PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Directrices sobre cuestiones éticas y jurídicas de la protección de datos en la investigación e innovación en materia de TIC

BIOMETRÍA

Esta obra está bajo una licencia de Creative Commons Reconocimiento-No comercial-Sin obras derivadas 4.0 Internacional.

Este proyecto ha sido financiado por el programa de investigación e innovación Horizonte 2020 de la Unión Europea mediante el acuerdo de subvención nº 788039. Este documento refleja únicamente las opiniones de los autores, y la Agencia no se hace responsable del uso que pueda hacerse de la información contenida en él.

La biometría en la investigación e innovación de las Tecnologías de la Información y la Comunicación (TIC)

Alessandro Ortalda, Carlotta Rigotti, Andrés Chomczyk Penedo, Paul De Hert (VUB)

Esta parte de la Guía fue revisada por Stefano Leucci (Supervisor Europeo de Protección de Datos), Ernestina Sacchetto (Universidad de Turín); Catherine Jasserand-Breeman (KU Leuven) y Lydia Belkadi (KU Leuven).

También fue revisado y validado por el profesor Gert Vermuelen (Universidad de Gante)

1 Introducción y ámbito de aplicación

Las actividades de investigación pueden implicar, a veces, el tratamiento de datos biométricos, lo que exige que los investigadores y las instituciones de investigación que actúan como responsables o encargados del tratamiento de datos, aborden los requisitos de protección de datos. Habida cuenta los datos biométricos gozan de un régimen de protección especial en el marco normativo de la UE, los investigadores que trabajan con datos biométricos deben cumplir no sólo los requisitos generales de protección de datos y los requisitos específicos previstos en el artículo 89 del Reglamento General de Protección de Datos (RGPD) europeo relacionados con las actividades[1] de investigación, sino que también deben aplicar garantías adicionales adaptadas a las especificidades de los datos biométricos y/o el tratamiento biométrico (véase "Protección de datos e investigación científica" dentro de la parte II, sección "Conceptos principales" de estas directrices).

Las siguientes directrices proporcionan orientación sobre cómo cumplir con las obligaciones legales consagradas en el régimen europeo de protección de datos. En particular, el documento se refiere a las actividades de investigación en materia de TIC que incluyen el desarrollo de sistemas de TIC que emplean datos biométricos. Los autores reconocen que, hoy en día, es habitual que estos sistemas adopten tecnologías de Inteligencia Artificial. En la parte III de estas directrices se incluye un capítulo dedicado a la Inteligencia Artificial.

Esta Parte VI se dirige a las instituciones de investigación de las TIC que trabajan con tecnología biométrica como responsables del tratamiento de datos, incluyendo no sólo a los investigadores, que podrían no ser conscientes de las obligaciones legales derivadas de sus actividades de investigación, sino también a otras partes interesadas, como los departamentos jurídicos o los comités éticos, que podrían estar más versados en los aspectos legales pero no necesariamente en

[1] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such' (2016).*

los regímenes especiales de protección de datos aplicables a los datos biométricos y a las actividades de investigación. Para garantizar ambas cosas, el público puede acceder fácilmente al contenido de las directrices. El documento intenta lograr un equilibrio entre los detalles técnicos (tanto en lo que respecta a las TIC y la tecnología biométrica como a la legislación sobre protección de datos) y la accesibilidad general.

2 Definiciones

2.1 Categorías especiales de datos personales

Antes de definir los datos biométricos, es necesario examinar las "categorías especiales de datos personales", también conocidas comúnmente como "datos sensibles". De hecho, el artículo 9.1 del RGPD agrupa los datos biométricos (o, al menos, algunos de ellos; véase la sección **¡Error! No se encuentra el origen de la referencia.** "Datos biométricos") en este grupo más amplio:

Categorías especiales de datos personales
Datos que revelan el origen racial o étnico
Datos que revelan la opinión política
Datos que revelan creencias religiosas o filosóficas
Datos que revelan la afiliación sindical
Datos genéticos
Datos biométricos (con el fin de identificar de forma única a las personas físicas)
Datos relativos a la salud
Datos relativos a la vida sexual u orientación sexual de una persona física

Por defecto, el artículo 9 del RGPD prohíbe el tratamiento de categorías especiales de datos personales, a menos que se produzca una de las excepciones enumeradas en el artículo 9.2 del RGPD. Una de estas excepciones se produce cuando el "tratamiento es necesario para [...] fines de investigación científica o histórica".

Cabe señalar que, para cumplir la normativa, no basta con que el tratamiento de categorías especiales de datos personales cumpla una de las excepciones enumeradas en el artículo 9.2 del RGPD. Además de eso, y antes de que comience el tratamiento, el responsable del tratamiento deberá identificar una base jurídica adecuada para el tratamiento de datos (véase la sección

¡Error! No se encuentra el origen de la referencia. "Identificar la base jurídica más adecuada")[2].

Los responsables del tratamiento también deben ser conscientes de que, según el artículo 9.4 del RGPD, los Estados miembros pueden introducir otras condiciones y aplicar requisitos y limitaciones adicionales en relación con el tratamiento de datos genéticos, datos biométricos o datos relativos a la salud. Así pues, los responsables del tratamiento que deseen tratar estas categorías especiales deberán comprobar siempre si existen requisitos nacionales específicos aplicables. Se puede encontrar más información en los informes nacionales elaborados por el consorcio PANELFIT (a los que se puede acceder en: https://www.panelfit.eu/national-reports/).

Aunque algunos datos no constituyen categorías especiales de datos personales por sí mismos, cuando se emplean junto con otros datos pueden constituir categorías especiales de datos personales. Por ejemplo, la dirección y la lengua materna de una persona no son categorías especiales de datos personales. Sin embargo, cuando se adjuntan al conjunto de datos el nombre, el lugar de nacimiento y otros datos del interesado, la combinación podría revelar información suficiente para identificar el origen racial o étnico del interesado con un grado razonable de certeza. En este caso, los datos deben estar sujetos a los mismos requisitos y limitaciones de las categorías especiales de datos personales, aunque no lo estén por sí mismos.

Conjunto de datos 1	**Conjunto de datos 2**
Dirección: Washington D.C.	Dirección: Washington D.C.
Lengua materna: Francés	Lengua materna: Francés
	Nombre: Seydou Kablan Bakayoko
	Lugar de nacimiento: Abiyán
	Otros idiomas conocidos: Cebaara, ingles
	Escuela primaria: École Konan Raphael, Abidjan
El conjunto de datos 1 no proporciona información sobre el origen racial o étnico del interesado	*La información proporcionada por el conjunto de datos 2 podría considerarse suficiente para revelar el origen racial o étnico del interesado (con un grado razonable de certeza)*

Cabe señalar, de nuevo, que los datos deben satisfacer un grado de certeza razonable. Este grado de certeza es contextual y debe evaluarse caso por caso.

[2] Véase también Ludmilla Georgieva and Christopher Kuner, 'Article 9. Processing of Special Categories of Personal Data', in *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford, United Kingdom: Oxford University Press, 2019), 376–77.

2.2 Datos biométricos

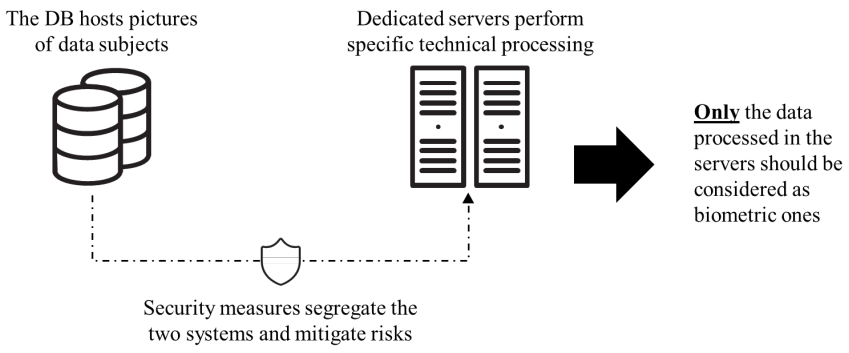
El término "datos biométricos" se define en el artículo 4.14 del RGPD. En consecuencia, los datos biométricos son "datos personales resultantes de un tratamiento técnico específico relativo a las características físicas, fisiológicas o de comportamiento de una persona física, que permiten o confirman la identificación única de dicha persona física". La definición sugiere que para que los datos personales se consideren "biométricos" deben cumplir cuatro *criterios*[3].

En primer lugar, tienen que ser "datos personales", definidos en el artículo 4.1 del RGPD como "información relativa a una persona física identificada o identificable". En segundo lugar, requieren un "tratamiento técnico específico" para extraer la información de la fuente de datos en bruto (por ejemplo, extraer los rasgos faciales de una fotografía para medirlos). El considerando 51 del RGPD establece que "el tratamiento de fotografías no debe considerarse sistemáticamente como tratamiento de categorías especiales de datos personales, ya que sólo se incluyen en la definición de datos biométricos cuando se tratan a través de un medio técnico específico que permite la identificación o autenticación única de una persona física". Así pues, los datos biométricos que no sean objeto de un "tratamiento técnico específico" no son datos biométricos en el contexto del RGPD[4]. Sin embargo, incluso cuando los datos no son datos biométricos en una fase determinada, pueden formar parte de un tratamiento de datos que los convierta en datos biométricos en una fase posterior. Por ejemplo, una base de datos puede albergar imágenes que se utilizarán para llevar a cabo la identificación biométrica mediante un tratamiento técnico específico en una fase posterior (por lo que todavía no son datos biométricos). Imagínese un escenario en el que dicha base de datos esté directamente vinculada al sistema que realiza la identificación biométrica (véase también la sección **¡Error! No se encuentra el origen de la referencia.** "Sistema biométrico"). En este caso, las partes no autorizadas podrían explotar este enlace para acceder a los datos biométricos. Por ejemplo, podrían exfiltrar las imágenes (no biométricas) alojadas en la base de datos y, tras haber violado el sistema que realiza la identificación biométrica, podrían pasar la imagen por él y realizar la identificación biométrica, obteniendo así acceso a los datos biométricos. En este escenario, una seguridad débil garantiza que partes externas puedan obtener los datos biométricos, incluso si estos datos biométricos aún no existen. Los responsables del tratamiento de datos deben abordar esta cuestión desde la perspectiva de la gestión de riesgos. Si no pueden garantizar una mitigación adecuada de los riesgos para los datos no biométricos (es decir, los riesgos de explotación), estos conjuntos de datos deberían considerarse biométricos y estar sujetos a todos los requisitos legales, aunque no cumplan -por sí mismos- los criterios para ser considerados datos biométricos.

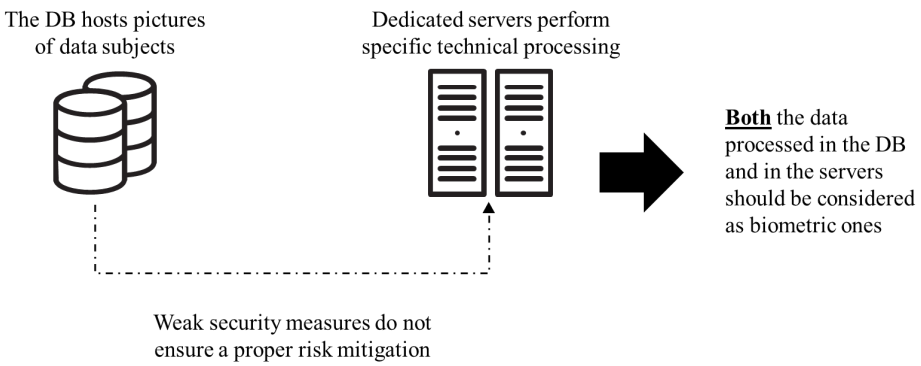
---

[3] Sobre el análisis de la definición prevista en el RGPD, véase C. Jasserand, 'Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data', *European Data Protection Law Review* 2, no. 3 (2016): 297–311, https://doi.org/10.21552/EDPL/2016/3/6.

[4] Los académicos debaten si esto debería aplicarse también a los procesos técnicos que son un requisito previo para la identificación, como el mero almacenamiento en bases de datos. Véase, por ejemplo, Kindt, *Having yes, using no? About the new legal regime for biometric data*, Computer Law and Security Review, 34, 2018, pp. 523-538. Para un análisis de las cuestiones en torno al formato distinto de las fotografías, véase Andras Nautsch *et al*., *Preserving privacy in speaker and speech characterization*, Computer Speech & Language, 58, 2018, p. 445.



Escenario de datos biométricos 1



Escenario de datos biométricos 2

El tercer *criterio* se refiere a las características de los interesados que se captan mediante el tratamiento técnico específico mencionado anteriormente. Estas características pueden ser "físicas", "fisiológicas" o "de comportamiento", y son diferentes de las cualidades accidentales como la dirección del interesado, su ubicación en un momento dado, los datos de empleo, etc. El cuarto y último *criterio* establece que para que los datos personales se consideren biométricos deben permitir o confirmar la identificación única de una persona física. De hecho, los datos biométricos no identifican necesariamente de forma única a las personas *en sí*. Por ejemplo, los datos biométricos podrían utilizarse para distinguir entre humanos y animales, o entre hombres y mujeres[5]. Sin embargo, a diferencia de otros identificadores como los nombres o los códigos de identificación, el tratamiento de los datos biométricos no devuelve una identificación clara. Más bien permite la identificación de individuos con un cierto grado de probabilidad. Según una opinión establecida, los datos deben considerarse biométricos "incluso si los patrones utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad"[6].

---

[5] Véase, por ejemplo '14 Misunderstandings with Regard to Identification and Authentication' (Agencia espanola proteccion datos, European Data Protection Supervisor, June 2020), 3.

[6] Grupo de Trabajo del Artículo 29, 'Opinion 4/2007 on the Concept of Personal Data', 2007, 8. Véase también Article 29 Data Protection Working Party, 'Opinion 3/2012 on Developments in Biometric Technologies', 2012, 6.

2.3 Sistema biométrico

El presente capítulo define el "sistema biométrico" como cualquier sistema capaz de identificar de forma exclusiva a personas físicas (con un cierto grado de probabilidad) mediante la realización de un tratamiento técnico específico relacionado con las características físicas, fisiológicas o de comportamiento de las personas físicas[7]. La definición abarca tanto los sistemas "todo en uno" que realizan todos los pasos (por ejemplo, la adquisición de datos, la elaboración de datos, el almacenamiento de datos, etc.) como los grupos de sistemas que realizan cada uno de los pasos individuales (por ejemplo, una red de módulo de captura de datos basada en una cámara, un software de mapeo biométrico y una base de datos para el almacenamiento). Cuando un sistema que realiza uno o más pasos individuales (en lo sucesivo, "sistema X") no se califica en sí mismo como sistema biométrico -según la definición anterior- pero forma parte, sin embargo, de un grupo de sistemas que incluyen los biométricos, el sistema X debe considerarse un sistema biométrico, a menos que pueda demostrarse -posiblemente mediante pruebas documentadas- que no procesa datos biométricos y que los riesgos están efectivamente mitigados (por ejemplo, el riesgo de que terceros no autorizados utilicen el sistema X para acceder a otro sistema directamente vinculado al sistema X en el que se procesan datos biométricos).

A menudo, los sistemas biométricos se basan en tecnología de inteligencia artificial. El uso de dicha inteligencia artificial plantea otros riesgos para la protección de datos que los responsables del tratamiento deben abordar. Por lo tanto, es aconsejable consultar la Parte III de estas Directrices.

2.4 Tipos de datos biométricos

Como ya se ha mencionado, los distintos datos biométricos pueden derivarse de diferentes características que presenta una persona física: físicas, fisiológicas y de comportamiento. La presente sección ilustra estos diferentes tipos de datos biométricos. La siguiente taxonomía no está establecida como un estándar y ciertos tipos de datos biométricos pueden ser categorizados de manera diferente por diferentes expertos. Por ejemplo, las taxonomías a veces agrupan los datos biométricos fisiológicos en datos biométricos físicos.

2.4.1 Datos biométricos físicos

Los datos biométricos físicos pueden generarse capturando rasgos corporales distintivos de los individuos. El carácter distintivo de estos rasgos puede emplearse como identificador. Algunas de las características biométricas físicas más comunes son las huellas dactilares, la forma de la mano, los rasgos faciales (como la redondez de la cara, la distancia entre los ojos, etc.) y los rasgos del iris.

2.4.2 Datos biométricos fisiológicos

Los datos biométricos fisiológicos pueden generarse mediante la observación de las funciones corporales y la captura de patrones distintivos asociados a ellas. Algunos de los datos biométricos

---

[7] Aunque la Organización Internacional de Normalización elaboró un vocabulario detallado de términos relacionados con la biometría, que incluye la definición de "sistema biométrico", los demás del presente documento prefieren adoptar una definición construida a partir de las disposiciones del RGPD. Véase International Standardization Organization and International Electrotechnical Commission, 'ISO/IEC 2382-37 - Information Technology - Vocabulary - Part 37: Biometrics', 2017.

fisiológicos más comunes se generan a partir de electrocardiogramas, patrones de respiración y electroencefalogramas.

Aunque los datos biométricos físicos se utilizan a menudo como sinónimo de datos biométricos fisiológicos -y viceversa-, los autores creen que una distinción podría ser beneficiosa para enmarcar mejor el debate, sobre todo teniendo en cuenta los recientes estudios sobre la relación entre la tecnología biométrica y ciertas funciones fisiológicas, como las neurofisiológicas[8].

2.4.3 Datos biométricos del comportamiento

Los datos biométricos del comportamiento pueden generarse observando el comportamiento de los individuos, para identificar patrones distintivos en dicho comportamiento. Algunos comportamientos son inherentes a los individuos -como la forma de andar o la voz-, mientras que otros requieren la interacción con herramientas específicas para manifestarse -como la escritura a mano, la dinámica de las teclas y el movimiento del ratón-.

A diferencia de los datos biométricos físicos, los datos biométricos de comportamiento requieren una observación de los individuos que introduce una variable temporal en la evaluación[9]. A menudo se sostiene que, a pesar de ser más volátiles a las fluctuaciones y cambios momentáneos a lo largo de la vida, los datos biométricos de comportamiento tienen la ventaja de ser menos intrusivos y rentables[10]. Sin embargo, algunos estudiosos han observado que los datos biométricos del comportamiento podrían introducir más riesgos para la privacidad en comparación con otros tipos de datos[11] biométricos, debido a su capacidad para revelar más información sobre los sujetos de los datos, a veces de naturaleza muy sensible, como el estado[12] de salud.

2.5 Actividad de investigación

El término "actividad de investigación" no tiene una definición clara en el marco jurídico. Según el considerando 159 del RGPD, "el tratamiento de datos personales con fines de investigación científica debe interpretarse de manera amplia, incluyendo, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación con financiación privada".

El Supervisor Europeo de Protección de Datos (SEPD) identifica el objetivo principal de las actividades de investigación en "el aumento del conocimiento y el bienestar colectivo de la

---

8 Véase, por ejemplo, Patrizio Campisi and Daria La Rocca, 'Brain Waves for Automatic Biometric-Based User Recognition', *IEEE Transactions on Information Forensics and Security* 9, no. 5 (May 2014): 782–800, https://doi.org/10.1109/TIFS.2014.2308640.

9 Véase Roman V. Yampolskiy and Venu Govindaraju, 'Behavioural Biometrics: A Survey and Classification', *International Journal of Biometrics* 1, no. 1 (2008): 81, https://doi.org/10.1504/IJBM.2008.018665.

10 Véase Madeena Sultana, Padma Polash Paul, and Marina Gavrilova, 'A Concept of Social Behavioral Biometrics: Motivation, Current Developments, and Future Trends', in *2014 International Conference on Cyberworlds* (2014 International Conference on Cyberworlds (CW), Santander, Cantabria, Spain: IEEE, 2014), 271–78, https://doi.org/10.1109/CW.2014.44.

11 Véase Günter Schumacher, 'Behavioural Biometrics: Emerging Trends and Ethical Risks', in *Second Generation Biometrics: The Ethical, Legal and Social Context*, ed. Emilio Mordini and Dimitros Tzovaras (Springer, 2012).

12 Véase, por ejemplo Marcos Faundez-Zanuy et al., 'Handwriting Biometrics: Applications and Future Trends in e-Security and e-Health', *Cognitive Computation* 12, no. 5 (September 2020): 940–53, https://doi.org/10.1007/s12559-020-09755-z.

sociedad, en lugar de servir principalmente a uno o varios intereses privados"[13]. Por lo tanto, parece que la mera investigación de una nueva tecnología comercial podría no equivaler a una "actividad de investigación" según el marco jurídico actual (véase la sección 4.1 "Protección de datos e investigación científica" del documento "Guidelines on Data Protection Ethical and Legal Issues in ICT Research and Innovation").

3 La tecnología biométrica en la investigación e innovación de las TIC. Directrices

La siguiente sección ofrece una visión general de las medidas prácticas que pueden adoptarse al desarrollar tecnologías biométricas o al emplear dichas tecnologías en el contexto de la investigación e innovación en materia de TIC. Estos pasos pueden ayudar a los investigadores a cumplir con las obligaciones de protección de datos. Las recomendaciones son aplicables a los sistemas biométricos, independientemente de los datos biométricos que generen y procesen (para más información, véase la sección **¡Error! No se encuentra el origen de la referencia.** "Sistema biométrico").

3.1 Fase de diseño

Durante la fase de diseño, los investigadores preparan el terreno identificando los objetivos y las necesidades de la actividad de investigación

3.1.1 Identificar los objetivos, si la actividad se califica como "investigación" y las funciones de las partes interesadas

Los investigadores deben identificar primero el objetivo de su actividad (por ejemplo, realizar un estudio teórico, desarrollar un sistema biométrico, probar uno existente, etc.). Este es un paso importante no sólo para definir los fines para los que se recogerán los datos personales, sino también para ayudar a los investigadores a identificar si la actividad se califica como "investigación" y, en consecuencia, si se aplican las disposiciones legales específicas para las actividades de investigación. El artículo 89.2 del RGPD, por ejemplo, introduce varias excepciones para el tratamiento de datos personales en el contexto de la investigación. En particular, el artículo reconoce que ciertos derechos de los interesados (derecho de acceso, derecho de rectificación, derecho de restricción, derecho de oposición. Para más información, véase "Derechos de los interesados" en la Parte II de estas Directrices) dificultarían o impedirían que algunas investigaciones alcanzaran sus objetivos. Por lo tanto, establece excepciones a estos derechos cuando se cumplen dos *criterios*. En primer lugar, la exención deberá estar explícitamente prevista por los Estados miembros o el Derecho de la Unión. Esto significa que, además de las disposiciones del RGPD, los investigadores pueden quedar exentos de la obligación de cumplir dichos derechos solo en la medida en que existan fundamentos jurídicos específicos en una ley nacional o en la legislación de la UE distinta del RGPD (véase la sección **¡Error! No se encuentra el origen de la referencia.** "Identificar la base jurídica más adecuada"). En segundo lugar, los investigadores aplicarán las medidas técnicas y organizativas adecuadas para salvaguardar los derechos y las libertades de los sujetos de los datos, tal y como

13 Supervisor Europeo de Protección de Datos (SEPD), 'A Preliminary Opinion on Data Protection and Scientific Research' (European Data Protection Supervisor, 6 January 2020).

exige el artículo 89.1 del RGPD. Dado el impacto potencial de cumplimiento para la actividad de investigación, es importante evaluar inmediatamente si la actividad se califica como "investigación".

También es necesario un alcance correcto de las actividades para que los investigadores comprendan los riesgos de protección de datos vinculados a la investigación. Por ejemplo, es probable que los sistemas que se utilicen en la asistencia sanitaria o en la aplicación de la ley requieran resultados más precisos que los empleados para actividades de ocio (como los servicios de transmisión de música). Dado que la precisión de un sistema puede depender en ciertos casos de la cantidad de datos personales que se procesen (por ejemplo, durante el entrenamiento de un algoritmo de IA), la necesidad de mayor precisión puede introducir más riesgos para la protección de datos. Los investigadores deben identificar con claridad qué nivel de precisión tendrá que satisfacer el sistema y definir estrategias para garantizar que dicha precisión se alcance introduciendo el menor nivel de riesgo posible, por ejemplo, limitando la cantidad de datos personales procesados (véase "Minimización de datos" en la sección "Principios" de la Parte II de estas Directrices).

Por último, pero no por ello menos importante, los investigadores tienen que entender su papel y el de otros actores implicados. Los investigadores tienen que examinar su participación en el tratamiento de datos previsto para entender si ellos (es decir, la entidad para la que trabajan) son las entidades con las principales responsabilidades sobre el tratamiento de datos (controlador de datos), si comparten el papel de controlador de datos con otras entidades (controlador conjunto), o si tratan los datos en nombre de otras entidades (procesador de datos). Las distintas funciones implican un reparto diferente de responsabilidades y obligaciones.

3.1.2 Confirmar la necesidad de procesar los datos biométricos

Como ya se ha mencionado, el RGPD prohíbe el tratamiento de categorías especiales de datos personales -por lo tanto, incluyendo los biométricos- a menos que se apliquen exenciones específicas (véase la sección **¡Error! No se encuentra el origen de la referencia.** "Identificar la base jurídica más adecuada"). Por lo tanto, los investigadores que tengan previsto tratar datos biométricos deben estar seguros de que su tratamiento es necesario para alcanzar el objetivo de la actividad de investigación. Por ejemplo, el objetivo de la investigación podría ser desarrollar y probar un nuevo enfoque para aumentar la precisión de los sistemas de detección de rasgos faciales. En este caso, el objetivo no es aumentar la precisión de la identificación única de los individuos, sino sólo la precisión de la detección de los rasgos faciales. Así, los investigadores podrían basarse en imágenes faciales generadas por ordenador en lugar de en fotografías de una persona física existente, eliminando la necesidad de procesar datos personales biométricos. En el caso del desarrollo del sistema, los investigadores también deben considerar cómo procesará el sistema biométrico los datos biométricos después de su despliegue. Los investigadores deben aplicar de antemano todas las medidas técnicas y organizativas para garantizar que se mitigue cualquier riesgo potencial y que el tratamiento de los datos que se produzca después del despliegue se realice de conformidad con el marco legal.

3.2 Fase de preparación

Durante la fase de preparación, los investigadores sientan las bases de la investigación llevando a cabo todos los trabajos preparatorios de la actividad investigadora.

3.2.1 Nombrar a un responsable de la protección de datos

El Delegado de Protección de Datos (DPD) ayuda al responsable o al encargado del tratamiento a cumplir las normas de protección de datos. El artículo 37 del RGPD ordena el nombramiento de un DPD en cinco casos específicos.

Requisitos que exige un Delegado de Protección de Datos	
Requisito 1	"El tratamiento es llevado a cabo por una autoridad u organismo público, excepto los tribunales que actúan en su capacidad judicial", artículo 37.1 del RGPD
Requisito 2	"Las actividades principales del responsable o del encargado del tratamiento consisten en operaciones de tratamiento que, en virtud de su naturaleza, su alcance y/o sus fines, requieren un seguimiento regular y sistemático de los interesados a gran escala", artículo 37.1 del RGPD
Requisito 3	"Las actividades principales del responsable o del encargado del tratamiento consisten en el tratamiento a gran escala de categorías especiales de datos con arreglo al artículo 9", artículo 37.1 del RGPD
Requisito 4	"Las actividades principales del responsable o del encargado del tratamiento consisten en el tratamiento a gran escala de [...] datos personales relativos a las condenas e infracciones penales a que se refiere el artículo 10", artículo 37.1 del RGPD
Requisito 5	"[E]l responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados del tratamiento podrán designar o, cuando así lo exija el Derecho de la Unión o de los Estados miembros, deberán designar un delegado de protección de datos", artículo 37.4 del RGPD

Los requisitos 1 y 3 son especialmente relevantes para este documento. El requisito 1 es pertinente porque no es infrecuente que las instituciones de investigación sean organismos públicos, como en el caso de los hospitales públicos y las universidades públicas. Cuando se da esta situación, el artículo 37.3 del RGPD establece que "podrá designarse un único delegado de protección de datos para varias de estas autoridades u organismos". Por ejemplo, los hospitales públicos podrían no haber designado un DPD, pero podrían confiar en el DPD para prestar su servicio. El requisito 3 es pertinente, ya que menciona el tratamiento de categorías especiales de datos personales -como los datos biométricos- como uno de los tres *criterios para la designación* obligatoria de un DPD. Los otros dos se dan cuando el tratamiento de datos personales se produce en el contexto de una actividad principal y se realiza a gran escala. Los términos "actividades principales" y "a gran escala" no se definen explícitamente en el RGPD. Sin embargo, el Grupo de Trabajo del Artículo 29 proporciona orientación interpretativa en sus Directrices sobre los Delegados de Protección de Datos. En consecuencia, las actividades principales son "operaciones clave para lograr los objetivos del responsable o del encargado del tratamiento"[14], por lo que se excluyen las actividades de apoyo o auxiliares. En el contexto de la investigación e innovación en materia de TIC, esto podría entenderse como cualquier actividad directamente relacionada con la ejecución de la investigación en materia de TIC y la consecución

14 Grupo de Trabajo del Artículo 29, 'Guidelines on Data Protection Officers ("DPOs")', April 2017, 20.

de la innovación en materia de TIC, como en el caso del desarrollo de un sistema biométrico. En cuanto al *criterio de* gran escala, el Grupo de Trabajo del Artículo 29 lo relaciona con "el número de sujetos de datos afectados -ya sea como número específico o como proporción de la población pertinente-, el volumen de datos y/o la gama de diferentes elementos de datos que se tratan, la duración, o la permanencia, de la actividad de tratamiento de datos, [y] la extensión geográfica de la actividad de tratamiento"[15].

Si es necesario nombrar a un DPD, debe hacerse lo antes posible. De hecho, el artículo 39.1(a) del RGPD establece que una de las responsabilidades del DPD es informar y asesorar al responsable del tratamiento durante todas las etapas de la investigación. Por lo tanto, obtener la asistencia de un DPD lo antes posible garantiza que los investigadores reciban una orientación adecuada sobre cómo abordar los requisitos de cumplimiento.

Los contactos del DPD deben publicarse y ponerse a disposición de los interesados.

3.2.2 Identificar el enfoque de recogida de datos

El siguiente paso para los investigadores es identificar si los datos personales van a ser recogidos directamente de los interesados, o indirectamente (por ejemplo, otros investigadores, bases de datos comerciales, etc.). Aunque esto no obliga necesariamente a los investigadores a adoptar una base jurídica concreta (véase la sección **¡Error! No se encuentra el origen de la referencia.** "Identificar la base jurídica más adecuada"), podría influir en dicha decisión. Por ejemplo, si los investigadores deciden recabar datos directamente de los interesados, podrían ser más favorables a utilizar el consentimiento como base jurídica, ya que de todos modos se va a establecer una relación directa con los interesados. Además, según los artículos 13 y 14 del RGPD, la elección de un enfoque directo o indirecto para la recogida de datos cambia la información que los responsables del tratamiento deben proporcionar a los interesados.

Información que debe proporcionarse a los interesados según el enfoque de la recogida		
	Directamente	**Indirectamente**
La identidad y los datos de contacto del responsable del tratamiento	⍰	⍰
En su caso, la identidad y los datos de contacto del representante del responsable del tratamiento	⍰	⍰
Los datos de contacto del delegado de protección de datos	⍰	⍰
Los fines del tratamiento	⍰	⍰
Las categorías de datos personales en cuestión		⍰
La base legal para el tratamiento	⍰	⍰

15 Grupo de Trabajo del Artículo 29, 21.

En su caso, los intereses legítimos perseguidos por el responsable del tratamiento o por terceros	☐	☐
Destinatarios o categorías de destinatarios de los datos personales	☐	☐
La intención del responsable del tratamiento de transferir datos personales a un tercer país u organización internacional	✓	☐
En caso de transferencia, la existencia o ausencia de una decisión de adecuación por parte de la Comisión o, en su caso, la referencia a las garantías y los medios para obtener una copia de los datos	☐	☐
El período durante el cual se almacenarán los datos personales o, si no es posible, los criterios utilizados para determinar dicho período	☐	☐
La existencia del derecho a solicitar el acceso y la rectificación o supresión de los datos o la limitación del tratamiento de los mismos, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos	☐	☐
En el caso del "consentimiento explícito" como base jurídica del tratamiento, la existencia del derecho a retirar el consentimiento en cualquier momento	☐	☐
Derecho a presentar una reclamación ante una autoridad de control	☐	☐
La fuente de los datos personales y, en su caso, si proceden de fuentes de acceso público		☐
Si el suministro de datos es un requisito legal o contractual, o un requisito para celebrar un contrato, y si el interesado está obligado a proporcionar los datos y las consecuencias de no hacerlo	☐	
La existencia de la toma de decisiones automatizada, incluida la elaboración de perfiles	☐	☐
En el caso de la toma de decisiones automatizada, información sobre la lógica implicada, el significado del tratamiento y sus consecuencias previstas para el sujeto	☐	☐

El RGPD reconoce que puede haber casos en los que este deber de información no sea aplicable y enumera las excepciones en el artículo 14.5 del RGPD. Estas excepciones son:

- El interesado ya dispone de la información;
- El suministro de dicha información:
    - resulta imposible;
    - implicaría un esfuerzo desproporcionado,
    - pueda hacer imposible o perjudicar gravemente la consecución de los objetivos de dicho tratamiento.

A este respecto, es importante aclarar que esta excepción se aplica en particular al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en cumplimiento de las condiciones y garantías consagradas en el artículo 89.1 del RGPD.

Además, en estos casos, el responsable del tratamiento adoptará las medidas adecuadas para proteger los derechos y libertades del interesado y sus intereses legítimos, incluida la puesta a disposición del público de la información;

- El responsable del tratamiento está obligado por la legislación de la UE o de los Estados miembros a obtener o revelar los datos personales; o
- Cuando los datos personales deban ser confidenciales en virtud de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación legal de secreto.

Independientemente de la forma en que se recojan los datos, el responsable del tratamiento adoptará las medidas adecuadas para garantizar que los datos sean exactos y estén actualizados (por ejemplo, mediante una auditoría periódica de exactitud). Recoger los datos directamente de los interesados puede ayudar a reducir el riesgo de inexactitud (especialmente en lo que respecta a los datos biométricos de comportamiento, que pueden cambiar con el tiempo). Asimismo, el responsable del tratamiento deberá garantizar la transparencia en todas las fases del proceso (véase "Legalidad, equidad y transparencia" en la sección "Principios" de la Parte II de estas Directrices). Para una explicación más detallada sobre el derecho a la información y sus matices, véase "Derechos del interesado" en la Parte II de estas Directrices.

3.2.3 Identificar la base jurídica más adecuada

Uno de los pasos más cruciales desde el punto de vista de la protección de datos es la identificación de la base jurídica para el tratamiento de los datos personales, que se enumeran en el artículo 6 del RGPD. Sin embargo, como ya se ha mencionado, el tratamiento de datos biométricos está prohibido y sólo puede producirse cuando se aplican exenciones específicas. Estas están previstas en el artículo 9.2 del RGPD y son de dos tipos. Las que son inmediatamente válidas y aplicables, y las que requieren una legislación adicional de la Unión o de los Estados miembros antes de poder ser empleadas para justificar un tratamiento de datos biométricos.

Bases legales disponibles previstas por el RGPD para el tratamiento de datos biométricos	
	Requiere legislación adicional de la UE o de los Estados miembros

Consentimiento explícito	
Empleo, seguridad social y protección social	?
Intereses vitales	
Actividades de asociaciones y otras entidades sin ánimo de lucro	
Los datos han sido publicados por el interesado	
Reclamaciones legales o actos judiciales	
Interés público sustancial	?
Salud o asistencia social	?
Interés público sanitario	?
Archivo, investigación y estadísticas	?

Cuando se aplica una de estas excepciones, el responsable del tratamiento puede seleccionar una de las bases jurídicas enumeradas en el artículo 6 del RGPD y tratar los datos personales en consecuencia.

Entre las diez exenciones del artículo 9.2 del RGPD, dos son especialmente relevantes en el presente documento. La primera es el requisito del "consentimiento explícito". En el contexto del tratamiento de datos biométricos, el consentimiento de los interesados deberá ser "explícito", lo que significa que deberá ser una declaración clara, específica e inequívoca de que los interesados consienten que sus datos biométricos sean tratados para los fines específicos identificados por el responsable[16] del tratamiento. Por ejemplo, en caso de tratamiento de datos biométricos extraídos de fotografías, no bastará con recoger el consentimiento de los interesados sobre el tratamiento de dichas fotografías. Se informará a los sujetos de que se extraerán y tratarán características biométricas, y se recogerá el consentimiento explícito.

16 El RGPD reconoce en el considerando 33 que podría no ser posible identificar plenamente la finalidad del tratamiento de datos en el momento de la recogida de los mismos y que, por lo tanto, debe permitirse a los interesados dar su consentimiento para determinados "ámbitos de la investigación científica". El punto planteado por el considerando 33 y una serie de retos interpretativos se han investigado en el documento "Issues and gaps analysis on informed consent in the context of ICT research and innovation".

Ejemplo: Consentimiento *versus* consentimiento explícito	
Consentimiento	**Consentimiento explícito**
"Por favor, proporcione una foto suya de frente, tomada en un entorno bien iluminado. La foto se utilizará para extraer características biométricas con el fin de desarrollar un nuevo sistema de reconocimiento biométrico."	"A - Por favor, proporcione una foto suya de frente, tomada en un entorno bien iluminado. B - La imagen se utilizará para extraer características biométricas con el fin de desarrollar un nuevo sistema de reconocimiento biométrico. C - Antes de enviar la fotografía, marque la siguiente casilla para indicar que da su consentimiento como interesado para que su fotografía sea tratada con el fin de extraer características biométricas que serán tratadas de acuerdo con la finalidad descrita en el punto B. Marque la casilla □"

Al hablar de consentimiento en el contexto de la investigación, también es importante distinguir entre el consentimiento para ser participante en el estudio y el consentimiento para que se procesen los datos personales. Se trata de dos tipos de consentimiento diferentes y deberán recogerse de forma independiente[17]. El equipo de investigación puede basarse en un único formulario de consentimiento, siempre que éste distinga claramente entre los dos tipos de consentimiento y no los recoja en un único acuerdo (para más información, véase el documento "Issues and gaps analysis on informed consent in the context of ICT research and innovation" en: https://www.panelfit.eu/wp-content/uploads/2020/11/D21-Issues-and-gaps-analysis-on-informed-consent-in-the-context-in-ICT-research-and-Innovation.pdf).

Otra exención al tratamiento de datos personales de categoría especial que es pertinente a efectos de este documento es la exención para el tratamiento necesario para las actividades de investigación. La exención requiere que se cumplan dos *criterios* para que sea aplicable. En primer lugar, el tratamiento debe estar sujeto a las garantías técnicas y organizativas apropiadas según el artículo 89.1 del RGPD. En segundo lugar, debe existir una legislación de la Unión o de los Estados miembros que proporcione un fundamento jurídico para el tratamiento en el contexto de una actividad de investigación. Este último *criterio* implica que la exención para fines de investigación puede no ser aplicable en todas partes. Por lo tanto, los investigadores deben llevar a cabo una revisión de las legislaciones nacionales de todos los Estados en los que se va a realizar la investigación para identificar si dichas normas están presentes (véase "Estudio comparativo de los informes nacionales" en https://www.panelfit.eu/national-reports/).

17 Véase European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679', May 2020, 30; European Data Protection Board, 'Opinion 3/2019 Concerning the Questions and Answers on the Interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation', 2019.

3.2.4 Crear un repositorio de documentación de apoyo

El RGPD exige a los responsables del tratamiento no sólo que cumplan con las obligaciones en materia de protección de datos, sino también que sean capaces de demostrar su cumplimiento de dichas obligaciones y de los principios consagrados en la norma. Esto significa que el responsable del tratamiento deberá mantener los registros y la documentación adecuados relativos al tratamiento de datos y a la gobernanza de dicho tratamiento.

Aparte de un conjunto limitado de documentos que son claramente obligatorios (como el registro de las actividades de tratamiento exigido por el artículo 30 del RGPD), es obligación del responsable del tratamiento identificar cuáles son los documentos necesarios para demostrar el cumplimiento. Las siguientes tablas presentan la lista de documentos exigidos por el RGPD con la ubicación correspondiente en el texto. Debe considerarse una base mínima y no una lista de comprobación exhaustiva. De hecho, aunque no es obligatorio, pueden ser necesarios otros documentos para demostrar el cumplimiento (por ejemplo, informes de consultas previas con las autoridades de control, descripción de las medidas técnicas y organizativas aplicadas, etc.)

Documentación: lista de control		
1	Política de protección de datos personales	Artículo 24.2
2	Aviso de privacidad	Artículos 12, 13, 14
3	Política de conservación de datos	Artículos 5, 13, 17 y 30
4	Calendario de conservación de datos	Artículo 30
5	Registro de actividades de procesamiento (si procede)	Artículo 30
6	Formulario de consentimiento (si procede)	Artículos 6, 7, 9
7	Acuerdo de procesamiento de datos con los proveedores	Artículos 28, 32, 82
8	Evaluación del impacto de la protección de datos	Artículo 35
9	Nombramiento de un representante de la UE (si procede)	Artículo 27
10	Procedimiento de respuesta y notificación de la violación de datos	Artículos 4, 33, 34
11	Notificación de la violación de datos a la Autoridad de Supervisión (si procede)	Artículo 33
12	Notificación de la violación de datos a los interesados (si procede)	Artículo 34

Algunos documentos son necesarios sólo cuando se aplican *criterios específicos*.

Documentación obligatoria condicionada	
Registro de actividades de procesamiento	Si se trata de 250 empleados o más, salvo que el tratamiento pueda suponer un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos personales relativos a condenas e infracciones penales
Formulario de consentimiento	Si el tratamiento se basa en el consentimiento como base jurídica, y si el tratamiento se ha recogido de forma[18] escrita
Nombramiento de un representante de la UE	Si el tratamiento afecta a sujetos de la UE y es realizado por un responsable o un encargado del tratamiento no establecido en la UE, a menos que sea ocasional, no implique un tratamiento a gran escala, ni categorías especiales de datos, ni datos personales relativos a condenas e infracciones penales, y sea improbable que suponga un riesgo para los derechos y las libertades de las personas físicas
Notificación de la violación de datos a la Autoridad de Supervisión	Sólo cuando se produzca una violación de datos que pueda suponer un riesgo para los derechos y libertades de las personas físicas
Notificación de la violación de datos a los interesados	Cuando se produzca una violación de datos que pueda suponer un alto riesgo para los derechos y libertades de las personas físicas o, cuando sea improbable que suponga un alto riesgo, si la autoridad de control lo requiere

Para que el mantenimiento de los registros sea más fácil y coherente, el investigador debe preparar plantillas adecuadas para los pasos que deben documentarse o consultar con el DPD o con su departamento jurídico en lugar del DPD, para comprobar si existen plantillas en la organización.

Antes de comenzar con la recogida y el tratamiento de datos personales, los investigadores deben recopilar la documentación sobre protección de datos ya disponible en su organización, y crear un *expediente* específico que contenga toda la documentación pertinente. Los nuevos documentos deben añadirse al *expediente* tan pronto como se creen. El objetivo del *expediente* es registrar los pasos y las decisiones tomadas por los investigadores y otros interesados en la protección de datos que participan en la actividad de investigación y presentar información suficiente para demostrar que se ha mantenido el cumplimiento durante todo el proceso.

El equipo de investigación debe considerar el *expediente* no como una mera obligación de registro. El *expediente* debe actuar como la formalización de las medidas prácticas que el equipo de investigación adopta para garantizar la salvaguarda de los datos personales. Por ejemplo, no basta con tener un procedimiento de notificación y respuesta a la violación de datos. Los investigadores deben ser capaces de demostrar que el procedimiento puede ponerse en marcha de forma rápida y eficaz, en caso de necesidad.

18 De hecho, el RGPD no exige que el consentimiento se recoja por escrito. Para más información, véase European Data Protection Board, 'Guidelines 05/2020 on Consent', 16.

3.2.5 Verificar si es necesaria una evaluación de impacto de la protección de datos

Según el Grupo de Trabajo del Artículo 29, una Evaluación de Impacto sobre la Protección de Datos (EIPD) es "un proceso diseñado para describir el tratamiento [de datos personales], evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales, evaluándolos y determinando las medidas para hacerles frente"[19].

El artículo 35.1 del RGPD exige a los responsables del tratamiento que realicen una EIPD cuando el tratamiento de datos pueda suponer un alto riesgo para los derechos y libertades de las personas físicas. Por lo tanto, la EIPD no siempre es obligatoria. Sin embargo, los responsables del tratamiento deben realizar siempre la evaluación preliminar de riesgos para determinar si es probable que el tratamiento dé lugar a riesgos elevados para los derechos y libertades de las personas físicas. Esta evaluación preparatoria forma parte del proceso de la EIPD. Por lo tanto, se puede decir que ciertos elementos de la EIPD son obligatorios para, al menos, determinar si es necesaria una EIPD.

Los riesgos para los derechos y libertades de los interesados se mencionan en el considerando 75 del RGPD. Se trata de los riesgos que podrían provocar un daño físico, material o inmaterial al interesado en cuestión (por ejemplo, que se le deniegue el acceso a un servicio tras una identificación falsa negativa).

Ejemplos de riesgos para los derechos y libertades	
Discriminación	Robo de identidad o fraude
Pérdida financiera	Daño a la reputación
Pérdida de la confidencialidad del secreto profesional	Anulación no autorizada de la seudonimización
Desventaja económica o social	Prevención del ejercicio del control de los datos personales

El RGPD no define el concepto de "alto riesgo". Sin embargo, el Grupo de Trabajo del Artículo 29 elaboró una lista de nueve *criterios que* los responsables del tratamiento pueden seguir para entender si el tratamiento puede considerarse de alto riesgo[20].

***Criterios* de tratamiento de alto riesgo**	
Criterio 1	Evaluación o puntuación (por ejemplo, elaboración de perfiles)
Criterio 2	Toma de decisiones automatizada con efectos legales o similares significativos

19 Grupo de Trabajo del Artículo 29, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679', October 2017, 4.

20 Grupo de Trabajo del Artículo 29, 9–11.

Criterio 3	Control sistemático
Criterio 4	Datos sensibles o de carácter muy personal
Criterio 5	Datos procesados a gran escala
Criterio 6	Cotejar o combinar conjuntos de datos (más allá de las expectativas razonables del interesado)
Criterio 7	Datos relativos a personas vulnerables
Criterio 8	Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas
Criterio 9	Cuando el tratamiento impide por sí mismo que los interesados ejerzan un derecho o utilicen un servicio o un contrato

Los investigadores que realicen sus actividades de investigación deben tener en cuenta todos ellos para saber si es necesario realizar una EIPD. Sin embargo, los *criterios* cuatro y ocho son especialmente relevantes a efectos de este documento. *El criterio* cuatro es importante cuando se procesan datos biométricos durante la actividad de investigación. *El criterio ocho es importante en el* contexto de la investigación sobre las TIC, ya que esta actividad podría introducir una nueva tecnología para procesar los datos (por ejemplo, formas innovadoras de capturar y analizar muestras de voz).

El artículo 35.4 del RGPD exige que las autoridades nacionales de control publiquen la lista de actividades de tratamiento de datos para las que es obligatoria una EIPD[21]. Esto podría ofrecer más orientación sobre lo que constituye una EIPD obligatoria de tratamiento, y los investigadores deben prestar atención a la posición de las autoridades de supervisión pertinentes. Asimismo, los investigadores deben solicitar orientación al DPD de la organización, dada la complejidad de la tarea en cuestión.

Para poder demostrar el cumplimiento, debe documentarse y conservarse la evaluación de si el tratamiento puede dar lugar a riesgos elevados para los derechos y libertades de las personas físicas.

3.2.6 Realizar una EIPD (si es necesario)

No existe una forma estándar de realizar una EIPD. Sin embargo, el artículo 35.7 del RGPD exige unos elementos específicos que deben estar siempre presentes. Estos son:

- una descripción sistemática de las operaciones de tratamiento previstas;
- los fines de las operaciones de tratamiento;

21 En este sentido, las autoridades nacionales de control han publicado en sus sitios web la lista correspondiente. En algunos casos, el Comité Europeo de Protección de Datos ya ha emitido un dictamen al respecto sobre las actividades incluidas en cada lista. Para más información, véase European Data Protection Board, 'Opinion 6/2019 on the Draft List of the Competent Supervisory Authority of Spain Regarding the Processing Operations Subject to the Requirement of a Data Protection Impact Assessment (Article 35.4 GDPR)', March 2019.

- una evaluación de la necesidad de las operaciones de tratamiento en relación con los fines;
- una evaluación de la proporcionalidad de las operaciones de tratamiento en relación con los fines;
- una evaluación de los riesgos para los derechos y libertades de los interesados;
- las medidas técnicas y organizativas previstas para hacer frente a los riesgos.

Los investigadores pueden incluir otros elementos para describir mejor el tratamiento y los riesgos subyacentes. Asimismo, si el responsable del tratamiento se da cuenta, tras haber realizado una EIPD, de que los riesgos para los derechos y las libertades del interesado no están adecuadamente mitigados por las medidas previstas para hacer frente a dichos riesgos, el responsable del tratamiento deberá solicitar una consulta previa a la autoridad de control siguiendo lo dispuesto en el artículo 36 del RGPD.

La ley no sanciona un formato para la EIPD. Éste puede ser elegido libremente por el responsable del tratamiento. Sin embargo, algunas autoridades de protección de datos han creado plantillas que los responsables del tratamiento pueden adoptar[22].

La EIPD no es una actividad puntual, sino un proceso continuo. Por ello, puede ser necesario realizar varias evaluaciones a lo largo del tiempo, por ejemplo, cuando los elementos del contexto cambian o cuando se dispone de nueva información.

Los resultados de las EIPD se registrarán y almacenarán como parte de la documentación de protección de datos.

3.2.7 Aplicar medidas de mitigación de riesgos

Según el considerando 78 del RGPD, "la protección de los derechos y libertades de las personas físicas en relación con el tratamiento de datos personales exige que se adopten las medidas técnicas y organizativas adecuadas para garantizar el cumplimiento de los requisitos del [RGPD]". Esta disposición, que representa una piedra angular del marco jurídico, se desarrolla aún más para el caso específico del tratamiento con fines de investigación. El considerando 156 del RGPD y el artículo 89 del RGPD exigen la aplicación de "garantías adecuadas", subrayando la importancia de salvaguardar los derechos y libertades de las personas físicas.

El RGPD no proporciona una lista exhaustiva de medidas técnicas y organizativas, dejando al responsable del tratamiento la tarea de identificarlas y evaluar su eficacia para mitigar los riesgos para los interesados. Asimismo, los investigadores deben considerar la posibilidad de realizar una auditoría externa de seguridad y protección de datos, para confirmar que las medidas de seguridad y cumplimiento son sólidas, y para demostrar aún más el cumplimiento del principio de responsabilidad.

Ejemplos de medidas técnicas y organizativas	
Medidas técnicas	**Medidas organizativas**

22 Véase, por ejemplo, Commision Nationale Informatique & Libertés, 'Privacy Impact Assessment (PIA). Templates', February 2018.

Anonimización o seudonimización de datos[23]	Políticas de seguridad
Cifrado de la comunicación	Planes de gestión de datos
Protección de los datos contra el acceso no autorizado	Programa de formación del personal
Evaluación de la vulnerabilidad / Pruebas de penetración	Auditorías y evaluaciones periódicas

3.3 Fase de ejecución

Una vez preparada adecuadamente la actividad de investigación, los investigadores pueden iniciar su trabajo y las operaciones de tratamiento de datos correspondientes. Esta etapa comienza con la recogida de los datos de acuerdo con el plan definido durante la fase de preparación.

3.3.1 Tratamiento de datos biométricos

Una vez que los investigadores han obtenido los datos biométricos necesarios, éstos pueden ser procesados para extraer los rasgos biométricos que se emplearán en la investigación. Aunque teóricamente es posible hacerlo "manualmente" (por ejemplo, mapeando manualmente los rasgos faciales en las fotografías, como la distancia entre los ojos, la forma de la cara, la altura de las orejas, etc.)[24], hoy en día este enfoque se considera generalmente inviable y se sustituye por medios automatizados basados a menudo en la tecnología de la inteligencia artificial (para una orientación específica, consúltese la Parte III de estas Directrices). Independientemente de esta distinción, cualquier actividad de tratamiento debe llevarse a cabo adoptando todas las garantías y precauciones establecidas durante la fase de preparación.

3.3.2 Desarrollo de sistemas biométricos e interfaces de usuario

Si el objetivo de la investigación es desarrollar un sistema biométrico, los investigadores deben poner especial cuidado en la creación de la interfaz de usuario, sobre todo si el sistema va a ser utilizado por el público. La interfaz debe diseñarse de la forma más fácil posible para el usuario con el fin de promover la transparencia y facilitar a los interesados el ejercicio de su derecho a la información. Hay tres aspectos principales que los investigadores deben tener en cuenta: la información disponible a través de la interfaz de usuario, las funcionalidades accesibles a través de la interfaz de usuario y la facilidad de uso general de la interfaz.

En primer lugar, el responsable del tratamiento se asegurará de que toda la información facilitada a los interesados con arreglo a los artículos 13 y 14 del RGPD esté disponible a través de la interfaz de usuario. Ésta debe ser fácilmente accesible y presentarse de forma clara y fácil de

23 Véase también la sección **¡Error! No se encuentra el origen de la referencia.**Borrado o destrucción de datos para más información sobre la anonimización. Para más información técnica, consulte "Identificación", "Pseudonimización" y "Anonimización" en la sección "Conceptos principales" de la Parte II de estas Directrices)

24 Algunas técnicas de reconocimiento biométrico se descubrieron por primera vez como técnicas manuales, e incluso son anteriores al nacimiento del sistema informático. Véase, por ejemplo Mark Maguire, 'The Birth of Biometric Security', *Anthropology Today* 25, no. 2 (April 2009): 9–14, https://doi.org/10.1111/j.1467-8322.2009.00654.x..

entender. Por ejemplo, el sistema puede presentar un botón visible en el que los interesados puedan hacer clic para abrir una ventana emergente con la información. Es aconsejable que la información esté fácilmente disponible en el sistema y evitar, en la medida de lo posible, los enlaces a repositorios o sitios web externos para minimizar el riesgo de inaccesibilidad debido, por ejemplo, a problemas de conectividad. La interfaz de usuario también debe aprovechar las capacidades del dispositivo a través del cual se accede a la información. Por ejemplo, en caso de que el sistema funcione en un smartphone, podría ofrecer la opción de llamar o enviar un correo electrónico directamente al DPD con un simple clic[25].

En segundo lugar, la interfaz de usuario debe presentar un conjunto de funcionalidades que faciliten a los interesados el ejercicio de sus derechos (siempre que no exista una exención para la aplicación de dichos derechos. Véase la sección **¡Error! No se encuentra el origen de la referencia.** "Identificar el enfoque de la recogida de datos"). Por ejemplo, la interfaz de usuario debe permitir a los interesados acceder a sus datos personales y rectificarlos o eliminarlos (en la medida en que ello no imposibilite la consecución de la finalidad del tratamiento). Disponer de funcionalidades específicas accesibles a los interesados no sólo les facilitará el ejercicio de sus derechos, sino que también debería reducir la carga de los responsables del tratamiento, ya que muchas de estas solicitudes serán realizadas directamente por los interesados. Por ejemplo, los usuarios de sistemas de reconocimiento facial pueden necesitar actualizar sus fotos (por ejemplo, después de una operación). Darles una forma directa de hacerlo, en lugar de tener que ponerse en contacto con el responsable del tratamiento, podría incentivarles a mantener los datos actualizados y, por lo tanto, también garantizará el cumplimiento del principio de exactitud. Sin embargo, la introducción de estas funcionalidades también puede aumentar los riesgos para los derechos y libertades de los interesados. Por ejemplo, en caso de que la cuenta de un usuario sea violada, esta "opción de autoservicio" da al atacante el control total de los datos personales de los interesados. Por lo tanto, el responsable del tratamiento de datos deberá garantizar siempre que cualquier riesgo adicional introducido por funcionalidades específicas se mitigue adecuadamente mediante medidas de seguridad apropiadas (por ejemplo, autenticación multifactor, actualización obligatoria de la contraseña, etc.). En caso de que los investigadores no puedan mitigar adecuadamente los riesgos tras la introducción de nuevas funcionalidades, deberán consultar previamente a la autoridad de control pertinente o evitar la introducción de las funcionalidades hasta que puedan encontrar un enfoque de mitigación viable.

En tercer lugar, la facilidad de uso general de la interfaz deberá promover la transparencia y evitar imponer cargas innecesarias a los interesados a la hora de ejercer sus derechos. Una interfaz de usuario adecuada debe tener en cuenta elementos como las características de los sujetos de los datos (por ejemplo, idioma, datos demográficos, etc.), la forma en que los usuarios interactúan con el sistema (por ejemplo, en un PC, un teléfono inteligente, un hardware personalizado, etc.), el lugar en el que los usuarios interactúan con el sistema (por ejemplo, en casa, en un espacio público, etc.), las opciones de retroceso (por ejemplo, cuando los usuarios cambian accidentalmente determinados ajustes) y muchos otros elementos. Además, los desarrolladores deben tener en cuenta que el sistema puede ser utilizado por sujetos vulnerables, como niños o personas con discapacidad visual. Por ello, la interfaz debe diseñarse de forma que les ayude a utilizar el sistema (por ejemplo, voz a texto, ampliación del texto, etc.).

25 No obstante, los contactos también se mostrarán, y el sistema no impondrá ningún medio de comunicación específico.

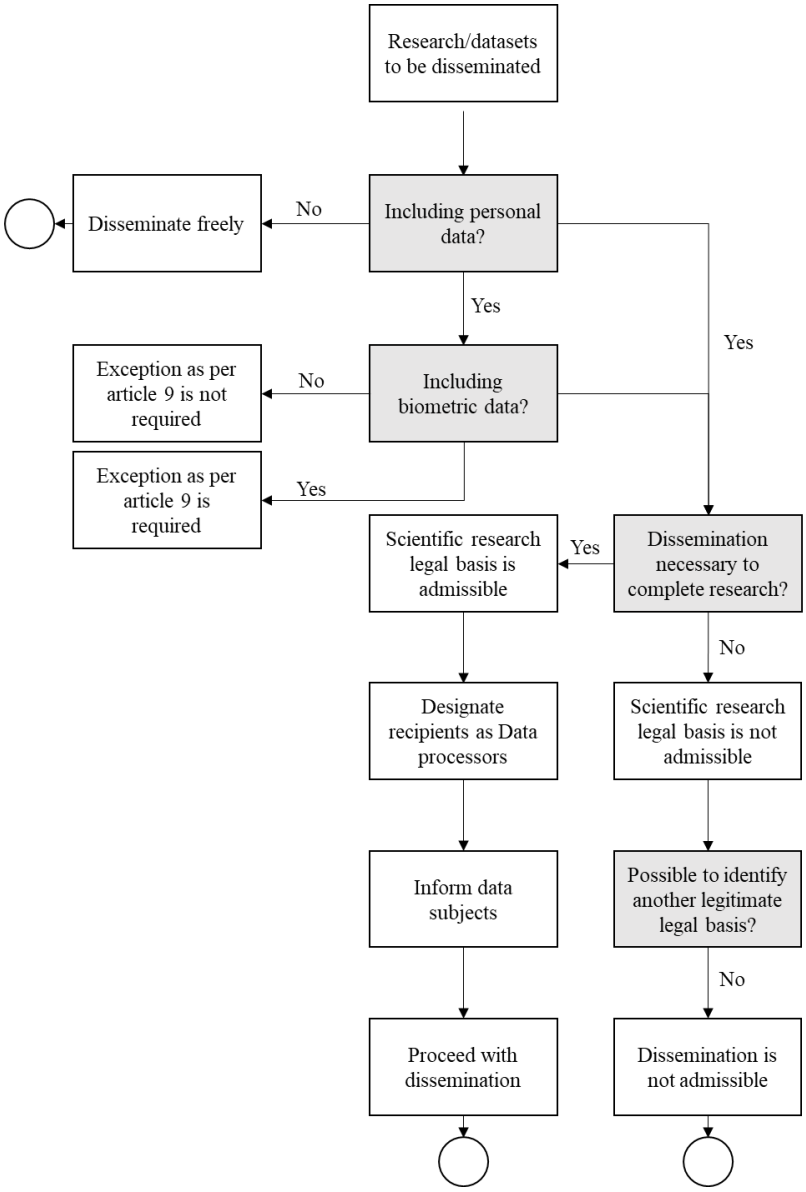
3.3.3 Pruebas del sistema biométrico

El último paso antes de desplegar el sistema biométrico es probarlo y validar sus resultados. Hay dos escenarios posibles. En el primero hay que recoger nuevos datos, mientras que en el segundo los investigadores emplean los mismos datos procesados durante la fase de desarrollo. El primer escenario se da cuando, por ejemplo, se traen nuevos sujetos específicamente para probar el sistema. En este caso, el responsable del tratamiento necesita realizar los pasos ya mencionados en relación con la fase de preparación. En el segundo escenario, los investigadores tienen que considerar si esta prueba adicional estaba comprendida entre los fines iniciales (para más información, véase "Limitación de la finalidad" en la parte II, sección "Principios"). En efecto, "probar el sistema" configura un tratamiento diferente al de "desarrollar el sistema" y, por lo tanto, podría requerir una base jurídica distinta, especialmente cuando ambos tratamientos requieren conjuntos de datos diferentes. En estos casos, los investigadores no deben suponer que, puesto que han cumplido con las obligaciones relacionadas con el desarrollo del sistema, cumplen automáticamente con las relacionadas con las pruebas. Es importante que consideren este paso con un enfoque crítico y tengan como objetivo prioritario minimizar los riesgos para los derechos y libertades de los interesados.

3.3.4 Difusión de los resultados

Al final de la actividad de investigación, los investigadores pueden decidir difundir su trabajo. Si la difusión no incluye los datos personales tratados durante la investigación, el trabajo puede difundirse a otras partes interesadas. Si la difusión sí incluye los datos procesados durante la investigación (por ejemplo, poner los datos a disposición de la comunidad científica para su revisión por pares), deberán tomarse medidas adicionales. La difusión de datos personales constituye una operación de tratamiento según el artículo 4.2 del RGPD y -como se ha descrito anteriormente- cualquier operación de tratamiento que incluya datos biométricos estará prohibida a menos que se apliquen exenciones. Por lo tanto, los investigadores deben repetir los pasos ya descritos en **¡Error! No se encuentra el origen de la referencia.** antes de proceder a la difusión. En particular, si el responsable del tratamiento se basa en la base jurídica de la "investigación científica", y si se cumplen todos los requisitos para adoptar dicha base jurídica (véase la sección **¡Error! No se encuentra el origen de la referencia.** 'Identificar la base jurídica más adecuada'), es posible distinguir además dos escenarios. En el primero, el equipo de investigación (Equipo A) ha completado la actividad de investigación y pretende difundir los datos en beneficio de otros equipos de investigación (Equipo B). En este caso, la difusión no es una operación necesaria para alcanzar los objetivos de investigación del equipo A, pero podría ser necesaria para los objetivos de investigación del equipo B. Por lo tanto, el equipo A no puede invocar la base jurídica de la "investigación científica". De ello se desprende que el Equipo A no tiene ningún fundamento jurídico para compartir los datos con el Equipo B, o con cualquier otro destinatario, a menos que se encuentre una base jurídica diferente (por ejemplo, el Equipo A puede recabar el consentimiento explícito con el fin de compartir los datos con el Equipo B). En el segundo escenario, el Equipo A se da cuenta, tras la recogida de los datos personales, de que no tiene la capacidad adecuada (por ejemplo, técnica) para procesar los datos y continuar con la investigación. Por lo tanto, el Equipo A decide confiar en la capacidad del Equipo B para procesar los datos. En esta situación, la difusión de los datos al Equipo B es un paso necesario para lograr los objetivos de investigación del Equipo A, y el Equipo B debe ser nombrado "encargado del tratamiento" de acuerdo con las disposiciones del artículo 28 del RGPD. El artículo 4.8 del RGPD define al encargado del tratamiento como "una persona física o jurídica, una autoridad pública, una agencia u otro organismo que trate datos personales por cuenta del

responsable del tratamiento". La designación y las funciones del encargado del tratamiento se comunicarán al interesado antes de la transferencia, y se regirán por un contrato o por el Derecho de la Unión o de los Estados miembros, que contendrá al menos el objeto y la duración del tratamiento, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y las categorías de interesados, así como las obligaciones y los derechos del responsable del tratamiento.



En caso de que sea necesario transferir datos personales fuera del Espacio[26] Económico Europeo, y siempre que dicha transferencia no esté sujeta a una o varias de las excepciones enumeradas en el artículo 49 del RGPD[27], deberán tomarse medidas adicionales. El RGPD prevé una serie de instrumentos para la transferencia internacional de datos. Sin embargo, no todos son aplicables en

26 Que incluye a todos los Estados miembros de la UE y a Islandia, Liechtenstein y Noruega.

27 Para más información, véase también European Data Protection Board, 'Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679', May 2018.

la actualidad, ya que las autoridades competentes todavía están trabajando para formalizar algunos de ellos.

Transferencia internacional de datos	
Perseguir una decisión de adecuación	Aplicable
Aplicación de las cláusulas estándar de protección de datos	Aplicable
Persecución de normas corporativas vinculantes	Aplicable
Cumplir con los códigos de conducta	Planificado
Perseguir los mecanismos de certificación	Planificado
Persecución de un instrumento jurídicamente vinculante entre autoridades u organismos públicos	Planificado[28]

En el primer caso (perseguir la decisión de adecuación), los datos pueden transferirse a otros estados de la UE si existe una decisión de adecuación por parte de la Comisión Europea. Se puede adoptar una decisión de adecuación si el otro Estado ofrece un nivel de protección de datos adecuado a la norma[29] europea. En el segundo caso, (perseguir las cláusulas estándar de protección de datos), los datos pueden transferirse si existe un acuerdo entre el exportador y el importador de datos y si dichos acuerdos contienen una serie de cláusulas estándar relativas a la protección de datos que han sido aprobadas previamente por la Comisión Europea[30]. En el tercer caso, si la transferencia extraterritorial se produce dentro de la misma entidad (por ejemplo, una transferencia entre dos sucursales de un grupo internacional), los datos pueden transferirse si existen normas corporativas vinculantes que ofrezcan garantías de protección de datos según el artículo 47 del RGPD y estén aprobadas por la autoridad de supervisión de protección de datos competente.

3.3.5 Borrado o destrucción de datos

Al final de las pruebas, el responsable del tratamiento debe suprimir el conjunto de datos utilizado para este fin, a menos que exista una necesidad legal de mantenerlos, por ejemplo, con el fin de perfeccionar o evaluar el sistema, o para otros fines compatibles con aquellos para los que se recogieron de acuerdo con las condiciones establecidas por el artículo 9.2 del RGPD.

28 A partir de julio de 2021, estas tres opciones para la transferencia internacional de datos están previstas, pero aún no se han aplicado.

29 La lista de países reconocidos mediante una decisión de adecuación puede consultarse en https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

30 La versión más actualizada de las cláusulas tipo puede encontrarse en European Commission, 'Implementing Decision 2021/914 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council' (2021), https://doi.org/10.5040/9781782258674.

Véase: "Identificación", "Pseudonimización" y "Anonimización" dentro de la sección "Conceptos principales" de la Parte II de estas Directrices).

4 La tecnología biométrica en la investigación e innovación de las TIC. Estudio de caso

La siguiente sección presenta una aplicación de los contenidos de la sección **¡Error! No se encuentra el origen de la referencia.** 'La tecnología biométrica en la investigación e innovación de las TIC. Directrices". El estudio de caso no se refiere a ninguna situación real.

Un equipo de desarrolladores de TIC decide diseñar un sistema de reconocimiento de manos para agilizar el proceso de identificación de los empleados a la entrada de los centros de trabajo. El objetivo de los investigadores es proponer un enfoque que preserve la privacidad, entender su viabilidad, desarrollar la tecnología correspondiente y publicar un artículo con los resultados.

El equipo de desarrolladores decide poner énfasis en tres aspectos:

- El sistema cumple plenamente las normas de protección de datos
- El sistema es lo suficientemente eficaz como para ser adoptado por las organizaciones
- El sistema no es percibido por los usuarios -empleados- como demasiado invasivo

Todos los desarrolladores trabajan para la misma empresa privada, Developing Inc. Ésta tiene su sede en el ficticio Estado europeo de Developonia. En el escenario, Developing Inc. actúa como controlador de datos.

4.1 Fase de diseño

4.1.1 Identifique los objetivos y si la actividad puede calificarse de "investigación".

Los promotores establecen los siguientes objetivos:

- diseñar un enfoque para agilizar la identificación de los empleados en los centros de trabajo
- para comprender su viabilidad
- desarrollar y probar la tecnología correspondiente
- publicar un artículo con los resultados.

Informados por los objetivos, los promotores proceden a evaluar si el proyecto es una "investigación científica". Para ello, tienen en cuenta la definición del SEPD (véase la sección **¡Error! No se encuentra el origen de la referencia.** "Actividad de investigación") y evalúan si la actividad contribuye a "aumentar el conocimiento y el bienestar colectivo de la sociedad, en lugar de servir principalmente a uno o varios intereses privados"[31]. Los promotores llegan a la conclusión de que la respuesta es positiva, ya que la actividad no tiene como objetivo la mera creación de una nueva tecnología comercial, sino la introducción de un enfoque de preservación de la privacidad de los trabajadores que será informativo para las aplicaciones de preservación de la privacidad en otros contextos.

Régimen jurídico: investigación			
¿Considera la actividad como "investigación"?	Sí	✓	Se aplica un régimen específico de investigación

31 European Data Protection Supervisor, 'A Preliminary Opinion on Data Protection and Scientific Research'.

	No		No se aplica el régimen específico de la investigación

4.1.2 Confirmar la necesidad de procesar los datos biométricos

Para la investigación específica, los desarrolladores deciden no recurrir a una base de datos comercial, ni utilizar imágenes generadas por ordenador. Los desarrolladores deciden recoger todos los datos (huellas palmares) necesarios para alcanzar los objetivos de su investigación directamente de las personas físicas. Los desarrolladores recogerán impresiones de las huellas palmares y extraerán los rasgos físicos distintivos (por ejemplo, las medidas de la mano) de estas impresiones.

Para entender si se trata de datos biométricos, los desarrolladores adoptan los *criterios del* artículo 4.14 del RGPD.

Lista de comprobación de datos biométricos		
☐	Cantidad de datos personales	Sí, ya que las huellas palmares se refieren a una "persona física identificada
☐	Se basan en un tratamiento técnico específico	Sí, ya que los rasgos distintivos se extraerán de las impresiones palmares mediante un procesamiento técnico
☐	Pertenece a las características físicas, fisiológicas o de comportamiento	Sí, ya que las huellas palmares se relacionan con las características físicas
☐	Permiten o confirman la identificación única de las personas físicas	Sí, ya que el objetivo del proyecto es utilizar las huellas palmares para identificar a las personas físicas

Régimen jurídico: categorías especiales de datos personales			
¿La actividad implica datos biométricos?	Sí	☐	Se aplica el régimen específico de las categorías especiales de datos personales
	No		No se aplica el régimen específico sobre categorías especiales de datos personales

4.2 Fase de preparación

4.2.1 Nombrar a un Delegado de Protección de Datos (DPD)

Para evaluar la necesidad de un DPD, los desarrolladores examinan los requisitos del artículo 37 del RGPD. Dado que estos mencionan a menudo el *criterio de* "gran escala", los desarrolladores deciden evaluar primero si el tratamiento puede considerarse de gran escala, adoptando el enfoque del Grupo de Trabajo del Artículo 29.

Evaluación para el criterio de "gran escala"	
Número de personas afectadas	Se esperan de 30 a 50 sujetos de datos
Volumen de datos y/o gama de datos diferentes que se procesan	Se tratarán datos personales (por ejemplo, nombre, edad, etc.) y categorías especiales de datos (huellas palmares)
Duración o permanencia de la actividad de tratamiento de datos	Los promotores esperan que el estudio dure un año
Alcance geográfico de la actividad de tratamiento	Los promotores esperan que el estudio tenga alcance local (municipio)

Tras la evaluación, los promotores deciden que la actividad de transformación puede configurarse como "a gran escala". Aunque no se disponga de *criterios* cuantitativos y, por tanto, el resultado de la evaluación no pueda considerarse concluyente, lo deciden así con vistas a mantener un enfoque más prudente.

Una vez evaluado el *criterio de* "gran escala", los promotores proceden a evaluar la necesidad de una OPD.

Requisitos que exigen un delegado de la protección de datos		
"El tratamiento es llevado a cabo por una autoridad u organismo público, excepto los tribunales que actúan en su capacidad judicial"	✗	No se aplica
"Las actividades principales del responsable o del encargado del tratamiento consisten en operaciones de tratamiento que, por su naturaleza, su alcance y/o sus fines, requieren un control regular y sistemático de los interesados a gran escala"	✗	No se aplica (no hay un seguimiento regular ni sistemático)

"Las actividades principales del responsable o del encargado del tratamiento consisten en el tratamiento a gran escala de categorías especiales de datos con arreglo al artículo 9"	✓	Se aplica (categorías especiales de datos y tratamiento "a gran escala")
"Las actividades principales del responsable o del encargado del tratamiento consisten en el tratamiento a gran escala de [...] datos personales relativos a las condenas penales y a las infracciones contempladas en el artículo 10"	✗	No se aplica (no hay datos personales relacionados con condenas e infracciones penales)
En todos los demás casos no enumerados por los requisitos 1 a 3, "el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados del tratamiento podrán designar o, cuando así lo exija el Derecho de la Unión o de los Estados miembros, deberán designar un delegado de protección de datos"	✗	No se aplica (no hay legislación específica de la UE o de los Estados miembros)

Dado que uno de los requisitos es aplicable, los desarrolladores deciden designar un DPD. El responsable del tratamiento (Developing Inc.) no tiene un DPD designado. Por lo tanto, los promotores proceden a contratar uno.

Régimen jurídico: categorías especiales de datos personales			
¿Cumple la actividad con uno de los requisitos de un DPD?	Sí	✓	La designación de un DPD es obligatoria
	No		La designación de un DPD es opcional

4.2.2 Identificar el enfoque de recogida de datos

Los desarrolladores deciden recoger los datos personales directamente de los interesados. Se les invitará al laboratorio de Design Inc., donde se tomarán impresiones de las huellas palmares.

4.2.3 Identificar la base jurídica más adecuada

Antes de determinar la base jurídica más adecuada, los promotores deben evaluar si se aplica alguna de las excepciones al tratamiento de categorías especiales de datos personales.

Bases legales disponibles previstas por el RGPD para el tratamiento de datos biométricos		
Consentimiento explícito	✓	Se aplica

Empleo, seguridad social y protección social	✗	No se aplica (requiere una ley adicional; una evaluación del cumplimiento confirmó que no existe en el Estado)
Intereses vitales	✗	No se aplica
Actividades de asociaciones y otras entidades sin ánimo de lucro	✗	No se aplica
Los datos han sido publicados por el interesado	✗	No se aplica
Reclamaciones legales o actos judiciales	✗	No se aplica
Interés público sustancial	✗	No se aplica (requiere una ley adicional; una evaluación del cumplimiento confirmó que no existe en el Estado)
Salud o asistencia social	✗	No se aplica (requiere una ley adicional; una evaluación del cumplimiento confirmó que no existe en el Estado)
Interés público sanitario	✗	No se aplica (requiere una ley adicional; una evaluación del cumplimiento confirmó que no existe en el Estado)
Archivo, investigación y estadísticas	✗	No se aplica (requiere una ley adicional; una evaluación del cumplimiento confirmó que no existe en el Estado)

Dado que la única excepción aplicable es el "consentimiento explícito", los promotores también deciden adoptar el "consentimiento" como base jurídica para el tratamiento de datos.

Una vez considerada la base jurídica y teniendo en cuenta que la recogida se realizará directamente de los interesados (véase la sección **¡Error! No se encuentra el origen de la referencia.** "Identificar el enfoque de la recogida de datos"), los promotores preparan la información que se facilitará a los interesados en el formulario de consentimiento.

Información que debe proporcionarse a los interesados según el enfoque de la recogida	
La identidad y los datos de contacto del responsable del tratamiento	Developing Inc. (controlador de datos) Calle de los Desarrolladores, 99, 21010, Developonia +00 - 0123456, info@developinginc.com
En su caso, la identidad y los datos de contacto del representante del responsable del tratamiento	No se aplica
Los datos de contacto del responsable de la protección de datos	John Doe (DPD de Developing Inc.) Calle de los Desarrolladores, 99, 21010 Developonia +00 - 0123457, dpo@developinginc.com
Los fines del tratamiento	Investigar un método para utilizar las huellas palmares para identificar a los trabajadores en los lugares de trabajo, desarrollar y probar su tecnología y publicar los resultados
Las categorías de datos personales en cuestión	Nombre, apellidos, fecha de nacimiento, dirección, número de teléfono, correo electrónico, impresiones palmares
La base legal para el tratamiento	Consentimiento explícito
En su caso, los intereses legítimos perseguidos por el responsable del tratamiento o por un tercero	No aplicable (no se persigue ningún interés legítimo)
Destinatarios o categorías de destinatarios de los datos personales	Developing Inc. (controlador de datos)
La intención del responsable del tratamiento de transferir datos personales a un tercer país u organización internacional	No aplicable (no hay transferencia)
En caso de transferencia, la existencia o ausencia de una decisión de adecuación, o la referencia a las garantías y los medios para obtener una copia de los datos	No aplicable (no hay transferencia)
El período durante el cual se almacenarán los datos personales o, si no es posible, los	Duración de la investigación (se espera que comience el 0101/2022 y

criterios utilizados para determinar dicho period	dure un año), hasta que se desarrolle y pruebe el sistema
La existencia del derecho de acceso, rectificación o supresión, limitación del tratamiento, oposición y portabilidad	Los interesados pueden ejercer sus derechos según los artículos 12-22 del RGPD
En el caso del "consentimiento explícito" como base jurídica, la existencia del derecho a retirar el consentimiento en cualquier momento y sin ninguna consecuencia negativa	Los interesados pueden retirar su consentimiento. Si esto ocurre, Developing Inc. identificará a los nuevos interesados
Derecho a presentar una reclamación ante una autoridad de control	Las reclamaciones pueden presentarse ante la DPD de Developonia. Se facilitarán los contactos
Si el suministro de datos es un requisito legal o contractual, o es necesario para celebrar un contrato, si el interesado está obligado a proporcionar los datos y las consecuencias de no hacerlo	La disposición no es un requisito legal o contractual
La existencia de la toma de decisiones automatizada, incluida la elaboración de perfiles	El tratamiento no incluye la toma de decisiones automatizada
En el caso de la toma de decisiones automatizada, información sobre la lógica implicada, su importancia y las consecuencias previstas para el sujeto	No se aplica

4.2.4 Crear un repositorio de documentación de apoyo

El DPD de Developing Inc. crea un depósito en el que se archiva la documentación relativa al tratamiento. Los documentos se almacenan localmente en los servidores de Developing Inc. La arquitectura de almacenamiento de Developing Inc. es redundante para garantizar la continuidad de la actividad, y el contenido de los servidores es objeto de copias de seguridad periódicas.

Los desarrolladores identifican la siguiente documentación obligatoria:

Documentación: lista de control		
Política de protección de datos personales	✓	Se aplica
Aviso de privacidad	✓	Se aplica

Política de conservación de datos	✓	Se aplica
Calendario de conservación de datos	✓	Se aplica
Registro de actividades de procesamiento (si procede)	✓	Se aplica (véase más abajo)
Formulario de consentimiento (si procede)	✓	Se aplica (consentimiento como base jurídica)
Acuerdo de procesamiento de datos con los proveedores	✗	No se aplica (no hay proveedores con acceso a datos personales)
Evaluación del impacto de la protección de datos	✓	Se aplica (véase la sección **¡Error! No se encuentra el origen de la referencia.**)
Cláusulas contractuales para la transferencia de datos personales (si procede)	✗	No se aplica (no hay transferencia)
Nombramiento de un representante de la UE (si procede)	✗	No se aplica (Developing Inc. tiene su sede en la Unión Europea)
Procedimiento de respuesta y notificación de la violación de datos	✓	Se aplica
Registro de violaciones de datos	✗	No se aplica (no se ha producido ninguna infracción)
Formulario de notificación de violación de datos a la Autoridad de Supervisión	✗	No se aplica (no se ha producido ninguna infracción)
Formulario de notificación de violación de datos a los interesados	✗	No se aplica (no se ha producido ninguna infracción)

En el escenario, Design Inc. tiene un registro de actividades de procesamiento. En efecto, aunque se trata de una pequeña organización con menos de 250 empleados, realiza regularmente tratamientos de datos sobre sus empleados (por ejemplo, gestión de salarios, organización de retiros corporativos, etc.). Developing Inc. no ha elaborado un modelo propio para el registro de actividades de tratamiento y ha adoptado el proporcionado por la Autoridad[32] de Supervisión francesa.

4.2.5 Verificar si es necesaria la Evaluación de Impacto de la Protección de Datos

El RGPD exige una EIPD cuando es probable que el tratamiento de datos suponga un alto riesgo para los derechos y libertades de las personas físicas. Los promotores, al no

32 Se puede acceder a la plantilla en Commision Nationale Informatique & Libertés, 'Record of Processing Activities', August 2019, https://www.cnil.fr/en/record-processing-activities.

estar seguros de que el tratamiento plantee tales riesgos, deciden evaluar el tratamiento adoptando los nueve *criterios* antes mencionados sugeridos por el Grupo de Trabajo del Artículo 29.

***Criterios* de tratamiento de alto riesgo**		
Evaluación o puntuación (por ejemplo, elaboración de perfiles)	✗	No se aplica
Toma de decisiones automatizada con efectos legales o similares significativos	✗	No se aplica
Control sistemático	✗	No se aplica
Datos sensibles o de carácter muy personal	✓	Se aplica (véase más abajo)
Datos procesados a gran escala	✓	Se aplica (véase la sección **¡Error! No se encuentra el origen de la referencia.**)
Cotejar o combinar conjuntos de datos (más allá de las expectativas razonables del interesado)	✗	No se aplica
Datos relativos a personas vulnerables	✗	No se aplica
Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas	✗	No aplica (ver abajo)
Cuando el tratamiento impide por sí mismo que los interesados ejerzan un derecho o utilicen un servicio o un contrato	✗	No se aplica

La evaluación revela que el tratamiento cumple al menos dos *criterios*. El primero se refiere al tipo de datos personales que se van a tratar. Dado que, en el contexto de esta actividad de investigación, las huellas palmares se han establecido como datos biométricos, los promotores concluyen que estos datos satisfacen el *criterio* de ser sensibles y de naturaleza altamente personal. El segundo *criterio* se refiere a la magnitud del tratamiento. Los desarrolladores ya establecieron que el tratamiento se califica como de "gran escala" (véase **¡Error! No se encuentra el origen de la referencia.** "Nombrar a un Delegado de Protección de Datos (DPD)").

Los promotores se interrogan también sobre el *criterio* "Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas". No se aplica, ya que la actividad se centra en la investigación y la aplicación concreta a un contexto organizativo no está prevista en la actividad actual.

Evaluación del impacto de la protección de datos			
¿El tratamiento es de "alto riesgo"?	Sí	✓	La EIPD es obligatoria
	No		La EIPD es opcional

4.2.6 Realizar una EIPD

Dado que la autoridad de control de Developonia no ha redactado orientaciones sobre cómo realizar una EIPD, y siguiendo el consejo del DPD, los promotores realizan la EIPD utilizando las orientaciones del Grupo de Trabajo del Artículo 29, refrendadas por el Comité Europeo de Protección de Datos o CEPD, y la plantilla proporcionada por la autoridad[33] de control francesa. El resultado de la EIPD muestra que todos los riesgos para los derechos y libertades de los interesados están mitigados hasta un nivel aceptable, que nunca es alto para todos los riesgos identificados.

El resultado de la EIPD se almacena en el depósito de documentación de apoyo.

4.2.7 Aplicar medidas de mitigación de riesgos

Tras realizar la EIPD, los promotores establecen que las medidas técnicas y de seguridad son adecuadas para proteger los derechos y las libertades de los interesados y pueden considerarse salvaguardias apropiadas según el artículo 89 del RGPD.

4.3 Fase de ejecución

4.3.1 Tratamiento de datos biométricos

El equipo de investigadores, tras haber distribuido toda la información a los sujetos y haber recogido su consentimiento explícito, procede a recoger los datos biométricos de los sujetos. Los investigadores toman impresiones de las manos de cada participante y las introducen en un sistema de inteligencia artificial para extraer las características biométricas (por ejemplo, formas de la mano, crestas y valles, etc.). Todos los componentes del sistema de inteligencia artificial, incluido el algoritmo subyacente, son desarrollados y mantenidos internamente por los investigadores, y ningún otro sujeto participa o accede a los datos procesados por el sistema de inteligencia artificial. Los componentes de inteligencia artificial del sistema se desarrollan siguiendo los pasos detallados en la Parte III de este documento.

4.3.2 Desarrollo de la interfaz de usuario del sistema biométrico

El equipo de investigación decide que la interacción con el sistema biométrico se producirá a través de quioscos específicos. Durante la investigación, los quioscos se

33 Commision Nationale Informatique & Libertés, 'Privacy Impact Assessment (PIA). Templates'.

colocarán en el laboratorio de los desarrolladores. Los quioscos recogerán datos y los almacenarán localmente, y los usuarios interactuarán con los quioscos en presencia del equipo de investigación. El uso de los quioscos en el entorno controlado del laboratorio informará a los desarrolladores de la viabilidad de la tecnología y servirá de prueba piloto para su futura implantación en lugares de trabajo reales.

Uno de los objetivos de la investigación es agilizar la autenticación de los trabajadores. Para lograr estos objetivos, los investigadores pretenden agilizar el proceso de autenticación aumentando la facilidad de uso, minimizando así el tiempo que pasa cada usuario en el quiosco. Por ello, deciden dividir las funcionalidades en dos tipos de quiosco diferentes: uno dedicado a la autenticación (quiosco de autenticación), y otro dedicado a otras funcionalidades, como el acceso a la información y la actualización de datos personales (quiosco extra). De este modo, los trabajadores que necesiten realizar acciones distintas de la autenticación no ralentizarán la autenticación de los demás trabajadores.

El quiosco de autenticación tiene dos componentes principales: un escáner para la mano y un monitor. Si la autenticación es correcta, aparece una marca verde, la puerta se abre y el trabajador puede continuar. La autentificación no se registra (ya que el objetivo no es medir las horas de trabajo de las personas), y el monitor no muestra ninguna información sobre la persona.

El quiosco adicional tiene los mismos elementos que el quiosco de autenticación, con la diferencia de que el monitor es táctil para garantizar que los usuarios puedan interactuar con el sistema. Además, el quiosco extra está encajonado para evitar la navegación por los hombros. Los usuarios pueden activar el quiosco adicional simplemente escaneando sus manos. Al hacerlo, el monitor muestra un menú con tres opciones:

- Mostrar información sobre el tratamiento de datos: esta opción abre una ventana emergente en la que se ofrece toda la información indicada en la sección **¡Error! No se encuentra el origen de la referencia.** "Identificar la base jurídica más adecuada";
- Acceder y rectificar los datos personales: esta opción abre una ventana emergente en la que se muestran todos los datos personales de los sujetos, y en la que el usuario puede rectificar dichos datos, incluyendo el registro de nuevas impresiones palmares;
- Ejercer el derecho de rectificación, limitación, portabilidad de datos u oposición: esta opción está actualmente desactivada en el prototipo de quiosco de investigación. Si un usuario la selecciona, los miembros del equipo de investigación reciben una alerta en sus dispositivos móviles y se les pide que verifiquen con los interesados si tienen intención de ejercer alguno de sus derechos.

4.3.3 Pruebas del sistema biométrico

Una vez desarrollado el sistema, los investigadores pueden probarlo y verificar su rendimiento (por ejemplo, la tasa de error, la velocidad de autenticación, el consumo de energía, etc.). Para ello, recopilan los datos de los sujetos para simular el uso del sistema.

Dado que la prueba del sistema es una de las actividades clave de la investigación, los sujetos de los datos ya han dado su consentimiento explícito a la prueba, y no se procesan datos personales adicionales, el equipo de investigación concluye que los riesgos para los derechos y libertades de los sujetos de los datos se abordan adecuadamente y proceden a la prueba.

4.3.4 Difusión de los resultados

Una vez concluida la actividad de pruebas y reunidos todos los datos de las mismas, el equipo de investigación puede finalmente redactar un artículo en el que se describe la tecnología y se presentan los resultados. Confiando en que el sistema funcionará de forma consistente, deciden hacer que la tecnología sea de código abierto para garantizar que otros investigadores puedan realizar sus propias pruebas y validar los resultados. Tras esta decisión, los investigadores deciden borrar todos los datos personales de los sujetos que participaron en la actividad de investigación.

4.3.5 Borrado o destrucción de datos

Todos los datos personales se eliminan por completo.

Estas listas de comprobación no han sido revisadas ni validadas externamente. No obstante, PANELFIT las considera firmemente adecuadas para el objetivo que persiguen estas Directrices.

Lista de control de la fase de diseño

Paso	Sección pertinente de las Directrices
☐ Identificar el objetivo o los objetivos de la actividad	3.1.1
☐ Evaluar si la actividad equivale a una "investigación	3.1.1
☐ Identificar las funciones del equipo de investigación y de otras partes interesadas	3.1.1
☐ Confirmar que el tratamiento de los datos biométricos es necesario para alcanzar los objetivos de la actividad	3.1.2

Lista de control de la fase de preparación

Paso	Sección pertinente de las Directrices
☐ Evaluar si se aplica uno de los cinco requisitos para un DPD	3.2.1
☐ Si es una autoridad pública, compruebe si el DPD puede ser nombrado por otra autoridad pública	3.2.1
☐ Publicar el contacto del DPD	3.2.1
☐ Identifique si la recogida de datos se realizará directamente de los interesados o indirectamente	3.2.2
☐ Evaluar si puede acogerse a una exención de la obligación de informar al interesado	3.2.2
☐ Registrar la evaluación del derecho a la exención de la obligación de informar	3.2.2
☐ Definir un proceso interno para garantizar la exactitud de los datos tratados	3.2.2
☐ Identificar si se aplican las exenciones al tratamiento de categorías especiales de datos personales	3.2.3
☐ Si se requiere una ley adicional, verifique su existencia. Si no hay ninguna, identifique otra exención	3.2.3

☐ Si se aplican exenciones, identifique la base jurídica para el tratamiento de datos según el artículo 6 del RGPD	3.2.3
☐ Si se basa en el consentimiento, asegúrese de que es explícito	3.2.3
☐ Mantener un registro de los formularios de consentimiento	3.2.3 / 3.2.4
☐ Crear un repositorio de documentos, que contenga al menos los documentos exigidos por el RGPD	3.2.4
☐ Evaluar si el tratamiento introduce un alto riesgo para los derechos y libertades de las personas físicas	3.2.5
☐ Registrar los resultados de la evaluación preliminar	3.2.5
☐ Si el tratamiento introduce riesgos elevados, realice una EIPD	3.2.6
☐ Si los riesgos no se mitigan con las medidas previstas, aplicar medidas adicionales adecuadas	3.2.7
☐ Si no se mitigan los riesgos y no es posible aplicar medidas adicionales, consulte con la autoridad de supervision	3.2.7
☐ Registrar los resultados de la EIPD	3.2.4 / 3.2.6 / 3.2.7

Lista de control de la fase de ejecución

Paso	**Sección pertinente de las Directrices**
☐ Procesar los datos aplicando las salvaguardias y precauciones establecidas durante la fase de preparación	3.3.1
☐ En caso de desarrollo de sistemas de TIC, garantizar que el interesado pueda acceder a la información necesaria a través de una interfaz de usuario adecuada	3.3.2
☐ En caso de desarrollo de sistemas de TIC, evaluar los riesgos para los interesados relacionados con cada función del sistema	3.3.2
☐ Registrar el resultado de la evaluación de los riesgos relacionados con las funciones del sistema	3.2.4 / 3.3.2
☐ Si no se pueden mitigar los riesgos, consultar con la autoridad de supervisión o no aplicar	3.3.2
☐ Tenga en cuenta los casos de uso que implican a sujetos vulnerables	3.3.2

☐ En el caso de las pruebas de sistemas de TIC, evaluar si las pruebas del sistema configuran un procesamiento diferente al del desarrollo del sistema	3.3.3
☐ Registrar el resultado de la evaluación sobre las pruebas como un tratamiento diferente	3.2.4 / 3.3.3
☐ Si al probar el sistema se configura un procesamiento diferente, evalúe si el propósito es compatible	3.3.3
☐ Registrar el resultado de la prueba de compatibilidad	3.2.4 / 3.3.3
☐ Evaluar si la difusión del resultado implica también la difusión de datos personales y de categorías especiales de datos personales	3.3.4
☐ Identificar las excepciones al tratamiento de categorías especiales de datos personales antes de la difusión	3.3.4
☐ Determinar la base jurídica más adecuada para el tratamiento de los datos personales antes de su difusión	3.3.4
☐ Designar a los destinatarios como procesadores de datos	3.3.4
☐ Informar a los interesados de la transferencia de datos	3.3.4
☐ Compruebe si la transferencia de datos es internacional	3.3.4
☐ Si la transferencia es internacional y no se aplican excepciones, identifique un instrumento para la transferencia	3.3.4
☐ Evaluar si es lícito conservar los datos personales	3.3.5
☐ Registrar el resultado de la evaluación sobre la legalidad de la retención de datos	3.2.4 / 3.3.5
☐ Si es ilegal conservar los datos personales, eliminarlos o anonimizarlos	3.3.5