WEB3 Technology B.V.

DOKUMENT PROCESOWY

Polityka prywatności

CASP licencjonowany w Niderlandach | Zezwolenie AFM nr 41000022

Ramy regulacyjne

DORA (UE) 2022/2554 · MiCA (UE) 2023/1114 · RODO (UE) 2016/679

Kontrola dokumentu

Pole	Szczegóły
Tytuł dokumentu	Polityka prywatności
Właściciel dokumentu	Dyrektor ds. Ryzyka i Zgodności (CRCO) / Inspektor Ochrony Danych (IOD)
Zakres stosowania	Wszyscy Użytkownicy usług WEB3 Technology B.V. oraz Serwisu / Aplikacji
Podstawa regulacyjna	RODO (UE) 2016/679 · niderlandzka ustawa o telekomunikacji (Tw) · Rozporządzenie MiCA 2023/1114 · Rozporządzenie TFR 2023/1113 · Dyrektywa DAC8 2023/2226 · Wwft · DORA
Wersja	v.26_9.0
Data wejścia w życie	27.10.2026
Cykl przeglądu	Corocznie lub w przypadku istotnej zmiany regulacyjnej lub operacyjnej
Zatwierdzony przez	Organ zarządzający / CRCO
Klasyfikacja	Publiczny — informacja o ochronie prywatności
Spółka	„Spółka” oznacza WEB3 Technology B.V., spółkę z ograniczoną odpowiedzialnością (besloten vennootschap) utworzoną zgodnie z prawem niderlandzkim, z siedzibą pod adresem Prins Hendrikkade 21E, 1012 TL Amsterdam, Niderlandy, wpisaną do Izby Handlowej (KvK) pod numerem 95206604, posiadającą zezwolenie AFM na świadczenie usług w zakresie kryptoaktywów nr 41000022.

W WEB3 Technology B.V. dokładamy wszelkich starań, aby chronić bezpieczeństwo powierzonych nam informacji oraz zapewnić, by zasady regulujące ich przetwarzanie były przejrzyste i łatwe do zrozumienia.

Chcemy, aby osoby korzystające z naszych usług wiedziały, jakie dane osobowe zbieramy, w jakich celach je przetwarzamy oraz jakie prawa przysługują im na mocy obowiązujących przepisów o ochronie danych. Przestrzegamy zasad określonych w RODO oraz we właściwych krajowych przepisach dotyczących prywatności, a nasze działania związane z przetwarzaniem danych organizujemy w sposób zapewniający bezpieczeństwo, poufność i zgodność z prawem.

Zanim zaczniesz korzystać z naszych usług, zachęcamy do zapoznania się z niniejszą Polityką prywatności, która zawiera najważniejsze informacje dotyczące przetwarzania Twoich danych osobowych.

1. Definicje stosowane w niniejszej Polityce prywatności

Termin	Definicja
Administrator / WEB3 Technology / „my”	WEB3 Technology B.V., spółka zarejestrowana w Niderlandach, posiadająca zezwolenie AFM jako dostawca usług w zakresie kryptoaktywów (CASP), nr rejestracyjny 41000022, z siedzibą pod adresem Prins Hendrikkade 21E, Amsterdam, 1012TL, Niderlandy | numer LEI 724500YJVIN0Q94ZZG58 | KVK: 95206604.
Dane osobowe	Wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej w rozumieniu art. 4 pkt 1 RODO.
Polityka	Niniejsza Polityka prywatności.
Polityka plików cookie	Polityka plików cookie mająca zastosowanie do Serwisów
Regulamin	Regulamin WEB3 Technology jest dostępny w Serwisie
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.
Rynki kryptoaktywów (MiCA)	Jako licencjonowany CASP w rozumieniu MiCA podlegamy obowiązkom w zakresie prowadzenia dokumentacji, komunikacji z klientami, rozpatrywania reklamacji oraz sprawozdawczości, które wymagają przetwarzania danych osobowych. Jeżeli takie przetwarzanie jest wymagane przez MiCA, jego podstawą prawną jest art. 6 ust. 1 lit. c RODO (wypełnienie obowiązku prawnego).
EOG	Europejski Obszar Gospodarczy.
Serwis lub Serwisy	Usługi online prowadzone przez Administratora pod adresem www.rgltd.com
Użytkownik	Każda osoba fizyczna odwiedzająca Serwis lub korzystająca z jednej lub kilku usług dostępnych za pośrednictwem Serwisu, w tym – jeżeli z usług korzysta osoba prawna lub korzystanie następuje w jej imieniu – każda osoba fizyczna działająca jako upoważniony przedstawiciel, beneficjent rzeczywisty, członek zarządu lub inna osoba kontaktowa takiej osoby prawnej, której dane osobowe są przetwarzane w związku ze świadczeniem usług przez Administratora.
Podmiot przetwarzający	Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora, w rozumieniu art. 4 pkt 8 RODO.
Strona trzecia	Osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, Administrator, Podmiot przetwarzający oraz osoby, które – z upoważnienia Administratora lub Podmiotu przetwarzającego – mogą przetwarzać dane osobowe, w rozumieniu art. 4 pkt 10 RODO.
Rozporządzenie eIDAS	Rozporządzenie (UE) nr 910/2014, zmienione rozporządzeniem (UE) 2024/1183, regulujące identyfikację elektroniczną i usługi zaufania w UE.

Europejski eID	Środek identyfikacji elektronicznej wydany w ramach systemu notyfikowanego na podstawie Rozporządzenia eIDAS lub europejski portfel tożsamości cyfrowej (EUDI Wallet), za pomocą którego potwierdzasz swoją tożsamość.

Wszelkie inne terminy pisane w niniejszej Polityce wielką literą mają znaczenie nadane im w Regulaminie dostępnym w Serwisach

2. Kto przetwarza Twoje dane osobowe?

Administratorem Twoich danych osobowych jest **WEB3 Technology B.V.**, z siedzibą pod adresem Prins Hendrikkade 21E, 1012 TL Amsterdam, Niderlandy, wpisana do rejestru pod numerem 95206604.

2.1 Jak się z nami skontaktować

Możesz skontaktować się z nami jako Administratorem Twoich danych osobowych, wysyłając korespondencję na adres siedziby Spółki (Prins Hendrikkade 21E, 1012 TL Amsterdam, Niderlandy) lub na adres e-mail dostępny w naszych Serwisach.

W celu zwiększenia ochrony Twoich danych osobowych wyznaczyliśmy wewnętrznego Inspektora Ochrony Danych. Jest to osoba, z którą możesz się kontaktować, jeżeli masz pytania dotyczące sposobu przetwarzania Twoich danych, chcesz skorzystać ze swoich praw lub potrzebujesz wyjaśnień w jakichkolwiek innych sprawach związanych z przetwarzaniem Twoich danych osobowych.

W tym celu możesz wysłać wiadomość na adres e-mail dostępny w naszych Serwisach lub list zaadresowany w następujący sposób: Inspektor Ochrony Danych · WEB3 Technology B.V. · Prins Hendrikkade 21E · 1012 TL Amsterdam · Niderlandy.

3. Dane osobowe osób poniżej 18. roku życia

Nasze usługi są przeznaczone dla osób, które ukończyły 18 lat. Administrator nie przetwarza świadomie danych osobowych osób małoletnich. W ramach procesu rejestracji (onboardingu) wiek każdego Użytkownika jest weryfikowany w ramach obowiązkowych procedur weryfikacji tożsamości (KYC), które obejmują pozyskanie i weryfikację urzędowych dokumentów tożsamości, takich jak paszport lub dowód osobisty. Jeżeli proces weryfikacji tożsamości wykaże, że dana osoba nie ukończyła 18 lat, rejestracja zostanie odrzucona, a wszelkie już zebrane dane osobowe zostaną niezwłocznie usunięte.

Jeżeli pomimo tych środków dowiemy się, że przekazano nam dane osobowe osoby poniżej 18. roku życia, dane te zostaną niezwłocznie usunięte. Jeżeli podejrzewasz, że mogliśmy otrzymać takie dane, skontaktuj się z Administratorem lub Inspektorem Ochrony Danych, aby można było podjąć odpowiednie działania.

4. Źródło danych

Administrator może pozyskiwać dane osobowe z następujących źródeł:

4.1 Bezpośrednio od osób, których dane dotyczą

Dane te są przekazywane dobrowolnie przez Użytkowników w związku z korzystaniem z usług Administratora, w szczególności poprzez:

- wypełnienie formularza kontaktowego w Serwisie lub złożenie prośby o oddzwonienie za pośrednictwem widżetu na stronie internetowej,
- zapisanie się do newslettera,
- przekazanie danych w celu przygotowania, zawarcia lub wykonania umowy z Administratorem, w tym korzystania z jego usług,
- przesłanie dokumentów aplikacyjnych (np. CV) w ramach procesów rekrutacyjnych,
- przekazanie danych w ramach procedur weryfikacji Użytkownika (KYC – Know Your Customer lub KYB – Know Your Business), w tym identyfikację za pomocą europejskiego eID, m.in. poprzez udostępnienie wybranych przez Ciebie atrybutów tożsamości z Twojego portfela EUDI Wallet lub krajowego eID, przeprowadzanych zgodnie z obowiązującymi przepisami dotyczącymi przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, w tym niderlandzką ustawą o zapobieganiu praniu pieniędzy i finansowaniu terroryzmu (Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft), a także obowiązującymi unijnymi przepisami AML/CFT i środkami wykonawczymi.

4.2 Od stron trzecich

W zakresie dozwolonym przez obowiązujące prawo Administrator może również pozyskiwać dane osobowe z innych źródeł, w tym:

- od podmiotów, z którymi Użytkownik jest powiązany (np. pracodawcy, partnera biznesowego lub podmiotu zlecającego usługę),
- od dostawców usług płatniczych, instytucji finansowych lub innych dostawców niezbędnych usług,
- z publicznie dostępnych rejestrów i baz danych, takich jak: izby handlowe, rejestry beneficjentów rzeczywistych / rejestry przejrzystości, rejestry przedsiębiorców, urzędowe listy sankcyjne oraz publicznie dostępne i wiarygodne źródła internetowe (np. wyszukiwarki) — w tym za pośrednictwem zewnętrznych dostawców usług weryfikacyjnych, od operatorów systemów eID, dostawców portfeli EUDI Wallet oraz dostawców usług zaufania, którzy potwierdzają nam Twoje atrybuty tożsamości, gdy korzystasz z europejskiego eID,
- z publicznie dostępnych sieci blockchain, w tym znaczniki czasu transakcji, identyfikatory transakcji, podpisy cyfrowe, kwoty transakcji i adresy portfeli, jeżeli dane te są przetwarzane w celu realizacji transakcji, zapewnienia bezpieczeństwa, zapobiegania nadużyciom oraz wypełnienia obowiązujących obowiązków prawnych,
- od dostawców usług technicznych i operacyjnych, którzy dostarczają informacje dotyczące transakcji lub statusu operacji,
- od partnerów marketingowych i afiliacyjnych: wyłącznie kod promocyjny lub link kampanii, za pośrednictwem którego się zarejestrowałeś(-aś). Nie przyjmujemy list danych osobowych od influencerów.

Administrator pozyskuje dane z powyższych źródeł wyłącznie wtedy, gdy jest to uzasadnione celem przetwarzania, niezbędne do świadczenia usług lub wymagane przez prawo.

4.3 Automatycznie

Podczas korzystania ze strony internetowej Administratora niektóre dane mogą być zbierane automatycznie, w tym: informacje o sposobie korzystania z usług (takie jak adres IP, data i godzina wizyty, wyświetlone strony i kliknięte linki), informacje techniczne o urządzeniu i oprogramowaniu (np. typ przeglądarki, system operacyjny, ustawienia językowe), a także

informacje zbierane za pomocą plików cookie i podobnych technologii (szczegółowe zasady ich stosowania opisano w Polityce plików cookie).

Możemy również zbierać informacje o tym, w jaki sposób Użytkownicy korzystają z naszego Serwisu i Usług, w tym dane dotyczące korzystania ze strony, dane o interakcjach oraz, w stosownych przypadkach, informacje o grupie wiekowej.

Ponadto w niektórych przypadkach możemy otrzymywać informacje bezpośrednio od Użytkowników przed utworzeniem konta, na przykład gdy Użytkownik bierze udział w ankietach lub kontaktuje się z nami przed zawarciem umowy.

5. Procesy, w ramach których przetwarzamy Twoje dane osobowe

PROCES	KATEGORIE DANYCH OSOBOWYCH	CELE I PODSTAWA PRAWNA PRZETWARZANIA	OKRES PRZECHOWYWANIA*
Korzystanie z Serwisu i Aplikacji (bez zakładania konta)	Adres IP, inne identyfikatory oraz informacje zbierane za pomocą plików cookie i podobnych technologii	Przetwarzamy dane, aby umożliwić Ci korzystanie z Serwisu, na podstawie prawnie uzasadnionego interesu Administratora (art. 6 ust. 1 lit. f RODO), polegającego na zapewnieniu prawidłowego funkcjonowania strony.	Przetwarzamy dane przez czas korzystania przez Ciebie z Serwisu.
Marketing na podstawie zgody (cold leads / newslettery)	Imię, nazwisko, adres e-mail	Przetwarzamy dane w celu przesyłania komunikatów marketingowych, newsletterów i treści promocyjnych na podstawie zgody Użytkownika (art. 6 ust. 1 lit. a RODO), art. 11.7 niderlandzkiej ustawy o telekomunikacji (Telecommunicatiewet), która wdraża w Niderlandach dyrektywę o prywatności i łączności elektronicznej (2002/58/WE), oraz zgodnie z obowiązującymi przepisami dotyczącymi komunikacji elektronicznej.	Możesz w każdej chwili wycofać zgodę, bez wpływu na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem.
Komunikacja marketingowa do obecnych klientów (podobne produkty i usługi)	Imię, nazwisko, adres e-mail	Przetwarzamy dane w celu marketingu własnych podobnych produktów lub usług skierowanego do obecnych klientów, na podstawie prawnie uzasadnionego interesu Administratora (art. 6 ust. 1 lit. f RODO), zgodnie z obowiązującymi przepisami dotyczącymi komunikacji elektronicznej. Użytkownicy mogą w każdej chwili wnieść sprzeciw wobec takiego przetwarzania.	Możesz w każdej chwili wnieść sprzeciw wobec takiego przetwarzania, korzystając z mechanizmu rezygnacji z subskrypcji zawartego w każdej wiadomości marketingowej lub kontaktując się z nami bezpośrednio.

Kody promocyjne (w tym kody powiązane z influencerami)	Zastosowany kod promocyjny (w tym kod powiązany z influencerem lub partnerem), data i godzina jego wykorzystania, identyfikatory konta i transakcji oraz źródło kampanii, za pośrednictwem którego do nas trafiłeś(-aś)	W celu przyznania przysługującego Ci rabatu (art. 6 ust. 1 lit. b RODO). W celu przypisania nowych Użytkowników do kampanii lub partnera, pomiaru wyników kampanii oraz wykrywania nadużyć, takich jak zakładanie wielu kont lub nieuprawnione wykorzystanie kodów (art. 6 ust. 1 lit. f RODO). Nie przekazujemy influencerom Twojego imienia i nazwiska, danych kontaktowych, historii transakcji ani innych danych konta. Otrzymują oni wyłącznie zagregowane wyniki kampanii.	Przez okres trwania kampanii. Dokumentacja stanowiąca część naszej dokumentacji finansowej jest przechowywana przez 7 lat od końca ostatniego właściwego roku kalendarzowego (art. 52 niderlandzkiej ordynacji podatkowej – Algemene wet inzake rijksbelastingen). Dane służące do wykrywania nadużyć są przechowywane przez [12] miesięcy od zakończenia kampanii
Reklama i pomiar skuteczności kampanii	Identyfikatory reklamowe i atrybucyjne, identyfikatory plików cookie i urządzeń oraz dane o interakcjach z kampanią	Reklama spersonalizowana i pomiar skuteczności kampanii na podstawie Twojej zgody wyrażonej za pośrednictwem naszego banera cookie (art. 6 ust. 1 lit. a RODO; art. 11.7a Telecommunicatiewet). Wykrywanie nieprawidłowego ruchu i oszustw na podstawie naszego prawnie uzasadnionego interesu (art. 6 ust. 1 lit. f RODO).	Do momentu wycofania zgody, nie dłużej jednak niż przez [x] miesięcy.
Założenie Konta Użytkownika w Serwisie i zarządzanie nim	Imię, nazwisko, adres e-mail, numer telefonu	Przetwarzamy dane w celu świadczenia usług związanych z zakładaniem, zarządzaniem i prowadzeniem Kont Użytkowników w Serwisie, na podstawie niezbędności do wykonania umowy (art. 6 ust. 1 lit. b RODO), a także w celu ustalenia, dochodzenia lub obrony roszczeń, na podstawie prawnie uzasadnionego interesu Administratora (art. 6 ust. 1 lit. f RODO), polegającego na ochronie jego praw.	Dane przetwarzane w celu wykonania umowy są przechowywane przez czas trwania umowy, a następnie przez okres do 6 lat, zgodnie z obowiązującymi wymogami prawnymi oraz z uwagi na ewentualne roszczenia.
Formularz kontaktowy	Dane niezbędne do nawiązania komunikacji, w tym: imię, nazwisko, adres e-mail, numer telefonu	Dane są przetwarzane w celu identyfikacji nadawcy i obsługi jego zapytania; podstawą prawną przetwarzania jest niezbędność do wykonania umowy (art. 6 ust. 1 lit. b RODO). Jeżeli Użytkownik poda dodatkowe dane, które nie są wymagane, podstawą prawną przetwarzania takich danych jest zgoda (art. 6 ust. 1 lit. a RODO).	Dane przetwarzane w celu identyfikacji i obsługi zapytania są przechowywane przez okres niezbędny do wykonania umowy, a następnie przez okres wymagany przez obowiązujące przepisy oraz przez okres do 6 lat w celu zabezpieczenia

			ewentualnych roszczeń. Dane przetwarzane na podstawie zgody są przechowywane do momentu jej wycofania.
Prośba o oddzwonienie za pośrednictwem widżetu na stronie internetowej	Numer telefonu i preferowana godzina oddzwonienia. Widżet automatycznie zbiera również adres IP oraz identyfikatory przeglądarki/urządzenia.	Przetwarzamy te dane, aby oddzwonić do Ciebie w sprawie Twojej prośby. Podstawa prawna: podjęcie działań na Twoje żądanie przed zawarciem umowy (art. 6 ust. 1 lit. b RODO). Jeżeli za Twoją zgodą widżet wykorzystuje analityczne pliki cookie, podstawą prawną jest Twoja zgoda (art. 6 ust. 1 lit. a RODO oraz art. 11.7a niderlandzkiej ustawy o telekomunikacji). Numer telefonu jest wykorzystywany wyłącznie do wykonania żądanego połączenia i nie jest wykorzystywany do celów marketingowych bez Twojej odrębnej zgody.	Przez czas niezbędny do obsługi Twojej prośby oraz przez 12 miesięcy po jej obsłużeniu. Jeżeli rozmowa doprowadzi do założenia konta, zastosowanie mają zasady przechowywania danych konta.
Weryfikacja tożsamości Użytkownika (KYC/KYB), ocena ryzyka AML/CFT	Dane identyfikacyjne (imię, nazwisko, krajowy numer identyfikacyjny, data urodzenia, obywatelstwo, adres zamieszkania), dane dokumentu tożsamości (rodzaj dokumentu, seria i numer, data ważności, kraj wydania), kopie dokumentów tożsamości (np. paszportu, dowodu osobistego, prawa jazdy) przesłanych w celu weryfikacji, wizerunek uzyskany ze zdjęcia lub nagrania wideo przesłanego w trakcie weryfikacji, informacje biometryczne wygenerowane z takich obrazów, w tym geometria twarzy uzyskana ze zdjęcia/nagrania wideo, przetwarzane	Przetwarzamy dane w celu wypełnienia obowiązków prawnych wynikających z przepisów o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, oceny ryzyka oraz zapewnienia bezpieczeństwa naszych usług. Podstawą prawną jest wypełnienie obowiązku prawnego (art. 6 ust. 1 lit. c RODO). W przypadku wykrywania oszustw podstawą prawną jest nasz prawnie uzasadniony interes (art. 6 ust. 1 lit. f RODO), polegający na ochronie przed oszustwami i zapewnieniu bezpieczeństwa transakcji. Weryfikacja za pomocą europejskiego eID jest przeprowadzana w celu zapewnienia zgodności z Wwft oraz obowiązującymi unijnymi przepisami AML/CFT (art. 6 ust. 1 lit. c RODO).	Przetwarzamy dane przez czas trwania relacji w zakresie świadczenia usług, a po jej zakończeniu przez dodatkowe 5 lat zgodnie z przepisami AML, a także przez okres niezbędny do ustalenia, dochodzenia lub obrony roszczeń — do 6 lat. Dane otrzymane za pośrednictwem europejskiego eID są przechowywane przez te same okresy co pozostałe dane weryfikacyjne.

	wyłącznie w celu jednoznacznej identyfikacji i weryfikacji tożsamości (elektroniczna weryfikacja tożsamości – EIDV), informacje o źródle środków, źródle majątku, sytuacji finansowej, dane dotyczące weryfikacji dochodów i/lub aktywów, doświadczenie w zakresie obrotu i inwestycji, dane logowania i dane transakcyjne. Jeżeli weryfikujesz się za pomocą europejskiego eID: atrybuty tożsamości udostępnione przez Twój eID lub portfel EUDI Wallet (takie jak imię i nazwisko, data urodzenia, obywatelstwo, numer dokumentu lub poświadczenia oraz kraj wydania), poziom zaufania eID oraz wynik weryfikacji i jej znacznik czasu. Żądamy wyłącznie atrybutów niezbędnych do stosowania środków należytej staranności wobec klienta. W przypadku Użytkowników biznesowych: dane spółki, numer identyfikacji podatkowej, numery w rejestrach przedsiębiorców oraz dane członków zarządu i beneficjentów rzeczywistych.		

Realizacja transakcji, księgowość oraz transfer środków lub kryptoaktywów	Dane identyfikacyjne (imię, nazwisko, adres e-mail, numer telefonu), dane transakcyjne (w tym adresy portfeli podane przez Użytkownika i powiązane informacje o trasowaniu transakcji), identyfikatory transakcji, hashe, historia transakcji, dane nadawcy i odbiorcy, kwota transakcji, preferencje walutowe, metoda płatności, data i/lub znacznik czasu) oraz dane płatnicze (np. informacje o metodach płatności, numer rachunku bankowego, dane karty płatniczej (takie jak PAN) oraz szczegóły rozliczenia)	Przetwarzamy dane w celu realizacji transakcji, ich prawidłowej rejestracji oraz obsługi rozliczeń finansowych. Podstawą prawną przetwarzania jest wykonanie umowy (art. 6 ust. 1 lit. b RODO). W celu wypełnienia obowiązków księgowych, podatkowych i AML podstawą prawną jest wypełnienie obowiązku prawnego ciążącego na Administratorze (art. 6 ust. 1 lit. c RODO). W celu ustalenia, dochodzenia lub obrony roszczeń przetwarzamy dane na podstawie naszego prawnie uzasadnionego interesu (art. 6 ust. 1 lit. f RODO), polegającego na ochronie praw Administratora i zapewnieniu bezpieczeństwa transakcji.	Przechowujemy dane przez dłuższy z następujących okresów: 7 lat od końca ostatniego właściwego roku kalendarzowego – do celów podatkowych (art. 52 niderlandzkiej ordynacji podatkowej); oraz 5 lat od zakończenia relacji gospodarczej – do celów AML (art. 33 ust. 3 Wwft). W celu ustalenia, dochodzenia lub obrony roszczeń dane mogą być przetwarzane przez kolejne maksymalnie 6 lat, zgodnie z obowiązującymi terminami przedawnienia.
Zapewnienie bezpieczeństwa i integralności Usług (zapobieganie oszustwom i wykrywanie nadużyć)	Dane identyfikacyjne (takie jak imię, nazwisko, adres e-mail, numer telefonu i identyfikatory konta Użytkownika), dane transakcyjne, dane dotyczące aktywności na koncie, dane komunikacyjne oraz inne dane przetwarzane w związku z korzystaniem z Usług	Przetwarzamy dane w celu monitorowania transakcji, wykrywania, zapobiegania i wyjaśniania oszustw, nadużyć, zachowań niezgodnych z prawem, naruszeń naszych polityk lub Regulaminu oraz innych zagrożeń bezpieczeństwa, a także w celu zapewnienia integralności i bezpieczeństwa naszych Usług. Podstawą prawną przetwarzania jest prawnie uzasadniony interes Administratora (art. 6 ust. 1 lit. f RODO), polegający na zabezpieczeniu platformy, ochronie Użytkowników i zapobieganiu nadużyciom Usług. W stosownych przypadkach przetwarzanie może być również prowadzone w celu wypełnienia obowiązków prawnych (art. 6 ust. 1 lit. c RODO), w szczególności wynikających z przepisów AML/CFT.	Dane są przetwarzane przez czas trwania relacji w zakresie świadczenia usług, a następnie przez okres niezbędny do wypełnienia obowiązków prawnych oraz ustalenia, dochodzenia lub obrony roszczeń, zgodnie z obowiązującymi terminami przedawnienia.
Obsługa klienta i komunikacja	Dane identyfikacyjne i kontaktowe (takie	Przetwarzamy dane w celu zapewnienia obsługi klienta, odpowiadania na zapytania,	Dane są przetwarzane przez okres niezbędny do

	jak imię, nazwisko, adres e-mail, numer telefonu i identyfikatory konta Użytkownika), dane komunikacyjne, w tym odpowiedzi na ankiety, informacje przekazane zespołom obsługi klienta lub badań użytkowników, interakcje z chatbotem oraz, w stosownych przypadkach, nagrania rozmów	rozpatrywania reklamacji oraz poprawy jakości i funkcjonalności naszych Usług. Podstawą prawną przetwarzania jest niezbędność do wykonania umowy (art. 6 ust. 1 lit. b RODO) oraz prawnie uzasadniony interes Administratora (art. 6 ust. 1 lit. f RODO), polegający na zapewnieniu skutecznej obsługi klienta i doskonaleniu usług.	obsługi zapytania lub zgłoszenia, a następnie przez okres wymagany przez obowiązujące przepisy lub niezbędny do ustalenia, dochodzenia lub obrony roszczeń.
Procesy rekrutacyjne (kandydaci do pracy)	Dane identyfikacyjne i kontaktowe (imię, nazwisko, adres e-mail, numer telefonu), dane zawodowe (CV, doświadczenie zawodowe, wykształcenie, kwalifikacje), informacje przekazane w trakcie procesu rekrutacji (w tym notatki z rozmów kwalifikacyjnych) oraz wszelkie inne dane dobrowolnie przekazane przez kandydata	Przetwarzamy dane w celu prowadzenia procesów rekrutacyjnych oraz oceny kandydatów do zatrudnienia lub współpracy. Podstawą prawną przetwarzania jest niezbędność do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (art. 6 ust. 1 lit. b RODO), wypełnienie obowiązków prawnych wynikających z obowiązującego prawa pracy (art. 6 ust. 1 lit. c RODO), prawnie uzasadniony interes Administratora (art. 6 ust. 1 lit. f RODO), polegający na prowadzeniu procesów rekrutacyjnych i wyborze odpowiednich kandydatów, a także zgoda (art. 6 ust. 1 lit. a RODO), jeżeli kandydat dobrowolnie przekazuje dodatkowe dane niewymagane przepisami prawa lub aplikuje w przyszłych procesach rekrutacyjnych.	Dane są przetwarzane przez czas trwania procesu rekrutacji, a następnie przez okres do 4 tygodni od jego zakończenia oraz przez każdy dłuższy okres wymagany przepisami prawa lub niezbędny do rozpatrzenia związanych z nim roszczeń. Jeżeli kandydat wyraził zgodę na udział w przyszłych procesach rekrutacyjnych, dane mogą być przetwarzane przez rok.
Wypełnianie obowiązkowych obowiązków sprawozdawczych w zakresie podatków wynikających z DAC8 (dyrektywa Rady (UE) 2023/2226) oraz ram sprawozdawczości OECD w zakresie kryptoaktywów (CARF)	Imię i nazwisko, data urodzenia, [miejsce urodzenia], adres zamieszkania, kraj(e) rezydencji podatkowej, numer(y) identyfikacji podatkowej (TIN) oraz Twoje oświadczenie o rezydencji podatkowej (samocertyfikacja), w tym data i oświadczenie, że informacje są	Przetwarzamy te dane w celu identyfikacji Użytkowników podlegających raportowaniu, uzyskania i weryfikacji Twojego oświadczenia o rezydencji podatkowej oraz przekazywania informacji niderlandzkiej administracji podatkowej i celnej (Belastingdienst). Podstawą prawną jest wypełnienie obowiązku prawnego (art. 6 ust. 1 lit. c RODO). Belastingdienst może wymieniać te informacje z organami podatkowymi innych państw członkowskich UE oraz jurysdykcji partnerskich CARF. Nie wykorzystujemy tych danych do celów marketingowych.	7 lat od końca ostatniego właściwego roku kalendarzowego – do celów podatkowych (art. 52 niderlandzkiej ordynacji podatkowej).

	prawidłowe i kompletne. W przypadku Użytkowników będących podmiotami: te same dane dotyczące podmiotu oraz, w stosownych przypadkach, osób sprawujących nad nim kontrolę. Adresy portfeli, identyfikatory transakcji oraz liczba jednostek, łączna wartość i liczba transakcji w podziale na kryptoaktywa i rok kalendarzowy, według rodzaju transakcji.		
Zapewnienie zgodności z rozporządzeniem w sprawie przekazów środków (TFR) — obowiązkowa wymiana danych inicjatora i beneficjenta podczas transferów kryptoaktywów w celu wykrywania prania pieniędzy i finansowania terroryzmu oraz zapobiegania im	Imię i nazwisko, identyfikator rachunku kryptoaktywów (adres portfela), numer referencyjny transakcji oraz, jeżeli jest to wymagane: adres zamieszkania, krajowy numer identyfikacyjny lub data i miejsce urodzenia inicjatora i/lub beneficjenta	Art. 6 ust. 1 lit. c RODO — wypełnienie obowiązku prawnego wynikającego z rozporządzenia (UE) 2023/1113. Odbiorcami są kontrahenci będący CASP oraz dostawcy usług w zakresie kryptoaktywów uczestniczący w transferze, zgodnie z wymogami prawa.	5 lat od dnia transferu, zgodnie z art. 26 rozporządzenia (UE) 2023/1113.

** Po upływie okresu przechowywania dane są nieodwracalnie usuwane lub anonimizowane.*

Co do zasady nie przetwarzamy szczególnych kategorii danych osobowych (takich jak dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, dane dotyczące zdrowia lub orientacji seksualnej). Jednak w celu weryfikacji tożsamości (KYC) przetwarzamy dane biometryczne (geometrię twarzy uzyskaną ze zdjęć lub nagrań wideo) wyłącznie w celu potwierdzenia tożsamości Użytkownika i zapobiegania oszustwom. Przetwarzanie to odbywa się w celu wypełnienia obowiązków prawnych wynikających z obowiązujących przepisów AML/CFT (art. 6 ust. 1 lit. c RODO) w związku z art. 9 ust. 2 lit. g RODO (przetwarzanie niezbędne ze względów związanych z ważnym interesem publicznym), zgodnie z obowiązującymi przepisami unijnymi i krajowymi w zakresie AML/CFT. Jeżeli wymagają tego obowiązujące przepisy, przetwarzanie takie może również opierać się na art. 9 ust. 2 lit. a RODO (wyraźna zgoda), uzyskanej w trakcie procesu weryfikacji.

Dane biometryczne są przetwarzane wyłącznie w zakresie ściśle niezbędnym do weryfikacji tożsamości, nie są wykorzystywane do żadnych innych celów, nie podlegają dalszemu przetwarzaniu wykraczającemu poza weryfikację tożsamości i zapobieganie oszustwom oraz są objęte wzmocnionymi środkami bezpieczeństwa. Jeżeli szczególne kategorie danych osobowych znajdą się przypadkowo w danych transakcyjnych lub innych informacjach przekazanych przez Użytkowników, dane takie nie są aktywnie wykorzystywane ani analizowane przez Administratora w żadnym konkretnym celu.

Jeżeli przetwarzanie opiera się na prawnie uzasadnionym interesie Administratora, przeprowadziliśmy test równowagi, aby upewnić się, że interesy te nie są nadrzędne wobec praw i wolności osoby, której dane dotyczą.

Jeżeli do tego samego zbioru danych ma zastosowanie więcej niż jeden okres przechowywania (na przykład dokumentacja AML objęta 5-letnim okresem przechowywania na podstawie Wwft, która jest również istotna dla toczącego się postępowania cywilnego objętego 6-letnim terminem przedawnienia), przechowujemy dane przez dłuższy z mających zastosowanie okresów. Okresy przechowywania biegną od zakończenia relacji gospodarczej lub od daty danej transakcji, w zależności od tego, która z tych dat jest późniejsza, chyba że powyżej wskazano inaczej.

6. Kto jeszcze ma dostęp do Twoich danych i w jakich celach?

6.1 Podmioty przetwarzające dane w naszym imieniu

W związku ze świadczeniem naszych usług Twoje dane osobowe mogą być ujawniane stronom trzecim. Ujawnienie takie następuje wyłącznie wtedy, gdy jest to niezbędne do osiągnięcia określonego celu, zgodnie z RODO, na podstawie odpowiednich umów i z zastosowaniem adekwatnych środków bezpieczeństwa.

Współpracujemy z zaufanymi dostawcami usług, którzy wspierają nas w technicznej i operacyjnej realizacji naszych usług. Mogą to być w szczególności: dostawcy usług IT, hostingu i cyberbezpieczeństwa; dostawcy oprogramowania i narzędzi wykorzystywanych do obsługi Użytkowników; biura rachunkowe; kancelarie prawne; firmy audytorskie; dostawcy usług chmurowych, poczty e-mail, archiwizacji i analityki; dostawcy usług komunikacyjnych i planowania oddzwonień; dostawcy usług elektronicznej weryfikacji tożsamości i usług zaufania, którzy w naszym imieniu weryfikują europejskie eID; a także podmioty wspierające procesy operacyjne i administracyjne.

Każdy podmiot przetwarzający działa wyłącznie na nasze polecenie i na podstawie umowy powierzenia przetwarzania danych, która określa techniczne i organizacyjne środki ochrony danych.

6.2 Podmioty przetwarzające dane we własnych celach (niezależni administratorzy)

W niektórych sytuacjach dane osobowe mogą być ujawniane podmiotom, które przetwarzają je jako niezależni administratorzy. Dotyczy to:

- podmiotów z grupy kapitałowej Administratora, jeżeli ujawnienie jest niezbędne do celów administracji wewnętrznej, wypełnienia obowiązków prawnych (w tym AML/CFT), zarządzania ryzykiem lub świadczenia usług; podmioty te działają jako niezależni administratorzy lub podmioty przetwarzające, w zależności od kontekstu przetwarzania,
- podmiotów dostarczających kluczowe systemy IT lub infrastrukturę wykorzystywane przy świadczeniu naszych usług (współadministratorzy w odniesieniu do określonego systemu),
- organów nadzorczych i instytucji publicznych, jeżeli ujawnienie jest wymagane przez prawo (w tym m.in. niderlandzkiego Urzędu ds. Rynków Finansowych – AFM, DNB oraz niderlandzkiej jednostki analityki finansowej – FIU-NL, a także innych organów ścigania i organów podatkowych),
- niderlandzkiej administracji podatkowej i celnej (Belastingdienst) — określone dane osobowe i transakcyjne naszych użytkowników będą zgłaszane do Belastingdienst. Dane te mogą następnie zostać udostępnione organom podatkowym innych państw członkowskich UE w ramach automatycznej wymiany informacji. Przetwarzamy te dane wyłącznie w celu wypełnienia naszych obowiązków prawnych i nie wykorzystujemy ich w żadnym innym celu,
- kontrahentów będących dostawcami usług w zakresie kryptoaktywów (Travel Rule) — jesteśmy prawnie zobowiązani do przekazywania danych osobowych inicjatora i beneficjenta do przyjmującego CASP lub dostawcy usług w zakresie kryptoaktywów przy realizacji transferów kryptoaktywów powyżej obowiązujących progów, a w niektórych przypadkach niezależnie od progu. Takie udostępnianie danych jest obowiązkowe i nie można z niego zrezygnować,
- instytucji finansowych i operatorów kart płatniczych (np. Mastercard, Visa) w związku z obsługą płatności,
- podmiotów uczestniczących w czynnościach audytowych lub kontrolnych,
- kancelarii prawnych i doradców zawodowych w związku z postępowaniami prawnymi,
- podmiotów uczestniczących w procesach korporacyjnych (np. transakcjach przejęcia lub restrukturyzacji), jeżeli ujawnienie jest niezbędne do zawarcia lub wykonania umowy.
- influencerów i partnerów marketingowych, którzy otrzymują wyłącznie zagregowane wyniki kampanii i nie mają dostępu do Twoich danych osobowych.
- operatorów systemów eID i dostawców portfeli EUDI Wallet, którzy przetwarzają Twoje dane jako niezależni administratorzy przy wydawaniu i obsłudze Twojego eID lub portfela.

W takich przypadkach każdy z tych podmiotów odpowiada za przetwarzanie danych zgodnie z własną polityką prywatności i obowiązującymi ramami prawnymi.

6.3 Sztuczna inteligencja (AI)

W ramach naszych procesów operacyjnych korzystamy z narzędzi opartych na sztucznej inteligencji, które wspierają określone funkcje, takie jak:

- weryfikacja tożsamości i porównywanie biometryczne (np. wykrywanie żywotności, uwierzytelnianie dokumentów) — zapewniane przez zewnętrznych, certyfikowanych dostawców usług KYC/IDV działających na podstawie umów powierzenia przetwarzania danych (DPA) i standardowych klauzul umownych (SCC),
- monitorowanie transakcji i ocena ryzyka AML — zautomatyzowane systemy oparte na regułach i uczeniu maszynowym, służące do wykrywania nietypowych wzorców i generowania alertów weryfikowanych przez człowieka,
- weryfikacja pod kątem sankcji i PEP — automatyczne porównywanie z listami sankcyjnymi (UE, ONZ, OFAC) oraz bazami danych osób zajmujących eksponowane stanowiska polityczne,

- wsparcie obsługi klienta — narzędzia AI wspomagające kategoryzację zgłoszeń i przygotowywanie odpowiedzi, przy czym zapytania dotyczące danych osobowych są przekazywane do pracowników.

Żadna w pełni zautomatyzowana decyzja wywołująca skutki prawne lub w podobny sposób istotnie wpływająca na osobę nie jest podejmowana bez zapewnienia, na żądanie, możliwości weryfikacji przez człowieka. Jeżeli zautomatyzowane systemy spowodują ograniczenie konta lub zablokowanie transakcji, pracownik ds. zgodności weryfikuje sprawę przed podjęciem ostatecznej decyzji.

Jeżeli narzędzia AI przetwarzają dane osobowe, przetwarzanie takie odbywa się zgodnie z niniejszą Polityką prywatności oraz obowiązującymi przepisami o ochronie danych.

Narzędzia AI wykorzystywane w naszej działalności są dostarczane przez zewnętrznych dostawców usług działających w naszym imieniu na podstawie odpowiednich umów.

6.4 Współadministrowanie (media społecznościowe)

Gdy kontaktujesz się z Administratorem za pośrednictwem platform mediów społecznościowych (np. Instagram, LinkedIn) lub gdy korzystamy z narzędzi reklamowych i pomiarowych udostępnianych przez operatorów platform, administratorami danych osobowych mogą być wspólnie my i właściciele tych platform. Wspólnie ustalamy cele i sposoby przetwarzania, a Użytkownik ma prawo wykonywać swoje prawa wynikające z RODO zarówno wobec operatora platformy, jak i wobec nas. Jeżeli działamy jako współadministratorzy, uzgodniliśmy podział obowiązków zgodnie z wymogami art. 26 RODO. Więcej informacji można znaleźć w politykach prywatności poszczególnych serwisów społecznościowych.

Chociaż WEB3 Technology oraz platformy mediów społecznościowych (lub dostawcy kluczowych systemów IT) wspólnie ustalają cele i sposoby przetwarzania, to przede wszystkim my zajmujemy się realizacją Twoich praw jako osoby, której dane dotyczą. Możesz jednak wykonywać swoje prawa wobec każdej ze stron.

Aktualna lista naszych podmiotów przetwarzających i podmiotów podprzetwarzających, obejmująca ich nazwę, kraj siedziby i cel przetwarzania, jest dostępna na żądanie przesłane na adres e-mail dpo@rgltd.com. Jeżeli wymagają tego nasze obowiązki wynikające z umów powierzenia przetwarzania danych (DPA), z wyprzedzeniem powiadomimy użytkowników o wszelkich istotnych zmianach w liście podmiotów podprzetwarzających.

7. Czy przekazujemy Twoje dane poza Europejski Obszar Gospodarczy (EOG)?

Twoje dane osobowe przetwarzamy przede wszystkim na terenie Europejskiego Obszaru Gospodarczego (EOG). Jednak w przypadku określonych usług (np. weryfikacji tożsamości lub infrastruktury technicznej) możemy przekazywać dane osobowe zaufanym partnerom spoza EOG („Państwa trzecie”).

Przekazujemy Twoje dane do Państwa trzeciego wyłącznie wtedy, gdy zastosowano jedno z następujących zabezpieczeń:

Decyzja stwierdzająca odpowiedni stopień ochrony

Komisja Europejska uznała, że dane państwo zapewnia odpowiedni stopień ochrony danych (np. Ramy ochrony danych UE-USA w przypadku certyfikowanych podmiotów z USA).

Standardowe klauzule umowne (SCC) i środki uzupełniające

Stosujemy standardowe klauzule umowne zatwierdzone przez Komisję Europejską. W takich przypadkach przeprowadzamy ocenę skutków transferu (TIA), aby ustalić, czy przepisy i praktyki państwa docelowego, w tym dostęp organów publicznych, mogą wpływać na poziom ochrony przekazywanych danych osobowych.

W razie potrzeby wdrażamy uzupełniające środki techniczne, organizacyjne i umowne (takie jak szyfrowanie, ograniczenia dostępu i minimalizacja danych), aby zapewnić, że dane osobowe pozostają chronione na poziomie zasadniczo równoważnym poziomowi gwarantowanemu w EOG.

Oceniamy transfery indywidualnie, a jeżeli nie można zapewnić odpowiedniego stopnia ochrony, odstępujemy od przekazania danych osobowych do danego państwa trzeciego.

Możesz zażądać kopii konkretnych zabezpieczeń stosowanych wobec Twoich danych, kontaktując się z nami pod adresem e-mail dpo@rgltd.com.

8. Czy podanie danych osobowych jest dobrowolne?

Podanie danych osobowych jest dobrowolne; jednak niektóre dane są niezbędne do świadczenia usług oferowanych za pośrednictwem naszego Serwisu i Aplikacji – na przykład dane wymagane do zapewnienia zgodności z przepisami KYC/AML oraz do wykonania umowy są obowiązkowe. Niepodanie takich danych może uniemożliwić korzystanie z określonych funkcji albo zawarcie lub wykonanie umowy z nami.

Dane oznaczone jako opcjonalne możesz podać według własnego uznania, a ich niepodanie nie wpływa na możliwość korzystania z podstawowych usług. Zawsze masz prawo zdecydować, jakie dane chcesz ujawnić.

Jeżeli dobrowolnie wyrazisz zgodę na przetwarzanie swoich danych osobowych w określonych celach (np. marketingowych), możesz ją w każdej chwili wycofać. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Nie powoduje ono również utraty dostępu do usług ani innych uprawnień, chyba że ich realizacja wymaga dalszego przetwarzania danych, których dotyczy zgoda.

Podanie informacji podatkowych na podstawie DAC8 i CARF jest wymogiem ustawowym. Musimy uzyskać ważne oświadczenie o rezydencji podatkowej od każdego Użytkownika, a w stosownych przypadkach także od osób sprawujących kontrolę nad Użytkownikami będącymi podmiotami. Jeżeli mimo naszych próśb i przypomnień nie otrzymamy wymaganych informacji, jesteśmy prawnie zobowiązani do ograniczenia Twojej możliwości przeprowadzania transakcji podlegających raportowaniu do czasu ich przekazania.

9. Czy Twoje dane osobowe podlegają profilowaniu?

Dane osobowe Użytkowników mogą podlegać profilowaniu, rozumianemu jako zautomatyzowane przetwarzanie określonych informacji o Użytkowniku w celu oceny

wybranych czynników dotyczących jego aktywności, wiarygodności lub ryzyka związanego z korzystaniem z usług. Profilowanie odbywa się w szczególności w celu wypełnienia obowiązków wynikających z przepisów o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu (AML), zapewnienia bezpieczeństwa usług oraz zapobiegania oszustwom.

Jeżeli zautomatyzowane przetwarzanie, w tym profilowanie, generuje wynik, który może prowadzić do decyzji wywołującej skutki prawne lub w podobny sposób istotnie wpływającej na osobę (np. odmowa w procesie KYC), wynik taki podlega obowiązkowej weryfikacji przez człowieka przed podjęciem ostatecznej decyzji; osoba, której dane dotyczą, ma prawo zażądać interwencji ludzkiej, zakwestionować decyzję oraz wyrazić własne stanowisko. Nieudana lub niedostępna weryfikacja za pomocą europejskiego eID sama w sobie nie prowadzi do odmowy. Oferujemy inną metodę weryfikacji i przed podjęciem ostatecznej decyzji rozpatrujemy sprawę ręcznie.

Wyniki procesów profilowania mają charakter wspierający i pomocniczy; ich celem jest umożliwienie oceny ryzyka, zapewnienie zgodności z obowiązkami prawnymi oraz zwiększenie bezpieczeństwa zarówno Użytkowników, jak i Administratora.

Jeżeli w trakcie korzystania z usług Użytkownik spełni określone kryteria lub uzyska wynik wskazujący na niższy poziom ryzyka (np. w ocenie AML), może to skutkować dostępem do określonych funkcjonalności.

W szczególności wyniki automatycznych kontroli przeprowadzanych w trakcie procesu weryfikacji tożsamości z wykorzystaniem wideo i biometrii (KYC), w tym mechanizmów rozpoznawania twarzy i wykrywania żywotności, są wykorzystywane wyłącznie jako informacje pomocnicze. Każda odmowa przyjęcia Użytkownika lub ograniczenie dostępu do Usług na podstawie takich wyników (w tym wyników automatycznej weryfikacji biometrycznej) podlega rzeczywistej weryfikacji i zatwierdzeniu przez człowieka, zanim wywoła skutki prawne lub w podobny sposób istotnie wpłynie na Użytkownika, zgodnie z art. 22 RODO.

W przypadku transakcji poniżej określonego progu Administrator nie prowadzi profilowania danych osobowych Użytkowników w rozumieniu art. 4 pkt 4 RODO. W takich przypadkach dane są przetwarzane wyłącznie w zakresie niezbędnym do realizacji transakcji i spełnienia wymogów prawnych, bez dokonywania jakiejkolwiek zautomatyzowanej oceny czynników dotyczących Użytkownika.

Proces profilowania może uwzględniać ogólne czynniki wymagane przez obowiązujące przepisy AML/CFT oraz standardowe praktyki w zakresie zapobiegania oszustwom, w tym publicznie dostępne dane z sieci blockchain (takie jak znaczniki czasu transakcji, identyfikatory transakcji, podpisy cyfrowe, kwoty transakcji i adresy portfeli). Mogą to być na przykład: przekroczenie przez transakcję progów określonych w przepisach prawa, częstotliwość lub charakter transakcji, niespójności geograficzne lub behawioralne, status weryfikacji tożsamości Użytkownika, a także informacje dotyczące interakcji Użytkownika z Serwisem lub Usługami (takie jak dane o korzystaniu, dane o interakcjach lub odpowiedzi na ankiety, w tym zebrane przed utworzeniem konta). Wskaźniki te są wykorzystywane wyłącznie do oceny ryzyka i zapewnienia zgodności z obowiązkami prawnymi; nie wiąże się to z ujawnianiem zastrzeżonych modeli ryzyka ani szczegółowej wewnętrznej logiki wykrywania oszustw.

10. Jakie prawa przysługują Ci w związku z przetwarzaniem przez nas Twoich danych osobowych?

Prawo	Opis
Prawo dostępu	Masz prawo wiedzieć, które Twoje dane osobowe przetwarzamy i w jakich celach, oraz uzyskać ich kopię.
Prawo do przenoszenia danych	Masz prawo otrzymać swoje dane osobowe w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, umożliwiającym przesłanie tych danych innemu administratorowi.
Prawo do sprostowania	Jeżeli Twoje dane są nieprawidłowe lub niekompletne, masz prawo żądać ich sprostowania lub uzupełnienia. Jeżeli masz Konto Użytkownika, niektóre dane możesz zaktualizować samodzielnie.
Prawo do ograniczenia przetwarzania / prawo do bycia zapomnianym	Masz prawo żądać ograniczenia przetwarzania lub usunięcia swoich danych osobowych, chyba że jesteśmy zobowiązani do dalszego ich przetwarzania z uwagi na obowiązujące obowiązki prawne lub w celu ustalenia, dochodzenia lub obrony roszczeń.
Prawo do wycofania zgody	Możesz w każdej chwili wycofać zgodę na przetwarzanie swoich danych osobowych. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem.
Prawo do sprzeciwu	Jeżeli Twoje dane osobowe są przetwarzane na podstawie prawnie uzasadnionych interesów Administratora lub do celów marketingu bezpośredniego, przysługuje Ci również prawo do wniesienia sprzeciwu wobec takiego przetwarzania.
Prawo do weryfikacji zautomatyzowanych decyzji przez człowieka	Jeżeli podejmujemy wobec Ciebie decyzje wyłącznie w sposób zautomatyzowany — w tym automatyczną odmowę w procesie KYC, ocenę ryzyka lub ograniczenia konta wynikające z procedur AML — które wywołują skutki prawne lub w podobny sposób istotnie na Ciebie wpływają, masz prawo: (i) żądać weryfikacji decyzji przez członka naszego zespołu; (ii) wyrazić własne stanowisko w sprawie zautomatyzowanej decyzji; oraz (iii) zakwestionować decyzję.

Aby skorzystać z któregokolwiek z powyższych praw, prześlij żądanie w formie pisemnej na adres: **e-mail** dpo@rgltd.com.

Odpowiemy na Twoje żądanie w terminie jednego miesiąca kalendarzowego od jego otrzymania. Ze względu na skomplikowany charakter żądania lub liczbę żądań możemy przedłużyć ten termin o kolejne dwa miesiące; w takim przypadku poinformujemy Cię o tym w ciągu pierwszego miesiąca i wyjaśnimy przyczynę przedłużenia (art. 12 ust. 3 RODO).

Rozpatrzenie Twojego żądania jest bezpłatne. Jeżeli jednak żądania są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na ich ustawiczny charakter, możemy pobrać rozsądną opłatę administracyjną albo odmówić podjęcia działań w związku z żądaniem (art. 12 ust. 5 RODO).

W celu ochrony Twoich danych przed rozpatrzeniem jakiegokolwiek żądania osoby, której dane dotyczą (DSAR), zweryfikujemy Twoją tożsamość. W tym celu możemy poprosić o kopię urzędowego dokumentu tożsamości lub wykorzystać posiadane przez nas dane z weryfikacji KYC. Dane służące do weryfikacji tożsamości przekazane wyłącznie na potrzeby DSAR nie będą przechowywane dłużej, niż jest to niezbędne do rozpatrzenia Twojego żądania.

Jeżeli uważasz, że Twoje dane osobowe są przetwarzane niezgodnie z prawem, masz prawo wnieść skargę do niderlandzkiego organu ochrony danych: Autoriteit Persoonsgegevens, Bezuidenhoutseweg 30, 2594 AV Den Haag, Niderlandy. Strona internetowa: www.autoriteitpersoonsgegevens.nl Telefon: +31 88 1805 250.

Ważne ograniczenie — dane on-chain: Pamiętaj, że jeżeli Twoje dane osobowe zostały zapisane w publicznym blockchainie (na przykład adres portfela lub hash transakcji, które można z Tobą powiązać), po ich potwierdzeniu w sieci (on-chain) usunięcie lub zmiana tych danych jest dla nas technicznie niemożliwa. Jest to nieodłączne ograniczenie technologii rozproszonego rejestru, pozostające poza naszą kontrolą jako administratora danych. W takich przypadkach usuniemy lub zanonimizujemy wszystkie powiązane zapisy poza blockchainem (off-chain), takie jak Twoje imię i nazwisko, adres e-mail i dane konta, w naszych systemach zgodnie z naszym harmonogramem przechowywania danych, a przy rozpatrywaniu Twojego żądania poinformujemy Cię o ograniczeniu dotyczącym danych on-chain.

11. Jak chronimy i przechowujemy dane osobowe

Wdrażamy odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, zgodnie z art. 32 RODO. Środki te obejmują w szczególności:

- ograniczenie dostępu do danych osobowych wyłącznie do upoważnionych pracowników,
- minimalizację danych i kontrolę dostępu opartą na rolach,
- szyfrowanie danych podczas przesyłania i przechowywania,
- monitorowanie systemów i działań do celów bezpieczeństwa i zapobiegania oszustwom,
- regularne przeglądy bezpieczeństwa, audyty i testy systemów IT,
- korzystanie z bezpiecznych, certyfikowanych dostawców usług spełniających standardy branżowe.

Dane osobowe są przechowywane wyłącznie przez okresy wskazane w niniejszej Polityce prywatności i wyłącznie w bezpiecznych środowiskach zapewniających poufność, integralność i dostępność danych. Po upływie odpowiednich okresów przechowywania dane są nieodwracalnie usuwane lub anonimizowane.

11.1 Zgłaszanie naruszeń ochrony danych

Prowadzimy wewnętrzną procedurę identyfikowania i oceny naruszeń ochrony danych osobowych oraz reagowania na nie, zgodnie z art. 33 i 34 RODO.

W przypadku naruszenia ochrony danych osobowych, które może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, zgłosimy je niderlandzkiemu organowi ochrony danych (Autoriteit Persoonsgegevens) bez zbędnej zwłoki i – w miarę możliwości – nie później niż w terminie 72 godzin od stwierdzenia naruszenia, chyba że jest mało prawdopodobne, by naruszenie skutkowało takim ryzykiem.

Jeżeli naruszenie może powodować wysokie ryzyko naruszenia Twoich praw i wolności — na przykład gdy dotyczy wrażliwych danych finansowych, dokumentów tożsamości lub danych biometrycznych — zawiadomimy o nim również bezpośrednio Ciebie, bez zbędnej zwłoki, korzystając z danych kontaktowych przypisanych do Twojego konta.

Prowadzimy wewnętrzny rejestr naruszeń, w którym dokumentujemy wszystkie incydenty, ich skutki oraz podjęte działania zaradcze, zgodnie z naszymi obowiązkami w zakresie rozliczalności wynikającymi z art. 5 ust. 2 RODO.

11.2 Dane zanonimizowane

W celu monitorowania i ograniczania ryzyka oszustw oraz innych zagrożeń, poprawy działania naszych usług oraz zwiększenia bezpieczeństwa możemy przetwarzać informacje w formie zanonimizowanej.

Dane zanonimizowane nie stanowią danych osobowych w rozumieniu RODO, ponieważ nie pozwalają na identyfikację osoby. Dane takie są przetwarzane wyłącznie do celów analitycznych, statystycznych i związanych z bezpieczeństwem.

Proces anonimizacji jest zaprojektowany tak, aby uniemożliwić ponowną identyfikację osób, bezpośrednio lub pośrednio.

12. Pliki cookie

Zasady i rodzaje stosowanych plików cookie i podobnych technologii zostały określone w Polityce plików cookie. Szczegółowy opis wykorzystywanych przez nas plików cookie i podobnych technologii można znaleźć w naszych Serwisach.

13. Zmiany Twoich danych osobowych

Ważne jest, aby przechowywane przez nas dane osobowe na Twój temat były prawidłowe i aktualne. Informuj nas, jeżeli Twoje dane osobowe ulegną zmianie lub jeżeli dowiesz się, że przechowywane przez nas dane osobowe są nieprawidłowe. Jeżeli zmieni się Twoja rezydencja podatkowa lub inne informacje podatkowe, niezwłocznie nas o tym poinformuj, abyśmy mogli zaktualizować Twoje dane.

14. Zmiany Polityki

Niniejsza Polityka prywatności obowiązuje od dnia 05.05.2026.

Możemy okresowo zmieniać niniejszą Politykę prywatności, aby odzwierciedlić zmiany w sposobie przetwarzania danych osobowych lub zmiany w przepisach o ochronie danych. Jeżeli nasza polityka ulegnie istotnej zmianie (tj. zmianie celów przetwarzania, tożsamości administratora lub sposobu, w jaki możesz wykonywać swoje prawa w związku z prowadzonym przez nas przetwarzaniem), poinformujemy Cię o tym i opublikujemy nową wersję w naszych Serwisach. Prosimy o regularne sprawdzanie naszej Polityki prywatności, aby być na bieżąco z wszelkimi zmianami. Data na początku niniejszej informacji wskazuje, kiedy została ona ostatnio zaktualizowana.

15. Oświadczenie dotyczące DPIA

Zgodnie z art. 35 RODO przeprowadzamy oceny skutków dla ochrony danych (DPIA) przed rozpoczęciem operacji przetwarzania, które mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. Obejmuje to w szczególności, choć nie wyłącznie: przetwarzanie danych biometrycznych w celu weryfikacji tożsamości, systematyczne zautomatyzowane monitorowanie zachowań transakcyjnych do celów AML/CFT oraz przetwarzanie na dużą skalę szczególnych kategorii danych. Wyniki DPIA stanowią podstawę naszych środków technicznych i organizacyjnych i są dokumentowane w wewnętrznym rejestrze czynności przetwarzania (RoPA) prowadzonym na podstawie art. 30 RODO.

16. Historia wersji

Wersja	Data zmiany	Autor zmiany	Opis zmiany
1.0	12.10.2024	DPO / CRCO	Wersja bazowa dokumentu — pierwsza publikacja. Zatwierdzona przez Organ zarządzający
2.0	05.05.2026	DPO / CRCO	Aktualizacja uwzględniająca obowiązki wynikające z DAC8 / CARF, Travel Rule zgodnie z TFR, korzystanie z narzędzi AI, współadministrowanie, oświadczenie dotyczące DPIA oraz ograniczenia dotyczące danych on-chain. Zatwierdzona przez Organ zarządzający.
3.0	27.10.2026	DPO / CRCO	Neutralne sformułowania dotyczące podmiotu: odniesienia do marki zastąpiono zdefiniowanym terminem „Spółka”. Dodano definicję Spółki. Historię wersji zaktualizowano w celu odzwierciedlenia obecnej struktury jako v.26_9.0. Rozszerzono wiersz dotyczący DAC8 / CARF (samocertyfikacja, osoby sprawujące kontrolę, odbiorca, okres przechowywania) i dodano informację o skutkach na gruncie DAC8; dodano informacje o kodach promocyjnych, reklamie i ujawnianiu danych partnerom. Dodano weryfikację za pomocą europejskiego eID i portfela EUDI Wallet.

© WEB3 Technology B.V. — Wszelkie prawa zastrzeżone.