Versión: 1.0 de octubre 28 de 2016

Términos de procesamiento de datos para los servicios gestionados[1]

El Cliente (definido más adelante) está aceptando estos Términos de Procesamiento de Datos, incluyendo las listas adjuntas (colectivamente, los "DPT"), porque ha celebrado cierto Acuerdo de Servicio (definido más adelante) con la Compañía (definida más adelante). Estos DPT los celebran el Cliente y la Compañía a partir de la fecha de vigencia del Acuerdo de Servicio. En caso de que el Acuerdo de Servicio se haya celebrado antes de la fecha de vigencia indicada anteriormente y dicho Acuerdo de Servicio esté sujeto a una extensión de su plazo, estos DPT sustituyen a cualesquiera términos de procesamiento de datos previamente contraídos por el Cliente y la Compañía.

Estos DPT se incorporan siempre en todos los Acuerdos de Servicio por referencia. En caso de conflicto o discrepancias entre los términos del Acuerdo de Servicio y los DPT, los términos de los DPT deben siempre prevalecer y regir. Se recomienda al Cliente leerlos. En el caso de que el Cliente esté en desacuerdo con algunos de estos términos, se le invita a aportar sus observaciones y comentarios antes de la firma del Acuerdo de Servicio. En caso de que la Compañía y el Cliente acuerden modificar los DPT, la enmienda acordada se anexará al Acuerdo de Servicio.

1- El motivo para los DPT

La Solución (definida más adelante), que se basa en software o en una combinación de software y hardware, permite el procesamiento de los Datos Personales del Cliente (definido más adelante) para dirigir los beneficios de la Solución (definida más adelante) al Cliente, así como en el caso de una Oferta del Cliente (definida más adelante) a los Usuarios Finales (definidos más adelante).

La Solución puede estar alojada en una Entidad de Hosting (definida más adelante) que no está controlada por la compañía. La Sección 4 abajo ofrece una explicación detallada de la función de Entidad de Hosting (definida más adelante).

El Cliente y la Compañía reconocen y aceptan que las Leyes de Protección de Datos Personales (definida más adelante) pueden aplicarse al procesamiento de los Datos Personales del Cliente. En tal caso, los DPT son aplicables.

2- Definiciones

No obstante cualquier definición contraria en el Acuerdo de Servicio, los términos en mayúsculas utilizados en estos DPT, ya sea en singular o en plural, tendrán los siguientes significados en el contexto de estos DPT:

Leyes aplicables de protección de datos: significa las Leyes de Protección de Datos Personales aplicables al Cliente como Controlador de Datos de los Datos Personales.

Empleados autorizados: significa los empleados del Gemalto Group que tienen necesidad de saber o acceder por otras causas a los Datos Personales del Cliente para permitir que se cumpla con el Acuerdo de Servicio.

Personas autorizadas: significa (i) Empleados Autorizados; y (ii) el Procesador Secundario que tienen necesidad de saber o acceder por otras causas a los Datos Personales del Cliente para permitir que se haga efectivo el Acuerdo de Servicio.

Infracción de la seguridad: significa la adquisición no autorizada o el uso no autorizado de (i) datos sin cifrar o (ii) datos cifrados electrónicos de datos y el proceso confidencial u otra llave que pueda comprometer

[1] Modelo de entrega de los servicios gestionados: prestado como un Servicio fuera de los locales del cliente.

la seguridad, confidencialidad o integridad de la información personal y que conserve una persona que cree un riesgo significativo de robo de identidad o fraude contra una persona.

Información del Cliente: significa información personal que puede recopilarse a partir de las interacciones de los empleados o agentes del Cliente con Gemalto Group en la prestación de los servicios de asistencia y mantenimiento.

Compañía: significa la entidad jurídica miembro del Gemalto Group que celebra el Acuerdo de Servicio.

Cliente: significa la entidad jurídica que celebra el Acuerdo de Servicio.

Datos Personales del Cliente: significa los Datos Personales contenidos en los datos transmitidos directamente por el Cliente, o en su nombre o por los Usuarios Finales, a la solución.

Oferta del Cliente: significa los servicios que ofrece el Cliente a los Usuarios Finales.

Centro de Datos: significa la propiedad física de Gemalto Group donde está instalada la solución.

Controlador de datos: significa a la persona física o jurídica que determina la finalidad y los medios para el procesamiento de los Datos Personales.

Leyes de Protección de Datos Personales: significa todas las leyes, reglas, regulaciones, requisitos gubernamentales, códigos y leyes internacionales, federales, estatales y provinciales aplicables a los Datos Personales.

Contrato modelo de la UE: significa las cláusulas contractuales estándar (procesadores) para la transferencia de Datos Personales a procesadores situados en terceros países que no garantizan un nivel adecuado de protección de los datos.

Usuarios finales: significa la persona física o jurídica que acepta recibir la Oferta del Cliente.

GDPR: significa la Regulación General de Protección de Datos (2016/679) del Parlamento Europeo y del Consejo sobre la protección de las personas físicas en relación con el procesamiento de los datos personales y la libre circulación de dichos datos, que deroga la Directiva 95/46/CE.

Gemalto Group: significa las entidades colectiva o individualmente controladas por Gemalto N.V., una compañía establecida según las leyes de Holanda. En este contexto, control significa la propiedad directa o indirecta (a través de cualquier número de niveles sucesivos) de: (a) más del cincuenta por ciento (50%) de las acciones en circulación con derecho a voto para la elección de directores u otra autoridad gestionadora de la entidad objeto; o (b) en el caso de una entidad que no tenga acciones en circulación (por ejemplo, una sociedad, empresa conjunta o asociación no incorporada), más del cincuenta por ciento (50%) de los intereses de propiedad que tenga el derecho de tomar decisiones para la entidad relativa.

Entidad de Hosting: significa una persona jurídica, que no es signataria del Acuerdo de Servicio, y que ha celebrado un acuerdo de externalización con el Administrador del Sistema para alojar la Solución.

Proceso legal: significa una solicitud de divulgación de datos hecha de conformidad con las leyes, una regulación gubernamental, orden judicial, citación, edicto, petición reglamentaria o agencia gubernamental, u otra autoridad legal, procedimiento legal o proceso similar válidos.

Datos personales: **:** significa (i) los datos que se refieren a un individuo viviente (ya sea en su vida personal o familiar, negocio o profesión) que puede ser identificado (a) a partir de esos datos, o (b) a partir de esos datos y otra información que estén en posesión del controlador de los datos, o que sea probable que puedan llegar a su posesión, así como (ii) información que puede utilizarse para identificar o rastrear la identidad de una persona, lo que incluye, entre otros datos, su nombre, dirección, número de la seguridad social, datos biométricos, fecha de nacimiento, etc. Esta definición puede adaptarse con respecto a la Ley Aplicable de Protección de Datos Personales (por ejemplo, algunas Leyes de Privacidad cubren no sólo a individuos, sino a entidades jurídicas, y no sólo a personas en vida, sino a fallecidas).

Programa de seguridad: significa el programa de seguridad adjunto como **Lista 1** de estos DPT.

Acuerdo de Servicio: significa cierto acuerdo celebrado entre el Cliente y la Compañía.

Datos de servicios: significa los datos que residen en la Solución a la que se da acceso a Gemalto para suministrar servicios de asistencia y mantenimiento (lo que incluye los entornos de nube, así como entornos de prueba, desarrollo y producción a los que se pueda acceder para realizar los servicios de asistencia y mantenimiento convenidos).

Solución: significa el sistema de información utilizado para almacenar, gestionar, utilizar y recopilar los Datos Personales del Cliente y los Datos de Servicios.

Procesador secundario: significa las personas jurídicas contratadas para proporcionar Servicios Específicos que pueden requerir algún procesamiento de los Datos Personales del Cliente.

A**dministrador de sistemas:** significa una entidad jurídica miembro de Gemalto Group que es responsable del mantenimiento, configuración y funcionamiento confiable de la Solución, tal como la instalación, la actualización de componentes informáticos y software, proporcionar automatización de rutina y mantener las políticas de seguridad.

Servicios específicos: significa fuera del ámbito de las tareas del Administrador del Sistema, determinados servicios que se estipulan en el Acuerdo de Servicio como son (a) la prestación de asistencia técnica a fin de resolver problemas específicos reportados, (b) la entrega de informes agregados analíticos y estadísticos.

Reclamación de un tercero: significa una demanda o una afirmación por un tercero que pretenda, como cuestión jurídica, el pago de dinero u otra reparación.

3- **Controlador de datos y procesador de datos**

3.1 El Cliente es el Controlador de Datos de los Datos Personales del Cliente y la Compañía, a través de su compromiso de los Procesadores Secundarios, es el procesador de los Datos Personales del Cliente. Además, el Administrador del Sistema mediante la contratación de la Entidad de Hosting o a través del Centro de Datos, puede procesar Datos Personales del Cliente al menos con respecto a facultar al Cliente para que almacene los Datos Personales del Cliente en la Solución.

3.2 En ciertos casos, el Cliente está conectado directamente a la Solución; así, el Cliente está realizando directamente, o permitiendo que los Usuarios Finales realicen, el aprovisionamiento de la Solución con los Datos Personales del Cliente.

3.3 Ni la Compañía, ni los Procesadores Secundarios, el Administrador del Sistema ni la Compañía de Hosting han recopilado los Datos Personales del Cliente. Los Procesador Secundarios y el Administrador del Sistema procesan los Datos Personales del Cliente como procesadores de datos bajo la dirección y previa aprobación del Cliente de acuerdo con los términos del Acuerdo de Servicio.

4- **Requisitos de transparencia**

4.1 Antes de celebrar el Acuerdo de Servicio con el Cliente, la Compañía entregará a éste un documento denominado "Formulario de procesamiento", una plantilla de la cual se adjunta como **Lista 2** a los DPT. Este documento describe el tipo de Datos Personales del Cliente que se procesarán mediante la Solución, el nombre y la ubicación de la Entidad de Hosting o el Centro de Datos donde esté alojada la Solución, el Administrador del Sistema y los Procesadores Secundarios involucrados en el Procesamiento de los Datos Personales del Cliente, cómo se procesan tales Datos Personales del Cliente, los flujos de los Datos

Personales del Cliente y el período de tiempo que se conservan los Datos Personales del Cliente durante la vigencia del Acuerdo de Servicio y después de la caducidad o finalización del Acuerdo de Servicio.

4.2 Una vez acordado, el Formulario de Procesamiento se anexa al Acuerdo de Servicio y se hace parte del mismo.

5- **Instrucciones del Cliente**

5.1 Los Datos Personales del Cliente sólo pueden procesarse en el ámbito de las instrucciones del mismo. El Acuerdo de Servicio establece las instrucciones del Cliente en relación con el tipo, alcance y método del Procesamiento de los Datos Personales del Cliente teniendo en cuenta las especificaciones de la Solución objeto del Acuerdo de Servicio y el contenido del Formulario de Procesamiento (al que se hace referencia en la sección 4 anterior). Con excepción de lo estipulado en estos DPT, ni la Compañía ni los Procesadores Secundarios, el Administrador del Sistema ni la Compañía de Hosting revisarán, compartirán, distribuirán, ni harán referencia a ningún Dato Personal del Cliente.

5.2 Cualquier cambio en el procesamiento de los Datos Personales durante la vigencia del Acuerdo de Servicio sólo puede producirse con la aprobación previa por escrito del Cliente.

6- **Entidad de Hosting y Centro de Datos**

6.1 En cuanto a los datos aplicables de los DPT, el Formulario de Procesamiento (según lo señala la Sección 4 arriba) identifica a cada Entidad de Hosting que ha celebrado, directa o indirectamente, un acuerdo específico de alojamiento con cada Administrador del Sistema relevante.

6.2 El Cliente utiliza la Solución alojada en el sistema de la Entidad de Hosting o Centro de Datos para transmitir o procesar los Datos Personales del Cliente. Tiene que entenderse que la Entidad de Hosting y el Centro de Datos no determinan ni tienen conocimiento de los tipos de datos almacenados por el Cliente o cómo se accede a esos datos, se intercambian, procesan o clasifican.

7- **Procesadores Secundarios**

7.1 En función del aprovisionamiento al Cliente de Servicios Específicos, la Compañía puede contratar al Procesador Secundario para proporcionar los Servicios Específicos en su totalidad o en parte.

7.2 Con respecto a los servicios de asistencia técnica que forman parte de los Servicios Específicos, el Cliente deberá tener en cuenta los términos estipulados en **Lista 3** que describen las prácticas de la organización de asistencia global ("OSG") de Gemalto Group referentes a los servicios de asistencia y mantenimiento.

7.3 En caso de que las estadísticas asociadas con un informe agregado, o los servicios de informes específicos para fines de facturación, se ofrezcan como parte del Servicio Específico, la entrega de tales Servicios Específicos requiere el uso de un programa de software que (i) tiene acceso a la base de datos de producción de la Solución de un modo seguro y (ii) extrae ciertos datos para almacenarlos en un almacén de datos situado en un local de Gemalto Group donde los datos son analizados para construir, en formato agregado, los paneles de mando e informes convenidos. Si tales estadísticas y servicios de informes se ofrecen como parte del Acuerdo de Servicio, se especificará en el Formulario de Procesamiento establecido en la Sección 4 anterior, indicando también dónde está situado el almacén de datos así como la identificación del Procesador Secundario.

7.4 La participación del Procesador Secundario requiere el consentimiento previo por escrito del Cliente, que se concede como parte de la firma del Acuerdo de Servicio.

7.5 Cuando el Procesador Secundario esté situado en un país no adecuado (un país que se considera que no proporciona un nivel adecuado de protección para los Datos Personales en el sentido de la Directiva de la UE 95/46/EC o GDPR), la Compañía deberá procurar que el Procesador Secundario celebre un Contrato de Modelo de la UE directamente con el Cliente. Tenga en cuenta que esta sección se basa en las leyes de privacidad de datos de la UE. Por lo tanto, puede no ser aplicable en ciertas jurisdicciones.

7.6 En caso de que la Compañía y el Cliente ya hayan celebrado un Acuerdo de Servicio y la Compañía esté planteándose contratar a un nuevo Procesador Secundario, ésta informará al Cliente dándole datos detallados sobre el Procesador Secundario y la parte del Acuerdo de Servicio que se subcontratará, y solicitará el consentimiento por escrito del Cliente mediante una enmienda del Acuerdo de Servicio. Si el cliente se opone a la contratación del nuevo Procesador Secundario, deberá informar inmediatamente a la Compañía por escrito. Inmediatamente después de recibir la objeción, el Cliente y la Compañía decidirán una solución alternativa.

8- **Transmisión de Datos Personales a otros países**

8.1 Como se indicó en la Sección 4 anterior, la Solución está alojada en la Entidad de Hosting o el Centro de Datos. En caso de que el uso de la Solución por parte del Cliente desencadene una transferencia transfronteriza de Datos Personales del Cliente, dicho Cliente entiende que tal transferencia transfronteriza de Datos Personales del Cliente puede estar sujeta a requisitos específicos impuestos por las Leyes de Protección de Datos Personales y la carga de tales requisitos específicos recae en el Controlador de Datos.

8.2 En caso de que tal traslado transfronterizo de Datos Personales del Cliente pudiera requerir la celebración de un acuerdo específico de transferencia transfronteriza a la luz de la ley de protección de Datos Personales aplicable. La Compañía y el Cliente colaborarán con el fin de cumplir con este requisito.

9- **Compromisos del Cliente**

9.1 El Cliente declara y garantiza que los Datos Personales del Cliente que proporciona para su Procesamiento pueden ser legalmente procesados (por ejemplo, recopilación legal, cumplimiento de la obligación de informar y cumplimiento de la Ley de Protección de Datos Personales).

9.2 El Cliente no pondrá, por ningún acto u omisión, a la Compañía, al Administrador del Sistema, al Procesador Secundario, a la Entidad de Hosting y Centro de Datos en una situación tal que infrinjan alguna Ley de Protección de Datos Personales en relación con el procesamiento de los Datos Personales del Cliente.

10- **Principios de seguridad**

10.1 De conformidad y dentro del límite del Programa de Seguridad, el Gemalto Group implementa medidas técnicas y organizativas para proteger los Datos Personales del Cliente contra las Infracciones de Seguridad. El Cliente acepta que es el único responsable del uso que haga de la Solución para el procesamiento de los Datos Personales del Cliente, lo que incluye sus credenciales de autenticación de la cuenta, y que la Compañía, el Administrador del Sistema, el Procesador Secundario, la Entidad de Hosting y el Centro de Datos no tienen ninguna obligación de proteger los Datos Personales del Cliente que éste opte por almacenar o transferir fuera del Procesador Secundario, la Entidad de Hosting y el Centro de Datos.

10.2 La Compañía tomará medidas razonables a fin de garantizar el cumplimiento del Programa de Seguridad por parte del Administrador del Sistema, el Procesador Secundario, la Entidad de Hosting y el Centro de Datos, en la medida aplicable a su ámbito de actuación.

10.3 (a) Si la Compañía tuviera conocimiento de una Infracción de Seguridad, notificará cuanto antes al Cliente de tal Infracción de Seguridad y tomará las medidas razonables para reducir al mínimo el daño y garantizar los Datos Personales del Cliente. Las notificaciones de Infracción de Seguridad se entregarán

mediante el contacto de notificación proporcionado por el Cliente en el Acuerdo de Servicio o, a discreción de la Compañía, mediante comunicación directa al Cliente (por ejemplo, mediante llamada telefónica o una reunión en persona). El Cliente reconoce que es el único responsable de garantizar que la información de contacto indicada anteriormente sea actual y válida, y del cumplimiento de cualquier obligación de notificación a terceros. La obligación de la Compañía de informar o responder a una Infracción de Seguridad bajo esta Sección 10.3 no se interpretará como un reconocimiento por parte de la Compañía de ninguna culpa o responsabilidad con respecto a la Infracción de Seguridad.

(b) Inmediatamente después de la notificación de la Compañía al Cliente de una Infracción de Seguridad, el Cliente y la Compañía se coordinarán entre sí para investigar dicha Infracción de Seguridad. La Compañía dirige la investigación y se compromete a cooperar de modo razonable con el Cliente en el manejo de la Infracción de Seguridad, incluyendo, entre otras cosas: (i) ayudar con cualquier investigación; (ii) proporcionar al Cliente acceso físico a las instalaciones y operaciones afectadas que estén bajo el control de Gemalto Group; (iii) facilitar entrevistas con las Personas Autorizadas; y (iv) poner a disposición los registros, bitácoras, archivos, informes de datos y otros materiales pertinentes relacionados con el Cliente, necesarios para cumplir con la Ley de Protección de Datos Personales o regulación aplicables, o según lo razonablemente requerido por el Cliente.

10.4 Sin perjuicio de cualquier cosa en contrario que haya en el Acuerdo de Servicio o el Programa de Seguridad, las obligaciones de la Compañía, el Procesador Secundario, el Administrador del Sistema, la Entidad de Hosting y el Centro de Datos se extienden solamente a los sistemas, redes, dispositivos de red, instalaciones y componentes sobre los cuales ejercen control. El Programa de Seguridad no se aplica a: (i) Los Datos Personales del Cliente compartidos ya sea con la Compañía, el Procesador Secundario, el Administrador del Sistema, la Entidad de Hosting y el Centro de Datos, que no sean datos almacenados en la Solución; (ii) Los Datos Personales del Cliente en la red privada virtual (VPN) del Cliente o de una red de terceros, o (iii) Datos Personales del Cliente procesados por el Cliente o sus usuarios infringiendo el Acuerdo de Servicio o el Programa de Seguridad.

10.5 La solicitud para auditar el Programa de Seguridad la enviará el Cliente a la Compañía por medio de la notificación de contacto prevista en el Acuerdo de Servicio. En particular, la Compañía (a través de su Departamento de Seguridad Corporativa) y el Cliente analizarán y acordarán por anticipado la identidad de un auditor externo independiente debidamente cualificado para realizar la auditoría y la fecha de inicio razonable (es decir, en un mínimo de treinta (30) días naturales desde la fecha en que la Compañía reciba la solicitud de auditoría), el ámbito y la duración de tal auditoría y los controles de seguridad y confidencialidad que le sean aplicables. Se hace consciente al Cliente de que la auditoría del Programa de Seguridad deberá tener en cuenta las normas y políticas de seguridad de cada Entidad de Hosting, Centro de Datos y Procesador Secundario, que pueden imponer límites sobre el alcance que el Cliente espera que tenga la auditoría. La Compañía (a través de su Departamento de Seguridad Corporativa) está disponible para proporcionar detalles sobre tales límites, de haberlos. La Compañía no es responsable por ningún costo en que incurra el Cliente, ni de honorarios cobrados por cualquier auditor externo designado por el Cliente en relación con una auditoría. Además, la Compañía se reserva el derecho a cobrar honorarios y costos de cualquier solicitud de la auditoría superior a una (1) por cada año natural.

10.6 Los Datos Personales del Cliente están sujetos a ciertas obligaciones de confidencialidad establecidos por el Programa de Seguridad. En consecuencia, una Infracción de Seguridad que exponga Datos Personales del Cliente no activará la disposición de confidencialidad establecida en el Acuerdo de Servicio que abarcan datos e información que se consideran información confidencial. Esta sección 10.6 regirá y prevalecerá en caso de conflicto con la disposición de confidencialidad establecida en el Acuerdo de Servicio.

11- **Cooperación con respecto a las solicitudes y consultas**

11.1 La Compañía informará prontamente al Cliente (y, en cualquier caso, a más tardar cinco (5) días naturales después de recibir una queja, solicitud o consulta) de las quejas, solicitudes o consultas recibidas

de los particulares, incluyendo, entre otras, las peticiones para corregir, borrar o bloquear Datos Personales del Cliente. La Compañía no responderá directamente a la persona a menos que específicamente así se lo indique el Cliente, salvo cuando la Compañía o el Procesador Secundario, el Centro de Datos, la Entidad de Hosting o el Administrador del Sistema deban responder por ley o mediante Proceso Legal, en cuyo caso responderá en un plazo razonable de tiempo y, en todo caso, según sea requerido por la ley aplicable. La Compañía cooperará con el Cliente para abordar y resolver tales quejas, solicitudes o consultas.

12- **Confidencialidad, archivado y destrucción de los Datos Personales**

12.1 Ni la Compañía ni el Procesador Secundario, Centro de Datos, Entidad de Hosting o Administrador del Sistema revelarán los Datos Personales del Cliente de ninguna manera a ningún tercero sin la previa autorización por escrito del Cliente, salvo cuando (i) la revelación sea necesaria para cumplir con el Acuerdo de Servicio o (ii) cuando, con arreglo a la Sección 10 anterior, los Datos Personales del Cliente tengan que ser revelados a una autoridad pública competente con el fin de cumplir con un Proceso Legal.

12.2 Como principio general, la Compañía o el Procesador Secundario, el Centro de Datos, la Entidad de Hosting o el Administrador del Sistema, conforme a los requisitos de las leyes aplicables, no conservarán los Datos Personales del Cliente más de lo necesario para el objetivo para el cual el Cliente confió dichos Datos Personales del Cliente a la Compañía según el Acuerdo de Servicio, o, según corresponda, dentro del límite de las normas PCI-DSS, PCI-CP o los requisitos de VISA, MASTERCARD o cualquier otro operador de red de pago.

12.3 A raíz de la implementación de la Sección 12.2 anterior, los Datos Personales se eliminan irrecuperablemente.

12.4 En caso de que el Cliente requiera que sus Datos Personales se archiven, la Compañía y el Cliente tendrán que celebrar un acuerdo de archivado que incluye, entre otras, las siguientes disposiciones:

a) Duración del archivado;
b) Tipo de almacenamiento;
c) Ubicación;
d) Condiciones de acceso;
e) Condiciones de precios;

13- **Procesamiento de la información de contactos de negocios**

13.1 El Cliente reconoce y acepta que sus empleados y agentes pueden tener que interactuar con la Compañía y los Procesadores Secundarios y, al hacerlo, podrían divulgar Información del Cliente. Se utilizará la información del Cliente con el fin de mantener el Acuerdo de Servicio, supervisar y administrar las compras y gestionar los servicios objeto del Acuerdo de Servicio.

13.2 De conformidad con la Sección 13.1 anterior, el Cliente, por la presente, declara y garantiza que ha obtenido el consentimiento necesario para los fines establecidos en la Sección 13.1 anterior y autoriza expresamente la utilización de los datos personales para tales fines, así como la cesión y transferencia de la Información del Cliente a nivel nacional e internacional según sea necesario para los efectos del Acuerdo de Servicio.

14- **Indemnización y responsabilidad legal**

14.1 Sujeto a la Sección 14.2 siguiente, la Compañía defenderá e indemnizará al Cliente de y contra cualesquiera y todas las pérdidas, daños y perjuicios, responsabilidades legales, acciones, juicios, intereses, sentencias, sanciones, multas, costos o gastos, incluyendo honorarios razonables de abogados ("Pérdidas"), directamente causados por o resultantes directamente de una Reclamación de un Tercero contra el Cliente que se desprenda de una Infracción de Seguridad que afecte a los Datos Personales del Cliente, siempre que se haya establecido que los términos del Programa de Seguridad han sido infringidos en todo o en parte, o que la Infracción de Seguridad ha sido causada por un defecto en el Programa de Seguridad.

14.2 La indemnización anterior está condicionada a que el Cliente: (a) notifique oportunamente a la Compañía por escrito de una Reclamación de un Tercero; (b) le otorgue a la Compañía el control exclusivo de la defensa contra ella, y cualesquiera negociaciones de solución relacionadas con ella; siempre y cuando, sin embargo, la Compañía no tenga autoridad para celebrar ninguna conciliación o compromiso en nombre del Cliente sin el previo consentimiento del mismo, el cual que no se retendrá ni diferirá sin motivo razonable. Si la Compañía no asume la defensa de una Reclamación de Terceros, el Cliente tendrá el derecho de llevar a cabo la defensa contra tal Reclamación de Terceros por sí mismo, siempre y cuando (i) nada de lo anterior limite o se considere que limita el derecho de una parte a disputar que una Reclamación de Terceros (o cualquier Pérdida que surja de la misma) se refiera a una Infracción de Seguridad, y (ii) si la Compañía ha aceptado que una Reclamación de Terceros se refiere a una Infracción de Seguridad, el Cliente no tendrá autoridad para celebrar ninguna conciliación o compromiso en nombre de la Compañía sin el consentimiento de ésta (el cual no se retendrá ni diferirá sin motivo razonable). En todo caso, el Cliente tendrá derecho a participar en la defensa de cualquier proceso con el abogado de su elección, a su exclusivo cargo, y cooperará con la Compañía en la defensa de una Reclamación de Terceros que se mantenga de tal manera.

15- **Cambios**

15.1 Si la Compañía:

a) determina que ella misma, o un Procesador Secundario, Centro de Datos, Entidad de Hosting o Administrador del Sistema no pueden en algún momento y por cualquier motivo cumplir con las obligaciones establecidas en estos DPT y no se puede reparar esta incapacidad para cumplir; o bien

b) tenga conocimiento de cualquier circunstancia o cambio en las Leyes de Protección de Datos Personales aplicable, que sea probable que tenga un efecto adverso sustancial sobre la capacidad de la Compañía, o el Procesador Secundario, Centro de Datos, Entidad de Hosting o Administrador del Sistema, para cumplir con las obligaciones establecidas en estos DPT:

La Compañía notificará de ello con prontitud al Cliente, en cuyo caso el Cliente tendrá el derecho de suspender temporalmente el procesamiento de los Datos Personales del Cliente hasta el momento en que el procesamiento se haya ajustado de modo tal que se subsane el incumplimiento.

16 - **Evolución de los DPT**

16.1 A petición del Cliente, la Compañía y el Cliente ocasionalmente evaluarán el procesamiento de los Datos Personales del Cliente. Si el Cliente considera que se requieren cambios en el procesamiento de los Datos Personales del Cliente a fin de cumplir con las Leyes de Protección de Datos Personales, el Cliente y la Compañía colaborarán para evaluar los cambios a realizar. La Compañía informará al Cliente de cualquier circunstancia que pueda ser relevante a este respecto, incluyendo, entre otras:

1) cambios relevantes en la prestación del Acuerdo de Servicio; o bien
2) fusión, reorganización, venta de todos o substancialmente todos los activos, cambio de control u operación de las leyes que afectan a la Compañía, el Procesador Secundario, el Centro de Datos, la Entidad de Hosting o el Administrador del Sistema.

Lista 1: Programa de seguridad

Principios básicos del programa de seguridad de Gemalto Group

Introducción:

Este documento detalla los principales elementos del programa de seguridad de Gemalto Group dedicado a la protección de los datos que se nos confían.

En caso de cualquier pregunta o la petición de detalles más a fondo, se invita a los clientes a comunicarse con su representante de Gemalto, quien posteriormente implicará al "Departamento de Seguridad Corporativa" de Gemalto Group según sea necesario.

Principios:

Este Programa de Seguridad tiene por objeto garantizar eso en el contexto actual de nuestras actividades internacionales.

Nuestro programa de seguridad pretende:

a) identificar, mediante el análisis de riesgos, las amenazas potenciales para la información del Cliente;
b) implementar soluciones de seguridad (tanto procesos como herramientas) a fin de limitar los riesgos para nuestros sistemas;
c) formar a nuestros empleados y proveedores externos de servicios de modo que implementen el Programa de Seguridad;
d) Monitorizar la seguridad de nuestros sistemas y procesos;
e) proporcionar información clara sobre el procesamiento de la información del Cliente;
f) responder a las consultas y solicitudes de los clientes sobre la protección de su información;
g) prepararnos en caso de crisis

Los siguientes párrafos describen más detalladamente los principios fundamentales del Programa de Seguridad que protege la información del Cliente.

A - Principios fundamentales

La gobernanza de nuestro programa de seguridad es:

- Con base en las varias políticas aplicables a Gemalto Group, así como a todos los empleados de Gemalto Group, empleados de proveedores de servicios externos y personas externas que presten servicio o se relacionen con el Sistema de Información (como se define más adelante).

- Bajo la responsabilidad del Departamento de Seguridad Corporativa y el departamento de IT, y a nivel local bajo la dirección del gerente designado de seguridad y IT. Y con el apoyo de los consejos de seguridad que funcionan de conformidad con la norma ISO27001.

- Se revisa periódicamente y su aplicación se comprueba durante auditorías de seguridad locales y centrales. Además, se llevan a cabo auditorías técnicas de seguridad a nivel corporativo y local. La periodicidad de tales auditorias varía teniendo en cuenta el nivel de seguridad, la sensibilidad y la vulnerabilidad del sistema.

Nuestro programa de seguridad se concentra en los siguientes elementos:

Identificación y clasificación de la información personal: El propósito de la política de identificación y clasificación de la información personal es establecer un sistema de prioridades para la protección de la información y los activos, con objeto de garantizar que los niveles de protección sean acordes con el valor de la información o el sistema que se están protegiendo a lo largo de todo su ciclo de vida, desde la elaboración a la destrucción. El uso de niveles de clasificación permite a la organización concentrar los costes de protección sobre la información de mayor valor. Esta política cubre los siguientes elementos principales:

- Establecer las normas corporativas de Gemalto Group para la gestión de la información, con respecto a su sensibilidad;
- Dimensión de la confidencialidad de la información a través de un sistema de etiquetado con cinco niveles de clasificación, desde Secreto (el más alto) hasta Público (el más bajo);
- Que la protección de la zona donde se encuentra la información sea la adecuada con el nivel de clasificación de la información;
- Acceso lógico restringido a ordenadores y redes sigue las mismas reglas que las restricciones de acceso físico;
- Registro de la recepción de medios físicos que contengan información confidencial;
- Reglas para la transmisión de información;
- Reglas para el almacenamiento físico, electrónico y de medios;
- Reglas para la destrucción;
- Regla de política de escritorio limpio.

Política de seguridad física y ambiental: Establecer los principales medios de defensa contra el robo o mal uso de productos y servicios suministrados por Gemalto Group y que se requieren para proteger nuestro know-how. También son una protección para nuestro personal. Esta política cubre los siguientes elementos principales:

- Aplicable a todos los emplazamientos de Gemalto Group. Un emplazamiento es un lugar físico donde los empleados de Gemalto Group están basados o donde se llevan a cabo operaciones de Gemalto;
- Todos los emplazamientos de Gemalto Group deben cumplir con características de seguridad mínimas definidas de acuerdo con sus dominios de actividad y los riesgos identificados de sus procesos;
- Todos los emplazamientos de Gemalto Group están sujetos a auditorías periódicas realizadas por el Equipo Corporativo de Seguridad para verificar el cumplimiento de la política;
- Todos los emplazamientos de Gemalto Group tienen un administrador de seguridad;
- Todos los emplazamientos de Gemalto Group están organizados en tres niveles de zona clasificados según los servicios de seguridad que ofrecen.

Política de seguridad del sistema de gestión de la configuración: Diseñado para establecer las normas de seguridad corporativas de Gemalto Group para la gestión de software durante su desarrollo y cuando se entregan. Esta política cubre los siguientes elementos principales:

- Principales temas de seguridad: confidencialidad, integridad, disponibilidad, rendición de cuentas y trazabilidad;
- Gestión del software a través de una herramienta de IT llamada un Sistema de Gestión de la Configuración (CMS);
- Aplicabilidad a todos los empleados, consultores o contratistas de Gemalto que trabajen en instalaciones de Gemalto o que estén conectados a través de redes o acceso remoto;
- La implementación de esta política se revisa durante auditorías de seguridad locales y centrales.
- Los roles y responsabilidades en la aplicación de esta política se asignan a un gran número de empleados de Gemalto, formado por personal de seguridad e involucrado en el desarrollo y gestión de software;
- Reglas que establecen acceso restringido a la sala donde se almacena el software sensible;
- Reglas que abordan el uso de cifrado para garantizar la confidencialidad.

Plan de Garantía de Seguridad para el desarrollo de software: A fin de proporcionar una seguridad constante de extremo a extremo y cumplir con las restricciones para el tiempo de comercialización, definimos "Objetivos de confianza". Esta noción modera la exposición general de riesgo según el contexto del proyecto. Con base en este objetivo, se realizan diversas actividades de seguridad durante el desarrollo de software. Así, las actividades de seguridad que se ponen en marcha se ven impulsadas por los riesgos que enfrentamos.

Esta calificación de confianza se puede realizar con el Cliente a fin de destacar los principales motores de riesgos.

Las actividades realizadas durante el desarrollo de software son:

- **Programa de educación** dedicado a equipos de desarrollo
- **Requisitos de estado basal**: requisitos básicos que proporcionan una protección "predeterminada" dentro del software. Con base en la Evaluación de Riesgos, se implementan contramedidas adicionales además de estos requisitos básicos.
- **Administración de riesgos**: identificación, clasificación y tratamiento de los principales riesgos impulsados por los casos de uso y el software de apoyo.
- **Revisión del código:** controles realizados en el código fuente (identificación y corrección de debilidades comunes)
- **Evaluación de la vulnerabilidad**: realizada durante y después del desarrollo. Proporciona una clasificación de las vulnerabilidades y lleva a acciones de contención y corrección.
- **Pruebas de seguridad**: asegura que se implementen todos los requisitos de seguridad y proporciona el nivel de protección esperado (prueba de cobertura del plan, pruebas de aplicaciones dinámicas, pruebas de penetración).

Reglas de seguridad para la subcontratación de desarrollo de software: Además de la Política de Seguridad del Sistema de Gestión de la Configuración, Gemalto Group ha diseñado una política que aborda la adquisición de servicios de desarrollo de software de terceros. Esta política tiene por objeto garantizar la confidencialidad de la información que se proporciona al proveedor del servicio. Esta política cubre los siguientes elementos principales:

- Definir tres niveles de seguridad, establecer un nivel de riesgo a la luz de la sensibilidad de la seguridad del software. El desarrollo de software con el más alto nivel de sensibilidad de seguridad (nivel 3) no se puede subcontratar;
- La externalización autorizada del software está sujeta a un contrato que impone la aplicación de la norma y auditoría de seguridad ISO 27001;

- El acceso a la red de Gemalto Group está sujeto a una evaluación del riesgo que se utiliza para definir el punto deseado de control, criterios de aceptación de la seguridad y la asignación de un representante de seguridad;
- Validación por parte del personal de seguridad de Gemalto Group de las configuraciones físicas y lógicas del proveedor del servicio;
- La información que se pone a disposición del proveedor de servicios es clasificada previamente por Gemalto de acuerdo con la política de identificación y clasificación de la información personal. Con base en tal clasificación, el proveedor de servicio está obligado a poner en vigor las normas aplicables de Gemalto Group;
- Los empleados del proveedor de servicios están sujetos a controles de seguridad para obtener acceso a la información. Sólo un número mínimo de empleados puede tener acceso a la información y tienen que estar formados en el nivel de seguridad correspondiente.

Política de Seguridad del Sistema de Información ("SI"): Diseñado de conformidad con la norma ISO27001 para (a) ilustrar los principios de seguridad del SI que son valiosos para elementos estratégicos clave, como los intereses implicados, los referenciales, las necesidades de seguridad de negocios y amenazas varias, y (b) garantizar que nuestros requisitos de seguridad estén de acuerdo con los requisitos de nuestros clientes. Esta política cubre los siguientes elementos principales:

- Especificaciones de las funciones y responsabilidades de los empleados de Gemalto Group involucrados en la seguridad del sistema;
- Aplicable a todos los emplazamientos de Gemalto Group, los empleados de Gemalto Group y los proveedores de servicio que trabajan en el SI de Gemalto Group;
- Revisión obligatoria de esta política cada dos años;
- Definir los niveles de seguridad para determinar la zonificación de seguridad aplicable por todos los emplazamientos de Gemalto;
- La zonificación de seguridad define las reglas de seguridad aplicables en función de la sensibilidad de la información que se procesa;
- Definir los roles y responsabilidades del personal de Gemalto Group encargado de garantizar la implementación de esta política;
- Proceso de evaluación de riesgos;
- Cumplimiento de los requisitos legales y reglamentarios en las jurisdicciones donde el Gemalto Group lleva a cabo sus operaciones;
- Reglas de seguridad aplicables a la utilización de equipos móviles (por ejemplo, ordenador portátil, tablet, teléfono móvil);
- Control de acceso dedicado en función del nivel de clasificación de seguridad;
- Reglas que deben seguir todas las personas a quienes se conceda acceso al SI, lo que incluye a los proveedores de servicios externos a fin de asegurarse de que se implemente el mismo nivel de seguridad;
- Principios de auditoría que definen el proceso de auditoría aplicable según el nivel de seguridad correspondiente;
- Se ponen en vigor pruebas de penetración de terceros con los proveedores externos;
- Controles de seguridad de SI mediante el uso de cortafuegos, detección de intrusos, sistemas de prevención y el uso de intranet y proxys de internet para proteger a SI de ataques exteriores;
- Protección contra código malintencionado a través de software de antivirus, detección de virus;
- Monitorización en tiempo real para enfrentar cualquier ataque externo a nuestro SI;
- Estudio de vulnerabilidad de nuestra SI que podría desencadenar la implantación de parches de seguridad;
- Implementación en los sitios de Gemalto de un plan de recuperación ante desastres para garantizar la disponibilidad de la SI.

B - Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) y Programa de Formación de Seguridad

Gemalto Group ha montado una organización centralizada a fin de reforzar la prevención y protección contra los riesgos de seguridad cibernética. Esta organización funciona de acuerdo con RFC2350 que especifica las expectativas de Respuesta a Incidentes de Seguridad Informática y tiene el apoyo de LEXSI, un CERT comercial.

El CSIRT de Gemalto está formado por varios expertos en defensa cibernética y respuesta a incidentes, que abarcan ciencia forense, investigaciones de red y pruebas de penetración. La mayor parte de nuestros expertos está certificada por: GIAC Forensics, EC-Couciel (CEH) en función de su ámbito de responsabilidades.

Cada usuario de la SI debe estar formado en las prácticas de seguridad de la información relevantes al uso que hacen de la información y sistemas de Gemalto. Se hace el seguimiento de las pruebas de conocimiento del usuario.

El Departamento de Recursos Humanos es responsable de la orientación de los nuevos empleados en cuanto a los principios básicos de la seguridad de la información. Los gerentes directos son responsables de informar a cada empleado, a través de programas de concientización, sobre la política de seguridad de la información, normas y procedimientos. Los administradores de IT son responsables de la formación técnica específica para cada trabajo del equipo de IT. El departamento de seguridad es responsable de la formación, certificación y seguimiento de las prácticas de seguridad de la información.

Lista 2: Formulario de procesamiento de datos

Esta lista proporciona la descripción del servicio que prestan las entidades legales mencionadas en este documento y que actúan como Procesadores de Datos, los tipos de datos que se van a procesar y los fines para los cuales dichos datos se procesan, y describe la duración del objetivo y los requisitos de retención obligatoria (si los hubiere).

Descripción de los servicios:

[PARA SER RELLENADO CON EL TIPO DE SERVICIO QUE SE PRESTARÁ]

Los clientes son:

[PARA SER RELLENADO CON LOS NOMBRES DE LOS CLIENTES]

Procesamiento de datos:

[PARA SER RELLENADO CON UNA DESCRIPCIÓN DEL PROCESAMIENTO LLEVADO A CABO POR CADA EMPRESA]

Desglose de los datos: [TABLA QUE DEBE RELLENARSE]

	Tipo de datos	Objetivo	Período de retención de datos
1.			
2.			
3.			
4.			
5.			

Ubicación de la Entidad de Hosting o Centro de Datos e identificación del Administrador del Sistema:

[PARA SER RELLENADO CON LA UBICACIÓN DEL EQUIPO DE PROCESAMIENTO, LO QUE INCLUYE LA UBICACIÓN DEL EQUIPO DE PROCESAMIENTO EMPLEADO PARA GENERAR UN RESULTADO ESTADÍSTICO]

Nombre y ubicación del Procesador Secundario que aporta los servicios de información para efectos de estadística y facturación.

[PARA SER RELLENADO CON LA UBICACIÓN DEL EQUIPO QUE APORTA LOS SERVICIOS DE INFORMACIÓN PARA PARA EFECTOS DE ESTADÍSTICA Y FACTURACIÓN.]

Nombre y ubicación del Procesador Secundario que aporta los servicios de asistencia

[PARA SER RELLENADO]

Entrega de los datos por parte del cliente:

[PARA SER RELLENADO CON UNA DESCRIPCIÓN DE LOS MEDIOS UTILIZADOS PARA ENTREGAR LOS DATOS A LOS PROCESADORES DE DATOS. POR EJEMPLO: El Cliente transmite los datos a través de un canal de comunicaciones cifradas a servidores seguros situados detrás del cortafuegos dedicado de la Entidad de Hosting/Centro de Datos.]

Lista 3: Términos de procesamiento de datos para los Servicios de Asistencia técnica

1. **Algunas definiciones**

Según se utilizan en el presente documento,

Sistema de gestión es la plataforma basada en la web de emisión de tickets conocida como STiM y que Gemalto utiliza en relación con el suministro del Servicio de Asistencia.

Apoyo remoto es el uso del teléfono, correo electrónico o una VPN para facilitar la resolución de una solicitud.

Solicitud es una petición de un cliente relacionada con el suministro del Servicio de Asistencia.

Registro de solicitudes es un registro en el sistema de gestión generado por Gemalto que anota las solicitudes y les da seguimiento.

Departamento de Servicio es el grupo de asistencia técnica de Gemalto que actúa como punto de contacto único entre Gemalto y el cliente a fin de administrar todas las solicitudes, comunicaciones y remisiones a instancias superiores con el Cliente.

Servicio de Asistencia es el objeto del servicio de asistencia de un acuerdo de nivel de servicio convenido.

VPN es una red privada virtual y proporciona un mecanismo de comunicación seguro para datos y otra información que se transmite entre dos puntos finales.

2. **Procesamiento de la información del Cliente**

En el momento de una solicitud, Gemalto está recolectando información del Cliente que está almacenada en el sistema de gestión ubicado en Francia. El objetivo de tal recolección es identificar el origen de la solicitud, asociar ésta con el Cliente, a fin de analizar, diagnosticar y resolver la Solicitud, y para efectos de facturación, mejoras de la Solución Interna y seguridad.

La información del Cliente se puede transferir al equipo de asistencia que suministra el Servicio de Asistencia, siempre que dicho equipo provoque una transferencia transfronteriza de datos sujeto a los términos de la sección 6 que aparece abajo.

3- **Apoyo remoto**

El Servicio de Asistencia se proporciona a través de un Departamento de Servicio (Nivel 1 de asistencia) ubicado en India, en SAFENET INFOTECH PVT LTD (una entidad legal miembro del grupo empresarial Gemalto). El Departamento de Servicio crea un registro de solicitud en el Sistema de Gestión y coordina la respuesta según el acuerdo de nivel de servicio convenido.

Si la solicitud debe remitirse al Nivel 2 de asistencia, la ubicación de los expertos a cargo del Nivel 2 de asistencia se encuentra en la Lista 2 del "Formulario de procesamiento" de DPT.

Si Gemalto tiene la opinión de que una Solicitud requiere una conexión remota a la Solución, se conectará a ella a través de una VPN segura.

La conexión remota a la Solución Interna está cubierta por los términos de seguridad estipulados en la Sección 4, más abajo.

Cuando esté conectado remotamente a la Solución, Gemalto tiene la capacidad de ver y usar los Datos de Servicio con el único propósito de proporcionar el Servicio de Asistencia. Gemalto no copia, modifica ni elimina los datos de servicio.

4- **Términos de seguridad**

4.1El Servicio de Asistencia sigue estos principios de seguridad:

- solamente se autoriza a las personas que necesitan acceso remoto;
- sólo se pueden realizar acciones autorizadas;
- el acceso a la Solución Interna se realiza a través de una interfaz confiable;
- se monitorizan las actividades sospechosas;
- se hace el seguimiento de las acciones para identificar roles y responsabilidades en caso de que haya investigaciones.

Más exactamente:

4.1.1 Aislamiento

Para aislar la Solución, Gemalto propone dos soluciones:

a) La primera se basa en un servidor de salto, que bloquea los accesos directos de los operadores de PC a la Solución Interna. Las operaciones sólo se pueden realizar desde el servidor de salto. Dado que el operador no tiene el derecho de administración de este servidor de salto, sólo puede utilizar software autorizado ya instalado en el servidor de salto;

b) La segunda solución se basa en una infraestructura dedicada. El operador tiene una PC dedicada sobre la cual dispone de derechos limitados. Hay software específico preinstalado en este equipo para realizar el mantenimiento y las operaciones de asistencia. Hay un servidor de archivos disponible para la transferencia de archivos de bitácora. También hay un antivirus instalado en este PC dedicado a fin de evitar cualquier infección.

El objetivo de estas dos soluciones es limitar tanto como sea posible el uso de aplicaciones inadecuadas y la transferencia de archivos dispuestos entre la Solución y el equipo de asistencia.

El segundo aspecto de este aislamiento se relaciona con el portador entre las infraestructuras. El canal de comunicación también tiene que protegerse. Para estas dos soluciones, el uso de una VPN es obligatorio a fin de proteger el vínculo entre la Solución y el equipo de asistencia.

4.1.2 Autenticación

El segundo aspecto importante es la capacidad de autenticar al operador. Esta autenticación debe ser lo suficientemente fuerte como para evitar una usurpación de identidades y para ser inaplicable en el caso de procedimientos legales.

Gemalto ha implementado su propio sistema basado en su sistema de autenticación de dos factores de forma. Se concede el acceso a la PC dedicada o al servidor de salto con la insignia personal del empleado. Esta insignia es única e incrusta una clave privada que se utiliza para esta autenticación.

Para tener acceso a estos sistemas, el operador debe presentar su insignia y el PIN asociado. La insignia combinada con un LDAP (Lightweight Directory Access Protocol) central proporciona varias ventajas. La primera de ellas consiste en validar la insignia en sí misma. La segunda es permitir una gestión de grupo. Con base en la autenticación LDAP, el sistema valida los accesos de los derechos del operador al servidor de salto y a la Solución Interna. El último punto es la facilidad de la gestión de accesos. La gestión de accesos y revocaciones de los recién llegados en el sistema central. Gracias a este método de autenticación fuerte, Gemalto garantiza que sólo las personas que se requiera tengan acceso a la Solución. Más aún, basándose en las definiciones de roles y de grupos, los derechos de acceso se limitan a la prestación del Servicio de Asistencia.

4.1.3 Auditabilidad

Además, con esta autenticación fuerte, se hace factible la capacidad de conseguir una detección de comportamientos sospechosos en tiempo real o realizar más análisis en caso de incidentes.

La detección en tiempo real se basa en detectores de seguridad a cargo del envío de alertas de seguridad. Estas alertas disparan un proceso interno a cargo de definir la importancia de la detección y para poner en marcha las acciones de contención correspondientes.

Los sistemas de bitácora registran las acciones realizadas por los operadores. Gracias al sistema de autenticación fuerte, las bitácoras asocian al dueño y a las acciones.

Debido a la confidencialidad de ciertos datos, las bitácoras están higienizadas. Estas bitácoras se almacenan en un espacio seguro y sólo los oficiales de seguridad pueden tener acceso a ellas.

Estos sistemas combinados permiten que Gemalto detecte los casos de alertas de seguridad y reaccione a ellos.

5- **Transferencia transfronteriza**

5.1 Como se indica en la Sección 3 anterior, la prestación del Servicio de Asistencia puede crear una transferencia transfronteriza de la información o Datos de Asistencia del Cliente; el Cliente entiende que tal traslado transfronterizo de su información o datos de asistencia puede estar sujeto a requisitos específicos impuestos por la Ley de Protección de Datos Personales aplicable donde la carga de tales requisitos específicos la tiene el Cliente al ser la entidad que pone a disposición de Gemalto la información o datos de asistencia del Cliente.

5.2 En caso de que tal traslado transfronterizo de la información o Datos de Asistencia del Cliente pudiera requerir la celebración de un acuerdo específico de transferencia transfronteriza a la luz de la Ley de Protección de Datos Personales aplicable. Gemalto y el Cliente colaborarán con el fin de cumplir con este requisito.