Examinada la consulta formulada por el Delegado de Protección de Datos de la entidad consultante, relativa a la utilización de un sistema de verificación biométrica facial uno-a-uno en el proceso de alta remota de nuevos clientes, así como la documentación aportada en relación con los juicios de idoneidad, necesidad y proporcionalidad del tratamiento, cúmpleme informar lo siguiente:

I

La consulta tiene por objeto recabar el criterio y orientación de esta Agencia respecto de la viabilidad del tratamiento de datos biométricos destinado a verificar la identidad de personas físicas que solicitan su alta como clientes de la entidad a través de un canal íntegramente remoto y, en particular, acerca de la adecuación de la metodología seguida por el responsable para valorar la idoneidad, necesidad y proporcionalidad de la incorporación de esta tecnología.

La propia entidad precisa que la solicitud no se formula como consulta previa en los términos del artículo 36 del Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos -en adelante, RGPD-, al considerar que, una vez aplicadas las medidas previstas en la evaluación de impacto, no subsiste un riesgo residual alto que determine la obligación de acudir a dicho procedimiento.

La presente contestación no constituye, por tanto, una autorización del tratamiento en el sentido del artículo 36 RGPD, ni supone la homologación de la concreta solución tecnológica propuesta, del proveedor seleccionado o de los parámetros técnicos configurados por el responsable. Tampoco corresponde a esta Agencia determinar el nivel de fiabilidad que deba reputarse suficiente desde la perspectiva de las obligaciones sectoriales de prevención del blanqueo de capitales y financiación del terrorismo, ni establecer el nivel de fraude que una entidad financiera deba asumir en el ejercicio de su actividad.

Sí corresponde, en cambio, analizar el marco de protección de datos aplicable, determinar los criterios jurídicos conforme a los cuales debe valorarse la licitud del tratamiento y precisar las exigencias derivadas de los principios de responsabilidad proactiva, necesidad, proporcionalidad, minimización, exactitud, seguridad y protección de datos desde el diseño y por defecto.

II

Según la documentación aportada, el tratamiento objeto de consulta se integra en el procedimiento de alta de nuevos clientes a través de un canal íntegramente remoto. [redacted]

La entidad manifiesta que este procedimiento ha permitido detectar intentos de fraude, pero que presenta limitaciones [redacted] La suficiencia de estas razones será objeto de valoración al examinar la idoneidad y necesidad de la nueva solución.

[redacted] Se mantienen la aportación del documento identificativo y la obtención de imágenes y vídeo del solicitante y, a partir de la fotografía contenida en el documento y de la imagen facial obtenida durante el proceso, se generan temporalmente referencias biométricas que se comparan entre sí para comprobar si corresponden a la misma persona.

Según la documentación aportada, el sistema no efectúa una búsqueda frente a una pluralidad de referencias ni incorpora las plantillas generadas a una base biométrica destinada a posteriores identificaciones o autenticaciones. Finalizada la comparación, dichas referencias son eliminadas y no se comunican a la entidad. En los resultados positivos se mantiene una revisión posterior por personal de backoffice, mientras que determinados resultados negativos impiden continuar por ese concreto flujo digital y determinan la derivación a un procedimiento alternativo no biométrico.

Nos encontramos, por tanto, ante la evolución de un procedimiento remoto ya existente: [redacted]

La generación y comparación de las referencias biométricas constituye un tratamiento técnico específico dirigido a verificar de manera unívoca la identidad de una persona física y queda sometida al artículo 9 RGPD.

A estos efectos, debe diferenciarse la identificación biométrica, que implica comparar los datos de una persona con una pluralidad de referencias para determinar su identidad, de la verificación o autenticación biométrica 1:1, en la que la identidad se encuentra previamente declarada y se comprueba su correspondencia con una única referencia. Esta distinción no excluye la aplicación del artículo 9 RGPD, pero sí resulta relevante para valorar la intensidad de la injerencia, los riesgos y las garantías exigibles. La utilización a gran escala de verificaciones 1:1 tampoco las transforma, por ese solo hecho, en operaciones de identificación uno-a-varios. Ello no impide que la escala y la arquitectura concreta del tratamiento -incluida la existencia, alcance y persistencia de repositorios o conjuntos de referencias biométricas- deban ser consideradas al evaluar el riesgo y determinar las garantías aplicables.

III

El análisis de la licitud exige distinguir la base jurídica prevista en el artículo 6.1 RGPD de la circunstancia que permita levantar la prohibición establecida en el artículo 9.1. Tratándose de categorías especiales de datos, ambos requisitos deben concurrir. Asimismo, el procedimiento de alta puede comprender distintas operaciones de tratamiento sometidas a bases jurídicas diferentes en función de su finalidad y necesidad. No procede, por tanto, atribuir de manera indiferenciada una única base jurídica a la totalidad del proceso ni acumular diferentes fundamentos como títulos intercambiables respecto de una misma operación.

La normativa de prevención del blanqueo de capitales impone a las entidades de crédito obligaciones específicas de identificación y comprobación de la identidad de las personas con las que establecen relaciones de negocio. Las operaciones de tratamiento que resulten necesarias para cumplir dichas obligaciones pueden encontrar fundamento en el artículo 6.1.c) RGPD. Del mismo modo, el artículo 6.1.b) podrá resultar aplicable a los tratamientos objetivamente necesarios para adoptar, a petición del interesado, medidas previas a la celebración de un contrato.

Ahora bien, la existencia de una obligación legal de identificación o el carácter precontractual del procedimiento no determinan por sí solos que una concreta modalidad tecnológica de verificación resulte necesaria a efectos de los artículos 6.1.c) o 6.1.b). La necesidad debe apreciarse respecto de la concreta operación de tratamiento.

Con carácter general, la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, constituye el fundamento normativo que permite a los sujetos obligados tratar los datos personales necesarios para identificar a nuevos clientes, siendo la base jurídica aplicable el artículo 6.1.c) del RGPD (cumplimiento de una obligación legal), ahora bien la

implantación de un procedimiento de identificación con base en tratamiento de datos biométricos requiere, con carácter previo y necesario, determinar la existencia de una causa que levante la prohibición general del tratamiento de datos sensibles habida cuenta del carácter especialmente protegido de estos datos.

Dicho lo cual, habida cuenta de la previsión contenida en el artículo 9.2.a) RGPD siempre que el consentimiento reúna los requisitos que se examinan en el fundamento siguiente, el consentimiento podrá constituir una circunstancia válida que permita levantar la prohibición general del tratamiento de datos personales especialmente protegidos, el cual será posible siempre que se realice con pleno respeto del RGPD, con particular referencia a los artículos 5 y 6 RGPD.

IV

Respecto del levantamiento de la prohibición establecida en el artículo 9.1 RGPD, la entidad fundamenta la operación biométrica en el consentimiento explícito previsto en el artículo 9.2.a).

El consentimiento deberá reunir los requisitos establecidos en los artículos 4.11, 7 y 9.2.a) RGPD y ser, por tanto, libre, específico, informado, inequívoco y explícito. En particular, su carácter libre exige que el interesado pueda rechazar el tratamiento biométrico sin que dicha decisión comporte un perjuicio o una presión indebida sobre su voluntad.

Esta exigencia obliga a examinar las alternativas realmente ofrecidas por el responsable, pero no determina que el procedimiento alternativo deba ser idéntico al biométrico. Modalidades distintas de identificación pueden presentar legítimamente diferencias en tecnología, intervención humana, rapidez, disponibilidad o facilidad de uso. Lo relevante es que quien no desee someterse al tratamiento biométrico disponga de una alternativa real, cierta y razonablemente accesible para acceder sustancialmente al mismo servicio, sin costes adicionales injustificados, pérdida de condiciones, exclusiones, retrasos desproporcionados u otras cargas que puedan operar materialmente como una presión para consentir, de manera que no resulte posible concluir que el consentimiento se presta en condiciones de libertad y de igualdad.

[redacted]

Sin embargo, de la exigencia de consentimiento libre no se deriva una obligación de conservar indefinidamente una concreta solución tecnológica u organizativa

por el hecho de haber sido utilizada con anterioridad. Lo exigible es que la evolución del procedimiento no prive al interesado de una alternativa efectiva ni convierta su negativa a la biometría en una opción artificialmente gravosa que determine la existencia de una suerte de presión al uso de la biometría, lo cual como venimos explicando diluiría la libertad del consentimiento y lo convertiría en un consentimiento no libre y, por ello, contrario al RGPD.

En consecuencia, la sustitución del procedimiento remoto actualmente utilizado debe valorarse atendiendo no solo a su existencia histórica, sino también a las razones objetivas alegadas por el responsable para modificarlo. [redacted] La suficiencia de estas razones para considerar que el procedimiento anterior no alcanza una eficacia equivalente será examinada específicamente al analizar la necesidad del tratamiento.

Según la consulta, la principal alternativa no biométrica ofrecida tras la implantación del nuevo sistema sería la identificación presencial a través de la red de oficinas de la entidad, lo que determinaría la eliminación de un sistema de identificación en remoto con la consiguiente pérdida del elemento de libertad que venimos comentando. La realidad de esta alternativa deberá apreciarse materialmente, atendiendo a la posibilidad efectiva de obtener el mismo servicio y a las cargas que comporte para el interesado. No existe, sin embargo, una exigencia de que deba existir una oficina en su mismo municipio ni cabe deducir que solo las entidades dotadas de una extensa red presencial puedan ofrecer procedimientos biométricos basados en consentimiento. La alternativa deberá pues articularse también mediante otros procedimientos no biométricos cuando resulten efectivamente disponibles y adecuados.

La existencia de una alternativa presencial no agota, en el supuesto analizado, las posibilidades de elección del interesado. En las circunstancias de este caso, resulta necesario que, junto a la opción presencial, se ofrezca también una alternativa no biométrica a distancia, en particular mediante mecanismos de identificación electrónica que el ordenamiento reconoce expresamente para el establecimiento de relaciones no presenciales, como los basados en firma electrónica cualificada y, cuando proceda, en el DNI electrónico. Ello permitiría al interesado optar entre la verificación biométrica, una vía remota no biométrica y la identificación presencial. Se trata, además, de mecanismos jurídicamente previstos que podrían articularse como alternativa a distancia. La decisión de las concretas formas de identificación segura a través de un canal remoto corresponde en todo caso al Responsable de Tratamiento, a fin de garantizar las

condiciones de igualdad en las que necesariamente habrá de prestarse el consentimiento al tratamiento de datos personales.

Como decimos, la disponibilidad de un procedimiento remoto no biométrico que mantenga niveles adecuados de seguridad y fiabilidad constituye un elemento especialmente relevante para acreditar la existencia de una elección efectiva.

La Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados constituye, en su específico ámbito de aplicación, un ejemplo de coexistencia entre una modalidad de identificación que puede implicar tratamiento de categorías especiales y otros métodos de identificación que no lo requieren, sin exigir que todas las alternativas sean tecnológicamente idénticas.

Debe diferenciarse, finalmente, este análisis del juicio de necesidad. Una alternativa puede ser suficiente para preservar la libertad del consentimiento y no alcanzar, sin embargo, una eficacia equivalente a la del tratamiento biométrico para la finalidad perseguida. A efectos del consentimiento debe determinarse si el interesado puede rechazar realmente la biometría sin sufrir un perjuicio que vicie su voluntad; a efectos de necesidad habrá que comprobar si existe una medida menos intrusiva capaz de alcanzar razonablemente la finalidad con igual eficacia.

A la vista de la información aportada, y sin que consten diferencias de producto o condiciones, costes adicionales u otras consecuencias asociadas a la negativa al tratamiento biométrico que permitan apreciar una presión indebida, la alternativa presencial descrita puede considerarse, en principio, suficiente para preservar la libertad de elección del interesado siempre que se acompañe de otra vía en remoto que no implique tratamiento biométrico a disposición de los interesados. La eventual disponibilidad adicional de mecanismos de identificación electrónica no biométrica a distancia permitiría apreciar esta posibilidad de elección, así como la concurrencia del requisito de libertad necesario para la validez del consentimiento.

V

La identificación de clientes en relaciones no presenciales no se encuentra vinculada por la normativa sectorial a una única solución tecnológica. El marco aplicable contempla distintos procedimientos de identificación a distancia y atribuye a las entidades la responsabilidad de seleccionar medios adecuados al riesgo y al nivel de fiabilidad requerido, debiendo establecer políticas y procedimientos para afrontar específicamente los riesgos asociados a las relaciones de negocio y operaciones no presenciales, conforme al artículo 12.2 de la Ley 10/2010, de 28 de abril.

En particular, el artículo 12.1.a) de la Ley 10/2010, de 28 de abril, permite establecer relaciones de negocio no presenciales cuando la identidad del cliente quede acreditada mediante firma electrónica cualificada regulada en el Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 (eIDAS), relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE. En este supuesto no resulta necesaria la obtención de copia del documento de identificación, aunque deben conservarse los datos que acrediten la validez del procedimiento. Por su parte, el artículo 21.1 del Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, contempla tanto la acreditación de la identidad conforme a la normativa sobre firma electrónica como la utilización de otros procedimientos seguros de identificación no presencial previamente autorizados por el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC).

Las Directrices EBA/GL/2022/15 sobre el uso de soluciones de alta de clientes a distancia con arreglo al artículo 13, apartado 1, de la Directiva (UE) 2015/849 (Directrices EBA), parten igualmente de un enfoque tecnológicamente neutral. Cuando se emplean soluciones que realizan un cotejo entre el cliente y la documentación presentada, exigen mecanismos suficientemente sólidos y fiables y prevén medidas adicionales cuando no se alcanza el nivel de confianza requerido. Al mismo tiempo, atribuyen especial relevancia a los sistemas de identificación electrónica notificados conforme al Reglamento eIDAS con niveles de seguridad “sustancial” o “alto” y a los servicios de confianza cualificados, como mecanismos específicamente configurados para la identificación remota.

Debe tenerse asimismo en cuenta que el DNI electrónico permite acreditar electrónicamente la identidad personal de su titular y la firma electrónica de documentos, en los términos previstos en la disposición adicional tercera de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. El ordenamiento atribuye, por tanto, tanto a la firma electrónica cualificada como al DNI electrónico una función específica de acreditación electrónica de identidad que puede permitir, cuando estos medios se encuentren efectivamente disponibles para el interesado y resulten adecuados al concreto procedimiento, mantener una modalidad de alta a distancia sin que la entidad tenga que efectuar el tratamiento biométrico objeto de esta consulta.

A estos efectos, debe diferenciarse la mera presentación remota de un documento de identidad de la utilización de mecanismos jurídicamente configurados para acreditar electrónicamente la identidad. La simple aportación de la imagen de un documento no permite por sí sola comprobar que quien la

presenta sea efectivamente su titular. Esta consideración no puede trasladarse sin más a mecanismos de identificación electrónica dotados de un régimen específico de garantías destinado precisamente a proporcionar un determinado grado de confianza sobre la identidad de quien los utiliza. Los niveles de garantía previstos en el Reglamento eIDAS responden, precisamente, al grado de confianza que proporciona el medio electrónico respecto de la identidad declarada.

En el supuesto consultado, estos mecanismos pueden, por tanto, ser considerados como posibles vías remotas no biométricas adicionales al procedimiento presencial para aquellos interesados que dispongan de ellos y puedan utilizarlos. Su disponibilidad resulta especialmente relevante desde la perspectiva de la libertad del consentimiento, al ampliar las posibilidades reales de elección sin obligar a mantener el procedimiento remoto manual actualmente utilizado, cuya menor fiabilidad frente a los riesgos identificados se examina posteriormente.

Esta orientación resulta además coherente con la evolución del marco europeo de prevención del blanqueo. El Reglamento (UE)2024/1624, del Parlamento Europeo y del Consejo, de 31 de mayo de 2024, relativo a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, aplicable con carácter general a partir del 10 de julio de 2027, contempla expresamente entre los medios de comprobación de la identidad los medios de identificación electrónica que alcancen los niveles de seguridad «sustancial» o «alto» conforme al Reglamento eIDAS y los servicios de confianza cualificados pertinentes. Esta evolución refuerza la conveniencia de que el responsable revise periódicamente las alternativas disponibles a medida que aumente su disponibilidad efectiva, sin alterar el análisis que corresponde efectuar con arreglo al marco actualmente aplicable.

VI

La entidad acompaña a su consulta un análisis específico de idoneidad, necesidad y proporcionalidad. El juicio de idoneidad exige determinar, con carácter previo, si el tratamiento proyectado es objetivamente apto para contribuir a la finalidad perseguida. No exige todavía demostrar que no exista una alternativa menos intrusiva, cuestión propia del posterior juicio de necesidad.

La finalidad identificada por la entidad consiste en verificar, en un proceso de alta íntegramente remoto, que la persona que interviene es efectivamente la titular del documento aportado, reforzando la prevención de la suplantación de identidad y del fraude. Desde esta perspectiva existe una conexión directa entre dicha finalidad y una operación de verificación facial 1:1 que compara la imagen obtenida del solicitante con la incorporada a su documento de identidad.

La necesidad de reforzar los mecanismos utilizados no se presenta en la documentación como una cuestión meramente hipotética. [redacted].

La documentación aportada incorpora asimismo evidencias técnicas dirigidas a acreditar la aptitud de la solución propuesta. [redacted].

Estas evidencias deben valorarse de acuerdo con su concreto alcance. Una evaluación de rendimiento del algoritmo, una certificación relativa a ataques de presentación o una certificación de un sistema de gestión no acreditan por sí solas la eficacia global del procedimiento frente al fraude en condiciones reales de producción. Sí constituyen elementos objetivos que, considerados conjuntamente con la prueba de vida, los controles documentales y la intervención posterior del backoffice en los resultados positivos, permiten apreciar prima facie que el tratamiento proyectado es técnicamente apto para contribuir a la finalidad declarada.

La determinación del nivel de eficacia necesario corresponde primariamente al responsable, atendiendo al contexto de su actividad, a los riesgos que conoce y a las obligaciones sectoriales que debe cumplir. No corresponde a esta Agencia fijar la tasa de fraude que una entidad financiera deba considerar aceptable ni determinar el concreto umbral de similitud que deba configurar en un sistema biométrico. Sí le corresponde comprobar que el nivel de eficacia requerido ha sido definido de forma objetiva, que las métricas utilizadas son pertinentes y que la decisión se encuentra suficientemente documentada conforme al principio de responsabilidad proactiva.

En esta valoración debe evitarse, además, trasladar automáticamente los resultados obtenidos en pruebas técnicas al comportamiento global del procedimiento. Las tasas de falsos positivos y falsos negativos dependen, entre

otros factores, de las condiciones de prueba, del umbral configurado y del contexto de utilización; del mismo modo, una determinada tasa de detección de ataques no equivale necesariamente a la tasa de fraude que será evitada en producción.

[redacted]

En consecuencia, la documentación permite apreciar en este momento una idoneidad ex ante suficientemente fundada, sin que ello equivalga a certificar la superioridad efectiva del sistema en producción. La continuidad de esta conclusión exige que el responsable contraste las hipótesis iniciales con los resultados reales obtenidos, monitorice los errores y posibles desviaciones y revise la evaluación cuando la evidencia disponible muestre que la eficacia real difiere de la prevista.

VII

El juicio de necesidad exige determinar si la finalidad perseguida puede alcanzarse razonablemente mediante otra medida menos intrusiva que proporcione un nivel de eficacia equivalente. La mera existencia de otro procedimiento posible no determina, por sí sola, que el tratamiento biométrico resulte innecesario.

Este estándar exige comparar alternativas desde una perspectiva funcional. El carácter menos intrusivo de una medida es condición relevante, pero no suficiente: para desplazar al tratamiento proyectado debe permitir satisfacer la misma necesidad con un nivel de eficacia equivalente.

[redacted]

[redacted]

[redacted]

A juicio de esta Agencia, la existencia del procedimiento manual actualmente utilizado no determina por sí sola la innecesariedad del tratamiento biométrico por el mero hecho de constituir una medida menos intrusiva. El juicio de necesidad no impone la elección de cualquier alternativa menos intrusiva por el solo hecho de serlo, sino que exige comprobar si existe otra medida que permita alcanzar razonablemente la misma finalidad con un nivel de eficacia equivalente. Solo cuando concurra esa equivalencia la existencia de la alternativa determinará que el tratamiento más intrusivo no resulte necesario. La documentación aportada ofrece razones objetivas suficientes, en términos ex ante, para considerar que dicha equivalencia no concurre respecto de los riesgos específicamente identificados.

La misma consideración resulta aplicable a los mecanismos de identificación electrónica examinados en el fundamento anterior. Su reconocimiento jurídico y su aptitud para constituir vías remotas no biométricas justifican que sean considerados entre las alternativas disponibles, pero no permiten presumir por sí solos su disponibilidad para todos los interesados ni su equivalencia funcional frente a los concretos riesgos analizados. Esta última cuestión deberá valorarse atendiendo a las características del mecanismo, su disponibilidad efectiva y el nivel de eficacia que proporcione en el contexto considerado.

Esta conclusión no se fundamenta primordialmente en razones de eficiencia, automatización o reducción de costes, aunque tales beneficios aparezcan en la documentación y sean elementos que en todo caso cabe tener en cuenta, sino que se centran en las razones de fiabilidad y seguridad frente a los riesgos de suplantación identificados por la entidad.

En consecuencia, y sobre la base de la información actualmente disponible, el tratamiento proyectado supera el juicio de necesidad. La ausencia de datos comparativos obtenidos en producción no impide esta conclusión ex ante, pues la necesidad puede justificarse mediante evidencia objetiva previa suficiente. El

piloto y la monitorización previstos constituyen, no obstante, una exigencia de responsabilidad proactiva destinada a comprobar que las premisas utilizadas permanecen válidas durante la aplicación del tratamiento. Si la experiencia obtenida evidenciara que la mejora de eficacia inicialmente apreciada no se produce o que aparecen alternativas menos intrusivas con eficacia equivalente, deberá revisarse la evaluación.

VIII

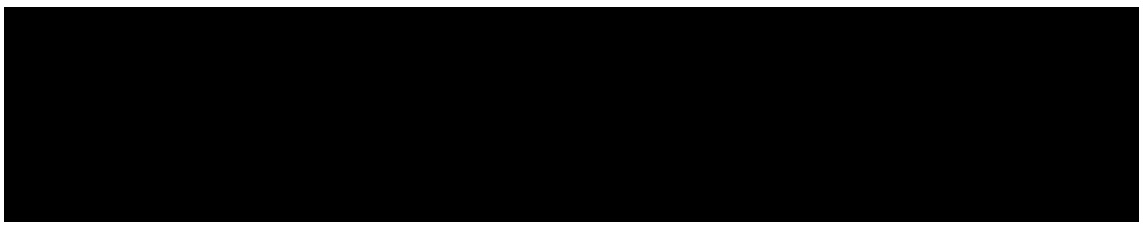
Superados los juicios de idoneidad y necesidad, procede determinar si la mayor injerencia derivada del tratamiento de datos biométricos resulta proporcionada a la finalidad perseguida y a los beneficios que cabe razonablemente esperar de la medida.

El tratamiento proyectado comporta riesgos específicos por afectar a datos biométricos. Frente a ellos, la finalidad perseguida comprende la prevención de altas fraudulentas realizadas mediante identidades ajenas y la protección de los propios interesados frente a las consecuencias económicas y jurídicas de una suplantación.

Resulta especialmente relevante la configuración concreta del tratamiento. Según la documentación aportada, se realiza una única comprobación 1:1 durante el alta, sin búsqueda frente a bases poblacionales, sin categorización ni inferencia de atributos y sin reutilización posterior de las plantillas. Las referencias biométricas se generan únicamente durante la operación y son eliminadas una vez efectuada la comparación, sin constituirse una base biométrica de clientes.

La solución incorpora, además, según manifiesta la entidad, referencias renovables caracterizadas por su irreversibilidad, revocabilidad y no interoperabilidad, junto con medidas de seguridad, limitación de accesos, trazabilidad y revisión humana posterior de los resultados positivos.

En atención a estas características, el tratamiento proyectado supera, en los términos descritos, el juicio de proporcionalidad en sentido estricto. La modalidad 1:1, el carácter puntual del tratamiento, la ausencia de un repositorio biométrico destinado a usos posteriores, la eliminación de las referencias una vez efectuado el cotejo y las restantes garantías previstas limitan suficientemente la intensidad de la injerencia en relación con la finalidad perseguida.



[redacted].

[redacted].

La aplicación del artículo 22.1 dependerá de que el resultado automatizado produzca efectos jurídicos sobre el interesado o le afecte significativamente de modo similar, extremo que no puede darse por acreditado únicamente porque determine un cambio del canal de identificación cuando subsista una vía efectiva para completar el alta. Corresponde al responsable valorar y documentar las consecuencias reales asociadas a dichos resultados. Si, atendiendo a tales consecuencias, resultara aplicable el artículo 22 RGPD, deberán cumplirse íntegramente los requisitos y garantías establecidos en dicho precepto. A estos efectos, la mera posibilidad de acudir a un procedimiento presencial alternativo no equivale, por sí sola, al derecho a obtener intervención humana sobre la concreta decisión automatizada.

IX

[redacted].

[redacted].

[redacted]

No cabe formular objeción a la diferenciación entre eliminación inmediata de las plantillas y conservación de evidencias cuando estas últimas respondan a finalidades y obligaciones jurídicas propias. Sí deberá identificarse con precisión el fundamento de cada plazo de conservación. [redacted]

Por otra parte, el proveedor que efectúa las operaciones biométricas deberá quedar sometido a las garantías del artículo 28 RGPD, incluidas las relativas a utilización de los datos exclusivamente conforme a instrucciones, subencargados, localización del tratamiento, seguridad, supresión efectiva y ausencia de utilización para finalidades propias. La afirmación de que las operaciones se realizan en entornos del Espacio Económico Europeo y de que las plantillas se destruyen inmediatamente deberá quedar adecuadamente documentada y ser verificable por el responsable.

X

La entidad fundamenta el levantamiento de la prohibición del artículo 9.1 RGPD principalmente en el consentimiento explícito del artículo 9.2.a). No resulta necesario, por tanto, determinar para resolver la presente consulta si el marco normativo de prevención del blanqueo constituye, por sí mismo, una habilitación suficiente conforme al artículo 9.2.g).

Cuando el tratamiento biométrico se encuentre estrictamente vinculado a una obligación legal de identificación y concurra un interés público esencial, la suficiencia del marco normativo deberá valorarse atendiendo conjuntamente al artículo 9.2.g) RGPD, al artículo 9.2 LOPDGDD y a las exigencias constitucionales de previsibilidad y garantías. La existencia de obligaciones legales de identificación no implica, por sí sola, que concurra un interés público esencial que habilite el tratamiento de datos biométricos. Hay que justificar separadamente la excepción del artículo 9.2 RGPD y comprobar que la norma ofrece una cobertura suficiente para el tratamiento concreto.

Como ya ha señalado esta Agencia, el grado de precisión normativa exigible debe ponerse en relación con la naturaleza, alcance y riesgo real del tratamiento, sin que resulte necesariamente exigible idéntica densidad normativa para una identificación biométrica masiva y para una verificación puntual, localizada y rodeada de garantías. Este criterio no elimina la reserva de ley ni las garantías exigidas por la doctrina constitucional, pero impide resolver la cuestión mediante el único automatismo de exigir que la norma mencione expresamente la concreta tecnología utilizada.

En el ámbito de prevención de blanqueo de capitales, la existencia de un marco legal y reglamentario específico sobre identificación formal y relaciones no presenciales, complementado por los procedimientos autorizados por SEPBLAC y las Directrices EBA, constituye un elemento que deberá ponderarse cuando proceda examinar esta vía.

Esta aproximación, basada en la valoración material de la función y del riesgo del tratamiento, encuentra además un elemento relevante de contexto en la evolución normativa europea actualmente en curso. La propuesta llamada "Ómnibus" de Reglamento COM(2025) 837, actualmente todavía en tramitación legislativa, propone incorporar al artículo 9.2 RGPD una nueva excepción específicamente referida al tratamiento de datos biométricos necesario para confirmar la identidad declarada de una persona -verificación- cuando los datos biométricos o los medios necesarios para realizarla permanezcan bajo el control exclusivo del interesado. La propuesta diferencia expresamente esta verificación uno-a-uno de los procedimientos de identificación uno-a-varios y atribuye especial relevancia a arquitecturas en las que el responsable no accede a la información biométrica o lo hace únicamente durante un período muy limitado.

Esta modificación no constituye Derecho vigente pero sí resulta significativa como manifestación de una evolución legislativa que diferencia entre tratamientos biométricos en función de su finalidad, arquitectura y garantías y reconoce que determinadas configuraciones de verificación 1:1 pueden presentar un perfil de riesgo sustancialmente distinto de otros usos de la biometría. El Consejo Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos, en su Dictamen conjunto 2/2026, han acogido favorablemente la introducción de esta nueva excepción precisamente por encontrarse limitada a supuestos de verificación 1:1 en los que los datos biométricos o los medios necesarios para la verificación permanezcan bajo el control exclusivo del interesado. Al mismo tiempo, ambas autoridades subrayan que incluso estos tratamientos deben superar los juicios de necesidad y proporcionalidad y estar acompañados de garantías adecuadas.

Lo anterior no permite afirmar que el sistema objeto de consulta responda al supuesto contemplado en la propuesta legislativa, en particular teniendo en cuenta las precisiones efectuadas en el fundamento VIII respecto del denominado control exclusivo del interesado.

XI

A la vista de la documentación aportada, esta Agencia considera que el sistema descrito supera, en términos ex ante, los juicios de idoneidad, necesidad y proporcionalidad examinados. Asimismo, la metodología seguida por el responsable para efectuar dichos juicios se considera, en lo sustancial,

adecuada a los criterios expuestos en el presente informe, sin perjuicio de las exigencias de documentación, seguimiento y revisión que se indican a continuación.

El tratamiento proyectado constituye una verificación biométrica uno-a-uno sometida al artículo 9 RGPD, sin que ello determine que su intensidad o perfil de riesgo resulte equivalente al de sistemas de identificación biométrica uno-a-varios, poblacionales o destinados a usos persistentes. En el supuesto analizado, la valoración favorable queda sujeta a que se garantice que el consentimiento se presta de conformidad con los requisitos exigidos en el RGPD y tiene especialmente en cuenta el carácter puntual de la operación, la ausencia de un repositorio biométrico destinado a usos posteriores, la eliminación de las referencias tras el cotejo, las garantías de seguridad descritas y la intervención humana prevista en los resultados positivos.

Siempre que reúna los requisitos examinados en este informe, el consentimiento podrá servir como base jurídica de la concreta operación biométrica conforme al artículo 6.1.c) RGPD y, por su carácter explícito, como circunstancia que permite levantar la prohibición del artículo 9.1 conforme al artículo 9.2.a). Su libertad exige que el interesado disponga de una alternativa no biométrica real y que su negativa no comporte un perjuicio capaz de condicionar su voluntad, sin que ello implique que dicha alternativa deba reproducir el mismo procedimiento tecnológico ni que deba mantenerse indefinidamente la concreta solución remota utilizada hasta ahora, sin perjuicio de que deba garantizarse la existencia de otra alternativa de identificación en vía remota a fin de garantizar el requisito de libertad analizado en este informe.

Este análisis debe diferenciarse del juicio de necesidad. Una alternativa puede ser suficiente para preservar la libertad del consentimiento y no proporcionar, sin embargo, una eficacia equivalente frente al riesgo que se pretende mitigar. La existencia de una medida menos intrusiva solo determinará la innecesariedad de la biometría cuando permita alcanzar razonablemente la finalidad perseguida con un nivel de eficacia equivalente.

La determinación del nivel de eficacia necesario corresponde primariamente al responsable, atendiendo al contexto de su actividad, a los riesgos identificados y a las obligaciones sectoriales que debe cumplir. Esta Agencia no determina el nivel de fraude asumible ni certifica la suficiencia de un determinado algoritmo, pero sí debe comprobar que la decisión se encuentra objetivamente fundamentada, que las evidencias y métricas empleadas son pertinentes y que las consecuencias para los derechos y libertades han sido adecuadamente evaluadas.

La valoración favorable anterior no excluye determinadas exigencias de documentación y responsabilidad proactiva. La entidad deberá armonizar la descripción de la arquitectura técnica respecto de las referencias a generación local y control exclusivo, justificar los concretos plazos de conservación y completar, en los términos señalados, la valoración de las consecuencias asociadas a los resultados negativos automatizados. Asimismo, la ausencia actual de resultados comparativos en producción no impide la conclusión alcanzada, pero exige que el piloto y la monitorización previstos permitan comprobar que las premisas sobre las que descansan los juicios de idoneidad, necesidad y proporcionalidad se mantienen durante la utilización efectiva del sistema. Si la experiencia obtenida las contradijera, deberá revisarse la evaluación.

Finalmente, no resulta necesario para resolver la presente consulta determinar si el marco normativo de prevención del blanqueo constituye, en este concreto supuesto, una habilitación suficiente conforme al artículo 9.2.g) RGPD. Ello no permite descartar de forma general dicha posibilidad respecto de tratamientos biométricos estrictamente vinculados a obligaciones legales de identificación. Su eventual aplicación deberá examinarse caso por caso atendiendo al conjunto normativo aplicable, al grado real de injerencia y a las garantías existentes, con pleno respeto del artículo 9.2 LOPDGDD y de las exigencias derivadas de la doctrina constitucional.

Esta respuesta constituye una actividad meramente informativa de la AEPD; no tiene efectos vinculantes, no modifica la situación jurídica del solicitante y no constituye un acto recurrible.