

Informacja o ochronie prywatności Tools for Humanity

Dziękujemy za zostanie częścią społeczności World! World jest protokołem typu open source, wspieranym przez globalną społeczność programistów, osób prywatnych i innych twórców.

Niniejsza Informacja o ochronie prywatności ma zastosowanie do danych, które użytkownik przekazuje nam korzystając z naszej witryny, aplikacji (zwanymi dalej "Aplikacjami") i innych usług powiązanych z niniejszą Informacją o ochronie prywatności (zwanymi łącznie "Usługami"). Niniejsza Informacja o ochronie prywatności jest włączona do [Regulaminu świadczenia usług](#) (zwanego dalej "Regulaminem") i podlega jego postanowieniom. Spółka Tools for Humanity Corporation (zwana dalej "amerykańskim oddziałem TFH"), wraz ze swoim niemieckim podmiotem zależnym Tools for Humanity GmbH (zwanym dalej "niemieckim oddziałem TFH"; zwane łącznie "TFH", "my", "nas"), przyczynia się do początkowego opracowania i rozwoju protokołu World (zwanego dalej "World").

1. Administrator danych

Jesteśmy administratorem wszystkich "Danych aplikacji World App", "Danych weryfikacyjnych" i innych "Danych biznesowych": Tools for Humanity Corporation, 548 Market Street, PMB 49951, San Francisco, CA 94104 USA. TFH posiada podmiot Tools for Humanity GmbH z siedzibą w Unii Europejskiej (zwanej dalej "UE").

- "Dane aplikacji World App" oznaczają wszystkie dane osobowe gromadzone i przetwarzane w związku z korzystaniem przez użytkownika z aplikacji World App, zgodnie z definicją w części 5 poniżej, z wyjątkiem wszelkich danych osobowych związanych z korzystaniem przez niego z protokołu World lub tokenów World (takich jak adres portfela i dane transakcyjne, których nie kontrolujemy).
- Dane weryfikacyjne oznaczają dane przetwarzane podczas weryfikacji metody uwierzytelniania w celu dodania jej do samodzielnego identyfikatora World ID użytkownika. Obejmuje to np. odczytywanie chipa NFC umieszczonego w paszporcie w celu bezpiecznego przechowywania danych paszportu na urządzeniu. Dane te pozostają pod kontrolą użytkownika, a po sprawdzeniu ważności metody uwierzytelniania TFH przechowuje zanonimizowany fragment skrótu unikalnego podpisu kryptograficznego metody uwierzytelnienia (np. paszportu), aby zapewnić, że każda poszczególna metoda uwierzytelniania może zostać dodana do World ID tylko raz.
- „Dane biznesowe” oznaczają wszystkie dane osobowe zgromadzone i przetwarzane przez naszą firmę w inny sposób podczas komunikacji lub w ramach współpracy bądź interakcji pomiędzy nami a użytkownikiem np. za pośrednictwem poczty elektronicznej, wideokonferencji lub naszych witryn internetowych. Informacje na temat przetwarzania danych w kontekście Aplikacji Orb można znaleźć w Informacji o ochronie prywatności aplikacji Orb, do której łącznie znajduje się w Aplikacji Orb. Informacje na temat przetwarzania danych w kontekście dedykowanego gromadzenia i testowania danych można znaleźć w odpowiedniej Informacji o ochronie prywatności dotyczącej gromadzenia i testowania, które można znaleźć w aplikacji testowej. Informacje na temat przetwarzania w kontekście naszej witryny internetowej można znaleźć w naszej Polityce dotyczącej plików cookie, do której łącznie znajduje się na naszej stronie internetowej.

2. Zmiany w niniejszej Informacji o ochronie prywatności

Okresowo aktualizujemy niniejszą Informację o ochronie prywatności. Jeśli wprowadzimy do niej istotne zmiany, na przykład dotyczące sposobu wykorzystywania danych osobowych użytkownika, poinformujemy go o tym za pośrednictwem poczty e-mail lub wiadomości w Aplikacji.

3. Co zawiera niniejsza Informacja o ochronie prywatności?

- Nasze zobowiązanie do ochrony prywatności i danych użytkownika
- Gromadzone przez nas dane i powód ich gromadzenia
- Sposób wykorzystywania gromadzonych przez nas danych
- Miejsce przetwarzania danych użytkownika

- Okoliczności udostępniania danych użytkownika
- Sposób zapisywania danych użytkownika w publicznej sieci blockchain
- Sposób wykorzystywania plików cookie
- Jak długo przechowujemy dane użytkownika
- Czym różni się niniejsza Informacja o ochronie prywatności w przypadku dzieci i młodzieży
- Przysługujące użytkownikowi prawa ustawowe
- Jak skontaktować się z nami w sprawie niniejszej Informacji o ochronie prywatności

4. Nasze zobowiązanie do ochrony prywatności i danych użytkownika

Jesteśmy głęboko zaangażowani na rzecz ochrony prywatności użytkownika i ochrony jego danych. Zdajemy sobie sprawę, że możemy wypełnić naszą misję sprawiedliwej dystrybucji naszych tokenów cyfrowych wśród jak największej liczby osób tylko wtedy, gdy inni będą nam ufać, a ochrona prywatności i bezpieczeństwa danych mają kluczowe znaczenie dla zdobycia zaufania użytkowników.

Prywatność

Nasze produkty i usługi stworzyliśmy z myślą o ochronie prywatności użytkownika. Dane gromadzimy w celu ulepszania naszych produktów i usług. Zawsze będziemy informować użytkownika, w niniejszej Informacji o ochronie prywatności lub w formularzach zgody na przetwarzanie danych dotyczących konkretnych produktów lub usług, jakie dane gromadzimy, dlaczego je gromadzimy i jak je wykorzystujemy.

Bezpieczeństwo danych

Mamy dedykowany zespół, który dba o dane użytkownika i wdrożyliśmy fizyczne i elektroniczne zabezpieczenia, które chronią jego dane zarówno podczas przesyłania, jak i przechowywania danych. Nie jesteśmy jednak w stanie zapewnić całkowitego bezpieczeństwa jakiegokolwiek usługi. W przypadku jakichkolwiek wątpliwości dotyczących swojego konta lub swoich danych prosimy o kontakt za pośrednictwem naszego [Portalu wniosków](#) lub napisanie do nas na adres Tools For Humanity Corporation, 548 Market Street, PMB 49951, San Francisco, CA 94104 USA.

5. Gromadzone przez nas dane i powód ich gromadzenia

5.1 Dane, które użytkownik nam przekazuje

Użytkownik nie musi podawać żadnych danych w celu uzyskania dostępu do Aplikacji. Podanie określonych danych może jednak być konieczne w celu skorzystania z funkcji w ramach Usług. Podstawą prawną przetwarzania w poniższych przypadkach jest zgoda użytkownika oraz wykonanie umowy (nasze zobowiązanie do świadczenia Usług). Poniżej znajduje się lista danych, które użytkownik może podać i do czego możemy je wykorzystać:

W kontekście aplikacji World App:

- **Numer telefonu.** Użytkownik może podać swój numer telefonu, aby powiązać go ze swoim kontem. Za zgodą użytkownika inni użytkownicy mogą być w stanie znaleźć jego konto za pomocą numeru telefonu. Możemy wymagać podania numeru telefonu użytkownika, gdy składa on żądanie jako osoba, której dane dotyczą. Podstawą prawną przetwarzania tych danych jest świadczenie Usługi na podstawie Regulaminu świadczenia usług.
- **Nazwa użytkownika.** Użytkownik może powiązać nazwę użytkownika ze swoim adresem w portfelu i zmienić nazwę użytkownika w dowolnym momencie.
- **Data urodzenia.** Użytkownik może ujawnić swoją datę urodzenia, aby zapewnić zgodność z wymogami dotyczącymi ograniczeń wiekowych. Nigdy nie będziemy przechowywać danych dotyczących daty urodzenia użytkownika – zamiast tego przechowujemy wyłącznie sumę kontrolną tych danych oraz to, czy użytkownik ma ukończone 18 lat.
- **Informacje zwrotne i korespondencja od użytkownika.** Obejmuje to wszelkie wiadomości e-mail, wiadomości na czacie lub inne

wiadomości, które użytkownik wysyła nam za pośrednictwem poczty elektronicznej lub zewnętrznych serwisów społecznościowych. Może to obejmować przetwarzanie adresów e-mail lub nazw profili w mediach społecznościowych, jeśli użytkownik chce się z nami skontaktować za pośrednictwem jednego z tych kanałów. Możemy korzystać z usług zewnętrznego usługodawcy w celu przeprowadzania ankiet dotyczących korzystania z naszych Usług. Podstawą prawną przetwarzania tych danych jest świadczenie Usługi na podstawie Regulaminu świadczenia usług.

- **Kontakty z książki adresowej.** Użytkownik może dać Aplikacji dostęp do swojej książki adresowej, aby włączyć funkcję ułatwiającą wyszukiwanie innych użytkowników, którzy mogą znajdować się w książce adresowej użytkownika, i wchodzenie z nimi w interakcje. Podstawą prawną przetwarzania tych danych jest uzasadniony interes osoby, której dane dotyczą, polegający na możliwości odnalezienia go w Aplikacji oraz interes użytkownika udostępniającego dane polegający na możliwości odnalezienia jego kontaktów w Aplikacji.

Uwaga: Użytkownik ponosi odpowiedzialność za zapewnienie, że udostępnianie jego danych kontaktowych jest zgodne z obowiązującymi przepisami prawa. Może to wymagać uzyskania zgody osób, do których należą dane kontaktowe, a użytkownik nie będzie udostępniać TFH żadnych danych kontaktowych innych osób bez ich wyraźnej zgody. Użytkownik może zmienić zdanie i wyłączyć nasz dostęp do jego kontaktów w dowolnym momencie w ustawieniach urządzenia. Jeśli użytkownik zdecyduje się zaimportować kontakty z książki adresowej swojego urządzenia do Aplikacji, aby dowiedzieć się, które osoby z jego listy kontaktów korzystają z naszych Usług lub zaprosić je do korzystania z naszych Usług, będziemy okresowo synchronizować numery telefonów jego kontaktów z tymi numerami i odpowiadającymi im adresami portfela podanymi przez innych użytkowników na naszych serwerach.

- **Informacje o lokalizacji.** Użytkownik może zdecydować się włączyć usługę wykorzystującą dane o lokalizacji (taką jak funkcja umożliwiająca znalezienie operatora Orb w pobliżu). Za wyraźną zgodą użytkownika możemy wówczas gromadzić informacje o lokalizacji użytkownika za pomocą funkcji GPS, aby umożliwić usłudze wykorzystującej lokalizację użytkownika wyświetlenie użytkownikowi listy Orbów w jego okolicy. Użytkownik może w dowolnym momencie dostosować uprawnienia w ustawieniach urządzenia. Pod warunkiem, że użytkownik nie znajduje się na terytorium Korei Południowej, możemy również przechowywać jego przybliżoną lokalizację niepowiązaną z jego kontem w aplikacji World App. Dane te wykorzystujemy w celu ulepszenia naszych usług, w szczególności, ale nie wyłącznie, w celu wyboru lokalizacji Orbów.
- **Platforma P2P Marketplace.** Jeśli użytkownik korzysta z usług platformy P2P Marketplace (jeśli są dostępne), które umożliwiają zakup tokenów cyfrowych od innych użytkowników, możemy gromadzić dodatkowe dane, takie jak adres portfela, dane kontaktowe (np. numer telefonu) i numer konta powiązany z transakcją (np. numer M-PESA). Rejestrujemy dane transakcji w ramach świadczenia Usług P2P Marketplace. Możemy również gromadzić dodatkowe dane w celu spełnienia obowiązujących wymogów ZK.
- **Metadane urządzenia.** Jeśli użytkownik korzysta z Aplikacji, gromadzimy metadane z jego urządzenia, aby upewnić się, że Aplikacja działa prawidłowo i że nie narusza on naszych Regulaminów. Obejmuje to gromadzenie identyfikatorów urządzeń i adresów IP.
- **Dane urządzenia World ID.** Przetwarzamy również metadane urządzenia użytkownika w celu obliczenia unikalnego cyfrowego odcisku palca urządzenia. Skrót tego odcisku palca służy jako sygnał potwierdzający unikalność urządzenia użytkownika World ID.

W kontekście przetwarzania danych biznesowych:

- **Imię i nazwisko.** Możemy przetwarzać imię i nazwisko użytkownika w celu realizacji uzasadnionego interesu związanego z utrzymywaniem i administrowaniem relacją biznesową z użytkownikiem.
- **Adres e-mail.** Użytkownik może również podać swój adres e-mail, aby zapisać się na naszą listę mailingową i otrzymywać aktualne informacje na temat projektu World. Możemy wymagać podania adresu e-mail użytkownika, gdy składa on żądanie jako osoba, której dane dotyczą. Możemy przetwarzać adres e-mail użytkownika w celu realizacji uzasadnionego interesu związanego z utrzymywaniem i administrowaniem relacją biznesową z użytkownikiem.
- **Numer telefonu.** Możemy przetwarzać numer telefonu użytkownika w celu realizacji uzasadnionego interesu związanego z utrzymywaniem i administrowaniem relacją biznesową z użytkownikiem.

- **Dane przedsiębiorstwa.** Jeśli użytkownik utrzymuje z nami relacje biznesowe (np. jeśli jest on operatorem Orb lub usługodawcą), możemy wymagać podania takich informacji, jak imię i nazwisko, adres korespondencyjny, adres e-mail, numer telefonu, adres portfela i inne dokumenty (takie jak dowód tożsamości) w ramach rozwijania tych relacji biznesowych i w celu spełnienia naszych zobowiązań dotyczących znajomości klienta (ZK). Możemy korzystać z usług podmiotów zewnętrznych, takich jak Onfido, które pomagają nam w gromadzeniu i przeglądaniu powyższych danych i dokumentacji w celu wypełnienia obowiązków w zakresie znajomości swoich klientów.
- **Dane dotyczące podania o pracę.** W przypadku chęci podjęcia pracy dla nas użytkownik zostanie poproszony o przesłanie nam swojego podania o pracę zawierającego list motywacyjny i CV, a także dane osobowe, które pragnie ujawnić.

Podstawę prawną przetwarzania w kontekście każdej z powyższych czynności przetwarzania danych można znaleźć na końcu niniejszej Informacji o ochronie prywatności w ZAŁĄCZNIKU I – Podstawy prawne/cele przetwarzania danych przez Tools for Humanity w podziale na jurysdykcje.

5.2 Dane gromadzone przez nas ze źródeł zewnętrznych

Możemy okresowo uzyskiwać informacje na temat użytkownika z następujących źródeł zewnętrznych:

- **Dane sieci blockchain.** Możemy uzyskiwać i analizować publiczne dane blockchain, aby się upewnić, że osoby korzystające z naszych Usług nie prowadzą niezgodnej z prawem lub zakazanej działalności zgodnie z Regulaminem świadczenia usług, a także w celu analizy trendów transakcyjnych do celów badawczo-rozwojowych.
- **Usługi weryfikacji tożsamości.** Możemy uzyskiwać informacje od usługodawców zewnętrznych wykorzystujących dane użytkownika w celu weryfikacji jego tożsamości, jeśli jest to wymagane przez przepisy prawa (np. obowiązujące wymogi dotyczące znajomości klienta). Dla wyjaśnienia, **nie** wykorzystujemy danych biometrycznych użytkownika podczas weryfikacji jego tożsamości zgodnie z wymogami prawa.
- **Bazy danych talentów.** Możemy gromadzić dane z różnych źródeł, aby składać oferty pracy utalentowanym osobom.

5.3 Dane, które gromadzimy automatycznie

Jeśli zezwalają na to obowiązujące przepisy prawa, możemy gromadzić pewne rodzaje danych automatycznie podczas interakcji użytkownika z naszymi Usługami. Dane te pomagają nam rozwiązywać problemy związane z obsługą klienta, poprawiać wydajność Usług, poprawiać komfort użytkowania i personalizować usługi oraz zabezpieczać dane uwierzytelniające kont. Dane gromadzone automatycznie obejmują:

- **Identyfikatory online:** Dane dotyczące geolokalizacji i śledzenia (opisane powyżej), systemu operacyjnego komputera lub telefonu komórkowego, nazwy i wersji przeglądarki internetowej oraz adresów IP. W bardzo ograniczonych przypadkach dane te są również wykorzystywane do wykrywania oszustw i niezgodnych z prawem przepływów finansowych. Służą one również zapewnieniu płynnego korzystania z naszego oprogramowania i zapobiegania oszustwom.
- **Dane dotyczące użytkowania:** Dane uwierzytelniające, pytania zabezpieczające i inne dane gromadzone za pośrednictwem plików cookie i podobnych technologii.
- **Pliki cookie:** niewielkie pliki danych przechowywane na dysku twardym lub w pamięci urządzenia użytkownika, które pomagają nam ulepszać nasze Usługi i komfort użytkowania, sprawdzać, które obszary i funkcje naszych Usług są popularne oraz jaka jest liczba wizyt na stronie. Aby uzyskać informacje na temat podstawy prawnej przetwarzania tych danych, należy zapoznać się z naszą [Polityką plików cookie](#), w której opisujemy różne rodzaje plików cookie, których używamy.

Na podobnej zasadzie Aplikacja gromadzi dane w celu rozwiązywania problemów i wprowadzania ulepszeń. Korzystamy z usług podmiotów zewnętrznych, takich jak Segment.io lub PostHog, aby wyświetlać zagregowane dane dotyczące użytkowania witryny i interakcji użytkowników końcowych. Gdy to możliwe, podejmujemy działania w celu zminimalizowania lub zamaskowania danych wysyłanych do podmiotów zewnętrznych (np. szyfrowanie danych).

5.4 Dane zanonimizowane i zbiorcze

Anonimizacja to technika przetwarzania danych, po zastosowaniu której dane przestają stanowić dane osobowe, ponieważ po

anonimizacji dane nie mogą zostać już powiązane z konkretną osobą fizyczną. Przykłady zanonimizowanych danych obejmują:

- dane dotyczące transakcji;
- dane dotyczące sekwencji odwiedzanych stron;
- wskaźniki wydajności; oraz
- wskaźniki oszustw (choć dane osobowe również są wykorzystywane w tym celu).

Agregujemy również dane, łącząc ze sobą duże ilości informacji, tak aby nie pozwalały one na ustalenie tożsamości ani nie odnosiły się do konkretnej osoby. Używamy zanonimizowanych lub zagregowanych danych do naszych celów biznesowych, takich jak zrozumienie potrzeb i zachowań użytkowników, ulepszanie naszych Usług, analityka biznesowa i marketing, wykrywanie zagrożeń dla bezpieczeństwa i szkolenie naszych algorytmów.

Podstawą prawną przetwarzania wyżej wymienionych danych jest uzasadniony interes związany z funkcjonowaniem aplikacji lub witryny internetowej, analiza działalności i zapobieganie oszustwom.

6. Sposób wykorzystywania gromadzonych przez nas danych

6.1 Opis ogólny

Aby być w stanie wykorzystywać dane osobowe użytkownika, musimy dysponować ku temu uzasadnionym powodem (czyli „podstawą prawną przetwarzania”). W niektórych przypadkach wykorzystywanie danych osobowych użytkownika nie wymaga uzyskania jego uprzedniej zgody. Wykorzystujemy dane użytkownika do następujących celów:

- do zapewniania i obsługi naszych produktów i usług zgodnie z Regulaminem świadczenia usług. Usługi te obejmują:
 - Aplikację, w której użytkownicy mogą zarządzać swoimi identyfikatorami World ID i tokenami cyfrowymi, a także dowiedzieć się więcej o kryptowalutach i projekcie World;
 - aplikację Operator App, za pomocą której operatorzy Orb mogą zarządzać swoimi Orbami i nadzorować je oraz wyświetlać ich statystyki;
 - platformę P2P Marketplace, dzięki której łączymy użytkowników z agentami (nie dotyczy użytkowników posiadających główne miejsce zamieszkania lub mieszkających w Niemczech bądź posiadających główny ośrodek życiowy lub siedzibę w Niemczech);
- ulepszanie i rozwijanie naszych produktów i usług, w tym usuwanie i naprawianie błędów w naszych Usługach;
- prowadzenie badań w zakresie nauki o danych;
- analizowanie korzystania przez użytkownika z naszych Usług w celu zapewnienia lepszego wsparcia;
- umożliwienie użytkownikowi publikowania informacji w sieci blockchain w celu udowodnienia swojej unikalności;
- korzystanie z adresu portfela do wysyłania użytkownikowi tokenów cyfrowych, które obsługujemy;
- przestrzeganie obowiązujących przepisów prawa, takich jak przepisy dotyczące przeciwdziałania praniu pieniędzy i sankcje. Obejmuje to:
 - używanie adresu IP użytkownika do blokowania osób mieszkających w kraju, który nie zezwala na uzyskiwanie dostępu do Usług;
 - udzielanie odpowiedzi na żądania osób, których dane dotyczą, zgodnie z obowiązującymi przepisami o ochronie danych, takie jak żądania dostępu do danych lub ich usunięcia;
 - monitorowanie potencjalnie niezgodnych z prawem przepływów finansowych, np. z portfeli wpisanych na czarną listę; oraz

- zachowanie zgodności z obowiązującymi przepisami prawa, np. regulacjami przeciwdziałającymi nielegalnym treściom.
- obsługę żądań, skarg i zapytań użytkownika dotyczących obsługi klienta;
- rozstrzyganie sporów, rozwiązywanie problemów i egzekwowanie postanowień naszych umów z użytkownikiem, w tym niniejszej Informacji o ochronie prywatności i Regulaminu świadczenia usług;
- kontaktowanie się z użytkownikiem w sprawie aktualizacji Usług.

6.2 Dane uwierzytelniające

TFH umożliwia użytkownikowi przechowywanie określonych danych uwierzytelniających lokalnie na urządzeniu użytkownika w celu udostępniania ich wewnątrz infrastruktury wykorzystującej zerową wiedzę protokołu World ID („Dane uwierzytelniające”). W kontekście Danych uwierzytelniających przetwarzamy wspomniane dane w następujący sposób:

- sprawdzamy ważność Danych uwierzytelniających użytkownika (w przypadku paszportów odbywa się to za pomocą sprawdzenia certyfikatu głównego kraju użytkownika);
- weryfikujemy użytkownika jako uprawnionego posiadacza metody uwierzytelniania (w przypadku paszportów odbywa się to lokalnie na urządzeniu użytkownika, a zdjęcie jego twarzy (selfie) nigdy nie jest zapisywane).
- Szyfrujemy, podpisujemy i przechowujemy Dane uwierzytelniające użytkownika w bezpiecznym środowisku na jego urządzeniu.
 - Nigdy nie mamy dostępu do danych osobowych zawartych w Danych uwierzytelniających użytkownika.
 - Użytkownik może następnie selektywnie udostępniać te informacje stronom polegającym na tych informacjach za pośrednictwem zabezpieczeń protokołu World ID (np. użytkownik może udowodnić, że ma ukończone 18 lat bez ujawniania swojego dokładnego wieku lub tożsamości).
- W przypadku paszportów TFH zachowuje zanonimizowany fragment skrótu unikalnego podpisu kryptograficznego paszportu, aby zapewnić, że każdy pojedynczy paszport może zostać zweryfikowany tylko raz.

Przetwarzanie to jest oparte na zgodzie użytkownika i nigdy nie uzyskujemy dostępu do jego danych osobowych z paszportu, który jest przechowywany na urządzeniu użytkownika. Dane te można usunąć ze swojego telefonu, usuwając aplikację World App.

6.3 Dane World ID

Identyfikator World ID użytkownika (tj. tajny numer wymagany do użycia protokołu World) jest przechowywany tylko na urządzeniu użytkownika (w przypadku posiadania kopii zapasowej, zaszyfrowana kopia zostanie zapisana wewnątrz kopii zapasowej). Ani spółka TFH, ani nikt inny nie ma dostępu do identyfikatora World ID użytkownika. Użytkownik może korzystać ze swojego identyfikatora World ID anonimowo. Za każdym razem, gdy użytkownik używa identyfikatora World ID w połączeniu z nową aplikacją, aplikacja otrzymuje wyłącznie jednorazowy numer („Szyfr”) nieujawniający identyfikatora World ID użytkownika. Jest to możliwe dzięki wykorzystaniu funkcji dowodów z wiedzą zerową (użytkownik musi udowodnić, że jest posiadaczem identyfikatora World ID, jednak nie musi przedstawiać konkretnego identyfikatora), a cały proces zapewnia, że nie jest możliwe śledzenie identyfikatora World ID używanego przez użytkownika. Oznacza to, że World ID nie jest identyfikatorem użytkownika przeznaczonym do użytku w Internecie.

Dowody w kontekście identyfikatorów World ID działają na podstawie otwartego protokołu uzyskującego dostęp do publicznego drzewa skrótów zawierającego skróty zweryfikowanych identyfikatorów World ID. Identyfikator World ID nie jest scentralizowaną usługą – jest to protokół, do którego każdy może uzyskać dostęp. Oferujemy interfejsy API ułatwiające dostęp do drzewa skrótów i dowodów w odniesieniu do identyfikatorów World ID, ale nigdy w tym kontekście nie otrzymujemy żadnych danych osobowych.

Ważne jest również, aby pamiętać, że nie przetwarzamy też żadnych danych związanych z identyfikatorem World ID użytkownika, które pozwoliłyby nam go zidentyfikować. Wszystkie przypadki przetwarzania danych osobowych w kontekście aplikacji World App, w szczególności adres portfela i dane dotyczące transakcji, są celowo zaprojektowane w taki sposób, aby dane te były odłączone od danych identyfikatora World ID.

7. Miejsce przetwarzania danych użytkownika

7.1 Przekazywanie danych.

Gdy użytkownik przekazuje swoje dane, mogą one być przekazywane, przechowywane lub przetwarzane w miejscu innym niż to, w którym zostały one pierwotnie zgromadzone. W kraju, w którym dane użytkownika są przekazywane, przechowywane lub przetwarzane, mogą nie obowiązywać te same przepisy dotyczące ochrony danych, co w kraju, w którym użytkownik pierwotnie podał dane.

Dokładamy wszelkich starań, aby przestrzegać zasad określonych w przepisach dotyczących ochrony prywatności w każdej jurysdykcji. Udostępniamy dane podmiotom przetwarzającym znajdującym się poza jurysdykcją użytkownika tylko wtedy, gdy takie przekazywanie jest zgodne z prawem i jeśli mamy pewność, że podmiot przetwarzający będzie chronił te dane zgodnie z wymogami obowiązującego prawa oraz zgodnie z naszymi standardami.

7.2 Ryzyko związane z przekazywaniem danych

Poniżej znajduje się lista możliwych zagrożeń, które mogą zaistnieć w przypadku przekazywania przez nas danych użytkownika do Stanów Zjednoczonych, Unii Europejskiej lub innego kraju. Poniżej podsumowujemy również, w jaki sposób zapobiegamy poszczególnemu ryzyku.

- Robimy, co w naszej mocy, aby zapewnić, że nasi podwykonawcy są umownie zobowiązani do odpowiedniej ochrony danych użytkownika, jednak podwykonawcy ci mogą nie podlegać przepisom o ochronie danych obowiązującym w kraju zamieszkania użytkownika. W przypadku dopuszczenia się przez podwykonawców przetwarzania danych użytkownika bez jego zgody, w sposób niezgodny z przepisami prawa, może być trudno dochodzić praw do prywatności użytkownika wobec tego podwykonawcy. Ograniczamy ryzyko w tym zakresie, zawierając z naszymi podwykonawcami rygorystyczne umowy dotyczące przetwarzania danych, które zobowiązują ich do ochrony danych na poziomie RODO i realizacji wniosków osób, których dane dotyczą.
- Istnieje możliwość, że przepisy dotyczące ochrony prywatności danych w kraju zamieszkania użytkownika są niespójne z przepisami dotyczącymi ochrony prywatności danych obowiązującymi w Stanach Zjednoczonych lub UE. Zawsze staramy się przestrzegać najwyższych standardów w zakresie ochrony danych, którym podlegamy.
- Istnieje możliwość, że do danych użytkownika dostęp będą mieli funkcjonariusze rządowi i urzędnicy. W takich przypadkach zobowiązaliśmy się kwestionować wszelkie nieważne, nadmierne lub niezgodne z prawem wnioski o dostęp w sądzie. Ponadto stosujemy zaawansowane szyfrowanie, aby uniemożliwić uzyskanie dostępu w sposób nieupoważniony.

Należy pamiętać, że lista ta zaledwie zawiera przykłady i może nie obejmować wszystkich możliwych czynników ryzyka, które mogą mieć zastosowanie do użytkownika.

7.3 Ramy ochrony danych dla danych przekazywanych do USA

TFH przestrzega Ram ochrony danych osobowych (Data Privacy Framework, DPF) UE-USA (DPF UE-USA), aneksu do Ram ochrony danych osobowych UE-USA w sprawie Wielkiej Brytanii oraz Ram ochrony danych osobowych Szwajcaria-USA (DPF Szwajcaria-USA) określonych przez Departament Handlu USA. TFH poświadczyła Departamentowi Handlu USA, że przestrzega zasad Ram ochrony danych UE-USA (Zasady Ram ochrony danych UE-USA) w odniesieniu do przetwarzania danych osobowych otrzymywanych z Unii Europejskiej w oparciu o Ramy ochrony danych UE-USA oraz z Wielkiej Brytanii (i Gibraltaru) w oparciu o aneks do Ram ochrony danych UE-USA w sprawie Wielkiej Brytanii. TFH poświadczyła Departamentowi Handlu USA, że przestrzega zasad Ram ochrony danych Szwajcaria-USA (Zasady Ram ochrony danych Szwajcaria-USA) w odniesieniu do przetwarzania danych osobowych otrzymywanych ze Szwajcarii w oparciu o Ramy ochrony danych Szwajcaria-USA. W przypadku rozbieżności pomiędzy postanowieniami niniejszej Informacji o Ramach ochrony danych i Zasadami Ram ochrony danych UE-USA lub Szwajcaria-USA, Zasady te mają znaczenie nadrzędne. Aby uzyskać więcej informacji na temat Ram ochrony danych (DPF) i zapoznać się z naszą certyfikacją, należy odwiedzić witrynę <https://www.dataprivacyframework.gov/>.

TFH odpowiada za przetwarzanie danych osobowych, które otrzymuje na mocy Ram ochrony danych, a następnie przekazuje podmiotom zewnętrznym działającym jako przedstawiciele w naszym imieniu. TFH przestrzega zasad Ram ochrony danych w odniesieniu do wszelkich przypadków dalszego przekazywania danych osobowych z UE, Wielkiej Brytanii i Szwajcarii, w tym postanowień dotyczących odpowiedzialności w związku z dalszym przekazywaniem.

Federalna Komisja Handlu (Federal Trade Commission, FTC) ma jurysdykcję nad przestrzeganiem przez TFH zasad Ram ochrony danych UE-USA, aneksu do Ram ochrony danych UE-USA w sprawie Wielkiej Brytanii i Ram ochrony danych Szwajcaria-USA. W określonych okolicznościach TFH może być zmuszona ujawnić dane osobowe w odpowiedzi na zgodne z prawem żądania organów władzy państwowej, w tym w celu spełnienia wymogów dotyczących bezpieczeństwa narodowego i egzekwowania prawa.

Zgodnie z postanowieniami Ram ochrony danych UE-USA i aneksu do Ram ochrony danych UE-USA w sprawie Wielkiej Brytanii oraz Ram ochrony danych Szwajcaria-USA TFH zobowiązuje się rozstrzygnąć związane z zasadami Ram ochrony danych skargi dotyczące gromadzenia i wykorzystywania przez nas danych osobowych użytkownika. Osoby fizyczne z UE i Wielkiej Brytanii oraz Szwajcarii, które mają pytania albo skargi dotyczące naszego postępowania z Danymi osobowymi otrzymanymi w oparciu o postanowienia Ram ochrony danych UE-USA i aneksu do Ram ochrony danych UE-USA w sprawie Wielkiej Brytanii oraz Ram ochrony danych Szwajcaria-USA powinny w pierwszej kolejności skontaktować się z TFH pod adresem: dpo@world.org.

Zgodnie z postanowieniami Ram ochrony danych UE-USA i aneksu do Ram ochrony danych UE-USA w sprawie Wielkiej Brytanii oraz Ram ochrony danych Szwajcaria-USA TFH zobowiązuje się współpracować i postępować zgodnie z zaleceniami panelu ustanowionego przez organy ochrony danych (Data Protection Authorities, DPA) UE, brytyjskie Biuro Komisarza ds. Informacji (Information Commissioner's Office, ICO), Organ regulacyjny Gibraltaru (Gibraltar Regulatory Authority, GRA) i szwajcarskiego Federalnego Komisarza ds. Ochrony Danych i Informacji (Federal Data Protection and Information Commissioner, FDPIC) w odniesieniu do nierozstrzygniętych skarg dotyczących naszego postępowania z danymi osobowymi otrzymanymi w oparciu o postanowienia Ram ochrony danych UE-USA i aneksu do Ram ochrony danych UE-USA w sprawie Wielkiej Brytanii oraz Ram ochrony danych Szwajcaria-USA.

W określonych okolicznościach użytkownik ma możliwość powołać się na prawo do rozstrzygnięcia sporu dotyczącego skarg w zakresie Tarczy Prywatności w drodze wiążącego arbitrażu, gdy mechanizmy Ram ochrony danych nie pozwolą na rozstrzygnięcie sporu. Więcej informacji można znaleźć na oficjalnej stronie Ram ochrony danych.

8. Kiedy udostępniamy dane użytkownika

Nigdy nie sprzedamy danych użytkownika.

Gdy udostępniamy dane użytkownika podmiotom poza naszą organizacją, zawsze:

- udostępniamy je w bezpieczny i odpowiedzialny sposób;
- podejmujemy kroki mające na celu zapewnienie, że są one traktowane w sposób zgodny z naszym zobowiązaniem na rzecz zachowania prywatności; oraz
- zabraniamy innym firmom wykorzystywania ich do celów własnych.

Udostępniamy dane użytkownika w ograniczony sposób:

- **Fundacji World Foundation:** możemy działać w charakterze podmiotów przetwarzających fundacji World Foundation w celu gromadzenia danych osobowych w imieniu World (więcej informacji na ten temat znajduje się w Informacji o ochronie prywatności World).
- **Wewnątrz naszej organizacji:** ujawniamy dane wyłącznie członkom naszego zespołu, którzy potrzebują dostępu do nich w celu wykonywania swoich zadań i obowiązków. Ujawniamy tylko taką ilość danych, jaka jest potrzebna do wykonania określonych zadań i obowiązków oraz posiadamy system ścisłej kontroli dostępu.
- **Kontrahentom i usługodawcom spoza naszej organizacji:** ujawniamy dane wyłącznie usługodawcom, na których usługach polegamy w celu przetwarzania danych i świadczenia użytkownikowi naszych Usług. Ujawniamy dane podmiotom weryfikującym tożsamość wyłącznie, gdy jest to wymagane przez prawo (np. wymogi dotyczące znajomości klienta).
- Kategorie takich usługodawców to:
- Podmioty świadczące usługi w chmurze
- Dostawcy rozwiązań SaaS; korzystamy z produktów SaaS w ramach następujących działań:

- zarządzanie bazą danych i infrastrukturą;
- bezpieczeństwo danych;
- rekrutacja;
- komunikacja;
- ankiety;
- znajomość klienta/biznesu, czyli weryfikacja oficjalnych dokumentów;
- zarządzanie wniosków od osób, których dane dotyczą;
- wsparcie techniczne;
- wsparcie użytkowników.
- Ekspertom zewnętrznym:
 - wyspecjalizowanym programistom;
 - specjalistom ds. prawnych;
 - doradcom podatkowym;
- bankom;
- dostawcom usług etykietowania (wyłącznie po zastosowaniu szczególnych zabezpieczeń);
- usługodawcom sprawdzającym przeszłość kandydatów i operatorów Orb;
- **organom porządkowym, urzędnikom lub innymi podmiotom zewnętrznym:** możemy ujawnić dane użytkownika w celu zachowania zgodności z obowiązującymi przepisami prawa i udzielenia odpowiedzi na bezwzględnie obowiązujące żądania prawne. Dokładnie przeanalizujemy każde żądanie, aby ustalić, czy jest ono zgodne z prawem, a w stosownych przypadkach możemy zakwestionować żądania, które będą nieważne, niezgodne z prawem lub których zakres będzie zbyt szeroki. Możemy udostępniać dane osobowe policji i innym organom rządowym, jeśli będziemy mieć uzasadnione przekonanie, że jest to konieczne do przestrzegania przepisów prawa lub innego procesu prawnego lub wywiązania się z obowiązku prawnego.
- Możemy udostępniać dane osobowe użytkownika, jeśli uznamy, że jego działania są niezgodne z naszym Regulaminem świadczenia usług, jeśli uznamy, że naruszył on prawo lub że jest to konieczne w celu ochrony naszych praw, własności i bezpieczeństwa, naszych użytkowników, społeczeństwa lub innych osób.
- Możemy udostępniać dane osobowe użytkownika naszym prawnikom i innym profesjonalnym doradcom, gdy będzie to konieczne w celu uzyskania porady lub ochrony naszych interesów biznesowych i zarządzania nimi.
- Możemy udostępniać dane osobowe użytkownika w związku z dowolną fuzją, sprzedażą aktywów spółki, finansowaniem bądź przejęciem całości lub części naszej działalności na rzecz innego przedsiębiorstwa albo podczas prowadzenia negocjacji w tym zakresie.
- Dane, w tym dane osobowe użytkownika, mogą być udostępniane pomiędzy naszymi obecnymi i przyszłymi spółkami dominującymi, jednostkami stowarzyszonymi i zależnymi oraz innymi spółkami powiązanymi z nami na zasadzie wspólnej własności albo kontroli.
- Możemy udostępniać dane osobowe użytkownika za jego zgodą lub na jego polecenie.

9. Sposób zapisywania danych użytkownika w publicznej sieci blockchain

Informacje o transakcjach związanych z korzystaniem przez użytkownika z naszych Usług mogą być rejestrowane w publicznej sieci blockchain.

Uwaga: Sieci blockchain to publiczny rejestr transakcji prowadzony w rozproszonych sieciach obsługiwanych przez podmioty zewnętrzne, które nie są kontrolowane ani zarządzane przez World. Ze względu na publiczny i niezmienny charakter rejestru sieci blockchain, nie możemy zagwarantować możliwości zmiany, usunięcia lub kontrolowania ujawnianych danych, które są przesyłane i przechowywane w sieci blockchain.

10. Jak wykorzystujemy pliki cookie?

Używamy plików cookie, aby poprawić działanie naszych Usług. Oprócz plików cookie możemy wykorzystywać inne podobne technologie, takie jak sygnały nawigacyjne, do śledzenia użytkowników naszych Usług. Sygnały nawigacyjne (zwane również „czystymi plikami GIF”) to niewielkie elementy graficzne o unikatowym identyfikatorze, działające podobnie do plików cookie. Nasza [Polityka plików cookie](#) została włączona do niniejszego dokumentu przez odniesienie.

Korzystamy również z Google Analytics. Więcej informacji o tym, w jaki sposób Google wykorzystuje dane użytkownika, gdy korzysta on z witryny i aplikacji partnerów Google: <https://policies.google.com/technologies/partner-sites>. Korzystając z Usług, użytkownik wyraża zgodę na przechowywanie i uzyskiwanie przez nas dostępu do plików cookie i innych danych na jego komputerze lub urządzeniu mobilnym oraz na korzystanie z Google Analytics w związku z takimi działaniami. Użytkownik powinien zapoznać się z informacjami dostępnymi w podanym łączu, aby wiedzieć, na co wyraża zgodę.

11. Okres przechowywania danych użytkownika

O ile obowiązujące przepisy prawa nie stanowią inaczej, przechowujemy dane użytkownika przez okres zasadnie konieczny do świadczenia mu naszych Usług, realizacji naszych uzasadnionych celów biznesowych oraz wypełniania naszych obowiązków prawnych. Jeśli użytkownik zlikwiduje swoje konto u nas, usuniemy jego dane z konta w ciągu jednego miesiąca; w przeciwnym razie usuniemy dane użytkownika z konta po dwóch latach braku aktywności. Jeśli będzie to wymagane przez prawo, będziemy nadal przechowywać jego dane osobowe w zakresie niezbędnym do wypełnienia naszych obowiązków prawnych, w tym monitorowania, wykrywania i zapobiegania oszustwom, a także wywiązywania się z obowiązków podatkowych, księgowych i sprawozdawczości finansowej.

Uwaga: Sieci blockchain to rozproszone sieci zewnętrzne, których nie kontrolujemy ani nie obsługujemy. Ze względu na publiczny i niezmienny charakter technologii blockchain, nie możemy zmieniać, usuwać ani kontrolować ujawnianych danych, które są przechowywane w sieci blockchain.

12. Czym różni się niniejsza Informacja o ochronie prywatności w przypadku dzieci i młodzieży?

Osoby poniżej 18. roku życia nie mogą korzystać z Usług, a my nie gromadzimy celowo danych od osób poniżej 18. roku życia. Jeśli użytkownik uważa, że jego dziecko w wieku poniżej 18 lat uzyskało dostęp do Usług bez jego zgody, należy zażądać usunięcia jego danych, kontaktując się z nami za pośrednictwem naszego [Portalu wniosków](#).

Jeśli dowiemy się, że zgromadziliśmy dane dotyczące dziecka poniżej 18. roku życia, niezwłocznie usuniemy takie dane. Podjęliśmy działania, takie jak wdrożenie automatycznego modelu sztucznej inteligencji wykrywającego wiek, instrukcje dla operatorów i potwierdzenia, aby ograniczyć korzystanie z Usług wyłącznie do osób, które ukończyły 18 lat. Nie sprzedajemy produktów ani usług dzieciom.

13. Jak skontaktować się z nami w sprawie niniejszej Informacji o ochronie prywatności?

Użytkownik może zdecydować się na usunięcie swoich danych z poziomu aplikacji w menu Ustawienia. W przypadku pytań lub wątpliwości dotyczących niniejszej Informacji o ochronie prywatności, chęci skorzystania ze swoich praw lub skontaktowania się z naszym Inspektorem ochrony danych (IOD), należy przesłać żądanie za pośrednictwem naszego [Portalu wniosków](#) lub napisać do nas na adres Tools For Humanity Corporation, 548 Market Street, PMB 49951, San Francisco, CA 94104, USA bądź na adres dpo@toolsforhumanity.com. Udzielamy odpowiedzi na każde żądanie otrzymane od osób, które chcą skorzystać z prawa do ochrony danych zgodnie z przepisami obowiązującego prawa o ochronie danych. Użytkownik może również usunąć swoje dane z poziomu aplikacji World.

W przypadku nierozstrzygniętych wątpliwości dotyczących ochrony prywatności albo wykorzystania danych, których nie rozwiązaliśmy w sposób zadowalający, można również kontaktować się z organem regulacyjnym ds. ochrony danych w danej jurysdykcji. Użytkownicy

zamieszkujący w UE mogą znaleźć swój organ regulacyjny ds. ochrony danych [tutaj](#).

14. Prawa użytkownika

Prawa te mają zastosowanie w zakresie, w jakim możemy zidentyfikować wnioskodawcę w naszej bazie danych i w zakresie, w jakim umożliwiając wykonawcy skorzystanie z praw nie naruszamy praw innych osób, których dane dotyczą:

- Użytkownik ma prawo do uzyskania od nas w dowolnym momencie na żądanie informacji o przetwarzanych przez nas danych osobowych, które go dotyczą. Użytkownik ma prawo do otrzymania od nas dotyczących jego danych osobowych.
- Użytkownik ma prawo żądać od nas niezwłocznego sprostowania dotyczących jego danych osobowych, jeżeli są one nieprawidłowe.
- Użytkownik ma prawo zażądać od nas usunięcia dotyczących go danych osobowych. Przesłanki te przewidują w szczególności prawo do usunięcia danych, jeżeli dane osobowe nie są już niezbędne do celów, dla których zostały zgromadzone lub są przetwarzane, pod warunkiem spełnienia wymogów dotyczących usunięcia danych wynikających z obowiązujących przepisów prawa (np. przepisy obowiązujące w niektórych jurysdykcjach zobowiązują nas do przechowywania informacji o transakcjach przez określony czas).
- Użytkownik ma prawo do dobrowolnego wycofania zgody na przetwarzanie danych na podstawie zgody lub do wniesienia sprzeciwu wobec przetwarzania danych, jeśli nie odbywa się ono na podstawie zgody.

15. DODATEK

Poniżej kilka dodatków zawiera wymagane prawem informacje na temat poszczególnych rynków, na których prowadzimy działalność. Informacje te stanowią część zgody w zależności od regionu, w którym mieszka osoba, której dane dotyczą. Informacje te mogą różnić się od informacji o Twojej lokalizacji, ponieważ blokujemy określone usługi w niektórych jurysdykcjach. W przypadku jakichkolwiek rozbieżności z powyższymi bardziej szczegółowymi stwierdzeniami dotyczącymi danej jurysdykcji pierwszeństwo mają następujące postanowienia:

Dodatek A: Europejski Obszar Gospodarczy ("EOG") i Wielka Brytania ("UK")

Jeśli użytkownik przebywa na terenie EOG albo lub Wielkiej Brytanii, zastosowanie mają następujące postanowienia: Użytkownikowi przysługują co najmniej poniższe prawa. Mogą przysługiwać mu też dodatkowe, wymienione poniżej prawa wynikające z ogólnego rozporządzenia o ochronie danych osobowych – rozporządzenia UE 2016/679 z 27 kwietnia 2016 r. (zwanego dalej "RODO"). Aby skorzystać ze swoich praw dostępnych na mocy RODO, należy skontaktować się z nami za pośrednictwem naszego [Portalu wniosków](#). Oprócz wyjątkowych przypadków rozpatrzmy wniosek w ustawowym terminie jednego miesiąca. Użycie słowa RODO w poniższym punkcie obejmuje również brytyjskie RODO transponowane do brytyjskiego prawa krajowego jako brytyjska Ustawa o ochronie danych z 2018 r. i zachowane w ramach prawa Anglii i Walii, Szkocji i Irlandii Północnej na mocy [ust. 3](#) Ustawy Unii Europejskiej (wycofanie) z 2018 r. i zmienionej [Załącznikiem 1](#) do Rozporządzenia o ochronie danych, prywatności i łączności elektronicznej (zmiany itp.) (wyjście z UE) z 2019 r. (SI 2019/419).

A.1 Prawa ustawowe wynikające z RODO

Niniejszy ustęp ma zastosowanie, jeśli do przetwarzania danych użytkownika mają zastosowanie postanowienia RODO (np. jeśli użytkownik jest rezydentem EOG lub Wielkiej Brytanii). Użytkownikowi mogą przysługiwać dodatkowe wymienione poniżej prawa na mocy RODO. Aby skorzystać ze swoich praw dostępnych na mocy RODO, należy skontaktować się z nami za pośrednictwem naszego [Portalu wniosków](#).

- Użytkownik ma prawo do uzyskania od nas informacji na temat danych osobowych, które przetwarzamy na jego temat, na żądanie, w zakresie art. 15 RODO.
- Użytkownik ma prawo żądać od nas niezwłocznego sprostowania dotyczących jego danych osobowych, jeżeli są one nieprawidłowe.
- Zgodnie z warunkami opisanymi w art. 17 RODO użytkownik ma prawo zażądać od nas usunięcia jego danych osobowych. Te warunki wstępne przewidują w szczególności prawo do usunięcia danych osobowych, jeżeli nie są one już potrzebne do celów,

dla których zostały zebrane lub w inny sposób przetworzone, a także w przypadku niezgodnego z prawem przetwarzania, istnienia sprzeciwu lub obowiązku usunięcia danych na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlegamy.

- Użytkownik ma prawo zażądać ograniczenia przetwarzania zgodnie z art. 18 RODO.
- Użytkownik ma prawo do otrzymania od nas danych osobowych, które nam przekazał, w ustrukturyzowanym, powszechnie używanym, nadającym się do odczytu maszynowego formacie zgodnie z art. 20 RODO.
- Użytkownik ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jego szczególną sytuacją – wobec przetwarzania dotyczących go danych osobowych, które odbywa się między innymi na podstawie art. 6 ust. 1 zdanie 1 lit. f RODO, zgodnie z art. 21 RODO.
- Użytkownik ma prawo skontaktować się z właściwym organem nadzorczym w przypadku skarg dotyczących przetwarzania danych przez administratora. Odpowiedzialnym organem nadzorczym jest: Bawarskie Państwowe Biuro Nadzoru nad Ochroną Danych (Bayerisches Landesamt für Datenschutz).
- Jeśli przetwarzanie danych osobowych odbywa się na podstawie zgody użytkownika, na mocy art. 7 RODO użytkownik ma prawo wycofać swoją zgodę na wykorzystywanie swoich danych osobowych w dowolnym momencie ze skutkiem na przyszłość, przy czym wycofanie jest równie łatwe, jak samo wyrażenie zgody. Należy pamiętać, że odwołanie wejdzie w życie tylko w przyszłości. Nie ma to wpływu na przetwarzanie, które miało miejsce przed odwołaniem.

A.2 Przekazywanie danych

- W przypadku przekazywania danych do kraju, w odniesieniu do którego nie wydano decyzji stwierdzającej odpowiedni stopień ochrony, stosujemy standardowe klauzule umowne UE. Obecnie przekazujemy dane osobowe wyłącznie do Stanów Zjednoczonych.
- Jeśli przetwarzanie danych osobowych odbywa się na podstawie zgody użytkownika, na mocy art. 7 RODO użytkownik ma prawo wycofać swoją zgodę na wykorzystywanie swoich danych osobowych w dowolnym momencie ze skutkiem na przyszłość, przy czym wycofanie jest równie łatwe, jak samo wyrażenie zgody. Należy pamiętać, że odwołanie wejdzie w życie tylko w przyszłości. Nie ma to wpływu na przetwarzanie, które miało miejsce przed odwołaniem. Należy pamiętać, że wycofanie zgody nie ma wpływu na przetwarzanie, które nie odbywa się w oparciu o zgodę.

DODATEK B: JAPONIA

W przypadku użytkowników zamieszkujących w Japonii zastosowanie mają następujące postanowienia dodatkowe:

B1. Informacje dotyczące japońskich przepisów

Przestrzegamy japońskich przepisów i regulacji, w tym Ustawy o ochronie danych osobowych w Japonii ("APPI"). Niniejszy ustęp dotyczy przetwarzania przez nas "danych osobowych" zgodnie z definicją zawartą w APPI i ma znaczenie nadrzędne w stosunku do innych części niniejszego Formularza zgody na przetwarzanie danych biometrycznych.

Przestrzegamy japońskich przepisów i regulacji, w tym Ustawy o ochronie danych osobowych w Japonii ("APPI"). Niniejszy ustęp dotyczy przetwarzania przez nas "danych osobowych" zgodnie z definicją zawartą w APPI i ma znaczenie nadrzędne w stosunku do innych części niniejszej Informacji o ochronie prywatności.

B2. Udostępnianie danych

O ile obowiązujące przepisy prawa nie stanowią inaczej, nie ujawniamy, nie sprzedajemy, nie przekazujemy, nie udostępniamy ani nie przekazujemy danych osobowych użytkownika żadnym osobom trzecim.

B3. Środki kontroli bezpieczeństwa

Stosujemy niezbędne i odpowiednie środki, aby zapobiec wyciekowi, utracie lub uszkodzeniu danych osobowych użytkownika oraz aby w inny sposób zachować bezpieczeństwo jego danych osobowych, takie jak ustanowienie zasad przetwarzania danych osobowych, regularne monitorowanie przetwarzania danych osobowych, regularne szkolenia pracowników w zakresie przetwarzania danych

osobowych, zapobieganie kradzieży lub utracie sprzętu używanego do przetwarzania danych osobowych oraz wdrożenie kontroli dostępu. Ponadto odpowiednio nadzorujemy naszych wykonawców i pracowników, którzy mają do czynienia z danymi osobowymi. Więcej informacji na temat środków kontroli bezpieczeństwa stosowanych w związku z przetwarzaniem danych osobowych można uzyskać, kontaktując się z nami za pośrednictwem naszego [Portalu wniosków](#).

B4. Informacje referencyjne dotyczące przekazywania danych osobowych podmiotom zewnętrznym w innych krajach

Dane osobowe użytkownika są przetwarzane w UE i USA.

B5. Prawa ustawowe wynikające z APPI

Aby skorzystać ze swoich praw przysługujących w ramach APPI, prosimy o kontakt z nami za pośrednictwem naszego [Portalu wniosków](#).

DODATEK C: ARGENTYNA

Użytkowników zamieszkujących w Republice Argentyńskiej informujemy, że AGENCJA DOSTĘPU DO INFORMACJI PUBLICZNYCH, działając jako Agencja Kontroli Prawa nr 25,326, ma prawo do rozpatrywania skarg i roszczeń składanych przez osoby, których prawa są uzależnione od nieprzestrzegania obowiązujących zasad dotyczących ochrony danych osobowych.

Z Agencją można się kontaktować w następujący sposób:

Adres Av. Pte. Gral. Julio A. Roca 710, 5. piętro – Autonomiczne miasto Buenos Aires

Kod pocztowy: C1067ABP

Numer telefonu (54-11) 3988-3968

Adres e-mail: datospersonales@aaip.gob.ar

DODATEK D: SINGAPUR

W przypadku mieszkańców Singapuru zastosowanie mają następujące postanowienia:

D1. Gromadzenie, wykorzystywanie i ujawnianie danych osobowych użytkownika

Jeśli użytkownik jest mieszkańcem Singapuru i za jego zgodą, będziemy gromadzić, wykorzystywać lub w inny sposób ujawniać jego dane osobowe w każdym z celów określonych w naszej informacji o ochronie prywatności. Użytkownik może skorzystać z prawa do wycofania zgody w dowolnym momencie, ale należy pamiętać, że możemy nie być w stanie nadal świadczyć mu naszych usług w zależności od charakteru i zakresu wniosku. Należy również pamiętać, że wycofanie zgody nie wpływa na nasze prawo do dalszego gromadzenia, wykorzystywania i ujawniania danych osobowych, jeśli takie gromadzenie, wykorzystywanie i ujawnianie bez zgody jest dozwolone lub wymagane przez obowiązujące prawo[1].

D2. Korzystanie z praw osób, których dane dotyczą

Użytkownik może kontrolować zgromadzone przez nas dane osobowe i skorzystać z dowolnych praw, kontaktując się z nami za pośrednictwem naszego [portalu wniosków](#). Naszym celem jest niezwłoczne udzielenie odpowiedzi na żądanie użytkownika, zazwyczaj w ciągu 30 dni. Poinformujemy użytkownika z wyprzedzeniem, jeśli nie będziemy w stanie odpowiedzieć na jego żądanie w ciągu 30 dni lub jeśli nie będziemy w stanie spełnić jego żądania i prześlemy uzasadnienie[2].

Tam, gdzie jest to dozwolone przez prawo, możemy obciążyć użytkownika opłatą administracyjną w celu spełnienia jego żądania.

D3. Przekazywanie danych osobowych użytkownika do innych krajów

Jeśli użytkownik jest mieszkańcem Singapuru, a zgromadziliśmy jego dane, możemy od czasu do czasu przekazywać jego dane poza Singapur. Zawsze będziemy jednak zapewniać objęcie danych osobowych użytkownika standardem ochrony, który będzie co najmniej porównywalny ze standardem zapewnionym na mocy singapurskiej Ustawy o ochronie danych osobowych z 2012 r., np. poprzez stosowanie standardowych klauzul umownych ASEAN.

DODATEK E – KOREA POŁUDNIOWA

Niniejszy Dodatek dla osób, których dane dotyczą, mieszkających w Korei dotyczy naszych praktyk w odniesieniu do danych osobowych, które przetwarzamy w związku z relacją użytkownika z nami, gdy jest on osobą, której dane dotyczą, zamieszkującą w Korei.

E.1 – Przekazywanie danych osobowych

Przekazujemy dane osobowe podmiotom zewnętrznym lub zlecamy ich przetwarzanie podmiotom zewnętrznym w sposób określony poniżej:

– Przekazywanie danych osobowych podmiotom zewnętrznym

Nazwa odbiorcy	Cele wykorzystywania przez odbiorcę	Dane osobowe przekazywane odbiorcy	Okresy przechowywania danych przez odbiorcę
Tools for Humanity GmbH	Cele opisane w części 6 niniejszej Informacji powyżej.	Pozycje opisane w części 5 niniejszej Informacji powyżej.	Okresy przechowywania określone w części 11 niniejszej Informacji powyżej.

– Powierzenie przetwarzania danych osobowych podmiotom zewnętrznym:

Listę wszystkich danych powierzonych do przetwarzania i odnośnych podmiotów przetwarzających można znaleźć pod adresem: <https://www.toolsforhumanity.com/processors>

Użytkownik może zlecać przetwarzanie jego danych osobowych lub przekazywać jego dane osobowe do celów przechowywania podmiotom zewnętrznym znajdującym się poza Koreą:

Jeśli użytkownik nie chce przekazywać swoich danych osobowych za granicę, może odmówić i nie wyrazić zgody na przekazywanie danych osobowych lub zażądać od nas zaprzestania transgranicznego przekazywania danych, jednak w przypadku odmowy użytkownik może nie być w stanie korzystać z naszych usług. Podstawą prawną powyższego transgranicznego transferu danych osobowych jest fakt, że stanowi on powierzenie przetwarzania lub przechowywania danych osobowych, które jest niezbędne do zawarcia i wykonania umowy z osobą, której dane dotyczą, a kwestie określone ustawowo zostały przedstawione w polityce prywatności (art. 28-8 ust. 1 lit. iii) ustawy o ochronie danych osobowych).

E.2 – Niszczenie danych osobowych

Gdy dane osobowe stają się zbędne z powodu upływu okresu przechowywania lub osiągnięcia celu przetwarzania itp., są niezwłocznie niszczone. Proces i metoda niszczenia zostały przedstawione poniżej:

1) Proces niszczenia: Wybieramy określone elementy danych osobowych do zniszczenia i niszczymy je za zgodą IOD.

2) Metoda niszczenia: Niszczymy dane osobowe zapisane i przechowywane w formie plików elektronicznych, stosując metodę techniczną (np. formatowanie niskiego poziomu) w celu zapewnienia, że dane nie będą mogły zostać odtworzone, a dane osobowe zapisane i przechowywane w formie dokumentów papierowych są niszczone lub spalane.

E.3 – Przechowywanie danych osobowych

W przypadku gdy mamy obowiązek przechowywać dane osobowe użytkownika zgodnie z obowiązującymi przepisami prawa, będziemy to robić w następujących celach i przez okres wymagany na mocy obowiązujących przepisów prawa.

E.4 – Prawa przysługujące użytkownikom

Użytkownik może dochodzić wobec nas swoich praw związanych z danymi osobowymi, w tym żądać dostępu do jego danych osobowych, ich modyfikacji, usunięcia lub zawieszenia ich przetwarzania, zgodnie z obowiązującymi przepisami prawa, w tym Ustawą o ochronie danych osobowych. Użytkownik może również skorzystać z prawa do wycofania zgody na

gromadzenie/wykorzystywanie/podawanie danych osobowych, prawa do przenoszenia danych oraz prawa dotyczącego zautomatyzowanego podejmowania decyzji. Z takich praw można również skorzystać za pośrednictwem przedstawicieli prawnych użytkownika lub innych należycie upoważnionych przez niego osób.

Użytkownik może skorzystać z przysługujących mu praw opisanych powyżej, kontaktując się z nami pod adresem world.org/requestportal.

E.5 – Środki bezpieczeństwa

Wdrożymy techniczne, organizacyjne i fizyczne środki bezpieczeństwa określone przez obowiązujące przepisy prawa koreańskiego w celu ochrony danych osobowych, w tym te wymienione poniżej:

- 1) Środki zarządcze: Wyznaczenie inspektora ochrony danych, opracowanie i wdrożenie wewnętrznego planu zarządzania, regularne szkolenia pracowników w zakresie ochrony danych itp;
- 2) Środki techniczne: Zarządzanie uprawnieniami dostępu do systemu przetwarzania danych osobowych, instalacja systemu kontroli dostępu, instalacja programów kontroli bezpieczeństwa itp.; oraz
- 3) Środki fizyczne: Ograniczenie dostępu do pomieszczeń i urządzeń służących do przechowywania danych osobowych, takich jak sale komputerowe i pomieszczenia do przechowywania danych itp.

E.6 – Kontakt z nami

W przypadku pytań lub wątpliwości związanych z prywatnością i ochroną danych należy skontaktować się z naszym Zespołem ds. ochrony danych pod adresem dpo@toolsforhumanity.com.

DODATEK F – USA

Kalifornijska ustawa dotycząca ochrony prywatności konsumentów, z późniejszymi zmianami wprowadzonymi na mocy przepisów kalifornijskiej ustawy dotyczącej praw w zakresie ochrony prywatności, nie ma obecnie do nas zastosowania.

DODATEK G – BRAZYLIA

G.1 Obowiązujące przepisy prawa, Administrator danych i Operator

Jeśli użytkownik mieszka w Brazylii, jeśli jego dane osobowe zostały zebrane w Brazylii lub jeśli korzysta z naszych usług w Brazylii, zastosowanie ma ustawa nr 13,709/2018 (Ogólne prawo o ochronie danych, "LGPD").

G.2 Prawo do sprzeciwu

Jeśli cel przetwarzania jest niezgodny z ustawą LGPD, użytkownik ma prawo wnieść sprzeciw wobec przetwarzania dotyczących go danych osobowych, które są przetwarzane na podstawie innej niż zgoda użytkownika. Jeśli sprzeciw użytkownika zostanie uhonorowany, nie będziemy już wykorzystywać jego danych osobowych do opracowywania i ulepszania funkcji i doświadczeń związanych z naszymi Usługami.

Należy pamiętać, że jeśli użytkownik nie poda określonych danych osobowych ani nie zezwoli na ich gromadzenie lub przetwarzanie, może to wpłynąć na jakość jego doświadczeń, możemy nie być w stanie zrealizować celów naszych Usług lub możemy nie być w stanie świadczyć na rzecz użytkownika określonych Usług.

W niektórych przypadkach dane użytkownika poddawane są anonimizacji, co oznacza, że nie będą one określać tożsamości użytkownika. Wobec wykorzystywania zanonimizowanych danych nie będzie możliwe wniesienie sprzeciwu, ponieważ danego tego rodzaju, zgodnie z ustawą LGPD, nie pozwalają na identyfikację użytkownika. Zanonimizowane dane wykorzystujemy do ulepszania naszych produktów i usług.

G.3 Prawa ustawowe wynikające z ustawy LGPD

Zgodnie z ustawą LGPD użytkownik ma prawo potwierdzić fakt dokonywania przetwarzania, uzyskania dostępu, wprowadzenia sprostowania lub żądania przeniesienia przetwarzanych danych. Ponadto użytkownik może zażądać informacji na temat zarówno

publicznych, jak i prywatnych podmiotów, z którymi wspólnie wykorzystujemy jego dane osobowe. Może on również zażądać informacji dotyczących możliwości nieudzielenia zgody i negatywnych konsekwencji takiego działania oraz zażądać usunięcia danych przetwarzanych za zgodą użytkownika. W aplikacji World App w menu Ustawienia można wybrać opcję usunięcia swoich danych.

W określonych okolicznościach użytkownik ma prawo sprzeciwić się przetwarzaniu jego danych osobowych lub ograniczyć sposób ich przetwarzania bądź wycofać swoją zgodę, na której polegamy przy przetwarzaniu przekazanych przez użytkownika informacji.

Użytkownik może skorzystać ze swoich praw wynikających z ustawy LGPD, składając wniosek do naszego IOD, korzystając z danych kontaktowych podanych w części H.4 poniżej lub za pośrednictwem naszego internetowego portalu wniosków. Jeśli użytkownik uważa, że jego prawa nie zostały odpowiednio poszanowane, może wówczas złożyć skargę do Autoridade Nacional de Proteção de Dados Pessoais (ANPD), wypełniając formularz dostępny pod adresem: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados.

G.4 Przekazywanie danych osobowych użytkownika za granicę

Jeśli LGPD ma zastosowanie do użytkownika i zgromadziliśmy jego dane osobowe, możemy również przesłać je poza granice kraju. Zawsze będziemy jednak zapewniać, że dane osobowe użytkownika są przekazywane wyłącznie do innych krajów lub organizacji międzynarodowych, które zapewniają poziom ochrony adekwatny do tego, który przewidziano w LGPD, zgodnie z decyzjami stwierdzającymi odpowiedni stopień ochrony wydanymi przez ANPD. W przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony będziemy nadal przestrzegać standardu ochrony, który jest co najmniej równoważny standardowi przewidzianemu w LGPD, z wykorzystaniem Standardowych klauzul umownych ustanowionych w przepisach ANPD lub po uzyskaniu przez nas wyraźnej i wyróżnionej zgody użytkownika na przekazywanie danych za granicę.

ZAŁĄCZNIK I – Podstawy prawne/cele przetwarzania danych przez Tools for Humanity

Użytkownicy

Cel przetwarzania danych	Przetwarzane dane osobowe	Podstawa prawna przetwarzania	Okres przechowywania
Utworzenie konta w aplikacji World App	Adres portfela, metadane, nazwa użytkownika	Realizacja umowy	Czas korzystania z usług lub do momentu zażądania usunięcia danych.
Upewnienie się, że użytkownik spełnia wymagania wiekowe	Data urodzenia	Obowiązek prawny	Dokładna data urodzenia użytkownika nigdy nie jest przechowywana. Odnotowujemy jedynie fakt, czy użytkownik ma ukończone 18 lat. Informację tę przechowujemy przez czas korzystania z usług lub do momentu zażądania usunięcia danych.
Opcjonalne umożliwienie kontaktom łatwej komunikacji i transakcji z użytkownikiem	Numer telefonu	Zgoda	Czas korzystania z usług lub do momentu zażądania usunięcia danych.
Umożliwienie użytkownikowi łatwej komunikacji i transakcji z jego kontaktami	Kontakty z książki adresowej	Zgoda	Czas korzystania z usług lub do momentu zażądania usunięcia danych.
Opcjonalne pokazanie użytkownikowi organizacji w	Informacje o lokalizacji	Zgoda	Do 24 miesięcy.

jego okolicy			
Zapobieganie oszustwom w kontekście zabezpieczania konta	Metadane, adres IP, identyfikator urządzenia	Uzasadniony interes, a mianowicie interes mający na celu zapobieganie określonym rodzajom oszustw (SPIS RODZAJÓW)	Do 24 miesięcy.
Aby zapewnić, że usługa jest dozwolona w kraju użytkownika	Adres IP, informacje o lokalizacji	Obowiązek prawny	Do 24 miesięcy.
Wyświetlenie portfela osobistego i zapewnienie interfejsu do transakcji w ramach portfela	Adres portfela, dane dotyczące transakcji	Realizacja umowy	W tym kontekście nie są przechowywane żadne dane osobowe.
Wyświetlenie własnego identyfikatora World ID użytkownika i zapewnienie interfejsu do weryfikacji	Informacje o identyfikatorze World ID	Realizacja umowy	W tym kontekście nie są przechowywane żadne dane osobowe.
Wyświetlenie danych uwierzytelniających do samodzielnego przechowywania danych i zapewnienie interfejsu do udostępniania danych uwierzytelniających	Informacje na temat danych uwierzytelniających, informacje o ważności metody uwierzytelniania	Realizacja umowy	W tym kontekście nie są przechowywane żadne dane osobowe.
Analizowanie i ulepszanie naszych usług oraz prowadzenie badań w zakresie nauki o danych	Dane dotyczące użytkownika i metadane, dane dotyczące transakcji publicznych	Zgoda	Do 24 miesięcy.
Przestrzeganie obowiązujących przepisów prawa, takich jak przepisy dotyczące przeciwdziałania praniu pieniędzy i sankcje	Dane dotyczące transakcji, adres portfela	Obowiązek prawny	Czas korzystania z usług.
Zachowanie zgodności z obowiązującymi przepisami prawa, np. regulacjami przeciwdziałającymi	Treść mini aplikacji	Obowiązek prawny	Czas korzystania z usług.

nielegalnym treściom			
Umożliwienie prowadzenia komunikacji i marketingu	Adres e-mail, powiadomienia push	Prawnie uzasadniony interes	Do 24 miesięcy.
	Korespondencja od użytkownika	Prawnie uzasadniony interes	Do 24 miesięcy.
	Opinie użytkownika	Prawnie uzasadniony interes	Do 24 miesięcy.
obsługę żądań, skarg i zapytań użytkownika dotyczących obsługi klienta;	Informacje dotyczące komunikacji oraz adresów e-mail lub nazw profili w mediach społecznościowych, jeśli użytkownik chce się z nami skontaktować za pośrednictwem jednego z tych kanałów	Realizacja umowy	
Zapewnienie płynnego działania aplikacji	Metadane	Realizacja umowy	Do 24 miesięcy.
Weryfikacja urządzenia	Dane identyfikatora World ID urządzenia (odcisk palca urządzenia)	Realizacja umowy	Czas korzystania z usług.
rozstrzyganie sporów, rozwiązywanie problemów i egzekwowanie postanowień naszych umów z użytkownikiem, w tym niniejszej Informacji o ochronie prywatności i Regulaminu świadczenia usług;			Czas korzystania z usług.

Partnerzy biznesowi

Cel przetwarzania danych	Przetwarzane dane osobowe	Podstawa prawna przetwarzania	Okres przechowywania
	Numer telefonu, adres	Uzasadnione interesy, tj. interes polegający	Czas trwania relacji biznesowej

komunikacja;	e-mail, imię i nazwisko	na komunikacji z partnerami biznesowymi.	lub do momentu zażądania usunięcia danych.
Utrzymywanie i administrowanie relacjami biznesowymi	Numer telefonu, adres e-mail, imię i nazwisko, dane przedsiębiorstwa	Uzasadnione interesy, tj. interes polegający na utrzymywaniu i administrowaniu relacjami biznesowymi z partnerami biznesowymi.	Czas trwania relacji biznesowej lub do momentu zażądania usunięcia danych.
Realizacja zobowiązań w zakresie ZK	Dane dotyczące paszportu, dane przedsiębiorstwa	Obowiązek prawny	Czas trwania relacji biznesowej i do 3 lat po rozwiązaniu umowy.
Rozpatrzenie podania	Dane dotyczące podania o pracę	Zgoda i kroki podejmowane na wniosek osoby, której dane dotyczą, przed zawarciem umowy.	Domyślnie do 3 miesięcy lub dłużej, jeśli użytkownik zgodzi się na włączenie do puli talentów.

TFHPS20241017