

- **Ref.: EXP202602591**
- **Asunto: Advertencia**

Primero. - En fecha 23 de enero de 2026 se recibió en esta Agencia Española de Protección de Datos (AEPD) un correo electrónico, en idioma inglés, firmado por **A.A.A.**, Data Protection Officer de Tools for Humanity con el siguiente contenido:

“Subject: Update on Tools for Humanity’s (“TFH”) operations and data processing activities in Spain

Your Excellency Mr. President,

Dear Members of the AEPD,

In line with our commitment to transparency regarding our technology and operations, and as part of our ongoing efforts to demonstrate compliance with applicable data protection legislation, we are writing to inform you of recent updates concerning the organizational structure, business operations, and products of Tools for Humanity (“TFH”).

Our operations in Spain

1. Across our operations, we continue to strengthen our data protection and privacy framework. Over the past year, we have introduced a number of technical and design improvements, including:

a. the open-source release of the Orb hardware to promote transparency and enable public audit;

b. the implementation of a personal custody model that grants users direct control over their biometric data and their World ID; and

c. the introduction of Anonymized Multi-Party Computation (AMPC), which enables verification without transferring or storing special categories of personal data.

2. Following the implementation of these enhancements, and as communicated in November 2025, we plan to relaunch our operations in Spain in February 2026 with the opening of a new location in Barcelona. We approach this new phase of our activities in Spain with great interest and reiterate our commitment to constructive cooperation with the AEPD.

Updates to the World App rewards model

3. In parallel with the relaunch of operations, we will pilot a new rewards model in Spain. Under this model, users may access benefits linked to local or online services and digital subscriptions, instead of receiving token-based rewards. This change is intended to align the user experience with the current

and future use cases of the World Network, while preserving transparency and user choice at all times.

Controller of personal data

4. *As of October 2025, Tools for Humanity GmbH acts as the sole data controller for all Orb-related processing activities involving the personal data of users located in Spain. Tools for Humanity GmbH has been designated as the single EU establishment of Tools for Humanity Corporation pursuant to Article 56 of the GDPR. This change reflects the consolidation of data protection responsibility within a single EU-based entity, ensuring clear accountability, streamlined supervisory oversight, and the consistent application of GDPR and UK GDPR requirements.*

5. *The Worldcoin Foundation remains the steward of the World ID protocol but is no longer involved in data processing activities. This change results from the introduction of Anonymized Multi-Party Computation (AMPC), which anonymizes data once it leaves the Orb.*

6. *These updates are reflected in the Privacy Policy published on our website: <https://www.toolsforhumanity.com/es-es/legal/privacy-notice>. The policy has been integrated into the consent process during World ID verification.*

Launch of the Credentials feature

7. *(...).*

8. *(...).*

9. *(...).*

We remain at your disposal and would be grateful if you could let us know whether you would be available on 3 or 4 March for an in-person meeting. It would be a pleasure to address any questions or comments you may have regarding the matters outlined above.

Yours sincerely,

A.A.A.

Data Protection Officer

Tools For Humanity”

La traducción al castellano de dicho correo electrónico es la siguiente (traducción no oficial):

Asunto: Actualización sobre las operaciones y actividades de tratamiento de datos de Tools for Humanity (“TFH”) en España

Excelentísimo Señor Presidente,

Estimados miembros de la AEPD:

En consonancia con nuestro compromiso con la transparencia en relación con nuestra tecnología y operaciones, y como parte de nuestros continuos esfuerzos por demostrar el cumplimiento de la legislación aplicable en materia de protección de datos, nos dirigimos a usted para informarle sobre las últimas novedades relativas a la estructura organizativa, las operaciones comerciales y los productos de Tools for Humanity (“TfH”).

Nuestras operaciones en España

1. En todas nuestras operaciones, seguimos reforzando nuestro marco de protección de datos y privacidad. Durante el último año, hemos introducido diversas mejoras técnicas y de diseño, entre ellas:

- a. la liberación de código abierto del hardware Orb para promover la transparencia y facilitar la auditoría pública;
- b. la implementación de un modelo de custodia personal que otorga a los usuarios control directo sobre sus datos biométricos y su World ID; y
- c. la introducción de la Computación Multipartita Anonimizada (AMPC), que permite la verificación sin transferir ni almacenar categorías especiales de datos personales.

2. Tras la implementación de estas mejoras, y tal como se comunicó en noviembre de 2025, tenemos previsto relanzar nuestras operaciones en España en febrero de 2026 con la apertura de una nueva sede en Barcelona. Abordamos esta nueva fase de nuestras actividades en España con gran interés y reiteramos nuestro compromiso de colaboración constructiva con la AEPD.

Actualizaciones del modelo de recompensas de la App World

3. Paralelamente al relanzamiento de operaciones, implementaremos un nuevo modelo de recompensas en España. Con este modelo, los usuarios podrán acceder a beneficios vinculados a servicios locales o en línea y suscripciones digitales, en lugar de recibir recompensas basadas en tokens. Este cambio busca alinear la experiencia del usuario con los casos de uso actuales y futuros de la Red World, preservando la transparencia y la capacidad de elección del usuario en todo momento.

Responsable del tratamiento de datos personales

4. A partir de octubre de 2025, Tools for Humanity GmbH actuará como único responsable del tratamiento de datos para todas las actividades de tratamiento relacionadas con Orb que involucren datos personales de usuarios ubicados en España. Tools for Humanity GmbH ha sido designada como la única entidad de la UE de Tools for Humanity Corporation, de conformidad con el artículo 56 del RGPD. Este cambio refleja la consolidación de la responsabilidad de la protección de datos en una única entidad con sede en la UE, lo que garantiza una rendición de cuentas clara, una supervisión optimizada y la aplicación coherente de los requisitos del RGPD y del RGPD del Reino Unido.

5. La Fundación Worldcoin sigue siendo la administradora del protocolo World ID, pero ya no participa en el procesamiento de datos. Este cambio se debe a la

introducción de la Computación Multipartita Anónima (AMPC), que anonimiza los datos una vez que salen del Orbe.

6. Estas actualizaciones se reflejan en la Política de Privacidad publicada en nuestro sitio web: <https://www.toolsforhumanity.com/es-es/legal/privacy-notice>. Esta política se ha integrado en el proceso de consentimiento durante la verificación de World ID.

Lanzamiento de la función Credenciales

7. (...).

8. (...).

9. (...).

Quedamos a su disposición y le agradeceríamos que nos informara si estaría disponible el 3 o 4 de marzo para una reunión presencial. Será un placer atender cualquier pregunta o comentario que pueda tener sobre los asuntos descritos anteriormente.

Atentamente,

A.A.A.

Delegado de Protección de Datos

Tools For Humanity

Con anterioridad, Tools for Humanity (en adelante “TfH”) había proporcionado a esta AEPD diversos documentos, en el marco de reuniones técnicas mantenidas con el equipo de TfH, relativos a las Evaluaciones de Impacto para la Protección de Datos (EIPDs) con relación a los tratamientos de datos personales que pretende iniciar en España.

Segundo. - Del texto del correo transcrito, y de información pública aparecida en prensa, resulta que TfH tiene previsto retomar las operaciones en España en fecha muy próxima, llevando a cabo tratamientos de datos personales.

Tercero.- El artículo 55.1 del Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos, RGPD) dispone que *“cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro”*.

El art. 58.2 del RGPD) establece que cada autoridad de control dispondrá de todos poderes correctivos indicados a continuación, y entre ellos el recogido en su letra a) de dirigir a todo responsable o encargado del tratamiento una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento.

De acuerdo con el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo,

LOPDGDD) corresponde a la AEPD, entre otras facultades, ejercer las potestades previstas en el artículo 58 del RGPD.

Cuarto. - Por otra parte, tal y como resulta de jurisprudencia constante del Tribunal de Justicia de la Unión Europea, el objetivo del RGPD (véase, por ejemplo, apartado 53 de la Sentencia del Tribunal de Justicia (Sala Cuarta), de 7 de marzo de 2024, C-604/22, consiste en *“garantizar un nivel elevado de protección de los derechos y libertades fundamentales de las personas físicas, sobre todo de su derecho a la vida privada respecto del tratamiento de los datos personales, consagrado en el artículo 8, apartado 1, de la Carta y en el artículo 16 TFUE, apartado 1 [sentencia de 4 de mayo de 2023, Bundesrepublik Deutschland (Buzón electrónico judicial), C-60/22, EU:C:2023:373, apartado 64].”*

Por ello, las facultades y poderes correctivos de las autoridades de control habrán de interpretarse de una manera amplia. Véase por analogía, apartado 37 de la sentencia del Tribunal de Justicia, de 26 de septiembre de 2024, C-768/21.

Quinto. - Por otro lado, no hay que olvidar que dentro de las facultades que configura el RGPD para las autoridades de control existe también una labor “cautelar” o “preventiva”. Así, por ejemplo, el apartado 188 de las Conclusiones del Abogado General Sr. Dean Spielmann, de 23 de septiembre de 2025, en el Asunto C-474/24 dice:

188. (...) el artículo 58, apartado 2, del mencionado Reglamento enumera los diferentes poderes correctivos de que dispone la autoridad de control, que cuenta, a este respecto, con un margen de apreciación en lo que atañe a la elección de los medios adecuados y necesarios. (112) Entre los poderes de la autoridad de control establecidos en el artículo 58, apartado 2, letra a), del RGPD, esta puede dirigir una «advertencia» a todo responsable del tratamiento cuando las operaciones de tratamiento «previstas» «puedan» infringir lo dispuesto en el RGPD, lo que se inscribe en un enfoque que cabe calificar de «cautelar» respecto de los derechos del interesado. (113)

Sexto.- Por lo demás, esa facultad cautelar o preventiva que el RGPD otorga a las autoridades de control está expresada en términos amplios en el art. 58.2.a) RGPD, de manera que esta norma ha otorgado a las autoridades de control la facultad de dirigir a todo responsable o encargado del tratamiento una advertencia, no necesariamente cuando esta haya comprobado que el tratamiento es contrario al RGPD, sino cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento.

La utilización de esta expresión “puedan” se inserta dentro de dicha función cautelar o preventiva, que hay que entenderla, cuando la autoridad de control decide dirigir una advertencia, no como una realidad de que dichas operaciones efectivamente infringen el RGPD, sino de que existe la posibilidad (como contrario a certeza) de que dichas operaciones pueden infringir el Reglamento.

Por ello, en el ejercicio de esta función cautelar, la autoridad de control podrá, sobre la base de la información recibida, e incluso de la que no haya recibido, emitir una advertencia al responsable o encargado del tratamiento, acerca de la posibilidad de que dichos tratamientos de datos infrinjan el Reglamento, para que el responsable o encargado extraiga de dicha advertencia las enseñanzas o criterios apropiados y,

conforme a su obligación de responsabilidad proactiva, pueda adaptar dichos tratamientos de datos al Reglamento.

No cabe, por último, tampoco, excluir que la información de que disponga la autoridad de control sea incompleta, por cualquier razón. Ello no hará menos efectiva su advertencia – y por tanto el objetivo del Reglamento de proteger a los interesados-, por cuanto el objetivo de la advertencia no es sancionar una conducta del responsable o encargado, sino advertir (esto es, llamar la atención del responsable o encargado) de que unos determinados tratamientos podrían infringir el Reglamento, sin necesidad de que exista una certeza de que dichos tratamientos incumplen el RGPD).

Séptimo. - Se ha analizado la documentación proporcionada por TfH que se ha expuesto en el apartado Primero de esta Resolución y la información pública, sobre este tratamiento de datos, disponible, en fecha de 6 de febrero de 2026, en su página web (toolsforhumanity.com) y en otras webs a las que enlaza desde la primera. Esta última información está disponible en los siguientes enlaces:

Política de Privacidad de TfH, <https://www.toolsforhumanity.com/es-es/legal/privacy-notice>

Política de conservación de datos biométricos, <https://www.toolsforhumanity.com/es-es/legal/biometric-policy>

ANEXO I Bases jurídicas/fines para las actividades de tratamiento de datos de TfH, <https://www.toolsforhumanity.com/es-es/legal/annex>

el Orb, <https://www.toolsforhumanity.com/es-es/orb>

World implements Personal Custody e Introducing AMPC: Another leap in privacy and performance for World ID, <https://world.org/es-es/blog/engineering/introducing-ampc-another-leap-privacy-performance-world-id>.

Como consecuencia del anterior análisis esta Agencia expone a TfH las siguientes consideraciones:

En las EIPDs que se encontraban en la documentación proporcionada, TfH manifiesta que, (...). Por otra parte, en las EIPDs, TfH manifiesta que la finalidad del tratamiento no es la identificación de una persona y, por tanto, concluyen que no se corresponde con el tratamiento de categorías especiales de datos personales del artículo 9.1 del RGPD.

No obstante, de acuerdo con la información disponible por la AEPD, TfH habría manifestado que:

“(...)”.

El RGPD define “datos biométricos” en el art. 4.14 como aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona.

Con relación a dicha definición, el tratamiento realizado por TfH en el Orb parecería implicar que:

- Los datos personales obtenidos: código de iris.
- El tratamiento técnico específico: el llevado a cabo en el Orb.
- Las características físicas de una persona física: imágenes del iris.
- El que permitan o confirmen la identificación única de dicha persona: este código se utiliza para verificar que la persona es única y que no ha registrado previamente.

Según TfH *“el Orb puede distinguirse del resto sin almacenar ningún dato personal, ni siquiera tu nombre.*

(...).

(...)”.

Esto parecería implicar que el código único es un patrón biométrico obtenido a partir de imágenes del iris y el rostro, tratado por el responsable, transformándolo mediante determinados algoritmos y almacenándolo con diversas técnicas criptográficas y de privacidad para garantizar unicidad. Por tanto, el responsable podría estar llevando a cabo un tratamiento de datos personales biométricos.

Por otro lado, sobre la custodia de los datos biométricos TfH aduce que:

“(...)”.

A su vez, sobre el tratamiento y almacenamiento de los datos en el dispositivo del usuario, TfH argumenta lo siguiente:

“(...)”.

(...)”.

Así es como funciona el proceso:

1. (...).
2. (...).
3. (...).
4. (...).
5. (...).

Dado que todos los datos están cifrados con su clave pública, el resultado final de este proceso es una colección de paquetes de datos cifrados que residen exclusivamente en su dispositivo. Su información siempre se elimina del Orb una vez que se ha enviado a su dispositivo, y el uso del doble cifrado dentro del sobre de cifrado de extremo a extremo es una medida de seguridad para proteger la confidencialidad y la privacidad de sus datos en caso de que su dispositivo se vea comprometido”.

Asimismo, en respuesta a la pregunta ¿Qué datos personales debo compartir para obtener un WorldID verificado?, TfH indica:

“Para validar tu prueba de singularidad, el Orb solo necesita un tipo de dato: imágenes de tus ojos y rostro. No te pedirá tu nombre, correo electrónico, género ni ningún otro dato personal.

(...).

Esto es lo que sucede, paso a paso, después de registrarte en World App:

1. (...).
2. (...).
3. (...).
4. (...).

Gran parte del proceso y el código relacionado con la verificación de humanidad y singularidad, incluido el AMPC y lo que ocurre en el Orb, es de código abierto para que cualquiera lo pueda ver y auditar”.

Cuando TfH hace mención a “*tu dispositivo*” parece referirse en la práctica a la “*aplicación de TfH instalada en el dispositivo de un usuario*”, aplicación que formaría parte del tratamiento de datos personales y sobre la que el responsable mantendría cierto grado de control. El usuario parece que no tendría control total sobre los datos en la medida en que su acceso a los datos estaría condicionado el al uso de la aplicación proporcionada por TfH.

(...).

La información aquí analizada parece implicar que el tratamiento de datos personales que pretende iniciar TfH podría suponer un tratamiento de datos biométricos de personas físicas (...).

De acuerdo con lo establecido en el artículo 35.1 del RGPD: “*Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales...*”

Por tanto, la EIPD es el instrumento exigido por el RGPD al responsable del tratamiento cuando el tratamiento sea considerado de “alto riesgo”, como ocurre con el uso de datos biométricos y con los tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas (criterios correspondientes a los números 4, 5 y 10 del listado de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos publicado por la AEPD).

El responsable del tratamiento, a través de la EIPD, debe justificar la necesidad y la proporcionalidad del tratamiento que se pretende poner en marcha. Proporcionalidad que también exige que, cuando existen varias medidas igualmente eficaces a partir del conocimiento del responsable del tratamiento, se opte por la menos gravosa, lo que incluye la valoración de una posible alternativa no biométrica. En este punto se tiene muy en cuenta la técnica elegida, las garantías y medidas de diseño orientadas a evitar riesgos para los derechos y libertades de las personas físicas. El responsable tendrá también que gestionar desde el diseño los riesgos específicos del tratamiento, con la

aplicación práctica de medidas efectivas que garanticen un umbral de riesgo aceptable durante todo el ciclo de vida del tratamiento, tal como se establece en el artículo 35 del RGPD, cuestiones que no quedan resueltas en los documentos aportados por TfH relativos a la EIPD. Procede recordar que no todos los tratamientos biométricos tienen la misma intensidad de impacto, ni requieren idénticas medidas de protección. La autenticación biométrica localizada, bien diseñada y según toda una serie de circunstancias a tener en cuenta en cada caso concreto, puede ser en muchos contextos más proporcionada y menos intrusiva que la identificación biométrica, que tiende a requerir justificaciones mucho más sólidas, siquiera sea porque un número mayor de interesados se ven afectados, lo que exige que estas diferencias en el impacto sobre los derechos de los interesados tengan reflejo en la EIPD.

(...). Por ello, como se ha indicado, será necesaria una valoración diferenciada en el estudio de impacto en la protección de datos, que incluya garantías y medidas de diseño específicas para cada una de las funcionalidades biométricas indicadas, orientadas a evitar o minimizar los riesgos para los derechos y libertades de las personas físicas que cada una de ellas conlleve. Para lo cual se tendrían, también, que aplicar cautelas que tengan en cuenta los superiores riesgos que implica un mayor o menor grado de almacenamiento centralizado de la información biométrica, frente a su exclusivo control por el interesado, como puede ocurrir, (...).

Se ha de añadir a lo anterior que el tratamiento de datos biométricos requiere también la concurrencia de una de las bases jurídicas establecidas en el artículo 6 del RGPD y alguna de las excepciones previstas en el artículo 9.2 del RGPD y, que en el caso de que la excepción se basare en el artículo 9.2.a) del RGPD, en el proceso del consentimiento durante la verificación de World ID, tal y como se señala en las actualizaciones se reflejan en la Política de Privacidad publicada su sitio web: <https://www.toolsforhumanity.com/es-es/legal/privacy-notice>, deberá asegurarse que este consentimiento y la verificación de edad cumplen con los requisitos previstos en el RGPD

Por otra parte, en relación con el principio de transparencia, esta Agencia no ha encontrado, ni en la Política de Privacidad de TfH, ni en el ANEXO I Bases jurídicas/fines para las actividades de tratamiento de datos de TfH, ni en la Política de Conservación de Datos Biométricos, en cuanto al tratamiento de datos biométricos, información sobre las bases legitimadoras, la circunstancia de levantamiento de la prohibición o el ejercicio de derechos.

Tampoco, se ha proporcionado la información complementaria al interesado que requiere un tratamiento leal y transparente, de acuerdo con el considerando 60 del RGPD, al no ser informado de los tratamientos que se podrían estar realizando con la información derivada del iris del usuario y almacenada en su propio dispositivo. Con relación a esto último, la documentación da a entender que se utiliza la aplicación de TfH que está en el dispositivo del usuario para la autenticación biométrica facial y, con una prueba generada, usaría una Blockchain para comprobar la inscripción en World y demostrar humanidad.

A la vista de lo anterior, RESUELVO, DIRIGIR a TOOLS FOR HUMANITY GmbH una ADVERTENCIA prevista en el artículo 58.2., letra a), del Reglamento General de Protección de Datos, por considerar que las operaciones de tratamiento previstas, a las que se hace referencia en el apartado 1 Primero de esta Resolución, puedan infringir lo

dispuesto en el citado Reglamento, a fin de trasladar al responsable el riesgo detectado y permitirle valorar la conveniencia de revisar y, en su caso, adecuar dichos tratamientos

290-030320

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos