

EIL – Lucha contra el fraude

La evaluación del interés legítimo (EIL) está diseñada para ayudar a decidir si la base del interés legítimo es o no aplicable al tratamiento de datos personales objeto de análisis. Es un documento validado por el DPO para garantizar su cumplimiento legal.

Parte 1: Prueba de propósito

Es necesario evaluar si existe un interés legítimo detrás del procesamiento.

CUESTIONES A VALORAR

- ¿Por qué desea procesar los datos?
- ¿Qué beneficio se espera obtener del tratamiento?
- ¿Alguna tercera parte se beneficia del tratamiento?
- ¿Hay beneficios públicos obtenidos gracias al tratamiento?
- ¿Cómo de importantes son los beneficios que usted ha identificado?
- ¿Cuál sería el impacto si no pudiera seguir adelante con el tratamiento?
- ¿Está cumpliendo con las normas específicas de protección de datos aplicables a su tratamiento (por ejemplo, requisitos de perfilado o la legislación sobre *e-privacy*)?
- ¿Está cumpliendo con otras leyes de aplicación?
- ¿Está cumpliendo con las directrices de la industria o los códigos de buenas prácticas de su sector?
- ¿Hay otras cuestiones éticas para tener en cuenta relacionadas con el procesamiento?

EVALUACIÓN

La Entidad desea procesar los datos de las operaciones que se realizan con sus productos financieros para detectar e impedir la comisión de delitos, principalmente fraudes.

La finalidad es doble:

1. Cumplir con sus obligaciones como persona jurídica relativas a prevenir la comisión de delitos tal como establece la legislación actual (Código Penal).
2. Evitar que sus productos financieros puedan ser utilizados para la comisión de delitos que perjudican a terceros (población en general entre la que pueden estar incluidos los socios de la Entidad).

Lo que hará básicamente el tratamiento es validar determinada información (intercambio de información sobre titularidad de cuentas con otras entidades financieras españolas) o buscar patrones de fraude (como el ingreso de cheques robados y manipulados) para detectar operaciones fraudulentas y pararlas, de ser posible, además de ponerlas en conocimiento de la Policía para que sean investigadas y perseguidas.

Los beneficios esperados son los siguientes:

1. Detectar y evitar la comisión de delitos en el uso de los productos y servicios de la Entidad.
2. Proteger a sus socios de ser víctimas de fraudes.
3. Colaborar en la lucha contra el fraude en el sistema financiero español.

El beneficio es general para la sociedad al ayudar a hacer más seguros los servicios financieros protegiendo a sus usuarios de ser víctimas de fraudes y poner a la Entidad en mejor disposición para colaborar con los cuerpos policiales en la identificación y persecución de los responsables de los mismos.

Si no se realiza el tratamiento, la Entidad perdería la capacidad de combatir la comisión de delitos, sobre todo en materia de prevención de los mismos, porque su conocimiento procedería únicamente de hechos ya consumados e incluso denunciados.

Los efectos perjudiciales de no llevar a cabo el tratamiento podrían ser varios:



1. Perjudicaría a la capacidad de la Entidad para acreditar el cumplimiento de sus obligaciones respecto a evitar la comisión de delitos (Código Penal-responsabilidad de personas jurídicas).
2. Perjudicaría a la protección de sus socios frente a fraudes cometidos utilizando los servicios financieros de la Entidad.
3. Perjudicaría a la propia Entidad si fuera considerada responsable y tuviera que responder por los delitos cometidos mediante sus productos y servicios.
4. Perjudicaría al sistema financiero español al no contar con la colaboración directa de la Entidad en la validación de titularidades de cuentas.

Los datos son tratados internamente y se mantienen en todo momento las protecciones establecidas por las políticas y normativas corporativas, además de aplicar criterios de minimización de datos (solo se utilizan los datos imprescindibles).

Se cumplen todas las leyes relacionadas con la banca: prevención de blanqueo, ley de cooperativas, MiFID II, PSD2...

Se cumplen las directrices del sector y los códigos de buenas prácticas.

Dada la categoría de los datos personales tratados no hay otras cuestiones éticas para valorar.

Parte 2: Prueba de la necesidad

Es necesario evaluar si el tratamiento es imprescindible para los fines que se hayan identificado.

CUESTIONES A VALORAR

- ¿Este tratamiento ayudará realmente a alcanzar su propósito?
- ¿Es el tratamiento proporcional a ese propósito?
- ¿Se puede lograr el mismo propósito sin el tratamiento?
- ¿Se puede lograr el mismo objetivo mediante el tratamiento de menos datos o mediante el tratamiento de los datos en otra forma más obvia o menos intrusiva?

EVALUACIÓN

El tratamiento es la única forma viable para alcanzar el propósito, dado que:

1. Se trata de operaciones realizadas con productos y servicios propios y la Entidad es la única que dispone de esta información.
2. Permitirá contrastar la identidad de las personas que contraten productos con la Entidad en el momento de su alta y evitar, así, que se puedan realizar operaciones delictivas.
3. Colaborará en el proceso de validación de la identidad de los socios en otras entidades, facilitando su inicio de relaciones con las mismas.

El tratamiento se considera proporcional, dado que para llevarlo a cabo:

1. Se tratarán los mínimos datos posibles.
2. En los análisis de operaciones para la prevención del fraude (limitadas a los últimos doce meses) únicamente se contará con la información transaccional originada por el uso de los productos y servicios de la Entidad.
3. Únicamente se intercambiará información con terceros en los siguientes casos:
 - a. Servicio de confirmación de titularidad de cuentas con otras entidades financieras mediante el servicio de [Iberpay](#).
 - b. Comunicación o denuncia ante la Policía cuando se detecten delitos.
4. No se incorporarán otros datos provenientes de terceros; únicamente se tratarán los que ya se encuentran bajo la responsabilidad de la Entidad y que se detallan en el documento de tratamiento de datos personales y los



obtenidos en el servicio de confirmación de titularidad de cuentas mencionado.

5. No se trasladarán a terceros, excepto en los casos indicados en el punto 3.

No es posible obtener este resultado sin llevar a cabo el tratamiento, que, como ya queda dicho, se hace a partir de los mínimos datos posibles y de la forma menos intrusiva posible (al aplicarse de forma no dirigida, sino basándose en alertas originadas por la identificación de patrones de fraude).

Parte 3: Prueba de equilibrio

Es necesario tener en cuenta el impacto en los intereses y derechos de los individuos y de sus libertades, evaluando si este impacto no es asumible y, por tanto, anula los intereses legítimos de la Entidad.

En primer lugar, hay que validar si es necesario realizar una EIPD (evaluación de impacto relativa a la protección de datos). Si es así, se deben evaluar los riesgos con más detalle.

La naturaleza de los datos personales

CUESTIONES A VALORAR

- ¿Son datos de categoría especial o datos de delitos?
- ¿Son datos que las personas probablemente consideran 'privados'?
- ¿Está tratando datos de menores o de otros colectivos vulnerables?
- ¿Son los datos sobre las personas de su ámbito personal o profesional?

EVALUACIÓN

Son los datos básicos de identificación (nombre, apellidos...), los datos sobre los productos/servicios contratados (código interno del producto, relación con el mismo...) y los datos transaccionales en el uso de los mismos mediante datos de contexto (IP, geolocalización, dispositivo utilizado...) y de las propias transacciones (cuentas de cargo, cuentas beneficiarias, fecha y hora de la transacción...).

No se tratan datos especialmente protegidos y su tratamiento tiene un enfoque indiscriminado basado en alertas ante la detección de patrones de fraude para reducir su intrusividad.

Expectativas razonables

CUESTIONES A VALORAR

- ¿Tiene una relación existente con el individuo?
- ¿Cuál es la naturaleza de la relación y cómo se han utilizado los datos en el pasado?
- ¿Se recogen los datos directamente de la persona? ¿Qué le han informado en el momento de recabar los datos?
- Si ha obtenido los datos de un tercero, ¿le informaron sobre el uso por parte de terceros para otros fines? ¿Estos fines cubren el tratamiento analizado?
- ¿Cuánto tiempo hace que recogió los datos? ¿Ha habido cambios en la tecnología o contexto desde entonces que hayan repercutido en las expectativas de los afectados?
- ¿Son los propósitos y métodos fácilmente entendidos?
- ¿La intención es hacer algo innovador?
- ¿Tiene alguna evidencia acerca de las expectativas (por ejemplo, de estudios de mercado, grupos de enfoque o de otras formas de consulta)?
- ¿Hay otros factores en este tratamiento que signifiquen que los afectados puedan no esperar este tratamiento?

EVALUACIÓN

Los datos son de socios con los que se han firmado contratos de prestación de productos o servicios financieros. Los socios son conscientes de que la Entidad tiene esta información, han venido voluntariamente a abrir una cuenta, proporcionan los datos directamente, reciben en el momento de la recogida de los datos toda la información relativa al tratamiento de sus datos personales que es requerida y operan libremente con los productos y servicios contratados.

Los datos los mantienen actualizados los propios afectados, dado que son datos necesarios para mantener la relación de prestación de servicios financieros y de seguros, o recopilados por la Entidad en el ejercicio de los servicios prestados según los contratos.

No se trata de ningún tratamiento innovador o poco conocido. Se trata de validar identidades con otras entidades financieras con las que las personas ya tienen establecidas relaciones o de revisar de forma indiscriminada las transacciones realizadas con los productos y servicios de la Entidad en busca de patrones de fraude que requieran la intervención de la Entidad para contrastarlos y actuar en consecuencia.

No se valora que pueda ser inesperado un tratamiento enfocado a combatir los delitos o fraudes en los servicios financieros. Estos han sido históricamente objeto de ataques por tratarse de servicios relacionados con el dinero, que es uno de los objetivos principales de los delincuentes. Y ante el incremento de ciberdelitos, suplantaciones de identidad, estafas en pagos, etcétera, cada vez es más patente la exigencia por parte de los usuarios de servicios financieros para que se les ofrezca mayor protección ante los delitos.

La Entidad, al ser una cooperativa de crédito y estar comprometida con sus socios, está obligada a adoptar medidas de protección y prevención de la comisión de delitos en los que tanto los socios como la propia Entidad puedan verse perjudicados directamente.

Impacto probable

CUESTIONES A VALORAR

- ¿Cuáles son los posibles efectos del tratamiento sobre las personas?
- ¿Pueden los individuos perder el control sobre el uso de sus datos personales?
- ¿Cuál es la probabilidad y severidad de cualquier impacto potencial?
- ¿Hay algunas personas que probablemente se opongan al tratamiento o les resulte intrusivo?
- ¿Usted estaría dispuesto a explicar el procesamiento de los datos personales con absoluta transparencia?
- ¿Se pueden adoptar medidas de seguridad para minimizar un posible impacto?

EVALUACIÓN

El impacto del tratamiento si se realiza erróneamente es que la Entidad no será capaz de evitar la comisión de fraudes. El perjuicio, por tanto, no viene tanto de haber realizado el tratamiento de forma incorrecta como de la materialización de la amenaza que se intenta evitar con el tratamiento.

La principal perjudicada sería, en primera instancia, la propia Entidad, que vería perjudicada su capacidad de acreditar un control efectivo para evitar la comisión de delitos. En segunda instancia, se verían perjudicados los propios socios que hayan sido afectados por la materialización del delito. Y en un tercer nivel, encontraríamos el perjuicio originado al sistema financiero español y a la sociedad por no colaborar efectivamente en la lucha para prevenir la comisión de delitos.

La información publicada en la web corporativa, que explica qué se hace con los datos de forma muy detallada (incluyendo categorías de datos, finalidad y base legítima), permite cumplir con la obligación de transparencia requerida a cualquier tratamiento de datos personales.

Las medidas internas de protección del servicio (con restricción al acceso a la información para unos perfiles muy determinados del ámbito de seguridad y con procesos automatizados de análisis de datos para generar alertas cuando se observe una coincidencia con un patrón de fraude, por ejemplo) minimizan la posibilidad de un mal uso del tratamiento y, por tanto, de un posible impacto para los afectados.

¿Se puede ofrecer a las personas una opción de exclusión?

Sí, pueden ejercer su derecho a la oposición de forma fácil y gratuita.

Tomar la decisión

En este apartado se valoran las respuestas a las partes 1, 2 y 3 para decidir si es viable contemplar el interés legítimo como base legal del tratamiento.

| | |
|--|--------------------|
| ¿Este tratamiento puede tener como base legal el interés legítimo? | Sí |
| ¿Tiene algún comentario para justificar su respuesta? (Opcional) Este tratamiento puede ser considerado una actividad esperada por los socios (que la Cooperativa de Crédito de la que son socios intente evitar la comisión de delitos en los que pueden verse perjudicados) y con un impacto muy bajo en caso de realizarse erróneamente. No se considera tampoco un tratamiento intrusivo ni se utilizan datos de categorías especialmente protegidas. | |
| EIL completada por | Caja de Ingenieros |
| Fecha de redacción | 30/04/2021 |
| Fecha de validación por el DPO | 10/05/2021 |

Tomar la decisión

En este apartado se valoran las respuestas a las partes 1, 2 y 3 para decidir si es viable contemplar el interés legítimo como base legal del tratamiento.

| | |
|---|--------------------|
| ¿Este tratamiento puede tener como base legal el interés legítimo? | Sí |
| <p>¿Tiene algún comentario para justificar su respuesta? (Opcional)</p> <p>Este tratamiento puede ser considerado una actividad esperada por los socios (que la cooperativa de crédito de la que son socios intente evitar la comisión de delitos en los que pueden verse perjudicados) y con un impacto muy bajo en caso de realizarse erróneamente. No se considera tampoco un tratamiento intrusivo ni se utilizan datos de categorías especialmente protegidas.</p> | |
| EIL completada por | Caja de Ingenieros |
| Fecha de redacción | 30/4/2021 |
| Fecha de validación por el DPO | 10/5/2021 |