

Polityka prywatności Tools for Humanity

Niniejsza Polityka prywatności wyjaśnia, w jaki sposób spółka Tools for Humanity Corporation („My”, „TFH”) przetwarza dane użytkowników korzystających z naszych stron internetowych, usług i aplikacji – takich jak World App, World ID i World Money, wraz z wszelkimi ich ewentualnymi aktualizacjami („Aplikacje”) – (łącznie zwanych naszymi „Usługami”). Staraliśmy się, aby treść niniejszej polityki była łatwa do zrozumienia i pragniemy podkreślić, że **nigdy nie sprzedajemy danych osobowych użytkowników**.

W przypadku korzystania z Usługi TFH lub Orba zbudowanego przez TFH w celu weryfikacji identyfikatora World ID, zastosowanie wobec użytkownika ma pierwsza część niniejszej Polityki prywatności. Inne firmy mogą tworzyć aplikacje („Kompatybilne aplikacje”) i/lub Orby, aby umożliwić użytkownikom tworzenie, przechowywanie, weryfikowanie lub używanie identyfikatorów World ID.

Weryfikacja World ID i Orb

Identyfikator World ID można utworzyć i zapisać za pomocą [Kompatybilnej aplikacji](#). Po utworzeniu i zapisaniu identyfikatora World ID można go zweryfikować.

Tworzenie identyfikatora World ID

Proces zaczyna się od zainstalowania Kompatybilnej aplikacji na telefonie. Kompatybilna aplikacja automatycznie utworzy losowy numer, który zostanie przypisany jako szyfr identyfikatora World ID. Zostanie on zapisany na telefonie użytkownika i nigdy nie jest nikomu ujawniany.

Weryfikacja identyfikatora World ID

Aby zweryfikować swój identyfikator World ID, użytkownik może umówić się na spotkanie z Orbem. Na spotkaniu Orb: sfotografuje twarz i oczy; przeanalizuje zdjęcia, aby potwierdzić, że użytkownik jest unikalnym człowiekiem; wygeneruje kod tęczy; zanonimizuje kod tęczy; zaszyfruje obrazy, kod tęczy i zanonimizowane dane, a następnie prześle je na telefon użytkownika; i trwale usunie wszystkie te dane z pamięci Orba. [Dowiedz się więcej o Orbie](#).

Ludzka tożsamość

W pierwszej kolejności sieci neuronowe w Orbie oceniają obrazy w celu ustalenia, czy osoba na obrazach jest żywym człowiekiem tak, aby zablokować obrazy i zdjęcia stworzone za pomocą technologii deepfake wyświetlane na ekranie w celu oszukania Orba.

Niepowtarzalność

W drugiej kolejności sprawdzamy, czy użytkownik nie zweryfikował już wcześniej World ID – to gwarantuje że użytkownik jest niepowtarzalny. W tym celu Orb generuje abstrakcje obrazów oka i tworzy kod tęczy. [Kod tęczy](#) jest wynikiem matematycznej reprezentacji obrazów oka użytkownika. Kod tęczy jest następnie dzielony na udziały kryptograficzne przy użyciu schematu Dzielenia sekretu i dystrybuowany pomiędzy niezależnymi węzłami w sieci obliczeń wielopodmiotowych –

proces ten nazywany jest zanonimizowanymi obliczeniami wielopodmiotowymi lub AMPC (Anonymized Multi Party Computation). [Dowiedz się więcej o obliczaniu AMPC](#). Po anonimizacji niepowtarzalność jest weryfikowana w drodze kryptograficznego porównywania udziałów obliczeń AMPC z dużymi bazami danych innych udziałów obliczeń AMPC, których nie da się powiązać z osobą fizyczną, aby sprawdzić, czy nowe udziały obliczeń AMPC są rzeczywiście niepowtarzalne.

Weryfikacja wieku

W ramach niektórych procesów weryfikacji lub bezpieczeństwa TFH może stosować technologie analizy twarzy lub szacowania wieku w celu oceny, czy dana osoba wydaje się spełniać wymogi dotyczące minimalnego wieku, lub w celu wykrycia potencjalnie niepełnoletnich użytkowników. Systemy te są używane wyłącznie w celach związanych z bezpieczeństwem, zachowywaniem zgodności z przepisami prawa oraz zapobieganiem oszustwom i nie służą do identyfikacji tożsamości osób.

Przechowywanie

Obrazy, kod tęczówki i udziały obliczeń AMPC są kryptograficznie podpisane i zaszyfrowane tak, aby można je było bezpiecznie przechowywać w telefonie i przysyłać. Dane są następnie trwale usuwane z pamięci Orba. Oznacza to, że tylko użytkownik dysponuje egzemplarzem swoich danych osobowych. [Dowiedz się więcej o osobistym przechowywaniu](#). W celach związanych z uwierzytelnianiem za pomocą twarzy można użyć obrazów w telefonie. Funkcja uwierzytelniania za pomocą twarzy dopasowuje selfie twarzy użytkownika do kryptograficznie podpisanych obrazów zrobionych przez Orb, aby upewnić się, że użytkownik jest prawowitym właścicielem poszczególnego identyfikatora World ID. Uwierzytelnianie za pomocą twarzy można też przeprowadzić w pełni na telefonie. [Dowiedz się więcej o uwierzytelnianiu za pomocą twarzy](#).

W jaki sposób dane są anonimizowane?

Proces szyfrowania udziałów obliczeń AMPC jest oparty na losowości – nawet jeśli użytkownik spróbuje dokonać weryfikacji dwukrotnie, za każdym razem udziały będą inne. Specjalna metoda, za sprawą której powstają udziały obliczeń AMPC, pozwala na wykorzystanie udziałów do ustalenia niepowtarzalności, jednak nie pozwala na nic więcej. Fakt, iż udziały obliczeń AMPC przechowywane są przez uniwersytety i inne strony, które cieszą się zaufaniem publicznym, gwarantuje, że udziały obliczeń AMPC nie będą ponownie łączone ani wykorzystywane do żadnych innych celów poza sprawdzaniem niepowtarzalności. Dzięki temu żadne dane osobowe nie są przechowywane ani dostępne dla żadnego autora lub uczestnika protokołu World Protocol ani żadnego podmiotu zewnętrznego.

Korzystanie z identyfikatora World ID

Jeśli weryfikacja użytkownika za pomocą Orba zakończy się powodzeniem, skrót szyfru identyfikatora World ID użytkownika (losowa liczba) zostanie dodany do [publicznej listy zweryfikowanych skrótów identyfikatorów World ID](#) bez poznawania tożsamości użytkownika i bez dostępu do danych zgromadzonych przez Orba. Gdy użytkownik używa swojego identyfikatora World ID, za pomocą telefonu udowadnia, że posiada szyfr identyfikatora World ID pasujący do jednego ze skrótów zapisanych w Drzewie skrótów, bez potrzeby ujawniania szyfru. Wykorzystanie w ramach tego procesu metody dowodu z wiedzą zerową gwarantuje, że użytkownik nie musi ujawniać skrótów, które wykorzystuje. Dzięki metodzie dowodu z wiedzą zerową można stworzyć nullifier skrótu dla określonego działania, które można najlepiej opisać jako konkretny, jednorazowy identyfikator World ID. Umożliwia to korzystanie z usługi World ID w sposób anonimowy. Oznacza to, że jeśli użytkownik zaloguje się do dwóch różnych usług za pomocą identyfikatora World ID, a usługi te spróbują użytkownika zidentyfikować, udostępniając nullifier skrótu, usługi te nie będą w stanie zidentyfikować użytkownika. Nie rozwiązuje to kwestii identyfikacji

ani nie powstrzymuje identyfikacji przez te usługi użytkownika za pomocą innych środków używanych w przeszłości przez platformy internetowe, ale z czasem może pomóc rozwiązać problem śledzenia użytkowników online. [Dowiedz się więcej o metodzie dowodu z wiedzą zerową.](#)

Dane osobowe, które zbieramy i wykorzystujemy

Zbieramy dane osobowe użytkownika w przypadkach, w których użytkownik takie dane nam przekazuje bądź gdy korzysta z naszych Usług. W ograniczonych przypadkach otrzymujemy również dane osobowe od podmiotów zewnętrznych. Jak [wyjaśniono poniżej](#), użytkownik może uzyskać dostęp do swoich danych osobowych oraz poprawić lub usunąć je w dowolnym momencie.

Dane osobowe, które użytkownik nam przekazuje

W pewnych okolicznościach i w zależności od funkcjonalności Aplikacji możemy prosić użytkownika o przekazanie nam danych lub użytkownik może przekazać nam dane z własnej inicjatywy. Użytkownik może zmodyfikować lub usunąć je w dowolnym momencie w ustawieniach naszych Aplikacji.

- Użytkownik może dodać swój **numer telefonu**. Pomaga to kontaktom użytkownika znaleźć go i nawiązać z nim kontakt. Numeru telefonu można też użyć, aby przywrócić kopie zapasowe lub skorzystać z naszego systemu poleceń ([patrz nasze rekomendacje partnerskie](#)).
- Użytkownik może zsynchronizować swoje **kontakty**. Umożliwia to sprawdzenie, które z kontaktów z książki adresowej użytkownika dodały swój numer telefonu do swojej Aplikacji, co pozwala użytkownikowi łatwiej się z nimi łączyć i wchodzić z nimi w interakcje. Kontakty użytkownika nie są przez nas zapisywane.
- Użytkownik może stworzyć **nazwę użytkownika**, którą można [zmienić w dowolnym momencie](#). Nazwa użytkownika jest powiązana wyłącznie z jego aplikacją, a nie identyfikatorem World ID.
- Użytkownik może nam udostępnić swoją **lokalizację geograficzną**, na przykład w celu znalezienia w pobliżu Orba i pomocy nam w zrozumieniu, gdzie w przyszłości powinniśmy umieścić nowe Orby.
- Użytkownik zostanie poproszony o wprowadzenie **daty urodzenia**. Data urodzenia użytkownika nie jest przechowywana i jest używana na urządzeniu użytkownika wyłącznie w celu ustalenia, czy spełnia on minimalne wymagania wiekowe do korzystania z Usług.
- W przypadku gdy użytkownik się z nami skontaktuje, na przykład w celu uzyskania pomocy lub wsparcia, będziemy przetwarzać **wiadomości i korespondencję** z użytkownikiem, które mogą zawierać dane osobowe użytkownika. W przypadku gdy użytkownik przekaże nam swoją opinię, odpowiadając na ankietę, uzyskane w ten sposób informacje zwrotne będą wykorzystane w celu poprawy naszych usług.
- W przypadku gdy użytkownik korzysta z funkcji czatu, **nie widzimy jego wiadomości ani nie mamy do nich dostępu**. Wiadomości i powiązane metadane są szyfrowane metodą end-to-end i nie możemy ich odszyfrować ani w inny sposób uzyskać do nich dostępu. Zasyfrowane wiadomości są przekierowywane przez nasz serwer bezpośrednio od nadawcy wiadomości do jej odbiorcy.
- Użytkownik może też podjąć decyzję o zezwoleniu nam na analizowanie informacji na temat **jego interakcji z naszymi Aplikacjami**, aby pomóc nam znaleźć błędy i usprawniać nasze produkty.
- Użytkownik może podać swoje dane w celu **usprawnienia World ID dla wszystkich**. Aby zapewnić bezpieczeństwo, niezawodność i integracyjność programu identyfikatorów World ID, modele, które go napędzają, wymagają danych szkoleniowych pochodzących od zróżnicowanej populacji. Aby pomóc w szkoleniu tych modeli, użytkownik może opcjonalnie

udostępnić swoje obrazy z Orba i zdjęcia, z których użytkownik korzysta w celach związanych z uwierzytelnianiem za pomocą twarzy.

- Do niektórych spośród naszych aplikacji można dodać **Dane uwierzytelniające**, takie jak paszport. Sprawdzimy podane przez użytkownika dane uwierzytelniające, potwierdzimy, że jego twarz pasuje do zdjęcia zawartego w przesłanych danych uwierzytelniających, a następnie zapiszemy dane uwierzytelniające na urządzeniu użytkownika. Nigdy nie mamy dostępu do danych osobowych zawartych w danych uwierzytelniających użytkownika.
- Użytkownik może podjąć decyzję o zweryfikowaniu swojego World ID za pomocą zdjęcia selfie (**Selfie Check**). Zdjęcie jest przechowywane lokalnie na urządzeniu użytkownika. Selfie jest przetwarzane w celu zapewnienia jego unikalności i człowieczeństwa, a przez TFH przechowywane są wyłącznie dane zanonimizowane.
- Użytkownik może zdecydować o korzystaniu z naszych funkcji Deep Face na niektórych platformach podmiotów zewnętrznych (np. aplikacjach do prowadzenia wideokonferencji i czatów wideo), aby pomóc chronić swoje konta przed podszywaniem się, deepfake'ami, atakami typu replay oraz innymi działaniami oszukańczymi. Po włączeniu tej funkcji obrazy twarzy, zdjęcia selfie, krótkie nagrania wideo lub powiązane z nimi dane weryfikacji biometrycznej mogą być przetwarzane w celu oceny człowieczeństwa i wykrycia żywotności oraz ustalenia, czy treść wydaje się autentyczna, czy wygenerowana syntetycznie. Wszystkie dane biometryczne są przetwarzane lokalnie na urządzeniu użytkownika, a TFH przechowuje wyłącznie dane zanonimizowane.

Informacje, które zbieramy, gdy użytkownik korzysta z naszych Usług

- Gdy użytkownik korzysta z naszych Aplikacji, zbieramy informacje o jego połączeniu, takie jak **adres IP**, rodzaj przeglądarki i inne powiązane dane, aby świadczyć nasze Usługi i dostosowywać je do kraju, w którym użytkownik się znajduje. Zbieramy także dodatkowe **metadane urządzenia**, takie jak rozdzielczość ekranu, system operacyjny, operator, język, pamięć, zainstalowane aplikacje, poziom naładowania baterii i numer urządzenia, aby zapewnić prawidłowe działanie aplikacji na urządzeniu i zgodność z naszym [Regulaminem](#). Dane te wykorzystujemy również do wykrywania oszustw i zapobiegania im.
- Zbieramy także dodatkowe informacje na temat **interakcji użytkownika z naszymi Aplikacjami**, aby zagwarantować, że działają one zgodnie z oczekiwaniami użytkownika (np. przechowujemy ustawienia i poziom weryfikacji w celu wyświetlenia odpowiedniego interfejsu).
- Gdy użytkownik po raz pierwszy otworzy aplikację World App na swoim telefonie, losowo wygeneruje ona portfel kryptograficzny zawierający **adres portfela** użytkownika. Adres tego portfela jest przez nas przetwarzany, aby umożliwić transakcje związane z portfelem. Klucz prywatny do portfela jest przechowywany tylko na urządzeniu użytkownika i nigdy nie będziemy mieć do niego dostępu.
- W celu spełnienia zobowiązań prawnych i zapewnienia interfejsu dla transakcji w technologii blockchain, zbieramy aktualne kopie stanu **publicznych sieci blockchain**, które mogą zawierać poprzednie, publiczne transakcje.
- Nasze strony internetowe wykorzystują **pliki cookie**. Pliki cookie to małe pliki tekstowe przechowywane na urządzeniu użytkownika, wykorzystywane przez usługi online do identyfikacji urządzenia i/lub preferencji użytkownika. Używamy funkcjonalnych plików cookie, aby zagwarantować użytkownikowi prawidłowe funkcjonowanie strony internetowej, oraz opcjonalnych plików cookie, aby analizować i usprawniać sposób korzystania z naszych stron internetowych. Pełną listę plików cookie oraz wyborów użytkownika w kwestii odrzucenia plików cookie innych niż niezbędne można znaleźć w naszej [Polityce dotyczącej plików cookie](#).

Informacje, które możemy otrzymywać od podmiotów zewnętrznych

- W przypadku gdy użytkownik będzie potrzebował skorzystać z naszego [portalu wsparcia](#) w celu weryfikacji wieku, zwrócimy się z prośbą o potwierdzenie od podmiotu zewnętrznego, który niezależnie zweryfikował wiek użytkownika, że użytkownik co najmniej osiągnął **pełnoletniość** w swoim kraju. Od wspomnianego podmiotu zewnętrznego nie otrzymujemy żadnych informacji.

- Aby zapobiegać oszustwom i nielegalnym działaniom w naszych Usługach, otrzymujemy od zewnętrznych dostawców informacje o urządzeniach i portfelach blockchain powiązanych z potencjalnymi oszustwami i nielegalną działalnością.

Udostępnianie danych osobowych

W ramach TFH mogą to robić wyłącznie ci członkowie zespołu, którzy muszą uzyskać dostęp do danych osobowych lub zobaczyć je, w związku z wykonywaniem swoich zadań, a my stosujemy ściśle środki kontroli dostępu, aby zapewnić przestrzeganie tej zasady. Zlecamy przetwarzanie danych wyłącznie zaufanym i bezpiecznym dostawcom oraz usługodawcom. Obejmuje to certyfikowanych dostawców usług w chmurze, dostawców oprogramowania i firmy zajmujące się bezpieczeństwem IT. Tutaj można znaleźć [pełną listą naszych zewnętrznych podmiotów przetwarzających](#).

Możemy udostępniać dane użytkownika w celu spełnienia wymogów prawnych lub w odpowiedzi na zgodne z prawem żądania organów ścigania. W przypadku gdy działania użytkownika naruszać będą postanowienia naszego [Regulaminu](#) lub stanowić będą zagrożenie dla naszych praw lub praw innych osób, możemy przekazać dane dotyczące użytkownika odpowiednim organom. Możemy udostępniać dane osobowe użytkownika za jego zgodą lub na jego polecenie.

TFH i protokół World ID zostały zaprojektowane tak, aby zminimalizować ilość danych osobowych udostępnianych tym podmiotom. Podczas korzystania przez użytkownika z World ID w aplikacjach, na stronach internetowych lub w usługach podmiotów zewnętrznych („Podmioty polegające na danych”), Podmioty polegające na danych nie otrzymują obrazów twarzy lub oczu, kodu tęczówki, szyfru identyfikatora World ID, ani innych źródłowych danych biometrycznych użytkownika. Zamiast tego podmioty te otrzymują dowody kryptograficzne lub wyniki weryfikacji wygenerowane przy użyciu [technologii dowodów z wiedzą zerową](#), które mają na celu potwierdzenie określonych faktów — takich jak to, że użytkownik jest unikalnym człowiekiem, że posiada ważne poświadczenie lub że nie wykonał wcześniej określonej czynności — bez ujawniania tożsamości użytkownika lub źródłowych informacji biometrycznych. W zależności od kontekstu i obowiązującego prawa, niektóre sygnały weryfikacyjne, identyfikatory lub powiązane metadane mogą stanowić dane osobowe. Strony polegające na danych są co do zasady niezależnymi administratorami wszelkich danych osobowych, które przetwarzają w związku ze swoimi usługami, a dokonywane przez nie przetwarzanie danych podlega ich odpowiednim politykom prywatności.

Jak długo przechowujemy dane osobowe?

Zasadniczo przechowujemy dane osobowe użytkownika w sposób opisany poniżej:

- dane osobowe, które są nam przekazywane przez użytkownika, przechowujemy tak długo, jak długo użytkownik korzysta z naszych Usług lub dopóki użytkownik nie zdecyduje się na ich modyfikację lub usunięcie;
- informacje, które zbieramy, gdy użytkownik korzysta z naszych Usług, przechowujemy nie dłużej niż dwa lata. Wcześniejsze interakcje użytkownika z aplikacją World App (które są wymagane do utrzymania działania aplikacji) przechowujemy przez okres korzystania z Usług lub do momentu usunięcia konta;
- dane uwierzytelniania za pomocą twarzy są przechowywane wyłącznie na urządzeniu użytkownika i pozostają na nim do momentu usunięcia aplikacji World App przez użytkownika lub usunięcia takich danych z urządzenia użytkownika;
- dane portfela są opublikowane na stałe w publicznej sieci blockchain, której zaktualizowaną kopię często pobieramy; oraz
- informacje, które możemy otrzymywać od podmiotów zewnętrznych (zazwyczaj w celu zapobiegania oszustwom i zapewnienia użytkownikowi i innym osobom bezpieczeństwa podczas korzystania z naszych Usług), przechowujemy przez rok, chyba że użytkownik naruszył nasz Regulamin, wówczas będziemy je przechowywać przez pięć lat.

- Automatycznie usuniemy dane osobowe użytkownika znajdujące się w aplikacji – w tym szczegóły profilu użytkownika, opcjonalne dane analityczne, preferencje powiadomień push oraz wszelkie obrazy przekazane do celów szkoleniowych – w przypadku gdy konto użytkownika będzie pozostawało nieaktywne przez okres 24 miesięcy. Uwaga: użytkownik nie otrzyma dodatkowego powiadomienia o takim usunięciu.

Jeśli będzie to wymagane przez prawo, będziemy przechowywać dane osobowe użytkownika 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.

Szczegółowe informacje na temat konkretnych podstaw prawnych i celów naszych działań związanych z przetwarzaniem danych można znaleźć w poniższej tabeli, w której opisano zbierane przez nas dane, cele ich wykorzystania i jak długo dane są przechowywane.

Prawa użytkownika

Dane użytkownika należą do użytkownika i uważamy, że użytkownik powinien być w stanie łatwo egzekwować swoje prawa w dowolnym momencie. Podczas korzystania z naszych Usług, użytkownik może zawsze:

- dowiedzieć się więcej o przetwarzaniu danych za pomocą [materiałów pomocniczych dostępnych tutaj](#) lub kontaktując się z naszym Inspektorem ochrony danych, którego dane kontaktowe znajdują się poniżej;
- uzyskać dostęp do swoich danych osobowych lub dokonać ich korekty w ustawieniach Aplikacji;
- usunąć dane osobowe w ustawieniach aplikacji; oraz
- wycofać swoją zgodę na przetwarzanie danych, które odbywa się na podstawie zgody użytkownika, lub wyrazić sprzeciw wobec przetwarzania na podstawie prawnie uzasadnionych interesów, w tym żądać ograniczenia przetwarzania poprzez przejście w Aplikacjach do ustawień w części „Prywatność i prawo”.

Użytkownik może skorzystać z przysługujących mu w odniesieniu do Aplikacji praw, klikając w ustawieniach część „Prywatność i prawo”; więcej informacji na temat usuwania można znaleźć [w tym artykule w naszym Centrum pomocy](#).

Ogólne

Przestrzegamy ram ochrony danych osobowych UE-USA (Data Privacy Framework, DPF), aneksu do ram ochrony danych osobowych UE-USA w sprawie Wielkiej Brytanii oraz ram ochrony danych osobowych Szwajcaria-USA (Data Privacy Framework, DPF) określonych przez Departament Handlu USA. Poświadczylimy przed Departamentem Handlu USA, że przestrzegamy zasad programu Ramy ochrony prywatności UE-USA (Zasady DPF UE-USA) w odniesieniu do przetwarzania danych osobowych otrzymywanych z Unii Europejskiej w oparciu o DPF UE-USA oraz z Wielkiej Brytanii (i Gibraltaru) w oparciu o aneks DPF UE-USA w sprawie Wielkiej Brytanii. Poświadczylimy przed Departamentem Handlu USA, że przestrzegamy zasad programu Ramy ochrony danych Szwajcaria-USA (Zasady DPF Szwajcaria-USA) w odniesieniu do przetwarzania danych osobowych otrzymywanych ze Szwajcarii w oparciu o DPF Szwajcaria-USA. W przypadku rozbieżności pomiędzy postanowieniami niniejszej Polityki prywatności i Zasadami DPF 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 [stronę internetową poświęconą ramom ochrony danych](#).

Aby korzystać z naszych Usług, użytkownik musi co najmniej osiągnąć pełnoletniość w swoim kraju (minimalnie 18 lat). Ochronę osób niepełnoletnich traktujemy bardzo poważnie – w przypadku podejrzeń, że osoba poniżej 18 roku życia korzysta z naszych Usług, prosimy o niezwłoczny kontakt za pośrednictwem naszego [Portalu prywatności](#) lub kanałów określonych powyżej.

Niniejsza Polityka prywatności może być przez nas aktualizowana w dowolnym momencie, jednak jeśli zmiany wpłyną na prawa użytkownika, użytkownik zostanie o tym powiadomiony z wyprzedzeniem. Jeśli następnie użytkownik nadal będzie korzystał z naszych Usług, będzie to równoznaczne z zaakceptowaniem naszej zaktualizowanej Polityki prywatności.

Jak się z nami skontaktować?

W przypadku pytań dotyczących niniejszej Polityki prywatności lub innych pytań dotyczących danych można się z nami w dowolnym momencie skontaktować. Użytkownicy zawsze mogą uzyskać kontakt z naszym Biurem ochrony danych oraz naszym Inspektorem ochrony danych (Marc Placzek) pod adresem dpo@toolsforhumanity.com lub wysyłając list na adres: DPO, Tools For Humanity Corporation, 650 7th St, San Francisco, CA 94103, USA.

Jeśli użytkownik mieszka w Stanach Zjednoczonych lub w innym kraju poza Unią Europejską, obszarem EFTA lub Wielką Brytanią, administratorem danych odpowiedzialnym za jego dane osobowe jest Tools For Humanity Corporation, z siedzibą pod adresem 650 7th St, San Francisco, CA 94103, Stany Zjednoczone.

Jeśli użytkownik mieszka w Unii Europejskiej, na obszarze EFTA lub w Wielkiej Brytanii, administratorem danych odpowiedzialnym za jego dane osobowe jest Tools for Humanity GmbH, z siedzibą pod adresem August-Everding-Straße 25, 81671 Monachium, Niemcy.

Użytkownik ma prawo zgłosić wątpliwości dotyczące praktyk w zakresie danych, kontaktując się z lokalnym organem nadzorczym lub organem nadzorczym sprawującym nadzór nad TFH GmbH – Bawarskim Organem Ochrony Danych ("BayLDA"), korzystając z danych kontaktowych podanych na stronie internetowej organu.

[ZAŁĄCZNIK I – Podstawy prawne / cele przetwarzania danych przez Tools for Humanity](#)

TFHPS20260701