane z bezpieczeństwem danych osobowych.

§ 4. Obowiązki Podmiotu powierzającego jako administratora

1. Podmiot powierzający oświadcza, że w odniesieniu do danych osobowych powierzanych Operatorowi do przetwarzania działa jako administrator danych osobowych w rozumieniu RODO oraz że posiada odpowiednią podstawę prawną do ich przetwarzania, w tym do powierzenia ich przetwarzania Operatorowi w zakresie i celu określonym w DPA, Regulaminie oraz zamówionych Usługach.

2. Podmiot powierzający ponosi odpowiedzialność za zgodność z prawem pozyskania danych osobowych, ustalenie właściwej podstawy prawnej ich przetwarzania, prawidłowe określenie zakresu danych powierzanych Operatorowi oraz spełnienie wobec osób, których dane dotyczą, obowiązków informacyjnych wynikających z art. 13 i 14 RODO.

3. Podmiot powierzający zobowiązuje się nie powierzać Operatorowi danych osobowych w zakresie szerszym niż niezbędny do korzystania z Usług ani danych, których przetwarzanie byłoby sprzeczne z przepisami prawa, Regulaminem lub DPA.

4. Operator nie ponosi odpowiedzialności za naruszenia przepisów o ochronie danych osobowych wynikające z braku lub wadliwości podstawy prawnej przetwarzania po stronie Klienta, niespełnienia przez Klienta obowiązków informacyjnych albo powierzenia Operatorowi danych osobowych w zakresie niezgodnym z DPA, Regulaminem lub przepisami prawa.

§ 5. Subprocesorzy

1. Aktualna lista Subprocesorów jest udostępniana w panelu Klienta lub Partnera. Operator zapewnia, że lista jest aktualizowana przed dodaniem lub zastąpieniem Subprocesora.
2. Podmiot Powierzający wyraża ogólną zgodę na korzystanie przez Operatora z dalszych podmiotów przetwarzających w zakresie niezbędnym do świadczenia Usług, obsługi Platformy, API, infrastruktury technicznej, płatności, komunikacji, usług AI, analityki, testów penetracyjnych oraz innych funkcjonalności opisanych w Regulaminie lub Polityce Prywatności. Aktualna lista dalszych podmiotów przetwarzających, wraz z informacją o celu przetwarzania, lokalizacji przetwarzania oraz ewentualnych transferach danych poza EOG, jest udostępniana w Polityce Prywatności lub panelu Klienta albo Partnera.
3. Operator informuje Podmiot Powierzający o planowanej zmianie dalszego podmiotu przetwarzającego z co najmniej 30-dniowym wyprzedzeniem, umożliwiając wniesienie uzasadnionego sprzeciwu. W przypadku braku możliwości usunięcia zastrzeżeń Podmiot Powierzający jest uprawniony do wypowiedzenia Umowy albo Umowy Partnerskiej w zakresie, w jakim dalsze korzystanie z Usług wymagałoby przetwarzania danych przez zakwestionowanego dalszego podmiotu przetwarzającego.
4. W przypadku wniesienia sprzeciwu Strony podejmą w dobrej wierze działania zmierzające do wyjaśnienia zastrzeżeń Klienta. Jeżeli zastrzeżenia nie zostaną usunięte, a korzystanie z danego Subprocesora jest niezbędne do dalszego świadczenia Usług, Klient jest uprawniony do wypowiedzenia Umowy w zakresie usług, których dotyczy sprzeciw.
5. Operator zapewnia, że powierzenie przetwarzania danych osobowych Subprocesorowi następuje na podstawie umowy zobowiązującej Subprocesora do stosowania odpowiednich środków technicznych i organizacyjnych oraz do realizacji obowiązków ochrony danych osobowych w zakresie nie mniej rygorystycznym niż wynikający z DPA.
6. Wniesienie sprzeciwu nie może prowadzić do obowiązku świadczenia przez Operatora Usług bez udziału Subprocesora, jeżeli udział takiego Subprocesora jest konieczny ze względów technicznych, organizacyjnych lub bezpieczeństwa.

§ 6. Transfer danych poza EOG

Operator nie przekazuje danych osobowych poza Europejski Obszar Gospodarczy, chyba że jest to niezbędne do świadczenia Usług lub korzystania z podwykonawców, oraz wyłącznie pod warunkiem zastosowania odpowiednich mechanizmów legalizujących transfer danych zgodnie z Rozdziałem V RODO. Mechanizmy te mogą obejmować w szczególności decyzję Komisji Europejskiej stwierdzającą odpowiedni stopień ochrony, standardowe klauzule umowne przyjęte przez Komisję Europejską lub inne prawnie dopuszczalne zabezpieczenia. Szczegółowe informacje dotyczące ewentualnych transferów danych poza EOG, w tym kategorii odbiorców, państw transferu oraz stosowanych zabezpieczeń, są udostępniane w Polityce Prywatności

§ 7. Naruszenie ochrony danych osobowych

Operator powiadamia Klienta o każdym naruszeniu ochrony danych osobowych dotyczącym danych powierzonych do przetwarzania bez zbędnej zwłoki, nie później jednak niż w terminie 48 godzin od powzięcia wiadomości o naruszeniu. Powiadomienie obejmuje informacje wymagane zgodnie z art. 33 ust. 3 RODO, w zakresie, w jakim są one dostępne Operatorowi na moment dokonania powiadomienia. Jeżeli przekazanie wszystkich informacji jednocześnie nie jest możliwe, Operator przekazuje je sukcesywnie, bez zbędnej zwłoki, w miarę ich ustalania.

§ 8. Czas trwania i rozwiązanie

1. DPA obowiązuje przez okres świadczenia Usług przez Operatora na rzecz Podmiotu Powierzającego oraz przez czas, w którym Operator przetwarza dane osobowe powierzone mu przez Podmiot Powierzający w związku z wykonywaniem Umowy, Umowy Partnerskiej, Regulaminu lub Order Form.
2. Po zakończeniu świadczenia Usług albo po zakończeniu przetwarzania danych osobowych na rzecz Podmiotu Powierzającego Operator, zgodnie z udokumentowanym poleceniem Podmiotu Powierzającego, usuwa albo zwraca powierzone dane osobowe oraz usuwa ich istniejące kopie, chyba że obowiązujące przepisy prawa nakazują dalsze przechowywanie danych.
3. W braku odrębnego polecenia Podmiotu Powierzającego Operator usuwa albo anonimizuje powierzone dane osobowe w terminie 30 dni od dnia zakończenia świadczenia Usług albo zakończenia przetwarzania, z zastrzeżeniem danych, których dalsze przechowywanie jest wymagane przez przepisy prawa albo niezbędne do ustalenia, dochodzenia lub obrony przed roszczeniami.

4. Postanowienia dotyczące poufności, bezpieczeństwa danych, współpracy Stron, odpowiedzialności oraz usunięcia lub zwrotu danych pozostają w mocy również po rozwiązaniu, wygaśnięciu albo zakończeniu obowiązywania DPA, w zakresie wynikającym z ich treści, charakteru lub przepisów prawa.