



REGLAS DE FUNCIONAMIENTO DE LOS SERVICIOS DEL SEPFRA

ÍNDICE

1. INTRODUCCIÓN.....	3
2. GLOSARIO DE TÉRMINOS UTILIZADOS EN ESTE DOCUMENTO	3
3. EL CODE	5
3.1. Definición y características	5
3.2. Funciones	5
3.3. Herramientas	6
3.4. Acuerdos de colaboración	6
3.5. Formación	7
3.6. Funcionalidades de la zona restringida de la página web del CODE.....	7
4. LOS FICHEROS DER, SOR Y SOL.....	10
4.1 Finalidad de los ficheros y legitimidad del tratamiento	10
4.2 Descripción de la información contenida en los ficheros	10
4.4 Consulta al Sepfra	13
4.5 Responsabilidades	13
4.6 Obligaciones de las Entidades.....	13
4.7 Derechos de los afectados	14
4.8 Confidencialidad y medidas de seguridad.....	15
4.9 Tiempo máximo de permanencia de los datos	15
4.10 Colaboración entre Experian y las Entidades.....	15
4.11 Requisitos de autoinclusión y forma de recogida de los datos en el DER.....	15
4.12 Suspensión temporal del tratamiento en los ficheros SOR y SOL.....	17
4.13 Formulario para la recogida de datos y cláusulas de consentimiento	18

1. INTRODUCCIÓN

El presente documento describe las características de funcionamiento de los diferentes instrumentos incluidos en el Sepfra, que a continuación se enumeran:

- Centro de Observación del Delito Económico (CODE).
- Fichero de Documentos Extraviados, Robados y de autoinclusión (DER).
- Fichero del Servicio de Operaciones Registradas (SOR).
- Fichero de SOLicitudes de operaciones (SOL).

2. GLOSARIO DE TÉRMINOS UTILIZADOS EN ESTE DOCUMENTO

- a) Afectado: persona física titular de los datos que son objeto de tratamiento en el Sepfra.
- b) CODE: es un observatorio dedicado al estudio del fraude. Este Centro contará, entre otros medios, con una página web en la que los usuarios del Servicio pueden consultar toda la información relevante en materia de fraude, intercambiar experiencias, y acceder a alertas en relación a actuaciones fraudulentas, y constituirá una red de alertas con los usuarios del Sepfra para la alerta temprana de actuaciones fraudulentas.
- c) Datos inexactos, incorrectos o incompletos: información incorporada en la solicitud de una operación que no se correspondan con la realidad, sea por acción o por omisión, esto es, incluso si la información aportada debería, de conformidad con el principio de buena fe, haber sido completada con datos o informaciones adicionales.
- d) DER: es un fichero de inclusión voluntaria que contiene datos identificativos del afectado para evitar que estos datos puedan ser utilizados de forma fraudulenta.
- e) Documento identificativo: cualquier documento expedido por una administración pública española o extranjera en que conste la fotografía y la firma del afectado, y cuya finalidad sea la de identificar a una concreta persona física.
- f) Encargado del tratamiento: persona que, sola o conjuntamente con otros, trata datos de carácter personal por cuenta del responsable.
- g) Entidades Adheridas o Entidades: entidades que se adhieran al presente servicio y que sean acreedores de una operación o a la que se haya solicitado una operación. Estas entidades tienen acceso a los ficheros y le podrán ser cedidos datos personales de los afectados y/o solicitantes. Es requisito imprescindible para la participación en el Sepfra que a la entidad le haya sido solicitada una operación con los datos que informa a los ficheros o proporciona al CODE
- h) Operación: cualquier relación jurídica que implique una prestación por parte de una entidad adherida a favor del afectado a cambio de un precio
- i) Operación registrada: conjunto de datos relativos a una solicitud de una operación que (i) contenga datos inexactos, incorrectos o incompletos; y (ii) dichos datos inexactos, incorrectos e incompletos tengan la relevancia suficiente para hacer que la Entidad pudiera conceder la operación solicitada, o en otras palabras, que si la entidad conociera o hubiera conocido la falta de adecuación a la realidad de la información que figura en la solicitud, probablemente no la concedería o no la

hubiera concedido. Los campos que se incluirán en el fichero, de entre todos los de la operación, y su formato, se ajustarán al documento técnico correspondiente que esté vigente en cada momento.

- j) Persona Autorizada de Contacto (PAC): persona o personas que dentro de la organización de las entidades adheridas, tienen la responsabilidad de realizar las comprobaciones oportunas en orden a verificar que los datos cumplimentados en la solicitud son inexactos, incorrectos o incompletos. Asimismo deberán realizar las modificaciones y cancelaciones de la información aportada a los ficheros cuando sea preciso.
- k) Responsable de los ficheros: la entidad que de conformidad con la legislación sobre protección de datos, ocupa la posición de responsable del fichero. El responsable de los ficheros DER, SOR y SOL es la asociación Centro de Cooperación Interbancaria.
- l) Responsable del tratamiento: entidad que aporta información al fichero, y de conformidad con la legislación sobre protección de datos, es responsable de la calidad, exactitud y veracidad de los datos.
- m) SOL: es un fichero que contiene un archivo de solicitudes de operaciones solicitadas a las Entidades adheridas, y el conjunto de herramientas informáticas que actuarán como motor de búsqueda y comparación para detectar incongruencias que luego deberán ser analizadas e investigadas.
- n) Solicitante: persona física o jurídica en cuyo favor se solicita la operación
- o) SOR: es un fichero que almacena los datos de operaciones registradas solicitadas a cualquier entidad adherida.

3. EL CODE

3.1. Definición y características

El CODE se encargará de prestar servicios a las entidades adheridas al servicio de prevención del fraude.

Las actividades del CODE estarán dirigidas y supervisadas por Experian. El CODE realizará todas sus funciones con estricto cumplimiento de la legalidad vigente, muy especialmente de la normativa sobre protección de datos, y del resto del ordenamiento jurídico.

Especialmente garantizará la mas estricta confidencialidad en el uso de los datos a los que tenga acceso dentro de las funciones que se le asignen, no comunicando bajo ninguna circunstancia el dato de la entidad adherida al Sepfra que se los ha proporcionado, salvo que dicha entidad autorice la difusión de esa información. Asimismo garantizará la custodia de la información a la que pueda tener acceso de modo que no pueda ser difundida de ningún modo más que los establecidos en el propio Sepfra.

Estará formado por personas expertas en la lucha contra el fraude encargadas de procesar la información aportada por las entidades adheridas a través de las herramientas informáticas y ficheros (DER, SOR y SOL) utilizadas en el servicio de prevención de fraude, recopilar y poner a disposición de las entidades adheridas información sobre fraude y transmitir alertas de fraude.

El CODE podrá establecer contactos con organismos que colaboren en la lucha contra el fraude tales como los cuerpos de seguridad del estado, el Banco de España y el Consejo General del Poder Judicial con el fin de llegar a acuerdo(s) de colaboración.

3.2. Funciones

Las funciones más relevantes que desarrollará el CODE son las siguientes:

- (a) Centro de coordinación del esfuerzo de lucha contra el fraude.
- (b) Difusión de alertas tempranas de nuevos fraudes.
- (c) Centro de referencia en el estudio del delito económico en España.
- (d) Labores de interlocución con los organismos oficiales que luchan contra el fraude.
- (e) Fuente de información actualizada sobre la evolución del fraude.
- (f) Organización de eventos y seminarios sobre temas de prevención, investigación y detección del fraude. Difusión de información sobre fraude.
- (g) Formación en la lucha contra el fraude, en especial a los PAC.

- (h) Verificar que los PAC son personas correctamente formadas en la lucha contra el fraude

3.3. Herramientas

3.3.1.- Red privada de intercambio de información

Es la red de personas de contacto autorizados (PAC) de las entidades adheridas al servicio de servicio de prevención del fraude.

Esta red de intercambio de información es imprescindible para el eficaz funcionamiento del CODE, y estará formada por los PAC designados por cada entidad adherida, que tendrán acceso a la zona restringida de la página web del CODE y los encargados de transmitir y recibir alertas e información relevante sobre fraude.

3.3.2.- Página web del CODE

El instrumento principal del CODE es una página web, desarrollada al efecto, a través de la cual se relacionará con los PAC designados en cada entidad adherida, y difundirá información que pueda ser de interés para la sociedad en general.

Dispone de dos zonas perfectamente diferenciadas:

- Una pública que facilita a los consumidores toda la información disponible sobre fraude y formas de prevenirlo. Pretende conseguir el conocimiento por parte de la sociedad de la existencia de las acciones del servicio de prevención del fraude para perseguir las actuaciones fraudulentas.
- Otra restringida a los PAC, que es el medio de difusión de información y alertas a los mismos, y de intercambio de información entre ellos. En el apartado 6 de este documento se describen con mayor detalle las funcionalidades de la zona restringida de la página web del CODE.

Las entidades adheridas informarán a sus clientes finales de la existencia de una página web del sector a la que pueden acceder para recabar información sobre fraude y formas de prevención del fraude, formas de actuar en caso de haber sido víctimas de fraude, teléfonos de consulta y asistencia, etc.

3.4. Acuerdos de colaboración

La colaboración de organismos públicos es esencial para luchar de forma efectiva contra el fraude. Desde el CODE se promoverá esta colaboración y se establecerán, en su caso, protocolos de colaboración con las Fuerzas de Seguridad del Estado, Banco de España y con el Consejo General del Poder Judicial (CGPJ), y con cualquier otro organismo público o privado que se considere oportuno.

Es importante transmitir que con esta iniciativa no sólo se lucha contra el fraude para reducir los perjuicios económicos que produce, sino también contra un problema social, cuyo último perjudicado es el consumidor. El apoyo institucional al servicio de prevención del fraude de organismos como el CGPJ y el Banco de España es de gran importancia para el desarrollo del mismo, este apoyo también contribuirá a que la sociedad perciba de forma positiva esta iniciativa del sector.

La colaboración con los cuerpos y fuerzas de seguridad del Estado es especialmente importante. Hay que buscar vías de colaboración que ayuden a los mismos a la prevención, lucha e investigación de los delitos de fraude, y que potencien la efectividad del sistema.

A modo enunciativo, que no restrictivo, algunas de esas vías pueden ser:

- Permitir el acceso, con los mismos privilegios y restricciones de cualquier otro usuario, a los cuerpos y fuerzas y seguridad del estado a la información incluida en el servicio de prevención del fraude, así como a la red privada de intercambio de información, cumpliendo siempre estrictamente la normativa sobre protección de datos de carácter personal.
- Centralización de la presentación y seguimiento de las denuncias relacionadas con el fraude, que evitará la presentación de múltiples denuncias sobre los mismos hechos.
- Apoyar la labor de la judicatura en las causas relacionadas con el fraude y delitos económicos.

3.5. Formación

El CODE se encargará de coordinar la formación con las entidades adheridas al servicio, en especial de los PAC, para la utilización de las distintas herramientas a medida que las mismas se vayan poniendo en marcha.

Verificará, con los procedimientos que se determinen, la adecuación de los PAC a la lucha contra el fraude.

Promoverá la realización de un foro anual con la participación de todos los sectores afectados por el fraude.

Organizará eventos de formación sobre la prevención del fraude, tanto para personal de las entidades adheridas como para personal de los distintos organismos públicos y asociaciones privadas involucrados en la lucha contra el fraude.

El CODE participará en organizaciones nacionales e internacionales dedicadas al estudio y análisis del fraude.

3.6. Funcionalidades de la zona restringida de la página web del CODE

3.6.1. Alertas

En este área se incluirán las alertas ante cualquier actuación o sospecha de actuaciones fraudulentas. El objetivo es que las entidades adheridas tengan conocimiento a la mayor

brevedad de estas actuaciones de modo que puedan poner en marcha los mecanismos necesarios para prevenir ser víctimas del mismo fraude.

Como los ataques suelen ir dirigidos a varias entidades a la vez o concentrarse en una determinada área geográfica, una alerta temprana por parte de la entidad que primero lo detecte supondrá un freno a estos ataques evitando que el resto pueda verse afectado.

El CODE recibirá la alerta de la entidad adherida mediante correo electrónico o por un formulario incluido en la misma página, publicará la alerta dentro de este apartado de la página Web, y enviará un correo electrónico a los PAC. Las alertas quedarán registradas por orden cronológico en la página.

La inclusión de alertas se podrá hacer asimismo desde los Cuerpos de Seguridad del Estado ante cualquier indicio de actuación de bandas organizadas, para que se extremen las precauciones en una determinada zona, o ante una determinada forma de operar por parte de las mismas.

Se trata de crear una red de comunicación de alertas tempranas que permita actuar y adoptar las medidas preventivas de forma inmediata.

3.6.2. Intercambio de Información

A través de esta página, las entidades adheridas podrán intercambiar experiencias, ideas e información en materia de fraude. Esta información será enviada al CODE por los PAC y será incluida en la página para que las entidades adheridas puedan acceder a la misma.

Sin ser un foro propiamente dicho, para lo cual sería necesario establecer la figura del moderador, este intercambio de experiencias entre entidades adheridas se constituye como una plataforma en la que los mismos podrán exponer sus ideas, inquietudes y preguntas, de forma que pueda compartirlas con el resto y recibir ayuda, comentarios o respuestas de otras Entidades Adheridas, siendo el CODE un filtro previo a la inclusión de dicha información en la página.

En éste área figurará la relación actualizada de PAC. Aunque no se publicarán los nombres y datos de los contactos, se dará la posibilidad de dirigirse personalmente por correo electrónico a cada uno de ellos (mensajes privados).

3.6.3. Estadísticas

A través de la página web, el CODE proporcionará información estadística, a partir de la información obtenida de los diferentes ficheros y la información aportada por las Entidades Adheridas. Esta información servirá para identificar tendencias y ver qué tipo de actuaciones fraudulentas experimentan un mayor crecimiento, que áreas geográficas se ven más afectadas, en que épocas del año aumenta la actividad delictiva, etc.

En el apartado de estadísticas se incluirán también estadísticas de fraude a nivel internacional, analizando las formas de operar que experimentan mayor crecimiento en aquellos países dónde el problema del fraude es mayor.

Como subproducto, en esta área se realizarán encuestas relacionadas con el fraude.

3.6.4. Boletín mensual

El boletín mensual será un resumen periódico de las actividades llevadas a cabo, alertas, noticias y artículos. Este boletín está abierto a que cualquier entidad adherida pueda participar cuando lo considere oportuno.

3.6.5. Formación y anuncio de eventos

En este apartado se darán a conocer todos los eventos, seminarios, conferencias y cursos, organizados o no por el CODE, relacionados con el delito económico, con el fin de que todas las entidades adheridas puedan tener la oportunidad de asistir a los que consideren de interés para su formación.

También incorporará la información pública de eventos ya realizados, y una sección de enlaces de interés.

3.6.6. Glosario

Glosario de términos relacionados con el fraude. Definiciones de los distintos tipos de fraude y términos relacionados con el delito económico.

3.6.7. Preguntas frecuentes

Recopilación de las preguntas más frecuentes relacionadas con el fraude.

3.6.8. Información

Toda aquella información de interés se incluirá en este apartado. Contendrá una sección de noticias publicadas en prensa, otra de artículos relacionados con el delito económico, y una sección dedicada a recoger aspectos legales y novedades regulatorias en materia de fraude.

3.6.9. Documentación

Contendrá la documentación en vigor del Sepfra.

4. LOS FICHEROS DER, SOR Y SOL

4.1 Finalidad de los ficheros y legitimidad del tratamiento

Los ficheros comunes DER, SOR y SOL (en adelante “los ficheros”), tienen como finalidad prevenir el fraude en el mercado, por la vigilancia de los datos personales de los afectados, y poniendo a disposición de las entidades adheridas una herramienta de investigación que les pueda ayudar a tomar una decisión sobre las solicitudes de operaciones que se les planteen, así como detectar de forma más rápida y segura situaciones de fraude ya cometido.

El tratamiento de datos personales se legitimará a través de la inserción de una cláusula de consentimiento que deberá ser firmada por el afectado antes de la inclusión de datos. La firma se recabará en el momento en que el afectado pida su inclusión en el fichero DER, o en los formularios de solicitud de operaciones, para los ficheros SOR y SOL. Sólo se podrán incluir en los ficheros datos personales respecto de los que el afectado haya dado su consentimiento.

El presente documento regula el sistema de consulta e incorporación de la información por parte de las entidades adheridas a los ficheros. Los datos serán incluidos en los ficheros por las Entidades adheridas, que serán responsables de la calidad, exactitud y veracidad de los datos, con estricta sujeción a lo establecido en este contrato y en la documentación técnica que forma parte del mismo.

El tratamiento de datos del fichero DER se realizará de forma voluntaria, de modo que el afectado libremente decidirá si quiere someter sus datos a vigilancia, y si los quiere someter de forma indefinida o por un tiempo determinado, sin perjuicio de que podrá retirar sus datos del fichero en todo momento. Tanto para la inclusión de datos, como para su modificación y baja, se requerirá la identificación del afectado, en los términos previstos en este documento.

En el fichero DER será posible también tratar datos personales de menores o incapaces sometidos a vigilancia por su representante legal. Este será el único supuesto en el que se admitirá la inclusión de datos en dicho fichero por medio de un representante.

La consulta a los ficheros se permitirá a aquellas empresas que se adhieran y cumplan con lo dispuesto en el presente documento.

Los ficheros funcionan en régimen de estricta reciprocidad, por lo que no podrán consultar el fichero las entidades que no aporten información a los mismos.

Las Entidades Adheridas y el Responsable del Fichero deberán cumplir con exactitud todos los aspectos de funcionamiento de los ficheros.

4.2 Descripción de la información contenida en los ficheros

La información contenida en los ficheros es estrictamente confidencial, por lo que únicamente las entidades adheridas podrán consultar los datos.

4.2.1 En el fichero DER

El fichero tendrá información relativa a:

- a) Identidad del afectado, incluyendo nombre y apellidos y número del documento identificativo.
- b) Domicilios (personal, profesional, etc.) del afectado y teléfonos de contacto.

- c) Situación laboral, y datos de la empresa en la que trabaja por cuenta ajena.
- d) En caso de que el motivo de inclusión en el DER sea “robo o sustracción del documento identificativo”, los datos relativos a la denuncia del presunto acto delictivo.
- e) En el caso de que los datos se incluyan por un representante legal del afectado, la identidad del representante.

En el momento de recabar el consentimiento se indicará al afectado qué datos son obligatorios y cuáles son de aportación voluntaria.

4.2.2 En los ficheros SOR Y SOL

Los ficheros SOR y SOL contendrán información relativa a los siguientes datos:

- a) Identidad de la entidad adherida que aporta los datos
- b) Datos identificativos del afectado incluyendo nombre y apellidos, número de documento identificativo, teléfonos, etc.
- c) Domicilios del afectado.
- d) Datos identificativos de la operación, incluyendo, en su caso, número de cuenta y/o de tarjetas de crédito.
- e) Datos de situación laboral y de la empresa donde trabaja el solicitante.

En la aportación de datos al SOL si la entidad detecta que alguno de los datos que figuran en la solicitud son inexactos, incorrectos o incompletos, deberá hacerlo constar, indicando cual o cuales de los bloques de datos señalados están en esa situación.

En la aportación de datos al SOR se hará constar cual o cuales de los bloques de datos señalados es incorrecto, así como el motivo de la inclusión en el fichero de entre una lista de motivos establecida.

4.3 Aportación de datos y calidad de datos

Los datos serán incorporados a los ficheros directamente por las entidades, en la forma y por el procedimiento dispuesto en los documentos técnicos de aplicación a los ficheros, que estén en vigor en cada momento.

Las entidades deberán facilitar la incorporación de datos de afectados al fichero DER. Deberán aportar a los ficheros SOL y SOR todos los datos relativos a todas las operaciones correspondientes a su actividad económica principal o típica, de conformidad con la descripción de la entidad que se hace en la en la cláusula cuarta del contrato, siempre que dichas operaciones cumplan con los requisitos que figuren en la documentación técnica aprobada por el responsable del fichero.

No podrán incluirse en los ficheros datos relativos a un afectado que no haya dado su consentimiento para ello. Los datos de los solicitantes que no hayan firmado la solicitud sólo podrán incluirse cuando sean personas jurídicas. No podrá incorporarse, en ningún caso, ninguna mención o referencia relativa a que al afectado le ha sido impuesta alguna condena de naturaleza penal o administrativa.

Cada entidad queda obligada a verificar que el afectado a quien se refieren los datos ha prestado su consentimiento, quedando obligada a conservar el documento acreditativo

de la prestación de dicho consentimiento, con independencia de la forma en que se haya prestado el mismo y del tipo de soporte en el que dicho documento quede almacenado.

Con independencia de los informes o verificaciones que pueda solicitar, la entidad siempre conservará la capacidad de decisión acerca de la inclusión, cancelación o rectificación de los datos de los ficheros.

Sólo podrán incluirse en el fichero SOR operaciones registradas. Cada entidad queda obligada, antes de incluir datos en el SOR, a verificar que se trata de operaciones registradas, conservando los documentos justificativos de tal carácter, o alternativamente debiendo estar en condiciones de proporcionar otras pruebas válidas en derecho de que ha realizado las verificaciones pertinentes y que éstas arrojaron como resultado que nos encontramos ante una operación registrada, durante al menos el tiempo de prescripción de las posibles responsabilidades de la entidad y del responsable del fichero.

En el caso de que la entidad detecte que alguno de los datos que figuran en el fichero SOL son inexactos, incorrectos o incompletos, deberá hacerlo constar en el mismo, haciendo referencia al bloque o bloques de datos afectados.

En el caso de que existan indicios o haya alguna apariencia de que alguno de los datos que figuren en el fichero SOL pudieran ser inexactos, incorrectos o incompletos, la entidad podrá indicar que el bloque o bloque de datos afectados se encuentran “bajo investigación”. La entidad que indique que algún dato se encuentra “bajo investigación” deberá investigar diligentemente y realizar todas las verificaciones necesarias para determinar si el dato es efectivamente inexacto, incorrecto o incompleto, al objeto de confirmar a la mayor brevedad posible dicha inexactitud, o bien, volverlo al estado “ok”. En todo caso, transcurridas tres semanas desde la indicación de que algún dato se encuentra “bajo investigación”, si la entidad no modificara dicho estado, el responsable del fichero cambiará automáticamente el dato al estado “ok”.

La consideración en el fichero SOL de algún dato como inexacto, incorrecto o incompleto deberá basarse en causas objetivas. La entidad deberá realizar una investigación y deberá conservar los documentos justificativos de la misma, o alternativamente deberá estar en condiciones de proporcionar otras pruebas válidas en derecho de que ha realizado las verificaciones pertinentes y que éstas arrojaron como resultado que los datos son inexactos, incorrectos o incompletos, durante al menos el tiempo de prescripción de las posibles responsabilidades de la entidad y del responsable del fichero.

En todo caso, la inclusión de cualquier registro en el SOR o de la marca de cualquier bloque de datos como inexacto, incorrecto o incompleto en el SOL debe contar con la aprobación expresa de un PAC de la entidad, cualquiera que sea la organización y estructura interna de cada una de ellas. Los PAC serán, a todos los efectos de funcionamiento de los ficheros, los representantes de la de la entidad en lo relativo a la inclusión de datos, su cancelación, rectificación o suspensión.

La entidad debe remitir al responsable del fichero, a requerimiento de este, copia de los documentos y soportes a que se refiere el presente artículo, en el plazo de cinco días hábiles desde que le sea solicitado. En caso de que la entidad sólo disponga de otros medios de prueba alternativos, éstos deberán también ponerse a disposición del responsable del fichero en la medida de lo posible, quedando obligada la entidad a

colaborar con éste en todo lo que requiera de cara a la prueba de que los datos eran inexactos, incorrectos o incompletos o que la información incluida correspondía a una operación registrada.

4.4 Consulta al Sepfra

La consulta de datos de los ficheros por parte de las Entidades se hará mediante conexiones en tiempo real (“*on line*”) por medio de un sistema de claves de acceso secretas (“*password*”) que permita el reconocimiento unívoco de cada usuario, o bien mediante un procedimiento “*batch*” –consulta masiva–, que deberá cumplir con las medidas de seguridad pertinentes, establecidas por el responsable del fichero.

Las consultas se realizarán únicamente con la finalidad de prevención del fraude.

Las entidades adheridas tienen libertad absoluta para fijar su propia política de actuación en relación con el Sepfra, por lo que cada una decidirá en qué supuestos va a consultar los ficheros y cómo debe reaccionar ante la alerta de que los datos del solicitante de una operación coinciden con otros incluidos e cualquiera de los ficheros. En cualquier caso, la alerta generada por la coincidencia de los datos personales del solicitante de una operación, con otros incluidos en los ficheros no podrá suponer, de por sí, la denegación del servicio solicitado. La Entidad deberá dar al afectado la oportunidad de explicar las circunstancias en que los datos fueron incluidos en el SOL y de que acredite su identidad por otros medios válidos, debiendo en todo caso la entidad realizar un examen más detenido de la documentación identificativa.

No se mostrará en la consulta la información relativa a la entidad que ha aportado los datos a los ficheros.

4.5 Responsabilidades

- a) CCI es el responsable de los ficheros, en el sentido que este término tiene en la legislación de protección de datos.
- b) Las entidades adheridas tienen la consideración de responsables del tratamiento de los ficheros, por lo que son responsables de la calidad, exactitud y veracidad de los datos que hayan aportado a los mismos, debiendo asimismo mantener la información permanentemente actualizada.
- c) Los solicitantes no podrán exigir responsabilidades, ni al responsable de los ficheros, ni a la entidad adherida, por ninguna circunstancia, y muy especialmente por cualquier posible daño derivado de la aprobación o ejecución de una operación o su denegación. Las entidades mantendrán indemne al responsable de los ficheros en caso de que sufra alguna reclamación o sanción que no se fundamente en el incumplimiento de sus obligaciones expresadas en este contrato.

4.6 Obligaciones de las Entidades

Las Entidades deberán:

- a) Garantizar que la información aportada a los ficheros sea veraz, exacta, completa y actualizada.

- b) Verificar, previamente a la marca de datos como inexactos, incorrectos o incompletos en el fichero, que dicha información tiene objetivamente tal carácter.
- c) Recabar el consentimiento de los afectados exclusivamente a través de la cláusula que figura en el presente documento.
- d) Verificar que la persona que presta su consentimiento es aquella a la que se refieren los datos.
- e) Actualizar los datos y cancelar o rectificar a la mayor brevedad posible los que no estén actualizados o que figuren en el fichero con incumplimiento de las obligaciones anteriormente expuestas.
- f) Conservar los soportes en que consten los documentos u otras pruebas válidas en derecho, acreditativas de que la información aportada al SOR contienen datos inexactos, incorrectos o incompletos.
- g) En el caso de que se marquen datos como inexactos, incorrectos o incompletos, conservar los soportes en que consten los documentos u otras pruebas válidas en derecho, acreditativas de que la información aportada al SOL contienen datos inexactos, incorrectos o incompletos.
- h) En todo caso, conservar el soporte donde figure el documento acreditativo de la prestación del consentimiento del afectado, con independencia de la forma en que se haya prestado el mismo y del tipo de soporte en el que dicho documento quede almacenado. Todos estos soportes y documentación, deberán conservarse al menos durante toda la permanencia del dato en el fichero, y después de su cancelación, durante el tiempo de prescripción de las posibles responsabilidades de la entidad adherida y del responsable del fichero. Finalizado este periodo de tiempo, los soportes deberán ser destruidos.
- i) Tomar las medidas oportunas para impedir la utilización de la información contenida en los ficheros para cualquier otra finalidad distinta de la de prevenir el fraude.
- j) Designar como PAC a las personas dentro de su organización con suficiente conocimiento de los asuntos de fraude y de seguridad, y asegurarse de que cumplan sus obligaciones de conformidad con el presente Documento.
- k) Cumplir con las medidas de seguridad de nivel medio establecidos en el Real Decreto 994/1999 en los datos obtenidos de la consulta a los ficheros.
- l) Garantizar la confidencialidad de los datos.
- m) Cumplir cualquier otra obligación derivada del presente documento.

4.7 Derechos de los afectados

Los derechos de acceso, rectificación, cancelación y oposición de los afectados serán tratados de acuerdo con la legislación vigente en materia de protección de datos personales y, en concreto, de acuerdo con lo establecido a este respecto por la Ley Orgánica 15/1999, de 13 de diciembre, por el Real Decreto 1332/1994, de 20 de junio y por la Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, o legislación que las sustituya.

En el caso de que el responsable del fichero lo solicite, la entidad informante al SOR o al SOL deberá pronunciarse sobre si la petición de cancelación o rectificación de datos

efectuada por cualquier persona física o jurídica debe ser estimada. En este caso, el responsable trasladará a la entidad informante la solicitud de rectificación o cancelación recibida. La entidad deberá pronunciarse en el plazo máximo de ocho días naturales. El responsable del fichero se limitará a ejecutar la decisión de la Entidad, y a contestar al solicitante. Si en el plazo indicado la entidad no hubiera contestado, el responsable del fichero cancelará o rectificará los datos, en los términos indicados en la solicitud.

4.8 Confidencialidad y medidas de seguridad

Las entidades adheridas a los ficheros no podrán incorporar los datos procedentes de las consultas a los mismos a ninguna base de datos propia o de terceros, ni ceder, reutilizar, explotar o comunicar los mismos a terceros, debiendo guardar estricta confidencialidad de la información obtenida, sin perjuicio del cumplimiento por las entidades adheridas de sus obligaciones legales en materia de colaboración y comunicación de datos a entidades públicas y organismos públicos.

Tanto el responsable del fichero como las entidades adheridas deberán adoptar las medidas de seguridad pertinentes para evitar la pérdida, alteración, tratamiento o acceso no autorizado a los datos, entendiéndose por tales las identificadas como de nivel medio en el Reglamento aprobado por Real Decreto 994/1999 de 1 de julio, o legislación que le sustituya.

4.9 Tiempo máximo de permanencia de los datos

Los datos incluidos en el DER serán tratados durante el tiempo que indique el afectado en el momento de la inclusión de sus datos. Si el afectado no indica nada al respecto, los datos serán cancelados a los seis años contados desde su inclusión en el fichero.

Los datos contenidos en el SOL no podrán permanecer más de un año en el fichero.

Los datos contenidos en el SOR no podrán permanecer más de seis años en el fichero.

4.10 Colaboración entre Experian y las Entidades

Experian deberá prestar toda la colaboración que sea razonablemente exigible a aquellas entidades que sean objeto de cualquier tipo de queja, reclamación o investigación de cualquier carácter realizada por cualquier entidad de naturaleza pública o privada, y que soliciten esta colaboración. A tal efecto Experian podrá solicitar a la entidad que, en su caso, haya incluido en el fichero los datos objeto de la queja, reclamación o investigación, copia de la cláusula de consentimiento y de toda la documentación que según las presentes Normas de funcionamiento deba incluirse en el mismo.

4.11 Requisitos de autoinclusión y forma de recogida de los datos en el DER

Sólo se podrán incluir datos en el fichero cuando se dé cualquiera de las siguientes circunstancias o motivos de inclusión:

- a) Alta voluntaria.
- b) Pérdida del documento identificativo.
- c) Robo o sustracción del documento identificativo.

- d) DNI duplicado.
- e) Revocación de DNI electrónico

El afectado indicará cual de estos cinco motivos hay que consignar en el fichero.

4.11.1 Formas de recabar el consentimiento.

Existirán las siguientes formas de recabar los datos:

- a) Identificación presencial en un establecimiento de la entidad adherida.
- b) Identificación presencial en un establecimiento del responsable del fichero.
- c) Correo postal enviado al responsable del fichero.
- d) Por vía telefónica, siempre que la entidad adherida tenga previamente identificado al afectado de forma indubitada con anterioridad al momento de recabar el consentimiento para incluir los datos en el fichero. La Entidad está obligada a facilitar al afectado el derecho de información y a recabar el consentimiento de conformidad con lo previsto en la legislación vigente. El consentimiento deberá recabarse en términos equiparables a los que figuran en el formulario de auto-inclusión que figura anexo al presente Documento.
- e) Por vía telemática, siempre que la entidad adherida tenga previamente identificado al afectado de forma indubitada con anterioridad al momento de recabar el consentimiento para incluir los datos en el fichero. En este caso, la entidad adherida y el responsable del fichero establecerán un canal seguro que redireccione al afectado cuyo consentimiento se está recabando, desde los sistemas informáticos de la entidad a los del responsable del fichero, donde éste le presentará el formulario de recogida de datos para recabar el consentimiento.

La Entidad adherida será responsable de la identificación del usuario en los casos a), d) y e). También será responsable en los casos a) y d) de que el consentimiento ha sido correctamente recabado. Además, en los supuestos a) y d), la entidad debe incluir los datos en el fichero, a través de los procedimientos dispuestos para ello por el responsable del fichero, por lo que, además será responsable de que los datos incluidos en el fichero coinciden con los que han sido facilitados por el afectado.

4.11.2 Procedimiento y documentación

En los casos a), b) y c) del apartado anterior, deberá utilizarse, única y exclusivamente el formulario de auto inclusión que se adjunta a las presentes Normas de Funcionamiento, que deberá ser firmado personalmente por el afectado o su representante legal. Además, en estos casos será necesario adjuntar al formulario la siguiente documentación:

- Cuando el motivo de inclusión sea *“alta voluntaria”*: fotocopia del Documento identificativo.
- Cuando el motivo de inclusión sea *“pérdida del documento identificativo”*: fotocopia del Documento identificativo (si es que ya se ha obtenido un duplicado del mismo) o fotocopia del resguardo provisional de estar tramitando la expedición del duplicado del Documento perdido u otro documento que acredite la pérdida del mismo así como de algún documento identificativo alternativo.

- Cuando el motivo de inclusión sea “robo o sustracción del documento identificativo”: fotocopia de la denuncia presentada ante cualquier cuerpo policial u órgano jurisdiccional.

- Cuando el motivo de inclusión sea “DNI duplicado”: fotocopia del DNI.

Cualquiera que sea el procedimiento de recabar datos, siempre que se incluyan datos de menores de edad o incapaces por su representante legal, el representante legal deberá acreditar su condición, debiendo adjuntar fotocopia del documento identificativo del representante y la documentación acreditativa de la representación.

4.11.3 Conservación de documentación y soportes

En el caso a) del apartado 4.11.1, la Entidad Adherida conservará el formulario de auto-inclusión original y la documentación aportada, aplicando las medidas de seguridad adecuadas.

En los casos b) y c) del apartado 4.11.1, el Responsable del fichero custodiará el formulario de auto-inclusión y la documentación aportada, aplicando las medidas de seguridad adecuadas.

En el caso d) del apartado 4.11.1, la entidad adherida deberá grabar la conversación telefónica donde el afectado dé el consentimiento para la auto inclusión en el fichero y deberá custodiar el soporte de grabación aplicando las medidas de seguridad adecuadas.

En el caso e) del apartado 4.11.1, tanto la entidad adherida como el responsable del fichero deberán custodiar el registro de la transacción electrónica producida en sus respectivos sistemas, custodiando el correspondiente soporte aplicando las medidas de seguridad adecuadas.

Los soportes deberán conservarse al menos durante todo el tiempo de la permanencia del dato en el fichero, y después de su cancelación, durante todo el tiempo de prescripción de las posibles responsabilidades de la entidad adherida y del responsable del fichero. Finalizado dicho periodo de tiempo, los soportes deberán ser destruidos.

En el caso de que los soportes los custodie la Entidad Adherida, ésta deberá remitir al responsable del fichero copia del formulario y de toda la documentación ajena, en el plazo de siete días naturales desde que el responsable del fichero se lo solicite.

4.12 Suspensión temporal del tratamiento en los ficheros SOR y SOL

Cualquier entidad adherida podrá ordenar al responsable del fichero que proceda a suspender temporalmente el tratamiento de uno o varios datos que haya aportado al fichero.

Igualmente, el responsable del fichero podrá suspender temporalmente el tratamiento de uno o varios datos, de oficio o a instancia de alguna entidad adherida distinta de la que aportó los datos, cuando tenga conocimiento o sospecha de que los datos han podido incluirse en el fichero con incumplimiento de cualquier aspecto del presente documento. En estos casos, el responsable del fichero comunicará a la entidad informante que el dato o datos han sido suspendidos temporalmente de tratamiento, y le requerirá para que indique si la suspensión debe mantenerse o si los datos deben ser cancelados.

La suspensión durará un máximo de diez días hábiles, desde la fecha en que fue adoptada por el responsable del fichero. Si en dicho plazo la entidad informante no levantara la suspensión, el responsable del fichero cancelará los datos.

La suspensión implicará la imposibilidad de consultar el dato o los datos correspondientes, de modo que para las entidades adheridas será, a todos los efectos como si los datos no estuvieran en el fichero durante el periodo de suspensión.

4.13 Formulario para la recogida de datos y cláusulas de consentimiento

4.13.1 Formulario de recogida de datos y cláusula de consentimiento del fichero DER

FORMULARIO DE AUTOINCLUSIÓN AL FICHERO DER

(*Campos obligatorios)

Datos del solicitante*

Nombre*:..... Apellido 1*:..... Apellido 2*:.....
 Fecha de Nacimiento:..... Correo Electrónico:..... Teléfono fijo:.....
 Teléfono móvil:..... Teléfono trabajo:..... País de Nacimiento:.....

Tipo Documento*: Documento Nacional de Identidad Pasaporte N° Documento*:.....
Marcar con X Tarjeta de Residencia Otros

Datos del domicilio personal*

1ª Dirección
 Tipo de Vía*:..... Nombre de Vía*:..... Resto Dirección*:.....
 Código Postal*:..... Localidad*:..... Provincia*:.....
 País de Residencia*:.....

2ª Dirección
 Tipo de Vía*:..... Nombre de Vía*:..... Resto Dirección*:.....
 Código Postal*:..... Localidad*:..... Provincia*:.....
 País de Residencia*:.....

Motivos de Inclusión*

Marcar con X Alta voluntaria Robo/sustracción de Documento Identificativo
 Pérdida de Documento Identificativo Documento Nacional de Identidad Duplicado
 Revocación de DNI electrónico

Acción*

Marcar con X Alta
 Modificación

Datos de identificación representante (Indicar si los datos han sido introducidos por representante legal)

Autorización Sí
Legal*: No
Marcar con X

Nombre Representante..... Apellido 1:..... Apellido 2:.....

Tipo Documento*: Documento Nacional de Identidad Pasaporte N° Documento:.....
Marcar con X Tarjeta de Residencia Otros

Otros datos (Será obligatorio si desea que sus datos se cancelen en un plazo inferior a 6 años)

Fecha de baja:.....

Datos de la denuncia (Rellénese en caso de robo del Documento Identificativo)

Fecha de la Denuncia..... N° referencia de denuncia:.....
 Cuerpo policial Comisaría

Se acompañará fotocopia del Documento Identificativo cuando el motivo de inclusión al fichero sea "alta voluntaria" o "DNI duplicado". Cuando el motivo de inclusión sea "pérdida del documento identificativo" se acompañará fotocopia del Documento Identificativo (si ya se ha obtenido un duplicado del mismo) o fotocopia del resguardo provisional de estar tramitando la expedición del duplicado del documento perdido u otro documento que acredite la pérdida del mismo, más la fotocopia de algún otro documento identificativo alternativo. Cuando el motivo de inclusión sea "robo o sustracción del documento identificativo" se acompañará fotocopia de la denuncia presentada ante cualquier cuerpo policial u órgano jurisdiccional. Por último, siempre que se incluyan datos de menores de edad o incapaces por su representante legal, el representante legal deberá acreditar su condición, debiendo adjuntar fotocopia del documento identificativo del representante así como fotocopia del documento acreditativo de la representación.

De conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, Ud. otorga expresamente su consentimiento y reconoce haber sido informado de que la entidad CENTRO DE COOPERACIÓN INTERBANCARIA (en adelante, CCI) con domicilio en la calle Miguel Ángel, 23 2º, 28010 Madrid, incluirá los datos personales que constan en la presente solicitud así como aquellos que figuren en la documentación aportada, en un fichero responsabilidad de CCI denominado "Documentos Extraviados y Robados y de autoinclusión" (en adelante, DER) con la finalidad de que sus datos sean sometidos a vigilancia y puedan contribuir a prevenir el fraude que se pueda cometer con los mismos. Igualmente, Ud. consiente expresamente y manifiesta haber sido informado de que CCI cederá sus datos a entidades financieras y bancarias, entidades del sector de las telecomunicaciones y de seguros, entidades de inversión, entidades de emisión de tarjetas de pago, entidades de renting ,operadores energéticos de gas o comercialización de electricidad, que se hayan adherido al servicio y las Administraciones Públicas que en el ejercicio de sus funciones necesiten los datos para las finalidades mencionadas anteriormente. Relación completa de las entidades adheridas al servicio en www..... CCI no concede, ni Ud. recibe, ninguna otra garantía, expresa o implícita, de que con el DER se pueda evitar un fraude que utilice sus datos personales. El solicitante podrá ejercitar sus derechos de acceso, rectificación, cancelación y oposición mediante solicitud firmada acompañada de fotocopia de su DNI al Apartado de Correos nº..... Asimismo Ud. exime de toda responsabilidad a CCI y a las entidades adheridas por los daños producidos como consecuencia de la aprobación o denegación del servicio cuando lo solicite Ud.

En.....a.....de.....de.....

Firma:.....

4.13.2 Cláusula de consentimiento de los ficheros SOR y SOL

La cláusula recogida mas adelante será de obligada firma por los solicitantes que tengan el carácter de persona física.

Si el solicitante es una persona jurídica, no será obligatorio recabar el consentimiento, aunque se recuerda que la Ley de Disciplina e Intervención de Entidades de Crédito recoge en la Disposición adicional Primera que “Las entidades ... están obligadas a guardar reserva de las informaciones relativas a saldos, posiciones, transacciones y demás operaciones de sus clientes sin que las mismas puedan ser comunicadas a terceros y objeto de divulgación.”.

Una interpretación amplia de este párrafo puede llevar a suponer que tampoco se podrían comunicar a terceros datos de peticiones de operaciones, por lo que las entidades usuarias del Sepfra deben considerar la obligatoriedad de que sus clientes personas jurídicas suscriban la cláusula que se detalla:

Contenido de la cláusula:

El solicitante otorga expresamente su consentimiento y reconoce haber sido informado de:

- *Que la ENTIDAD cederá los datos personales que constan en la presente solicitud así como, en su caso, aquellos que figuren en la documentación aportada por el solicitante, a Centro de Cooperación Interbancaria (en adelante CCI) con la finalidad de que los incorpore a un fichero común, del que es Responsable, para la prevención del fraude en las solicitudes de un producto o servicio.*
- *Que la ENTIDAD consultará el fichero común como parte del estudio dirigido a determinar la procedencia de conceder el producto o servicio solicitado.*
- *Que dicho fichero común tiene como finalidad detectar automáticamente la existencia de datos potencialmente erróneos o fraudulentos mediante la verificación de la corrección y congruencia de los datos facilitados a través de la presente solicitud y, en su caso, de la documentación que acompañe, así como mediante su comparación con: (i) datos que figuren en el fichero común como consecuencia de solicitudes aportadas por las ENTIDADES participantes en este fichero común; (ii) resultados sobre exactitud, corrección y congruencia aportados por las ENTIDADES participantes en el fichero común; (iii) datos que la ENTIDAD pueda disponer con motivo de otras relaciones contractuales mantenidas con el solicitante; (iv) datos disociados que figuren en fuentes externas (callejeros, guía de sucursales bancarias, etc.), incluyendo bases de datos de segmentación geodemográfica; (v) datos personales que figuren en fuentes accesibles al público (guías telefónicas, boletines oficiales, etc.); y (vi) el fichero DER (documentos extraviados o robados), del que es responsable CCI y donde están incluidos los datos identificativos de aquellas personas que voluntariamente han decidido someterlos a vigilancia para prevenir el fraude.*
- *Que si se diera el caso de que alguno de los datos aportados por Vd. o que figuren en la documentación requerida fuera inexacto, incorrecto o incongruente, la ENTIDAD podrá comunicar dichos datos personales al fichero común con la mención de "operaciones registradas", pudiendo ser considerados, como tales, por las ENTIDADES participantes en el sistema. Igualmente, si de alguno de los datos aportados en la solicitud y/o la documentación se dedujera la existencia de indicios sobre la comisión o tentativa de un delito, se comunicarán los datos relevantes a las Fuerzas o Cuerpos de Seguridad, la Fiscalía o los órganos jurisdiccionales competentes.*

- *Que, en consecuencia, CCI realizará los tratamientos expuestos y cederá sus datos personales con las finalidades descritas en el apartado anterior, a todas las ENTIDADES que participen en el fichero común.
e podrá ejercitar sus derechos de acceso, rectificación, cancelación u oposición, dirigiéndose para ello a la siguiente dirección:*