COMISIÓN
PARA EL MERCADO
FINANCIERO

PROPUESTA CONCEPTUAL

CONSENTIMIENTO EN EL SISTEMA DE FINANZAS ABIERTAS

Noviembre 2023
www.cmfchile.cl

I. INTRODUCCIÓN

El 4 de enero de 2023 se publicó en el Diario Oficial la Ley N°21.521, conocida como Ley Fintec. Esta ley, con el objetivo de promover la competencia, innovación e inclusión en el sistema financiero, en su Título III establece las reglas y principios básicos para la implementación de un sistema de finanzas abiertas, que permita el intercambio -entre distintos prestadores de servicios- de información y otros tipos de datos de clientes financieros que hayan consentido expresamente en ello.

La presente propuesta conceptual propone lineamientos regulatorios sobre la forma en que se reputará otorgado el consentimiento expreso de los clientes para todos los efectos legales y la forma en que el cliente podrá revocar dicho consentimiento. Asimismo, la información que tanto los Proveedores de Servicios Basados en Información (PSBI) como los Proveedores de Servicio de Iniciación de Pago (PSIP) deberán proporcionar a los clientes respecto a las solicitudes de información o iniciación de pagos ejecutados conforme a las autorizaciones correspondientes.

Estos lineamientos pretenden cubrir lo que la propia Ley Fintec encomienda a esta Comisión en su artículo 23, así como áreas de preocupación que han sido manifestadas por organismos internacionales y estudios en torno al consentimiento.

II. ESTUDIOS, PRINCIPIOS Y RECOMENDACIONES INTERNACIONALES

El sistema de finanzas abiertas brinda a los titulares de datos más control sobre su información financiera y la posibilidad de decidir con quién les gustaría compartir esta información con el objeto de obtener ofertas de productos o servicios, ya sea por primera vez, adicionales, más convenientes y atractivos (Medine y Plaitakis, 2023)[1].

Bajo este contexto, el consentimiento del titular de datos es clave. Existen una serie de documentos publicados por distintos organismos internacionales, así como estudios, que se refieren y coinciden en los desafíos que se presentan para validar/confirmar/asegurar el consentimiento del titular de los datos.

Investigaciones muestran la carga que supone para los titulares de datos leer las políticas de privacidad para el otorgamiento del consentimiento. Además, a medida que crece el comercio y las actividades en el mundo digital. Dicha carga no sólo se relaciona al tiempo que le tomaría a los clientes leer la información proveída en este proceso, sino que además a la dificultad para entenderla,

[1] Medine, David and Plaitakis, Ariadne. 2023. "Combining Open Finance and Data Protection for Low-Income Consumers." Washington, D.C.: CGAP. Recuperado de https://www.rfilc.org/wp-content/uploads/2023/03/Combining-Open-Finance-and-Data-Protection-for-Low-Income-Consumers.pdf

incluso si son individuos alfabetizados y educados, debido al lenguaje jurídico que se emplea. Por otra parte, los tamaños y formatos utilizados generalmente hacen más difícil la identificación rápida de datos o temas clave, convirtiéndose en otro factor que contribuye a que el consentimiento no sea informado.

Adicionalmente, se observa que, en la mayoría de los casos, el consentimiento para compartir información se presenta junto con otros acuerdos entre la institución y el cliente, lo que hace que la mayoría de las personas no estén consciente de estar consistiendo el uso de sus datos personales. En ocasiones el consentimiento se recoge a través de marcas en casillas o a través de otras formas, que no permiten que el cliente pueda comprender realmente el alcance de lo que está aceptando ni sus implicancias, muchas veces consintiendo el tratamiento de datos personales que no son necesarios para el acceso o uso del producto o servicio que quieren contratar.

El **Panel de Consumidores de Servicios Financieros** (FSCP, por sus siglas en inglés) encargaron una investigación, antes del lanzamiento de la Banca Abierta en Reino Unido, con la finalidad de levantar información sobre la gobernanza y seguridad de los datos en el contexto de los clientes que dan su consentimiento a aplicaciones y servicios de terceros que les permiten acceder a sus datos de transacciones financieras[2].

Entre los temas que el FSCP estaba interesado en profundizar, se encontraba el saber hasta qué punto los clientes entienden: i) el tipo de consentimiento que han otorgado a los Proveedores de Servicios de Información de Cuentas (AISP, por sus siglas en inglés) para hacer uso de sus datos; y ii) los términos y condiciones del servicio al que se han suscrito (con respecto al consentimiento que han otorgado).

Respecto al primero, la evidencia de la investigación empírica sugirió que el consentimiento frecuentemente no se otorga libremente, ni es inequívoco ni completamente informado. Más de la mitad de los encuestados afirmaron no leer los términos y condiciones de los productos y servicios a los que se suscriben, incluidos los servicios específicos que acceden a sus datos financieros. De manera similar, sólo una pequeña proporción de participantes respondió correctamente una pregunta sobre un detalle de la política, incluso después de haber tenido la oportunidad de releer la política en un entorno de investigación.

Para otros, el consentimiento se daría independientemente de lo especificado en los términos y condiciones porque ya habían decidido utilizar la aplicación o el servicio. Por último, otro grupo dijo dar el consentimiento y simplemente confiar en suposiciones sobre el entorno regulatorio, incluida la protección de datos y la supervisión de los servicios financieros, si surgieran problemas.

[2] Whitley E., y Pujadas R. (2018): "Report on a study of how consumers currently consent to share their financial data with a third party". Recuperado de https://www.fs-cp.org.uk/sites/default/files/fscp_report_on_how_consumers_currently_consent_to_share_their_data.pdf

Sobre al segundo tema, el informe señala que, dada la escasa comprensión de los términos y condiciones, tal vez no sea sorprendente que, durante las entrevistas, pocos participantes en la investigación apreciaran plenamente las consecuencias de lo que habían firmado, incluidos algunos que creían que ni siquiera habían dado su consentimiento para que se compartieran sus datos.

Como se puede ver, los resultados de dicha investigación reafirman lo señalado previamente sobre las problemáticas que presenta el consentimiento, que finalmente podrían impedir que éste sea una herramienta que otorgue al interesado control sobre el procesamiento de sus datos, en cuyo caso no constituiría una base jurídica válida para el tratamiento, considerándola ilegítima, de acuerdo con lo que indica el **Comité Europeo de Protección de Datos.**[3]

Para enfrentar algunos de estos desafíos, el **Banco Mundial**[4] ha señalado que el consentimiento se debe entender como parte de un enfoque más integral de protección de los intereses de los titulares de datos. Para aquello, es necesario que el sistema de finanzas abiertas cuente con un marco adecuado de protección de datos y del titular de los mismos. En algunos casos, esto implica aportes, supervisión y retroalimentación de los titulares de datos. En otros, se relacionan con la "arquitectura de privacidad" integrada en los productos y servicios financieros, de la que los titulares de datos tal vez nunca sean conscientes.

Para abordar lo anterior, los avisos de privacidad que establecen los términos y condiciones para el tratamiento de los datos del titular, y que son requeridos por la ley y/o la regulación, son valiosos tanto para los reguladores como para establecer expectativas de comportamiento en toda la industria, ya que crean la base para la supervisión y el cumplimiento regulatorio, y deberían estar disponibles al público en general.

Los paneles de control, por su parte, son una herramienta de gestión común con una visualización consolidada de información, utilizados en muchas industrias para que los clientes administren sus conexiones con los proveedores de servicios, y se consideran como un enfoque innovador para aumentar la transparencia y que los titulares tengan control de sus datos. Asimismo, los paneles de control pueden abordan algunas limitaciones que presentan los formularios de otorgamiento del consentimiento en papel o virtuales, ya que permiten a los individuos revisar rápidamente la información personal que comparten. Además, al existir una ubicación común para la información, sería

[3] EDPB (European Data Protection Board). 2020b. "Guidelines 05/2020 on Consent under Regulation 2016/679." Version 1.1, adopted on May 4, 2020. Recuperado de https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[4] The World Bank Group (2021): "The Role of Consumer Consent in Open Banking". Recuperado de https://documents1.worldbank.org/curated/en/099425002082230437/pdf/P1705050aeb8e704f088260f228802b73b8.pdf

más fácil para los titulares de datos informarse de los datos que han compartido, durante cuánto tiempo y con quién.

Medine y Plaitakis (2023) señalan que, bajo el contexto de finanzas abiertas, ciertos pasos pueden mejorar la probabilidad de obtener un consentimiento expreso. Citan una investigación realizada por el Grupo Consultivo para Ayudar a los Pobres (CGAP, por sus siglas en inglés) que reveló que muchas personas que no saben leer ni escribir prefieren formas de consentimiento más visuales, verbales o en video que puedan comprender fácilmente sin depender de otros para ello. Otra opción es incluir un proceso de consentimiento por separado, en forma independiente de otras partes de los acuerdos con el cliente (por ejemplo, en una página o pantalla separada).

Por su parte, un enfoque común de otorgamiento de consentimiento también contribuiría a que éste fuera expreso, ya que a medida que los titulares de datos se familiaricen con sus opciones, ya no deberían tener la carga de averiguar el enfoque de cada proveedor para dar su consentimiento (Medine y Plaitakis, 2023).

En ese sentido, Tiwari et al., (2022)[5] proponen un sistema de gestión del consentimiento que permita a los titulares de datos utilizar su información personal y financiera para su propio beneficio. Para ello, señalan que un sistema eficaz de intercambio de datos en el marco de un sistema de finanzas abiertas, basado en el consentimiento, debiera contener dos pilares. El primero, un marco de políticas de protección de datos; y el segundo, una infraestructura que permita una implementación amigable de este marco.

Respecto a al segundo pilar, indican que debe ser independiente del sector para permitir aplicaciones intersectoriales. Para dar cabida a los numerosos actores involucrados, como los proveedores de servicios financieros y de datos, así como a las instituciones del sector público y privado, las plataformas sobre las que opera la infraestructura deben ser abiertas, interoperables y no discriminatorias. Al mismo tiempo, su diseño debe garantizar la seguridad de los datos.

Ahora, se debe tener presente que la cantidad de datos que deben gestionarse dentro del sistema de finanzas abiertas es enorme, considerando la necesidad de granularidad del consentimiento, y que los datos deben distribuirse entre muchos usuarios y proveedores. Por lo tanto, para ahorrar en costos, la gestión de datos debe tener una base digital y ser escalable para un gran número de usuarios.

Cuando los datos se comparten entre proveedores y usuarios de datos, el sistema de gobernanza de datos debe especificar qué datos se solicita compartir,

[5] Tiwari, S., Sharma, S., Shetty, S., & Packer, F. (2022): "The design of a data governance system". BIS Papers.

durante cuánto tiempo serán retenidos por los que traten dichos datos y quién los tratará.

III. EXPERIENCIAS REGULATORIAS EN JURISDICCIONES EXTRANJERAS

1. Unión Europea

La Directiva de Servicios de Pagos Revisada o Segunda Directiva de Servicios Pagos (PSD2, por sus siglas en inglés)[6], es la que regula los servicios de pago electrónico e incluye el marco regulatorio para la banca abierta. Además, el tratamiento de datos de personales está regulado por el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés)[7]

El GDPR señala que el consentimiento es considerado válido si este se dio "*mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen con una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal*."

Asimismo, este Reglamento establece cuatro condiciones adicionales para el consentimiento: (i) la necesidad de demostrar que el interesado ha dado su consentimiento para el procesamiento de sus datos personales, (ii) la solicitud de consentimiento se presentará de manera que sea claramente distinguible de los demás asuntos, en forma inteligible y fácilmente accesible, y que utilice un lenguaje claro y sencillo, (iii) el derecho a retirar su consentimiento en cualquier momento; será tan fácil revocar el consentimiento como darlo, y (iv) cuando el consentimiento esté condicionado a la ejecución de un contrato, el tratamiento de datos personales se limitará a lo necesario para la ejecución de ese contrato.

El GDPR no define el consentimiento explícito; sin embargo, se pueden encontrar directrices respecto a éste en el Comité Europeo de Protección de Datos (EDPB, por sus siglas en inglés)[8], el que se señala que "*explícito se refiere a la manera en que el interesado expresa el consentimiento. Significa que el interesado debe realizar una declaración expresa de consentimiento.".* Para lo cual el interesado puede *"emitir la declaración requerida rellenando un impreso electrónico,*

---

[6] Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32015L2366

7 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&qid=1693779118167

[8] EDPB (European Data Protection Board). 2020b. "Guidelines 05/2020 on Consent under Regulation 2016/679." Version 1.1, adopted on May 4, 2020. Recuperado de https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

enviando un correo electrónico, cargando un documento escaneado con su firma o utilizando una firma electrónica".

Asimismo, agrega el EDPB, que "*un responsable del tratamiento puede obtener también consentimiento explícito de una persona que visita su sitio web ofreciendo una pantalla de consentimiento explícito que contenga casillas de Sí y No, siempre que el texto indique claramente el consentimiento, por ejemplo, «Yo, doy mi consentimiento al tratamiento de mis datos» y no, por ejemplo, «Tengo claro que mis datos van a ser tratados».*"

EDPB, en línea con la PSD2, contempla la verificación del consentimiento en dos etapas como "*una forma de garantizar que el consentimiento explícito sea válido*". Por ejemplo, un interesado (titular de datos en nuestra legislación local) recibe una notificación por correo electrónico sobre la intención del controlador (responsable de datos) de procesar un registro que contiene datos. El controlador explica en el correo electrónico que solicita consentimiento para el uso de un conjunto específico de información para un propósito específico. Si el interesado acepta el uso de estos datos, el responsable del tratamiento le solicita una respuesta por correo electrónico que contenga la declaración "Estoy de acuerdo". Después de enviar la respuesta, el interesado recibe un enlace de verificación en el que debe hacer clic, o un mensaje SMS con un código de verificación, para confirmar el acuerdo.

Respecto a la revocación del consentimiento, el responsable del tratamiento debe garantizar que el interesado pueda retirar el consentimiento con la misma facilidad con la que lo otorga y en cualquier momento. En ese sentido, el EDPB menciona que, si el consentimiento se obtiene por medios electrónicos con un solo clic, deslizamiento o pulsación de tecla del ratón, los interesados deben, en la práctica, poder revocar ese consentimiento con la misma facilidad. Cuando el consentimiento se obtiene mediante el uso de una interfaz de usuario específica de un servicio, un interesado debe poder revocar el consentimiento a través de la misma interfaz electrónica.

Además, el EDPB agrega que el interesado debe poder retirar su consentimiento sin que ello le reporte perjuicio alguno, lo que implicaría que la revocación del consentimiento debe ser gratuita.

2. **Reino Unido**

Para facilitar el cumplimiento de las obligaciones del GDPR y el Reglamento de servicios de pago de 2017 (PSR, por sus siglas en inglés)[9], la Entidad de implementación de Banca Abierta en Reino Unido, OBIE (por sus siglas en inglés)[10], ha diseñado un conjunto de estándares sobre la materia.

Dentro de esos estándares, se incluyen los relativos a los paneles de control para garantizar que los clientes puedan ver y administrar (es decir, cancelar/revocar si lo deseaban) los consentimientos de terceras partes (TPP) y los acuerdos de acceso del Proveedor de Servicios de Pago de Servicios de Cuenta (ASPSP, por sus siglas en inglés)[11,12].

A su vez, en materia de vigencia del consentimiento, se ha establecido que, si nada dice el cliente, será de un máximo de 90 días, en tanto éste no lo hubiere revocado.

Con el objeto de conocer la aplicación práctica de esos estándares, se revisaron los sitios de algunas entidades de esta jurisdicción, observándose un caso en que la entidad solicita al titular de datos que indique: (i) a quién se le otorgan acceso a sus datos (identidad TPP); (ii) con qué propósito usarán sus datos (pago/ detalles de la cuenta); (iii) durante qué período de tiempo podrán usar sus datos (número de días); y (iv) proceso de vencimiento (cuándo caducará y cómo el usuario puede revocar el consentimiento). La interfaz muestra al usuario qué información se solicita y con qué fines. El usuario puede optar por no participar y hay suficiente información disponible sobre el permiso de duración determinada (será utilizada tanto por el TPP como por las interfaces bancarias). Una vez que se informa al usuario sobre cómo dar su consentimiento, es responsabilidad del banco hacerse cargo y proporcionarle al usuario mecanismos de autenticación para garantizar la seguridad de los datos del cliente. Luego, se presentan al usuario los detalles sobre el consentimiento requerido en la interfaz de usuario-banco y se le pide que permita o rechace la solicitud del TPP para acceder a los datos mostrados. La respuesta del usuario debe registrarse y almacenarse.

---

[9] PS2 es transpuesta al régimen de Reino Unido a través de PSR.

[10] OBIE fue fundada por la CMA9 como una sociedad limitada, Open Banking Limited (OBL). Recuperado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1086515/Consultation_response_publication.pdf . La CMA determina la gobernanza, la composición y el presupuesto de la OBIE.

[11] Open Banking. Recuperado de https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/obie_submission_to_edpb_on_guidelines_06.2020_on_the_interplay_of_psd2_and_gdpr.pdf; https://standards.openbanking.org.uk/customer-experience-guidelines/dashboards/about/latest/

[12] Los proveedores de servicios de pago de servicios de cuenta (ASPSP) proporcionan y mantienen una cuenta de pago para un pagador según lo definido por los PSR y, en el contexto del ecosistema de banca abierta, son entidades que publican API de lectura/escritura para permitir, con el consentimiento del cliente, pagos iniciados por proveedores externos y/o poner los datos de transacciones de la cuenta de sus clientes a disposición de proveedores externos a través de sus puntos finales API. Los ASPSP suelen ser bancos e instituciones financieras similares, incluidas sociedades de construcción y empresas de pagos.

3. **Singapur**

Las Finanzas Abiertas en este país son una iniciativa liderada por el mercado, y cubre muchos productos y servicios, desde pagos digitales hasta seguros, pasando por productos de crédito y de inversión.

La Autoridad Monetaria de Singapur (MAS, por sus siglas en inglés) ha fomentado la creación de un ecosistema robusto de banca abierta, sin desarrollar legislaciones de cumplimiento obligatorio, que regulen el acceso a los datos por parte de terceros.

Cabe señalar que la Comisión de Protección de Datos Personales también es un participante activo, dado el papel de la Ley de Protección de Datos Personales (PDPA, por sus siglas en inglés)[13] en el entorno de las finanzas abiertas.

La MAS y el Grupo de Gobierno Digital y Nación Inteligente (SNDGG), con el apoyo del Ministerio de Mano de Obra (MOM), desarrollaron una infraestructura digital pública llamada SGFinDex (Intercambio de Datos Financieros de Singapur, por sus siglas en inglés) que utiliza una identidad digital nacional (Singpass)[14] y un sistema de consentimiento en línea administrado centralmente. Permite a las personas acceder a su información financiera que se encuentra en diferentes agencias gubernamentales e instituciones financieras, tales como depósitos, tarjetas de crédito, préstamos, detalles de pólizas de seguro e inversiones.

El SGFinDex está diseñado para garantizar la protección de datos y la privacidad de la información financiera personal; por ello solo transmite y no almacena ningún dato financiero personal. Los datos financieros solo se pueden recuperar mediante el consentimiento explícito del individuo, cuya identidad debe verificarse a través de SingPass[15]. Todos los datos transmitidos a través de SGFinDex están cifrados y solo pueden leerse en las aplicaciones de planificación financiera que reciben los datos.

El periodo de consentimiento en SGFinDex tiene una duración de un año, y las personas no pueden elegir la fecha de vencimiento de su consentimiento. El consentimiento brindado a las respectivas instituciones financieras caducará un año a partir del momento en que fue otorgado a la primera institución financiera. Sin embargo, los individuos pueden revocar el consentimiento para algunas o

[13] Advisory Guidelines on Key Concepts In The Personal Data Protection Act. Recuperado de https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-17-May-2022.pdf

[14] El signpass es la identidad digital confiable de los ciudadanos y residentes de Singapur para un acceso conveniente y seguro a miles de servicios gubernamentales y del sector privado, en línea y en persona. Recuperado de https://www.singpass.gov.sg/main/html/faq.html

[15] SGFinDex llevará a los usuarios a través de un proceso de dos pasos: (a) conectar bancos a SGFinDex; y (b) solicitar la recuperación de datos de estos bancos.

todas las instituciones financieras a las que haya otorgado antes de que finalice el período de validez de un año[16].

4. **Australia**

En Australia, la banca abierta se pudo desarrollar a través de la implementación del Derecho de Datos del Consumidor (CDR, por sus siglas en inglés)[17]. El CDR se introdujo para dar a los consumidores un mayor control sobre sus datos de consumo, permitiéndoles ordenar a quienes tienen su información, que la proporcionen (Datos CDR) a un destinatario de datos acreditado, en un formato compatible con CDR.

Por su parte, las Reglas de Competencia y Consumidor (Derechos de Datos del Consumidor) de 2020 (en adelante las Reglas CDR)[18], proporcionan el marco para el funcionamiento del CDR. Las Reglas CDR definen los elementos para el consentimiento, describen el marco de acreditación y detallan los aspectos de privacidad del esquema. Además, existen estándares de datos elaborados por el Organismo de Estándares de Datos, incluidos estándares sobre el formato y el proceso para transferir datos[19].

Bajo el marco australiano, el consentimiento debe ser voluntario, expreso, informado, específico en cuanto a su propósito, tiempo limitado, y fácilmente retirado. En ese sentido, las reglas CDR entregan instrucciones claras, ya que tienen como objetivo garantizar que las solicitudes de consentimiento para recopilar y utilizar datos CDR sean transparentes y que los usuarios comprendan las posibles consecuencias de lo que están consintiendo. Además, en ellas se incluyen orientación práctica adicional, entregando ejemplos específicos.

Las reglas CDR exige que las instituciones implementen políticas y procesos de gestión del consentimiento eficaces y eficientes y establezcan paneles de control.

En Australia, la duración del consentimiento corresponde a 12 meses para personas naturales, y 7 años para personas jurídicas desde la fecha de su otorgamiento.

En cuanto a la revocación del consentimiento, el usuario puede retirarlo en cualquier momento a través del panel de control dispuesto para aquello, o empelando un método de comunicación alternativo simple que quien maneja sus

---

[16] Frequently Asked Questions on Singapore Financial Data Exchange (SGFinDex). Recuperado de https://abs.org.sg/docs/library/sgfindex-frequently-asked-questions.pdf

[17] El Ministro designó al sector bancario para ser parte del sistema CDR a través de la "Designación de Derecho de Datos del Consumidor (Instituciones Autorizadas de Depósito) 2019". Este instrumento establece las clases de información que están sujetas a la CDR, así como quién posee esta información y está obligado a transferirla a solicitud del consumidor. Tal designación se puede encontrar en https://www.legislation.gov.au/Details/F2019L01153

[18] Competition and Consumer (Consumer Data Right) Rules 2020. Recuperado de https://www.legislation.gov.au/Details/F2023C00735

[19] Consumer Data Standars están disponibles en https://consumerdatastandards.gov.au/

datos (*data holder*) deberá disponer para tal fin. Si el usuario opta por la segunda opción, el *data holder* deberá dar efecto a la revocación tan pronto como sea posible y, en cualquier caso, dentro de los 2 días hábiles siguientes a la recepción de la solicitud.

5. **India**

En 2016, ante la ausencia de una ley de protección de datos[20], el Banco de la Reserva de India (RBI) crea a los "Agregadores de Cuentas" (AA, por sus siglas en inglés)[21]- Los AA actúan como intermediarios cuya única función es transferir datos financieros de manera segura entre los tenedores de datos - proveedores de información financiera (FIP, por sus siglas en inglés) - y los usuarios de datos - usuario de información financiera (FIU, por sus siglas en inglés)-, sobre la base del consentimiento expreso del cliente.[22] Este sistema, llamado Ecosistema de Agregación de Cuentas, facilita el intercambio de información financiera en tiempo real entre entidades reguladas.

El AA ayuda a las personas a compartir sus datos financieros con terceros de forma segura y les brinda un mayor control sobre cómo se utilizan sus datos. Los AA no pueden almacenar datos de los usuarios, ya que éstos fluyen a través de ellos de forma encriptada y solo pueden ser procesados por los FIU. Los agregadores solo pueden encargarse de gestionar el consentimiento (administrador del consentimiento) y deben estar registrados en el RBI.

Por otra parte, Sahamati[23] es un ecosistema colectivo de agregadores de cuenta no gubernamental, creado a través de una alianza en la industria, formada para promover y fortalecer el Ecosistema AA en la India. Es una sociedad de responsabilidad limitada sin fines de lucro, encargada de acrecentar el ecosistema de agregadores de cuentas y ser una entidad coordinadora de agregadores de cuentas.[24] En esta última función, Sahamati asume una parte de la gobernanza del sistema, que incluye la elaboración de directrices de certificación sobre software y la emisión de normas técnicas.

La Arquitectura de protección y empoderamiento de datos (DEPA, por sus siglas en inglés) es un enfoque de gestión y procesamiento de datos personales centrado en el consentimiento de las personas. DEPA permite la recopilación y el uso de datos personales de manera que permitan a las personas acceder a

[20] Hasta esa fecha no existía una Ley de Protección de Datos, sin embargo, actualmente cuentan con una que fue emitida en agosto de 2023.
[21] "Account Aggregator"
[22] Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016, actualizada en diciembre de 2022. Recuperado de https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598
[23] El sitio web de Sahamati es https://sahamati.org.in/
[24] Datwani y Raman, 2020. Recuperado de https://www.cgap.org/research/publication/indias-new-approach-to-personal-data-sharing

mejores servicios financieros, servicios de atención médica y otros servicios socioeconómicamente en tiempo real, preservando al mismo tiempo la seguridad y privacidad del usuario.

6. **Brasil**

La Resolución respecto a la Regulación de la Banca Abierta en Brasil[25] define el consentimiento como "una manifestación de voluntad libre, informada, previa e inequívoca, realizada a través de canales electrónicos, por la que un cliente acepta compartir datos o servicios para fines específicos". En ese sentido, el consentimiento no se puede obtener basándose en un acuerdo estándar con el cliente o el uso de un formulario precargado.

El artículo 10 de la Resolución establece que una institución receptora de datos debe identificar al cliente y obtener su consentimiento, antes de compartirlos. El consentimiento deberá solicitarse utilizando un lenguaje claro, objetivo y adecuado; debe referirse a fines específicos; debe tener una vigencia de 12 meses; se debe identificar la institución transmisora de datos o el proveedor de servicios de cuenta; se debe especificar los datos o servicios que serán compartidos; e incluir la identificación del cliente. Si hay un cambio en el propósito, período de validez, institución transmisora de datos o proveedor de servicios de cuenta, o si los datos van a comunicarse o cederse, o el servicio va a ser compartido, se requiere un nuevo consentimiento del cliente.

El sistema de finanzas abiertas debe cumplir con lo estipulado en la Ley Real de Protección de Datos Personales[26], que crea un nuevo marco legal para el uso y protección de datos personales en Brasil por parte de los sectores público y privado.

Las instituciones ponen a disposición del cliente la opción de revocar el consentimiento a través, de al menos, el mismo canal de atención por el cual fue otorgado.

Cabe señalar que, las instituciones en Brasil no pueden sugerir a los clientes que revoquen su consentimiento, excepto en casos de sospecha de fraude. Esto posiblemente se deba a que las instituciones que no quieran que los clientes participen en las finanzas abiertas puedan animarlos a revocar el consentimiento para compartir información, limitando el alcance y los beneficios de las finanzas abiertas.

---

[25] Resolución N°1 de 4 de mayo de 2020, Regulation on Open Banking. Recuperado de https://www.bcb.gov.br/content/config/Documents/Open_Banking_CMN_BCB_Joint_Resolution_1_2020.pdf

[26] Lei Geral de Proteção de Dados Pessoais 2014, LGPD. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato 2015-2018/2018/lei/L13709compilado.htm

También, las instituciones tienen prohibido establecer obstáculos al intercambio de datos, incluido pedir a los clientes autorizaciones adicionales o validar su consentimiento, lo que inhibiría la participación de sus clientes en las finanzas abiertas.

7. Resumen del Análisis Comparado

La siguiente tabla resume los aspectos generales del consentimiento de las jurisdicciones revisadas.

	Tipo de consentimiento	Duración del Consentimiento	Sistema de Gestión del Consentimiento
Unión Europea	Voluntad libre, específica, informada, e inequívoca		Descentralizado
Reino Unido	voluntad libre, específica, informada, e inequívoca	90 días	Descentralizado
Singapur	Explícito	12 meses	Centralizado
Australia	Voluntario, expreso, informado, específico en cuanto a su propósito, tiempo limitado, y fácilmente retirado.	12 meses	Descentralizado
India	Expreso		Centralizado
Brasil	Voluntad libre, informada, previa e inequívoca	12 meses	Descentralizado

Fuente: Elaboración Propia

En resumen, se puede observar las siguientes áreas de preocupación respecto al consentimiento en un sistema de finanzas abiertas:

1. La forma y oportunidad en que se otorga el consentimiento, a objeto de facilitar la comprensión, a cabalidad, de los efectos y consecuencias de la autorización que otorgan. El que se obtenga el consentimiento para acceder y compartir datos personales, en conjunto con otras materias o contratos, puede atentar contra ese objetivo.

2. Desincentivos del cliente a informarse de los datos y usos que está autorizando, al entregársele información o requerírsele autorizaciones en exceso. Lo anterior puede ocurrir porque se le abruma con información o solicitudes, por ejemplo, al requerirle el consentimiento en múltiples oportunidades (lo que la literatura ha denominado "fatiga del

consentimiento"). Situación que termina desincentivando la correcta comprensión de la información que efectivamente está autorizando sea compartida. Por ejemplo, en el caso de políticas de privacidad que se presentan junto al otorgamiento del consentimiento y que, por extensión, lenguaje técnico, tamaños y formatos que se emplean, tienden a producir esa fatiga y dificultar la identificación rápida de datos o temas clave.

3. Los clientes, a pesar de otorgar su consentimiento, no están teniendo un control adecuado sobre sus datos, llegando incluso a desconocer cuales de éstos han compartido, cuándo, con quién y con qué fines.

4. Las personas al operar con distintos proveedores del servicio deben enfrentarse a una multiplicidad y diversidad de interfaces cada vez que deben otorgar su consentimiento, dificultando a los clientes familiarizarse con estos procesos, su aprendizaje y confianza.

Existen varios enfoques y mecanismos que están siendo utilizados por las jurisdicciones revisadas, o recomendados por organismos internacionales, para abordar estas problemáticas, dentro de los cuales los más destacados son:

1. Concebir un proceso de otorgamiento del consentimiento separado, distinto de cualquier otro acuerdo que los clientes celebren con las diferentes instituciones, aun cuando versen sobre asuntos complementarios o conexos.

2. Los términos utilizados en el proceso del otorgamiento del consentimiento deben presentarse en un lenguaje claro y sencillo, fácilmente comprensible para un ciudadano promedio.

3. Las políticas de privacidad deben ser de una extensión razonable -pero incluyendo todos los aspectos fundamentales-, para no abrumar al consumidor, propiciando su lectura y comprensión y evitando incluir información irrelevante que induzca al cliente desistir de completar su lectura.

4. El empleo de paneles de control que contengan información respecto de los consentimientos otorgados, revocados o caducados, y que les permita revisar rápidamente la información que comparten, quienes tienen acceso a ella, con qué fines y por cuánto tiempo.

5. Algunas jurisdicciones, con la finalidad de contar con proceso uniforme que facilite la experiencia usuaria, han optado por la centralización de la gestión del consentimiento.

6. Revocación de consentimiento expedita y pudiendo utilizar el mismo canal por el cual se brindó el consentimiento.

IV. PROPUESTA CONCEPTUAL

Esta sección contiene los lineamientos regulatorios que buscan cubrir lo que la propia Ley Fintec encomienda a esta Comisión en su artículo 23, así como áreas de preocupación que han sido manifestadas por organismos internacionales y estudios en torno al consentimiento, de acuerdo al análisis presentado previamente.

Los elementos que se propone contenga la normativa de la CMF son los siguientes:

1. *Requerir que el consentimiento sea solicitado en forma separada de cualquier otra manifestación de voluntad que dé el cliente, aun cuando se trate de acuerdos complementarios o conexos.*

   Al efecto se pretende evitar que, por el hecho de incluir otras materias en el otorgamiento del consentimiento -que puede ser en un contrato o términos y condiciones- la persona no logre un adecuado conocimiento del alcance de la autorización respecto al acceso tanto de su información personal como financiera.

2. *Reforzar como principio rector en materia de obtención del consentimiento que la entidad que lo solicita deba emplear un lenguaje claro y sencillo, sin usar tecnicismos, a menos que sea estrictamente necesario, ni textos extensos, particularmente en lo referido a las materias clave para el cliente. Además, propender al empleo de metodologías educativas para proporcionar información al cliente.*

   Ello, con el objeto de facilitar a las personas comprender qué están consintiendo y los efectos de ello, resguardando los derechos de los clientes y su autonomía.

3. *Establecer una duración determinada para la vigencia del consentimiento. La duración de caducidad propuesta será, por regla general, de 180 días desde la primera autorización. No obstante, para ciertos tipos de información o usos, se propondrá que caduque con el primer uso o que pueda durar hasta 12 meses, según corresponda.*

   Esta medida busca evitar que, por el transcurso del tiempo, el cliente pueda olvidar que otorgó el consentimiento para datos o usos que no ameritan plazos tan extensos, generando una mayor confianza y transparencia en el sistema de finanzas abiertos local. No obstante, se quiere compatibilizar ese objetivo con la necesidad de los prestadores de contar con acceso a los datos durante tiempos más prolongados para finalidades que así lo requieren.

4. *Establecer que quien gestione el consentimiento debe mantener habilitado el mismo canal de revocación que se empleó para la obtención del*

consentimiento. Lo cual no obstará a la existencia de otros canales tanto digitales como no digitales dispuestos para ello.

Esta medida busca garantizar el control y la autonomía del cliente sobre el uso de sus datos personales. Además, proporciona a los clientes la flexibilidad de cambiar sus preferencias de privacidad según sus necesidades y expectativas cambiantes. Por otra parte, al ofrecer otros canales para revocar el consentimiento, les entrega a los clientes diversas opciones para ejercer este derecho, asegurando un proceso accesible y confiable.

5. *Reforzar el principio respecto a que la institución debe abstenerse de ejercer cualquier influencia indebida sobre el cliente, debiendo haber una acción positiva e inequívoca por parte de éste para que exista consentimiento.*

   Lo anterior, a objeto de prevenir prácticas que fuercen al cliente a otorgar su consentimiento y, en caso de que ocurran, sancionarlas.

6. *Exigir que la institución deba implementar paneles de control para que el cliente pueda gestionar de manera simple, remota y gratuita los consentimientos que hubiere otorgado. Tales paneles, deberán contar con información completa, íntegra, actualizada y fidedigna de todos los consentimientos otorgados, revocados y caducados, de ser el caso.*

   La medida tiene por finalidad reforzar la comprensión del cliente respecto a los consentimientos que ha otorgado y facilitar la gestión de los mismos por parte de éste.

7. *Mandatar a las entidades para que informen a sus clientes, de manera anual, de cada uno de los consentimientos que se otorgaron, revocaron o caducaron en el período; aquellos que se encuentren vigentes; y del uso o tratamiento que se dio a sus datos.*

   Esto permite que los clientes estén al tanto de cómo se están utilizando sus datos, fomentando la transparencia y brindándoles la oportunidad de tomar decisiones informadas sobre su privacidad y la gestión de sus preferencias. Lo anterior, sin que se vea abrumado por el envío constante de información. La menor periodicidad es consecuencia de la implementación de la medida referida a la exigencia de los paneles de control que facilitarán al usuario la información y gestión de sus consentimientos, no siendo tan necesario que se le mantenga informado sobre la materia con mayor frecuencia.

8. *Facilitar la externalización de algunos servicios, cumpliendo siempre los requisitos establecidos por normativa.*

   Externalizar algunos servicios relacionados al consentimiento podría facilitar tanto la experiencia del usuario como la interoperabilidad entre

diferentes servicios y aplicaciones financieras, permitiendo una gestión más armoniosa de los consentimientos en un entorno de finanzas abiertas.

V. CONTRIBUCIONES AL PROCESO CONSULTIVO

Sin perjuicio de los demás elementos, sugerencias u observaciones que los distintos actores o usuarios del mercado financiero pudieren manifestar con respecto a los lineamientos presentados, se espera conocer de quienes participen bajo el sistema de finanzas abiertas, lo siguiente:

1. ¿Es razonable que el consentimiento caduque a los 180 días por regla general y que, para ciertos casos particulares, caduque en su primer uso o pueda durar hasta 12 meses? ¿Para qué casos de uso o tipos de información resulta necesario o conveniente establecer una vigencia del consentimiento distinta a la regla general?, ¿cuál sería y por qué?

2. ¿Es un método adecuado para la gestión del consentimiento la implementación de paneles de control, y que se pueda externalizar en un órgano privado? ¿Qué problemas o beneficios observa en que esa obligación sea gratuita y de acceso remoto para el cliente?

3. ¿Es la periodicidad anual para el reporte de tratamiento de información una frecuencia razonable, atendidas las demás exigencias que facilitan al cliente informarse y gestionar los consentimientos por sí mismo?

4. ¿Ve algún efecto negativo en que se separe el otorgamiento del consentimiento respecto a cualquier otra forma de manifestación de voluntad o, por el contrario, lo ve como una medida razonable, pertinente o necesaria?

5. ¿Hay alguna materia que no haya sido abordada en la propuesta conceptual de la Comisión que estime necesario o conveniente sea abordada en la normativa, en materia de otorgamiento, revocación y, en general, gestión del consentimiento?

COMISIÓN
PARA EL MERCADO
FINANCIERO

REGULADOR Y SUPERVISOR FINANCIERO DE CHILE

www.cmfchile.cl