

Datenschutzrichtlinie für Tools for Humanity

Diese Datenschutzrichtlinie erläutert, wie Tools for Humanity Corporation („wir“, „TFH“) Ihre Daten verarbeitet, wenn Sie unsere Websites, Services und Apps – wie World App, World ID und World Money nutzen, die von Zeit zu Zeit aktualisiert werden können („Apps“) – (zusammen bezeichnet als unsere „Services“). Wir haben uns bemüht, diese Richtlinie einfach zu halten, und **wir verkaufen niemals Ihre personenbezogenen Daten**.

Wenn Sie einen TFH-Service oder einen von TFH entwickelten Orb nutzen, um Ihre World ID zu verifizieren, ist der erste Abschnitt dieser Datenschutzrichtlinie für Sie relevant. Andere Unternehmen können Apps („Kompatible Anwendungen“) und/oder Orbs entwickeln, mit denen Menschen ihre World ID erstellen, speichern, verifizieren oder nutzen können.

World ID und Orb-Verifizierungen

Sie können eine World ID erstellen und speichern, indem Sie eine [kompatible Anwendung](#) verwenden. Sobald Sie Ihre World ID erstellt und gespeichert haben, können Sie sich entscheiden, Ihre World ID zu verifizieren.

Erstellen einer World ID

Sie beginnen, indem Sie eine kompatible Anwendung auf Ihrem Smartphone installieren. Die kompatible Anwendung erstellt automatisch eine Zufallszahl – Ihr World ID Secret. Diese verbleibt auf Ihrem mobilen Gerät und wird niemals offengelegt.

Verifizieren einer World ID

Um Ihre World ID zu verifizieren, können Sie anschließend einen Termin mit einem Orb vereinbaren. Der Orb wird die folgenden Schritte durchführen: Ihr Gesicht und Ihre Augen fotografieren; die Fotos analysieren, um zu bestätigen, dass Sie ein unverwechselbarer Mensch sind; einen Iris-Code erzeugen; diesen Iris-Code anonymisieren; die Fotos, den Iris-Code und die anonymisierten Daten verschlüsseln und an Ihr Smartphone senden; und all diese Daten dauerhaft vom Orb löschen.

[Erfahren Sie mehr über den Orb.](#)

Menschlichkeit

Zunächst bewerten neuronale Netzwerke auf dem Orb die Fotos, um festzustellen, ob es sich bei der abgebildeten Person um einen lebenden Menschen handelt, und so Deepfake-Bilder und auf einem Bildschirm angezeigte Fotos zu blockieren, mit denen versucht wird, den Orb zu täuschen.

Einzigartigkeit

Zweitens prüfen wir, ob Sie nicht bereits eine World ID verifiziert haben, um sicherzustellen, dass Sie einzigartig sind. Zu diesem Zweck erstellt der Orb Abstraktionen der Augenbilder, um einen Iris-Code zu erzeugen. Ein [Iris-Code](#) entsteht aus einer mathematischen Darstellung Ihrer Augenfotos. Der Iris-Code wird dann mithilfe eines Secret-Sharing-Schemas in kryptografische Fragmente aufgeteilt und über unabhängige Knoten in einem Multi-Party-Computation-Netzwerk verteilt; dies

wird als Anonymized Multi Party Computation oder AMPC bezeichnet. [Erfahren Sie mehr über AMPC](#). Nach der Anonymisierung wird die Einzigartigkeit verifiziert, indem die AMPC-Fragmente kryptografisch mit großen Datenbanken anderer AMPC-Fragmente, die nicht mit einer Person verknüpft werden können, abgeglichen werden, um festzustellen, ob die neuen AMPC-Fragmente tatsächlich einzigartig sind.

Altersprüfung

In einigen Verifizierungs- oder Sicherheitsabläufen kann TFH Technologien zur Gesichtsanalyse oder Altersschätzung verwenden, um zu beurteilen, ob eine Person dem Anschein nach die Mindestaltersvoraussetzungen erfüllt, oder um potenziell minderjährige Nutzer zu erkennen. Diese Systeme werden ausschließlich zu Zwecken der Sicherheit, der Einhaltung gesetzlicher Vorschriften und der Betrugsprävention verwendet und dienen nicht dazu, Personen zu identifizieren.

Datenverwahrung

Die Fotos, der Iris-Code und die AMPC-Fragmente werden kryptografisch signiert und verschlüsselt, sodass sie sicher übertragen und auf Ihrem Smartphone gespeichert werden können. Die Daten werden dann dauerhaft aus dem Orb gelöscht. Das bedeutet, dass ausschließlich Sie selbst eine Kopie Ihrer personenbezogenen Daten besitzen. [Erfahren Sie mehr über die Selbstverwahrung](#). Sie können die Bilder auf Ihrem Smartphone zur Gesichtsauffertifizierung verwenden. Die Gesichtsauffertifizierung gleicht ein Selfie Ihres Gesichts mit den vom Orb aufgenommenen kryptografisch signierten Fotos ab, um sicherzustellen, dass Sie der rechtmäßige Inhaber der World ID sind. Die Gesichtsauffertifizierung erfolgt ebenfalls vollständig auf Ihrem Smartphone. [Erfahren Sie mehr über die Gesichtsauffertifizierung](#).

Wie werden die Daten anonymisiert?

Die Verschlüsselung in AMPC-Anteile erfolgt zufällig – selbst wenn Sie versuchen, sich zweimal zu verifizieren, sind die Fragmente jedes Mal völlig unterschiedlich. Durch das spezielle Verfahren zur Berechnung der AMPC-Anteile ist es möglich, die Einzigartigkeit festzustellen, jedoch keine weiteren Rückschlüsse zu ziehen. Die Speicherung der AMPC-Fragmente bei Universitäten und anderen Stellen, die öffentliches Vertrauen genießen, stellt sicher, dass AMPC-Fragmente nicht rekombiniert oder zu anderen Zwecken als dem Einzigartigkeitstest verwendet werden. So werden keine personenbezogenen Daten gespeichert oder für Mitwirkende oder Teilnehmende am World-Protokoll oder Dritte zugänglich gemacht.

Verwendung der World ID

Wenn Ihre Orb-Verifizierung erfolgreich war, wird der Hash Ihres World ID Secret (einer Zufallszahl) in die [öffentliche Liste verifizierter World ID Hashes](#) aufgenommen, ohne dass jemals bekannt wird, wer Sie sind oder welche Daten am Orb erfasst wurden. Wenn Sie Ihre World ID verwenden, beweisen Sie von Ihrem Smartphone aus, dass Sie das World ID Secret zu einem der Hashes im Hash-Baum besitzen, ohne offenzulegen, welcher Hash es ist. Ein Zero-Knowledge-Proof (ZKP) stellt sicher, dass Sie nicht offenlegen, auf welchen Hash Sie sich stützen. Stattdessen erzeugt der ZKP einen Nullifizierer-Hash für die jeweilige Aktion – dieser lässt sich am besten als aktionsspezifische, einmalige World ID beschreiben. So können Sie die World ID anonym verwenden. Das bedeutet: Wenn Sie sich bei zwei verschiedenen Services mit Ihrer World ID anmelden und diese versuchen, Sie anhand des geteilten Nullifizierer-Hashes zu identifizieren, ist das nicht möglich. Dies verhindert jedoch nicht, dass diese Dienste Sie über andere, bislang übliche Methoden identifizieren, könnte aber langfristig dazu beitragen, das Problem des Online-Trackings zu verringern. [Erfahren Sie mehr über ZKPs](#).

Personenbezogene Daten, die wir erheben und verwenden

Wir erheben Ihre personenbezogenen Daten, wenn Sie uns diese zur Verfügung stellen oder unsere Services nutzen. In bestimmten Fällen erhalten wir personenbezogene Daten auch von Dritten. Wie [nachfolgend näher erläutert](#), können Sie jederzeit auf Ihre personenbezogenen Daten zugreifen, diese berichtigen oder löschen.

Personenbezogene Daten, die Sie uns bereitstellen

Unter bestimmten Umständen und abhängig von der Funktionalität der App können wir Daten von Ihnen anfordern, oder Sie stellen uns von sich aus Daten bereit. Sie können es sich jederzeit anders überlegen und die Daten in den Einstellungen unserer Apps ändern oder löschen.

- Sie können Ihre **Telefonnummer** hinzufügen. Dies hilft Ihren Kontakten, Sie zu finden und mit Ihnen zu interagieren. Sie können Ihre Telefonnummer auch verwenden, um Backups wiederherzustellen und an unserem Empfehlungsprogramm teilzunehmen ([siehe unsere Partnerempfehlungen](#)).
- Sie können Ihre **Kontakte** synchronisieren. So können Sie sehen, welche Ihrer Kontakte ihre Telefonnummer in ihrer App hinzugefügt haben, damit Sie leichter mit ihnen in Kontakt treten und interagieren können. Wir speichern Ihre Kontakte nicht.
- Sie können einen **Benutzernamen** erstellen, den Sie [jederzeit ändern können](#). Ihr Benutzername ist nur mit Ihrer App verknüpft und nicht mit Ihrer World ID.
- Sie können Ihre **Standortdaten** mit uns teilen, beispielsweise um einen Orb in Ihrer Nähe zu finden und uns dabei zu helfen, zu verstehen, wo wir Orbs künftig bereitstellen sollten.
- Sie werden aufgefordert, Ihr **Geburtsdatum** einzugeben. Ihr Geburtsdatum wird nicht aufbewahrt oder gespeichert und ausschließlich auf Ihrem Gerät verwendet, um festzustellen, ob Sie die Altersvoraussetzungen für die Nutzung der Services erfüllen.
- Wenn Sie uns kontaktieren, zum Beispiel für Hilfe oder Support, verarbeiten wir **Nachrichten und Mitteilungen** mit Ihnen, die Ihre personenbezogenen Daten enthalten können. Wenn Sie Feedback über Umfragen geben, verwenden wir dieses Feedback zur Verbesserung unserer Services.
- Wenn Sie Chatfunktionen nutzen, **können wir Ihre Chatnachrichten weder sehen noch darauf zugreifen**. Die Nachrichten und zugehörigen Metadaten sind Ende-zu-Ende-verschlüsselt, und wir können sie weder entschlüsseln noch anderweitig darauf zugreifen. Wir leiten die verschlüsselten Nachrichten lediglich über unseren Server vom Absender an den Empfänger weiter.
- Sie können uns gestatten, Informationen über **Ihre Interaktionen mit unseren Apps** zu analysieren, damit wir Fehler finden und unsere Produkte verbessern können.
- Sie können sich dazu entscheiden, Ihre Daten **zur Verbesserung der World ID für alle** bereitzustellen. Um sicherzustellen, dass World ID sicher, zuverlässig und inklusiv ist, benötigen die zugrunde liegenden Modelle Trainingsdaten aus einer vielfältigen Population. Sie können optional Ihre Orb-Fotos und Fotos für die Gesichtsauthentifizierung teilen, um beim Training dieser Modelle zu helfen.
- Sie können **Nachweise** wie einen Reisepass zu einigen unserer Apps hinzufügen. Wir überprüfen die Gültigkeit Ihres Nachweises, bestätigen, dass Ihr Gesicht mit dem Foto auf dem Nachweis übereinstimmt, und speichern die Daten des Nachweises anschließend sicher auf Ihrem Gerät. Wir haben keinen Zugang zu den personenbezogenen Daten auf Ihrem Nachweis.
- Sie können sich dafür entscheiden, Ihre World ID mit einem Selfie-Foto (**Selfie Check**) zu verifizieren. Das Foto wird lokal auf Ihrem Gerät gespeichert. Das Selfie wird verarbeitet, um Einzigartigkeit und die Eigenschaft als echter Mensch sicherzustellen; TFH bewahrt nur anonymisierte Daten auf.

- Auf bestimmten Drittanbieterplattformen (z. B. Videokonferenz- und Videochat-Apps) können Sie sich dafür entscheiden, unsere Deep Face-Funktionen zu nutzen, um Ihre Konten vor Identitätsmissbrauch, Deepfakes, Replay-Angriffen und anderen betrügerischen Aktivitäten zu schützen. Wenn diese aktiviert sind, können Gesichtsfotos, Selfies, kurze Videoaufnahmen oder zugehörige biometrische Verifizierungsdaten verarbeitet werden, um die Eigenschaft als echter Mensch und Lebendigkeit zu beurteilen sowie festzustellen, ob Inhalte authentisch erscheinen oder synthetisch erzeugt wurden. Alle biometrischen Daten werden lokal auf Ihrem Gerät verarbeitet, und TFH bewahrt nur anonymisierte Daten auf.

Informationen, die wir erfassen, wenn Sie unsere Services nutzen

- Wenn Sie unsere Apps verwenden, erfassen wir Informationen über Ihre Verbindung, wie etwa Ihre **IP-Adresse**, Ihren Browsertyp und zugehörige Daten, um unsere Services bereitzustellen und sie auf das Land abzustimmen, in dem Sie sich befinden. Wir erfassen weitere **Metadaten zum Gerät**, wie Ihre Bildschirmauflösung, das Betriebssystem, den Mobilfunkanbieter, die Sprache, den Speicher, installierte Apps, den Akkustand und die Geräteummer, um sicherzustellen, dass Ihre App auf Ihrem Gerät ordnungsgemäß funktioniert und unseren [Nutzungsbedingungen](#) entspricht. Wir verwenden diese Informationen auch, um Betrug zu erkennen und zu verhindern.
- Wir erfassen weitere Informationen über Ihre **Interaktionen mit unseren Apps**, um sicherzustellen, dass diese wie von Ihnen erwartet funktionieren (z. B. durch Speichern Ihrer Einstellungen und Ihrer Verifizierungsstufe, um Ihnen die passende Benutzeroberfläche anzuzeigen).
- Wenn Sie die World App zum ersten Mal auf Ihrem Smartphone öffnen, wird automatisch eine Krypto-Wallet einschließlich einer **Wallet-Adresse** für Sie generiert. Wir verarbeiten diese Wallet-Adresse, um Transaktionen mit Ihrer Wallet zu ermöglichen. Der zugehörige Private Key der Wallet wird ausschließlich auf Ihrem Gerät gespeichert, und wir haben niemals Zugriff darauf.
- Zur Erfüllung gesetzlicher Verpflichtungen und zur Bereitstellung einer Schnittstelle für Blockchain-Transaktionen erfassen wir aktuelle Kopien des Zustands von **öffentlichen Blockchains**, die Ihre früheren öffentlichen Transaktionen enthalten können.
- Unsere Websites verwenden **Cookies**. Cookies sind kleine Textdateien, die auf Ihrem Gerät gespeichert werden und von Onlinediensten genutzt werden, um Ihr Gerät und/oder Ihre Präferenzen zu erkennen. Wir verwenden funktionale Cookies, um eine funktionsfähige Website bereitzustellen, und optionale Cookies, um die Nutzung unserer Websites zu analysieren und zu verbessern. Eine vollständige Liste der verwendeten Cookies sowie Ihre Möglichkeiten, nicht erforderliche Cookies abzulehnen, finden Sie in unserer [Cookie-Richtlinie](#).

Informationen, die wir gegebenenfalls von Dritten erhalten

- Wenn Sie unser [Support-Portal](#) zur Altersverifizierung nutzen, fordern wir eine Bestätigung von einem Dritten an, der Ihr Alter unabhängig verifiziert hat und bestätigt, dass Sie mindestens das **Volljährigkeitsalter** in Ihrem Land erreicht haben. Wir erhalten keine weiteren Informationen von diesem Dritten.
- Um Betrug und unzulässige Aktivitäten im Rahmen unserer Services zu verhindern, erhalten wir Informationen von Drittanbietern über Geräte und Blockchain-Wallets, die mit potenziellem Betrug und/oder unzulässigen Aktivitäten in Verbindung stehen.

Weitergabe personenbezogener Daten

Innerhalb von TFH haben nur Teammitglieder Zugriff auf personenbezogene Daten, die diese zur Erfüllung ihrer Aufgaben benötigen, und wir haben strenge Zugriffskontrollen implementiert, um dies sicherzustellen. Wir lagern die Datenverarbeitung nur an vertrauenswürdige und sichere Anbieter und Dienstleister aus. Zu diesen Dienstleistern gehören zertifizierte Cloud-Dienstleister,

Anbieter von Software-as-a-Service-Lösungen und IT-Sicherheitsunternehmen. Die [vollständige Liste unserer Auftragsverarbeiter](#) finden Sie hier.

Wir können Ihre Daten weitergeben, um gesetzlichen Anforderungen nachzukommen oder auf rechtmäßige Anfragen von Strafverfolgungsbehörden zu reagieren. Wenn Ihre Handlungen gegen unsere [Nutzungsbedingungen](#) verstoßen oder die Rechte anderer oder unsere Rechte gefährden, können wir Ihre Informationen an die zuständigen Behörden weitergeben. Wir werden Ihre personenbezogenen Daten mit Ihrer Einwilligung oder auf Ihre Anweisung hin weitergeben.

TFH und das World ID-Protokoll sind darauf ausgelegt, die Weitergabe personenbezogener Daten an diese Parteien zu minimieren. Wenn Sie World ID mit Anwendungen, Websites oder Services von Drittanbietern („Vertrauende Parteien“) verwenden, erhalten Vertrauende Parteien keine Gesichts- oder Augenfotos von Ihnen, keinen Iris-Code, kein World ID Secret und keine anderen zugrunde liegenden biometrischen Daten. Stattdessen erhalten sie kryptografische Nachweise oder Verifizierungsergebnisse, die mithilfe von [Zero-Knowledge-Proof-Technologien](#) generiert werden und darauf ausgelegt sind, bestimmte Tatsachen— zu bestätigen, etwa dass Sie ein unverwechselbarer Mensch sind, über einen gültigen Nachweis verfügen oder eine bestimmte Aktion zuvor noch nicht ausgeführt haben—, ohne Ihre Identität oder zugrunde liegende biometrische Daten offenzulegen. Je nach Kontext und geltendem Recht können bestimmte Verifizierungssignale, Identifikatoren oder zugehörige Metadaten personenbezogene Daten darstellen. Vertrauende Parteien sind im Allgemeinen eigenständige verantwortliche Stellen in Bezug auf alle personenbezogenen Daten, die sie im Zusammenhang mit ihren eigenen Services verarbeiten; ihre Verarbeitung richtet sich nach ihren jeweiligen Datenschutzhinweisen.

Speicherdauer personenbezogener Daten

Grundsätzlich bewahren wir Ihre personenbezogenen Daten wie folgt auf:

- Die personenbezogenen Daten, die Sie uns bereitstellen, speichern wir so lange, wie Sie unsere Services nutzen oder bis Sie diese ändern oder löschen;
- Informationen, die wir im Rahmen Ihrer Nutzung unserer Services erfassen, speichern wir nicht länger als zwei Jahre; Ihre bisherigen Interaktionen mit der World App (die erforderlich sind, damit die App funktioniert), bewahren wir für die Dauer Ihrer Nutzung der Services oder bis zur Löschung Ihres Kontos auf;
- Daten zur Gesichtsauffertifizierung werden ausschließlich auf Ihrem Gerät gespeichert und verbleiben dort, bis Sie die World App löschen oder die Daten von Ihrem Gerät entfernen.
- Wallet-Daten werden dauerhaft auf der öffentlichen Blockchain veröffentlicht, von der wir regelmäßig eine aktualisierte Kopie abrufen; und
- Informationen, die wir gegebenenfalls von Dritten erhalten (in der Regel zur Betrugsprävention und um Sie und andere bei der Nutzung unserer Services zu schützen), bewahren wir ein Jahr lang auf, es sei denn, Sie haben gegen unsere Nutzungsbedingungen verstoßen; in diesem Fall bewahren wir sie fünf Jahre lang auf.
- Wir löschen automatisch Ihre personenbezogenen Daten in der App, einschließlich Ihrer Profildaten, optionaler Analysedaten, Einstellungen für Push-Benachrichtigungen sowie aller für Trainingszwecke gesendeten Fotos, wenn Ihr Konto für einen Zeitraum von 24 Monaten inaktiv bleibt. Bitte beachten Sie, dass Sie über diese Löschung nicht zusätzlich benachrichtigt werden.

Falls gesetzlich vorgeschrieben, werden wir Ihre personenbezogenen Daten aufbewahren, soweit dies zur Erfüllung unserer rechtlichen und regulatorischen Verpflichtungen erforderlich ist, einschließlich zur Betrugsüberwachung, -erkennung und -prävention sowie für Steuer-, Buchhaltungs- und Finanzberichterstattungspflichten.

Ausführliche Informationen zu den konkreten Rechtsgrundlagen und Zwecken unserer Datenverarbeitungstätigkeiten finden Sie in der nachstehenden Tabelle, die erläutert, welche Daten wir erfassen, wofür wir sie verwenden und wie lange sie aufbewahrt werden.

Ihre Rechte

Ihre Daten gehören Ihnen, und wir sind der Auffassung, dass Sie Ihre Rechte jederzeit problemlos ausüben können sollten. Wenn Sie unsere Services nutzen, können Sie jederzeit:

- weitere Informationen zur Datenverarbeitung über die [hier verfügbaren Hilfematerialien](#) oder durch Kontaktaufnahme mit unserem Datenschutzbeauftragten über die unten angegebenen Kontaktdaten erhalten;
- auf Ihre personenbezogenen Daten in den Einstellungen der Apps zugreifen oder diese berichtigen;
- personenbezogene Daten in den Einstellungen der Apps löschen und
- Ihre Einwilligung zu einer auf Einwilligung beruhenden Datenverarbeitung widerrufen oder der Verarbeitung auf Grundlage berechtigter Interessen widersprechen, einschließlich des Rechts, die Einschränkung der Verarbeitung zu verlangen, indem Sie in den Einstellungen der Apps den Bereich Datenschutz und Rechtliches aufrufen.

Sie können diese Rechte in unseren Apps ausüben, indem Sie unter „Einstellungen“ auf „Datenschutz und Rechtliches“ klicken; weitere Informationen zur Löschung finden Sie in [diesem Hilfecenter-Artikel](#).

Allgemeines

Wir befolgen den EU-US-Datenschutzrahmen (EU-US DPF), die britische Erweiterung des EU-US DPF und den Schweizer-US-Datenschutzrahmen (Schweizer-US DPF) in der vom US-Handelsministerium festgelegten Version. Wir haben gegenüber dem US-Handelsministerium zertifiziert, dass das Unternehmen die Grundsätze des EU-US-Datenschutzrahmens (EU-US DPF-Grundsätze) in Bezug auf die Verarbeitung personenbezogener Daten einhält, die es aus der Europäischen Union im Verlass auf den EU-US DPF und aus dem Vereinigten Königreich im Verlass auf die britische Erweiterung des EU-US DPF erhalten hat. Wir haben gegenüber dem US-Handelsministerium zertifiziert, dass das Unternehmen die Grundsätze des Schweizer-US-Datenschutzrahmens (Schweizer-US DPF-Grundsätze) in Bezug auf die Verarbeitung personenbezogener Daten einhält, die es aus der Schweiz im Verlass auf den Schweizer-US DPF erhalten hat. Sollte ein Konflikt zwischen den Bestimmungen in dieser Datenschutzrichtlinie und den EU-US DPF-Grundsätzen und/oder den Schweizer-US DPF-Grundsätzen existieren, haben die Grundsätze Vorrang. Wenn Sie mehr über das Programm zum Datenschutzrahmen (Data Privacy Framework, DPF) und unsere Zertifizierung erfahren möchten, besuchen Sie bitte die [Website zum Datenschutzrahmen](#).

Sie müssen mindestens das Volljährigkeitsalter in Ihrem Land erreicht haben (und mindestens 18 Jahre alt sein), um unsere Services nutzen zu dürfen. Wir nehmen den Schutz Minderjähriger sehr ernst—wenn Sie glauben, dass jemand unter 18 Jahren unsere Services nutzt, kontaktieren Sie uns bitte umgehend über unser [Datenschutzportal](#) oder über die oben genannten Kanäle.

Wir können diese Datenschutzrichtlinie jederzeit aktualisieren, aber wenn sich die Änderungen auf Ihre Rechte auswirken, werden wir Sie im Voraus benachrichtigen. Wenn Sie unsere Services danach weiterhin nutzen, akzeptieren Sie die aktualisierte Datenschutzrichtlinie.

So können Sie uns kontaktieren

Wenn Sie Fragen zu dieser Datenschutzrichtlinie oder zu anderen datenschutzbezogenen Themen haben, können Sie sich jederzeit an uns wenden. Sie können sich jederzeit an unser Datenschutzbüro und unseren Datenschutzbeauftragten Marc Placzek unter dpo@toolsforhumanity.com oder per Brief an folgende Anschrift wenden: DPO, Tools For Humanity Corporation, 650 7th St, San Francisco, CA 94103, USA.

Wenn Sie in den Vereinigten Staaten oder in einem anderen Land außerhalb der Europäischen Union, der EFTA-Staaten oder des Vereinigten Königreichs leben, ist die für Ihre personenbezogenen Daten verantwortliche Stelle die Tools for Humanity Corporation mit der Anschrift 650 7th St, San Francisco, CA 94103, USA.

Wenn Sie in der Europäischen Union, den EFTA-Staaten oder dem Vereinigten Königreich leben, ist die für Ihre personenbezogenen Daten verantwortliche Stelle die Tools for Humanity GmbH mit der Anschrift August-Everding-Straße 25, 81671 München, Deutschland.

Wenn Sie Bedenken hinsichtlich unserer Datenverarbeitung haben, haben Sie das Recht, sich an Ihre örtliche Aufsichtsbehörde oder an die federführende Aufsichtsbehörde der TFH GmbH, das Bayerische Landesamt für Datenschutzaufsicht („BayLDA“), zu wenden. Die Kontaktdaten finden Sie auf der Website der Behörde.

ANHANG – Rechtsgrundlagen/Zwecke der Datenverarbeitungstätigkeiten von Tools for Humanity

TFHPS20260701