

Polityka Prywatności

WEB3 Technology B.V. (RGLTD)

Tytuł dokumentu	Polityka Prywatności
Właściciel dokumentu	Dyrektor ds. ryzyka i zgodności (CRCO) / Inspektor ochrony danych (IOD)
Dotyczy	Wszystkich Użytkowników usług WEB3 Technology B.V. oraz strony internetowej / aplikacji
Podstawa prawna	RODO (UE) 2016/679 · Holenderska ustawa o telekomunikacji (Tw) · Rozporządzenie MiCA 2023/1114 · Rozporządzenie TFR 2023/1113 · Dyrektywa DAC8 2023/2226 · Wwft · DORA
Wersja	2.0
Data wejścia w życie	05.05.2026
Cykl przeglądu	Roczny lub w przypadku istotnych zmian regulacyjnych lub operacyjnych
Zatwierdzone przez	Organ zarządzający / CRCO
Klasyfikacja	Publiczne — Informacja o ochronie prywatności

W WEB3 Technology B.V. zobowiązujemy się do ochrony bezpieczeństwa informacji, które nam Państwo powierzają, oraz do zapewnienia, że zasady regulujące ich przetwarzanie są przejrzyste i łatwe do zrozumienia. Chcemy, aby osoby korzystające z naszych usług wiedziały, jakie dane osobowe gromadzimy, w jakich celach je przetwarzamy oraz jakie prawa przysługują im na mocy obowiązujących przepisów o ochronie danych. Przestrzegamy zasad określonych w RODO oraz odpowiednich krajowych przepisach dotyczących prywatności, a nasze działania związane z przetwarzaniem danych organizujemy w taki sposób, aby zapewnić bezpieczeństwo, poufność i zgodność z prawem.

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

1. Definicje stosowane w niniejszej Polityce prywatności

Administrator danych / WEB3 Technology / „my”	„RGLTD” to nazwa handlowa spółki WEB3 Technology B.V., spółki zarejestrowanej w Holandii, posiadającej licencję AFM jako dostawca usług w zakresie kryptoaktywów, nr rejestracji 41000022, z siedzibą pod adresem Prins Hendrikkade 21E, Amsterdam, 1012TL, Holandia numer LEI 724500YJVIN0Q94ZZG58 KVK: 95206604.
Dane osobowe	Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgodnie z definicją zawartą w art. 4 ust. 1 RODO.
Polityka	Niniejsza Polityka prywatności.
Polityka dotycząca plików cookie	Polityka dotycząca plików cookie obowiązująca na stronie internetowej rqltd.com

Warunki korzystania z usługi	Warunki korzystania z usług WEB3 Technology są dostępne na stronie internetowej rgltd.com
RODO	Rozporządzenie (UE) 2016/679 Parlamentu Europejskiego i Rady 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 uchyłające dyrektywę 95/46/WE.
Rozporządzenie w sprawie rynków kryptoaktywów (MiCA)	Jako licencjonowany CASP zgodnie z MiCA podlegamy obowiązkom w zakresie prowadzenia dokumentacji, komunikacji z klientami, rozpatrywania skarg oraz sprawozdawczości, które wymagają przetwarzania danych osobowych. W przypadkach, gdy takie przetwarzanie jest wymagane przez MiCA, podstawą prawną jest art. 6 ust. 1 lit. c) RODO (wykonanie obowiązku prawnego).
EOG	Europejski Obszar Gospodarczy.
Strona internetowa	Serwis internetowy prowadzony przez Administratora danych pod adresem rgltd.com
Użytkownik	Każda osoba fizyczna odwiedzająca Stronę internetową lub korzystająca z jednej lub kilku usług dostępnych za pośrednictwem Strony internetowej, w tym – w przypadku gdy z usług korzysta osoba prawna lub korzysta z nich w jej imieniu – każda osoba fizyczna pełniąca funkcję upoważnionego przedstawiciela, beneficjenta rzeczywistego, dyrektora lub innej osoby kontaktowej takiej osoby prawnej, której dane osobowe są przetwarzane w związku ze świadczeniem usług przez Administratora.
Podmiot przetwarzający	Osoba fizyczna lub prawna, organ publiczny, agencja lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora, zgodnie z definicją zawartą w art. 4 ust. 8 RODO.

Strona trzecia Osoba fizyczna lub prawna, organ publiczny, agencja lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający oraz osoby, które pod bezpośrednim nadzorem Administratora lub Podmiotu przetwarzającego, są upoważnione do przetwarzania danych osobowych, zgodnie z definicją zawartą w art. 4 ust. 10 RODO.

Wszelkie inne terminy pisane wielką literą w niniejszej Polityce mają znaczenie nadane im w Warunkach korzystania z serwisu rgltd.com

2. Kto przetwarza Państwa dane osobowe?

Administratorem Państwa danych osobowych jest spółka **WEB3 Technology B.V.** z siedzibą pod adresem Prins Hendrikkade 21E, 1012 TL Amsterdam, Holandia, zarejestrowana 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, Holandia) lub pocztą elektroniczną na adres dpo@rgltd.com

Aby zwiększyć ochronę Państwa danych osobowych, wyznaczyliśmy wewnętrznego inspektora ochrony danych. Jest to osoba, z którą mogą Państwo się skontaktować, jeśli mają Państwo jakiegokolwiek pytania dotyczące sposobu przetwarzania Państwa danych, chcą Państwo skorzystać ze swoich praw lub potrzebują Państwo wyjaśnień w innych sprawach związanych z przetwarzaniem Państwa danych osobowych.

W tym celu można wysłać wiadomość e-mail na adres dpo@rgltd.com lub list na następujący adres: Inspektor Ochrony Danych · WEB3 Technology B.V. · Prins Hendrikkade 21E · 1012 TL Amsterdam · Holandia.

3. Dane osobowe osób poniżej 18 roku życia

Nasze usługi są przeznaczone dla osób, które ukończyły co najmniej 18 lat. Administrator nie przetwarza świadomie danych osobowych osób niepełnoletnich. W ramach procesu rejestracji wiek każdego Użytkownika jest weryfikowany poprzez

nasze obowiązkowe procedury weryfikacji tożsamości (KYC), które obejmują gromadzenie i weryfikację oficjalne dokumenty tożsamości, takie jak paszport lub dowód osobisty. Jeżeli w trakcie weryfikacji tożsamości okaże się, że dana osoba nie ukończyła 18 lat, rejestracja zostanie odrzucona, a wszelkie już zebrane dane osobowe zostaną usunięte bez zbędnej zwłoki.

Jeśli pomimo tych środków dowiemy się, że przekazano nam dane osobowe osoby poniżej 18 roku życia, dane te zostaną usunięte bez zbędnej zwłoki. Jeśli podejrzewają Państwo, że mogliśmy otrzymać takie dane, prosimy o kontakt z Administratorem danych 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:

- wypełnianie formularza kontaktowego na Stronie internetowej,
- zapisanie się do newslettera,
- przekazywanie danych w celu przygotowania, zawarcia lub wykonania umowy z Administratorem, w tym korzystania z jego usług,
- przysyłanie dokumentów aplikacyjnych (np. CV) w ramach procesów rekrutacyjnych,
- przekazywanie danych w ramach procedur weryfikacji Użytkowników (KYC – Know Your Customer lub KYB – Know Your Business) przeprowadzanych zgodnie z obowiązującymi przepisami dotyczącymi przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, w tym holenderskiej ustawy o zapobieganiu praniu pieniędzy i finansowaniu terroryzmu (Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft), a także obowiązujących unijnych rozporządzeń i środków wykonawczych w zakresie AML/CFT.

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. pracodawca, partner biznesowy lub podmiot zlecający usługę),
- od dostawców usług płatniczych, instytucji finansowych lub innych dostawców usług niezbędnych, z publicznie dostępnych rejestrów i baz danych, takich jak: izby handlowe, rejestry rzeczywistych właścicieli/rejestry przejrzystości, rejestry przedsiębiorstw, oficjalne listy sankcji oraz publicznie dostępne i wiarygodne źródła internetowe (np. wyszukiwarki) — w tym za pośrednictwem zewnętrznych dostawców usług weryfikacyjnych,
 - z publicznie dostępnych sieci blockchain, w tym znaczników czasu transakcji, identyfikatorów transakcji, podpisów cyfrowych, kwot transakcji i adresów portfeli, w przypadku gdy dane te są przetwarzane w celu realizacji transakcji, zapewnienia bezpieczeństwa, zapobiegania oszustwom oraz wypełniania obowiązujących zobowiązań prawnych,
- od dostawców usług technicznych i operacyjnych, którzy dostarczają informacje dotyczące transakcji lub statusu operacji.

Administrator danych 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 gromadzone automatycznie, w tym: informacje o sposobie korzystania z usług (takie jak adres IP, data i godzina wizyty, przeglądane Strony internetowej i kliknięte linki), informacje techniczne dotyczące urządzenia i oprogramowania (np. typ przeglądarki, system operacyjny, ustawienia językowe), a także informacje gromadzone za pomocą plików cookie i podobnych technologii (szczegółowe zasady ich stosowania opisano w Polityce plików cookie).

Możemy również gromadzić informacje o tym, w jaki sposób Użytkownicy wchodzą w interakcję z naszą Stroną internetową i Usługami, w tym dane dotyczące korzystania ze Strony internetowej, dane dotyczące interakcji oraz, w stosownych przypadkach, informacje o przedziale wieowym.

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 Państwa dane osobowe

Korzystanie ze Strony internetowej i aplikacji (bez zakładania konta)	Adres IP, inne identyfikatory oraz informacje gromadzone za pomocą plików cookie i podobnych technologii	Przetwarzamy te dane, aby umożliwić Państwu korzystanie ze Strony internetowej, w oparciu o prawnie uzasadniony interes administratora (art. 6 ust. 1 lit. f) RODO), polegający na zapewnieniu prawidłowego funkcjonowania Strony internetowej.	Przetwarzamy dane przez cały okres korzystania przez Państwa ze Strony internetowej.
Marketing oparty na zgodzie (potencjalni klienci/newslettery)	Imię, nazwisko, adres e-mail	Przetwarzamy dane w celu wysyłania komunikatów marketingowych, biuletynów i treści promocyjnych na podstawie zgody użytkownika (art. 6 ust. 1 lit. a) RODO), art. 11 ust. 7 holenderskiej ustawy o telekomunikacji (Telecommunicatiewet), która wdraża dyrektywę o prywatności i łączności elektronicznej (2002/58/WE) w Holandii oraz zgodnie z obowiązującymi przepisami dotyczącymi łączności elektronicznej.	W każdej chwili mogą Państwo wycofać swoją zgodę, bez wpływu na zgodność z prawem przetwarzania, które miało miejsce przed jej wycofaniem.
Komunikaty marketingowe skierowane do obecnych klientów (podobne produkty i usług)	Imię, nazwisko, adres e-mail	Przetwarzamy dane w celu promowania naszych własnych, podobnych produktów lub usług wśród obecnych klientów na podstawie prawnie uzasadnionego interesu administratora (art. 6 ust. 1 lit. f) RODO), zgodnie z obowiązującymi przepisami dotyczącymi łączności elektronicznej. Użytkownicy mogą w dowolnym momencie zgłosić sprzeciw wobec takiego przetwarzania.	W każdej chwili mogą Państwo wnieść sprzeciw wobec takiego przetwarzania, korzystając z mechanizmu rezygnacji z subskrypcji zawartego w każdej wiadomości marketingowej lub skontaktowanie się z nami bezpośrednio.
Tworzenie konta Użytkownika na Stronie internetowej i zarządzanie nim	Imię, nazwisko, adres e-mail, numer telefonu	Przetwarzamy dane w celu świadczenia usług związanych z tworzeniem, zarządzaniem i obsługą kont Użytkowników na Stronie internetowej, na podstawie konieczności wykonania umowy (art. 6 ust. 1 lit. b) RODO), a także w celu ustalenia, dochodzenia lub obrony roszczeń prawnych, 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 okres obowiązywania umowy, a następnie przez okres do 6 lat, zgodnie z obowiązującymi wymogami prawnymi i w związku z ewentualnymi roszczeniami.
Formularz kontaktowy	Dane niezbędne do nawiązania kontaktu, w tym: imię, nazwisko, adres e-mail, numer telefonu	Dane są przetwarzane w celu identyfikacji nadawcy i rozpatrzenia jego zapytania; podstawą prawną przetwarzania jest konieczność wykonania umowy (art. 6 ust. 1 lit. b) RODO). Jeśli 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 prawo oraz przez okres do 6 lat w celu zabezpieczenia ewentualnych roszczeń.

			Dane przetwarzane na podstawie zgody są przechowywane do momentu wycofania zgody.
--	--	--	---

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. paszport, karta identyfikacyjna, prawo jazdy, obraz uzyskany ze zdjęcia lub nagrania wideo przedłożonego podczas weryfikacji, informacje biometryczne wygenerowane na podstawie takich obrazów, w tym geometrię twarzy wynioskowaną ze zdjęcia/nagrania, przetwarzane wyłącznie w celu jednoznacznej identyfikacji i weryfikacji tożsamości (elektroniczna weryfikacja tożsamości – EIDV), informacje o źródłach pochodzenia środków, źródła majątku, sytuacji finansowej, danych dotyczących weryfikacji dochodów i/lub aktywów, doświadczenia w zakresie handlu i inwestycji, danych logowania oraz danych transakcyjnych. W przypadku Użytkowników biznesowych: dane firmy, numer identyfikacji podatkowej, numery z rejestru przedsiębiorstw ,oraz dane dotyczące dyrektorów i beneficjentów rzeczywistych.	Przetwarzamy te dane w celu wypełnienia obowiązków prawnych wynikających z przepisów dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, w celu 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 uzasadniony interes (art. 6 ust. 1 lit. f) RODO), polegający na ochronie przed oszustwami i zapewnieniu bezpieczeństwa transakcji.	Przetwarzamy dane przez cały okres trwania relacji usługowej, a po jej zakończeniu przez kolejne 5 lat zgodnie z przepisami dotyczącymi przeciwdziałania praniu pieniędzy, a także przez okres niezbędny do ustalenia, dochodzenia lub obrony roszczeń prawnych — do 6 lat.
--	---	---	--

Realizacja transakcji, księgowość i transfer środków lub kryptoaktywów	Dane identyfikacyjne (imię, nazwisko, adres e-mail, numer telefonu), dane transakcyjne (w tym adresy portfeli podane przez Użytkownika oraz powiązane informacje o trasie transakcji), identyfikatory transakcji, hashe, historia transakcji, dane nadawcy i odbiorcy, kwota transakcji, preferencje walutowe, metoda płatności, data i/lub znacznik czasu) oraz dane dotyczące płatności (np. informacje dotyczące metod płatności, numer rachunku bankowego, dane karty płatniczej (takie jak PAN) oraz szczegóły rozliczenia)	Przetwarzamy dane w celu realizacji transakcji, ich prawidłowego rejestrowania oraz obsługi rozliczeń finansowych. Podstawą prawną przetwarzania jest wykonanie umowy (art. 6 ust. 1 lit. b) RODO). W celu wypełnienia obowiązków księgowych, podatkowych i związanych z przeciwdziałaniem praniu pieniędzy podstawą prawną jest wypełnienie obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c) RODO). W celu ustalenia, dochodzenia lub obrony roszczeń prawnych przetwarzamy dane w oparciu o nasz uzasadniony interes (art. 6 ust. 1 lit. f) RODO), polegający na ochronie praw administratora oraz zapewnieniu bezpieczeństwa transakcji.	Przechowujemy dane przez okres wymagany przepisami podatkowymi — 5 lat od zakończenia roku podatkowego — oraz przez dodatkowe 5 lat zgodnie z obowiązkami w zakresie przeciwdziałania praniu pieniędzy. Na potrzeby roszczeń prawnych dane mogą być przetwarzane przez dodatkowy okres do 6 lat zgodnie z obowiązującymi terminów przedawnienia.
Zapewnienie bezpieczeństwa, ochrony oraz integralności Usług (oszustwa zapobiegania oszustwom i wykrywania nadużyć)	Dane identyfikacyjne (takie jak imię, nazwisko, adres e-mail, numer telefonu i identyfikatory konta), 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 prowadzenia dochodzeń w sprawie oszustw, nadużyć, zachowań niezgodnych z prawem, naruszeń naszych zasad lub Warunków oraz innych zagrożeń dla 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 oraz zapobieganiu nadużyciom w zakresie korzystania z Usług. W stosownych przypadkach przetwarzanie może również odbywać się w celu wypełnienia obowiązków prawnych (art. 6 ust. 1 lit. c) RODO), w szczególności wynikających z przepisów dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/CFT).	Dane są przetwarzane przez cały czas trwania relacji usługowej, a następnie przez okres niezbędny do wypełnienia obowiązków prawnych oraz do ustalenia, dochodzenia lub obrony roszczeń prawnych, zgodnie z obowiązującymi terminami przedawnienia.

Obsługa klienta i komunikacja	Dane identyfikacyjne i kontaktowe (takie jak imię, nazwisko, adres e-mail, adres, numer telefonu oraz identyfikatory konta Użytkownika), dane dotyczące komunikacji, w tym , informacje przekazane zespołom obsługi klienta lub zespołom zajmującym się badaniami Użytkowników, interakcje z chatbotami oraz, w stosownych przypadkach, nagrania rozmów	Przetwarzamy dane w celu zapewnienia obsługi klienta, odpowiadania na zapytania, rozpatrywania skarg oraz poprawy jakości i funkcjonalności naszych Usług. Podstawą prawną przetwarzania jest konieczność 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.	Dane są przetwarzane przez okres niezbędny do rozpatrzenia zapytania lub zgłoszenia pomocy, a następnie przez okres wymagany przez obowiązujące prawo lub w celu ustalenie, dochodzenie lub obronę roszczeń prawnych 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 rekrutacyjnego (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 konieczność podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy (art. 6 ust. 1 lit. b) RODO), wypełnienie obowiązków prawnych wynikających z obowiązujących przepisów prawa pracy (art. 6 ust. 1 lit. c) RODO) oraz prawnie uzasadniony interes administratora (art. 6 ust. 1 lit. f) RODO), polegający na prowadzeniu rekrutacji procesów rekrutacyjnych i wyboru odpowiednich kandydatów – zgoda (art. 6 ust. 1 lit. a) RODO), w przypadku gdy kandydat dobrowolnie przekazuje dodatkowe dane, które nie są wymagane przez prawo, lub zgłasza się do udziału w przyszłych procesach rekrutacyjnych.	Dane są przetwarzane przez cały czas trwania procesu rekrutacyjnego, a następnie przez okres niezbędny do sfinalizowania rekrutacji i rozpatrzenia wszelkich związanych z nią roszczeń. Jeśli kandydat wyraził zgodę na udział w przyszłych procesach rekrutacyjnych, dane mogą być przetwarzane przez okres jednego roku.
Zgodność z obowiązkowymi zobowiązaniami w zakresie sprawozdawczości podatkowej wynikającymi z DAC8 (dyrektywa Rady 2023/2226/UE) oraz Ramami Sprawozdawczości w zakresie Kryptoaktywów (CARF)	Pełne imię i nazwisko, data urodzenia, adres zamieszkania, kraj(e) rezydencji podatkowej, numer(y) identyfikacji podatkowej (TIN), łączne wartości transakcji według rodzaju kryptoaktywa w roku kalendarzowym, identyfikatory portfeli	art. 6 ust. 1 lit. c) RODO — wypełnienie obowiązku prawnego. Odbiorcą danych jest holenderska administracja podatkowo-celna (Belastingdienst) oraz, w stosownych przypadkach, właściwe organy podatkowe państw członkowskich UE w ramach automatycznej wymiany informacji.	7 lat od zakończenia roku sprawozdawczego, w którym dane zostały zebrane, zgodnie z holenderskimi wymogami dotyczącymi okresu przechowywania danych podatkowych.
Zgodność z rozporządzeniem w sprawie transferu środków (TFR) — obowiązkowa wymiana danych inicjatorzy i beneficjenci podczas przelewów kryptoaktywów w celu wykrywania i zapobiegania praniu pieniędzy i finansowaniu terroryzmu	Pełne imię i nazwisko, identyfikator konta kryptoaktywów (adres portfela), numer referencyjny transakcji oraz, w razie potrzeby: adres zamieszkania, numer identyfikacyjny lub data i miejsce urodzenia inicjatorzy i/lub beneficjenci	art. 6 ust. 1 lit. c) RODO — wypełnienie obowiązku prawnego wynikającego z rozporządzenia (UE) 2023/1113. W przypadku gdy odbiorcami są kontrahenci będący dostawcami usług w zakresie kryptoaktywów (CASPs) oraz usługodawców kryptoaktywów zaangażowanych w przelew, zgodnie z wymogami prawa.	5 lat od daty przelewu, zgodnie z art. 21 rozporządzenia (UE) 2023/1113.

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

Zasadniczo nie przetwarzamy szczególnych kategorii danych osobowych (takich jak dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne, dane dotyczące zdrowia lub orientacji seksualnej). Jednakże w celu weryfikacji tożsamości (KYC) przetwarzamy dane biometryczne (geometrię twarzy uzyskaną ze zdjęć lub filmów) wyłącznie w celu potwierdzenia tożsamości Użytkownika oraz zapobiegania oszustwom. Przetwarzanie to odbywa się w celu wypełnienia obowiązków prawnych wynikających z obowiązujących przepisów dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (art. 6 ust. 1 lit. c) RODO), w połączeniu z art. 9 ust. 2 lit. g) RODO (przetwarzanie niezbędne ze względu na istotny interes publiczny), zgodnie z dalszymi szczegółowymi przepisami obowiązującego unijnego i krajowego prawa w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. W przypadkach wymaganych przez obowiązujące prawo przetwarzanie to może również opierać się na art. 9 ust. 2 lit. a) RODO (wyrażna zgoda), uzyskana w trakcie procesu weryfikacji.

Dane biometryczne są przetwarzane wyłącznie w zakresie ściśle niezbędnym do weryfikacji tożsamości, nie są wykorzystywane do żadnych innych celów i nie podlegają dalszemu przetwarzaniu wykraczającemu poza weryfikację tożsamości i zapobieganie oszustwom, a także podlegają wzmocnionym środkom bezpieczeństwa. W przypadku gdy szczególne kategorie danych osobowych są przypadkowo zawarte w danych transakcyjnych lub innych informacjach przekazanych przez Użytkowników, dane te nie są aktywnie wykorzystywane ani analizowane przez Administratora w żadnym konkretnym celu.

W przypadku gdy przetwarzanie opiera się na prawnie uzasadnionym interesie Administratora, przeprowadziliśmy test wyważenia interesów, aby zapewnić, że prawa i wolności osoby, której dane dotyczą, nie mają pierwszeństwa przed tymi interesami.

W przypadku gdy do tego samego zbioru danych ma zastosowanie więcej niż jeden okres przechowywania (na przykład dokumentacja dotycząca przeciwdziałania praniu pieniędzy podlegająca 5-letniemu okresowi przechowywania zgodnie z ustawą Wwft oraz dokumentacja mająca również znaczenie dla toczących się postępowań cywilnych, podlegająca 6-letniemu okresowi przedawnienia), przechowujemy dane przez dłuższy z obowiązujących okresów. Okresy przechowywania rozpoczynają się od zakończenia relacji biznesowej lub od daty odpowiedniej transakcji, w zależności od tego, która z tych dat jest późniejsza, o ile nie określono inaczej powyżej.

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

6.1 Podmioty przetwarzające dane w naszym imieniu

W związku ze świadczeniem naszych usług Państwa dane osobowe mogą zostać ujawnione stronom trzecim. Takie ujawnienie ma miejsce wyłącznie wtedy, gdy jest to konieczne do osiągnięcia określonego celu, zgodnie z RODO, na podstawie odpowiednich umów oraz przy zastosowaniu odpowiednich środków bezpieczeństwa.

Współpracujemy z zaufanymi dostawcami usług, którzy wspierają nas w technicznej i operacyjnej realizacji naszych usług. Mogą to być w szczególności: dostawcy usług informatycznych, hostingowych i z zakresu cyberbezpieczeństwa; dostawcy oprogramowania i narzędzi wykorzystywanych do obsługi Użytkowników; firmy księgowe; kancelarie prawne; firmy audytorskie; dostawcy usług w chmurze, poczty elektronicznej, archiwizacji i analityki; a także podmioty wspierające procesy operacyjne i administracyjne.

Każdy podmiot przetwarzający działa wyłącznie zgodnie z naszymi instrukcjami oraz na podstawie umowy o przetwarzaniu danych, która określa środki techniczne i organizacyjne służące ochronie danych.

6.2 Podmioty przetwarzające dane na własne potrzeby (niezależni Administratorzy)

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

- podmioty należące do grupy kapitałowej Administratora, w przypadku gdy takie ujawnienie jest niezbędne do wewnętrznych celów administracyjnych, wypełnienia obowiązków prawnych (w tym w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu), zarządzania ryzykiem lub świadczenia usług; podmioty te działają jako niezależni administratorzy lub podmioty przetwarzające, w zależności od kontekstu przetwarzania,
- podmioty dostarczające kluczowe systemy informatyczne lub infrastrukturę wykorzystywaną do świadczenia naszych usług (współadministratorzy w odniesieniu do konkretnego systemu),
- organy nadzorcze i instytucje publiczne, w przypadku gdy ujawnienie jest wymagane przez prawo (w tym między innymi holenderski Urząd ds. Rynków Finansowych – AFM, DNB oraz Jednostka Wywiadu Finansowego – Holandia (FIU-NL) oraz inne organy ścigania i organy podatkowe),

- Holenderska Administracja Podatkowa i Celna (Belastingdienst) — niektóre dane osobowe i transakcyjne naszych Użytkowników będą przekazywane 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 do żadnych innych celów,
- kontrahenci świadczący usługi w zakresie kryptoaktywów (zasada „Travel Rule”) — zgodnie z prawem jesteśmy zobowiązani do przekazywania danych osobowych inicjatora i beneficjenta do przyjmującego dostawcy usług w zakresie kryptoaktywów (CASP) podczas przetwarzania przelewów kryptoaktywów powyżej obowiązujących progów, a w niektórych przypadkach niezależnie od progu. Udostępnianie tych danych jest obowiązkowe i nie można się z niego wycofać,
- instytucje finansowe i operatorzy kart płatniczych (np. Mastercard, Visa) w związku z przetwarzaniem płatności,
- podmioty zajmujące się audytem lub kontrolą,
- kancelarie prawne i profesjonalni doradcy w kontekście postępowań sądowych,
- podmioty zaangażowane w procesy korporacyjne (np. transakcje przejęcia lub restrukturyzacji), w przypadku gdy ujawnienie danych jest niezbędne do zawarcia lub wykonania umowy.

W takich przypadkach każdy z tych podmiotów jest odpowiedzialny za przetwarzanie danych zgodnie z własną polityką prywatności oraz obowiązującymi ramami prawnymi.

6.3 Sztuczna inteligencja (AI)

W ramach naszych procesów operacyjnych korzystamy z narzędzi opartych na sztucznej inteligencji w celu wspierania określonych funkcji, takich jak:

- Weryfikacja tożsamości i porównanie danych biometrycznych (np. wykrywanie żywości, uwierzytelnianie dokumentów) — zapewniane przez certyfikowanych zewnętrznych dostawców usług KYC/IDV działających na podstawie DPA i SCC • Monitorowanie transakcji i ocena ryzyka AML — zautomatyzowane systemy oparte na regułach i uczeniu maszynowym, służące do wykrywania nietypowych wzorców i generowania alertów do weryfikacji przez człowieka
- Sprawdzanie sankcji i osób zajmujących eksponowane stanowiska polityczne (PEP) — automatyczne porównywanie z listami sankcyjnymi (UE, ONZ, OFAC) oraz bazami danych osób zajmujących eksponowane stanowiska polityczne
- Wsparcie obsługi klienta — narzędzia do wstępnej klasyfikacji i reagowania wspomagane przez sztuczną inteligencję, w ramach których zapytania dotyczące danych osobowych są przekazywane do konsultacji z pracownikami

Żadna w pełni zautomatyzowana decyzja o skutkach prawnych lub o podobnym znaczeniu nie jest podejmowana bez możliwości przeprowadzenia weryfikacji przez człowieka na żądanie. W przypadku gdy systemy automatyczne powodują ograniczenie konta lub blokadę transakcji, przed podjęciem ostatecznej decyzji sprawę weryfikuje pracownik ds. zgodności.

W przypadku przetwarzania danych osobowych przez narzędzia oparte na sztucznej inteligencji przetwarzanie to odbywa się zgodnie z niniejszą Polityką prywatności oraz obowiązującymi przepisami o ochronie danych.

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

6.4 Współadministrowanie danymi (media społecznościowe)

Gdy kontaktujesz się z administratorem danych za pośrednictwem platform mediów społecznościowych (np. Instagram, LinkedIn), dane osobowe, których to dotyczy, są przetwarzane wspólnie przez nas i właścicieli tych platform. Wspólnie określamy cele i sposoby przetwarzania, a Użytkownik ma prawo do wykonywania swoich praw wynikających z RODO zarówno wobec nas, jak i operatora platformy. Więcej szczegółów można znaleźć w politykach prywatności poszczególnych serwisów społecznościowych.

Chociaż firma WEB3 Technology i platformy mediów społecznościowych (lub główni dostawcy systemów informatycznych) wspólnie określają cele i sposoby przetwarzania, to przede wszystkim my zajmujemy się realizacją praw Użytkownika jako osoby, której dane dotyczą. Użytkownik może jednak dochodzić swoich praw wobec każdej ze stron.

Aktualna lista naszych podmiotów przetwarzających dane i podwykonawców przetwarzania danych, zawierająca ich nazwy, kraje siedziby oraz cele przetwarzania, jest dostępna na żądanie wysłane pocztą **elektroniczną na adres dpo@rgltd.com**. W przypadku konieczności wynikającej z naszych zobowiązań wynikających z umowy o przetwarzaniu danych (DPA) będziemy z wyprzedzeniem powiadamiać Użytkowników o wszelkich istotnych zmianach w naszej liście podwykonawców przetwarzania danych.

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

Twoje dane osobowe przetwarzamy głównie w Europejskim Obszarze Gospodarczym (EOG). Jednak w przypadku określonych usług (np. weryfikacji tożsamości lub infrastruktury technicznej) możemy przekazywać dane osobowe zaufanym partnerom spoza EOG („państwa trzecie”).

Przekazujemy Państwa dane do państwa trzeciego wyłącznie wtedy, gdy zastosowano jedno z poniższych zabezpieczeń:

Decyzja o adekwatności

Kraj ten został uznany przez Komisję Europejską za zapewniający odpowiedni poziom ochrony danych (np. ramy ochrony danych UE–USA dla certyfikowanych podmiotów amerykańskich).

Standardowe klauzule umowne (SCC) i środki uzupełniające

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

W razie potrzeby wdrażamy dodatkowe środki techniczne, organizacyjne i umowne (takie jak szyfrowanie, ograniczenia dostępu i minimalizacja danych), aby zapewnić ochronę danych osobowych na poziomie zasadniczo równoważnym z poziomem gwarantowanym w EOG.

Oceniamy przekazywanie danych indywidualnie dla każdego przypadku, a w sytuacji, gdy nie można zapewnić odpowiedniego poziomu ochrony, powstrzymujemy się od przekazywania danych osobowych do danego państwa trzeciego.

Możesz poprosić o kopię konkretnych zabezpieczeń stosowanych w odniesieniu do Twoich danych, kontaktując się z nami pod adresem dpo@rgltd.com

8. Czy podanie danych osobowych jest dobrowolne?

Podanie danych osobowych jest dobrowolne; jednakże niektóre dane są niezbędne do świadczenia usług oferowanych za pośrednictwem naszej Strony internetowej i aplikacji, np. dane wymagane do zapewnienia zgodności z wymogami KYC/AML oraz do wykonania umowy są obowiązkowe. Niepodanie takich danych może uniemożliwić Państwu korzystanie z określonych funkcji lub zawarcie lub wykonanie umowy z nami.

Dane oznaczone jako opcjonalne można podać według własnego uznania, a rezygnacja z ich podania nie wpływa na możliwość korzystania z podstawowych usług. Zawsze masz prawo zdecydować, które dane chcesz ujawnić.

Jeśli dobrowolnie wyrażą Państwo zgodę na przetwarzanie swoich danych osobowych w określonych celach (np. marketingowych), mogą Państwo wycofać tę zgodę w dowolnym momencie. Wycofanie zgody nie ma wpływu na zgodność z prawem przetwarzania, które miało miejsce na podstawie zgody przed jej wycofaniem. Nie powoduje ono również utraty dostępu do usług ani innych praw, chyba że ich realizacja wymaga dalszego przetwarzania danych, których to dotyczy.

Podanie niektórych danych osobowych może stanowić wymóg prawny lub umowny, w szczególności wynikający z przepisów dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/CFT). Niepodanie takich danych może skutkować niemożnością nawiązania lub kontynuowania relacji biznesowej lub realizacji transakcji.

9. Czy Państwa dane osobowe podlegają profilowaniu?

Dane osobowe Użytkowników mogą podlegać profilowaniu, rozumianemu jako zautomatyzowane przetwarzanie określonych informacji o Użytkowniku w celu oceny wybranych czynników związanych z jego aktywnością, wiarygodnością lub ryzykiem związanym z korzystaniem z usług. Profilowanie odbywa się w szczególności w celu wypełnienia obowiązków wynikających z przepisów dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML), zapewnienia bezpieczeństwa usług oraz zapobiegania oszustwom.

W przypadku gdy zautomatyzowane przetwarzanie, w tym profilowanie, generuje wynik, który może prowadzić do podjęcia decyzji o skutkach prawnych lub o podobnym znaczeniu (np. odrzucenie wniosku KYC), wynik ten podlega obowiązkowej weryfikacji przez osobę fizyczną przed podjęciem ostatecznej decyzji; osoba, której dane dotyczą, ma prawo zażądać weryfikacji przez osobę fizyczną, zakwestionować decyzję oraz wyrazić swoje stanowisko.

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

Jeśli w trakcie korzystania z usług Użytkownik spełni określone kryteria lub uzyska wynik wskazujący na niższy poziom ryzyka (np. w ramach oceny AML), może to skutkować uzyskaniem dostępu do określonych funkcji.

W szczególności wyniki automatycznych kontroli przeprowadzanych podczas procesu weryfikacji tożsamości za pomocą wideo i danych biometrycznych (KYC), w tym mechanizmów rozpoznawania twarzy i wykrywania żywności, są wykorzystywane wyłącznie jako informacje pomocnicze. Każda odmowa rejestracji Użytkownika lub jakiegokolwiek ograniczenie dostępu do Usług na podstawie takich wyników (w tym wyników automatycznej weryfikacji biometrycznej) podlega merytorycznej weryfikacji przez osobę fizyczną i zatwierdzeniu, zanim wywoła jakiegokolwiek skutki prawne lub równie istotne, zgodnie z art. 22 RODO.

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

Proces profilowania może uwzględniać czynniki ogólnego charakteru wymagane na mocy obowiązujących przepisów dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/CFT) oraz standardowych praktyk w zakresie zapobiegania oszustwom, w tym publicznie dostępne dane z łańcucha bloków (takie jak znaczniki czasu transakcji, identyfikatory transakcji, podpisy cyfrowe, kwoty transakcji i adresy portfeli). Mogą one obejmować na przykład to, czy transakcja przekracza progi określone przepisami prawa, częstotliwość lub charakter transakcji, niespójności geograficzne lub behawioralne, status weryfikacji tożsamości Użytkownika, a także informacje dotyczące interakcji Użytkownika ze Stroną internetową lub Usługami (takie jak dane dotyczące Użytkownika, dane dotyczące interakcji lub odpowiedzi na ankiety, w tym te zebrane przed utworzeniem konta). Wskaźniki te są wykorzystywane wyłącznie do oceny ryzyka i zapewnienia zgodności z obowiązkami prawnymi; nie wiążą się one z ujawnieniem zastrzeżonych modeli ryzyka ani szczegółowej wewnętrznej logiki wykrywania oszustw.

10. Jakie prawa przysługują Państwu w związku z przetwarzaniem przez nas Państwa danych osobowych?

Prawo dostępu	Mają Państwo prawo wiedzieć, które z Państwa danych osobowych przetwarzamy, w jakich celach, oraz uzyskać kopię tych danych.
Prawo do przenoszenia danych	Mają Państwo prawo do otrzymania swoich danych osobowych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, umożliwiającym przekazanie tych danych innemu administratorowi.
Prawo do sprostowania	Jeśli Twoje dane są nieprawidłowe lub niekompletne, masz prawo do ich sprostowania lub uzupełnienia. Jeśli posiadasz konto Użytkownika, możesz samodzielnie zaktualizować niektóre dane.
Prawo do ograniczenia przetwarzania / prawo do bycia zapomnianym	Masz prawo zażądać ograniczenia przetwarzania lub usunięcia swoich danych osobowych, chyba że jesteśmy zobowiązani do dalszego przetwarzania tych danych ze względu na obowiązujące wymogi prawne lub w celu ustalenia, dochodzenia lub obrony roszczeń prawnych.

Prawo do wycofania zgody	W każdej chwili możesz wycofać swoją zgodę na przetwarzanie danych osobowych. Wycofanie zgody nie ma wpływu na zgodność z prawem przetwarzania, które miało miejsce przed wycofaniem zgody.
Prawo do wniesienia sprzeciwu	W przypadku gdy Państwa dane osobowe są przetwarzane na podstawie prawnie uzasadnionych interesów administratora lub w celach marketingu bezpośredniego, mają Państwo również prawo do wniesienia sprzeciwu wobec takiego przetwarzania.
Prawo do weryfikacji zautomatyzowanych decyzji przez człowieka	W przypadku gdy podejmujemy decyzje dotyczące Państwa wyłącznie w sposób zautomatyzowany — w tym automatyczne odrzucenie wniosku w ramach procedury KYC, ocena ryzyka lub ograniczenia konta wynikające z przepisów AML — które wywołują skutki prawne lub skutki o podobnym znaczeniu, masz prawo do: (i) zwrócenia się z prośbą o weryfikację decyzji przez członka naszego zespołu; (ii) wyrażenia swojego stanowiska w sprawie zautomatyzowanej decyzji; oraz (iii) zakwestionowania decyzji.

Aby skorzystać z któregośkolwiek z wyżej wymienionych praw, prosimy o przesłanie pisemnego wniosku na adres: **dpo@rgltdcom**

Odpowiemy na Państwa wniosek w ciągu jednego miesiąca kalendarzowego od jego otrzymania. W przypadku złożoności sprawy lub dużej liczby wniosków możemy przedłużyć ten termin o kolejne dwa miesiące; w takim przypadku poinformujemy Państwa o tym w ciągu pierwszego miesiąca i wyjaśnimy powód przedłużenia (art. 12 ust. 3 RODO).

Rozpatrzenie Państwa wniosku jest bezpłatne. Jednakże w przypadku wniosków ewidentnie bezzasadnych lub nadmiernych, w szczególności ze względu na ich powtarzalny charakter, możemy albo pobrać rozsądną opłatę administracyjną, albo odmówić rozpatrzenia wniosku (art. 12 ust. 5 RODO).

W celu ochrony Państwa danych przed rozpatrzeniem każdego wniosku o dostęp do danych (DSAR) zweryfikujemy Państwa tożsamość. W tym celu możemy poprosić o kopię dokumentu tożsamości wydanego przez organ państwowy lub skorzystać z naszych istniejących danych weryfikacyjnych KYC. Dane służące do weryfikacji tożsamości, przekazane wyłącznie na potrzeby wniosku DSAR, nie będą przechowywane dłużej niż jest to konieczne do rozpatrzenia Państwa wniosku.

Jeśli uważają Państwo, że Państwa dane osobowe są przetwarzane niezgodnie z prawem, mają Państwo prawo złożyć skargę do holenderskiego organu ochrony danych: Autoriteit Persoonsgegevens, Bezuidenhoutseweg 30, 2594 AV Den Haag, Holandia. Strona internetowa: www.autoriteitpersoonsgegevens.nl Telefon: +31 88 1805 250.

Ważne ograniczenie — dane w łańcuchu bloków: Należy pamiętać, że w przypadku, gdy Państwa dane osobowe zostały włączone do publicznego łańcucha bloków (na przykład adres portfela lub hash transakcji, który można powiązać z Państwem), technicznie nie jest możliwe usunięcie lub zmiana tych danych po ich potwierdzeniu w łańcuchu bloków. Jest to nieodłączne ograniczenie technologii rozproszonego rejestru, które pozostaje poza naszą kontrolą jako Administratora danych. W takich przypadkach usuniemy lub zanonimizujemy wszystkie powiązane zapisy poza łańcuchem (takie jak imię i nazwisko, adres e-mail oraz dane konta) w naszych systemach zgodnie z naszym harmonogramem przechowywania danych, a podczas rozpatrywania Państwa wniosku poinformujemy Państwa o ograniczeniu dotyczącym danych w łańcuchu bloków.

11. Jak chronimy i przechowujemy dane osobowe

Wdrażamy odpowiednie środki techniczne i organizacyjne w celu zapewnienia poziomu bezpieczeństwa odpowiedniego do ryzyka związanego z przetwarzaniem danych osobowych, zgodnie z art. 32 RODO. Środki te obejmują w szczególności:

- Ograniczenie dostępu do danych osobowych wyłącznie do upoważnionego personelu
- Minimalizację danych oraz kontrolę dostępu opartą na rolach
- Szyfrowanie danych w trakcie przesyłania i przechowywania
- Monitorowanie systemów i działań w celu zapewnienia bezpieczeństwa i zapobiegania oszustwom
- Regularne przeglądy bezpieczeństwa, audyty i testy systemów informatycznych
- Korzystanie z usług bezpiecznych, certyfikowanych dostawców usług, którzy spełniają standardy branżowe

Dane osobowe są przechowywane wyłącznie przez okresy wskazane w niniejszej Polityce prywatności i wyłącznie w bezpiecznych środowiskach, które zapewniają poufność, integralność i dostępność danych. Po upływie odpowiednich

, dane są nieodwracalnie usuwane lub anonimizowane.

11.1 Powiadamianie o naruszeniu ochrony danych

Stosujemy wewnętrzną procedurę identyfikacji, oceny i reagowania na naruszenia ochrony danych osobowych zgodnie z art. 33 i 34 RODO.

W przypadku naruszenia ochrony danych osobowych, które może stanowić zagrożenie dla praw i wolności osób fizycznych, bez zbędnej zwłoki powiadomimy o tym holenderski organ ochrony danych (Autoriteit Persoonsgegevens), a w miarę możliwości nie później niż 72 godziny po stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, aby naruszenie to spowodowało takie zagrożenie.

W przypadku gdy naruszenie może spowodować wysokie ryzyko dla Państwa praw i wolności — na przykład gdy dotyczy wrażliwych danych finansowych, dokumentów tożsamości lub danych biometrycznych — powiadomimy Państwa również bezpośrednio, bez zbędnej zwłoki, korzystając z danych kontaktowych podanych na Państwa koncie.

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

11.2 Dane zanonimizowane

W celu monitorowania i ograniczania oszustw oraz innych zagrożeń, poprawy jakości 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 konkretnej osoby. Dane takie są przetwarzane wyłącznie do celów analitycznych, statystycznych i związanych z bezpieczeństwem.

Proces anonimizacji ma na celu zapewnienie, że osoby fizyczne nie mogą zostać ponownie zidentyfikowane, ani bezpośrednio, ani pośrednio.

12. Pliki cookie

Zasady i rodzaje stosowanych plików cookie oraz podobnych technologii zostały określone w Polityce plików cookie. Szczegółowy opis stosowanych przez nas plików cookie i podobnych technologii można znaleźć na Stronie internetowej: rgltd.com

13. Zmiany w danych osobowych

Ważne jest, aby dane osobowe, które posiadamy na Państwa temat, były dokładne i aktualne. Prosimy o poinformowanie nas, jeśli Państwa dane osobowe ulegną zmianie lub jeśli zauważą Państwo, że jakiegokolwiek dane osobowe, które posiadamy, są nieprawidłowe.

14. Zmiany w Polityce

Niniejsza Polityka prywatności wchodzi w życie z dniem 05.05.2026 r.

Od czasu do czasu możemy modyfikować niniejszą Politykę prywatności, aby odzwierciedlić wszelkie zmiany w sposobie przetwarzania danych osobowych lub zmiany w przepisach dotyczących ochrony danych. W przypadku istotnych zmian w naszej polityce (tj. zmiany celów przetwarzania, zmiany tożsamości Administratora danych lub zmiany sposobu, w jaki mogą Państwo wykonywać swoje prawa w związku z naszym przetwarzaniem), informujemy Państwa o tym i opublikujemy nową wersję na naszej Stronie internetowej (www.rgltd.com). Prosimy o regularne sprawdzanie naszej Polityki prywatności, aby być na bieżąco z wszelkimi zmianami. Data podana na górze niniejszego oświadczenia wskazuje, kiedy zostało ono ostatnio zaktualizowane.

15. Oświadczenie dotyczące oceny skutków dla ochrony danych (DPIA)

Zgodnie z art. 35 RODO przeprowadzamy oceny skutków dla ochrony danych (DPIA) przed podjęciem czynności przetwarzania, które mogą stwarzać wysokie ryzyko dla praw i wolności osób fizycznych. Obejmuje to między innymi: przetwarzanie danych biometrycznych w celu weryfikacji tożsamości, systematyczne zautomatyzowane monitorowanie zachowań transakcyjnych do celów przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/CFT) oraz przetwarzanie na dużą skalę danych należących do kategorii szczególnych. Wyniki ocen wpływu na ochronę danych stanowią podstawę naszych środków technicznych i organizacyjnych oraz są dokumentowane w naszych wewnętrznych rejestrach czynności przetwarzania (RoPA) prowadzonych zgodnie z art. 30 RODO.

16. Historia wersji

1.0 120.10.2024	Inspektor ochrony danych / CRCO	Dokument bazowy — pierwsza publikacja. Zatwierdzony przez organ zarządzający
2.0 05.05.2026	IOD / CRCO	Zaktualizowano w celu uwzględnienia zobowiązań wynikających z DAC8 / CARF, zasady TFR Travel Rule, wykorzystania narzędzi AI, wspólnej kontroli, oświadczenia dotyczącego DPIA oraz ograniczeń dotyczących danych w łańcuchu bloków. Zatwierdzono przez organu zarządzającego.