

- **Expediente N.º: EXP202317887**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: La Agencia Española de Protección de Datos ha tenido conocimiento de ciertos hechos que podrían constituir una posible infracción imputable a YOTI LTD con NIF 08998951 (en adelante, YOTI) en relación con el cumplimiento de la normativa de protección de datos en el tratamiento de los datos que ésta realiza.

SEGUNDO: Como consecuencia de los hechos conocidos, con fecha 12 de diciembre de 2023, la directora de la Agencia Española de Protección de Datos instó a la Subdirección General de Inspección de Datos (SGID) a iniciar las actuaciones previas de investigación a las que se refiere el artículo 67 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD). A este respecto, se tuvo en consideración que

Yoti es una solución de gestión de la identidad digital que permite trabajar tanto en entornos físicos como virtuales a usuarios con un mínimo de 13 años, contando ya con millones de usuarios y un uso muy extendido. La información que recoge Yoti como intermediario en procesos de verificación de identidad y de edad puede permitirle asociar a personas reales concretas con accesos a sitios físicos o en Internet y con operaciones o actividades específicas. Se desconocen muchos detalles sobre la arquitectura de seguridad y privacidad de la solución de Yoti y sobre muchas de sus decisiones de diseño, así como también sobre cómo se gestionan los metadatos (direcciones IP, geolocalizaciones), entornos de desarrollo y pruebas, copias de seguridad, sobre tiempos de retención, qué datos se cifran y cómo, entre otros. En particular, no se ha encontrado ninguna información respecto de la diferenciación de tratamiento de los datos de un niño de 13 años (edad mínima para poder utilizar el servicio o para instalarse la app) y los de un adulto.

Por otro lado, los usuarios de la app de Yoti consienten por defecto a que sus datos biométricos se empleen en tratamientos de 'investigación y desarrollo', incluidos los datos de menores de 14 años, ya que para tratar datos biométricos de menores solo hay que marcar una declaración de ser mayor de edad.

Teniendo en cuenta la relevancia de la información, resulta necesario por esta Agencia conocer en profundidad dicha plataforma y los tratamientos llevados a cabo, especialmente, la forma en la que se recaban los datos de los usuarios para los diferentes tratamientos que ofrece la aplicación y sobre el consentimiento para el uso de éstos, así como los detalles de seguridad y privacidad de la aplicación, para, en su caso, determinar las consecuencias que de ellos pueden derivarse para los derechos y libertades de las personas.

TERCERO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VIII, de la LOPDGDD.

Como consecuencia de las actuaciones realizadas, se ha tenido conocimiento de los siguientes extremos:

De acuerdo con lo que indica YOTI

“Nuestros servicios de verificación de edad comprenden una serie de servicios, enumerados a continuación (si bien no todos son comercializados en España):

- Estimación facial de la edad.*
- Con documento de identidad.*
- Con tarjeta de crédito.*
- Con número de móvil.*
- Mediante comprobación contra bases de datos.*
- Servicio eID (DNI electrónico).*
- Mediante permiso de conducir móvil estadounidense.*

Cuando estos servicios se ofrecen en régimen de software como servicio (“SaaS”) a los clientes de YOTI, dichos clientes son los responsables del tratamiento de datos y determinan los medios y fines del tratamiento. YOTI trata los datos de los clientes basándose en las decisiones y requisitos de nuestros clientes.

YOTI también proporciona una App para teléfonos móviles (‘App Digital ID’ o la ‘aplicación’) que puede ser elegida por nuestros clientes como método de verificación de la edad. Sin embargo, la verificación real se realiza dentro de la aplicación y YOTI es el responsable de los datos.

Cuando un cliente desea ofrecer a los usuarios la opción de verificar su edad a través de la App Digital ID, la persona escanea código QR utilizando su App y puede optar por compartir su atributo de edad verificada con el cliente de YOTI. El cliente es, a estos efectos, el responsable de tratamiento para el atributo de edad verificada que recibe”.

Acreditan el Registro de Actividades de Tratamiento (RAT), este documento está en lengua inglesa e incluye las siguientes actividades de tratamiento relacionadas con los procesos de verificación de edad que realiza YOTI. (traducción no oficial):

- o *Digital ID App.* Se incluye la siguiente tipología de datos personales tratada para la verificación de edad:
 - **Atributo de edad:** *fecha de nacimiento obtenida de documento identificativo verificado, la finalidad de este tratamiento es calcular la edad del usuario y enviar el recibo al cliente que lo*

solicita (share receipt), este recibo puede incluir bien la edad de la persona bien el valor "Más de X o Menos de X" (el cliente no recibe la fecha de nacimiento ni copia del documento de identificación). El atributo de edad es almacenado en los centros de datos de UK de YOTI y se elimina tan pronto como se completa la verificación de edad. YOTI actúa como encargado de tratamiento de este dato, siendo el cliente de YOTI que lo recibe el responsable.

- **Imagen facial/Selfie:** *para comprobar coincidencia de rostros y detección de vida, esto lo puede activar el cliente como servicio opcional. Se toman entre una y 6 fotografías para verificar que la persona delante de la cámara es real y para cotejarla con la imagen contenida en el documento de identificación (si el cliente lo ha habilitado en el servicio contratado), YOTI actúa como encargado de tratamiento de este dato, que se elimina de los centros de datos tan pronto como se completa la verificación de edad. Se afirma que, si el Cliente habilita las verificaciones manuales, el centro de seguridad YOTI en India accede y verifica de forma remota a los datos en el servidor del Reino Unido.*
- **Fecha y marca de tiempo:** *instante temporal en que se comparte el atributo de edad.*

Se comprueba que la App recaba un mayor número de datos personales (tal y como se demuestra en las evidencias capturadas y comentadas más adelante en este informe). No obstante YOTI afirma que estos datos son los utilizados de forma exclusiva para los servicios prestados de verificación de edad.

- o *Verificación de Edad mediante Documento Identificativo. Incluye el tratamiento de los siguientes tipos de datos:*
 - **Fotografía del documento identificativo:** *se verifica que es un documento auténtico, se extrae la fecha de nacimiento y, si el cliente lo ha optado, se realiza comparación facial con una selfie tomada del usuario. YOTI actúa como encargado de tratamiento de este dato, que se almacena en los centros de datos de UK de YOTI. Se afirma que la imagen del documento se elimina tan pronto como se completa la verificación de edad, excepto cuando el cliente ha habilitado la opción de realizar una verificación manual del documento, en estos casos se conserva 28 días y luego se elimina. Se afirma que los datos también se comparan contra bases de datos para la prevención de fraude, tanto internas como de terceros (no obstante, afirman que están alojadas internamente y el tercero no ve los datos). Si el cliente habilita la comprobación manual de los datos como opción a la extracción automática OCR, se realiza mediante el acceso remoto a los centros de datos (en Reino Unido) por parte de personal del centro de YOTI ubicado en India.*

- **Imagen facial/Selfie:** para verificar que coincide con el incorporado en el documento identificativo y para la detección de que el usuario es una persona real, este servicio se contrata de forma opcional por el cliente. Se tratan datos biométricos, actuando YOTI como encargado de tratamiento. La imagen Selfie se elimina tan pronto como se completa la verificación de edad, excepto cuando se realizan revisiones manuales del documento (servicio opcional contratado por el cliente), en estos casos la selfie se guarda durante 28 días y luego se elimina.
- o *Estimación de la Edad*, incorpora el siguiente tratamiento de datos:
 - **Imagen facial/Selfie:** Para estimar la edad y proporcionar el resultado al cliente. Se afirma que la imagen se elimina según resultado.
 - **Selfie adicional:** para la detección real de vida, si el cliente lo ha habilitado.
- o *Verificación de Edad mediante Número de Teléfono Móvil:* se recaba el **número de teléfono móvil** y, *de forma opcional*, el **nombre**, la **fecha de nacimiento** y la **dirección del usuario**. YOTI se posiciona como encargado de tratamiento de estos datos, siendo su cliente el responsable de tratamiento. Se afirma que los datos se recaban con la finalidad de remitirlos a terceros proveedores de servicios móviles que confirman si estos datos coinciden con los de la cuenta titular, esta información es utilizada por YOTI para hacer una suposición de la edad del usuario y devolver el resultado al cliente. El número de teléfono es procesado por los servidores de YOTI en Reino Unido y luego se elimina (se afirma que algunos proveedores de telefonía móvil mantienen de forma independiente este número de teléfono cifrado como registro de facturación, siendo responsables de tratamiento independientes para esto). En esta actividad también se trata como dato personal la clave OTP enviada para verificar que el número de móvil está en posesión del usuario en el momento de la verificación.
- o *Verificación de Edad mediante Tarjeta de Crédito:* en esta actividad se tratan los datos de la tarjeta, fecha de expiración, CVV y PostCode. YOTI es encargado de tratamiento, se afirma que los datos se remiten directamente del usuario a un proveedor externo de pagos para inferir que el usuario tiene más de la edad requerida.
- o *Verificación de Edad mediante Reutilización de una Verificación Previa:* incluye el tratamiento de un token de edad, un nombre de usuario y una contraseña. El token de edad es un tipo de cookie almacenada en navegador de usuario y contiene información de resultados de verificación de edad previos y momento temporal en que se realizó. YOTI actúa como responsable de tratamiento de estos datos, se afirma como base que legitima este tratamiento la formalización de contrato. Los datos se almacenan en los servidores de YOTI en Reino Unido.
- o *Actividad Verificación de Edad mediante chequeo contra Bases de Datos:* entre los datos vinculados a esta actividad está la dirección postal, el nombre y la fecha de nacimiento. YOTI actúa como encargado de tratamiento. Los datos se comparten directamente desde los usuarios a los proveedores externos. YOTI no retiene datos, solo el registro de haber realizado la verificación.

- o Otros datos que se recaban de forma general en las actividades de verificación de edad de YOTI:
 - Datos de geolocalización: Código de país, ciudad y estado de un usuario según la dirección IP. YOTI es responsable de tratamiento.
 - Resultados de verificaciones: la edad en años o valor de mayor o menor de una determinada edad, ID de sesión, método utilizado, consentimiento (dependiendo de las configuraciones específicas del cliente en cada caso). YOTI actúa como encargado de tratamiento.
 - Logs de verificaciones realizadas (no incluye datos personales: se trata de registros de que una verificación ha sido realizada en nombre de un determinado cliente).
 - Datos analíticos (no incluye datos personales): datos anonimizados relacionados con la ubicación del usuario que realiza la verificación, información de dispositivo utilizado y métricas de tiempo.
- Se acredita documento con la Evaluación de Impacto para la Protección de Datos (EIPD) de las soluciones de verificación de edad, el documento está en lengua inglesa e incorpora un historial de revisiones y actualizaciones, la fecha inicial de creación es de julio de 2018. De su análisis se extrae la siguiente información (traducción no oficial, se subraya texto más relevante):
 - o Incluye las siguientes afirmaciones:

“Los Servicios de Verificación de Edad de YOTI (AVS) ofrecen a los usuarios ocho formas posibles de acreditar la edad:

- I. *Usando la Estimación de Edad*
 - II. *Usando App Digital ID.*
 - III. *Usando un Documento Identificativo.*
 - IV. *Usando una Tarjeta de Crédito.*
 - V. *Usando un Número de Móvil.*
 - VI. *Usando Chequeo contra Base de Datos.*
 - VII. *Usando servicio de identificación electrónica eID.*
 - VIII. *Usando una licencia de conducir móvil de EE.UU.*
- I. *Usando la Estimación de Edad: se captura una imagen facial del usuario que es analizada por nuestra tecnología de estimación de edad. El cliente puede recibir la edad estimada en años o un valor 'por encima' o 'por debajo' de un umbral. Para una mayor seguridad, el cliente puede requerir una prueba de vida para garantizar que el usuario es una persona real y no hay un ataque de presentación. La tecnología funciona procesando la(s) imagen(es) a través de una secuencia de redes neuronales profundas. Yoti elimina la imagen tan pronto se obtiene un resultado.*
 - II. *Usando la App Digital ID: el usuario escanea QR con la propia App para compartir su edad, antes debe haber creado una cuenta verificada con un documento identificativo y una*

selfie. El cliente puede recibir la edad en años o un valor 'por encima' o 'por debajo' de un umbral. Los usuarios obtienen un recibo en la App que detalla la información que se compartió, con quién y cuándo se realizó el trámite. Yoti también obtiene un recibo pero únicamente con la fecha (sello temporal) y que un atributo de edad fue compartido pero sin incluir la fecha de nacimiento, Yoti almacena esta información cifrada en los centros de datos de UK.

- III. "Usando un Documento Identificativo: el usuario toma foto del documento identificativo con la cámara del dispositivo, la tecnología de Yoti valida el documento y extrae la fecha de nacimiento, como capa de seguridad adicional se realiza comprobación de rostro. El cliente puede habilitar revisiones manuales requeridas. El cliente recibe la edad en años o valor 'por encima/por debajo'. Yoti retiene un log de cada verificación pero no almacena detalles. El documento de identidad y la imagen del rostro son eliminadas.
- IV. "Utilizando Tarjeta de Crédito: el usuario introduce número de tarjeta de crédito, fecha de expiración, CVV y PostCode. Los datos se envían a un proveedor de pagos y se realiza una retención temporal de 0.30 Libras para verificar que la tarjeta es válida. Yoti utiliza esto para inferir si el usuario tiene más de 18 años, luego se elimina el cargo retenido.
- V. "Utilizando Número de Teléfono: el usuario introduce el número de teléfono, el nombre, fecha de nacimiento y dirección. Los datos se envían a uno de los proveedores externos, el usuario puede opcionalmente recibir un SMS con un código de verificación OTP para comprobar que está en posesión del número teléfono. El proveedor verifica si el teléfono está asociado con un individuo mayor de 18 años y confirma si los datos proporcionados coinciden con los de la cuenta suscriptora del número de teléfono. Yoti utiliza esto para inferir que el usuario está por encima de los 18 años, información que se proporciona al cliente. Yoti no almacena los datos aportados por el usuario.
- VI. "Usando chequeo contra base de datos: el usuario introduce nombre, fecha de nacimiento, dirección y número de seguridad social (dependiendo de la jurisdicción). Yoti envía estos datos a un proveedor de crédito para confirmar que los datos son precisos o confirmar la fecha de nacimiento. Yoti utiliza esto para determinar que el usuario es mayor de 18 años. Yoti no almacena estos datos.
- VII. "Usando un servicio E-ID: se utilizan esquemas de verificación en Suiza, Dinamarca y Finlandia.
- VIII. "Usando licencia de conducir móvil en EEUU.

Para reducir el número de veces que un usuario necesita verificar su edad online, Yoti ha creado un sistema de Tokens de Edad.

- Token de Edad: si lo habilita el cliente de Yoti, estos tokens permiten al usuario reutilizar una verificación de

edad previa durante el tiempo que el cliente lo permita. El token de edad se crea cuando el usuario ha verificado previamente su edad con Yoti y contiene el resultado de esta verificación e información de cómo y cuándo fue realizada. No contienen información personal adicional y no realizan trazabilidad del usuario ni identifican donde ha estado un usuario (o de donde proceden). Los tokens se almacenan en el navegador del usuario en forma de cookie y tiene una duración temporal. Los usuarios pueden eliminarlo borrando la cache del navegador. Cuando el usuario accede a la web del cliente, este podrá leer el token de edad del navegador, si este token cumple con los criterios establecidos por el cliente, se devuelve un resultado confirmando que el usuario se ha verificado previamente. Si el usuario no tiene un token de edad que cumple criterios del cliente, se le da opción a que pruebe con otro método.

- *Cuenta de edad: los usuarios pueden almacenar los tokens de edad en sus 'cuentas de edad', esto les permite acceder a sus tokens desde un navegador o dispositivo distinto. Una vez que el usuario ha probado su edad con algún método establecido, tendrán la opción de crear una cuenta de Yoti con un nombre de usuario y una contraseña. Si el cliente habilita la opción de verificarse con cuenta de edad, los usuarios tendrán una nueva opción de hacer login en su cuenta y reutilizar un token de edad previamente creado.*

2) Para casos específicos Yoti hace posible una integración directa con una API de Estimación Facial de edad y con la App Digital ID.

- API de estimación facial: tecnología Machine Learning que estima la edad a partir de la imagen facial del usuario, la imagen es borrada tras el análisis. El usuario permanece anónimo, no hay identificación única y no se provee información adicional. La imagen se transmite de forma segura a los servidores donde es analizada y se obtiene estimación de edad y nivel de confianza de la respuesta. La foto no es visualizada por personal de Yoti y no es compartida con terceros. Se utiliza para confirmar si el usuario está por encima o por debajo de cierta edad.

- o La EIPD incluye el listado de cookies utilizadas por YOTI para desplegar sus servicios de verificación de edad, entre ellas está la cookie utilizada para almacenar el Token de Edad, esta cookie tiene de nombre (...) y se afirma disponer de una duración temporal de 30 días.
- o Se afirma que YOTI es responsable de tratamiento de los datos recabados del usuario para proporcionar un atributo de edad a través de la App Digital ID, para el resto de los Servicios de Verificación de Edad YOTI actúa como encargado de los tratamientos de los datos que se recaban, siendo los clientes de YOTI los responsables de tratamiento.

- o Para los tratamientos en los que YOTI actúa como responsable afirman que se recaban los siguientes tipos de datos a través de la App:
 - Documento identificativo subido por el usuario.
 - La edad generada por YOTI a partir de la fecha de nacimiento contenida en documento anterior.
 - Fotografía Selfie del usuario (tomada cuando el cliente ha habilitado la opción de llevar a cabo el cotejo de rostros/prueba de vida).
- o En relación con el acceso a los datos personales desde ubicaciones distintas (transferencias internacionales de datos), se afirma en esta EIPD:
 - YOTI dispone de un Centro de Seguridad ubicado en India que provee soporte para los usuarios que realizan el proceso de alta en la App (onboarding) creando una nueva cuenta. Una vez que se ha realizado el onboarding, los datos se almacenan separados y encriptados. Por otro lado, cuando se verifica la edad subiendo un documento identificativo, el centro de Seguridad en India puede proporcionar al cliente verificaciones manuales opciones. La arquitectura de diseño técnico de la plataforma Yoti garantiza que estos datos sean solo visibles en forma no cifrada a través de 'terminales tontos' para el personal que trabaja dentro del Centro de Seguridad de Yoti en India. Ningún otro miembro del personal de Yoti puede ver estos datos.
- o La EIPD incluye el siguiente listado de medidas para garantizar la seguridad de los datos personales tratados por YOTI:
 - (...)
 - o En relación con los periodos de retención de los datos incluye:

"Para los Servicios de Verificación de Edad no se retienen datos por parte de YOTI. En el caso de subida de documento identificativo y cuando el cliente habilita la verificación manual, se almacena durante 28 días. En la Estimación Facial de la Edad, la fotografía es borrada tras obtener el resultado. Para el token de edad y los datos de la Digital ID App, la retención queda establecida mientras el usuario mantiene activa la cuenta o después de tres años de inactividad".
 - o Para el tratamiento de los datos personales por parte de YOTI como responsable de tratamiento, manifiestan como Base Legítima la ejecución de un contrato, afirmando que "el tratamiento se hace sobre la base de una solicitud del propio usuario y es parte del servicio Digital ID proporcionado por YTI según los términos de uso establecidos". Cuando YOTI actúa como encargado de tratamiento afirman que la Base Legítima debe establecerla el cliente, como responsable de tratamiento, pudiendo ser alguna de las siguientes: *consentimiento, ejecución de contrato o interés legítimo*.
 - o En relación con el tratamiento de datos de menores de edad, afirman en la EIPD:

“Que los menores de edad esperan y comprenden el uso que Yoti realiza de sus datos, Yoti es explícito al trasladar que el uso del producto tiene la finalidad de verificar la edad. Yoti además ha realizado una investigación experiencial con jóvenes a través de PlayVerito (<https://www.yoti.com/blog/play-verito-research-young-peoples-attitudes-towards-facial-age-estimation/>) y trabajó con la ICO para desarrollar materiales educativos para jóvenes, durante el Sandbox de la ICO.

“Se recaba la información necesaria para verificar la edad de los usuarios. No existe ningún tipo de intrusión o perfilado y no se toman decisiones a partir de ningún tipo de perfil. No se comparten datos con terceros salvo los utilizados para verificar que el usuario es mayor de edad. El estado actual de la tecnología en esta área es avanzado, el producto de YOTI protege a los niños de los riesgos en línea, y están diseñados teniendo en cuenta como esencia la privacidad y la seguridad de los niños”.

- o La EIPD incluye apartado con análisis de la necesidad y proporcionalidad del tratamiento de datos que realiza YOTI, de este apartado se extraen las siguientes afirmaciones:

“Cuando YOTI actúa como responsable de tratamiento, La App Digital ID proporciona una vía para disponer de atributos de edad que puedan ser compartidos con otras personas u organizaciones según sea necesario. Para ello es necesario y proporcionado procesar la fecha de nacimiento obtenida del documento identificativo (para proporcionar atributos de edad verificados) y la fotografía del usuario para proporcionar un atributo de edad estimado. Para los Servicios de Verificación de Edad de Yoti (AVS), se proporcionan ocho métodos posibles para verificar la edad, Yoti devuelve la información mínima necesaria para la verificación. Es la solución más respetuosa posible con la privacidad. La organización que verifica la edad (como responsable de los datos) tiene la responsabilidad de decidir qué información personal se recaba y si ésta es necesaria y proporcional. Para el servicio de Estimación de edad mediante reconocimiento facial, el único dato personal utilizado es la imagen del usuario y se elimina una vez realizado el tratamiento facial, este borrado es auditado como parte del proceso PAS 1296:2018 de Yoti.
- o En relación con la licitud del tratamiento cuando YOTI actúa como responsable (Digital Id App), se afirma que la Base Legítima corresponde con el art 6.1.b (ejecución de contrato). Cuando YOTI actúa como encargado se indica que son los clientes de YOTI (responsables de tratamiento) los que deben tener una base legítima de este tratamiento, afirmando que *“Las soluciones de YOTI proporcionan una forma respetuosa con la privacidad para confirmar la edad sin revelar una fecha de nacimiento completa. Los servicios AVS proporcionan múltiples métodos para que los clientes garanticen la máxima accesibilidad y Yoti ha trabajado para reducir sesgo discernible en la estimación de la edad facial”.*

- o Realiza análisis del principio de minimización y exactitud de los datos cuando YOTI actúa como responsable de tratamiento (Digital ID App), afirmándose:
 - “Yoti proporciona un atributo de fecha de nacimiento verificada a un usuario que proviene de un documento identificativo que el propio usuario sube a su cuenta. Los datos personales se conservan mientras el usuario tiene la cuenta. El usuario puede eliminar su cuenta en cualquier momento”.*
 - “Es probable que la fecha de nacimiento sea exacta ya que proviene del documento de identificación que se verifica bien al configurar la cuenta o como parte del proceso de verificación. El resultado de la verificación de edad será preciso ya que se basará en la fecha de nacimiento que Yoti tiene en el momento de la solicitud, esta fecha proviene de una identificación válida y verificada del documento”.*
 - “Respecto a los datos tratados para Estimación Facial de la Edad la imagen es precisa ya que será del propio individuo frente a la cámara. La política de YOTI incorpora medidas anti-spoofing y de aseguramiento de que nuestro aprendizaje automático utiliza un conjunto representativo de datos de entrenamiento”.*
- o Realiza análisis del principio de transparencia, afirmándose:
 - “En la política de privacidad de la App se cubre la creación de un atributo de edad a partir del documento identificativo del usuario. Previamente a que el usuario comparta los datos a través de la App, se le muestra un aviso previo (just-in-time notice) que incluye información de privacidad para explicar lo que se está solicitando”.*
 - “Para la estimación facial de la edad, el cliente que utiliza el servicio es el responsable del tratamiento y el que tiene la responsabilidad de proporcionar la información al usuario sobre el método de verificación de edad utilizado”.*
 - “Para los Servicios de Verificación de Edad ofrecidos por YOTI, pese a que actúa como encargado de tratamiento, se proporciona un aviso de privacidad en su sitio web para explicar a usuarios finales sobre el funcionamiento del servicio, este aviso puede ser enlazado desde el propio sitio web del cliente”.*
- o Realiza análisis de la atención a los derechos de protección de datos, actuando YOTI como responsable y encargado de tratamiento de los datos.
- o En relación con las transferencias internacionales, se afirma: *“El centro de datos de Yoti se encuentra en el Reino Unido, en los casos de transferencias desde Reino Unido a la India Yoti se basa en las cláusulas contractuales estándar de la UE con la adenda del Reino Unido y también ha completado una evaluación de impacto”.*
- o En relación con el uso de categorías especiales de datos, se afirma: *“La estimación de la edad a través de reconocimiento facial no utiliza categorías especiales de datos debido a que el procesamiento no tiene el propósito de identificar o autenticar a un individuo”.* Se incluye URL que enlaza con un informe realizado por ICO (Information

Commissioner's Office) a partir de un análisis de la solución de estimación de la edad mediante reconocimiento facial de Yoti, se crea diligencia y se guarda en objetos asociados con nombre "Informe ICO de Estimación Facial de YOTI.pdf". De su análisis se extraen los siguientes fragmentos de texto relevantes (traducción no oficial):

"Yoti afirma que la estimación de la edad facial se basa en redes neuronales, entrenadas para poder estimar la edad humana mediante un proceso de aprendizaje automático, una forma de inteligencia artificial (IA). El producto funciona identificando primero el rostro humano dentro de la imagen para garantizar que el producto esté evaluando a un ser humano genuino. El producto divide la imagen en píxeles, cada píxel es solo un conjunto de números que se introducen en la red neuronal artificial. Esta es una red de procesamiento matemático por nodos dispuestos en capas, análogo a las conexiones en el cerebro humano. Mientras que un cerebro típico tiene alrededor de 100 mil millones de neuronas, la red neuronal artificial tiene solo cientos de miles de nodos. Los números (datos de píxeles) se alimentan y se filtran a través de la red neuronal. Cada nodo realiza una función matemática con los datos de píxeles y pasa el resultado a los nodos de la siguiente capa, hasta que un número finalmente emerge del otro lado de la red, este número es una edad estimada. Funciona rápidamente, devolviendo una estimación en alrededor de 1 a 1.5 segundos. El usuario necesita presentar su cara a la cámara descubierta (las gafas no suelen presentar un problema). La participación de Yoti en Sandbox de ICO se centró en el desarrollo de su producto de estimación de la edad, ya que la organización pretendía ampliar el uso del producto a niños de entre 6 y 12 años".

"El ICO aconsejó a Yoti que tuviera en cuenta los riesgos para la protección de datos asociados a la ampliación del intervalo de edad de su tecnología de estimación de la edad a través de una Evaluación de Impacto relativa a la protección de datos. Yoti lo hizo revisando su EIPD de estimación de la edad existente para incluir una visión de los riesgos asociados con el procesamiento de datos de niños para trabajar su modelo eficazmente en niños de entre 6 y 12 años. Yoti trabajó para obtener datos de entrenamiento de varias fuentes con el fin de obtener los datos necesarios para entrenar el modelo, en concreto:

-Recopilación datos a través de un portal web. Este método de recopilación consistió en solicitar a los usuarios adultos que proporcionaran una imagen de su hijo, mes y año de nacimiento, y el consentimiento explícito de los padres o tutores para que estos datos se trataran a efectos de entrenar el algoritmo de estimación de la edad de Yoti para niños de 6 a 12 años.

-Recopilación de datos a través de una organización de bienestar digital familiar (Be In Touch) ubicada en Sudáfrica. Este método de recogida consistió en utilizar la relación de Be In Touch con una red de escuelas de

Sudáfrica. Yoti envió una carta a los padres o tutores de los niños que asisten a estas escuelas con un formulario de consentimiento por escrito e información de privacidad adecuada para recopilar y procesar los datos de los estudiantes. El ICO no lo aconsejó debido a las implicaciones de protección de datos de esta colección de datos personales”.

“Durante el curso de la recopilación de datos, la ICO proporcionó guías ad hoc y asesoramiento a Yoti a medida que desarrollaban avisos de consentimiento y privacidad. La ICO aconsejó sobre cómo hacer que el contenido más accesible para los niños”.

“En octubre de 2021, Yoti publicó su White Paper de estimación de edad facial, que proporciona detalles sobre su éxito en la creación de un modelo viable de estimación de la edad para niños de 6 a 12 años. En el libro blanco, Yoti afirmaba que el modelo era preciso dentro de 1,28 años y funcionó de manera efectiva a través del género y el tono de piel. Habiendo considerado cómo funciona la herramienta de estimación de edad (como nos explicó Yoti) hemos llegado a la conclusión de que puede ser distinguida de otras tecnologías de reconocimiento facial (FRT), ya que Yoti no está utilizando la herramienta con el propósito de identificar de forma única a las personas cuyas imágenes se capturan, se está utilizando para categorizarlos por edad sin identificarlos de manera única.

- o Incorpora apartado con la evaluación de los riesgos de privacidad y las medidas concluidas, incluyendo el siguiente texto:

“Riesgos de incumplimiento de los principios de privacidad y obligaciones legales: No existen riesgos de incumplir los principios de protección de datos ya que las soluciones de verificación de edad incluyen la privacidad desde el diseño. Los clientes de YOTI tienen la obligación de evaluar este cumplimiento”

“Riesgos de potencial impacto en los individuos (por daño físico, emocional o material): Riesgo de que el cliente haga mal uso de los datos de edad que recibe de YOTI” (riesgo intrínseco MEDIO y residual nivel BAJO). Como medida mitigadora nuestros contratos estándar requieren que los clientes tengan un aviso de privacidad y también eviten revender o transferir datos de verificación de edad”.

“Riesgos de seguridad: No hay riesgos de seguridad específicos identificados para las soluciones de control de edad. Diseñamos nuestros sistemas para construir altos niveles de seguridad en cada etapa. El cliente de Yoti tiene la responsabilidad de determinar cualquier riesgo de seguridad de la información personal recibida mediante el uso de la solución de verificación de edad. Yoti incorpora un proceso de gestión de riesgos de

seguridad para todos los productos, que considera factores de riesgo tanto internos como externos y que incluye:

-(...)

- o Incorpora apartado incluyendo recomendaciones aportadas por el DPO a la evaluación de impacto, en concreto:

“Las soluciones de verificación de edad están diseñadas para ser la forma más respetuosa con la privacidad de verificar la edad/elegibilidad. El procesamiento de datos personales de Yoti para proporcionar atributos de edad a los usuarios es mínimo y no plantea problemas de cumplimiento. Como encargado de tratamiento, las soluciones brindan información mínima según las circunstancias y, en algunos casos, no requieren que se envíen datos personales al cliente. Los Servicios de verificación de Edad de Yoti (AVS) han sido diseñados para maximizar la privacidad y reducir el riesgo para Yoti y el cliente, los datos se eliminan inmediatamente y sólo se devuelve al cliente un atributo de edad superior a umbral o edad en años. (...) y se obtiene la cantidad mínima de datos del usuario. En la Estimación Facial de la Edad

se proporciona una forma respetuosa con la privacidad de verificar la edad. Para el atributo de edad de la App Digital ID, el cálculo de la edad será preciso al basarse en documento de identificación válido y verificado. Por lo tanto, los clientes que realizan verificaciones de edad disponen de una forma respetuosa con la privacidad de realizarlo”.

- Se acredita documento con el informe de auditoría de conformidad con la norma ISAE3000 SOC 2, realizada para periodo comprendido entre enero y diciembre de 2022. De su análisis se extrae la siguiente información relevante (el documento está en lengua inglesa, se proporciona traducción no oficial):
 - (...)
- Se acredita el *****DOCUMENTO.1 e ***DOCUMENTO.2**, con fecha de validez hasta 22 de agosto de 2026.
- Se acredita documento interno con la Declaración de Aplicabilidad para cumplimiento con *****DOCUMENTO.1 e ***DOCUMENTO.2**, con fecha de creación inicial 2015 y varias actualizaciones posteriores, fecha de última actualización febrero de 2024. Del análisis de este documento destaca el siguiente contenido:
 - o (...) Este documento ha sido analizado con detalle en punto anterior.
- Aportan documento que ilustra el flujo de los datos personales como parte de los procesos de verificación de edad, incluyendo los sistemas afectados en cada etapa del tratamiento.
- Afirman que los datos personales se almacenan principalmente en servidores propiedad de Yoti alojados en centros de datos del Reino Unido, utilizándose adicionalmente un proveedor de servicios en nube (...), fijándose su almacenamiento también en Reino Unido, habiéndose aceptado las condiciones estándar (...) y el correspondiente acuerdo de encargo de tratamiento (se acredita documentalmente, no obstante, no incluye firma ni fecha de creación).
- Manifiestan que YOTI utiliza tecnología de terceros proveedores para llevar a cabo el reconocimiento facial 1-1 entre la selfie del usuario y la foto del

- documento identificativo y comprobar signos vitales en la selfie, no obstante, afirman que la tecnología empleada está desplegada en servidores propios de YOTI y los proveedores externos no tratan ningún dato personal.
- Afirman que YOTI conserva los datos de forma que se permite la identificación de los interesados únicamente durante el tiempo necesario para alcanzar los fines para los que se recabaron, manifiestan que el proceso de supresión es automático y se somete al proceso de control de cambios antes de su puesta en el entorno de producción. Estos controles se verifican en el marco de las auditorías *****SISTEMA.1 y ***SISTEMA.2 (...)**, acreditado documentalmente.
 - En relación con la información que se proporciona a los usuarios sobre los riesgos del tratamiento, afirman que Yoti no es responsable de proporcionar información de privacidad a los usuarios finales, siendo responsabilidad de los clientes de YOTI. Sin embargo, afirman que YOTI ha redactado información de privacidad sobre sus productos de verificación de edad que puede complementar la información de privacidad de los clientes e informar a las personas sobre cómo YOTI utiliza sus datos. Esto se puede encontrar en el sitio web de YOTI (<https://www.yoti.com/privacy/age-verification/>). Se crea diligencia y se adjunta en objetos asociados con nombre *"Información proporcionada sobre el tratamiento.pdf"*. Se acredita captura de pantalla con la información que visualiza el usuario cuando se le muestra pantalla ofreciendo varias opciones como métodos para confirmar su edad, en concreto *ID Verification, Age Estimation, Digital ID App*.
 - En relación con el perfilado de los usuarios, YOTI afirma que sus productos de verificación de edad no implican la creación de perfiles en el sentido del RGPD, ya que los datos personales sólo se utilizan con el fin de completar las comprobaciones, no implican un seguimiento continuo, y los datos no están vinculados a la identidad de un individuo para construir un perfil. Afirman que YOTI no utiliza datos personales para analizar o predecir aspectos relacionados con el desempeño laboral, la situación económica, la salud, las preferencias o intereses personales, la confiabilidad o el comportamiento, la ubicación o los movimientos precisos de los interesados.
 - En relación con el uso de datos biométricos de usuarios para finalidades de investigación y desarrollo (I+D), se acredita documento sobre la evaluación de impacto de los tratamientos de datos en la App para la finalidad I+D en su tecnología de estimación facial. YOTI no considera que los datos personales utilizados para mejorar su tecnología sean datos biométricos de categoría especial en sentido RGPD, ya que no se utilizan para identificar de manera única a las personas. Afirman que tampoco hay forma de vincular los datos utilizados (por el equipo de I+D) con los datos almacenados como parte de la App Digital ID. Del análisis del documento proporcionado se extrae la siguiente información relevante (traducción no oficial):
 - o Incluye la fecha de última actualización 1 de marzo de 2024.
 - o Incluye URL al *White Paper* sobre la tecnología de estimación facial de Yoti con información actualizada a fecha 2 de septiembre de 2024 (se diligencia como objeto asociado con nombre *"Facial Age Estimation White Paper Yoti 1 y 2.pdf"*), del análisis de este enlace se destacan las siguientes afirmaciones de YOTI sobre su algoritmo:

"(...)"

 - o *Los tipos de datos recopilados y procesados como parte de este proyecto son:*

- *Imagen facial junto con una marca de tiempo de la captura de imagen. Estas imágenes faciales proceden de:*
 - *a) Flujo de selfies: La aplicación puede pedir a los usuarios que tomen una selfie al realizar ciertas acciones en la aplicación (por ejemplo, al restablecer el PIN o recuperación de la cuenta) para asegurarse de que es realmente el usuario;*
 - *b) Pruebas de vida: Los usuarios individuales realizan una «prueba de vida» durante la incorporación para demostrar que son una persona real. La App Digital ID presenta al usuario tres palabras generadas al azar, y solicita que las hablen en voz alta en su dispositivo móvil. Los fotogramas se extraerán de los videos.*
- *Mes y año de nacimiento de la persona en la imagen facial (se obtienen del documento identificativo del usuario).*
- *Información de género (si está disponible) con el fin de reducir el sesgo.*
- *Información sobre el tipo de documento identificativo.*
- *Código del país/país emisor.*
- o *Con el fin de limitar la influencia de la demografía sobrerrepresentada en el rendimiento del modelo, las imágenes de entrenamiento se agrupan primero por rango de edad, género y tono de piel. El equipo de I+D de Yoti considera 12 rangos de edad (0-1, 2-3, 4-6, 7-9, 10-12, 13-15, 16-17, 18-24, 25-29, 30-39, 40-49, 50-60), 4 grupos de género (masculinos, femeninos, otros y desconocidos) y 3 grupos de tonos de piel que se basan en la escala de Fitzpatrick. Esto da un total de 144 combinaciones. Los datos demográficos con un recuento de imágenes por encima de un umbral predefinido se sub muestrean a esa cantidad. Este umbral se ajusta empíricamente y depende del volumen de datos de entrenamiento disponible en ese momento. El proceso se repite antes de cada entrenamiento para que finalmente todas las imágenes disponibles se utilicen durante el entrenamiento.*
- o *El equipo de I+D también necesita crear un conjunto de datos de prueba con imágenes que estén etiquetadas con el género y tono de piel (en la escala de Fitzpatrick). Esto es para asegurarse que el modelo sea lo más imparcial posible. El etiquetado del conjunto de pruebas se realizó originalmente manualmente, pero posteriormente el equipo de I+D ha migrado a un sistema automatizado para el etiquetado de datos.*
- o *Datos utilizados:*
 - *Foto (con fondo recortado automáticamente), junto con una marca de tiempo de cuándo se tomó la foto.*
 - *Año y mes de nacimiento de los documentos identificativos.*
 - *Género de los documentos identificativos (si están disponibles).*
 - *Grabación de vídeo.*
 - *Grabación de audio.*
 - *Información del dispositivo.*
 - *Datos de comportamiento del usuario.*
 - *Información relacionada con la salud.*

- *Raza / origen étnico (solo para el etiquetado del conjunto de datos de prueba y solo la estimación del tono de piel en la escala de Fitzpatrick).*
- *Datos de los niños. Los datos de producción incluyen datos de niños de 13 a 18 años que son usuarios de aplicaciones digitales.*
- *Datos biométricos.*
- *Otros datos no personales: tipo de documento y país emisor.*
- o *Se consideran los siguientes principios en el diseño de la tecnología de Yoti:*
 - *El Interés superior del menor: Tenemos una información clara en la aplicación de cómo los usuarios pueden optar por no utilizar los datos con fines de I+D a través de la configuración de la App. Esto también está cubierto en el aviso de privacidad de la Ditial ID App.*
 - *Aplicación adecuada a la edad: no podríamos restringir el uso de los datos de los niños más de lo que ya lo hemos hecho. Sin datos de menores no podemos construir un modelo que pueda estimar con precisión los datos de los niños y, por lo tanto, no podemos usar el modelo para su beneficio en la aplicación y el ecosistema de Yoti.*
 - *Transparencia: los menores de 18 años deben ser capaz de entender tanto las interfaces de la App como el Aviso de privacidad con respecto al uso de sus datos. Hemos encargado la investigación de usuarios y nuestro DPO ha liderado un proyecto para hacer que las interfaces y Política de privacidad sean más transparentes.*
 - *Los datos están protegidos por los extensos controles de seguridad *****DOCUMENTO.1 y ***SISTEMA.1 (...)**. Yoti no reutiliza los datos para otro fin.*
 - *Ajustes predeterminados: En la App Digital ID el valor por defecto es que los datos se puedan usar para I+D. Yoti ha tomado medidas para dejar esto claro a los usuarios. Los usuarios pueden optar por excluirse, evitando que sus datos se utilicen para I+D, haciendo para ello uso de la configuración de la App.*
 - *Minimización de datos: se aplican las mismas normas a los datos de niños que a los de adultos. Solo tomamos la imagen facial y el mes y año de nacimiento para el conjunto de datos de producción.*
 - *Intercambio de datos: los datos no se comparten con ningún tercero.*
 - *Geolocalización: no utilizado.*
 - *Control parental: La App no puede ser utilizada por personas menores de la edad digital de consentimiento, es decir, 13 en el Reino Unido y 14 en España. La App tiene un sistema de control de edad basado en la jurisdicción para garantizar que no permitimos el uso de la App a las personas menores de la edad según jurisdicción. Incluye captura de interfaz de ejemplo*

mostrada a un usuario de España, esta captura incluye el texto: “Confirma tu edad”, dando dos opciones, “Soy mayor de 14 años” “Tengo 13 años o menos”.

- *Elaboración de perfiles: no se elaboran perfiles que tengan algún impacto en el niño.*
- o Incluye análisis de necesidad y proporcionalidad, afirmándose:

“La única forma de entrenar el modelo de estimación de la edad facial de manera efectiva es proporcionándole imágenes de calidad y ángulos similares, con un mes y año de nacimiento precisos. La desventaja de los conjuntos de datos disponibles públicamente es que no están disponibles para uso comercial, son pequeños y contienen muestras mal identificadas (como edad incorrecta y ojo de pez) o no es posible utilizar estos datos de conformidad con los requisitos pertinentes de protección de datos (como base legal, transparencia, etc.). Estos factores reducen considerablemente la precisión del modelo. Por lo tanto, el uso de datos de producción de la App Digital ID es necesario para mitigar este problema y asegurarnos de desarrollar un modelo competitivo de clase mundial”.

“Con respecto al uso de datos de producción, este proyecto implicará la información mínima requerida para los fines mencionados anteriormente, como selfies y una imagen recortada de la cara de una persona para entrenar el modelo en verificación facial. Esta información no es (y no será) accesible fuera del equipo de I+D y administradores de bases de datos. Los usuarios pueden optar por no utilizar los datos con fines de I+D en la configuración de la App en cualquier momento. Esto se deja claro tanto en el proceso de alta como en el aviso de privacidad”.

“No hay una forma menos intrusiva en privacidad para lograr el mismo resultado. En cualquier caso, la intrusión en la privacidad es mínima, ya que el equipo de I+D no tiene ninguna información para vincular la foto a la identidad de la persona. La mayor parte de la actividad de I+D implica mirar los resultados (cifras y estadísticas), no los datos subyacentes, ya que solo se accede a estos datos cuando existe una anomalía inexplicable con los resultados o para etiquetar imágenes con fines de prevención de sesgos”.

“El procesamiento está justificado en relación con los beneficios, ya que permitirá a Yoti desarrollar un software de estimación de la edad facial de clase mundial en el que se puede confiar, al haber supervisado todos los aspectos de su desarrollo y tomar medidas para abordar el sesgo”.
- o Se incluyen las siguientes afirmaciones relevantes:

“No se realizan perfiles, no obstante, se señala que el conjunto de datos de pruebas tendrá asignados tonos de piel”.

“Los riesgos asociados al uso de las imágenes se han minimizado en la medida de lo posible en el diseño de la fase de recogida de este proyecto. La intención es que estas imágenes se recorten antes de que puedan ser utilizadas por I+D. Un

riesgo identificado es que esta automatización diseñada para minimizar los datos disponibles para el tratamiento falle, provocando la recogida de datos excesivos e innecesarios. Esto es revisado constantemente por el equipo del R&D para asegurarse de que está funcionando correctamente”.

“El conjunto de datos de prueba debe equilibrarse entre géneros y etnias. Yoti tiene un control limitado sobre los datos de producción, ya que proviene directamente de los usuarios de la App Digital ID. Parte del trabajo I+D es etiquetar datos con información como el tono de piel para poder abordar y mitigar cualquier sesgo en el modelo. No hay terceras partes (proveedores externos) involucrados en el tratamiento, todo se hace de forma interna. Los Selfies se recortarán enviados a la base de datos de I+D para eliminar imágenes de fondo. Los únicos datos asociados con los datos de producción son el mes y el año de nacimiento, la base de datos de I+D no recibe otros datos”.

- o Incluye varias capturas de pantallas con la información que se proporciona al usuario en el momento del alta en la App (“onboarding”) en relación con el tratamiento de I+D. Estas capturas proporcionan los siguientes textos:

“¿Cómo utilizamos tus datos? Queremos ofrecerte la mejor experiencia posibles y ello lo alcanzamos con: datos analíticos (obtenemos datos para entender cómo los usuarios usan la App, puedes optar por no participar a través de la configuración de tu cuenta. Consulta nuestra política de privacidad), Investigación interna (extraemos algunos datos para ayudar a entrenar y mejorar nuestra tecnología y hacerla más segura, esto incluye: copia separada de tu fotografía, mes y año de nacimiento, género y tipo de documento aportado. Puedes optar por no participar a través de mis datos>consentimiento biométrico). Necesitamos tu consentimiento. Utilizamos un escaneo facial para asegurarnos de que el documento de identificación aportado corresponde con la persona que está utilizando la App. No puedes utilizar la App sin este escaneo facial (mapa digital único de las características de tu rostro)”.

- o En relación con la Base Legítima utilizada para este tratamiento de datos, (imagen facial, mes y año de nacimiento, tipo de documento y género) se afirma por YOTI que existe un Interés Legítimo, manifestando:

“Yoti tiene un interés legítimo importante en desarrollar su tecnología de estimación de edad y mejorar el rendimiento del modelo en particular en lo que se refiere a la reducción del sesgo. El procesamiento de los datos de la manera descrita en esta EIPD promoverá este interés con un impacto o riesgo mínimo de daño para el individuo. Las personas son informadas sobre este procesamiento y se les ofrece una opción de exclusión. Cabe señalar que Yoti no considera que los datos utilizados sean datos biométricos de categoría especial en el sentido del RGPD ya que no se utilizan con el fin de identificar

de forma única al usuario y no hay forma de vincular los datos utilizados por el equipo de I+D a los datos almacenados en la Digital ID App”.

“Para los datos de categoría especial (etiquetado racial/étnico de las imágenes) se utiliza Interés Público Esencial 9.2.g) RGPD, que establece que el tratamiento debe ser: necesario por razones de interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que será proporcionado al objetivo perseguido, respetará el contenido esencial del derecho a la protección de datos y prever medidas adecuadas y específicas para salvaguardar los derechos fundamentales y los intereses de los datos”. Esto se hace sobre la base de la igualdad de oportunidades o condición de tratamiento establecida en el Anexo 1, Parte 2, Párrafo 8 del Data Protection Act 2018. Más concretamente, este tratamiento refleja el interés público esencial en prevenir la discriminación, de conformidad con el artículo 14 del Convenio Europeo de Derechos Humanos (es decir, prohibición de la discriminación)”.

“Yoti ha llevado a cabo una prueba de equilibrio de intereses legítimos y ha determinado que el procesamiento es necesario para un interés legítimo (desarrollando este modelo en beneficio de los usuarios de la aplicación Digital ID y otros usuarios en el ecosistema de Yoti) que no anula los intereses o los derechos fundamentales de los interesados. En particular:

-Existe un interés público abrumador en desarrollar este modelo para la protección de los niños en la aplicación de identificación digital y en Internet en general. Esta tecnología también permite un enfoque más inclusivo para demostrar la edad, por ejemplo, para las personas que no tienen documento de identidad o no se sienta cómodo utilizando su propio documento de identidad para este fin.

-Las personas no son identificables por el equipo de I+D y no hay forma posible de vincular los datos en el conjunto de datos de producción utilizados por I+D a otros datos en poder de Yoti.

-Los usuarios pueden optar por no formar parte del I+D en cualquier momento a través de la configuración de la App Digital ID.

-Los datos de I+D solo son accesibles para el personal interno de I+D y los administradores de bases de datos, este acceso está estrictamente controlado.

-Se minimizan los datos del conjunto de datos de producción de I+D

“Se considera un tratamiento justo y leal ya que los usuarios de la App Digital ID son informados explícitamente sobre este procesamiento antes de proporcionar sus datos, incluyendo la forma en que pueden optar fácilmente por no participar en cualquier momento sin ningún impacto en el uso de la

aplicación. Por esta razón, el tratamiento se considera justo y dentro de las expectativas razonables de una persona”.

- En relación con el consentimiento informado para el tratamiento de datos biométricos afirman: *“Al incorporarse los usuarios a través de la App Digital ID deben dar su consentimiento para usar la aplicación, ya que dicha aplicación implica el tratamiento de datos biométricos. Observamos que este proceso de alta en la App (onboarding) es independiente de la verificación de edad que realiza YOTI y que el cliente puede solicitar”.* Se acreditan capturas de pantallas con las interfaces mostradas en el proceso de ‘onboarding’ de la App.
- En relación con la forma de proceder de YOTI con los datos personales recabados cuando detecta que el usuario que verifica su edad es menor, afirman:

“La App Digital ID no puede ser utilizada por personas menores de la edad de consentimiento digital, es decir, 13 años en el Reino Unido y 14 años en España. La App Digital ID cuenta con un sistema de control de edad basado en la jurisdicción para garantizar que no se permite que personas que afirman ser menores de la edad de consentimiento digital en esa jurisdicción en particular utilicen dicha aplicación”.

Con objeto de aclarar algunos aspectos de la investigación, en fecha 14 de mayo de 2024 se decide realizar nuevo requerimiento de información a YOTI marcado por la siguiente línea de investigación:

- Que confirmen cuales de los métodos de verificación de edad que proporcionan se están utilizando por usuarios residentes en España.
- Que acrediten el modelo de contrato de encargo de tratamiento que se formaliza con los clientes que utilizan YOTI en España.
- Que aporten información adicional aclaratoria sobre los datos que almacena YOTI cuando un usuario ha compartido su atributo de edad a través de la App (*share receipt*).
- Investigar con más detalles los tiempos de retención de los documentos identificativos de los usuarios que han realizado el proceso de alta (*onboarding*) en la App.
- Investigar las garantías de seguridad implantadas para el acceso a los documentos identificativos y la fotografías selfies por parte de empleados de YOTI cuando el cliente ha solicitado comprobación manual.
- Investigar el uso de los datos personales recabados por Yoti con la finalidad de para evitar casos de fraude.
- Investigar el proceso de verificación de edad de YOTI mediante el chequeo contra bases de datos para usuarios residentes en España.
- Investigar el proceso verificación de edad de YOTI mediante proveedores de telefonía móvil para usuarios residentes en España.
- Investigar el proceso de verificación de edad de YOTI mediante tarjetas de crédito para usuarios residentes en España.
- Investigar los datos de geolocalización que se almacenan en los servidores de YOTI para usuarios menores de edad.

En fecha 7 de junio de 2024 y registro de entrada REGAGE24e00042560090 se recibe respuesta al requerimiento anterior, de su análisis se extrae la siguiente información relevante para la investigación:

- Afirman que todos los servicios de verificación de edad de YOTI están disponibles para su uso en España. A modo indicativo de los volúmenes recientes, afirman que en el periodo entre febrero y abril de 2024 se realizaron en España los siguientes controles de edad:
 - o Mediante teléfono móvil: 0
 - o Mediante chequeo contra bases de datos: 0
 - o Mediante estimación de edad: 39772
 - o Mediante documento identificativo: 737
 - o En la App Digital ID: 16
 - o Mediante tarjeta de crédito: 1
- Afirman que los clientes de Yoti tienen un contrato para la prestación de servicios que incluye un acuerdo de tratamiento de datos estándar como parte de los términos de Yoti o bien un acuerdo de tratamiento de datos personalizado negociado con el cliente de Yoti. No acreditan modelo de encargo.
- En relación con la conservación de los datos por YOTI afirman:

“Cuado YOTI actúa como responsable conserva los datos de la cuenta mientras el usuario tenga una cuenta con Yoti y durante los próximos tres años de inactividad de dicho usuario. Los usuarios pueden eliminar estos datos, o su cuenta, en cualquier momento y los datos son borrados automáticamente al caducar los 3 años de inactividad. Yoti no puede acceder a los datos de las cuentas de los usuarios, cada registro de datos se almacena por separado y se encriptan, lo que significa que no hay forma de combinar los datos para crear un perfil de una persona individual. Solo el usuario individual tiene acceso a la clave de descifrado en su propio dispositivo; sin esta clave de descifrado del usuario, Yoti no tiene forma de descifrar los datos. Cuando YOTI actúa como encargado almacenamos el atributo de edad resultado (Yoti no lo vincula a ningún otro dato identificable, como el nombre o el documento de identidad) siempre que el cliente tenga la cuenta con Yoti o mientras el cliente establezca la retención de estos datos”. Aportan captura de pantalla acreditándolo.

“Cuando los usuarios realizan el proceso de onboarding en la App Digital ID, pueden optar por agregar un documento de identidad. Si no es posible realizar una verificación automatizada de dicho documento, el documento de identidad, junto con la imagen ‘selfie’ se envía al centro de seguridad de Yoti a través del sistema interno de Yoti para una revisión manual por parte de nuestros especialistas en verificación de identidad. Como se ha indicado, esta revisión manual sólo se produce en el caso de que no sea posible una verificación automatizada, por ejemplo, mediante el chip NFC del documento de identidad. Si hay una verificación manual, los especialistas de Yoti revisarán el documento para asegurarse de que sea genuino y también compararán la foto del documento de identidad con la imagen ‘selfie’, para asegurarse de que sean la misma persona. Estos datos son visibles para los empleados individuales de Yoti en el centro de

seguridad durante 28 días, después de lo cual se eliminan del sistema de administración”.

- En relación con los procesos antifraude establecidos por YOTI y la comparación con bases de datos internas de YOTI para esta finalidad, afirman:
“Los documentos identificativos subidos por el usuario en el proceso de verificación de edad se cotejan con una base de datos utilizando el número de documento, tipo de documento y el país emisor. Si se encuentra una coincidencia, la verificación enviará una alerta de ‘Coincidencia de base de datos de fraude’ al cliente solicitante. Si un cliente pregunta los motivos de la coincidencia, Yoti puede brindar información adicional sobre por qué se marcó como fraude, es decir, por manipulación, falsificación, etc., teniendo en cuenta que el cliente, por su parte, tiene acceso a la imagen del documento. El usuario simplemente recibirá un mensaje de ‘fallo’ en su verificación, pero no se le informará sobre el motivo. Yoti no conserva de forma independiente el documento de identificación enviado por el usuario”.
- En relación con el uso del servicio de verificación de edad mediante teléfono móvil, aportan una relación con los proveedores externos utilizados en España para realizar comprobaciones de números de teléfonos móviles que aportan los usuarios, en concreto afirman:
 - o *“*****PROVEEDOR.1**: este proveedor toma el número de teléfono ingresado por el usuario (y opcionalmente otros datos) y verifica si coincide con un registro al que tiene acceso a través de operadores de redes móviles o sus otros registros. El proveedor recibe el número de teléfono móvil y de forma opcional el nombre, fecha de nacimiento y dirección (Datos del pagador de la factura)”.*

Se realiza diligencia de la siguiente documentación obtenida de la página web del proveedor *****PROVEEDOR.1 (***URL.1)**:

- Política de Privacidad (objeto asociado al expediente **“***EXPEDIENTE.1”**).
- Información de seguridad (objeto asociado al expediente **“***EXPEDIENTE.2”**).
- Información del servicio de verificación de edad de *****PROVEEDOR.1** (objeto asociado **“***EXPEDIENTE.3”**).
- Información sobre el servicio de recuperación de datos identificativos de usuarios (objeto asociado **“***EXPEDIENTE.4”**)

Llama especialmente la atención las dos últimas diligencias con la descripción de los servicios que proporciona la empresa, a través de los cuales un cliente puede obtener datos identificativos y de contacto de usuarios vinculados a un número de teléfono móvil proporcionado.

Adicionalmente, se insiste en una búsqueda abierta en el espacio de internet con objeto de obtener información más detallada sobre la

lógica de funcionamiento del servicio ofrecido por la empresa *****PROVEEDOR.1** y cómo recaban los datos para ofrecer su servicio, obteniéndose como resultado varias páginas de internet donde se denuncia un posible perfilado en secreto de usuarios mundiales realizado por esta compañía. En concreto, llama especialmente la atención un documento obtenido de la página web de la organización NOYB (*European Center for Digital Rights*), con la denuncia que este organismo presentó ante la Autoridad de Protección de Datos Belga sobre múltiples posibles infracciones en materia de protección de datos realizadas por esta compañía, en concreto se denuncia la falta de transparencia en los tratamientos de datos de usuarios, tratamientos de datos sin una base legítima válida, perfilado y toma de decisiones automáticas, transferencias internacionales sin garantías e incumplimiento con el principio de exactitud y limitación de la conservación de datos. Se crea diligencia de este documento y se guarda en objetos asociados con nombre “*Denuncia NOYB a ***PROVEEDOR.1 ante DPA Belga.pdf*”. No se han encontrado resultados sobre posibles resoluciones publicadas por esta DPA en relación con esta denuncia.

- o “Operadores *****PROVEEDOR.2** y *****PROVEEDOR.3**: estos proveedores se utilizan por Yoti para confirmar mediante SMS (contraseña de un solo uso) que el número/teléfono móvil está en posesión del usuario real en el momento de la verificación (después de esta confirmación, sus detalles se verificarán con *****PROVEEDOR.1**).”.
- En relación con el uso del sistema de verificación de edad mediante tarjeta de crédito, manifiestan:
 - o “Yoti utiliza *****EMPRESA.1** para realizar comprobaciones de tarjetas de crédito. En tal caso, *****EMPRESA.1** actúa como procesador/sub encargado. El Acuerdo de tratamiento de datos con *****EMPRESA.1** se adjunta a esta respuesta como Documento 2. El acuerdo de servicio principal con *****EMPRESA.1** también está disponible en línea aquí como referencia (...). Se crea diligencia de la URL anterior y se adjunta como objeto asociado (...)”.

Del análisis del acuerdo de encargo de tratamiento de datos formalizado se extrae la siguiente información relevante:

- El documento no contiene firmas e incluye la fecha de última actualización, 15 de diciembre de 2023.
- No se identifican partes suscriptoras del acuerdo ni firmas.
- Se trata de un documento que describe de forma general el tipo de datos tratados por *****EMPRESA.1** cuando actúa como responsable y como encargado de tratamiento de los datos, incluyendo la tipología de datos que trata en cada caso, las obligaciones asumidas por la empresa y las medidas de seguridad implantadas.
- Incluye apartado con las obligaciones de *****EMPRESA.1** cuando actúa como encargado de tratamiento de los datos. Incluye anexo con detalles de todas las medidas de seguridad implantadas por *****EMPRESA.1**

- Incluye texto afirmando la necesidad de llevar a cabo transferencias internacionales de datos a Estados Unidos para la prestación del servicio por parte de *****EMPRESA.1**, así como las transferencias de datos a terceras empresas que se realizan por parte de *****EMPRESA.1** para la prestación del servicio. Hacen referencia a la URL *****URL.2** como adenda al contrato y garantía de las transferencias realizadas. Se crea diligencia de la URL anterior y se guarda como objeto asociado “(...)”
- En relación con el Servicio de Verificación de Edad mediante atributo reutilizable, se afirma la posibilidad de realizarse a través del “token de edad” y la “cuenta de edad” del usuario, en concreto aclaran:

“Los Tokens de Edad son un tipo de cookie que se almacena en el navegador de un usuario. Contiene un indicador sobre los resultados de la verificación de edad, el tipo de verificación realizada y cuándo se realizó. Cuando un cliente ha habilitado los tokens de edad como método aceptado de verificación de edad y, simultáneamente, el contenido del token de edad cumple con los criterios establecidos por ese cliente específico, se puede utilizar este token como método verificación de edad. Incluye una firma que se puede validar utilizando la clave pública de Yoti para verificar que el token se haya emitido legítimamente. Un ejemplo de formato sería:

(...)”

“Cuenta de Edad: los usuarios pueden optar por almacenar sus tokens de edad en una cuenta de edad y reutilizar las comprobaciones de edad en otro navegador o dispositivo (si lo habilita el cliente Yoti). La cuenta de edad contiene:

- El Token de Edad.
- Un nombre de usuario y una contraseña de usuario segura con hash.
- Un ID aleatorio generado por el sistema (UUIDv4) y otro ID de visitante aleatorio generado por el sistema (UUIDv4).
- Un correo electrónico opcional con hash y salted.
- Metadatos adicionales con los registros de creación de cuenta y último cambio realizado en esta”.
- En relación con el Servicio de Verificación de Edad mediante Chequeo contra Bases de Datos (Database Check), aportan la siguiente afirmación:

*“Yoti emplea *****SISTEMA.3** para realizar comprobaciones contra bases de datos en España. Con respecto al procesamiento de datos personales por parte de *****SISTEMA.3**, Yoti es el encargado y *****SISTEMA.3** es el subencargado, el cliente de Yoti es el responsable”. Se acredita contrato de encargo formalizado, el documento está en lengua inglesa, incluye fecha de firma 11 de enero de 2017 y está firmado por los suscriptores *****EMPRESA.2** y Yoti Limited. El objeto del encargo (finalidad del acuerdo) es cotejar los datos de *****SISTEMA.3** con los datos aportados por YOTI, para autenticar o verificar a las*

personas usuarias. Los datos personales afectados son el nombre, dirección y fecha de nacimiento de usuarios que desean registrarse con la App de Yoti. El contrato entra en vigor el 7 de diciembre de 2017 e incluye renovación anual automática cada 12 meses.

Se realiza búsqueda de información pública en internet sobre el funcionamiento de los servicios de verificación de edad prestados por la empresa *****EMPRESA.2 (***URL.3)**, creándose las siguientes diligencias:

- Información del funcionamiento del servicio de verificación de edad prestado por esta empresa (se adjunta como objeto asociado “(...))”, destacando el texto:

“Verifique instantáneamente la edad y la identidad de los visitantes del sitio web con una base de datos completa de documentos de identidad emitidos por el gobierno para ciudadanos de 135 países de todo el mundo. Siempre en cumplimiento con las leyes y las pautas de verificación de edad aceptadas a nivel internacional, con información en tiempo real. Con una base de datos que abarca más de 3400 millones de ciudadanos en todo el mundo”.
- Política de privacidad del servicio prestado por *****EMPRESA.2 (...)**, destacando:

“Para operar los servicios mantenemos bases de datos internas (y tenemos acceso a bases de datos proporcionadas por gobiernos y otros terceros) que contienen información personal, como nombres, direcciones, números de teléfono, fechas de nacimiento y datos de identificación emitidos por el gobierno, direcciones IP, datos de redes sociales, así como detalles relevantes para los requisitos de Conozca a su cliente (“KYC”), como listas de vigilancia financiera y datos de personas políticamente expuestas. Durante el uso de nuestros servicios, las personas relevantes (o nuestros clientes, con el consentimiento de dichas personas o sus padres, tutores u otros representantes legales apropiados) nos brindan información similar (a través de conexión de datos, correo electrónico, videoconferencia u otros medios) para verificar la edad o identidad de las personas relevantes, para validar de otro modo a las personas para el cumplimiento legal, financiero y antifraude de los servicios con restricción de edad, o para otros fines KYC.

El uso de nuestros Servicios de Integridad requiere el consentimiento de (i) la persona cuya información personal se está procesando o (ii) el padre, tutor u otro representante legal apropiado de esa persona”.

- En relación con la retención de datos de geolocalización, se afirma:
“Los datos de geolocalización retenidos por Yoti y derivados de la dirección IP se limitan al código de país y la provincia de cada usuario individual. Esta información se obtiene antes de completar cualquier verificación de edad; por lo tanto, en esta etapa Yoti no puede distinguir si el usuario en particular es menor o no. El período de retención de los datos de geolocalización es actualmente de 5 años”.
- Se aporta documento con el análisis del impacto, la precisión y los sesgos del algoritmo implantado por YOTI para realizar la estimación facial de la edad. El documento está redactado en lengua inglesa y con fecha de creación julio de 2019, de su análisis se extraen las siguientes afirmaciones relevantes (traducción no oficial):

“Yoti proporcionó un conjunto de datos de muestra de 4372 registros, los datos se etiquetaron manualmente por tono de piel en las 6 categorías de Fitzpatrick, género (masculino y mujer) y edad. Las tendencias en el sesgo muestran un sesgo contra la piel más oscura de sujetos y, en particular, para las mujeres, que es más pronunciada en el rango de edad más avanzada. Sin embargo, es menos probable que el error en las personas mayores tenga un alto impacto en la mayoría de los casos de uso actuales ya que el interés regulatorio se centra actualmente en las edades más jóvenes. Una razón clave para tal sesgo es la infrarrepresentación de estos grupos, Yoti lo reconoce y asume abordarlo aumentando la demografía clave en el conjunto de datos. El algoritmo en sí mismo o el conjunto de datos puede no ser el único responsable de los diferenciales, también la tecnología de la cámara requiere una mejor calibración para tonos de piel negro. Yoti afirma que no hay un sesgo significativo por tipo de piel para edades clave comprendidas entre 13-30 años, y los datos respaldan esta afirmación. Sin embargo, dependiendo del caso de uso y el tipo de métrica utilizada, pueden existir algunos sesgos para mujeres con tonos de piel de los tipos IV, V y VI. Yoti ha implantado estrategias para mitigar los sesgos, particularmente la aplicación de colchones de confianza”.

“Los datos utilizados para el modelo estimación facial de la edad (18 de marzo de 2019) se obtuvieron a partir de usuarios de la App de Yoti, conservándose datos biométricos con fines de investigación, específicamente fotografía y año de nacimiento. Los usuarios son conscientes de esto al crear su cuenta ya que se proporcionan detalles completos en la Política de Privacidad”.

“Para abordar la escasa representación de los tonos de piel más oscuros, que probablemente influyó en la menor precisión para estos grupos, Yoti llevó a cabo una actividad de recopilación de datos en Nairobi. Se recopilaron datos de forma presencial en sitios públicos en lugar hacerlo mediante recopilación on line. Las fotografías se recogieron utilizando una cámara portátil, con personas recolectoras capacitadas que brindaban explicaciones claras de cómo se utilizarían los datos, los participantes firmaron un acuerdo de privacidad y fueron incentivados con créditos gratuitos para sus teléfonos móviles. Los

datos se cifraron y se cargaron en el centro de datos seguro de Yoti al final de cada día de trabajo de campo. El ejercicio recopiló datos de 5138 sujetos únicos (57% hombres y 43% mujeres). A pesar de la adición del conjunto de datos, Yoti afirma que todavía existe una mayor tasa de MAE (Mean Absolute Error) para la piel con tono Tipo V y VI, particularmente con mujeres”.

“El análisis de los datos mostró que los individuos que figuraban con mucho maquillaje tenían más probabilidades de ser estimados incorrectamente (con 5 años o más). En general, el maquillaje excesivo estima que las personas parecen más jóvenes de lo que son, aunque no de modo significativo. Si bien en esencia esto no se considera un factor significativo, sería conveniente advertir a los usuarios que el maquillaje excesivo puede aumentar las posibilidades de estimación de edad incorrecta. Por otro lado, las barbas también pueden dar lugar a estimaciones incorrectas, y los jóvenes individuos con barba (o maquillaje similar a la barba) parecen mayores”.

El documento finaliza con las siguientes conclusiones:

“Hay un sesgo dentro del conjunto de datos debido a la infrarrepresentación de datos demográficos clave, en particular mujeres de grupos de edad más avanzada y grupos de piel más oscuros. Este sesgo también es evidente en los resultados del algoritmo con las mujeres de tipo VI de tono de piel, siendo el grupo que experimenta más sesgo. Yoti lo reconoce y ha empleado estrategias de mitigación aplicando colchones de confianza en el umbral de edad clave utilizado. A pesar del sesgo inherente, el sistema Yoti Age Scan ofrecería una ventaja significativa para filtrar usuarios que son significativamente mayores que el mínimo requerido edad”.

Para finalizar investigación, se ha instalado la App de Yoti en un terminal de prueba y se ha registrado un nuevo usuario para tener conocimiento de su funcionamiento real, creando varios videos como resultado de las pruebas. Se crea un primer video-diligencia que muestra el primer acceso a la aplicación (se guarda en objetos asociados con nombre “Video App YOTI_Descarga y primer acceso.mov”), destacando:

- En la primera pantalla, antes de introducir ningún dato personal, se proporciona un texto informando al usuario que todos los datos a proporcionar se van a cifrar con una clave privada, incluyéndose un enlace a la Política de Privacidad junto a un botón con el texto “Entendido”. Se constata que la App permite pulsar el botón (y continuar con el registro en la App) sin comprobar si el usuario ha pinchado y accedido al enlace con la política de privacidad.
- Se diligencia y analiza la Política de Privacidad del punto anterior (objeto asociado con nombre “Política de Privacidad de YOTI registro en App.pdf”), obteniéndose los siguientes puntos de interés (se subraya parte relevante):

“Para creación y gestión de la cuenta de usuario YOTI trata los siguientes tipos de datos:

-Número de teléfono móvil.

-Foto del usuario que se vincula a la cuenta.

-Foto del usuario para realizar determinadas acciones en la App.
-Plantilla de datos biométricos que almacenan de forma segura.
Se utiliza para comprobar que determinadas acciones realizadas en la App son realizadas por el usuario real que creó la cuenta, por ejemplo cuando el usuario quiere cambiar el PIN de la cuenta, compartir datos de su cuenta o eliminar su cuenta (se vuelve a solicitar nueva foto o video en ese instante para comparar “automáticamente” con la plantilla almacenada). Se conserva esta información hasta que se cierra la cuenta.
-Documentos identificativos oficiales, se extrae la foto y la fecha de nacimiento. Se verifica que el documento no está caducado. La foto se utiliza para contrastarla con la tomada cuando se configuró la cuenta para comprobar que se trata de su documento real. Cuando identifican documentos fraudulentos se pueden mantener por un plazo de hasta dos años y lo utilizan para entrenar el software a fin de que detecte mejor los documentos falsos. La imagen del documento también se almacena.
-Dirección de correo electrónico y dirección física. La primera se verifica enviando código, para la segunda se da opción al usuario de verificarla con un tercero, si no se verifica o la verificación falla se marca como no verificada, informando que aun así el usuario puede compartirla, pero informando que algunas organizaciones solo aceptan direcciones verificadas.
-Edad estimada por YOTI: se da la opción al usuario de utilizar la tecnología de YOTI para calcular la edad a través de la App. La tecnología de YOTI calcula al instante si es mayor de 18 años con el mapa digital del rostro creado cuando se creó la cuenta. Al considerar los errores de cálculo y por seguridad de los usuarios, se debe lucir al menos siete años mayor que el umbral de 18. Si YOTI calcula que el usuario es mayor de 28 años se agrega a la cuenta una edad calculada de mayor de 21”.

En relación con la ubicación de los datos se informa de lo siguiente:

“La información que proporcione se almacena por separado y se cifra. Mantenemos toda la información personal que agregue a su cuenta en centros de datos altamente seguros del Reino Unido. Contamos con un centro en India para realizar todas las comprobaciones para la prevención de fraudes cuando configura su cuenta de la App, la información no sale del centro de Reino Unido y el acceso es remoto para cumplir su función. Tenemos en vigor cláusulas contractuales del modelo aprobado por la UE entre YOTI Reino Unido y YOTI India”.

Otra información relevante que destacar de la Política de Privacidad:

“El objetivo de nuestro uso de datos biométricos para identificarlo o autenticarlo es evitar el uso fraudulento de la App y proteger sus datos. Son parte clave para garantizar el bloqueo

de documentos falsos y garantizar que es el usuario real es que está actuando en la App”.

“¿Qué datos biométricos utiliza la App y por qué?

Cuando configura su cuenta escaneamos el rostro para crear plantilla biométrica que almacenamos de forma segura. Cuando realiza determinadas acciones en la App le pediremos que se tome una foto o grabe un video y lo comparamos con la plantilla para comprobar que coincide, comprobando que la imagen sea de una persona real. Estas comprobaciones garantizan que solo el usuario pueda realizar las acciones. Cuando agrega un documento comparamos su foto con la plantilla de rostro para asegurarnos de que los usuarios solo carguen sus propios documentos.

En relación con el uso de datos para I+D la Política de Privacidad afirma:

“También usamos algunos datos de usuarios en nuestra investigación y desarrollo internos (I+D), lo que podría incluir sus datos biométricos. Puede excluirse de esto en la configuración de la App, lo que le permitirá seguir usando la App”.

“Para probar y mejorar nuestra tecnología de cálculo de edad, I&D necesita imágenes de rostros y la edad verificada de ese rostro. Por lo tanto, usan fotos que toman en la app e imágenes fijas del video. Para la edad verificada, utilizan el mes y año de nacimiento de un documento de identidad que agregue y que contenga esta información. También se obtiene su género si aparece en el documento de identidad. Esto se utiliza para evitar el sesgo, según se describe a continuación”.

“Actualmente usamos tecnología de terceros para realizar una corroboración facial entre las fotos que usted toma con la foto de su documento de identidad a fin de asegurar que solo cargue sus propios documentos. Estamos desarrollando nuestra propia tecnología para realizar esta corroboración facial, la que también estará disponible para otras organizaciones. Para desarrollar, probar y mejorar esta tecnología, el equipo de I&D necesita tanto las fotos que se toma en la app como una imagen de alta calidad recortada de su documento de identidad. No tienen ninguna otra información de usted”.

“I&D sigue las buenas prácticas de investigación aceptadas y etiqueta algunos datos de las imágenes con información sobre género, tono de piel u otros rasgos. El hecho de contar con estas etiquetas garantiza que los datos de nuestra investigación sean equilibrados y representativos”.

“En la configuración de la app puede excluirse de permitir que se utilicen sus datos para fines de I&D. Esto le permitirá seguir usando la app, lo que incluye las características esenciales de seguridad de datos biométricos. Excluirse significa que sus datos ya no se enviarán a I&D, y que se eliminarán todos los datos que ya tengamos disponibles para uso por parte de I&D. Considere que si sus datos ya se utilizaron para capacitación o para desarrollar un modelo o algoritmo de aprendizaje automático, no es posible extraer sus datos de ese modelo”.

En relación con la revocación del consentimiento para el uso de datos biométricos se afirma:

“Esperamos que comprenda los motivos por los que los datos biométricos son una parte esencial de seguridad de nuestra app, pero si cambia de opinión puede revocar su consentimiento en cualquier momento mediante la eliminación de su cuenta en la configuración de la app. No existe una versión sin datos biométricos de la app, así que sin esa información la app no funciona”.

- Al pasar pantalla de la Política de Privacidad se muestra segunda pantalla con el texto “Confirmar tu Edad” en la que se aprecia que la propia App ha detectado que el usuario se encuentra en España y ofrece dos alternativas distintas “Tengo 14 o más” o “Tengo 13 o menos”, permitiendo continuar únicamente si se pulsa el botón declarando tener más de 14 años. La pantalla también incluye el texto:

“Necesitamos tu consentimiento para utilizar escaneo facial...el escaneo facial es el único dato biométrico que utilizamos. La utilizamos para proteger tu cuenta, así como para asegurarnos de que eres tú quien está usando la App y que cualquier documento de identidad añadido te pertenece... No puedes utilizar la App sin proporcionar tus datos biométricos, ya que es el método que nos permite protegerte. Si deseas retirar tu consentimiento más adelante, puedes hacerlo en cualquier momento en Mis Datos y Permisos”.

Al pulsar el botón declarando ser mayor de 14 años se muestra una nueva pantalla con el título “Necesitamos tu consentimiento”, incluyendo el siguiente texto junto un botón con el título “Entiendo y doy mi consentimiento”:

“Utilizamos escaneo facial para asegurarnos de que eres tú quien está usando la App y que cualquier documento que agregues te pertenece... No puedes utilizar la App sin escanear tu rostro, ya que es el método que nos permite protegerte”.

Una vez pulsado botón de consentimiento, la App recaba la imagen facial del usuario a través de la cámara del dispositivo móvil.

- En el siguiente paso se muestra nueva pantalla con el texto informativo “Cómo utilizamos tus datos”, incluyendo información sobre el uso de datos para análisis y el uso de datos para investigación interna, destacando:

“Extraemos algunos datos para ayudar a probar y mejorar nuestra tecnología y hacerla más segura, los datos usados incluyen una copia separada de tu foto tomada cuando realizamos el escaneo facial, y el mes y año de nacimiento, sexo y tipo de documento obtenido al incorporar documento de identidad. Puedes elegir no participar en Mis Datos Personales. Solo para uso interno, estos datos están cifrados por lo que nadie puede identificarte”.

La App no ofrece ninguna opción para oponerse a este tratamiento, únicamente informa que puede revocarlo posteriormente a través de la configuración de la App.

- En la pantalla siguiente se muestra texto “*Términos y Condiciones. Al pulsar Aceptar y Continuar aceptas los Términos y Condiciones de Yoti*”, incluyendo enlace a la página web con los términos y condiciones redactados, junto a un botón para aceptarlas (se diligencia como objeto asociado “*Términos y Condiciones App YOTI.pdf*”). La APP permite avanzar de pantalla sin comprobar si el usuario ha pinchado sobre el enlace para acceder al contenido. Se analiza el texto con los “*Términos y Condiciones*” y se destacan los siguientes apartados relevantes:

“Al registrarse para obtener una cuenta o al agregar sus primeros documentos de identidad, le pediremos que complete una breve prueba para demostrar que se trata de una persona viva real. Esta prueba podría incluir, entre otras opciones, repetir algunas palabras en un video grabado o podríamos pedirle que mueva su teléfono siguiendo su rostro para capturar varias imágenes (verá las instrucciones de este proceso en ese momento). Si le pedimos que use el método del video, el video grabado se cargará en nuestro servidor y, a menos que se nos exija conservarlo por motivos reglamentarios, lo eliminaremos permanentemente dentro de 30 días desde la fecha de su grabación. Si le pedimos que utilice otro método, la información se procesará automáticamente en su teléfono y recibirá una aprobación o rechazo al instante”.

“Yoti almacenará una plantilla de datos biométricos de su rostro, tomada a partir del escaneo facial capturado durante la prueba de vida que completó en el registro, a fin de comprobar que siempre es usted quien intenta acceder a su cuenta de Yoti”.

“Después de ingresar y comprobar la información, esta se cifrará de manera independiente y Yoti no podrá verla ni acceder a ella. Solo usted contará con las claves de cifrado (números imprevisibles y únicos que se utilizan para descifrar la información), almacenadas en su teléfono móvil u otros dispositivos, de modo que solo usted pueda acceder a su cuenta. Es su responsabilidad mantener su teléfono móvil y otros dispositivos seguros, y evitar que otras personas tengan acceso no autorizado a ellos.

Una vez que su cuenta esté cerrada, eliminaremos de nuestro servidor todos los atributos de identificación, todos los datos biométricos que utilizó y otros atributos (como el correo electrónico)”.

“La empresa Yoti con la que celebra este contrato aplica la legislación a estos términos y tribunales que juzgarán cualquier controversia dependiendo del lugar donde usted viva:

-Si vive en la India, usted celebra el contrato con Yoti Biometric Identity Private Ltd.....

-Si vive en los Estados Unidos, usted celebra el contrato con Yoti USA Inc.....

-Si vive en cualquier otro lugar del mundo, usted celebra un contrato con Yoti Limited, una empresa registrada en Inglaterra con el número 08998951 y cuya dirección es Fountain House, 5th Floor, 130 Fenchurch St, London, EC3M 5DJ. Sujeto a cualquier requisito obligatorio de su legislación local que anule este párrafo, la legislación inglesa aplica a cualquier controversia o reclamación que surja de estos términos y condiciones o de su uso de nuestros Productos (sea esta contractual o no contractual) y ambos podemos presentar las acciones judiciales ante los tribunales ingleses”.

- La siguiente pantalla muestra el texto “*Proteger tu Cuenta*”, requiriendo al usuario introducir obligatoriamente un número de teléfono móvil al que envían clave OTP para su verificación, posteriormente solicitan crear un PIN para acceso futuro a la cuenta de YOTI.

Una vez realizado el primer acceso en la App, se crea un segundo video-diligencia mostrando las distintas opciones internas de esta App haciendo uso del usuario registrado (objeto asociado con nombre “*Uso interno de la App YOTI.mp4*”), destacando:

- Existe un apartado para cumplimentar datos personales que permite realizar al usuario las acciones:
 - o *Agregar una foto*: se afirma que por seguridad se verifica que la foto coincida con el escaneo facial introducido en el registro inicial de la App.
 - o *Agregar Nombre Completo*: para ello obliga introducir un documento identificativo que lo contenga (en caso de no haberlo realizado aún), permitiendo como opciones: pasaporte, documento de identidad y licencia de conducir.
 - o *Agregar Fecha de Nacimiento*: igual que en apartado anterior, obliga a introducir documento identificativo que la contenga.
 - o *Agregar Dirección*: igual que en apartado anterior, obliga a introducir un documento identificativo.
 - o *Agregar Correo Electrónico*: valida la dirección introducida enviando un código de verificación.
 - o *Agregar Género*: obliga a introducir documento identificativo que lo contenga.
 - o *Agregar Nacionalidad*: obliga a introducir documento identificativo que la contenga.
 - o *Calcular Edad de YOTI*: permite al usuario obtener una edad estimada a través de la tecnología de YOTI que será almacenada en su App para

que el usuario pueda compartirla. Muestra el siguiente texto al entrar en esta opción (se subraya parte relevante),

“Nuestra tecnología calcula al instante si eres mayor de 18 ,19 o 21 años a través del mapa digital de tu rostro que capturamos cuando creaste tu usuario YOTI. Al considerar los errores de cálculo y por seguridad de nuestros usuarios, debes lucir al menos siete años mayor que 18 para obtener una edad calculada, ya que mayor de 18 es la edad calculada mínima que ofrecemos. Entonces, al considerar los errores de cálculo y por la seguridad de nuestros usuarios, debes lucir mayor de 25 para que te podamos ofrecer la edad calculada. Algunas empresas aceptarán una edad calculada como prueba de edad para acceder a bienes o servicios con restricción de edad. Enviamos una copia del mapa digital de tu rostro desde tu YOTI a nuestros servidores. Lo usamos para calcular tu edad y luego lo eliminamos. Puedes quitar tu edad calculada al reemplazarla con un documento de identidad que incluya tu fecha de nacimiento”.

Tras ejecutarse la opción se devuelve resultado al usuario en pocos segundos y muestra el texto: *“Tu edad calculada es Mayor de 21. Algunas empresas aceptarán esto como prueba de edad para bienes y servicios de restricción de edad. Recuerda, esto es solo un cálculo aproximado. Hemos agregado tu edad calculada a tu YOTI, puedes encontrarla en datos personales.*

Se crea un tercer y último video-diligencia con las opciones de configuración que se ofrecen al usuario dentro de la App haciendo uso del usuario registrado (“Opciones Configuración App YOTI.mp4”), todas las opciones se encuentran en el menú de la App “Mis Datos y Permisos”:

- Existe opción que permite al usuario descargar todos sus datos en fichero formato ZIP.
- Existe opción con título “Seguridad de los Datos” mostrando información al usuario:
 - o *Toda la información personal se cifra con AES de 256 bits.*
 - o *Las claves privadas que desbloquean los datos se almacenan en el dispositivo y nadie puede acceder a ellas, ni siquiera YOTI.*
 - o *Se usan centros de datos de nivel 3 del Reino Unido para almacenar los datos personales y realizar copias de seguridad periódicas para garantizar que no se pierdan los datos y se someten a pruebas de penetración periódicas.*
- Existe opción de configuración con título “Consentimiento de datos biométricos” donde se muestra el texto: *“Autorizaste a YOTI para usar tu escaneo facial de las siguientes formas: Enlace a la Política de Privacidad”.* Por otro lado, muestra una casilla declarativa activada por defecto a través de la cual el usuario puede oponerse al tratamiento de sus datos biométricos para fines de investigación interna.
- Existe una última opción que permite al usuario oponerse al tratamiento de sus datos con *finde análisis*, existe casilla declarativa activada por defecto y mostrando el siguiente texto:

“necesitamos saber qué funciona y qué no, cuántas personas usan nuestra app, en qué lugar del mundo están y qué productos o características son más populares. Recopilamos información sobre tu dispositivo y tu uso de la app mediante análisis internos y de terceros. Despersonalizamos la información para que no sea posible identificarte personalmente... No creamos perfiles de las personas, simplemente buscamos tendencias y patrones para informar las decisiones empresariales. Si no deseas compartirnos datos de análisis puedes desactivar la función. Cierta información se comparte automáticamente cuando usas nuestros productos y no podemos desactivarla”.

CUARTO: Con fecha 5 de junio de 2025, la Presidencia de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción del artículo 5.1.e), del artículo 6, del artículo 7 del RGPD y del artículo 9, todos del RGPD, tipificadas en el artículo 83.5 a) del RGPD.

QUINTO: Notificado el citado acuerdo de inicio conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP) y transcurrido el plazo otorgado para la formulación de alegaciones, se ha constatado que no se ha recibido alegación alguna por la parte reclamada.

El artículo 64.2.f) de la LPACAP -disposición de la que se informó a la parte reclamada en el acuerdo de apertura del procedimiento- establece que si no se efectúan alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, cuando éste contenga un pronunciamiento preciso acerca de la responsabilidad imputada, podrá ser considerado propuesta de resolución. En el presente caso, el acuerdo de inicio del expediente sancionador determinaba los hechos en los que se concretaba la imputación, la infracción del RGPD atribuida a la reclamada y la sanción que podría imponerse. Por ello, tomando en consideración que la parte reclamada no ha formulado alegaciones al acuerdo de inicio del expediente y en atención a lo establecido en el artículo 64.2.f) de la LPACAP, el citado acuerdo de inicio es considerado en el presente caso propuesta de resolución.

SEXTO: De acuerdo con la información de que se dispone, YOTI es una empresa constituida en el año 2014, y con un volumen de negocios de 15.029.907 euros según los datos publicados en marzo de 2025.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

PRIMERO: YOTI es un proveedor de servicios de verificación de la edad que proporciona en España los siguientes servicios de verificación de la edad en régimen de *software como servicio* (“SaaS”) mediante: teléfono móvil; chequeo contra bases de

datos; estimación de edad; documento identificativo; tarjeta de crédito. En estos supuestos, son los clientes de YOTI los que tienen la condición de responsables del tratamiento

YOTI también proporciona una App para teléfonos móviles ('App Digital ID') que permite la verificación real dentro de la aplicación. YOTI es el responsable del tratamiento de datos personales que se realiza dentro de esta aplicación.

Todos los servicios de verificación de edad de YOTI están disponibles para su uso en España

SEGUNDO: El centro de datos de YOTI se encuentra en el Reino Unido y, para las transferencias de datos personales desde Reino Unido a la India, YOTI se basa en las cláusulas contractuales estándar de la UE con la adenda del Reino Unido.

TERCERO: Para el tratamiento de los datos personales por parte de YOTI como responsable de tratamiento, manifiestan como base de licitud del tratamiento la ejecución de un contrato, afirmando que *"el tratamiento se hace sobre la base de una solicitud del propio usuario y es parte del servicio Digital ID proporcionado por YOTI según los términos de uso establecidos"*.

CUARTO: De acuerdo con lo afirmado por YOTI, *"La App Digital ID no puede ser utilizada por personas menores de la edad de consentimiento digital, es decir, 13 años en el Reino Unido y 14 años en España. La App Digital ID cuenta con un sistema de control de edad basado en la jurisdicción para garantizar que no se permite que personas que afirman ser menores de la edad de consentimiento digital en esa jurisdicción en particular utilicen dicha aplicación"*.

Del proceso de creación de una cuenta de usuario en la App de YOTI destacan los siguientes aspectos:

- i) En la primera pantalla, y antes de introducir ningún dato personal, se proporciona un texto informando al usuario de que todos los datos a proporcionar se van a cifrar con una clave privada, incluyéndose un enlace a la Política de Privacidad junto a un botón con el texto *"Entendido"*. La App permite pulsar el botón (y continuar con el registro en la App) sin comprobar si el usuario ha pinchado y accedido al enlace con la política de privacidad.
- ii) La segunda pantalla del proceso de configuración de la cuenta en la APP de YOTI contiene el texto *"Confirmar tu Edad"*. La propia APP detecta la ubicación del usuario y, en virtud de ello, para el caso de usuarios radicados en España ofrece dos alternativas distintas *"Tengo 14 o más"* o *"Tengo 13 o menos"*. Sólo puede continuarse con el proceso si se pulsa el botón declarando tener más de 14 años. La pantalla también incluye el texto (el subrayado es de esta AEPD):

"Necesitamos tu consentimiento para utilizar escaneo facial...el escaneo facial es el único dato biométrico que utilizamos. La utilizamos para proteger tu cuenta, así como para asegurarnos de que eres tú quien está usando la App y que cualquier documento de identidad añadido te pertenece... No

puedes utilizar la App sin proporcionar tus datos biométricos, ya que es el método que nos permite protegerte. Si deseas retirar tu consentimiento más adelante, puedes hacerlo en cualquier momento en Mis Datos y Permisos".

- iii) Posteriormente, se muestra una nueva pantalla con el título "Necesitamos tu consentimiento. El consentimiento se recaba tras pulsar el botón declarando ser mayor de 14 años. Se incluye el siguiente texto junto un botón con el título "Entiendo y doy mi consentimiento" (el subrayado es de esta AEPD):

"Utilizamos escaneo facial para asegurarnos de que eres tú quien está usando la App y que cualquier documento que agregues te pertenece... No puedes utilizar la App sin escanear tu rostro, ya que es el método que nos permite protegerte".

Una vez pulsado botón de consentimiento, la App recaba la imagen facial del usuario a través de la cámara del dispositivo móvil.

QUINTO: Según YOTI "La estimación de la edad a través de reconocimiento facial no utiliza categorías especiales de datos debido a que el procesamiento no tiene el propósito de identificar o autenticar a un individuo". En relación con el consentimiento informado para el tratamiento de datos biométricos afirman: "Al incorporarse los usuarios a través de la App Digital ID deben dar su consentimiento para usar la aplicación, ya que dicha aplicación implica el tratamiento de datos biométricos.

En la política de privacidad de YOTI a la que se tiene acceso en la App digital se indica lo siguiente (el subrayado es de esta AEPD):

"Para creación y gestión de la cuenta de usuario YOTI trata los siguientes tipos de datos:

-Número de teléfono móvil.

-Foto del usuario que se vincula a la cuenta.

-Foto del usuario para realizar determinadas acciones en la App.

-Plantilla de datos biométricos que almacenan de forma segura. Se utiliza para comprobar que determinadas acciones realizadas en la App son realizadas por el usuario real que creó la cuenta, por ejemplo cuando el usuario quiere cambiar el PIN de la cuenta, compartir datos de su cuenta o eliminar su cuenta (se vuelve a solicitar nueva foto o video en ese instante para comparar "automáticamente" con la plantilla almacenada). Se conserva esta información hasta que se cierra la cuenta.

-Documentos identificativos oficiales, se extrae la foto y la fecha de nacimiento. Se verifica que el documento no está caducado. La foto se utiliza para contrastarla con la tomada cuando se configuró la cuenta para comprobar que se trata de su documento real. Cuando identifican documentos fraudulentos se pueden mantener por un plazo de hasta dos años y lo utilizan para entrenar el software a fin de que detecte mejor los documentos falsos. La imagen del documento también se almacena.

-Dirección de correo electrónico y dirección física. La primera se verifica enviando código, para la segunda se da opción al usuario de verificarla con un

tercero, si no se verifica o la verificación falla se marca como no verificada, informando que aun así el usuario puede compartirla, pero informando que algunas organizaciones solo aceptan direcciones verificadas.

-Edad estimada por YOTI: se da la opción al usuario de utilizar la tecnología de YOTI para calcular la edad a través de la App. La tecnología de YOTI calcula al instante si es mayor de 18 años con el mapa digital del rostro creado cuando se creó la cuenta. Al considerar los errores de cálculo y por seguridad de los usuarios, se debe lucir al menos siete años mayor que el umbral de 18. Si YOTI calcula que el usuario es mayor de 28 años se agrega a la cuenta una edad calculada de mayor de 21”.

Respecto del tratamiento de datos biométricos, la Política de Privacidad señala lo siguiente: *“El objetivo de nuestro uso de datos biométricos para identificarlo o autenticarlo es evitar el uso fraudulento de la App y proteger sus datos. Son parte clave para garantizar el bloqueo de documentos falsos y garantizar que es el usuario real es que está actuando en la App”.* *“¿Qué datos biométricos utiliza la App y por qué?”*

Cuando configura su cuenta escaneamos el rostro para crear plantilla biométrica que almacenamos de forma segura. Cuando realiza determinadas acciones en la App le pediremos que se tome una foto o grabe un video y lo comparamos con la plantilla para comprobar que coincide, comprobando que la imagen sea de una persona real. Estas comprobaciones garantizan que solo el usuario pueda realizar las acciones. Cuando agrega un documento comparamos su foto con la plantilla de rostro para asegurarnos de que los usuarios solo carguen sus propios documentos.

Asimismo, YOTI utiliza datos biométricos de usuarios para finalidades de investigación y desarrollo (I+D), tal y como consta en el documento sobre la evaluación de impacto de los tratamientos de datos en la App para la finalidad I+D en su tecnología de estimación facial.

En relación con la revocación del consentimiento para el uso de datos biométricos, en la política de privacidad de la App se afirma:

“Esperamos que comprenda los motivos por los que los datos biométricos son una parte esencial de seguridad de nuestra app, pero si cambia de opinión puede revocar su consentimiento en cualquier momento mediante la eliminación de su cuenta en la configuración de la app. No existe una versión sin datos biométricos de la app, así que sin esa información la app no funciona”.

En el texto “*Términos y Condiciones*. Al pulsar Aceptar y Continuar aceptas los *Términos y Condiciones de Yoti*”, accesible en el proceso de configuración de la cuenta de usuario, destaca lo siguiente:

“Yoti almacenará una plantilla de datos biométricos de su rostro, tomada a partir del escaneo facial capturado durante la prueba de vida que completó en el registro, a fin de comprobar que siempre es usted quien intenta acceder a su cuenta de Yoti”.

YOTI no considera que los datos personales utilizados para mejorar su tecnología sean datos biométricos de categoría especial en sentido RGPD, ya que no se utilizan para identificar de manera única a las personas.

SEXTO: Entre las opciones que se encuentran en el menú de la App “Mis Datos y Permisos” se encuentra una opción de configuración con título “Consentimiento de datos biométricos” donde se muestra el texto: “Autorizaste a YOTI para usar tu escaneo facial de las siguientes formas: *Enlace a la Política de Privacidad*”. En la misma se encuentra una casilla declarativa activada por defecto a través de la cual el usuario puede oponerse al tratamiento de sus datos biométricos para fines de investigación interna.

Existe también una opción que permite al usuario oponerse al tratamiento de sus datos con *finés de análisis*, pero en la que figura una casilla declarativa activada por defecto y en la que se indica el siguiente texto:

“necesitamos saber qué funciona y qué no, cuántas personas usan nuestra app, en qué lugar del mundo están y qué productos o características son más populares. Recopilamos información sobre tu dispositivo y tu uso de la app mediante análisis internos y de terceros. Despersonalizamos la información para que no sea posible identificarte personalmente...No creamos perfiles de las personas, simplemente buscamos tendencias y patrones para informar las decisiones empresariales. Si no deseas compartirnos datos de análisis puedes desactivar la función. Cierta información se comparte automáticamente cuando usas nuestros productos y no podemos desactivarla”.

SÉPTIMO: En relación con la conservación de los datos por YOTI:

“Cuando YOTI actúa como responsable conserva los datos de la cuenta mientras el usuario tenga una cuenta con Yoti y durante los próximos tres años de inactividad de dicho usuario. Los usuarios pueden eliminar estos datos, o su cuenta, en cualquier momento y los datos son borrados automáticamente al caducar los 3 años de inactividad. (...)”.

“Cuando los usuarios realizan el proceso de onboarding en la App Digital ID, pueden optar por agregar un documento de identidad. Si no es posible realizar una verificación automatizada de dicho documento, el documento de identidad, junto con la imagen ‘selfie’ se envía al centro de seguridad de Yoti a través del sistema interno de Yoti para una revisión manual por parte de nuestros especialistas en verificación de identidad. Como se ha indicado, esta revisión manual sólo se produce en el caso de que no sea posible una verificación automatizada, por ejemplo, mediante el chip NFC del documento de identidad. Si hay una verificación manual, los especialistas de Yoti revisarán el documento para asegurarse de que sea genuino y también compararán la foto del documento de identidad con la imagen ‘selfie’, para asegurarse de que sean la misma persona. Estos datos son visibles para los empleados individuales de Yoti en el centro de seguridad durante 28 días, después de lo cual se eliminan del sistema de administración”.

De acuerdo con la EIPD proporcionada por YOTI *Para el token de edad y los datos de la Digital ID App, la retención queda establecida mientras el usuario mantiene activa la cuenta o después de tres años de inactividad.*

En relación con los periodos de retención de los datos, la EIPD de YOTI señala lo siguiente:

“Para los Servicios de Verificación de Edad no se retienen datos por parte de YOTI. En el caso de subida de documento identificativo y cuando el cliente habilita la verificación manual, se almacena durante 28 días. En la Estimación Facial de la Edad, la fotografía es borrada tras obtener el resultado. Para el token de edad y los datos de la Digital ID App, la retención queda establecida mientras el usuario mantiene activa la cuenta o después de tres años de inactividad”.

Por otra parte, en relación con la retención de datos de geolocalización:

“Los datos de geolocalización retenidos por Yoti y derivados de la dirección IP se limitan al código de país y la provincia de cada usuario individual. Esta información se obtiene antes de completar cualquier verificación de edad; por lo tanto, en esta etapa Yoti no puede distinguir si el usuario en particular es menor o no. El período de retención de los datos de geolocalización es actualmente de 5 años”.

En el proceso de configuración de la cuenta de usuario, en relación con el texto “*Términos y Condiciones. Al pulsar Aceptar y Continuar aceptas los Términos y Condiciones de Yoti*”, destaca lo siguiente:

“Al registrarse para obtener una cuenta o al agregar sus primeros documentos de identidad, le pediremos que complete una breve prueba para demostrar que se trata de una persona viva real. Esta prueba podría incluir, entre otras opciones, repetir algunas palabras en un video grabado o podríamos pedirle que mueva su teléfono siguiendo su rostro para capturar varias imágenes (verá las instrucciones de este proceso en ese momento). Si le pedimos que use el método del video, el video grabado se cargará en nuestro servidor y, a menos que se nos exija conservarlo por motivos reglamentarios, lo eliminaremos permanentemente dentro de 30 días desde la fecha de su grabación. Si le pedimos que utilice otro método, la información se procesará automáticamente en su teléfono y recibirá una aprobación o rechazo al instante”.

“Yoti almacenará una plantilla de datos biométricos de su rostro, tomada a partir del escaneo facial capturado durante la prueba de vida que completó en el registro, a fin de comprobar que siempre es usted quien intenta acceder a su cuenta de Yoti”.

“Después de ingresar y comprobar la información, esta se cifrará de manera independiente y Yoti no podrá verla ni acceder a ella. Solo usted contará con las claves de cifrado (números imprevisibles y únicos que se utilizan para descifrar la información), almacenadas en su teléfono móvil u otros dispositivos, de modo que solo usted pueda acceder a su cuenta. Es su responsabilidad mantener su

teléfono móvil y otros dispositivos seguros, y evitar que otras personas tengan acceso no autorizado a ellos.

Una vez que su cuenta esté cerrada, eliminaremos de nuestro servidor todos los atributos de identificación, todos los datos biométricos que utilizó y otros atributos (como el correo electrónico)".

FUNDAMENTOS DE DERECHO

I

Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para resolver este procedimiento la Presidencia de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II

Cuestiones previas

El artículo 4.1) del RGPD, define «dato personal» como: *"toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona"*.

El artículo 4.2) del RGPD, define «tratamiento» como: *"cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción."*

El artículo 4.7) del RGPD, define al «responsable del tratamiento» o «responsable» como: *"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el*

responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros”.

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 y 4.2 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que YOTI realiza, entre otros tratamientos y a través de su APP digital ID, la recogida y conservación de datos personales de personas físicas tales como su documento nacional identificativo- con datos como nombre y apellidos, fecha de nacimiento y género-, su fotografía o su patrón biométrico facial.

YOTI realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD.

III

Obligación incumplida. Tratamiento de categorías especiales de datos personales

Cabe señalar en un primer momento el sentido en que se pronuncia el RGPD en algunos de sus considerandos (el subrayado es de esta AEPD):

51. Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término «origen racial» en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas. El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de

actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales.

Considerando 89. *La Directiva 95/46/CE estableció la obligación general de notificar el tratamiento de datos personales a las autoridades de control. (...) Por tanto, estas obligaciones generales de notificación indiscriminada deben eliminarse y sustituirse por procedimientos y mecanismos eficaces que se centren, en su lugar, en los tipos de operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas. Estos tipos de operaciones de tratamiento pueden ser, en particular, las que implican el uso de nuevas tecnologías, o son de una nueva clase y el responsable del tratamiento no ha realizado previamente una evaluación de impacto relativa a la protección de datos, o si resultan necesarias visto el tiempo transcurrido desde el tratamiento inicial.*

Considerando 90. *En tales casos, el responsable debe llevar a cabo, antes del tratamiento, una evaluación de impacto relativa a la protección de datos con el fin de valorar la particular gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento.*

Considerando 91. (...) *La evaluación de impacto relativa a la protección de datos debe realizarse también en los casos en los que se tratan datos personales para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basada en la elaboración de perfiles de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas. (...)*

Artículo 4. Definiciones

14) «datos biométricos»: *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, como imágenes faciales o datos dactiloscópicos;*

Por su parte, el artículo 9 del RGPD, que regula el tratamiento de categorías especiales de datos personales, establece lo siguiente (el subrayado es de esta AEPD):

"1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión o de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional;

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud."

De los preceptos anteriores pueden alcanzarse las siguientes conclusiones:

- Los datos de carácter biométrico, tales como los que permiten la identificación unívoca de una persona a través de sus rasgos faciales, son datos de carácter personal, considerados categorías especiales de datos por el RGPD.
- El tratamiento de datos biométricos se considera como de alto riesgo para los derechos y libertades de las personas físicas en la medida en que su tratamiento en general escapa del poder de disposición del interesado y el mismo puede entrañar una mayor afectación a los derechos de éste.
- Un responsable del tratamiento debe valorar si el tratamiento es necesario y proporcional para alcanzar la finalidad querida y si la finalidad del tratamiento puede lograrse razonablemente por otros medios que sean menos intrusivos para los derechos y libertades fundamentales del interesado. Este examen es especialmente importante y debe de realizarse con extremado cuidado cuando el tratamiento de datos personales entraña un alto riesgo.
- El tratamiento de los datos considerados como de categoría especial está, con carácter general, prohibido. Dicho tratamiento sólo será posible si se cumple alguna de las circunstancias previstas en el artículo 9.2 del RGPD para el levantamiento de la prohibición de tratamiento, siempre y cuando el tratamiento sea necesario y proporcional.

Sentado lo anterior, cabe hacer hincapié en que, de acuerdo con el artículo 4.14 del RGPD (en relación con el artículo 4.1 del RGPD) son datos biométricos de carácter personal todos aquellos que: (i) sean relativos a las características físicas, fisiológicas o conductuales de una persona física; (ii) su finalidad sea la de permitir o confirmar la identificación única de una persona física (incluyendo sistemas de autenticación 1:1 e identificación 1:N); (iii) y que se sometan a un tratamiento técnico específico dirigido a permitir o confirmar la identidad unívoca de las personas (que dé lugar a la generación, archivo, explotación y destrucción de plantillas biométricas obtenidas de las muestras del dato capturado en bruto).

Asimismo, siempre que se realice un tratamiento de datos de carácter personal que sean biométricos de acuerdo con la definición del artículo 4.14 del RGPD, estos serán, a su vez (i) datos personales de categoría especial según el artículo 9 RGPD, (ii) y el tratamiento de los mismos podrá ser considerado de “alto riesgo” según el artículo 35 del RGPD.

Teniendo esto en cuenta, los datos biométricos que permitan la identificación unívoca de una persona son considerados categoría especial de datos personales cuyo tratamiento, en aplicación del artículo 9.1 RGPD está prohibido salvo que dicha prohibición sea levantada por la concurrencia de alguna de las circunstancias previstas en el apartado 2 del mismo precepto.

Según se ha señalado, para la creación de la cuenta en YOTI se exige, como primer paso, confirmar la edad y dar consentimiento para un escaneo facial. Así, en el apartado “*Confirmar tu Edad*” se aprecia que la propia App ha detectado que el usuario se encuentra en España y ofrece dos alternativas distintas “*Tengo 14 o más*” o “*Tengo 13 o menos*”, permitiendo continuar únicamente si se pulsa el botón declarando tener más de 14 años. La pantalla también incluye el texto (el subrayado es de esta AEPD):

“Necesitamos tu consentimiento para utilizar escaneo facial...el escaneo facial es el único dato biométrico que utilizamos. La utilizamos para proteger tu cuenta, así como para asegurarnos de que eres tú quien está usando la App y que cualquier documento de identidad añadido te pertenece... No puedes utilizar la App sin proporcionar tus datos biométricos, ya que es el método que nos permite protegerte. Si deseas retirar tu consentimiento más adelante, puedes hacerlo en cualquier momento en Mis Datos y Permisos”.

Al pulsar el botón declarando ser mayor de 14 años se muestra una nueva pantalla con el título “*Necesitamos tu consentimiento*”, incluyendo el siguiente texto junto un botón con el título “*Entiendo y doy mi consentimiento*”:

“Utilizamos escaneo facial para asegurarnos de que eres tú quien está usando la App y que cualquier documento que agregues te pertenece... No puedes utilizar la App sin escanear tu rostro, ya que es el método que nos permite protegerte”.

Una vez pulsado botón de consentimiento, la App recaba la imagen facial del usuario a través de la cámara del dispositivo móvil.

Por otro lado, según informa YOTI (el subrayado es nuestro) en el marco de las actuaciones de investigación desarrolladas, sin que haya aportado ningún dato

adicional una vez iniciado el presente procedimiento sancionador, a cuyo acuerdo de inicio no formuló alegaciones, se realiza un escaneo facial o video para demostrar que el usuario que está creando la cuenta es una persona real. Escaneo o video también toma una imagen fija del usuario a partir de la que, indican, “creamos una plantilla de datos biométricos que almacenamos de forma segura. Esta plantilla es un mapa digital de su rostro. Siempre que realice determinadas acciones en el futuro y necesitemos comprobar que se trata realmente de usted, le pediremos que repita el video o que tome una foto y compare la imagen con el mapa digital. Cuando agrega un documento, restablece su PIN o necesita recuperar su cuenta (por ejemplo, si pierde su teléfono) realizamos el escaneo de su rostro y el video como una medida de seguridad adicional para verificar que siempre se trata de usted intentando realizar esas acciones. Comparamos automáticamente el escaneo facial con el que realizó cuando configuró su cuenta. Si le pedimos que diga algunas palabras, nuestro Centro de seguridad también revisa el video. (...). Si desea eliminar su cuenta, le pedimos que tome una foto. La comparamos automáticamente con el escaneo facial que realizó cuando configuró su cuenta. Los escaneos y el video nos ayudan a garantizar que usted es una persona viva real y evitan que otra persona con acceso a su teléfono realice las acciones antes mencionadas. Eliminamos el video después de 14 días. Es posible que usemos algunos videos dentro del plazo de 14 días para pruebas internas con el objetivo de mejorar nuestras comprobaciones de seguridad. Utilizamos algunas secciones del video para investigación y desarrollo internos con el fin de mejorar nuestras medidas de prevención del fraude. Consulte la sección sobre datos biométricos para obtener más información acerca del escaneo facial, la plantilla de datos biométricos y el trabajo de investigación. Detección de sonido: cuando le pedimos que diga algunas palabras durante el video recopilamos el modelo de dispositivo, el idioma y los niveles de sonido. (...) Las fotos que toma y su plantilla de datos biométricos: conservamos esta información hasta que usted o nosotros cerremos la cuenta y eliminemos la información.

Por otro lado, según consta en el expediente, la política de privacidad de YOTI (APP digital) indica lo siguiente (el subrayado es de esta AEPD):

“Para creación y gestión de la cuenta de usuario YOTI trata los siguientes tipos de datos:

- Número de teléfono móvil.
- Foto del usuario que se vincula a la cuenta.
- Foto del usuario para realizar determinadas acciones en la App.
- Plantilla de datos biométricos que almacenan de forma segura. Se utiliza para comprobar que determinadas acciones realizadas en la App son realizadas por el usuario real que creó la cuenta, por ejemplo cuando el usuario quiere cambiar el PIN de la cuenta, compartir datos de su cuenta o eliminar su cuenta (se vuelve a solicitar nueva foto o video en ese instante para comparar “automáticamente” con la plantilla almacenada). Se conserva esta información hasta que se cierra la cuenta.
- Documentos identificativos oficiales, se extrae la foto y la fecha de nacimiento. Se verifica que el documento no está caducado. La foto se utiliza para contrastarla con la tomada cuando se configuró la cuenta para comprobar que se trata de su documento real. Cuando identifican documentos fraudulentos se pueden mantener por un plazo de hasta dos años y lo utilizan para entrenar el

software a fin de que detecte mejor los documentos falsos. La imagen del documento también se almacena.

-Dirección de correo electrónico y dirección física. La primera se verifica enviando código, para la segunda se da opción al usuario de verificarla con un tercero, si no se verifica o la verificación falla se marca como no verificada, informando que aun así el usuario puede compartirla, pero informando que algunas organizaciones solo aceptan direcciones verificadas.

-Edad estimada por YOTI: se da la opción al usuario de utilizar la tecnología de YOTI para calcular la edad a través de la App. La tecnología de YOTI calcula al instante si es mayor de 18 años con el mapa digital del rostro creado cuando se creó la cuenta. Al considerar los errores de cálculo y por seguridad de los usuarios, se debe lucir al menos siete años mayor que el umbral de 18. Si YOTI calcula que el usuario es mayor de 28 años se agrega a la cuenta una edad calculada de mayor de 21”.

Otra información relevante que destacar de la Política de Privacidad es la siguiente:

“El objetivo de nuestro uso de datos biométricos para identificarlo o autenticarlo es evitar el uso fraudulento de la App y proteger sus datos. Son parte clave para garantizar el bloqueo de documentos falsos y garantizar que es el usuario real es que está actuando en la App”.

“¿Qué datos biométricos utiliza la App y por qué?

Cuando configura su cuenta escaneamos el rostro para crear plantilla biométrica que almacenamos de forma segura. Cuando realiza determinadas acciones en la App le pediremos que se tome una foto o grabe un video y lo comparamos con la plantilla para comprobar que coincide, comprobando que la imagen sea de una persona real. Estas comprobaciones garantizan que solo el usuario pueda realizar las acciones. Cuando agrega un documento comparamos su foto con la plantilla de rostro para asegurarnos de que los usuarios solo carguen sus propios documentos.

En definitiva, según se informa en el proceso de creación de la cuenta de usuario y en la propia política de privacidad de la aplicación, la App genera una plantilla biométrica facial del usuario que servirá i) en el momento de creación de la cuenta, para acreditar que el usuario es una persona real ii) con posterioridad, para acreditar que quien desea realizar acciones como cambio de PIN o recuperación de cuenta es el usuario que se dio de alta originalmente en la aplicación. En este segundo momento se compara el patrón digital creado a través de un nuevo escaneo facial con el que se guardó en el momento de dar de alta la cuenta de usuario.

Por lo tanto, YOTI realiza un escaneo facial del usuario de su App al objeto de obtener una plantilla biométrica que, como expresamente señalan, tiene como finalidad *“asegurarnos de que eres tú quien está usando la app y de que cualquier documento de identidad que agregas te pertenece”*.

Se trata, de acuerdo con los preceptos antes señalados, de un tratamiento cuya finalidad es la identificación unívoca de una persona física y, por lo tanto, entra dentro del concepto de categoría especial de datos del artículo 9. 1 RGPD. Unos datos

personales a los que, al tratarse de una categoría especial, se les aplica una prohibición general de tratamiento; prohibición que sólo puede ser levantada por la concurrencia de alguna de las circunstancias señaladas en el artículo 9.2. A pesar de ello, YOTI considera que no realiza un tratamiento de categorías especiales de datos porque, a su juicio, el tratamiento *no tiene el propósito de identificar o autenticar a un individuo*. Una conclusión que es errónea en atención a la finalidad que expresamente señala YOTI tiene el tratamiento de la plantilla biométrica facial que se crea.

Al no considerar que trata una categoría especial de datos, YOTI no ha fundamentado su tratamiento- justificando el levantamiento de la prohibición general de tratamiento- en ninguna de las causas previstas en el artículo 9.2, por lo que está infringiendo la prohibición de tratar este tipo de datos prevista en el art. 9.1 RGPD. Así, al entender que no se están tratando datos biométricos, considerados de categoría especial, el *consentimiento* recabado para el tratamiento de datos en el uso de la app sólo puede ser considerado como *imperfecto* y, por lo tanto, no válido para cumplir los requerimientos del RGPD en lo relativo al tratamiento de datos personales de naturaleza biométrica de carácter especial.

Por tanto, se considera que los hechos conocidos son constitutivos de una infracción, imputable a YOTI, por vulneración del artículo 9.1 del RGPD.

IV

Tipificación de la infracción del artículo 9 del RGPD y calificación a efectos de prescripción

El artículo 83.5 del RGPD tipifica como infracción administrativa la vulneración de los artículos siguientes, que se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

"a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;"

Por su parte, la LOPDGDD en su artículo 71, Infracciones, señala que:

"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".

A los solos efectos del plazo de prescripción, el artículo 72.1 de la LOPDGDD establece lo siguiente:

"En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

e) El tratamiento de datos personales de las categorías a las que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que concurra alguna de las circunstancias previstas en dicho precepto y en el artículo 9 de esta ley orgánica."

V

Sanción

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos que señalan:

“1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

- a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;*
- b) la intencionalidad o negligencia en la infracción;*
- c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;*
- d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;*
- e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;*
- f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;*
- g) las categorías de los datos de carácter personal afectados por la infracción;*
- h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;*
- i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;*
- j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y*
- k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción”.*

Por su parte, el artículo 76 “Sanciones y medidas correctivas” de la LOPDGDD dispone:

“1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:
- a) El carácter continuado de la infracción.
 - b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
 - c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
 - d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
 - e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
 - f) La afectación a los derechos de los menores.
 - g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
 - h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado”.

En el presente caso, considerando la gravedad de la posible infracción atendiendo especialmente a las consecuencias que su comisión provoca en los afectados, corresponde la imposición de multa, además de la adopción de medidas.

La multa debe ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD. Para garantizar estos principios, se considera, con carácter previo, el volumen de negocio de YOTI 15.029.907 euros según los últimos datos publicados de marzo de 2025.

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía se considera que procede graduar la sanción a imponer de acuerdo con las circunstancias siguientes, contempladas en los preceptos antes citados.

Con carácter previo, se estima que concurren las circunstancias siguientes:

- *La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido* (artículo 83.2, letra a), del RGPD): de acuerdo con lo señalado, YOTI estaría realizando un tratamiento de datos biométricos, considerados categorías especiales de datos para el que no acredita que concorra alguna de las circunstancias previstas en el art. 9.2 del RGPD para el levantamiento de la prohibición general de tratamiento aplicable a este tipo de datos personales. De igual forma, ha de tenerse en consideración que los datos son objeto de tratamiento fuera del control del usuario, en servidores situados fuera de la Unión Europea, circunstancia que influye de forma más negativa en su facultad de disposición.
- *Intencionalidad/ Negligencia en la infracción* (artículo 83.2, letra b), del RGPD): a pesar de que YOTI afirma reiteradamente- tanto en el proceso de creación de una cuenta de usuario como en la política de privacidad, por ejemplo,- que la finalidad del tratamiento del patrón biométrico facial obtenido es garantizar la identificación del usuario, no considera que esté realizando un tratamiento de datos de carácter personal de categoría especial, circunstancia que denota una

especial negligencia en su condición de responsable de tratamiento de estos datos personales.

- *Las categorías de los datos de carácter personal afectados por la infracción* (artículo 83.2, letra g), del RGPD): en el presente caso, se está realizando un tratamiento de datos incluidos en el artículo 9 del RGPD que los considera categoría especial precisamente por la importancia que tiene que ese tratamiento se realice garantizando el pleno cumplimiento de la normativa de protección de datos. Y ello debido a las posibles consecuencias que tendría para el titular de los datos un posible incumplimiento en el tratamiento de dichos datos personales

Asimismo, se consideran los siguientes factores de graduación en calidad de agravantes:

- *La afectación a los derechos de los menores* (artículo 76.2, letra f), de la LOPDGDD): como hemos señalado, la APP DIGITAL de YOTI se configura como una herramienta que permite verificar la edad y que, previsiblemente, será utilizada en gran medida por menores.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 9 del RGPD, permite fijar una sanción de multa administrativa de **500.000,00 euros**.

VI

Obligación incumplida. Condiciones del consentimiento

El artículo 4.11 del RGPD define el consentimiento del interesado como *“toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen”*.

En este sentido, el artículo 6.1 de la LOPDGDD entiende por consentimiento *“toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen”*.

En relación con las condiciones para el consentimiento, el artículo 7 del RGPD dispone:

1. *Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.*
2. *Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No*

será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato

Cuando se realizan actividades que conllevan el tratamiento de datos personales, un responsable del tratamiento debe siempre detenerse a considerar cuál va a ser el fundamento jurídico del tratamiento previsto. En general, el consentimiento solo puede ser una base jurídica adecuada si se ofrece al interesado control y una capacidad real de elección con respecto a si desea aceptar las condiciones ofrecidas o rechazarlas sin sufrir perjuicio alguno. Cuando solicita el consentimiento, el responsable del tratamiento tiene la obligación de evaluar si dicho consentimiento cumple todos los requisitos para la obtención de un consentimiento válido. Si se obtiene en pleno cumplimiento del RGPD, el consentimiento es una herramienta que otorga a los interesados el control sobre si los datos personales que les conciernen van a ser tratados o no. Si no es así, el control del interesado será meramente ilusorio y el consentimiento no será una base jurídica válida para el tratamiento, lo que convertirá dicha actividad de tratamiento en una actividad ilícita.

El Comité Europeo de Protección de Datos analizó estas cuestiones en su documento “Directrices 05/2020 sobre el consentimiento con arreglo al Reglamento 2016/679”, de 04/05/2020. De lo indicado en este documento, interesa destacar algunos aspectos relacionados con la validez del consentimiento, en concreto sobre los elementos “específico”, “informado” e “inequívoco”:

“3.2. Manifestación de voluntad específica

El artículo 6, apartado 1, letra a), confirma que el consentimiento del interesado para el tratamiento de sus datos debe darse «para uno o varios fines específicos» y que un interesado puede elegir con respecto a cada uno de dichos fines. El requisito de que el consentimiento deba ser «específico» tiene por objeto garantizar un nivel de control y transparencia para el interesado. Este requisito no ha sido modificado por el RGPD y sigue estando estrechamente vinculado con el requisito de consentimiento «informado». Al mismo tiempo, debe interpretarse en línea con el requisito de «disociación» para obtener el consentimiento «libre». En suma, para cumplir con el carácter de «específico» el responsable del tratamiento debe aplicar:

- i) la especificación del fin como garantía contra la desviación del uso,*
- ii) la disociación en las solicitudes de consentimiento, y*
- iii) una clara separación entre la información relacionada con la obtención del consentimiento para las actividades de tratamiento de datos y la información relativa a otras cuestiones.*

(...)

“3.3. Manifestación de voluntad informada

El RGPD refuerza el requisito de que el consentimiento debe ser informado. De conformidad con el artículo 5 del RGPD, el requisito de transparencia es uno de los principios fundamentales, estrechamente relacionado con los principios de lealtad y licitud. Facilitar información a los interesados antes de obtener su consentimiento es esencial para que puedan tomar decisiones informadas, comprender qué es lo que están autorizando y, por ejemplo, ejercer su derecho a retirar su consentimiento. Si el responsable no proporciona información accesible, el control del usuario será ilusorio y el consentimiento no constituirá una base válida para el tratamiento de los datos. Si no se cumplen los requisitos relativos al consentimiento informado, el consentimiento no será válido y el responsable podrá estar incumpliendo el artículo 6 de RGPD.

3.3.1. Requisitos mínimos de contenido para que el consentimiento sea «informado»

Para que el consentimiento sea informado es necesario comunicar al interesado ciertos elementos que son cruciales para poder elegir. Por tanto, el GT29 opina que se requiere, al menos, la información siguiente para obtener el consentimiento válido:

- i) la identidad del responsable del tratamiento,*
- ii) el fin de cada una de las operaciones de tratamiento para las que se solicita el consentimiento,*
- iii) qué (tipo de) datos van a recogerse y utilizarse,*
- iv) la existencia del derecho a retirar el consentimiento,*
- v) información sobre el uso de los datos para decisiones automatizadas de conformidad con el artículo 22, apartado 2, letra c), cuando sea pertinente, e*
- vi) información sobre los posibles riesgos de transferencia de datos debido a la ausencia de una decisión de adecuación y de garantías adecuadas, tal y como se describen en el artículo 46”.*

Si bien YOTI fundamenta el tratamiento de datos que realiza a través de la App Digital en la ejecución de un contrato (art. 6.1 b) del RGPD), ha de entenderse que, con carácter previo a un tratamiento de datos destinado a la ejecución de un contrato debe de acordarse dicho contrato mediante la manifestación de voluntad de las partes del mismo.

Por lo tanto, con carácter previo a considerar que se realiza un tratamiento de datos para ejecutar un contrato, ha de existir dicho contrato y ha de contarse, por lo tanto, con el consentimiento de las partes para la vinculación por los términos del mismo. Es por ello por lo que YOTI pide el consentimiento del usuario en diversos pasos del proceso de creación de la cuenta en la App Digital; y ello por cuanto es el consentimiento del interesado el que ha de obtenerse para proceder con el tratamiento de datos pretendido.

Un consentimiento que, como hemos señalado, al referirse a un tratamiento de datos personales biométricos, considerados como de categoría especial, y al no aludir su obtención a esta circunstancia, no podría considerarse conforme con el RGPD.

Por otro lado, sentado lo anterior, según ha quedado acreditado, en el proceso de creación de una cuenta en la App de YOTI figura que la obtención del consentimiento para que los datos personales proporcionados sean también tratados con fines de investigación y al objeto de mejorar los servicios proporcionados por YOTI se realiza a través de una casilla premarcada. En este sentido, no se estaría recabando el

consentimiento *stricto sensu* sino que el mismo estaría otorgado a no ser que, expresamente y de forma activa, el usuario desmarcara la casilla. Y ello por cuanto los consentimientos realizados mediante casilla declarativas activadas por defecto no son el resultado de un acto afirmativo y claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca.

En estas condiciones, no puede afirmarse que el consentimiento cumpla los requisitos establecidos en la normativa anteriormente señalada.

Según consta en el expediente, por ser información proporcionada por YOTI *En la App Digital ID el valor por defecto es que los datos se puedan usar para I+D. Yoti ha tomado medidas para dejar esto claro a los usuarios. Los usuarios pueden optar por excluirse, evitando que sus datos se utilicen para I+D, haciendo para ello uso de la configuración de la App.*

Asimismo, existe opción de configuración de la App con el título “Consentimiento de datos biométricos” donde se muestra el texto: “Autorizaste a YOTI para usar tu escaneo facial de las siguientes formas: *Enlace a la Política de Privacidad*”. Por otro lado, muestra una casilla declarativa activada por defecto a través de la cual el usuario puede oponerse al tratamiento de sus datos biométricos para fines de investigación interna.

Existe una última opción que permite al usuario oponerse al tratamiento de sus datos con *finés de análisis*, y existe casilla declarativa activada por defecto y mostrando el siguiente texto:

“necesitamos saber qué funciona y qué no, cuantas personas usan nuestra app, en qué lugar del mundo están y qué productos o características son más populares. Recopilamos información sobre tu dispositivo y tu uso de la app mediante análisis internos y de terceros. Despersonalizamos la información para que no sea posible identificarte personalmente...No creamos perfiles de las personas, simplemente buscamos tendencias y patrones para informar las decisiones empresariales. Si no deseas compartirnos datos de análisis puedes desactivar la función. Cierta información se comparte automáticamente cuando usas nuestros productos y no podemos desactivarla”.

Por tanto, se considera que los hechos conocidos son constitutivos de una infracción, imputable a YOTI, por vulneración del artículo 7 del RGPD.

VII

Tipificación de la infracción del artículo 7 del RGPD y calificación a efectos de prescripción

El artículo 83.5 del RGPD tipifica como infracción administrativa la vulneración de los artículos siguientes, que se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

"a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;

Por su parte, la LOPDGDD en su artículo 71, Infracciones, señala que:

"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".

A los solos efectos del plazo de prescripción, el artículo 72.1 de la LOPDGDD establece lo siguiente:

"En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

c) El incumplimiento de los requisitos exigidos por el artículo 7 del Reglamento (UE) 2016/679 para la validez del consentimiento"

VIII Sanción

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos que señalan:

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

- a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;*
- b) la intencionalidad o negligencia en la infracción;*
- c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;*
- d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;*
- e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;*
- f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;*
- g) las categorías de los datos de carácter personal afectados por la infracción;*

- h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;*
- i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;*
- j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y*
- k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción”.*

Por su parte, el artículo 76 “Sanciones y medidas correctivas” de la LOPDGDD dispone:

“1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

- a) El carácter continuado de la infracción.*
- b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.*
- c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.*
- d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.*
- e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.*
- f) La afectación a los derechos de los menores.*
- g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.*
- h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado”.*

En el presente caso, considerando la gravedad de la posible infracción atendiendo especialmente a las consecuencias que su comisión provoca en los afectados, corresponde la imposición de multa, además de la adopción de medidas.

La multa que se imponga debe ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD. Para garantizar estos principios, se considera, con carácter previo, el volumen de negocio de YOTI 15.029.907 euros según los últimos datos publicados de marzo de 2025.

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, se considera que procede graduar la sanción a imponer de acuerdo con las circunstancias siguientes, contempladas en los preceptos antes citados.

Con carácter previo, se estima que concurren las circunstancias siguientes:

- *La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido* (artículo 83.2, letra a), del RGPD): según se ha indicado, YOTI establece con casilla premarcada la obtención del consentimiento para que los datos suministrados sean utilizados con fines de investigación interna (I+D). Se trataría de datos que son objeto de un tratamiento posterior distinto a la finalidad inicial para la que fueron recabados y en el que el consentimiento obtenido no cumpliría lo establecido en el RGPD. Ha de señalarse igualmente que esta finalidad ulterior atiende a intereses que le son propios como compañía mercantil puesto que tienen como objeto mejorar el producto que ofrecen. De igual forma, ha de tenerse en consideración que los datos son objeto de tratamiento fuera del control del usuario, en servidores situados fuera de la Unión Europea, circunstancia que influye de forma más negativa en su facultad de disposición
- *Intencionalidad/ Negligencia en la infracción* (artículo 83.2, letra b), del RGPD): se detecta una particular negligencia en YOTI por cuanto señala conscientemente que el consentimiento otorgado por defecto puede ser revocado, sin atender que no ha de optarse por una revocación posterior a instancias del interesado, sino por una obtención del consentimiento de acuerdo a las salvaguardas y garantías que establece el RGPD.
- *Las categorías de los datos de carácter personal afectados por la infracción* (artículo 83.2, letra g), del RGPD): en el presente caso, se está realizando un tratamiento de datos incluidos en el artículo 9 del RGPD que los considera categoría especial precisamente por la importancia que tiene que ese tratamiento se realice garantizando el pleno cumplimiento de la normativa de protección de datos. Y ello debido a las posibles consecuencias que tendría para el titular de los datos un posible incumplimiento en el tratamiento de dichos datos personales

Asimismo, se consideran los siguientes factores de graduación en calidad de agravantes:

- *La afectación a los derechos de los menores* (artículo 76.2, letra f), de la LOPDGDD): como hemos señalado, la APP DIGITAL de YOTI se configura como una herramienta que permite estimar y verificar la edad y que, previsiblemente, será utilizada en gran medida por menores.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 7 del RGPD, permite fijar una sanción de multa administrativa de **200.000,00 euros**.

IX

Obligación incumplida. Limitación del plazo de conservación

La letra e) del artículo 5.1 del RGPD propugna:

"1. Los datos personales serán:

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);"

Ha de recordarse que, según se informa en la EIPD proporcionada por YOTI *Para el token de edad y los datos de la Digital ID App, la retención queda establecida mientras el usuario mantiene activa la cuenta o después de tres años de inactividad".*

Asimismo, en relación con la conservación de los datos por YOTI afirman:

"Cuando YOTI actúa como responsable conserva los datos de la cuenta mientras el usuario tenga una cuenta con Yoti y durante los próximos tres años de inactividad de dicho usuario. Los usuarios pueden eliminar estos datos, o su cuenta, en cualquier momento y los datos son borrados automáticamente al caducar los 3 años de inactividad.

Entre esos datos que se retienen durante todo el período de activación de la cuenta o, cuando ésta carece de actividad, después de tres años de inactividad, se encuentran datos biométricos considerados categoría especial de datos de acuerdo con el art. 9 del RGPD.

De acuerdo con lo señalado en apartados precedentes, el patrón biométrico obtenido tras el escaneo facial del usuario tendía como finalidad tanto el comprobar que el usuario es una persona real en el momento de configuración de la cuenta como la identificación del usuario- cotejando un nuevo patrón obtenido mediante un nuevo escaneo facial con el almacenado- al realizar operaciones como modificación del PIN de acceso o recuperación de cuenta. Al respecto, ha de entenderse:

- Que la finalidad de comprobación de la naturaleza *real* del usuario se completa cuando la indicada comprobación constata que se trata de una persona. Una conservación de este dato personal- recordemos, considerado como de categoría especial- más allá de dicha comprobación incumpliría el principio de limitación del plazo de conservación.
- Las operaciones para las que YOTI considera necesario cotejar de nuevo los patrones faciales del individuo pueden no darse nunca en todo el período de activación de la cuenta. Por lo tanto, se estarían conservado datos considerados de categoría especial con base en una pretendida finalidad que puede no llegar a darse nunca.

Por otra parte, en relación con la retención de datos de geolocalización, se afirma:

“Los datos de geolocalización retenidos por Yoti y derivados de la dirección IP se limitan al código de país y la provincia de cada usuario individual. Esta información se obtiene antes de completar cualquier verificación de edad; por lo tanto, en esta etapa Yoti no puede distinguir si el usuario en particular es menor o no. El período de retención de los datos de geolocalización es actualmente de 5 años”.

Debemos recordar que la información de la IP y los datos de geolocalización se obtienen y son objeto de tratamiento en el marco de la verificación de que el usuario que está creando una cuenta en la app de YOTI es mayor de 14 años. Por lo tanto, la finalidad de tratamiento de la IP, esto es, conocer qué normativa tenían que aplicar, se alcanza con la autodeclaración para conocer la aplicabilidad de las restricciones de edad, por lo que no existen argumentos- máxime cuando YOTI no ha realizado alegaciones al acuerdo de inicio- que permitan fundamentar que el tratamiento de la IP del usuario es necesaria más allá de esa verificación inicial.

Por lo tanto, el cumplimiento del principio de limitación del plazo de conservación también implicaría que, verificada dicha circunstancia, los datos dejaran de ser objeto de tratamiento.

Por otro lado, las actuaciones previas de investigación desarrolladas por esta AEPD analizaron los “*Términos y Condiciones*” de la app de YOTI, documento en el que se destacan los siguientes apartados relevantes (el subrayado es de esta AEPD):

“Al registrarse para obtener una cuenta o al agregar sus primeros documentos de identidad, le pediremos que complete una breve prueba para demostrar que se trata de una persona viva real. Esta prueba podría incluir, entre otras opciones, repetir algunas palabras en un video grabado o podríamos pedirle que mueva su teléfono siguiendo su rostro para capturar varias imágenes (verá las instrucciones de este proceso en ese momento). Si le pedimos que use el método del video, el video grabado se cargará en nuestro servidor y, a menos que se nos exija conservarlo por motivos reglamentarios, lo eliminaremos permanentemente dentro de 30 días desde la fecha de su grabación. Si le pedimos que utilice otro método, la información se procesará automáticamente en su teléfono y recibirá una aprobación o rechazo al instante”.

De nuevo, se constata que YOTI continúa con el tratamiento de datos personales- en este caso, el video que sea grabado como prueba de vida real- en un período que excede el derivado de dicha finalidad. Y ello por cuanto, en el momento en que se constata que la persona que es grabada es real, el tratamiento de los datos personales contenidos en dicho video durante un período de 30 días superaría, de nuevo, el principio de limitación en el plazo de limitación del plazo de conservación.

Finalmente, consta información proporcionada por YOTI en el sentido de que *Para creación y gestión de la cuenta de usuario YOTI trata los siguientes tipos de datos (...):*

-Documentos identificativos oficiales, se extrae la foto y la fecha de nacimiento. Se verifica que el documento no está caducado. La foto se utiliza para contrastarla con la tomada cuando se configuró la cuenta para comprobar que se trata de su documento real. Cuando identifican documentos fraudulentos se pueden mantener por un plazo de hasta dos años y lo utilizan para entrenar el

software a fin de que detecte mejor los documentos falsos. La imagen del documento también se almacena.(...)

Es decir, se retienen nuevamente datos personales, en este caso relativos a un documento identificativo oficial que hubiera sido identificado como fraudulento, por un plazo que excede la finalidad para la que fue originalmente recabado este documento- la verificación de la identidad del usuario-.

Por tanto, se considera que los hechos conocidos son constitutivos de una infracción, imputable a YOTI, por vulneración del artículo 5.1 e) del RGPD.

X

Tipificación de la infracción del artículo 5.1.e) del RGPD y calificación a efectos de prescripción

El artículo 83.5 del RGPD tipifica como infracción administrativa la vulneración de los artículos siguientes, que se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;

Por su parte, la LOPDGDD en su artículo 71, Infracciones, señala que:

“Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica”.

A los solos efectos del plazo de prescripción, el artículo 72.1 de la LOPDGDD establece lo siguiente:

“En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679.”

XI

Sanción

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos que señalan:

“1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

- a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;*
- b) la intencionalidad o negligencia en la infracción;*
- c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;*
- d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;*
- e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;*
- f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;*
- g) las categorías de los datos de carácter personal afectados por la infracción;*
- h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;*
- i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;*
- j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y*
- k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción”.*

Por su parte, el artículo 76 “Sanciones y medidas correctivas” de la LOPDGDD dispone:

“1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

- a) El carácter continuado de la infracción.*
- b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.*
- c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.*
- d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.*

- e) *La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.*
- f) *La afectación a los derechos de los menores.*
- g) *Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.*
- h) *El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado”.*

En el presente caso, considerando la gravedad de las posibles infracciones atendiendo especialmente a las consecuencias que su comisión provoca en los afectados, corresponde la imposición de multa, además de la adopción de medidas.

La multa que se imponga debe ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD. Para garantizar estos principios, se considera, con carácter previo, el volumen de negocio de YOTI 15.029.907 euros según los últimos datos publicados de marzo de 2025.

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, se considera que procede graduar la sanción a imponer de acuerdo con las circunstancias siguientes, contempladas en los preceptos antes citados.

Con carácter previo, se estima que concurren las circunstancias siguientes:

- *La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido (artículo 83.2, letra a), del RGPD):* YOTI conserva datos personales que exceden, con mucho, la finalidad para que los datos son tratados. Esta vulneración del principio de limitación de tratamiento afectaría a todos los usuarios que crearan su cuenta en la App de YOTI, con independencia de que usaran los servicios que se proporcionan a través de la misma. De igual forma, ha de tenerse en consideración que los datos son objeto de tratamiento fuera del control del usuario, en servidores situados fuera de la Unión Europea, circunstancia que influye de forma más negativa en su facultad de disposición
- *Intencionalidad/ Negligencia en la infracción (artículo 83.2, letra b), del RGPD):* YOTI actúa de forma especialmente negligente estableciendo plazos de conservación que exceden de forma holgada el necesario para llevar a cabo la operación de tratamiento para la que los datos se recaban. Asimismo, YOTI no justifica dicho plazo de conservación ni la necesidad de los mismos.
- *Las categorías de los datos de carácter personal afectados por la infracción (artículo 83.2, letra g), del RGPD):* Algunos de los datos personales que se conservan excediendo el plazo necesario para alcanzar la finalidad del tratamiento son datos considerados como de categoría especial, que requieren de una especial protección debido a las consecuencias que tendría para los afectados que se vieran vulnerados.

Asimismo, se consideran los siguientes factores de graduación en calidad de agravantes:

- *La afectación a los derechos de los menores* (artículo 76.2, letra f), de la LOPDGDD): como se ha indicado en apartados precedentes, los datos afectan en gran parte a menores de edad, los principales potenciales usuarios de la app de YOTI, orientada a verifica la edad de los usuarios cuando así sea requerido.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 5.1 e) del RGPD, permite fijar una sanción de multa administrativa de **250.000,00 euros**.

XII

Medidas correctivas

De acuerdo con lo establecido en el artículo 58.2.d) del RGPD, cada autoridad de control podrá *“ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado...”*

En aplicación de lo anterior, se considera que procede adoptar la medida correctiva consistente en requerir a YOTI para que, en el plazo máximo de SEIS MESES, a contar desde la fecha de ejecutividad de la presente resolución finalizadora de este procedimiento, adopte las medidas siguientes:

- Acreditar que el tratamiento de datos personales biométricos, considerados categorías especiales de datos, se realiza conforme lo dispuesto en el RGPD.
- Acreditar que los tratamientos de datos personales basados en el consentimiento del interesado cumplan lo prescrito al respecto en el RGPD.
- Acreditar que los datos personales objeto de tratamiento son conservados durante el plazo estrictamente necesario para el cumplimiento de la finalidad del tratamiento, de acuerdo con el artículo 5.1 e) del RGPD.

La imposición de estas medidas es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución del presente procedimiento sancionador podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Presidencia de la Agencia Española de Protección de Datos **RESUELVE**:

PRIMERO: IMPONER a YOTI LTD, con NIF 08998951:

- Por la infracción del artículo 9 del RGPD: 500.000 euros.
- Por la infracción del artículo 7 del RGPD: 200.000 euros.
- Por la infracción del artículo 5.1 e) del RGPD: 250.000 euros

Total: **950.000,00** euros

SEGUNDO: ORDENAR a YOTI LTD, con NIF 08998951, que en virtud del artículo 58.2.d) del RGPD, en el plazo máximo de SEIS MESES desde que la presente resolución sea firme y ejecutiva, acredite

- Que el tratamiento de datos personales biométricos, considerados categorías especiales de datos, se realiza conforme lo dispuesto en el RGPD.
- Que los tratamientos de datos personales basados en el consentimiento del interesado cumplan lo prescrito al respecto en el RGPD.
- Que los datos personales objeto de tratamiento son conservados durante el plazo estrictamente necesario para el cumplimiento de la finalidad del tratamiento, de acuerdo con el artículo 5.1 e) del RGPD.

SEGUNDO: NOTIFICAR la presente resolución a YOTI LTD.

TERCERO: Esta resolución será ejecutiva una vez finalice el plazo para interponer el recurso potestativo de reposición (un mes a contar desde el día siguiente a la notificación de esta resolución) sin que el interesado haya hecho uso de esta facultad. Se advierte al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº **IBAN: ES00-0000-0000-0000-0000-0000 (BIC/Código SWIFT: CAIXESBBXXX)**, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública. La publicación se realizará una vez la resolución haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Presidencia de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [<https://sedeaepd.gob.es/sede-electronica-web/>], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-180725

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