POLÍTICA DE PROTECCIÓN DE INFORMACIÓN PERSONAL.

6 de agosto de 2024.

Contenidos

Sección 1

Presentación y Alcance.

La información personal (“IP”) es aquella relacionada directamente a los datos de identificación de un individuo. Marsh & McLennan Companies, Inc y sus empresas filiales (colectivamente la “Empresa”) respetan la privacidad, la seguridad y la integridad de la IP que nos confían nuestros clientes, socios comerciales y colegas. Esta Política establece pautas mínimas para facilitar el cumplimiento de la Empresa con los requisitos contractuales y normativos correspondientes, así como también con nuestras obligaciones profesionales para con nuestros clientes, socios comerciales y colegas.

A medida que cualquier empresa filial de la Empresa esté sujeta a leyes o normas que imponen obligaciones más estrictas con respecto a la IP, esa empresa y sus colegas deberán cumplir con esas obligaciones más estrictas.

Esta Política se aplica a todos los directores, funcionarios, empleados y empleados temporales de la Empresa y sus subsidiarias alrededor del mundo, quienes recolectan, utilizan, divulgan, transfieren, retienen, procesan, destruyen (colectivamente denominado “proceso”) o de algún otro modo, tienen acceso a IP relacionada con la Empresa

Sección 2

Declaración de políticas.

La Empresa se compromete a proteger la IP que recolectemos, utilicemos o de algún otro modo procesemos, incluyendo aquella de nuestros clientes, socios comerciales y colegas mediante la implementación procedimientos y medidas de seguridad adecuadas y razonables y mediante el cumplimiento con las leyes y las normas relevantes.

La Empresa recolecta, utiliza y de algún otro modo procesa IP con los siguientes fines comerciales legítimos:

- Ejecución de procesos comerciales, inclusive para prestación de servicios a los clientes
- Gestión de nuestra empresa, incluyendo en la recolección de ingresos, realización de pagos, obtención de mercaderías y servicios, concesión de licencias y el cumplimiento de leyes/regulaciones tales como de impuestos, anticorrupción, sanciones económicas y otras leyes.
- Comunicación interna y externa.

La empresa se esfuerza por cumplir con los siguientes principios al momento de procesar IP:

- Procesamiento justo y legítimo de la IP
- Recolección, utilización y de algún otro modo procesamiento de IP solamente para propósitos legítimos compatibles con los propósitos comerciales enumerados anteriormente
- Recolección, utilización y de algún otro modo procesamiento de IP de manera tal que ayude a garantizar que es exacta y cuando sea necesario, su actualización
- Retención de la IP durante el tiempo necesario o durante el período exigido por la ley o regulación, programas de retención de registro u otro.
- Transmisión de la IP fuera de la empresa o a terceros solamente cuando sea necesario para fines comerciales específicos y legítimos y de manera tal que proteja la IP y cumpla con las leyes y normas correspondientes.
- Protección de la IP a través de mecanismos técnicos diseñados para prevenir el acceso no autorizado, procesos ilegales y/o pérdida, destrucción o daño no autorizado o accidental a la IP

La metodología adoptada para respaldar estos principios debe ser adecuada para la protección de la IP que se esté procesando, sin dejar de lado el tipo de IP, los requisitos legales correspondientes y los riesgos relacionados con la empresa en particular

Sección 3

Definiciones

La información personal (denominada “datos personales” en algunos países) es toda aquella información relacionada directamente con una persona identificada o identificable, tal como el nombre de una persona cuando se procesa en relación con cualquier otra información específicamente relacionada con esa persona. Los datos anónimos y sin referencias personales no están sujetos a esta Política.

Ciertos tipos de IP, tal como información de atención médica personal, se consideran “sensibles”. El nombre de una persona junto a un número de cuenta bancaria, un número de tarjeta de crédito o un número de identidad personal emitido por el gobierno, tal como un número de seguro social, también podría considerarse sensible (dependiendo de la legislación). La IP considerada sensible en ciertas jurisdicciones puede estar sujeta a niveles superiores de medidas de seguridad.

La categorización de la IP sensible varía según la ubicación y la empresa. El área de Cumplimiento o Legal le proporcionarán directrices sobre el alcance de la IP sensible para su empresa y las medidas de seguridad y los requisitos específicos para procesarla.

Sección 4

Responsabilidades de los empleados.

Usted debe cumplir con los siguientes requisitos de esta política cuando procese IP. Además, debe cumplir con todos los procedimientos correspondientes específicamente para su empresa. Si un cliente busca imponer otros requisitos, consulte con el área de Cumplimiento o Legal.

Recolección, uso y claridad de la información personal

Usted tiene permiso para recolectar y utilizar solamente IP que sea razonablemente necesaria para un propósito comercial legítimo. Si recibe de forma innecesaria o por error algún tipo de IP, esta deberá destruirse o devolverse de manera segura.

Usted debe seguir una serie de medidas razonables para mantener la precisión de la IP que procesa, tal como corregir la IP si le solicitan que lo haga. El área de Cumplimiento o Legal pueden orientarlo acerca de los requisitos pertinentes, tales como el tiempo mínimo de respuesta para cualquier solicitud.

Seguridad de la información personal

Usted debe seguir todos los pasos necesarios para proteger razonablemente la IP, mediante el buen juicio con respecto a esta Política y a todos los procedimientos adicionales pertinentes emitidos conforme a esta Política.

Debe hacer los esfuerzos razonables para limitar el acceso a la IP solamente para aquellos colegas que necesiten acceder a ella para brindar productos o servicios con los cuales la Empresa esté comprometida o de cualquier otra manera, que cumplan con los requisitos de su función. También debe hacer los esfuerzos razonables para prevenir el acceso no autorizado de terceros que no deberían tener ese acceso.

No debe tratar de obtener acceso a IP que no sea adecuada para su función. Si accede a esa IP por accidente, no debe arriesgar la seguridad o exactitud de la IP.

Si almacena la IP electrónicamente, debe hacerlo de manera segura conforme a esta Política. Por lo general, debe utilizar solamente computadoras, laptops y dispositivos de almacenamiento de información aprobados o proporcionados por la Empresa para su trabajo. Si su computadora, computadora portátil u otro dispositivo de almacenamiento de información portátil que contiene IP está sin vigilancia, deberá activar su protección de contraseña electrónica. Los dispositivos portátiles no deben dejarse en lugares públicos sin vigilancia.

Usted debe almacenar documentos impresos que contengan IP de manera tal que el acceso inadecuado se vea limitado. Por ejemplo, debe limpiar y asegurar los escritorios u otras áreas sin vigilancia donde sea posible encontrar IP.

Además, al almacenar IP, también deberá cumplir con todos los demás procedimientos correspondientes a su empresa, así como también con los requisitos pertinentes del cliente que su empresa ha aceptado.

Transferencia de información personal

No debe transferir IP fuera de la Empresa o entre empresas de la Empresa a menos que la transferencia sea razonablemente necesaria para un propósito comercial legítimo. Antes de cualquier transferencia, usted deberá confirmar que la transferencia cumplirá con todas las protecciones requeridas tal como se establece en todos los procedimientos advertidos por el área de Cumplimiento o Legal. Estas protecciones pueden incluir la existencia de un contrato formal que controle la relación con el receptor de la IP.

La transferencia de IP sensible generalmente requiere medidas de seguridad específicas, tales como mecanismos de encriptación al hacer transferencias electrónicas. Comuníquese con el servicio de ayuda de TI local para obtener las soluciones que pueda necesitar.

Cuando transfiera IP de manera electrónica y no electrónica fuera del país, ya sea que la transferencia ocurra fuera o dentro de la Empresa, deberá cumplir con las leyes y regulaciones del país de origen además de cumplir con todos los procedimientos de IP pertinentes específicamente para su empresa.

El área de Cumplimiento o Legal pueden ayudarlo a comprender estos requisitos.

Destrucción de información personal

Usted debe destruir la IP que ya no sea necesaria para un propósito comercial legítimo de manera segura de acuerdo con las políticas de retención de documentos pertinentes. Sin embargo, no es posible destruir la IP que esté sujeta a una retención legal o regulatoria o a otra acción judicial. Consulte con el área de Cumplimiento o Legal si no está seguro de si la IP en cuestión esté sujeta a este requisito.

La Empresa debe realizar operativamente la supresión del dato de tal manera que la eliminación no permita la recuperación de la información.

En caso de que no sea posible destruir la IP por razones contractuales, legales o técnicas, usted deberá retenerla de acuerdo con esta Política y todos los procedimientos pertinentes. Consulte con el servicio de ayuda de TI local o con el Oficial de Cumplimiento para obtener soluciones para la retención de IP electrónica.

CONSENTIMIENTO INFORMADO.

Para todas las operaciones de La Empresa en las que se recolecte información personal, será necesario contar con un consentimiento informado, en virtud del cual los titulares de la información autorizan a La Empresa a tratar los mismos. El modelo aplicable a cada Compañía Operativa (OpCo) podrá ser encontrado en el anexo aplicable a cada país.

REVOCATORIA DE LA AUTORIZACIÓN.

Los Titulares de los datos personales pueden revocar el consentimiento al tratamiento de sus datos personales en cualquier momento, siempre y cuando no lo impida una disposición legal o contractual, mediante los canales establecidos por La Empresa.

Se deberá tener en cuenta que existen dos modalidades en las que la revocación del consentimiento puede darse. La primera puede ser sobre la totalidad de las finalidades consentidas, esto es, que La Empresa deberá dejar de tratar por completo los datos del titular; la segunda, puede ocurrir sobre tipos de tratamiento determinados, como para fines comerciales o educativos.

Por lo anterior, será necesario que el Titular al momento de elevar la solicitud de revocatoria indique en ésta si la revocación que pretende realizar es total o parcial

Sección 5

Responsabilidades de la gerencia.

Los Oficiales de Cumplimiento de toda la empresa son responsables de evaluar el riesgo comercial relacionado con el procesamiento de IP y de trabajar con la gerencia para desarrollar requisitos de procedimientos, controles, capacitación y documentación adecuados para el riesgo.

Este proceso incluye lo siguiente:

- Determinar qué se considera como IP sensible en base a la ley aplicable en cada jurisdicción.
- Establecer las medidas de seguridad técnicas, físicas y administrativas basadas en los riesgos para proteger la IP, lo cual incluye medidas de seguridad para el equipo, las instalaciones y las ubicaciones donde esté almacenada la IP.
- Establecer mecanismos y procedimientos para procesar ciertos tipos de IP de acuerdo con requisitos específicos de la industria, tales como los Estándares de Seguridad de Datos para la Industria de Tarjeta de Pago (PCIDSS) para la información de tarjetas de pago.
- Cuando lo exija la ley, establecer procedimientos para notificar a las personas acerca de cómo se procesa su IP y para obtener su consentimiento a ese procesamiento.
- Cuando lo exija la ley, establecer procedimientos para permitirles a las personas acceder a la IP que la Empresa mantiene sobre ello y enmendar una IP incorrecta o incompleta.
- Establecer procedimientos y requisitos para transferir una IP a países que no sea el país en el que se recolectó y para transferir una IP a terceros, tal como los proveedores de servicio que crean o procesan la IP en nombre de la Empresa o para esta.
- Establecer mecanismos para implementar estos procedimientos; Y,
- Designar oficiales de privacidad tal como lo exige la ley o según sea necesario para cumplir con esta Política.

Sección 6

Derechos de los consumidores.

De conformidad con lo establecido en la normatividad vigente, el Titular de los datos personales tiene los siguientes derechos:

a) Conocer, actualizar y rectificar sus datos personales frente a La Empresa.

b) Solicitar prueba de la autorización otorgada a La Empresa en su condición de Responsable/encargado del Tratamiento.

c) Ser informado acerca de los usos o Tratamiento otorgado a los datos personales del Titular, previa consulta por parte de éste.

d) Presentar ante los entes reguladores quejas por infracciones a lo dispuesto en la Ley, una vez haya agotado el trámite de consulta o reclamo ante La Empresa.

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.

f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento

Sección 7

Deberes de la empresa.

La Empresa tendrá presente en todo momento, que los datos personales son propiedad de los Titulares de la información y que solo ellas pueden decidir sobre los mismos. En este sentido, hará uso de ellos sólo para aquellas finalidades para las que se encuentra autorizado debidamente, y respetando en todo caso la Ley que protección de datos personales. La Empresa se compromete a cumplir en forma permanente con los siguientes deberes en lo relacionado con el Tratamiento de datos personales:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de habeas data.

b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, perdida, consulta, uso o acceso no autorizado o fraudulento.

c) Realizar oportunamente la actualización, rectificación o supresión de los datos;

d) Tramitar consultas y los reclamos formulados por los Titulares de los datos personales.

e) Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por un ente de control.

f) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella de acuerdo con la Ley.

g) Informar a los entes reguladores cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;

h) Cumplir las instrucciones que impartan los respectivos entes de control sobre la materia.

Sección 8

Responsabilidades de terceros.

Si la Empresa mantiene relación con terceros que procesan o tengan acceso a una IP relacionada con la Empresa, los colegas que supervisan al tercero deberán exigirle, por contrato lo siguiente:

(i) Cumplir con todas las normas de privacidad y seguridad de los datos correspondientes;

(ii) Esta Política

(iii) Todos los procedimientos emitidos conforme a esta Política; e

(iv) Informar inmediatamente a su contacto de la Empresa acerca de cualquier incidente supuesto o real de seguridad de datos (electrónicos o no electrónicos) que implique la IP relacionada con la Empresa.

Debe trabajar con el área de Cumplimiento o Legal sobre estos requisitos contractuales antes de contratar a terceros que procesen o tengan acceso a la IP relacionada con Empresa

Sección 9

Medidas de seguridad.

En desarrollo del principio de seguridad La Empresa adoptará las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros, evitando su adulteración, perdida, consulta, uso o acceso no autorizado o fraudulento.

La Empresa mantendrá protocolos de seguridad de obligatorio cumplimiento para el personal con acceso a los datos de carácter personal y a los sistemas de información. El procedimiento deberá considerar como mínimo los siguientes aspectos:

a) Ámbito de aplicación del procedimiento con especificación detallada de los datos protegidos.

b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en la Ley.

c) Funciones y obligaciones del personal.

d) Procedimientos de realización de copias de respaldo y de recuperación (back up) de los datos.

e) Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el procedimiento de seguridad.

¿CÓMO INFORMAR INCIDENTES?

De forma inmediata deberá informar cualquier incidente que implique la pérdida supuesta o real, el robo, la divulgación no autorizada o el uso inadecuado de la IP (electrónica o no electrónica) al Servicio de Ayuda de TI local y al área de Cumplimiento. Si un tercero que procese IP relacionada con la Empresa o tenga acceso a esta información le notifica acerca de un incidente de este tipo, deberá informar al Servicio de Ayuda de TI local y al área de Cumplimiento. También deberá informar todos aquellos incidentes que impliquen pérdida o robo de cualquier dispositivo electrónico relacionado con la Empresa (incluso si no cree que el dispositivo contenga una IP).

El Equipo de Respuesta a Incidentes de The Marsh & McLennan Companies, que incluye representantes de las funciones y las empresas relevantes, investigará las implicaciones y la importancia del incidente y determinará las obligaciones de la Empresa conforme al marco legal, técnico, de seguridad, regulatorio y/o legal pertinente.

Sección 10

Misceláneos.

Capacitación.

Los gerentes son responsables de garantizar que los colegas que supervisan reciban una copia de esta Política y asistan a la capacitación requerida.

El área de Cumplimiento brindará capacitación y comunicaciones en relación con esta Política y mantendrá registros de dicha capacitación y comunicaciones durante cinco años.

Control y monitoreo.

Para evaluar el cumplimiento con esta Política, TI puede hasta donde lo permita la ley, controlar periódicamente los sistemas informáticos para comprobar que se ha hecho un uso autorizado de la IP o que se ha tenido un acceso autorizado a esta.

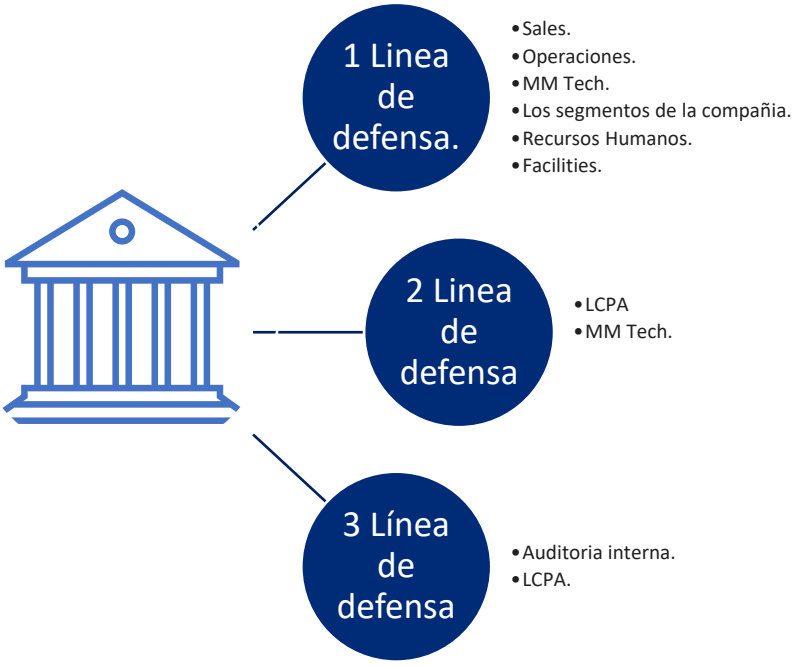
El área de Cumplimiento y de Auditoría Interna controlarán periódicamente el cumplimiento general de esta Política y procedimientos de las Empresas Operativas relacionadas e informarán, según sea apropiado, a la Gerencia o al Directorio.

Cumplimiento de la política.

Si no se cumple con esta Política o con las leyes de seguridad y privacidad de datos pertinentes, la Empresa y las personas involucradas pueden estar sujetas a penas civiles y criminales y pueden dañar gravemente la reputación de la Empresa. Consecuentemente, no cumplir con esta Política (lo cual incluye no informar los incidentes) puede llevar a acciones disciplinarias de acuerdo con la legislación local o los procedimientos internos, hasta la terminación del empleo o del contrato de servicios. Si usted o un tercero se percatan de cualquier infracción o supuesta infracción, comuníquese con el área de Cumplimiento o Legal.

Área encargada de la protección de datos y gobierno corporativo.

La Empresa y sus funcionarios están comprometidos con la protección de datos personales y la responsabilidad en su manejo, por ello, ha destinado el siguiente gobierno corporativo y sus diferentes líneas de defensa, quienes tendrán la función de proteger, en sus respectivos niveles la información personal que llegue a conocerse:



Recursos.

Para información relacionada con el manejo local de IP, por favor consulta los anexos aplicables para los siguientes países Costa Rica, Colombia, Panamá, Puerto Rico, República Dominicana, Venezuela.

Contacto.

En caso de preguntas, contactarse con el buzón solicitudeslcpa@marsh.com

Fecha de entrada en vigor: 6 de agosto de 2024.

Legal Compliance and Public Affairs.

Sección 11

Aspectos locales sobre la protección de información personal.

Colombia.

1. ¿QUE LEGISLACIÓN SE DEBE TENER EN CUENTA?

Deberán tenerse en cuenta las disposiciones contenidas en los Artículos 15 y 20 de la Constitución Política, la Ley 1581 de 2012 "*Por la cual se dictan disposiciones generales para la protección de datos personales"* y el Decreto 1377 de 2013 "*por el cual se reglamenta parcialmente la ley 1581 de 2012*" así como también lo establecido en la Ley 2300 de 2023.

2. ¿DEBO CONTAR CON AUTORIZACIÓN PARA TRATAR DATOS PERSONALES?

Si, La recolección, almacenamiento, uso, circulación o supresión de datos personales por parte de La Empresa requiere del consentimiento libre, previo, informado y expreso del Titular de estos.

La Empresa en su condición de Responsable/Encargado del tratamiento de datos personales, ha dispuesto los mecanismos necesarios para obtener la autorización de los titulares garantizando en todo caso que sea posible verificar el otorgamiento de dicha autorización.

La Autorización del Titular deberá contener como mínimo la siguiente información.

a) Objeto de la autorización.
b) Finalidad del Tratamiento de Datos Personales.
c) Usuarios de la información.
d) Transferencia Internacional de información a terceros países
e) Datos personales de niños, niñas y adolescentes.
f) Responsables y encargados de la información.

3. ¿CÓMO Y EN DONDE CONSULTAR LAS CONDICIONES DEL TRATAMIENTO DE DATOS PERSONALES?

El aviso de privacidad podrá encontrarse en el siguiente link: https://www.marsh.com/co/privacy-notice.html

Para información adicional sobre el tratamiento de datos personales, por favor acceder al siguiente link: https://www.marsh.com/co/about/about-marsh/attention-to-financial-consumers.html

4. ¿COMO REALIZAR SOLICITUDES RELACIONADOS CON DATOS PERSONALES?

De conformidad con lo establecido en el artículo 15 de la Ley 1581 de 2012, el Titular o sus causahabientes que consideren que la información contenida en una Base de Datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes establecidos por la Ley 1581 de 2012, podrán presentar un reclamo ante La Empresa. mediante el siguiente correo electrónico solicitudeslcpa@marsh.com, el cual será tramitado siempre que la reclamación reúna los siguientes requisitos:

1. El reclamo lo podrá presentar el Titular informando lo siguiente:

a) Número de identificación del Titular.
b) Descripción de los hechos que dan lugar al Reclamo.
c) Dirección para responderle.
d) Documentos que se requieran para hacer valer la reclamación.

2. Una vez La Empresa reciba la reclamación, requerirán al interesado dentro de los cinco (5) siguientes a su recepción para que subsane las fallas, en los eventos en que la reclamación no cumpla con los requisitos establecidos.

3. Transcurridos dos (2) meses desde la fecha del requerimiento sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

4. Una vez recibido el reclamo completo por parte La Empresa, se incluirá en la base de datos “SICS” que mantiene La Empresa una leyenda que diga reclamo en “tramite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles.

   Dicha leyenda deberá mantenerse hasta que el reclamo sea atendido a satisfacción del Titular.

5. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atenderlo dentro de dicho término, se informará al interesado antes del vencimiento del referido plazo los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Si por alguna circunstancia se recibe un reclamo que en realidad no debería ir dirigido contra La Empresa, se dará traslado de la misma, en la medida de sus posibilidades, a quien corresponda, en un término máximo de dos (2) días hábiles, e informará de la situación al interesado.

5. CUMPLIMIENTO DE LA LEY 2300 DE 2023.

La Ley 2300 de 2023 más conocida como la “Ley dejen de fregar”, busca proteger el derecho a la intimidad de los consumidores y regular la cantidad de mensajes publicitarios, canales y horarios en los que las personas pueden ser contactadas para realizar gestión de cobro o recibir información de carácter comercial.

En cumplimiento de esta ley, la Empresa solo podrá contactar a los clientes podrán únicamente por los canales que ellos autoricen para tal efecto, los cuales deberán ser informados y socializados previamente, con el fin de que los consumidores elijan cuáles autoriza.

Las prácticas de cobranzas y envío de mensajes de carácter comercial o publicitario se deberán realizar de manera respetuosa y sin afectar la intimidad personal ni familiar del consumidor de lunes a viernes de 7:00 am a 7:00 pm y sábados de 8:00 am a 3:00 pm. Una vez establecido un contacto directo con el consumidor, este no podrá ser contactado por parte de gestores de cobranza mediante varios canales dentro de una misma semana ni en más de una ocasión durante el mismo día.

La única excepción a lo anterior aplica en caso de que el consumidor requiera ser contactado en horarios distintos a los establecidos, para lo cual, así deberá manifestarlo expresamente a través de un instrumento distinto al contrato o acto que rige la relación jurídica entre el consumidor y el gestor de cobranza y posterior a la suscripción de este.

La normatividad exige, particularmente lo siguiente:

1. En ningún caso las Empresa adelantando gestiones de cobranza de forma directa, por medio de terceros o por cesión de la obligación incluyendo a las personas naturales; podrán contactar a las referencias personales o de otra índole.
2. No podrá obligarse al consumidor a aceptar recibir mensajes comerciales de ninguna índole cuando se realice una transacción comercial de bienes o servicios, o se ingrese a un edificio o local.

3. La empresa deberá habilitar y disponer de un mecanismo ágil, sencillo y eficiente para cancelar en cualquier momento la recepción de mensajes y correos, siempre y cuando no exista el deber contractual de permanecer en la respectiva base de datos de cobro.

4. Las personas naturales y jurídicas se abstendrán de adelantar visitas de cobro al lugar de trabajo o domicilio. Aplican las siguientes excepciones:

    4.1. Cuando se trate de obligaciones adquiridas a través de microcrédito, crédito de fomento, desarrollo agropecuario o rural siempre y cuando exista autorización expresa del consumidor.

    4.2. Cuando las personas naturales y jurídicas gestoras de cobranza, no cuenten con información actualizada de los canales autorizados.

4.3. Cuando los operadores de telefonía y empresas de mensajería física o electrónica reporten imposibilidad de contactar o entregar los mensajes al consumidor destinatario, todo lo cual deberá constar en el registro respectivo.

5. Se exceptúan de las medidas consagradas en la ley 2300 de 2023, las siguientes comunicaciones:

5.1. Aquellas comunicaciones que tengan como finalidad informar al consumidor sobre confirmación oportuno de las operaciones monetarias realizados, sobre ahorros voluntarios y cesantías.

5.2. Enviar información solicitado por el consumidor.

5.3. Generar alertos sobre transacciones fraudulentos, inusuales o sospechosos.

6. CONSULTAS.

El poder de disposición o decisión que tiene el Titular sobre la información que le concierne conlleva necesariamente el derecho de acceder y conocer si su información personal está siendo objeto de tratamiento por parte de La Empresa, así como el alcance, condiciones y generalidades de dicho Tratamiento.

De esta manera La Empresa debe garantizar al Titular el derecho de acceso a través de dos canales gratuitos:

a. Mediante petición escrita en forma de derecho de petición el cual deberá dirigirse a Servicio al Cliente mediante el siguiente canal: servicioalcliente.delima@marsh.com

b. Mediante solicitud a través del correo electrónico solicitudeslcpa@marsh.com

En cualquier caso, independientemente de los canales mencionados para la atención de solicitudes de consulta, las mismas serán atendidas en un término máximo de quince (10) días hábiles contados a partir de la fecha de su recibo.

Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los diez (10) días, expresando los motivos de la demora y señalando la fecha en que se atenderá la consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer plazo.

Legal Compliance and Public Affairs.

Control de versiones.

No de Versión.	Fecha de aprobación.	Responsable.
Versión No 2	6 de agosto de 2024	Omar León/LCPA Jhonatan Gómez./LCPA Mariano Alva/LCPA