Estándar 4D

Privacidad de los Datos de los Clientes

La privacidad de los datos de clientes individuales será respetada de acuerdo con las leyes y reglamentaciones de jurisdicciones individuales. Estos datos solo serán utilizados para los fines especificados en el momento de recolectar la información o según lo permitan las leyes, a menos que se acuerde de otra forma con el cliente.

> Práctica Esencial 4D.1 Los datos de los clientes se resguardan de manera segura y confidencial. (Norma de Protección al Cliente 6.1)

> Práctica Esencial 4D.2 Se informa a los clientes sobre la privacidad de sus datos y el consentimiento para el uso de sus datos. (Norma de Protección al Cliente 6.2)

4D.1 IMPLEMENTAR UNA POLÍTICA DE PRIVACIDAD Y TECNOLOGÍAS ADECUADAS

Sus clientes comparten información personal y financiera muy importante con su organización, y usted tiene la responsabilidad de proteger la privacidad y la confidencialidad de estos datos. El uso indebido de datos como fotografías de clientes, números de cuenta y documentos de identificación personal puede tener efectos devastadores en los clientes.

Independientemente de la reglamentación nacional, su institución debe tener una política de privacidad y procedimientos escritos que rijan la recolección, el procesamiento, el uso, la distribución y el almacenamiento de información del client.[108] La política debe abarcar a los empleados actuales, pero también al personal que deja la organización. Especifique sanciones o penalizaciones en caso de que los empleados violen la política de privacidad, por ejemplo, el uso u obtención inadecuados de datos del cliente, fuga de información o exposición de datos del cliente a terceros sin el consentimiento del cliente.

Si trabaja con proveedores de terceros que tienen acceso a datos de clientes, por ejemplo, proveedores de seguros, agentes de pagos, empresas de marketing, su contrato con estos proveedores debe especificar que mantendrán la seguridad y la confidencialidad de los datos del cliente. Monitoree si los contratistas de terceros están cumpliendo su compromiso con la confidencialidad de los datos, por ejemplo mediante preguntas sobre la seguridad de sus sistemas, entrevistas a los clientes acerca de sus experiencias con respecto a la seguridad de los datos (por ejemplo, "¿El agente le pidió que firmara este acuerdo de privacidad? Y compruebe el proceso del proveedor a través de compras misteriosas.

El personal que deja su institución ya no tiene muchos incentivos para proteger los datos de los clientes. Establezca un proceso para salvaguardar los datos del uso indebido de ex empleados. Tales medidas pueden incluir la terminación de las credenciales de acceso del empleado, la recolección de todos los equipos de trabajo (computadoras portátiles, llaves de construcción, etc.) y la eliminación (borrado de la información) de los propios dispositivos del empleado (por ejemplo, teléfono móvil).

Sus sistemas informáticos también son vulnerables al mal uso. Establezca medidas de seguridad para proteger contra el acceso no autorizado a los datos, mediante la inclusión de contraseñas, diferentes niveles de acceso para diferentes empleados e infraestructura de software adecuada. Cambie las contraseñas de TI periódicamente y permita un acceso diferente a los datos según la posición del miembro del personal que accede a los datos. Además, realice copias de seguridad de sus sistemas diariamente, con copias de seguridad almacenadas de forma segura fuera del sitio.

FUBODE (Bolivia) tiene asignada una sala específica dentro de cada sucursal para almacenar los documentos físicos de los clientes. Cada una de estas habitaciones cuenta con detectores de humo, cámaras profesionales, sensores de movimiento y armarios laterales resistentes al fuego para almacenar los documentos físicos de los clientes. La sala restringe el acceso a solo un miembro del personal por sucursal. Además, la PSF invirtió un promedio de USD 3,500 por sucursal para instalar en cada sucursal cámaras de vigilancia y un botón de pánico para cada cajero, así como un sistema de alarma supervisado por una oficina central de terceros.[109]Tanto si están computarizados como si no, sus sistemas de información deben garantizar la seguridad y la privacidad de los datos del cliente. No permita a los empleados tomar libremente los archivos del cliente o copias de las bases de datos, y mantenga registros de los nombres del personal que solicita y/o a quien se le otorga permiso para acceder a los archivos del cliente fuera de condiciones normales. Mantenga los archivos del cliente impresos en un lugar seguro, con acceso controlado. Por ejemplo, la política de FinDev (Azerbaiyán[110] sobre seguridad de datos establece: "Los contratos de préstamo y copias de todos los demás documentos oficiales con respecto al expediente de préstamo del cliente se guardan en cajas de hierro en la sala del gerente de finanzas. Otros documentos se guardan en estanterías cerradas bajo la supervisión del oficial de préstamo respectivo. " Planifique cómo mantener la seguridad de los datos en caso de interrupción no planificada de la red o de emergencia. Un plan de continuidad de negocios que cubra varios de los escenarios más probables (como una brecha de seguridad, una sobrecarga de red y una desaceleración, o un desastre natural que desconecte la alimentación y la conectividad) ayudará a mantener la información segura durante eventos inesperados cuando los datos se vuelven vulnerables.

[108] La política debe definir qué datos del cliente están cubiertos; quién en la institución es el responsable final de asegurar la privacidad de los datos de los clientes; qué tipo de datos se pueden obtener, por quién, de dónde y para qué;y cualquier requisito legal y regulatorio para recopilar, compartir y usar la información.

[109] Encuentre más información sobre este ejemplo de campo en el Estudio de Protección de Clientes en América Latina y el Caribe de Smart Campaign.

[110] Puede encontrar extractos de la política de FinDev aquí.

Finalmente, todos los contratos de productos deben incluir una cláusula de privacidad que especifique cómo se usarán y protegerán los datos. Esta cláusula debe incluirse en idioma simple y mostrarse de manera destacada en el contrato; por ejemplo, no ocultarla en letra pequeña. Para los productos de ahorros, debe estar claro quién tiene acceso a la cuenta del cliente; para los productos de crédito, los clientes deben conocer si su información será compartida con un buró de crédito, u otros, como compañías de seguros o agentes de cobros.

- La *Herramienta de Capacitación sobre Privacidad de Datos* de Smart Campaign contiene varios miniestudios de casos sobre cómo los datos de los clientes pueden ser mal administrados y cómo evitar estas situaciones.
- El estudio de caso de Azerbaiyán sobre la protección de datos de los clientes de FINCA detalla las medidas de seguridad utilizadas para proteger la información del cliente, incluidas las restricciones de acceso a la base de datos y los procedimientos estrictos para almacenar archivos físicos.
- FinAmérica ofrece a los clientes un folleto de bolsillo con consejos sobre cómo proteger su seguridad y prevenir el robo de identidad, robos y otras posibles amenazas a la privacidad de su información personal. También disponible en español y francés.

EJEMPLO DE CAMPO 44. SKS Y EQUITAS PROTEGEN LOS DATOS DE CLIENTES[111]

SKS (India) tiene una política por escrito sobre el intercambio de información de clientes con partes externas. Claramente clasifica los tipos de información en "confidencialidad crítica" y "confidencialmente sensible" y establece el proceso para manejar cada categoría, con mayores protecciones para los datos en la categoría de "confidencialidad crítica". El PSF también tiene una política de privacidad de los datos del cliente que se aplica a todos los empleados. La política establece que SKS no comparte los datos de los clientes con nadie excepto con las autoridades reguladoras como el Banco de la Reserva de la India, agencias de crédito, organizaciones autorreguladoras, tribunales y agencias gubernamentales con el propósito de cumplir con los requisitos de cumplimiento. SKS garantiza que sus contratos con los proveedores de servicios y los acuerdos de no divulgación sean exhaustivos y que cubran prudentemente la confidencialidad de la información del cliente.

Equitas (India) fue la primera IMF de la India en tener una solución bancaria central, TEMENOS-T24. Este producto es una extensión del software T24 Banking, desarrollado específicamente para microfinanzas y el sector bancario comunitario. La información del cliente está altamente protegida y bien protegida en TEMENOS, con acceso de usuario y contraseñas definidos. Todos los empleados de la oficina de apoyo están entrenados en el uso de este sistema. El personal de la sucursal no tiene acceso a los datos de los clientes, excepto lo que es necesario para manejar las recaudaciones a través de las hojas de recaudación. Equitas tiene un sistema de archivo de cliente distinto y almacenamiento seguro de los archivos de información del cliente. Las copias virtuales de los archivos del cliente se almacenan en el software, mientras que las copias impresas de los archivos del cliente y los documentos de préstamo se codifican, se apilan y se mantienen protegidos en un depósito de datos en Chennai. Equitas invierte regularmente en auditoría y mantenimiento de TI para revisar la seguridad del cliente.

[111] Encuentre más información sobre este ejemplo de campo en *Implementar la Protección de Clientes en las Microfinanzas Indias* de Smart Campaign aquí.

4D.2 INFORMAR A LOS CLIENTES Y OBTENER EL CONSENTIMIENTO DEL CLIENTE ANTES DE COMPARTIR DATOS

Además de contar con sistemas internos para mantener seguros los datos de los clientes, su institución debe ser completamente transparente con los clientes sobre cómo se utilizará su información personal y debe obtener su consentimiento antes de compartir sus datos fuera de su institución. Sus contratos de producto deben tener una explicación clara de cómo los datos del cliente serán protegidos, cómo se pueden utilizar o compartir, y con quién.

A partir del momento de la solicitud, obtenga el consentimiento del cliente *antes* de compartir información personal con cualquier audiencia externa, lo que incluye agencias de crédito, miembros de la familia, garantes, agentes de seguros, compañías de recaudación y material de marketing (por ejemplo, sus informes anuales, contenido público). Si corresponde, exija que los clientes nombren un beneficiario para su póliza de seguro de vida, para que la institución pueda proteger la cuenta de los clientes de todas las otras personas que no han sido nombradas como beneficiarias. Consulte el Cuadro 19 para obtener un formulario de consentimiento para compartir datos de los clientes.

Con el fin de informar a sus clientes sobre la privacidad de los datos, primero asegúrese de que su personal está bien capacitado en el tema. La privacidad de los datos del cliente debe ser parte del entrenamiento de capacitación del personal. El entrenamiento variará según la posición del empleado; asegúrese de que el personal de campo entienda y pueda explicar la parte de consentimiento para compartir datos del contrato del cliente. De igual forma, capacite a los líderes de los grupos de clientes sobre la importancia de salvaguardar la información sensible de los miembros del grupo, en particular los saldos de las cuentas de ahorro, las fechas de pago del préstamo y la información sobre los problemas de pago.

Cuando hable con los clientes, haga hincapié en las propias responsabilidades de los clientes para mantener los datos privados, como almacenar registros en una ubicación segura y no compartir números de identificación personal (PIN). Finamérica (Colombia) publica un folleto para clientes[112] con consejos para la seguridad de la información que incluye cómo evitar a falsos empleados bancarios, evitar robos, mantener las tarjetas de débito seguras, proteger la información personal y contactar al banco si se detecta un problema de seguridad.

Finalmente, verifique que los proveedores de terceros entrenen a sus propios representantes en los procedimientos de privacidad de datos.

[112] También disponible en español y francés.

CUADRO 19. MUESTRA DE FORMULARIO DE CONSENTIMIENTO PARA COMPARTIR LOS DATOS DEL CLIENTE

Además de tener un formulario de consentimiento como el siguiente, los contratos de productos deben contener un acuerdo de privacidad de datos más largo. Un acuerdo de ejemplo está disponible en la Herramienta de Documentos esenciales para nuevos clientes de Smart Campaign (consulte la sección "Acuerdo de privacidad de datos de ejemplo").

MacroDreams respeta la privacidad y la seguridad de los datos del cliente. Este formulario de consentimiento permitirá a MacroDreams utilizar su foto para fines públicos y/o compartir su información personal y financiera con terceros.

Instrucciones: Por favor, lea las siguientes dos declaraciones y firme la línea debajo de cada uno.

Declaración 1. Compartir su fotografía

Autorizo a MacroDreams a usar y publicar mi nombre, imagen, declaración de entrevista y/o información que me identifique a mí ya mi negocio. Esto puede hacerse en forma de fotografías impresas o electrónicas, video, declaraciones grabadas, publicaciones, ilustraciones, presentaciones u otras actividades de medios impresos, digitales o electrónicos, como Internet. Entiendo que tendré derecho a una indemnización en relación con los derechos arriba mencionados.

Su firma: Al firmar en la línea de abajo, usted reconoce que entiende la declaración anterior.

_____ _____ _____

Nombre del cliente (en imprenta) Firma del cliente Fecha

_____ _____

Firma de empleado de MacroDreams Fecha

Declaración 2. Compartir su información personal y financiera

I Autorizo a MacroDreams a compartir mi información personal y financiera con la Oficina Nacional de Crédito; la Red Nacional de Microfinanzas; proveedores de servicios de terceros, incluida la Compañía de Seguros Protecta; agencias de cobros (en caso de incumplimiento grave); y miembros de mi grupo (si corresponde). Entiendo que MacroDreams hará todo lo posible por mantener seguros mis datos, como se describe en la Declaración de privacidad de datos de MacroDreams.

Su firma: Al firmar en la línea de abajo, usted reconoce que entiende la declaración anterior.

_____ _____ _____

Nombre del cliente (en imprenta) Firma del cliente Fecha

_____ _____

Firma de empleado de MacroDreams Fecha

CUADRO 20. CÓMO PUEDE DAÑAR A SU INSTITUCIÓN LA DIVULGACIÓN DE DATOS NO AUTORIZADA

La siguiente historia[113] de un PSF ficticio se basa en experiencias reales de varios proveedores indios.

Parivartan es un PSF bien establecido en el sur de la India que publica regularmente "historias de éxito" de clientes/perfiles de clientes que han utilizado los servicios financieros para mejorar sus vidas. Uno de esos perfiles contó la historia de un cliente llamado Shubham, propietario de un restaurante en su tercer ciclo de préstamos.

Parivartan quería mostrar la historia de éxito del Sr. Shubham, y por lo tanto tomó algunas fotos del cliente y su restaurante, y publicó estas fotos en su folleto de productos, su informe anual y en su sitio web. El PSF no solicitó la aprobación verbal o escrita del cliente antes de usar su foto para promover la institución, pero esto no molestó al Sr. Shubham, quien mostró con orgullo los materiales en su restaurante.

Un día, muchos meses después, uno de los clientes habituales de Shubham, un abogado, visitó el restaurante. Al ver los materiales promocionales, preguntó casualmente si Parivartan había compensado al Sr. Shubham por su papel en la promoción del PSF. El Sr. Shubham respondió que no solo no había recibido ningún pago, sino que se había sorprendido de ver su foto en los materiales. No había sido consultado y había supuesto que las fotos tomadas por su oficial de préstamos eran estrictamente a los efectos de la solicitud de préstamo. El abogado se sorprendió al escuchar la historia de Shubham y percibió la oportunidad de demandar a Parivartan sobre la base de que el PSF había utilizado las fotos para obtener ganancias comerciales sin comunicación escrita ni consentimiento algunos.

Aunque el Sr. Shubham no procedió con la demanda, confrontó a su oficial de préstamos sobre por qué no había sido consultado y compensado. El oficial de préstamos planteó el problema con su gerente de sucursal, quien elevó el problema a los gerentes sénior. La gerencia pronto se dio cuenta de que había escapado por poco de una costosa batalla legal y decidió crear una política para obtener el consentimiento del cliente antes de usar las fotos de los clientes en cualquier formato público. Añadieron una política sencilla al Manual de crédito de Parivartan y proporcionaron a los oficiales de préstamo un formulario de consentimiento del cliente. Los oficiales de préstamos también recibieron capacitación sobre cómo comunicarse con los clientes sobre el uso de sus fotos y utilizar el formulario de consentimiento.

- La herramienta Smart Operations de Smart Campaign detalla las funciones y las responsabilidades de las diferentes áreas operativas (Gestión Ejecutiva, ICT y Legal) en la creación de una política de privacidad de datos y su aplicación. También disponible en español y francés.
- El estudio de caso de FINCA Azerbaiyán sobre la protección de datos de los clientes detalla las medidas de seguridad utilizadas para salvaguardar la información del cliente, lo que incluye la capacitación del personal en procedimientos de seguridad y el consentimiento del cliente antes de compartir datos

[113] Adaptado del document de Smart Campaign Herramienta de entrenamiento en la privacidad de los datos, página 3.

EJEMPLO DE CAMPO 45. CAJA MORELIA VALLADOLID PROTEGE LOS DATOS DEL CLIENTE

Tras la transformación de una cooperativa a una institución financiera regulada, Caja Morelia (México) debió cumplir con requisitos de gestión e información de datos federales de México. Este período de transformación proporcionó al proveedor la motivación para fortalecer su sistema de Tecnología de la Información y Comunicaciones (TIC, o ICT por sus siglas en Ingles).

Caja Morelia actualizó su sistema para incluir las siguientes funciones:

- Una única base de datos electrónica "maestra" con acceso remoto para sucursales. Cada sucursal puede modificar datos del cliente para su propia cartera, pero no puede descargar la base de datos maestra. El personal en la sede central puede acceder a toda la base de datos, pero no puede cambiar los perfiles del cliente. Esto evita los problemas de control de versiones y garantiza que los empleados solamente tengan acceso al mínimo de datos del cliente necesario para llevar a cabo sus obligaciones.
- Cada una de las personas que accede a la base de datos usa un nombre de usuario y contraseña individuales. Los usuarios deben cambiar sus contraseñas cada cuatro meses y no pueden repetir contraseñas anteriores. Cuando un empleado inicia sesión en la base de datos, su nombre, la información que consultan y la hora en que realizan la solicitud, se registra en un registro de consulta.
- Los empleados de la sede central ingresan y dejan la oficina principal utilizando un escáner de huella digital del pulgar y un proceso de registro que evita el acceso no autorizado a la información del cliente almacenada allí.
- Los cambios en la información del cliente deben ser autorizados por dos o más personas, con frecuencia de diferentes departamentos. Esto impide el uso erróneo de los datos por cualquier persona.
- Cada uno de los equipos del PSF está configurado para acceder al sistema para un único departamento (p ej., un equipo configurado para Recursos Humanos no puede ser utilizado por el departamento de Contabilidad). Esto ayuda a evitar el acceso a los datos por parte de empleados no autorizados.
- Durante el proceso de cobros, solamente el agente de cobros, el gerente de la sucursal y el departamento de Cobros de la sede central tienen acceso a información personal de clientes con préstamos adeudados. Cuando el banco usa una firma de cobros externa especializada, comparte únicamente la información más necesaria para la firma a fin de recuperar el préstamo.
- To enforce the above changes, Caja Morelia requires employees to sign client data confidentiality agreements. In-house software developers also sign contracts to protect the proprietary nature of the software. The FSP has the right to bring criminal charges for violations of these agreements.

Conozca más sobre este ejemplo en la página de Smart Campaign.