

## Manual para protección de datos

Fecha	03 de mayo de 2018
Autor	MKM / FLO
Revisor	CPF
Versión	2.2

### Índice de materias

<b>1</b>	<b>Introducción</b> .....	<b>2</b>
<b>2</b>	<b>Definiciones</b> .....	<b>3</b>
<b>3</b>	<b>Exigencias reglamentarias</b> .....	<b>3</b>
<b>4</b>	<b>Funcionalidades y características de SecuTix 360°</b> .....	<b>5</b>
4.1	Legitimidad de la finalidad y licitud del tratamiento de los datos.....	5
4.2	Lealtad y transparencia de la recogida y del tratamiento de datos .....	6
4.3	Pertinencia, adecuación y estricta necesidad de los datos .....	7
4.4	Utilización de cookies en la interfaz o el módulo web .....	13
4.5	Duración de conservación de los datos.....	17
4.6	Datos exactos y actualizados. Derechos de acceso, de rectificación, de supresión y de portabilidad. Derecho a la limitación del tratamiento y derecho de oposición al tratamiento. ....	18
4.7	Seguridad de los datos.....	21
4.8	Encargados del tratamiento, encargados de tratamientos adicionales y flujos transfronterizos .....	23
4.9	Utilización de datos con fines de marketing.....	24
4.10	Procedimientos .....	27
	<b>Anexo 1. Lista de verificación a completar por su organismo que afecta a los tratamientos de datos personales aplicados en la solución SecuTix 360°</b> .....	<b>28</b>
	<b>Anexo 2. Lista de los encargados de tratamiento posteriores de SecuTix SA</b> .....	<b>30</b>

## 1 Introducción

Como organismo que utiliza la solución SecuTix 360°, usted recoge y trata, en calidad de responsable de tratamiento, datos personales que afectan especialmente a sus clientes compradores de billetes, sus clientes potenciales, sus operadores... Estos datos pueden también ser transmitidos o tratados por SecuTix SA, en calidad de encargado de tratamiento, para las necesidades de suministro y de las prestaciones o servicios que ha suscrito con nosotros.

En el ámbito de la recogida, del tratamiento y de la transmisión de estos datos personales, debe respetar la reglamentación aplicable en materia de protección de datos personales. El respeto a las exigencias que le son aplicables en materia de protección de datos es, en su calidad de responsable de tratamiento, de su exclusiva responsabilidad.

En Unión Europea (UE), la reglamentación aplicable proviene de un reglamento europeo, el reglamento europeo 2016/679 de 27 de abril de 2016 relativo a la protección de datos personales físicos ante el tratamiento de datos personales (llamado «RGPD»), aplicable directamente en todos los países miembros de la UE a partir del 25 de mayo de 2018.

SecuTix SA está sometido a la legislación suiza de protección de datos (ver cuadro a continuación). Esta legislación es muy similar, en ciertos aspectos idéntica, a la de los países de la Unión Europea (UE). Por decisión de la Comisión Europea (decisión de la Comisión 2000/518 CE de 26/07/2000), Suiza ya ha sido reconocida como garante de un nivel adecuado de protección de los datos personales transferidos desde la UE.

También, SecuTix SA pone a su disposición una solución que le permite respetar las exigencias europeas en la materia. A continuación, le mostramos, sin pretensión de exhaustividad, las posibilidades técnicas y organizacionales ofrecidas por SecuTix 360° con este fin.

### **Precisiones preliminares**

A título preliminar, se precisa que:

- el presente pliego de protección de datos tiene únicamente vocación de presentarle las funcionalidades ofrecidas por la solución SecuTix 360° desde una óptica de sensibilización y de información tratándose de precauciones tomadas por nosotros para permitirle respetar ciertas exigencias legales o reglamentarias que podrían serle aplicables en su calidad de responsable de tratamiento;
- este documento no constituye en ninguna medida instrucciones a su atención o consejos con vocación jurídica;
- la determinación de los fines y los medios del tratamiento depende de sus exclusivas decisiones y de su única responsabilidad, sus instrucciones deben sernos transmitidas mediante la lista de verificación que figura en el Anexo 1.

## 2 Definiciones

**Datos personales:** toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social (sinónimo en el presente documento «datos personales»);

**Tratamiento:** cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

**Responsable del tratamiento:** la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros (sinónimo en el presente documento «usted», «su organismo»);

**Encargado del tratamiento:** la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento (sinónimo en el presente documento «nosotros», «SecuTix SA»);

**Persona interesada:** persona física cuyos datos personales son objeto de un tratamiento en la utilización de la solución SecuTix 360°;

**Violación de la seguridad de los datos personales:** toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

## 3 Exigencias reglamentarias

La reglamentación europea impone a todo responsable del tratamiento el respeto a los siguientes principios:

- la recogida y el tratamiento de los datos deben responder a los principios de licitud, lealtad y transparencia;
- la finalidad del tratamiento de los datos debe ser determinada, explícita y legítima. Los datos personales no deben ser tratados posteriormente de forma incompatible con este fin;
- los datos recogidos y tratados deben ser adecuados, pertinentes y limitados a lo que es necesario ante los fines perseguidos. Deben ser exactos y actualizados. Los datos considerados sensibles solo pueden ser recogidos y tratados bajo ciertas condiciones, especialmente con el consentimiento de las personas interesadas;
- la duración de conservación de los datos no debe ser excesiva, si no, al contrario, estrictamente proporcionada al (o a los) fin(es) perseguido(s);

- las personas interesadas deben ser informadas del tratamiento de sus datos personales, y, llegado el caso, su consentimiento debe ser registrado para ciertos tratamientos. La información que poner en conocimiento de dichas personas interesadas debe contener un cierto nombre de mencione obligatorias;
- las personas interesadas deben tener garantizado un derecho de acceso, de rectificación, de supresión y de portabilidad de sus datos, así como un derecho a la limitación y un derecho de oposición al tratamiento de dichos datos. Tienen derecho asimismo a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.
- medidas técnicas y organizacionales deben desplegarse para garantizar la seguridad de los datos, y especialmente su protección ante todo acceso o toda destrucción, alteración o difusión no autorizadas de dichos datos (un análisis de impacto es en ciertas hipótesis necesario para evaluar las medidas adecuadas a desplegar, de lo que puede resultar una obligación de consulta de la autoridad de control competente). Las violaciones de datos personales deben ser objeto de un proceso específico de notificación ante la autoridad de control competente, incluso de una información sobre las personas interesadas en ciertas hipótesis;
- el recurso a los encargados de tratamiento y a encargados de tratamiento posteriores para el tratamiento de los datos personales debe ser objeto de un marco contractual específico (cf. cláusulas obligatorias);
- los flujos transfronterizos de datos hacia Estados no miembros de la UE y no reconocidos como garantes de un nivel de protección adecuado de los datos pueden ser aplicados bajo reserva de garantías suficientes, especialmente contractuales;
- todo organismo que recoge y trata datos personales debe elaborar y mantener actualizado:
  - un registro de sus actividades de tratamiento de datos personales aplicados en calidad de responsable del tratamiento;
  - un registro de sus actividades de tratamiento de datos personales aplicados en calidad de encargado del tratamiento.

**Enfoque - los principios y compromisos sobre la protección de datos en Suiza (Ley federal sobre la protección de datos):**

Todo tratamiento de datos debe ser lícito. Su tratamiento debe ser efectuado conforme a los principios de la buena fe y de la proporcionalidad. Los datos personales solo deben ser tratados con el objetivo que se indica durante su recogida, que está previsto por una ley o que proviene de las circunstancias. La recogida de datos personales, y en particular los fines del tratamiento, deben ser reconocibles por la persona interesada. Cuando se requiere su consentimiento para justificar el tratamiento de datos personales que le afectan, la persona interesada solo consiente legítimamente si expresa su voluntad libremente y después de haber sido debidamente informada. Cuando se trata de datos sensibles y de perfiles de la personalidad, su consentimiento deber ser, además, explícito. Los datos personales deben ser protegidos contra todo tratamiento no autorizado por medidas organizacionales y técnicas apropiadas.

## 4 Funcionalidades y características de SecuTix 360°

Este párrafo 4 describe:

- las exigencias y obligaciones que respetar, tales como se recuerdan en el párrafo 3 anterior;
- las funcionalidades y características de la solución SecuTix 360° le ofrecen la posibilidad de ajustarse a ellas.

### 4.1 Legitimidad de la finalidad y licitud del tratamiento de los datos

#### 4.1.1 Principios

Corresponde al responsable del tratamiento asegurarse de:

- que los datos son efectivamente recogidos para fines determinados, explícitos y legítimos, y no son tratados posteriormente de una forma incompatible con estos fines (cf. principio de finalidad);
- del carácter lícito de la recogida y del tratamiento de los datos en la solución SecuTix 360° (cf. principio de licitud).

Como recordatorio, el tratamiento de datos personales solo será lícito si se cumple al menos una de las siguientes condiciones:

- el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
- el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
- el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
- el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
- el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
- el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

#### 4.1.2 La solución SecuTix 360°

La solución informática SecuTix 360° ofrece las funcionalidades siguientes:

- gestión de entradas: configuración, planificación, reserva, venta, emisión, impresión, control de accesos, gestión de operadores...

- gestión de relaciones de contacto (clientes y clientes potenciales): campañas de marketing, operaciones de prospección y de solicitud, operaciones técnicas asociadas: selección, segmentación, mejora de datos, identificación, buzoneo electrónico, análisis y seguimiento (navegación web y buzoneo electrónico), informes (estadísticas y prestaciones)
- gestión de eventos: organización, planificación, conferenciantes/guías...
- gestión de tiendas y de ventas: inventario/compra/gestión de proveedores

Como responsable de tratamiento de datos, ha elegido la solución SecuTix 360° como el medio según usted más adecuado para realizar el tratamiento de datos personales cuyo fin, determinado por usted, le es propio. Le corresponde asegurar que se respetan los principios citados anteriormente de finalidad y de licitud.

## 4.2 Lealtad y transparencia de la recogida y del tratamiento de datos

### 4.2.1 Principios

Los interesados deben ser informados por el responsable de tratamiento de los tratamientos aplicados que afectan a sus datos personales (cf. principio de lealtad y de transparencia), conforme a las disposiciones aplicables en materia de protección de datos personales. Deben, asimismo, en ciertos casos, haber consentido (cf. párrafos 3.1, 4.3 y 4.9 especialmente).

Además, una mención de información debe figurar sobre todo formulario de recogida de datos.

### 4.2.2 La solución SecuTix 360°

En su calidad de responsable de tratamiento, le corresponde informar a los interesados como los citados anteriormente, incluso recoger su consentimiento. Por supuesto, nosotros nos ponemos a su disposición para proporcionarle bajo demanda las informaciones en nuestra posesión que le serán útiles a este fin.

Además, para permitirle respetar sus obligaciones en este sentido, le informamos que:

- SecuTix 360° integra en su interfaz web un apartado titulado «Carta de confidencialidad», accesible desde todas las páginas web, y que reenvía por un enlace hipertexto hacia una página que puede contener su carta o política de protección de datos, esta carta o política debe ser elaborada por su organismo:

© 2018 SECUTIX | CREADO POR SECUTIX | CONDICIONES GENERALES | POLÍTICAS DE PRIVACIDAD | PREGUNTAS FRECUENTES

- si utiliza nuestro módulo web integrado en su sitio web, le convendrá integrar en su sitio web dicho apartado;
- todos los formularios de recogida de datos en línea que figuran en nuestra interfaz web y en nuestro módulo web (si está integrado en su sitio web) incluyen un recuadro que les permite integrar su mención de información confidencial (cuya redacción y alojamiento le pertenecen), una casilla de verificación a marcar para recoger el consentimiento, y un enlace hacia la Carta de confidencialidad (cuya redacción y alojamiento le pertenecen). Estos dos enlaces se han completado mediante los parámetros de los puntos de venta en internet.

Además, le recordamos que las personas que reservan por otro medio diferente a una reserva web deben asimismo ser informados. Por lo tanto, conviene que se asegure de que para cada modo de recogida de datos se despliega un proceso de información conforme a las disposiciones aplicables en materia de protección de datos (por ejemplo, en el guion de los operadores o en un servidor vocal interactivo en caso de recogida de datos por teléfono, por visualización en caso de recogida de datos en la taquilla, etc.).

En cualquier caso, todas las personas interesadas (diferentes tipos de contactos, operadores, proveedores, clientes potenciales... cuyos datos podrían figurar en la solución SecuTix 360°) deberán ser informados por su organismo, y no únicamente las personas que proceden a realizar una reserva. También, le corresponde asegurarse y desplegar los procedimientos en este sentido.

## **4.3 Pertinencia, adecuación y estricta necesidad de los datos**

### **4.3.1 Principios**

Los datos recogidos y tratados deben ser adecuados, pertinentes y limitados a lo que es necesario ante los fines perseguidos (cf. principio de minimización de los datos recogidos).

Se trata de solo recoger y tratar los datos necesarios para el fin del tratamiento (por ejemplo, para la reserva de billetes, la atribución de plazas, el pago del pedido...). La recogida de datos no indispensables para el fin del tratamiento debe ser facultativa para la persona interesada, habiéndose precisado que toda recogida de datos sin relación con el fin del tratamiento está estrictamente prohibida.

Además, un cierto número de datos particularmente sensibles no deben recogerse. Efectivamente, por principio se prohíben la recogida y el tratamiento de los datos siguientes:

- los datos llamados «particulares», que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como los datos genéticos, datos biométricos, los datos relativos a la salud o los datos relativos a la vida sexual o la orientación sexual de una persona física;
- las informaciones relativas a infracciones, condenas o medidas de seguridad asociadas (por ejemplo, «prohibición de acceso a los estadios»).

Hay excepciones a estas prohibiciones. Como ejemplo, los datos llamados «particulares» pueden ser tratados si son necesarios para el tratamiento en las hipótesis siguientes:

- consentimiento del interesado;
- tratamiento efectuado por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro y con un fin político, filosófico, religioso o sindical (bajo ciertas condiciones);
- datos manifiestamente hechos públicos por el interesado.

Sin embargo, estas excepciones deben interpretarse de forma estricta.

Estos principios se aplican sean cuales sean las modalidades de recogida, de introducción y de tratamiento de la información por las herramientas. Los campos de comentarios libres deben ser especialmente utilizados con prudencia.

#### 4.3.2 La solución SecuTix 360°

En su calidad de responsable de tratamiento, le corresponde asegurarse del respeto a estos principios de minimización de datos y de prohibición de recogida de ciertos datos.

La solución SecuTix 360° le ofrece campos de recogida de datos por defecto, tanto en el back-office como en la interfaz o módulo web puesto a su disposición. Estos campos son limitados en una óptica de minimización de datos. Sin embargo, se recuerda que:

- no se trata de campos proporcionados por defecto que usted pueda ajustar (bajo reserva de ciertos campos estrictamente obligatorios para el buen funcionamiento de la solución pero que son muy limitados; a título de ejemplo, los únicos datos estrictamente obligatorios en la solución tratándose de contactos son los datos siguientes: tratamiento, apellidos y nombre). Como responsable de tratamiento, le corresponde la determinación de los campos a utilizar e incluso a añadir, según los elementos que le pedimos que complete en el Anexo 1 para indicarnos sus instrucciones en este sentido:
- es lo mismo tratándose de la definición de datos llamados «calculados» en el ámbito de las funcionalidades de segmentación, por ejemplo, que puede elegir especificar en el Anexo 1.

A este respecto, si la solución SecuTix 360° le da acceso a funcionalidades de segmentación y eventualmente de perfilado, usted es la única persona con poder de decisión (y por tanto el único responsable) de los segmentos que desea utilizar, los fines perseguidos, la pertinencia, la adecuación y el carácter necesario de los datos tratados en este contexto, de las decisiones que eventualmente debería tomar con respecto a estos segmentos y de las consecuencias que pueden producirse para las personas interesadas.

También se recuerda que la toma de decisiones individuales automatizadas mediante, por ejemplo, funcionalidades de segmentación o incluso de perfilado puede ser sometida a precauciones particulares que debe respetar (consentimiento, intervención humana, posibilidad de impugnar la decisión...);

- las mismas reglas y principios son aplicables a la elección y a la utilización de criterios de informes o de extracciones a partir de las funcionalidades de la solución. Además, teniendo en cuenta los riesgos para los datos, relacionados con la volatilidad de los informes o extracciones una vez realizados, se recomienda aplicar una política de habilitaciones que solo autorice a las personas que tienen estrictamente interés en poder proceder a las extracciones (a precisar en el Anexo 1).

La solución SecuTix 360° le ofrece, entre otros, centenares de funcionalidades destinadas a permitirle respetar los principios aplicables tratándose de los datos recogidos. A modo de ejemplo:

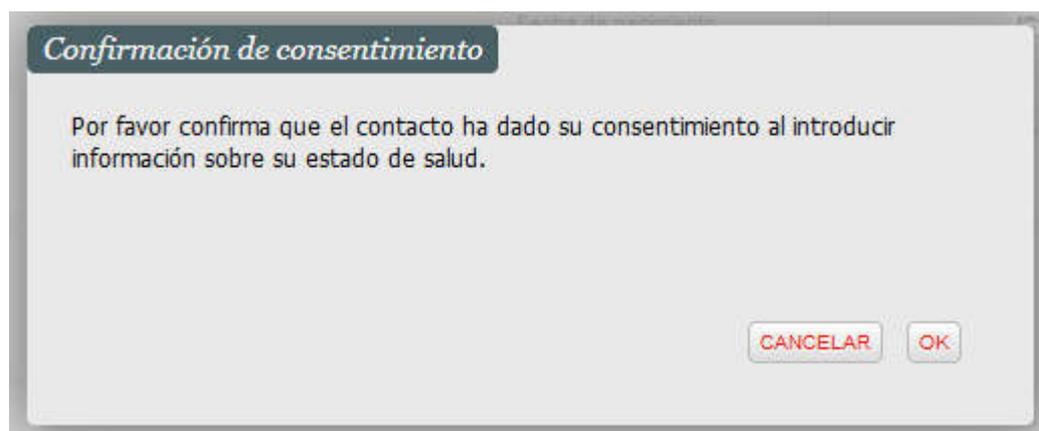
- el valor por defecto para una discapacidad es «ninguna discapacidad». Asimismo, este campo se presenta en forma de menú desplegable que limita las

opciones del operador durante la introducción de la información para limitar el riesgo de que se recojan datos no estrictamente necesarios.

Para registrar otro valor, el operador de su organismo debe confirmar que ha solicitado el consentimiento al contacto marcando una casilla de verificación de la forma siguiente:



The image shows a dropdown menu for the field 'Tipo de minusvalía'. The menu is open, showing the following options: 'Sin minusvalía', 'Seleccionar...', 'Sin minusvalía', 'Asientos en el extremo fila', 'Estar cerca del escenario', 'Silla de ruedas', and 'Sin silla de ruedas'. The 'Sin minusvalía' option is currently selected.



The image shows a dialog box titled 'Confirmación de consentimiento'. The text inside reads: 'Por favor confirma que el contacto ha dado su consentimiento al introducir información sobre su estado de salud.' At the bottom right, there are two buttons: 'CANCELAR' and 'OK'.

- para registrar una fotografía, el operador de su organismo debe confirmar que ha solicitado el consentimiento al contacto marcando una casilla de la forma siguiente:



The image shows a dialog box titled 'Subiendo la imagen del contacto'. The text inside reads: 'Confirma que tienes el consentimiento del contacto antes de subir la imagen del contacto'. At the bottom, there are two buttons: 'SÍ' and 'NO'.

Le corresponde también prever la recogida de este consentimiento (en su Carta de confidencialidad) cuando elija permitir a los internautas cargar su fotografía en línea (cf. vía interfaz o módulo web).

- los datos de tarjeta de pago no son accesibles «en abierto» para los operadores en la solución SecuTix 360°. Sin embargo, pueden conservarse de manera cifrada y segura, después de una compra efectuada por un contacto, con el consentimiento de este último, por ejemplo, con vistas a la realización de compras posteriores (excepto CVV / criptograma). Por defecto, esta funcionalidad de conservación de información de tarjeta de pago está desactivada. La activación de esta funcionalidad requiere el consentimiento del interesado, tanto:
  - mediante una casilla para marcar por el interesado en la interfaz o el módulo web (no premarcada);
  - mediante una casilla para marcar en el back-office de la solución (no premarcada y con mención de la obligación de solicitar el consentimiento explícito del contacto).
  
- en lo que concierne a las zonas de comentarios libres que figuran en la solución, en el momento de introducir los datos el operador de su organismo debe marcar una casilla para confirmar que el comentario es conforme a las disposiciones aplicables en materia de protección de datos personales. Además, un enlace proporciona información suplementaria al operador si desea más información, como sigue:

GUARDAR Y CERRAR

### Nota > Nuevo

**Nota**

**Título \***

**Contenido**

Confirmando que el comentario cumple con las leyes y reglamentos relativos a la protección de datos. Encontrará recomendaciones [aquí](#)

### Recomendaciones para la introducción de notas

#### Los datos introducidos en los campos de comentarios deben:

- Ser relevantes, adecuados y no excesivos con relación al contexto de tratamiento informático en el que se han recogido ;
- Ser objetivos, no pueden resultar de un juicio de valor o de la apreciación de un comportamiento por parte de los interesados ;
- No destacar, directamente o indirectamente, el origen racial, las opiniones políticas, religiosas o filosóficas, afiliaciones sindicales o morales ;
- Prohibir todas las expresiones que podrían ser consideradas como relativas a datos prohibidos por la ley o como ofensivas, despectivas o perjudiciales para la reputación, la consideración o la vida privada de las personas

CERRAR

- en lo que concierne a las zonas de comentarios libres de la interfaz o módulo web ofrecidos durante la finalización de los pedidos/reservas/opciones, le corresponde sensibilizar a los operadores e instaurar los procesos necesarios para la moderación de estos comentarios. Además, se ha introducido una mención de advertencia simplificada a la atención de los contactos con el texto por defecto:

*«Los datos introducidos en esta zona de comentarios solo deber tener como objetivo precisar los elementos estrictamente necesarios para transmitir y/o ejecutar su pedido. Además, le recordamos que la información que puede comunicar vía esta zona de texto libre está sometida a disposiciones aplicables en materia de protección de datos personales, que se compromete a respetar (datos lícitos, objetivos, pertinentes, adecuados y limitados a lo necesario respecto al fin perseguido, lealtad de la recogida y del tratamiento de los datos, etc.).»*

- las pantallas de la solución permitirán realizar informes o extracciones que incluyan una mención de advertencia a la atención de los usuarios de la solución, como sigue:

*«Realizando una exportación de estos datos, debe asegurarse de que actúa respetando los principios aplicables en materia de protección de datos personales. Debe asegurarse especialmente de que el fichero que va a ser creado será utilizado únicamente como prolongación del tratamiento inicial y, en particular, para los mismos fines que se perseguían en el uso de la presente aplicación. Asimismo, debe asegurarse de que los datos extraídos son pertinentes, adecuados y estrictamente necesarios para el fin para el que pretende utilizarlos y solo los comunicará a las personas autorizadas. Le corresponde velar para tomar todas las medidas destinadas a asegurar la seguridad de los datos, y especialmente su confidencialidad. El fichero de exportación debe ser conservado solo con la duración prevista para los datos tratados al ejecutar la presente aplicación.»*

## **4.4 Utilización de cookies en la interfaz o el módulo web**

### **4.4.1 Principios**

SecuTix 360° permite analizar el comportamiento de los internautas mediante la solución Google Analytics. Esta funcionalidad de medición de audiencia y de estadísticas de visitas y de navegación puede ser utilizada por su organismo o por SecuTix SA con el objetivo de mejorar el servicio.

El internauta debe ser informado de la utilización de las cookies de Google Analytics y consentir su obtención y su explotación.

Para ello, el internauta que accede a un sitio web (página de inicio o página secundaria) debe ser informado mediante un banner:

- de los fines precisos de las cookies utilizadas;
- de la posibilidad de oponerse a estas cookies y de cambiar los parámetros haciendo clic en un enlace presente en el banner (este enlace debe reenviar a una política de «cookies» que presente a los internautas de manera simple e inteligible soluciones puestas a su disposición para aceptar o rechazar todas o una parte de las cookies);
- del hecho que la continuación de su navegación es acorde al guardado de cookies en su terminal.

En la medida en que el consentimiento no debe ser ambiguo, este banner no debe desaparecer mientras la persona no ha continuado su navegación, es decir, mientras no ha ido a otra página del sitio web o no ha hecho clic sobre un elemento del sitio (imagen, enlace, botón «buscar»).

Así, salvo consentimiento previo del internauta, el guardado y la lectura de cookies sometidas al consentimiento no deben efectuarse:

- si el internauta va al sitio web y no continúa su navegación: una simple ausencia de acción no se considerará una manifestación de voluntad;
- si hace clic en el enlace presente en el banner que le permite definir los parámetros de las cookies y, en su caso, rechazar el guardado de cookies.

Finalmente, las personas que hayan dado su consentimiento para el guardado o la lectura de las cookies deben estar en condiciones de retirarlo en todo momento. En caso de consentimiento del interesado, se le debe volver a pedir el consentimiento en cualquier caso después de un plazo de 13 meses (cf. duración de vida máxima de las cookies).

Para información, existe una excepción a la necesidad de pedir el consentimiento para las cookies de medición de audiencia si se cumplen las condiciones siguientes:

- el internauta está informado (cf. banner);
- dispone de la facultad de oposición mediante un mecanismo de oposición fácilmente utilizable en el conjunto de los terminales, de los sistemas de explotación, de las aplicaciones y de los navegadores de internet; ninguna información relativa a las personas que hayan decidido ejercer su derecho de oposición debe recogerse ni transmitirse al editor de la herramienta de análisis de visitas;
- el fin del dispositivo debe ser limitado a la medición de audiencia del contenido visualizado para permitir una evaluación de los contenidos publicados y de la ergonomía del sitio o de la aplicación;
- los datos recogidos no deben recuperarse mediante otros tratamientos (ficheros clientes o estadísticas de visitas de otros sitios, por ejemplo); la utilización de la cookie aceptada debe ser estrictamente limitada a la producción de estadísticas anónimas; su alcance debe limitarse a un solo editor y no debe permitir el seguimiento de la navegación de la persona que utilice diferentes aplicaciones o que navegue por diferentes sitios web;
- la utilización de la dirección IP para geolocalizar al internauta no debe proporcionar una información más precisa que la población; esta dirección IP también debe ser suprimida o anonimizada cuando se haya efectuado la geolocalización, para evitar cualquier otra utilización de este dato o cualquier cotejo con otras informaciones personales;
- tratándose de cookies, no deben tener una duración que supere los trece meses y esta duración no debe ser prorrogada automáticamente durante nuevas visitas; la información recogida por el intermediario de las cookies debe ser conservada durante una duración de trece meses máximo.

#### **4.4.2 La solución SecuTix 360°**

En su calidad de editor del sitio web (tanto si utiliza nuestra interfaz web o nuestro módulo web integrado en su propio sitio web), le corresponde informar y recoger el consentimiento de los internautas en vistas al depósito y la lectura de las cookies.

A este respecto, le informamos que:

- bajo demanda nuestro servicio encargado del soporte, nuestra interfaz y nuestro módulo web le ofrecen la visualización de un banner de información y de recogida del consentimiento para la instalación de cookies durante la primera visita de un internauta. La formulación de la información para comunicar a los internautas mediante este banner es su responsabilidad. A los efectos oportunos le ofrecemos la formulación siguiente, a su cargo está modificarla o ajustarla en función de las especificidades eventualmente ligadas a su propio sitio web:

Continuando su navegación en este sitio, acepta la utilización de cookies o tecnologías similares que tengan como fin la realización de estadísticas de visitas a nuestro sitio (tests y medidas de audiencia, de visitas, de navegación, de rendimiento), pero también **[a completar en su caso con otros fines en función de su interfaz web]**.

Para saber más y definir los parámetros de sus opciones en materia de cookies y otras tecnologías similares, haga clic aquí [insertar un enlace hacia la política de cookies].

Este banner debe implementarse tanto si utiliza nuestra interfaz web como nuestro módulo web integrado en su sitio web. Este banner debe implementarse en la primera página a la que llega el internauta, incluso si se trata de una página secundaria y no de la página de inicio;

- La redacción de la «política de cookies» es responsabilidad suya. Sin embargo, le informamos que las cookies que utilizamos en el ámbito de su interfaz web son las siguientes:

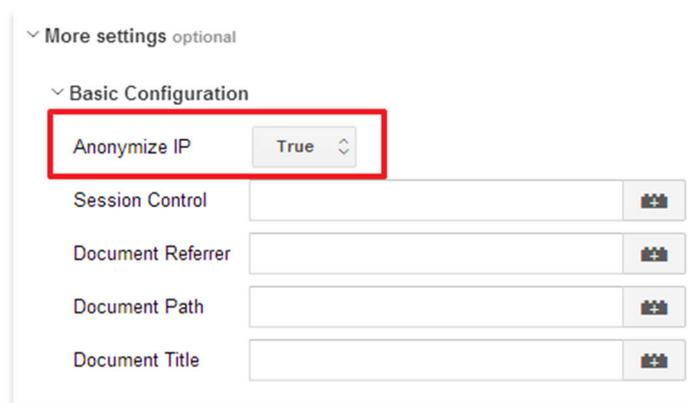
Tipo	Nombre	Editor	Fines	Duración
<b>Cookie permanente de estadística y de seguimiento de medición de audiencia y de visitas</b>	_ga	Google Inc. (Google Analytics)	Si Google Analytics está activado, estas cookies se aplican a la base de informaciones recogidas durante la navegación del usuario, especialmente la dirección url desde la cual el usuario ha accedido al sitio web, el proveedor de acceso a internet del usuario, el tipo, la configuración y la configuración del navegador... Estas cookies se utilizan para distinguir los visitantes únicos en un sitio web atribuyendo un número generados de forma aleatoria como un nombre de usuario. Este último se actualiza en cada página visitada y permite especialmente calcular el número de visitantes, de sesiones...  Más información: <a href="https://support.google.com/analytics/answer/6004245">https://support.google.com/analytics/answer/6004245</a> Módulo de desactivación de Google Analytics: <a href="https://support.google.com/analytics/answer/181881?hl=fr&amp;ref_topic=2919631">https://support.google.com/analytics/answer/181881?hl=fr&amp;ref_topic=2919631</a> . o <a href="https://tools.google.com/dlpage/gaoptout">https://tools.google.com/dlpage/gaoptout</a> .	En función de los parámetros elegidos por el cliente
<b>Cookie limitada a la sesión</b>	Idioma		Esta cookie permite recordar la elección de la lengua del contacto.	Sesión
<b>Cookie de sesión con objetivo técnico</b>	SESIÓN		Identificador técnico de la sesión	Sesión
<b>Cookie limitada a la sesión con</b>	BIGipServer_XXX		Esta cookie permite dirigir el contacto hacia la misma máquina para obtener opciones de almacenamiento en caché.	Sesión

<b>objetivo técnico</b>				
<b>Cookie limitada a la sesión con objetivo técnico</b>	AcpAT_XXX		Esta cookie permite validar que el contacto haya pasado por PeakProtect (herramienta de gestión de fuertes afluencias)	Sesión

Estos elementos de información deberán ser insertados por usted en su política de cookies.

Esta política de cookies debe implementarse tanto si utiliza nuestra interfaz web como nuestro módulo web integrado en su sitio web;

- por principio, conviene que las cookies no se instalen mientras el internauta no haya continuado su navegación y el banner debe reaparecer después de un período de 13 meses desde la obtención del consentimiento para las cookies. Es esta configuración la que se ofrece por defecto en las interfaces web puestas a disposición por SecuTix SA tras una demanda de servicio de su parte en este sentido. Conviene que asegure el respeto de esta obligación tanto en su propio sitio web como si utiliza nuestro módulo integrado en su sitio web;
- si desea eludir esta obligación de consentimiento (para que las cookies se puedan instalar desde la página de inicio), conviene definir los parámetros de las cookies según los principios recordados anteriormente que afectan a las cookies de medición de audiencia no sometidas a consentimiento. Especialmente (pero no exclusivamente) conviene que un operador de su organismo configure Google Analytics para anonimizar las direcciones IP antes de enviar datos a Google en Estados Unidos para que ninguna valoración personal sea posible:



Las demás obligaciones necesarias para esta excepción al consentimiento también deberán ser respetadas.

Atención, esta excepción al consentimiento solo es válida para las cookies de medición de audiencia: la utilización de cookies diferentes a las cookies publicitarias está sometida a un consentimiento previo del internauta.

## 4.5 Duración de conservación de los datos

### 4.5.1 Principios

Las disposiciones en materia de protección de datos personales imponen al responsable de tratamiento que solo conserve los datos durante un período adecuado para los fines perseguidos. En cambio, no dan indicaciones sobre la duración exacta de conservación. El almacenaje ilimitado de los datos personales no está autorizado en ningún caso.

### 4.5.2 La solución SecuTix 360°

En su calidad de responsable de tratamiento, le corresponde determinar y hacer aplicar una duración máxima de conservación de los datos en las herramientas que utilice para el tratamiento de datos personales, especialmente en la solución SecuTix 360°. Esta duración de conservación máxima afecta a los datos del conjunto de personas interesadas cuyos datos son recogidos y tratados en la solución SecuTix 360°.

La solución SecuTix 360° ofrece diversas funcionalidades en vista a la supresión de los datos por usted:

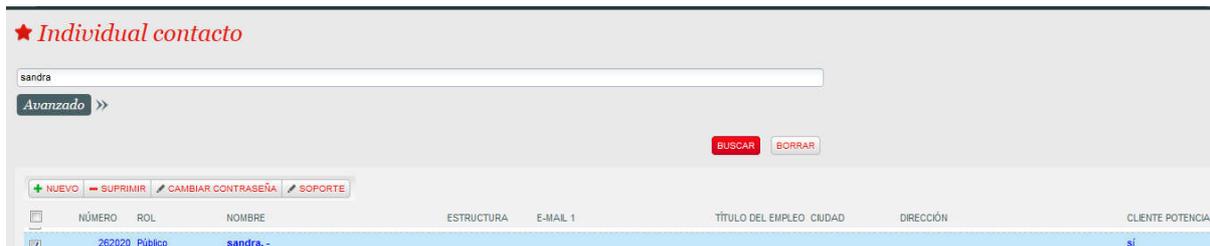
- los contactos que disponen de una cuenta personal en línea tienen la posibilidad de suprimir sus datos desde esta cuenta:

#### Eliminación de la cuenta

Si decides eliminar tu cuenta, no podrás realizar ninguna reclamación en caso de pérdida o no recepción de tus entradas.

#### Eliminar mi cuenta

- los operadores de su organismo tienen la posibilidad de suprimir contactos:



★ *Individual contacto*

sandra

Avanzado >>

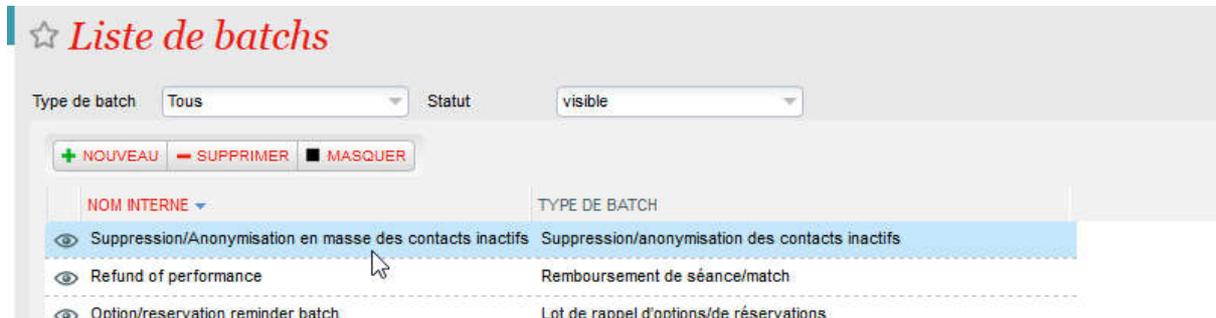
BUSCAR BORRAR

+ NUEVO - SUPRIMIR CAMBIAR CONTRASEÑA SOPORTE

	NÚMERO	ROL	NOMBRE	ESTRUCTURA	E-MAIL	TÍTULO DEL EMPLEO	CIUDAD	DIRECCIÓN	CLIENTE POTENCIAL
<input checked="" type="checkbox"/>	262020	Público	sandra, -						sí

- en estos dos casos, la cuenta del contacto se ha suprimido, la información de marketing (historial e indicadores) se ha suprimido y todos los pedidos se convierten en anónimos. La anonimización de los datos se convierte en irreversible durante la supresión de los registros, es decir, después de un plazo de 12 meses (cf. duración de conservación de los registros);
- los operadores de su organismo tienen la posibilidad de suprimir los clientes potenciales;
- los operadores de su organismo tienen la posibilidad de anonimizar manualmente los datos de todo interesado;

- SecuTix 360° tiene también una funcionalidad, puesta a su disposición, que le permite según su elección, sus prácticas, su sector de actividad y las disposiciones que le son aplicables, detectar los contactos inactivos durante más de X meses y suprimirlos/anonimizarlos en masa:



- después de haber pasado una cuenta operador al estado «suspendida», puede anonimizarla simplemente reemplazando sus apellidos/nombre/correo electrónico/etc. por XXXX. La anonimización de los datos se convierte en irreversible durante la supresión de los registros, es decir, después de un plazo de 12 meses (cf. duración de conservación de los logs). Atención, es imposible modificar/anonimizar el código de conexión de los operadores. También, es responsabilidad de los administradores que crean los operadores no introducir una información que permita identificar al individuo.

En cualquier caso, cuando finaliza del contrato, sus datos se extraen y se le devuelven en un formato estándar respecto al estado de la técnica y del mercado. A continuación, se suprimen de la solución y siguen las mismas reglas de vaciado que durante una supresión manual (cf. véase arriba).

## 4.6 Datos exactos y actualizados. Derechos de acceso, de rectificación, de supresión y de portabilidad. Derecho a la limitación del tratamiento y derecho de oposición al tratamiento.

### 4.6.1 Principios

De acuerdo a las disposiciones aplicables en materia de protección de datos personales, los datos tratados deben ser exactos y, si es necesario, estar actualizados. El responsable del tratamiento debe tomar medidas apropiadas para que los datos inexactos, desde el punto de vista para el que son tratados, sean borrados o rectificadas.

Las personas interesadas deben tener garantizado un derecho de acceso a sus datos, un derecho a la portabilidad de sus datos y un derecho de rectificación y de supresión de dichos datos.

Además, estas personas disponen de un derecho a la limitación del tratamiento, así como de un derecho de oposición al tratamiento de sus datos.

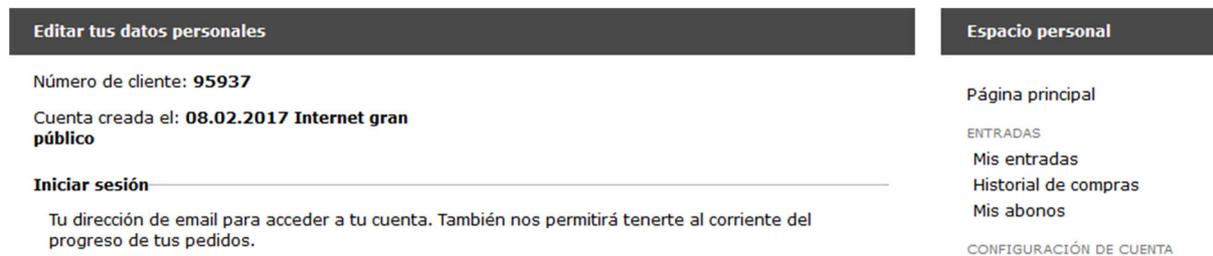
Estas obligaciones deben ser asumidas por el responsable de tratamiento. No obstante, el encargado del tratamiento debe ayudar al responsable de tratamiento a liberarse de su obligación de responder a las solicitudes en que los interesados se le dirigen para ejercer sus derechos citados anteriormente.

#### 4.6.2 La solución SecuTix 360°

En calidad de responsable de tratamiento, debe asegurarse que aporta a los interesados las respuestas previstas por las disposiciones aplicables en caso de ejercicio por estos de sus derechos citados anteriormente, y que sus solicitudes (bajo reserva de que cumplan las condiciones requeridas) se hagan efectivas. A este respecto, se ha ya precisado que en caso de demanda que nos sea dirigida directamente, le informaremos, ya que la respuesta a estas demandas y las acciones que deben desplegarse serán de su sola responsabilidad.

SecuTix 360° dispone de funcionalidades que permiten la gestión de las demandas de rectificación o de supresión de datos presentes en la base de datos de SecuTix 360°.

- los internautas pueden en todo momento modificar los datos de su perfil en su cuenta personal en línea:



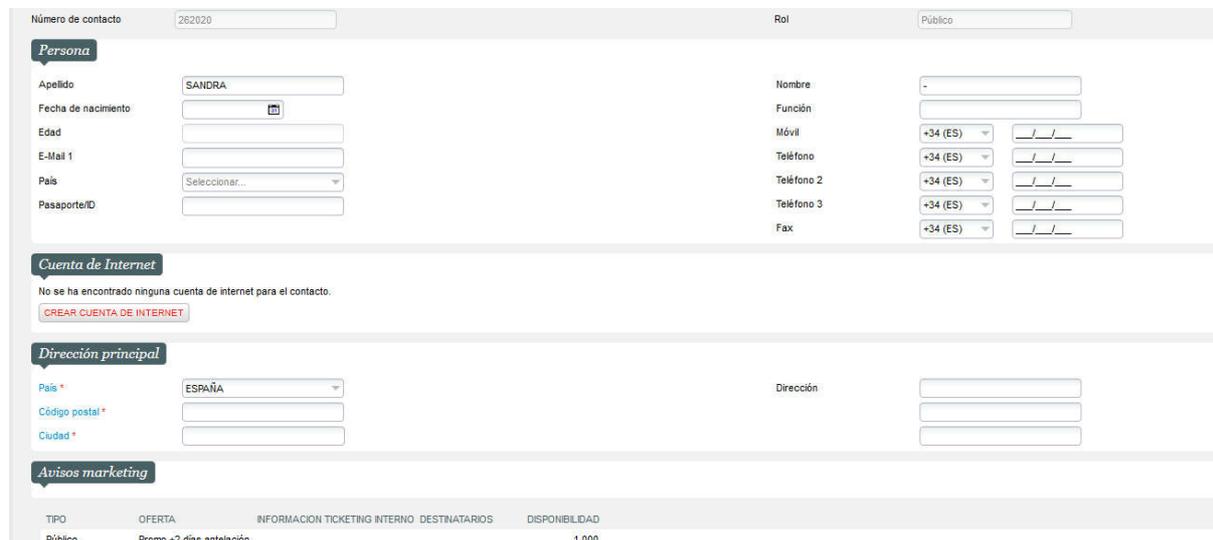
The screenshot shows the 'Editar tus datos personales' (Edit your personal data) section. It includes the following information:

- Número de cliente:** 95937
- Cuenta creada el:** 08.02.2017 **Internet gran público**
- Iniciar sesión** (Login button)
- Tu dirección de email para acceder a tu cuenta. También nos permitirá tenerte al corriente del progreso de tus pedidos.**

On the right side, there is a sidebar titled 'Espacio personal' (Personal space) with the following links:

- Página principal
- ENTRADAS
  - Mis entradas
  - Historial de compras
  - Mis abonos
- CONFIGURACIÓN DE CUENTA

- los operadores de su organismo pueden poner al día las fichas de contactos:



The screenshot shows the contact management form with the following sections:

- Número de contacto:** 262020
- Rol:** Público
- Persona** (Personal information):
  - Apellido: SANDRA
  - Fecha de nacimiento: [input]
  - Edad: [input]
  - E-Mail 1: [input]
  - País: Seleccionar...
  - Pasaporte/ID: [input]
- Cuenta de Internet** (Internet account):
  - No se ha encontrado ninguna cuenta de internet para el contacto.
  - [CREAR CUENTA DE INTERNET](#)
- Dirección principal** (Main address):
  - País: ESPAÑA
  - Código postal: [input]
  - Ciudad: [input]
  - Dirección: [input]
- Avisos marketing** (Marketing notices):
 

TIPO	OFERTA	INFORMACION TICKETING INTERNO	DESTINATARIOS	DISPONIBILIDAD
Público	Promo +2 días antelación			1 000

- sobre las solicitudes de supresión de datos, véase el parágrafo 4.5.

Un contacto puede solicitar el conjunto de informaciones personales que le afectan en el ejercicio de su derecho de acceso o de su derecho a la portabilidad de sus datos. Los operadores de su organismo tienen acceso a los datos de los contactos para responder a estas solicitudes. Además, bajo demanda ante SecuTix SA, un operador de su organismo puede obtener el conjunto de la información almacenada que afecta a un contacto (ficha de contacto, histórico de compra, histórico relacional).

Además:

- el origen de la información de la ficha contacto se indica con la forma «información introducida por el internauta», «información introducida por un operador de su organismo», «información recogida mediante importación de datos»:

☆ *Contacto individual > 262020 Señor, Señora - sandra (Cliente potencial)*

Resumen	General	Marketing	Gestión	Notas	Administración
Creado desde	IMPORT	Creado el	25/07/2016		
Creado por	IMPCTCT_SERV-240	Modificado el	15/08/2017		
Modificado por	STX-73980-pre				

- la fecha de creación de una cuenta personal está disponible en dicha cuenta:

**Editar tus datos personales**

Número de cliente: **95937**

Cuenta creada el: **08.02.2017 Internet gran público**

**Iniciar sesión**

Tu dirección de email para acceder a tu cuenta. También nos permitirá tenerte al corriente del progreso de tus pedidos.

- la fecha de creación de una ficha de contacto y la fecha de la última modificación se indican en la ficha contacto:

☆ *Contacto individual > 262020 Señor, Señora - sandra (Cliente potencial)*

Resumen	General	Marketing	Gestión	Notas	Administración
Creado desde	IMPORT	Creado el	25/07/2016		
Creado por	IMPCTCT_SERV-240	Modificado el	15/08/2017		
Modificado por	STX-73980-pre				

Finalmente, le corresponde gestionar en la solución las solicitudes de limitación del tratamiento o de oposición al tratamiento de los datos.

En cualquier caso, nos comprometemos a aplicar todos los medios para comunicarle, bajo demanda, los elementos en nuestra posesión que permiten aportar una respuesta a las solicitudes de ejercicio de sus derechos por los interesados.

## 4.7 Seguridad de los datos

### 4.7.1 Principios

Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
- la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Deben aplicar medidas de seguridad y de confidencialidad adecuadas. Para obtener recomendaciones en materia de seguridad de los datos, puede consultar: <https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles>.

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento debe realizar, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

Además, en caso de violación de datos personales (a saber, toda violación de la seguridad comportando accidentalmente o de manera ilícita la destrucción, la pérdida, la alteración, la divulgación o el acceso no autorizado a los datos personales objeto de un tratamiento), el responsable del tratamiento debe tomar a su cargo una obligación de notificación ante la autoridad de control competente, en el plazo más corto posible y, si es posible, 72 horas como muy tarde después de tener conocimiento. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento deberá comunicarla al interesado sin dilación indebida.

### 4.7.2 La solución SecuTix 360°

En su calidad de responsable de tratamiento, le corresponde asegurarse que se respeta el conjunto de estas obligaciones.

SecuTix SA, en su calidad de encargado del tratamiento, debe tomar a su cargo la obligación de desplegar medidas de seguridad apropiadas, de notificar al responsable del tratamiento de toda violación de datos personales en el plazo más corto posible después de tener conocimiento de ello, y de forma más general la obligación de cooperar con el responsable de tratamiento para el respeto por este último de sus propias obligaciones (despliegue de las medidas apropiadas de seguridad y análisis de impacto especialmente).

SecuTix SA garantiza el cumplimiento de las exigencias y que ha obtenido los certificados de conformidad según las normas ISO/IEC 27001:2013 y PCI DSS v3.2. Por tanto, SecuTix SA se compromete a aplicar las medidas técnicas y organizacionales de seguridad identificadas en estas normas.

Además, tratándose de la solución SecuTix 360°:

- Los datos se duplican en tiempo real en diferentes discos redundantes.
- Los datos se duplican casi en tiempo real en dos centros de datos distantes varios kilómetros.
- Para proteger los servidores y la solución de forma apropiada, SecuTix SA toma todas las medidas técnicas y organizativas necesarias, especialmente los controles de acceso, la utilización de cortafuegos y programas antivirus actualizados, encriptados SSL y logs/registros durante los cambios manuales de bancos de datos.
- El área de pagos de SecuTix 360° está certificada según PCI DSS y es auditada una vez al año.
- Las contraseñas deben tener un número y una combinación segura de caracteres y de cifras para ser válidas.
- SecuTix 360° posee un plan de continuidad para el paso de un centro de datos al otro.
- Los accesos físicos de personas a los centros de datos están estrictamente controlados mediante código, seguimiento, alarmas, tarjetas de identificación, videovigilancia...
- Los datos enviados al sitio de emergencia están cifrados vía VPN o HTTPS.

Además, de conformidad a nuestras obligaciones, nos comprometemos a cooperar con usted en relación con:

- el cumplimiento por usted de sus propias obligaciones en materia de seguridad y especialmente de confidencialidad de los datos personales;
- la realización por usted de análisis de impacto de los tratamientos sobre la protección de datos personales si la naturaleza de los tratamientos en los que intervenimos lo exige, y de la eventual consulta de la autoridad de control en su caso tratándose de estos mismos tratamientos de datos.

el respeto de su obligación de notificación a la autoridad de control y de información del interesado en caso de violación de datos personales. Con este fin, le notificaremos toda violación de datos personales de la que tengamos conocimiento. Nos comprometemos también a aplicar todos los medios y a comunicarle, a su demanda, la documentación en nuestra posesión que será útil para permitirle, si es necesario, proceder a las notificaciones citadas anteriormente cuando se requieran.

También conviene que tome las medidas técnicas y organizacionales oportunas en su organismo para contribuir al alcance de un nivel apropiado de seguridad de los datos tratados en el ámbito de la solución SecuTix 360°. Así, se recomienda, por ejemplo:

- proteger y mantener los accesos a SecuTix 360° actuales (hardware, software, red, acceso a Internet);

- asegurar la confidencialidad de las contraseñas con las que los operadores de su organismo se conectan a SecuTix 360° y velar para que se despliegue una política de contraseña según las recomendaciones aplicables (cf. véanse a título de ilustración las recomendaciones accesibles aquí: <https://www.cnil.fr/fr/authentication-par-mot-de-passe-les-mesures-de-securite-elementaires>);
- tener al día el antivirus en todos los puestos de trabajo;
- ...

## **4.8 Encargados del tratamiento, encargados de tratamientos adicionales y flujos transfronterizos**

### **4.8.1 Principios**

Áquellos que usan encargados de tratamiento y encargados de tratamiento adicionales para el tratamiento de los datos personales deben ser objeto de un marco contractual específico que comporte un cierto número de cláusulas obligatorias.

Los flujos transfronterizos de datos hacia Estados no miembros de la UE y no reconocidos como garantes de un nivel de protección adecuado de los datos pueden ser aplicados únicamente mediante acreditación de garantías suficientes, especialmente contractuales.

### **4.8.2 La solución SecuTix 360°**

En el marco de la operativa de la solución SecuTix 360° para su organismo, podemos tener que tratar datos personales por su cuenta, en calidad de encargado del tratamiento. Los documentos contractuales que ofrecemos comportan una cláusula conforme a las exigencias del RGPD que tienen el objetivo de enmarcar nuestras prestaciones en calidad de encargado del tratamiento por su cuenta en materia de tratamiento de datos personales.

Con vistas a la operativa de esta solución, las diferentes entidades de nuestro grupo pueden también precisar tratar datos personales por su cuenta. A este respecto, le informamos que las entidades de nuestro grupo están principalmente establecidas en la Unión Europea o en Suiza, país que garantiza un nivel adecuado de protección de datos. Sin embargo, hay una entidad establecida en Vietnam. Conforme a las disposiciones aplicables en materia de protección de datos, los flujos transfronterizos de datos hacia esta entidad están enmarcados por una convención de flujos transfronterizos elaborados según la base de modelos suizos propuestos por el Préposé Fédéral à la Protection des Données et à la Transparence (PFPDT) y los modelos europeos establecidos por la Comisión Europea.

Además, para suministrarle el conjunto de funcionalidades propuestas en el marco de la solución SecuTix 360°, podemos, en función de las prestaciones y servicios que haya suscrito, tener que recurrir a encargados de tratamiento adicionales cuya lista encontrará en el Anexo 2.

## 4.9 Utilización de datos con fines de marketing

### 4.9.1 Principios

Tratándose de la utilización de datos con fines de marketing, son aplicables los principios siguientes:

- necesidad de un consentimiento expreso (opt-in mediante una casilla de verificación no premarcada redactada de manera positiva) para los intercambios por correo electrónico, sms, mms, fax y sistema automatizado de comunicaciones electrónicas (cf. Llamadas automatizadas, por ejemplo);
- necesidad de una ausencia de oposición previa para los intercambios por correo electrónico o telefonía con intervención humana;
- cada envío (especialmente por correo electrónico y sms) debe ofrecer un medio simple y gratuito de anulación de suscripción (derecho de oposición) para las comunicaciones por esta vía, junto con la necesidad, para los envíos por correo electrónico de indicar un objeto en relación con el contenido y precisar por cuenta de quién se envía.

En lo que concierne a los envíos por correo electrónico, sms o mms, conviene precisar que una excepción al consentimiento puede ser ejercida siempre que se cumplan las condiciones acumulativas siguientes:

- los datos del destinatario han sido proporcionadas por él mismo con ocasión de una venta o de una prestación de servicio;
- la comunicación cumple las disposiciones aplicables en materia de protección de datos personales, especialmente las que afectan a la información de las personas;
- la prospección directa afecta productos o servicios análogos ofrecidos por la misma persona física o jurídica;
- se debe ofrecer al destinatario, de forma expresa y sin ambigüedad, la posibilidad de oponerse, sin gastos, exceptuando los relacionados con la transmisión del rechazo, y de forma simple, a la utilización de sus datos de contacto en el momento en que se le envía un correo electrónico comercial.

### 4.9.2 La solución SecuTix 360°

SecuTix 360° le ofrece funcionalidades de marketing que permiten dirigir mensajes publicitarios a sus contactos (clientes y clientes potenciales). Sin embargo, será considerado como único responsable de la utilización que haga de estas funcionalidades, y debe respetar los principios indicados a continuación.

Para permitirle realizar sus operaciones de marketing conforme a los principios citados anteriormente, SecuTix SA ha implementado las funcionalidades siguientes:

- el formulario de creación de cuenta personal en línea por un internauta vía nuestra interfaz o nuestro módulo web incluye un texto destinado a integrar la mención de información cuya redacción deberá realizar. Esta mención deberá ser completada por usted con las casillas de verificación (no premarcadas) y las frases de recogida de consentimiento / oposición . Estos elementos se configuran en el «punto de venta» de internet;

- los internautas disponen por defecto de varias funcionalidades en su cuenta personal en línea, como sigue:
  - inscripción/anulación de suscripción al/los boletines electrónicos (adaptable a sus necesidades):

Me gustaría recibir o ya recibo el boletín informativo \*  Sí  No

- elección de la recepción de los medios de comunicación y de los remitentes (adaptable a sus necesidades):

#### Editar tus datos personales

Número de cliente: **95937**

Cuenta creada el: **08.02.2017 Internet gran público**

#### Iniciar sesión

Tu dirección de email para acceder a tu cuenta. También nos permitirá tenerte al corriente del progreso de tus pedidos.

- en la taquilla (en el back-office):
  - un operador de su organismo puede determinar si un contacto acepta recibir comunicaciones de su organismo, de socios de su organismo o de terceros:

#### Datos legales

Acepto comunicación de la institución  sí  no

Acepto transmisión de datos a terceros  sí  no

Acepto comunicación de un socio.  sí  no

- un operador puede determinar los canales de comunicación deseados por el contacto:

#### Comunicación

Canal de communication préfééré

SMS/MMS  sí  no

Teléfono  sí  no

Correo electrónico  sí  no

Correo  sí  no

Estado bounce

- por defecto, no se ha marcado ninguna opción. Así toda «marca» resulta necesariamente de una acción positiva del internauta o del operador. Conviene que tenga en cuenta estas reglas de gestión para realizar las operaciones de marketing conforme a los principios apuntados en el parágrafo 4.9.1.

Además, conviene que tenga en cuenta las solicitudes de oposición a la prospección puestas en su conocimiento por los interesados, en función de los medios con los que se dirige a ellos (marcando los medios de comunicación utilizados con «no»).

Con fines de sensibilización de los usuarios de la solución, SecuTix 360° integra una mención de advertencia a su atención en las pantallas que permiten la realización de operaciones de prospección comercial, redactado de la forma siguiente:

*«En el marco de las operaciones de prospección comercial que desee desplegar, le recordamos que conviene que tenga en cuenta los principios siguientes:*

- *está prohibida la prospección de un contacto mediante un medio de comunicación marcado con «no»;*
- *la prospección por correo electrónico, sms, mms, telecopia e incluso un sistema automatizado de comunicaciones electrónicas es posible únicamente vía un medio de comunicación marcado con «sí»;*
- *la prospección por correo postal o por telemarketing es posible con un medio de comunicación marcado con «sí» o no marcado (cf. ni «sí» ni «no»).*»

Los boletines electrónicos enviados por SecuTix 360° según sus instrucciones comportan, por lo menos, la información que permite a los destinatarios ejercer su derecho de oposición (i.e. su voluntad de no recibir más envíos de este tipo). Efectivamente, en estas comunicaciones, un enlace permite anular la suscripción. La anulación de la suscripción se tiene en cuenta automáticamente en SecuTix 360° (marca en «no»):

Pour ne plus recevoir notre lettre d'information, des offres promotionnelles exclusives et les eNotes de programme : [cliquez ici](#) .

Para incluir esta funcionalidad en sus envíos por correo electrónico, incluya en la configuración mensajes de correo electrónico configurados según una de las dos soluciones siguientes:

- en un correo electrónico enviado, el operador de su organismo configura el enlace «URL de anulación de suscripción». La anulación de suscripción tiene lugar automáticamente cuando el contacto hace clic en el enlace:

Unsubscribe URL <https://citm-daysoff.shop.secutix.com/api/1/redirect/unsubscribe?id=xEiA2Zzp1h7SfxnCB%2FV9yP1qDbw%3D>

- en el correo electrónico enviado, el operador de su organismo pone un enlace que le redirige hacia el espacio personal. El contacto va a poder desmarcar su suscripción o modificar sus preferencias en su espacio personal.

## **4.10 Procedimientos**

### **4.10.1 Principios**

Cada responsable del tratamiento lleva un registro de las actividades de tratamiento efectuadas bajo su responsabilidad.

Cada encargado llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable del tratamiento.

Estos registros deben presentarse en forma escrita, incluido formato electrónico. El responsable del tratamiento o el encargado pondrán el registro a disposición de la autoridad de control que lo solicite.

### **4.10.2 La solución SecuTix 360°**

En calidad de responsable de tratamiento, debe integrar los tratamientos de datos personales aplicados a través de la solución SecuTix 360° en su registro «responsable de tratamiento» de las actividades de tratamiento.

Por nuestro lado, en calidad de encargado de tratamiento, integramos los tratamientos de datos personales aplicados a través de la solución SecuTix 360° por su cuenta en nuestro registro «encargado del tratamiento» de las actividades de tratamiento.

## Anexo 1. Lista de verificación a completar por su organismo que afecta a los tratamientos de datos personales aplicados en la solución SecuTix 360°

Pregunta	Respuesta	comentario
Finalidades de utilización de la solución prestaciones/servicios suscritos		Objetivos perseguidos, funcionalidades de aplicación elegidas, usos reales o previstos, finalidades que responden a disposiciones específicas, consecuencias del tratamiento,...
Datos recogidos y tratados en la solución	...	Detalles de los datos que el cliente desea recopilar y procesar cuando utiliza la solución SecuTix 360
Personas autorizadas a añadir nuevos campos + procedimiento para realizar las solicitudes en este sentido ante SecuTix SA		Comunicar la identidad de las personas autorizadas en el cliente + especificar cómo se pueden hacer las solicitudes a SecuTix SA
Personas autorizadas a añadir nuevos criterios de segmentación + procedimiento para realizar las solicitudes en este sentido ante SecuTix SA		Comunicar la identidad de las personas autorizadas en el cliente + especificar cómo se pueden hacer las solicitudes a SecuTix SA
Personas autorizadas a añadir nuevos criterios de informes/extracciones + procedimiento para realizar las solicitudes en este sentido ante SecuTix SA		Comunicar la identidad de las personas autorizadas en el cliente + especificar cómo se pueden hacer las solicitudes a SecuTix SA
Destinatarios de los identificadores de "administrador"		Es entonces responsabilidad del cliente determinar y configurarse las personas que pueden tener acceso a los datos, así como los detalles de las autorizaciones a los datos, pantallas, funcionalidades (ej: consulta, entrada, reporte / extracción,...).
Duración de conservación de los datos deseada en la solución		La solución SecuTix 360° ofrece una funcionalidad de gestión de vida útil que proporciona al cliente los medios para establecer por sí mismo la vida útil deseada.
Contacto en el organismo para las solicitudes de ejercicio de sus derechos para las personas interesada		Comunicar la identidad y la información de contacto al cliente
Contacto en el organismo en caso de violación de datos		Comunicar la identidad y la información de contacto al cliente

Persona de referencia en materia de protección de datos

Comunicar la identidad y los datos de contacto del responsable de la protección de datos del cliente, o al menos del referente de la "protección de datos personales".

Otras instrucciones de la organización a SecuTix

Especifique cualquier otra instrucción del revendedor a la atención de SecuTix SA

## Anexo 2. Lista de los encargados de tratamiento posteriores de SecuTix SA

Nombre	Actividad	País	Datos personales transferidos
Amazon Web Services	Alojamiento de archivos públicos	EEUU	No
Google Maps for Work	Normalización, validación y autosugestión de direcciones postales	EEUU	No
Pca Predict	Normalización, validación y autosugestión de direcciones postales	UK	No
Ingenico ePayment	Prestatario de servicio de pago	Francia/Bélgica	Sí
Datatrans	Prestatario de servicio de pago	Suiza	Sí
Orange Business Services – Contact Everyone	Expedición de SMS	Francia	Sí
MaxMind	Geolocalización de direcciones IP	EEUU	Sí
EFSTA	Recibos fiscales	Austria	Sí
Nazaries	servicio cliente	España	Sí
SecuTix SA	Distribuidor, servicio cliente	Francia	Sí
SecuTix Iberia S.L.	Distribuidor	España	Sí
SecuTix Ltd	Distribuidor	UK	Sí
Elca Informatique SA	Desarrollo de software, nuevo cliente onboarding, servicio cliente, explotación y mantenimiento, alojamiento	Suiza	Sí
Elca Spain	Desarrollo de software e integración, servicio cliente	España	Sí
Elca Information Technology Ltd	Desarrollo de software, nuevo cliente onboarding, servicio cliente, explotación y mantenimiento	Vietnam	Sí
Eric David	Desarrollo de software, servicio cliente, onboarding	Suiza	Sí
Agorasophia Edutainment Spa Management	Ventas y onboarding	Italia	Sí
Swantegy USA LLC	Ventas y onboarding	EEUU	Sí
Softjour, Inc	Ventas y onboarding	EEUU	No