La salvaguarda de los principios del RGPD en el modelo de Open Finance de la Unión Europea

Resumen / Abstract

El presente trabajo analiza el cambio de paradigma que supone el marco FIDA, la propuesta legislativa europea que busca transformar el Open Banking en un ecosistema integral de Open Finance. A diferencia de modelos previos, limitados a servicios de pago (PSD2), FIDA expande el perímetro de intercambio de datos a sectores como inversiones y seguros, imponiendo el uso obligatorio de APIs y certificados eIDAS para garantizar la seguridad en el acceso.

Este artículo se centra en los riesgos para la privacidad: la sobreexposición del usuario mediante el perfilado con modelos de lenguaje (IA), la ambigüedad jurídica entre el "permiso FIDA" y el "consentimiento RGPD", así como los desafíos de ciberseguridad ante flujos masivos de datos financieros. Para abordar las posibles medidas de mitigación, se examinan las posiciones de la Comisión, el Parlamento y el Consejo, junto con las recomendaciones del Supervisor (EDPS) y el Comité (EDPB) europeos de protección de datos.

Ante este escenario, la figura del Delegado de Protección de Datos (DPO) se consolida como un aliado estratégico dentro de las organizaciones. Se concluye que su intervención permitirá que la innovación financiera no derive en una vigilancia total o en la exclusión de perfiles vulnerables, logrando que la circulación de la información redunde exclusivamente en beneficio de la ciudadanía. En definitiva, su rol materializa la ambición de la Estrategia Europea de Datos: demostrar que es posible liderar la economía digital situando los derechos de las personas y los valores europeos en el centro del desarrollo tecnológico.

1. Introducción

Para definir Open Finance (finanzas abiertas) nos tenemos que remitir al eslabón de la cadena inmediatamente anterior, el modelo Open Banking (banca abierta), cuya regulación en Europa (la Directiva de servicios de pago, en adelante PSD2, por sus siglas en inglés) es tan novedosa como obsoleta.

A falta de definición formal, el Comité de Supervisión Bancaria de Basilea (BCBS, 2019)[1] ofrece una definición que sirve como referencia: el Open Banking es “el intercambio y aprovechamiento de datos autorizados por el cliente por parte de los bancos con desarrolladores y empresas externas para construir aplicaciones y servicios”.

Si el Open Banking es una evolución significativa de la forma en la que los bancos tradicionalmente han tratado los datos de sus clientes, el Open Finance representa el siguiente paso lógico, pues amplía el perímetro de aquel, con lo que ello conlleva. Así pues, ya no se propone abrir únicamente los datos vinculados a pagos, sino extender el acceso y el intercambio al resto de actividades financieras (como los servicios de inversión o los seguros).

Hay quien prefiere (Coelho et al., 2025)[2] no conceder un espacio estanco al Open Finance y encuadrarlo dentro del Open Data. En esta visión, la evolución financiera no puede entenderse de forma aislada, sino como parte de un movimiento global de "datos abiertos" (datos de salud, datos financieros, huella digital). Esta lógica aspira a que la información completa del usuario circule de forma segura, estandarizada y reutilizable.

Para el profesional de la privacidad, este escenario supone un reto de primer orden y de naturaleza multidimensional ya que sus funciones crecerán a la misma velocidad que las expectativas de Negocio. El ecosistema Open Finance aglutina, de forma

[1] https://www.bis.org/bcbs/publ/d486.pdf

[2] Coelho, L. F., Custódio, R., y Matos, M. (2025). The Open Paradigm: A Systematic Analysis of Evolutionary Frameworks and Cross-Sectoral Applications in Data-Driven Ecosystems. [Manuscrito no publicado]. Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina

simultánea, los desafíos más complejos de la práctica actual: desde la gobernanza de la inteligencia artificial o el perfilado hasta la gestión de cadenas complejas de proveedores, la ciberseguridad o la ética algorítmica.

2. FIDA: la revolución en construcción

Antes de desmembrar FIDA (Reglamento sobre el acceso a los datos financieros o Framework for Financial Data Access, por sus siglas en inglés) y de exponer sus implicaciones en privacidad, es preciso contextualizar su origen y objetivos. FIDA se constituye como un elemento estratégico dentro de la arquitectura de la economía digital de la Unión Europea. La Estrategia Europea de Datos (publicada por la Comisión el 19 de febrero de 2020)[3] es el marco horizontal que promueve, como se indica en la propia comunicación, "el desarrollo de espacios comunes de datos europeos en sectores económicos estratégicos y en ámbitos de interés público". Sobre esta base, el 24 de septiembre de 2020, la Comisión despliega la Estrategia de Finanzas Digitales[4], cuyo objetivo es detallar las prioridades para la transformación digital del sector financiero de la UE, entre ellas el marco de finanzas abiertas (FIDA).

Detrás de este plan se encuentran objetivos políticos y sociales de primer nivel, tales como: reducir la dependencia tecnológica de la UE, permitir a las empresas europeas competir por mérito y no por control de infraestructuras o promover un modelo de innovación que sitúe los valores europeos y la protección de los derechos de la ciudadanía en el centro del desarrollo tecnológico.

La iniciativa FIDA, a fecha de la elaboración de este artículo, continúa en fase de negociación. No obstante, a partir de los distintos borradores y opiniones publicados se pueden inferir los riesgos de privacidad, lo que nos permite anticipar la dirección del modelo y los desafíos que acompañarán al DPO en su implementación.

---

[3] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0066
[4] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0591

Dado que en este artículo se va a esbozar una comparativa de la posición de las instituciones europeas, el Supervisor Europeo de Protección de Datos (en adelante EDPS, por sus siglas en inglés) y el Comité Europeo de Protección de Datos en adelante EDPB, por sus siglas en inglés), conviene esquematizar cuándo se encuadran sus respectivas intervenciones. A partir de estas aportaciones, se identificarán sus prioridades y el alcance de sus preocupaciones.

- Propuesta Inicial de la Comisión (28 de junio de 2023)[5], que incluye el primer borrador de FIDA y una propuesta de PSD3 y PSR. Esta última como evolución al modelo de servicios de pago.
- Fase de Consulta y Opiniones (julio 2023 – marzo 2024), en la que intervienen autoridades supervisoras y representantes de la industria financiera. En materia de protección de datos, destacan:
    - EDPS: Opinión 38/2023 (22 agosto 2023)[6] sobre la propuesta FIDA.
    - EDPB: Declaración 2/2024 (23 mayo 2024)[7], emitida sobre el paquete completo FIDA+PSR+PSD3 como reacción al borrador del Parlamento.
- Enmiendas del Parlamento Europeo a la Propuesta de la Comisión (30 de abril de 2024)[8].
- Propuesta del Consejo (02 de diciembre de 2024)[9].
- El "Non-Paper" de la Comisión (16 de mayo de 2025)[10] que tiene como objetivo la simplificación de las decisiones tomadas en la primera fase de trílogos, Se trata de un documento de trabajo que no ha sido adoptado ni respaldado

[5] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52023PC0360
[6] https://www.edps.europa.eu/data-protection/our-work/publications/opinions/2023-08-22-edps-opinion-382023-regulation-framework-financial-data-access_en
[7] https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-22024-financial-data-access-and-payments-package_en
[8] https://www.europarl.europa.eu/doceo/document/A-9-2024-0183_ES.html
[9] https://data.consilium.europa.eu/doc/document/ST-16312-2024-INIT/en/pdf
[10] https://pensionseurope.eu/wp-content/uploads/Commission-non-paper-on-FIDA-simplification-16.05.25-1.pdf

formalmente por la Comisión Europea. La razón por la que se cita en este artículo no es otra que entenderlo como una pieza clave de las negociaciones de FIDA y de la dirección que están tomando.

Actualmente, la norma continúa en la fase de trílogos (negociaciones a tres bandas entre la Comisión, el Parlamento y el Consejo). Se trata de un momento crítico en el que se pulen los últimos detalles antes de la publicación del texto final.

3. FIDA: el esqueleto

FIDA nace con el propósito de devolver a los clientes un mayor control sobre sus datos financieros y, con ello, estimular la innovación en el sector. La propuesta de la Comisión Europea subraya que facilitar a los usuarios el acceso a su propia información financiera es un objetivo estratégico para la Unión. Según este planteamiento, abrir estos datos permitiría desarrollar servicios más centrados en las necesidades reales de las personas: desde asesoramiento de inversión más personalizado hasta evaluaciones automatizadas de solvencia que podrían mejorar el acceso de las pymes a la financiación

Los límites del tratamiento de datos personales son de sobra conocidos por cualquiera que esté familiarizado con el Reglamento General de Protección de Datos (en adelante, RGPD, por sus siglas en inglés)[11]: debe ceñirse a sus principios y garantías, más allá del entusiasmo por la transformación tecnología. Sin embargo, trasladar la normativa de privacidad al ecosistema FIDA, tan complejo como ambicioso, está resultando ya difícil en la propia producción legislativa. Con más razón lo será en la práctica para un DPO, que deberá aplicar la responsabilidad proactiva e interpretar y asesorar a Negocio.

[11] https://www.boe.es/doue/2016/119/L00001-00088.pdf

Simplificando una iniciativa que lleva años en la mesa del legislador, el modelo FIDA plantea el flujo que se resume en este apartado.

La diferencia principal con PSD2 es la prohibición absoluta de técnicas de *screen scraping*, permitidas en la regulación de servicios de pago bajo escenarios de contingencia. Como ya conoce el lector, el *screen scraping* es un método donde un programa externo lee la pantalla de la banca online del usuario como si fuera una persona, copiando la información que aparece a la vista tras entrar con las claves del cliente. FIDA elimina esta práctica al considerarla incompatible con la seguridad moderna.

1. La entidad financiera, en su condición de poseedora de los datos (en adelante, el data holder), debe poner interfaces de programación de aplicaciones (APIs) a disposición de terceros autorizados para que estos accedan a la información financiera. Asimismo, la entidad está obligada a ofrecer a sus clientes un panel de control (dashboard) que les permita gestionar de forma sencilla los permisos de acceso otorgados a dichos terceros para cada categoría de datos.
2. El acceso por terceros (Financial Information Service Providers, en adelante FISPs) – rol que nace con FIDA y que es inexistente en los modelos actuales - no es discrecional. La identificación se rige por el marco eIDAS[12] (marco europeo de identidad digital o Electronic IDentification, Authentication and trust Services, por sus siglas en inglés), utilizando certificados cualificados que aseguran la autenticidad del solicitante. Cualquier intento de alteración en el tránsito de la información —lo que comprometería la viabilidad técnica y la seguridad — provoca la ruptura del sello y el rechazo inmediato de la operación por parte del data holder.

[12] https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-80608

3. La soberanía del interesado se operativiza a través de un panel de gestión de permisos (dashboard). Este mecanismo transforma la portabilidad en un derecho dinámico, permitiendo al inversor visualizar, en tiempo real, la vigencia de las "llaves" concedidas a terceros y ejercer su derecho de revocación de forma inmediata.
4. Una vez dentro de los FISPs, los datos en crudo de uno o varios data holder se procesan mediante modelos de lenguaje capaces de combinarlos con información externa para extraer patrones o previsiones, con implicaciones evidentes en materia de perfilado y decisiones automatizadas.
5. Los FISP ponen a disposición de los data user los datos ya procesados. Esto permite a los data user: (i) la prestación de servicios más personalizados al cliente final o (ii) la adquisición resultados agregados y anonimizados que funcionan como la materia prima para impulsar la innovación.

4. Análisis de los riesgos de privacidad en la normativa FIDA

4.1. Principales riesgos de privacidad en los *borradores* de FIDA

En esta sección se presentan los principales riesgos de privacidad recogidos en las distintas versiones de FIDA, así como las medidas de mitigación que las instituciones europeas (Comisión, Parlamento y Consejo) han ido proponiendo en sus revisiones. Cabe indicar que otros actores relevantes —incluidos diversos think tanks—han emitido análisis y posicionamientos sobre estos riesgos, sin embargo, dichas aportaciones no se han incorporado en este documento.

1. **Perímetro de los datos:**

El principal debate en torno a FIDA surge alrededor del listado de datos que el data holder debe poner a disposición del data user.

<u>Problemas planteados:</u>

a) Los datos personales que trata una entidad financiera son de diversa naturaleza (incluidos datos especialmente protegidos, como son los de salud o las opiniones políticas y/o religiosas inferidas a partir de los patrones de gasto o de determinadas transacciones). Esto genera un riesgo evidente de sobreexposición del individuo.
b) Existe debate sobre si los data holder deberían compartir no solo datos brutos, sino también datos elaborados internamente (por ejemplo, puntuaciones de riesgo o los derivados de un perfilado). Las entidades financieras se oponen, ya que consideran que esto afectaría al núcleo de su negocio y podría revelar secretos comerciales. Además, si estos datos se transfieren, el cliente podría "arrastrar" su nivel de riesgo o categorización a una nueva entidad, sin posibilidad de empezar de cero.

<u>Medidas propuestas</u>

- Propuesta original de la Comisión Europea

El texto inicial establece un perímetro de uso de datos personales, excluyendo la información sobre solvencia y seguros de vida o salud para proteger la privacidad de los interesados, si bien delega en las Autoridades Europeas de Supervisión (en adelante ESAs, por sus siglas en inglés) la tarea de desarrollar directrices específicas que regulen cómo otros datos financieros sí pueden integrarse en la evaluación crediticia y en la fijación de precios de seguros.

- EDPS

El EDPS propuso excluir de la definición de "datos de cliente" aquellos datos generados mediante perfilado —es decir, datos inferidos o derivados— argumentando que compartir lo que una entidad "piensa" del cliente puede interferir en los derechos del interesado.

- Posición del Parlamento Europeo

El Parlamento acogió la recomendación del EDPS e incorporó esta exclusión en su versión del texto. El EDPB, en su Declaración 2/2024, celebra que el Parlamento busque la exclusión de los datos derivados o inferidos.

- Posición del Consejo

El Consejo amplía la exclusión no solo a los datos inferidos o derivados, sino también a cualquier dato procesado internamente. Con esta medida, se refuerza la protección tanto de los secretos comerciales como de la privacidad de los usuarios. Asimismo, el Consejo introduce la posibilidad de que el esquema limite el acceso a datos con más de diez años de antigüedad cuando estos no se encuentren digitalizados.

- Documento no oficial de la Comisión

De las propuestas del Parlamento y el Consejo, la Comisión solo incluye la regla de los diez años.

2. Granularidad de los datos

Entendemos por "granularidad" la capacidad de permitir el acceso selectivo sobre un conjunto de datos o, lo que es lo mismo, tener la capacidad de compartir ciertos tipos de datos, pero no todos. Esta concepción se alinea con las Directrices 05/2020 del EDPB[13], que establecen que el consentimiento debe ser "granular", es decir, que el interesado debe poder aceptar unas finalidades o categorías de datos y rechazar otras.

Problemas planteados:

a) La ausencia de granularidad obliga al interesado a compartir todos sus datos o a renunciar al servicio por completo.
b) Si el control no es granular, se pueden compartir datos sensibles que podrían usarse para perfilado, discriminación de precios o denegación de servicios.

13 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf

c) Si los datos no están estandarizados a un nivel granular (campos de datos específicos), es técnicamente imposible para el usuario separar qué comparte y qué no.

Medidas propuestas

- Propuesta original de la Comisión Europea

El dashboard debe mostrar "las categorías de datos que se comparten. El enfoque de la Comisión es que el permiso se otorgue para una "finalidad concreta acordada.

- EDPS

El EDPS recomienda incluir un requisito para que los data user describan claramente los tipos específicos de datos que solicitan. Utiliza como ejemplo que un cliente debería poder compartir información sobre su cuenta de ahorros con un data user y, al mismo tiempo, negarle el acceso a sus datos de pensiones.

- Posición del Parlamento Europeo

El Parlamento incluye la recomendación del EDPS. Además, identifica el riesgo de los patrones oscuros (dark patterns), explicados por la AEPD como las “interfaces e implementaciones de experiencia de usuario destinadas a influenciar en el comportamiento y las decisiones de las personas en su interacción con webs, apps y redes sociales, de forma que tomen decisiones potencialmente perjudiciales para la protección de sus datos personales”[14].

Su propuesta prohíbe diseñar la solicitud de manera que incentive o influya indebidamente en el cliente o distorsione su capacidad de decisión libre.

[14] https://www.aepd.es/prensa-y-comunicacion/blog/dark-patterns-manipulacion-en-los-servicios-de-internet

- Posición del Consejo

Exige que la solicitud de permiso incluya las categorías de datos que se comparten. Un punto técnico muy importante del Consejo es que permite a los esquemas de intercambio de datos (Financial Data Sharing Schemes, en adelante FDSS, por sus siglas en inglés) acordar la granularidad de la estandarización de los puntos de datos. Esto significa que la tecnología subyacente debe estar preparada para distinguir datos al detalle, lo que permitirá una elección "a la carta" para el interesado.

- Documento no oficial de la Comisión

La Comisión apuesta por simplificar primero qué datos entran el modelo. Su solución es reducir el volumen total de datos obligatorios y estandarizar técnicamente el resto para que no sea costoso de implementar.

3. Combinación de fuentes

La combinación de fuentes implica que el data user agregue, cruce u enriquezca los datos obtenidos a través del marco FIDA con otros conjuntos de datos que ya posee o que obtiene de terceros (fuentes de datos tradicionales, redes sociales, historial previo o datos de otras filiales del grupo).

<u>Problemas planteados:</u>

a) Combinar los datos financieros (FIDA) con datos de terceros (redes sociales, data brokers, IoT, etc.) permite crear perfiles extremadamente detallados.
b) El cruce de los datos en posesión de diferentes actores puede dar lugar a la denegación de servicios, la generación de perfiles o la diferenciación de precios.
c) Por otro lado, si se vinculan los datos financieros con el rastro digital masivo de las *Big Tech*, el riesgo de privacidad se podría elevar hasta una vigilancia total.

<u>Medidas propuestas</u>

- Propuesta original de la Comisión Europea

La Comisión no desarrolla límites materiales a la combinación de fuentes, pero delega en las *ESAs* la elaboración de directrices para cubrirlo.

- EDPS

Recomienda que las directrices de las *ESAs* delimiten la combinación de los datos de FIDA con otros tipos de datos personales, específicamente datos de redes sociales, *data brokers* y tecnologías de rastreo *(cookies*).

- Posición del Parlamento Europeo

El Parlamento propone que ni los gatekeepers (definidos por el Reglamento de Mercados Digitales, DMA por sus siglas en inglés, como grandes plataformas digitales que constituyen una puerta de acceso entre prestadores de servicios y usuarios finales)[15] ni las entidades bajo su control puedan obtener la licencia FISP. No obstante, para las entidades financieras tradicionales que sean propiedad de un gatekeeper, propone una evaluación específica realizada por la autoridad nacional, pero sujeta a un dictamen vinculante de la ESA correspondiente.

Adicionalmente, el Parlamento incorpora una salvaguarda sobre la combinación de datos, al recoger que debe hacerse en el "mejor interés del cliente" para evitar la discriminación de precios.

- Posición del Consejo

El Consejo aboga por autorizar a los gatekeepers siempre que: (i) exista una segregación de datos real entre los obtenidos en el marco de FIDA y los datos de sus plataformas; (ii) garanticen que no se usarán las ventajas de red ni datos cruzados para dominar mercados.

Por tanto, la decisión final correspondería a la autoridad nacional competente, pero esta debería justificar cualquier desviación respecto del criterio fijado por las ESAs en su

[15] https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81470

dictamen previo, elaborado tras consultar a la Comisión y al EDPB. Con este mecanismo se pretende garantizar una mayor coherencia en la aplicación del marco a nivel europeo.

- Documento no oficial de la Comisión

La Comisión quiere eliminar el proceso de evaluación previa que proponen el Consejo y el Parlamento al considerar que incrementarían la carga burocrática a la par que potenciarían la existencia de diversos criterios, en función del país. Su propuesta es apoyarse en los principios horizontales de la DMA.

4. Base de licitud

El interesado debe otorgar permiso, a través del panel, para que el data user acceda a sus datos personales en posesión del data holder. Este permiso, entendido como la "llave" para la transferencia de datos, es diferente a la base de licitud que legitima el tratamiento de los datos.

Problemas planteados

a) Determinar una base de licitud adecuada y específica para cada finalidad de tratamiento.
b) Riesgo de que el permiso en el dashboard se interprete de facto como un consentimiento único y genérico a todos los tratamientos.

Medidas propuestas

- Propuesta original de la Comisión Europea

Establece el “permiso” (mediante su activación en el dashboard) como disparador del acceso, pero reconoce que el tratamiento de datos personales requiere una base legal válida bajo el RGPD, sin aclarar del todo cómo se articulan ambas capas.

- EDPS

Alerta de que la ambigüedad crea inseguridad jurídica sobre si el permiso sustituye al consentimiento o al contrato del RGPD y reclama que se aclare expresamente que el permiso no equivale a ninguna base de licitud del RGPD.

- Posición del Parlamento Europeo

El Parlamento introduce la obligación de que el data user demuestre al data holder que cuenta con una base legal válida bajo el RGPD antes de acceder a los datos. El EDPB acoge con satisfacción este planteamiento.

Además, propone reiterar que, en caso de tratamiento de datos de categoría especial se requiere el cumplimiento de alguna de las excepciones del artículo 9 del RGPD. Cabe señalar que los datos financieros pueden revelar datos de categoría especial y con esta precisión se aclara que FIDA no crea una nueva base legal ni una excepción automática para tratar datos sensibles, sino que se subordina al RGPD.

- Posición del Consejo

Comparte que el permiso de FIDA es independiente al cumplimiento del RGPD y recoge parcialmente la inquietud del EDPS y EDPB, al proponer que se muestre en el dashboard la finalidad, etiqueta legal que pedían los supervisores.

Por último, aclara que el cliente tiene derecho a retirar el permiso FIDA en cualquier momento, y que este es independiente al derecho de retirar el consentimiento bajo el RGPD. Si el cliente retira el permiso en el dashboard, el data user debe: (i) cortar el acceso y dejar de recoger más datos y (ii) eliminar el histórico, sin dilación indebida.

- Documento no oficial de la Comisión

Sin entrar en el debate sobre la información de la base de licitud, busca la simplificación de la identificación del cliente cuando este proporcione el permiso en el dashboard a través del uso voluntario de las Carteras Europeas de Identidad Digital (EUDI Wallets)[16].

5. Seguridad de la información

FIDA implica flujos masivos de datos financieros sensibles mediante APIs, lo que podría multiplicar el número de ataques y la magnitud de las brechas de seguridad. A esto se suma una preocupación adicional: la irrupción de los FISPs, cuya supervisión podría no ser equivalente a la de las entidades tradicionales.

Problemas planteados

a) Asimetría en la supervisión: los FISPs, al ser nuevos actores no regulados previamente, manejarán volúmenes altos de datos personales sin supervisión equivalente a las entidades financieras.

b) La ausencia de estándares uniformes en el desarrollo de APIs, protocolos de autenticación y mecanismos de reporte de podría incrementar el riesgo de ciberseguridad.

Medidas propuestas

- Propuesta original de la Comisión Europea

El primer borrador de la Comisión se fundamenta en la autorización previa de los FISPs por la autoridad nacional competente, delegando en la Autoridad Bancaria Europea (EBA, por sus siglas en inglés) la elaboración de los estándares técnicos de regulación de dichas autorizaciones.

Asimismo, en materia se ciberseguridad, destaca que los data holder deben contar con APIs seguras, permitiéndoles cobrar una compensación razonable para su desarrollo.

[16] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202401183

- EDPS

Recomendó que los FDSS no solo definan estándares de interfaz, sino que “establezcan las medidas técnicas y organizativas mínimas” que todos los miembros del esquema deben implementar para garantizar un nivel adecuado de seguridad.

- Posición del Parlamento Europeo

El Parlamento acoge la recomendación del EDPS de no dejar la seguridad a discreción de cada entidad, esto es, de estandarizarla dentro del esquema, y añadió explícitamente el componente de lucha contra el fraude. Para ello, introduce la obligación de que los FDSS incluyan un mecanismo para compensar económicamente a los clientes por pérdidas de datos, fraudes o perjuicios, mencionando explícitamente los casos en que los datos se transfieran a terceros sin permiso expreso. Asimismo, exige que los miembros del esquema determinen contractualmente quién es responsable en caso de datos inexactos, fallos de seguridad o uso indebido, asegurando que siempre haya una entidad a la que reclamar.

Es importante apuntar que el EDPB, al publicar su Declaración tras la intervención del Parlamento, fue un paso más allá que el EDPS. Pidió que las APIs de los data holder tuvieran medidas técnicas para impedir que los terceros recuperen más datos de los necesarios (aterrizando a la técnica el principio de minimización de datos del RGPD). Aunque el Consejo y el Parlamento han reforzado la seguridad legal, no han incluido explícitamente esta obligación de "bloqueo técnico" en la API con la contundencia que pedía el EDPB.

- Posición del Consejo

Para garantizar una supervisión efectiva de la ciberseguridad, el Consejo endurece los requisitos de autorización exigiendo que los FISPs tengan su domicilio social en el Estado miembro donde lleven a cabo al menos una parte de sus actividades empresariales sustantivas. Esta medida busca erradicar las “entidades buzón” (*letterbox*

entities) que carecen de operaciones independientes o personal real, impidiendo así que eludan la normativa de la UE.

Aunque la prohibición del uso de credenciales compartidas es un pilar fundamental de la propuesta original de la Comisión (parte del ADN de FIDA), el Consejo refuerza la seguridad operativa introduciendo explícitamente la obligación del uso de métodos de identificación y autenticación electrónica seguros. Esto obliga a que: (i) el data user se identifique inequívocamente ante el data holder (regulación eIDAS) y (ii) el interesado se autentique mediante tokens o validaciones externas sin revelar sus claves.

Para implementar esto último, tanto el Consejo como la Comisión señalan a las EUDI Wallets como la herramienta idónea para gestionar la identidad y los permisos en el dashboard.

- Documento no oficial de la Comisión

En aras de buscar la simplificación del texto, propone saldar el debate delegando en las Organizaciones Europeas de Normalización la creación de estándares armonizados para un Marco Europeo de Datos de Confianza. De esta forma se eleva la seguridad técnica a un estándar oficial de la UE.

5.3. Riesgos específicos en entidades que actúan como data holder y data user al mismo tiempo

Es previsible que un número significativo de entidades financieras no solo pongan a disposición de terceros los datos personales que sus clientes soliciten compartir (rol de data holder), sino que, simultáneamente, mejoren la calidad de sus propios servicios incorporando datos procedentes de terceros (rol de data user). Esta dinámica introduce riesgos adicionales desde la óptica de la privacidad que el DPO debe saber gestionar.

Los datos recibidos, en calidad de data user, solo pueden emplearse para la finalidad específica autorizada por el titular; no existe base jurídica que permita registrarlos o tratarlos más allá de ese propósito concreto.

En este contexto, el DPO deberá asesorar a las áreas de negocio y de sistemas para garantizar la adecuada segregación entre los datos propios y los datos recibidos.

A diferencia de lo que ocurre con los datos personales de los que el data holder actúa como responsable del tratamiento, el permiso de los datos recibidos es volátil. El DPO debe supervisar que los sistemas sean capaces de procesar las revocaciones de permiso que el interesado otorgue ante un data holder, procediendo a la eliminación inmediata o el bloqueo de la información en los sistemas propios.

Durante el tiempo que los datos personales de terceros se traten por la entidad, el DPO debe asesorar en la implementación de medidas para evitar que aquellos alimenten los perfiles internos, generando una sobreexposición no solicitada por el cliente.

5.4. Riesgo específico del data user

En el modelo FIDA, un data user puede optar por dos vías de acceso: (i) conexión directa, al integrarse directamente con la API del data holder para obtener y procesar los datos en crudo o (ii) contratar a un FISP que actúe como agregador y, como valor añadido, normalice e interprete la información dispersa del titular.

Si bien FIDA impone obligaciones directas a los FISP, el DPO del data user debe considerar que la externalización no exime de responsabilidad. En este sentido, se le plantean, como mínimo, los siguientes retos:

- Diligencia en la cadena de valor: Es imperativo auditar la cadena de contratación y los algoritmos de los FISP. El DPO debe verificar que los modelos de interpretación no introduzcan sesgos que atenten contra el principio de no discriminación. Un diagnóstico basado en datos sesgados resultaría en un

servicio "contaminado" que podría vulnerar los derechos fundamentales del cliente desde su origen.

- Sinergia normativa (DORA y RIA): ambas normas son claros aliados. Estos marcos permiten ejercer una debida diligencia robusta sobre la resiliencia operativa y la ética algorítmica de los proveedores tecnológicos.
- RGPD: El data user debe reafirmar los principios del RGPD, garantizando que los datos recibidos (ya sean crudos o interpretados) permanezcan vinculados exclusivamente a la finalidad autorizada. Se debe evitar estrictamente que esta información externa "alimente" o se consolide en los perfiles históricos o registros permanentes de la entidad.

5. El ejercicio de la profesión: El DPO como aliado estratégico

Esta sección se plantea como un ejercicio de prospectiva al escenario FIDA, fundamentado en la aplicación de los principios inamovibles del RGPD. Al tratarse de una iniciativa en plena gestación, conviene mantenerse desde la distancia reflexiva, analizando con prudencia las obligaciones de fondo que, con independencia del texto definitivo, recaerán sobre el DPO.

En primer lugar, es preciso recordar quién es el interesado: un cliente financiero, en la mayoría de los casos, retail. Una gestión deficiente de su privacidad no solo supone una pérdida de control sobre su información, sino que puede derivar en exclusión financiera o en la imposición de condiciones abusivas. Por el contrario, una arquitectura de datos bien configurada bajo la supervisión del DPO puede generar ventajas competitivas y servicios personalizados que mejoren su salud financiera.

Ante un entorno tan complejo, nos imaginamos a un DPO que reúna habilidades multidisciplinares.

- **De carácter técnico:**

- RGPD como cimiento.
- FIDA, marco regulatorio a implementar en la entidad por Negocio.
- eIDAS II: conocimiento sobre el sellado de peticiones y el uso de certificados cualificados.
- DORA[17]: nociones suficientes de los requisitos de resiliencia operativa digital para asegurar una gestión robusta de riesgos tecnológicos y cumplimiento regulatorio.
- RIA[18]: los datos financieros, objeto de FIDA, se procesan mediante algoritmos de IA para crear perfiles, por lo que la relación entre las dos normas es fundamental.
- Ley de Gobernanza de Datos (DGA, por sus siglas en inglés)[19] y Data Act[20]: los principios generales de estas normas pueden servir al DPO para reforzar la aplicación del RGPD en el entorno FIDA.

- **Habilidades Éticas:**
  - Etiquetado de datos: El etiquetado de datos se constituye como el pilar básico en la implementación de FIDA. Este trabajo se torna fundamental para: (i) atender las solicitudes de los clientes; (ii) evitar una sobreexposición de datos o (iii) mantener registros actualizados y segmentados, evitando la combinación indebida de datos.
  - Respuesta inmediata: El DPO debe velar por que revocar el permiso, a través del dashboard, sea tan sencillo como otorgarlo. En este sentido, la capacidad de respuesta inmediata es clave para asegurar: (i) la

[17] https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81962
[18] https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81079
[19] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022R0868
[20] https://www.boe.es/doue/2023/2854/L00001-00071.pdf

eliminación definitiva de la información de exclientes; (ii) la depuración de datos obsoletos tras la cancelación de un servicio o el ejercicio de derechos o (iii) la exclusión precisa de aquellos datos que el usuario decida dejar de compartir.

    - Responsabilidad ética: Aunque la responsabilidad legal del data holder pudiera diluirse tras la transmisión, la ética profesional del DPO trascendería esa frontera. Por consiguiente, su labor sería asegurar que el "producto" que recibe el tercero sea éticamente apto.

- **Habilidades de Gobernanza (privacidad desde el diseño):**

    - Transparencia: La labor del DPO no consistiría en diseñar el dashboard, sino en mitigar el riesgo de los patrones oscuros (dark patterns).

    - Gobernanza: El DPO tendría que liderar el marco de controles sobre el ciclo de vida del dato financiero.

    - Supervisión: Su labor sería documentar y reportar si los estándares técnicos aplicados permiten el ejercicio del derecho sin barreras injustificadas, cumpliendo así con el deber de responsabilidad proactiva ante las autoridades de control.

6. Conclusiones

La implementación de FIDA no representa solo una evolución regulatoria para el sector financiero, sino un cambio estructural de la banca tal y como la conocemos.

El éxito de FIDA se medirá por la capacidad de la Unión Europea de demostrar que es posible liderar la economía digital sin sacrificar sus valores más genuinos. Prueba de ello es el debate entre el Parlamento, el Consejo y la Comisión por crear los nuevos cimientos de la Europa tecnológica.

En esta transformación la figura del DPO es fundamental, puesto que su asesoramiento tiene que servir para que la innovación no se construya a costa de la intimidad de las personas.

Así pues, la privacidad desde el diseño debe superar el cumplimiento formal, articulándose, entre otros, sobre los siguientes pilares:

- Seguridad, entendida más allá de la protección técnica frente a ciberataque: se requiere trabajar en la prevención de riesgos socioeconómicos, como la exclusión financiera de clientes vulnerables o la imposición de condiciones abusivas.
- Ética frente al perfilado invisible: se pretende lograr que el flujo masivo de datos no etiquete al usuario y culmine en una sobreexposición no deseada.
- Convergencia normativa práctica: se busca superar el conocimiento puramente teórico para liderar la confluencia regulatoria.
- Devolver al cliente el poder sobre sus datos: se persigue que la información circule en su pleno beneficio y no para alimentar su vigilancia.